Empresa de Logística
LOGIBUR

Universidad de Burgos

Autor del proyecto: Héctor Alonso García
Tutor del proyecto: Prof. Miguel Ángel Davara Rodríguez
Directores del Magíster:
Dr. Emilio S. Corchado Rodríguez
Dr. Álvaro Herrero Cosío

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

UNIVERSIDAD DE BURGOS
II Edición. Burgos, Septiembre 2010.

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

Índice

Introducción

El presente trabajo pretende reflejar los conocimientos adquiridos en el Magíster en Asesoría y Consultoría en Tecnologías de la Información y las Comunicaciones de la Universidad de Burgos.

El trabajo se divide en cinco grandes bloques: Protección de Datos, Comercio Electrónico, Propiedad Industrial, Contratación Informática y Administración Electrónica.

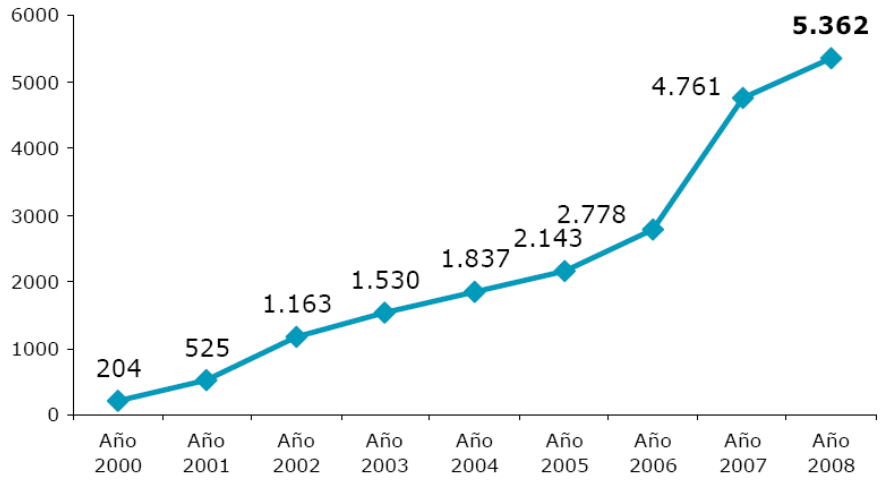
Para cada uno de estos bloques se encuentra una serie de apartados mostrando información teórica, que sirve de base para la realización de una sección en la que se indica la aplicación práctica en la empresa.

Logística y LOGIBUR

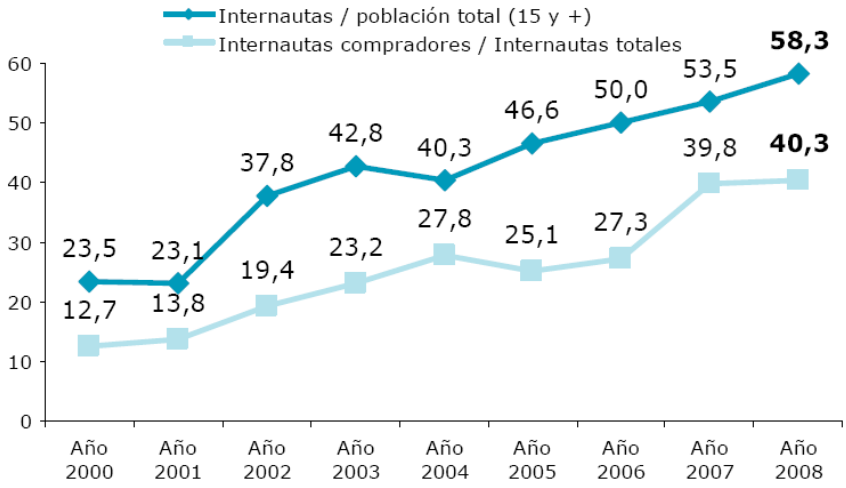
Todos los estudios realizados recientemente sobre el uso del comercio electrónico (Asociación Española de Comercio Electrónico, Red.es, yStats.com, The Center for Retail Research, etc…) coinciden en el crecimiento que está experimentando la venta on-line en los últimos años y su tendencia a seguir continuando.

Se estima que en España, más de 9 millones de personas, compran de manera habitual por Internet.

La facturación del comercio electrónico de tipo B2C en 2008 alcanzó, en España, los 5.362 millones de euros, según el informe de Comercio Electrónico de Red.es realizado por el ONTSI, En el siguiente gráfico se puede observar la tendencia de crecimiento que experimenta este tipo de comercio:



Este crecimiento se ve reforzado por el aumento de usuarios de Internet que tiene como consecuencia un mayor número de personas que utilizan esta forma de compra.



La logística puede definirse como la parte de la gestión de la cadena de suministro que planifica, implementa y controla el flujo y el almacenamiento eficaz y eficiente de los bienes, servicios e información relacionada desde el punto de origen al punto de consumo con el objetivo de satisfacer los requerimientos de los consumidores.

Se puede observar fácilmente la unión entre comercio electrónico y logística ya que las empresas necesitan de una buena logística que se encargue de suministrar todo los bienes necesarios para el correcto funcionamiento de la empresa.

El auge del comercio electrónico, ofrece grandes posibilidades a empresas de logística, debido al aumento de usuarios que realizan compras por Internet.

El último estudio sobre comercio electrónico B2C de Red.es refleja dos datos destacables:

- El 59,5% de usuarios que tiene inconvenientes con la compra es debido a problemas logísticos. Los usuarios alegan retrasos en la recepción y casi el 20% declara que ha recibido el pedido con desperfectos.
- El 7,5% de no compradores declaran que si la Red les generara más confianza en temas relacionados con la recepción y posible devolución del producto, estarían más predispuestos a realizar compras on-line.

LOGIBUR nace con la pretensión de aprovechar este auge del comercio electrónico. La calidad de sus servicios es uno de los puntos clave de la empresa. Gracias a ello, LOGIBUR puede llegar a importantes acuerdos con empresas que precisen de los servicios logísticos que la empresa ofrece.

Protección de Datos

Antecedentes

La Ley Orgánica de Protección de Datos (LOPD) es la ley que regula actualmente la protección de datos en España. Pero antes de esta ley ya existía protección de datos con la Ley Orgánica de Regulación del Tratamiento Automatizado de los Datos de carácter personal (LORTAD). Esta ley fue creada en 1992 y el motor que impulsó su promulgación fue el mandato constitucional contenido en el artículo 18.4 de nuestra Constitución, el cual dice 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."*

El Gobierno fue el encargado de presentar el proyecto en las Cortes Generales. El estudio y aprobación del mismo por las Cortes, fue propiciado por tres documentos claves:

- *El Convenio de Europa*, de 28 de enero de 1981, para la protección de las personas con relación al tratamiento automatizado de datos de carácter personal, ratificado por España el 27 de enero de 1984.
- El *Acuerdo de Schengen*, de 14 de junio de 1985, relativo a la supresión gradual de los controles entre las fronteras comunes.
- *La Propuesta de Directiva del Consejo de la Comunidad Económica Europea*, de 24 de septiembre de 1990, relativa a la protección de las personas en lo referente al tratamiento de datos personales (modificada el 15 de octubre de 1992), hoy Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995.

Los orígenes de la LOPD se encuentran en agosto de 1998, momento en el que el gobierno remite al Parlamento un Proyecto de Ley de modificación de la LORTAD. La LORTAD esta basada en un Proyecto de Directiva anterior (del 24 de septiembre de 1990) y por lo tanto no se había tenido en cuenta ciertos aspectos de la Directiva comunitaria 95/46/EC. Por esta razón fue necesaria la modificación de la Ley.

Pero del Proyecto de Ley, que se presentó en las Cortes Generales como una simple transposición de una Directiva para adecuar la LORTAD, surgió finalmente una nueva Ley con varias modificaciones.

Por esta razón, ante las 114 enmiendas presentadas al proyecto inicial, los diputados encargados de redactar el Informe sobre el Proyecto de Ley decidieron proponer un texto nuevo completo derogando la Ley anterior. Después de unos largos trámites parlamentarios, el Congreso de los Diputados aprobó, a finales de noviembre de 1999, el texto de la nueva Ley conocida como LOPD, la cual carece de Exposición de Motivos que explique qué razones han llevado a su aprobación, cuando la LORTAD había sido aprobada tan sólo siete años antes.

La nueva Ley surge gracias a:

- El lobby de todos los sectores empresariales afectados por la Ley de 1992, (empresas de marketing, instituciones de crédito, entidades financieras y aseguradoras).
- De las peculiaridades que implica el modelo español de Estado de Comunidades Autónomas.
- De los acuerdos parlamentarios que precisaba un Gobierno que, en aquel entonces, no tenía mayoría en las Cámaras legislativas para aprobar esta Ley.

Como ya se ha dicho, el objeto de la LORTAD estaba claramente definido, era el desarrollo del artículo 18.4 de la Constitución Española. Con ello se trataba de frenar el uso de las nuevas tecnologías en referencia al peligro para el honor y la intimidad de los ciudadanos.

Sin embargo, el objeto de la LOPD es mucho más amplio:

- Garantizar y proteger, en lo que concierne a los datos de carácter personal, las libertades públicas y los derechos fundamentales de las personas físicas, especialmente su honor e intimidad personal y familiar.
- Es aplicable tanto a los ficheros públicos como privados que contengan datos de carácter personal.

Normativa

La LOPD se estructura en siete Títulos, conformados por 49 artículos y 6 disposiciones adicionales, 3 disposiciones transitorias, una disposición derogatoria y 3 disposiciones finales, que regulan y disponen:

- El objeto y ámbito de aplicación de la Ley.
- Los principios en materia de protección de datos.
- Los derechos de las personas.
- Régimen jurídico de los ficheros, tanto de titularidad privada como pública.
- Regulación de la transferencia internacional de datos.
- El régimen jurídico de la Agencia Española de Protección de Datos.
- Régimen de infracciones y sanciones.

Esta estructura conforma los principios básicos en materia de protección de datos de carácter personal que deben ser completados con:

- *Las instrucciones de la Agencia Española de Protección de Datos*: No se trata de normas, sino de la base de los criterios establecidos por la Agencia y tiene el objeto de aclarar la interpretación de la Ley tanto desde el punto de vista del tratamiento como de los principios establecidos en la misma.
- *Recomendaciones de la Agencia*: Se trata de documentos desarrollados por la Agencia a partir de las inspecciones de oficio que realiza la misma en sectores en los que la Agencia considera que la protección de datos se encuentra de algún modo comprometida.

El 19 de enero de 2008 se publicó en el Boletín Oficial del Estado el Real Decreto por el que se aprueba el reglamento de desarrollo de la ley orgánica 15/1999, de 13 de diciembre de protección de datos de carácter personal (RD 1720/2007) que deroga al anterior Reglamento de desarrollo promulgado por el Real Decreto 994/1999, de 11 de junio.

El Reglamento de desarrollo es creado con el objetivo de no reiterar los contenidos de la LOPD y de desarrollar los mandatos contenidos en la misma.

El reglamento se estructura en nueve títulos cuyo contenido desarrolla los aspectos esenciales en esta materia:

- *Título I.*
    - Contempla el objeto y ámbito de aplicación del reglamento.
    - Se aclaran las definiciones de los conceptos de ficheros y de tratamientos relacionados con actividades personales o domésticas.
    - Se aportan una serie de definiciones que ayudan a comprender la norma dada su excesiva tecnificación.
    - Se fija el criterio a seguir en materia de cómputo de plazos con el fin de homogeneizar el trato de los ficheros públicos respecto de los privados.
- *Título II.*
    - Establece los principios en materia de protección de datos de carácter personal.
    - Establece el modo de captación del consentimiento atendiendo especialmente a los servicios de comunicaciones electrónicas y a la captación de datos de los menores.
    - Se aporta mayor definición y concreción a la figura del encargado del tratamiento que se completa con lo dispuesto en el Título VIII en materia de seguridad dotando de un marco coherente a la actuación del encargado.
- *Título III.*
    - Se ocupa de regular los derechos de las personas, que constituyen el conjunto de facultades que emanan del derecho fundamental a la protección de datos y sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre

sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer.

- *Títulos IV a VII.*
    - Aportan claridad en la aplicación de criterios específicos a determinados tipos de ficheros de titularidad privada:
        - Ficheros sobre solvencia patrimonial y crédito.
        - Ficheros utilizados en actividades de publicidad y prospección comercial.
    - Además, tratan sobre el conjunto de obligaciones materiales y formales que deben conducir a los responsables a la creación e inscripción de los ficheros, los criterios y procedimientos para la realización de las transferencias internacionales de datos, y, sobre la regulación de los "Código tipo".
- *Título VIII.*
    - Está dedicado a regular la seguridad en lo relativo a la atribución de los niveles de seguridad, fijación de las medidas a adoptar en cada caso y en la revisión de éstas en caso de que resulte necesario.
    - Se ordena y aclara el contenido y las obligaciones vinculadas al documento de seguridad y se contempla la posibilidad de regular la materia de modo que contemple múltiples formas de organización tanto material como personal de la seguridad.
    - Por último, regula el conjunto de medidas destinadas a los ficheros y tratamientos no automatizados
- *Título IX.*

- Regula y define los procedimientos tramitados por la Agencia Española de Protección de Datos, tratando, únicamente aquellas especialidades que diferencian, a los distintos procedimientos tramitados por la Agencia, de las normas generales contenidas en la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, cuya aplicación se declara supletoria al reglamento.

Definiciones

A continuación se detallan una serie de definiciones útiles para el correcto entendimiento de los apartados posteriores.

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.

Autenticación

Procedimiento de comprobación de la identidad de un usuario.

Cesión o comunicación de datos

Tratamiento de datos que supone su revelación a una persona distinta del interesado.

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.

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.

Datos de carácter personal

Cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables.

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.

Encargado del tratamiento

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

Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

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.

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.

Fuentes accesibles al público

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. En el caso de Colegios profesionales, podrán indicarse como datos de pertenencia al grupo los de número de colegiado, fecha de incorporación y situación de ejercicio profesional

Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación.

Para que los supuestos indicados puedan ser considerados fuentes accesibles al público, será preciso que su consulta pueda ser realizada por cualquier persona, no impedida por una norma limitativa, o sin más exigencia que, en su caso, el abono de una contraprestación.

Incidencia

Cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos.

Identificación

Procedimiento de reconocimiento de la identidad de un usuario.

Procedimiento

Secuencia de operaciones que se realizan para desarrollar cierto cometido o resolver un determinado problema.

Procedimiento de disociación

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

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.

Recurso

Cualquier parte componente de un sistema de información.

Responsable del fichero o tratamiento

Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados.

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.

Sistemas de información

Conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y 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 susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

Usuario

Sujeto o proceso autorizado para acceder a datos o recursos.

Bloqueo de datos

La identificación y reserva de los datos (un registro o varios registros) con el fin de impedir su tratamiento. El bloqueo puede producirse por iniciativa del responsable del fichero o a instancia del afectado.

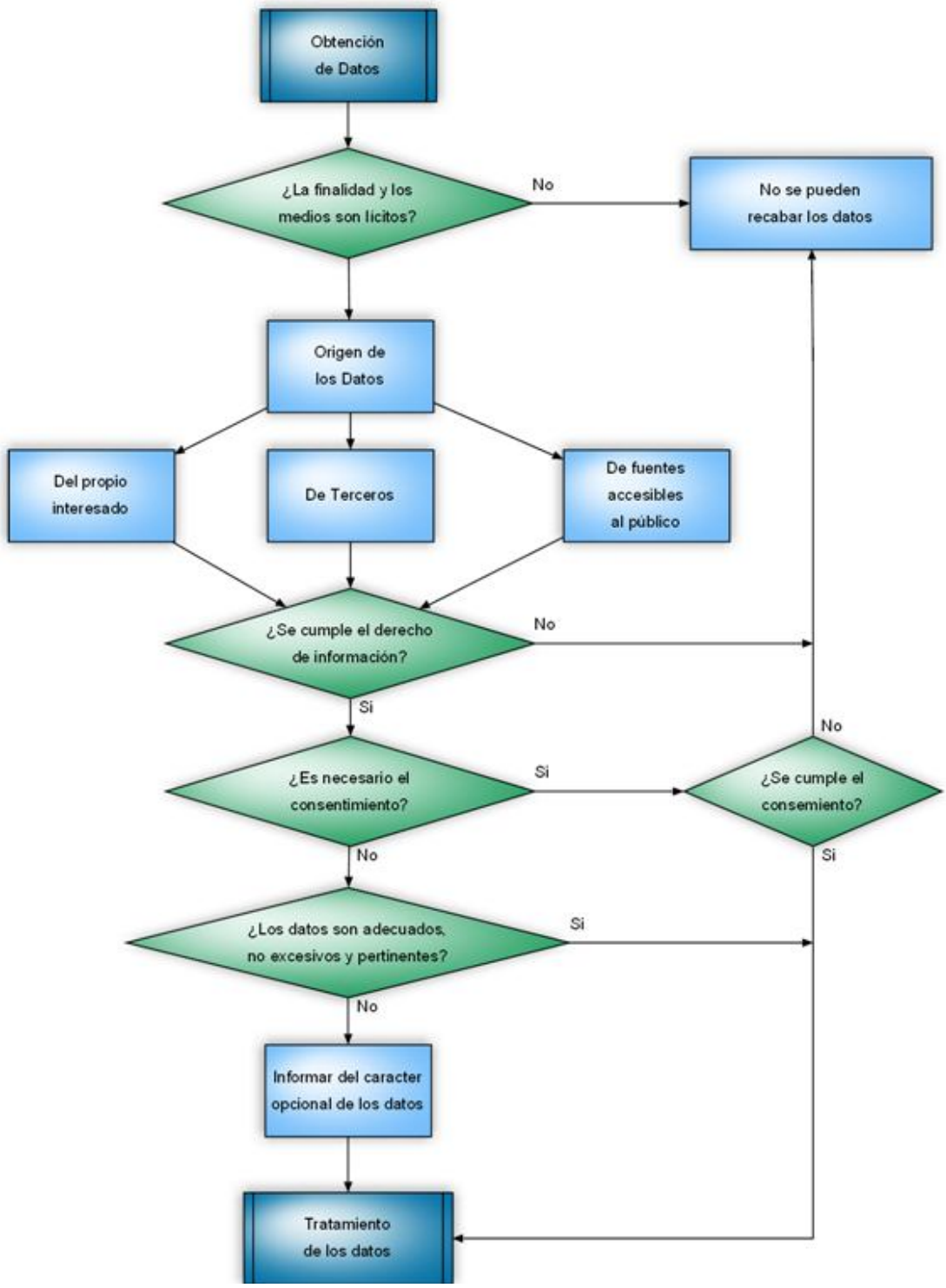
Fases del tratamiento

Existen tres fases fundamentales por las que puede atravesar el proceso del tratamiento de los datos: la recogida, tratamiento y posibles comunicaciones y cesiones de los mismos:

- *Primera fase.* Momento de recabar los datos, bien sea del interesado o de un tercero. Es importante en este momento la licitud y lealtad de la recogida de datos, juntos con las características de conocimiento y, en su caso, consentimiento del afectado.
- *Segunda fase.* El tratamiento de datos, que pueden ser cruzados y relacionados junto con otros datos, buscando definir un perfil determinado del afectado que incluso él mismo llega a desconocer.
- *Tercera fase.* El momento de la utilización y, en su caso, comunicación a terceros de los resultados del tratamiento, conocida esta última como cesión o comunicación de datos, en la que, se tiene también en cuenta el conocimiento y consentimiento del titular.

En las tres fases están presentes los principios de la protección de datos, los derechos de los ciudadanos y los procedimientos que permitan ejercer esos derechos o, en su caso, es tutelen o sirvan como control del cumplimiento de la norma.

En el siguiente gráfico se pueden observar los pasos necesarios para la obtención de datos de carácter personal de manera adecuada

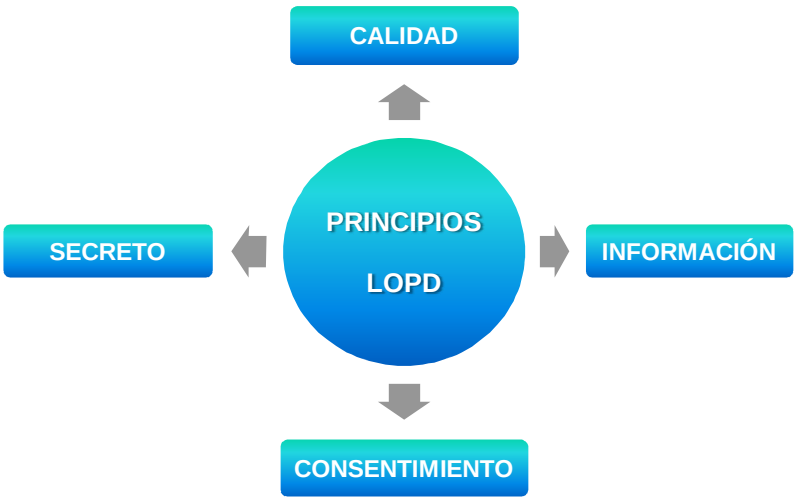

Obtención de Datos
¿La finalidad y los medios son lícitos?
No
No se pueden recabar los datos
Origen de los Datos
Del propio interesado
De Terceros
De fuentes accesibles al público
¿Se cumple el derecho de información?
No
Si
¿Es necesario el consentimiento?
Si
¿Se cumple el consemiento?
No
Si
No
¿Los datos son adecuados, no excesivos y pertinentes?
Si
No
Informar del caracter opcional de los datos
Tratamiento de los datos

Principios y derechos de la Protección de Datos

Principios de la protección de datos

Este apartado de la LOPD (artículos 4 a 12) constituye la base en el tratamiento de datos de carácter personal centrándose en los aspectos relacionados con la manipulación y gestión de la información de un modo general y exponiendo una serie de principios básicos que deberán ser contemplados por cualquier ente, público o privado, que desee manipular información de carácter personal.

Los cuatro principios básicos en materia de protección de datos pueden verse en el siguiente gráfico:



Consentimiento del titular de los datos

El Artículo 6 de la ley trata sobre este principio que representa la obligación de requerir el consentimiento del afectado para recoger sus datos.

El consentimiento puede ser de tres clases:

- *Expreso:* Se manifiesta mediante un acto positivo o declarativo de voluntad. Puede ser de forma oral o escrita. En cualquier caso para probar que se ha emitido, deberá utilizarse uno de los medios de prueba admitidos por el derecho.
- *Tácito:* Se produce cuando pudiendo manifestar un acto de voluntad contrario, éste no se lleva a cabo, es decir, cuando el silencio se presume como un acto de aceptación.
- *Presunto:* No se deduce ni de una declaración ni de un acto de silencio positivo, sino de un comportamiento o conducta que implica aceptación de un determinado compromiso u obligación.

Sin embargo, existen excepciones, ya que, siempre que no se vulneren los derechos y libertades fundamentales del interesado, no será preciso su consentimiento en los siguientes casos:

- Cuando los datos se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias.
- Cuando se refieran a las partes en una relación negocial (por ejemplo un contrato de arrendamiento), laboral (contratos de trabajo) o administrativa, siempre que sea necesario para el cumplimiento de la relación de que se trate.
- Cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado.
- Cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido.

De todas formas, en los casos en que no es necesario el consentimiento del afectado, se reconoce éste el derecho a quedar excluido del tratamiento de los datos (derecho de oposición), siempre que una ley no disponga lo contrario y existan motivos fundados y legítimos relativos a una concreta situación personal.

Calidad de los datos

El artículo 4 proporciona unas directrices fundamentales sobre la calidad de los datos. Estas directrices van dirigidas hacia el tratamiento legal de los datos obligando a que los datos sean pertinentes, adecuados y no excesivos en relación con el ámbito y finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.

Se pueden destacar los siguientes puntos:

- Los datos de carácter personal se podrán recoger para un uso adecuado, y siempre que no sobrepasen la información necesaria para la finalidad a la que sirven. Además, no se podrán usar para un fin distinto al inicialmente propuesto y serán eliminados cuando este fin haya sido alcanzado y no sea necesario su mantenimiento.
- El responsable del fichero o de tratamiento deberá poner los medios necesarios para comprobar la exactitud de los datos registrados y asegurar su puesta al día, de manera que respondan a la situación actual del afectado.
- En el caso de que los datos sean inexactos, deberán ser cancelados o sustituidos por los correctos.
- Los datos deberán desaparecer del fichero una vez se haya cumplido el fin para el que fueron recabados, es decir, si los datos pierden su finalidad originaria deberán ser cancelados.
- No podrán ser conservados (salvo en el caso en que se decida su mantenimiento por valores históricos, científicos o estadísticos) una vez que dejen de ser útiles para la función prevista, con excepción de la legislación específica prevista al efecto.
- Por último, destacar el último punto de este artículo, en el que se dice, textualmente: *"Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos"*. Cabe destacar que este tipo de actos están recogidos en la ley como faltas muy graves.

Deber de información

El titular del fichero tiene la obligación de informar al afectado cuando se recaban los datos, para que éste pueda conocer quién, cómo y para qué se tratan sus datos. Para esto el interesado debe ser informado antes de que se traten sus datos de lo siguiente:

- La existencia del fichero o tratamiento de datos, la finalidad de la recogida y los destinatarios de la información.
- El carácter optativo y obligatorio de las preguntas contenidas en el cuestionario.
- Las consecuencias que puede tener la obtención de datos, así como la posibilidad de negarse a suministrarlos.
- La identidad y dirección del responsable del tratamiento.
- La posibilidad que tiene de cancelar y modificar estos datos (derechos de acceso, rectificación, cancelación y oposición)
- En el caso de que los datos no hayan sido directamente pedidos al interesado la empresa tiene el deber de comunicárselo al usuario en un plazo máximo de 3 meses desde su inclusión en el registro de datos. Esto no se contempla cuando los datos sirvan para fines históricos, científicos o estadísticos, ni en el caso de datos públicos (nombre, dirección) que puedan ser usados para publicidad. En este último caso tan solo se le informará al interesado de sus derechos y del origen de los datos cuando reciba dicha publicidad.

Existen algunas excepciones al deber de información, entre las que cabe destacar:

- Cuando los datos proceden de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial: En este caso, habrá de informarse en cada comunicación dirigida al interesado del origen de los datos, de la identidad del responsable del tratamiento y de los derechos que le asisten. Esto es importante porque las comunicaciones que se quieran realizar con información contenido en ficheros adquiridos legalmente de empresas con fines publicitarios, deben contener este aviso, es decir que todos los mails que se envíen para hacer publicidad de la empresa, deberán incluir información del origen de los datos para cumplir con las obligaciones que marca la ley.

- La información referida al carácter obligatorio u optativo de la información, las consecuencias sobre la obtención de datos y la posibilidad de ejercer los derechos del titular de los datos, no es necesaria si su contenido se deduce claramente de la naturaleza de los datos personales que se solicitan o las circunstancias en que se recaban.

Por otro lado, si los datos no han sido recabados directamente del interesado, éste deberá ser informado, de forma expresa, dentro de los tres meses siguientes al momento del registro de los datos.

Datos especialmente protegidos

Existe una categoría de datos que la LOPD denomina "especialmente protegidos" y que son aquellos datos a los que la norma otorga un mayor grado de protección, imponiendo especiales obligaciones respecto de los mismos, tales como la necesidad de obtener el consentimiento expreso, y en su caso por escrito. Estos datos se extraen como conclusión de algunos apartados de la Constitución donde se dice que nadie podrá ser obligado a declarar sobre su ideología, religión o creencias. Los siguientes puntos detallan más claramente el trato que la ley le da a este tipo de datos:

- Solo se podrán tratar los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias con el consentimiento expreso y por escrito del afectado. Las entidades sin ánimo de lucro cuyo fin sea político, religioso, filosófico o sindical están exentas de este requisito.
- Con respecto a los datos sobre salud, raza o vida sexual solo podrán ser tratados cuando el afectado consienta expresamente, cuando la ley así lo disponga o cuando sean datos necesarios para el tratamiento médico.
- De cualquier modo, queda expresamente prohibido por la ley crear ficheros cuya única finalidad sea la de recabar información sobre ideologías, afiliaciones sindicales, religión, creencias, origen racial, o vida sexual.

Sin el consentimiento sólo podrán ser objeto de tratamiento datos sobre ideología, afiliación sindical, religión, creencias, salud, vida sexual y origen racial cuando sean absolutamente necesarios para los fines de una investigación concreta realizada por las Fuerzas y Cuerpos de Seguridad.

Los ficheros exclusivamente dedicados a datos relativos a la ideología, afiliación sindical, religión creencias, origen racial o vida sexual quedan totalmente prohibidos.

Deber de secreto

El deber de secreto es uno de los nueve principios a través de los cuales la LOPD establece las condiciones en que se deben recoger, tratar y ceder los datos de carácter personal para salvaguardar la intimidad y demás derechos fundamentales de los ciudadanos. A través de este principio (artículo 10 de la ley), se establece que el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que permanecen aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo

Por lo tanto, tanto el responsable del fichero como cualquier otra persona que tenga acceso a un fichero de datos de carácter personal están obligados a guardar secreto profesional sobre los datos personales contenidos en dicho fichero, sin embargo cuando alguien vulnera el deber de secreto y comete alguna de las infracciones previstas en la LOPD, la Agencia Española de Protección de Datos va a sancionar por ello únicamente al responsable del fichero y no al autor de la infracción, sin perjuicio, de las posibles acciones civiles y penales que posteriormente se puedan emprender contra la persona que no ha respetado su deber de secreto. Por consiguiente, el responsable del fichero no solo debe preocuparse por respetar su propio deber de secreto, sino también debe asegurarse de que todo el personal a su servicio mantiene la confidencialidad del tratamiento, para lo cual sería recomendable adoptar, al menos, las siguientes medidas:

- *Informar al personal de su deber de secreto:* El responsable del fichero deberá asegurarse de que todo el personal a su cargo (tanto personal interno en régimen

laboral como externos y subcontratado) conoce su obligación de guardar secreto respecto de los datos personales a los que tenga acceso, por lo que sería conveniente informarles del contenido del deber de secreto y de las consecuencias de su incumplimiento a través de algún medio que sirva de prueba en caso de problemas (como ,por ejemplo, a través de cláusulas de confidencialidad en los contratos).

- *Adoptar las medidas necesarias para garantizar la confidencialidad de los datos:* El responsable del fichero debe implantar en su organización las medidas de carácter técnico y organizativo necesarias para impedir que el personal a su servicio pueda revelar datos de carácter personal a otra persona que no sea el titular de los datos.

El responsable del fichero debe tener en cuenta que recoger, tratar y ceder datos de carácter personal vulnerando los principios y garantías establecidas en la LOPD puede ser constitutivo de infracción leve, grave o muy grave según sea el caso de que se trate, pudiendo ser sancionado por la Agencia Española de Protección de Datos (AEPD) con multas de hasta 600.000 euros por la infracción más grave. Las infracciones y sanciones vienen detalladas en el artículo 44 de la ley y se tratan en el apartado *"Infracciones y sanciones"* de este trabajo.

La persona que vulnere el deber de secreto, debe saber que, además de incurrir en alguna de las infracciones previstas en la LOPD, puede estar cometiendo un delito de descubrimiento y revelación de secretos regulados en los artículos 197 a 201 del Código penal.

Comunicación o cesión de datos

Existe la posibilidad de ceder a un tercero los datos personales siempre que sea para fines directamente relacionados con el propietario de los datos y el responsable del archivo, y siempre con el consentimiento previo del primero.

En los Artículos 11 y 12 se pretende regular las condiciones específicas de utilización de datos que han sido recabados por otras personas.

El Artículo 11 se ocupa de la comunicación de los datos que solo podrán ser comunicados a un tercero para el cumplimiento de fines propios del cedente y cesionario. En este apartado se impone con carácter general la obligación de informar al afectado de la indicada comunicación.

Así mismo, en el Artículo 12 se ocupa específicamente del acceso a los datos por parte de un tercero cuando el mismo sea necesario para la prestación de un servicio al responsable del fichero. En este caso no se considera comunicación de datos pero deberá realizarse un contrato por escrito y cumplida la prestación de los servicios con los datos serán destruidos o devueltos al responsable.

En el acceso de datos por cuenta de terceros hay que destacar los siguientes puntos:

- La obligación legal, consistente en que la realización de tratamientos por cuenta de terceros deba estar regulada en un contrato por escrito, u otra forma que permita acreditar su celebración y contenido.
- Dicho contrato deberá incluir, entre otras, las siguientes menciones:
    - Indicación de que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del fichero.
    - El fin del contrato y que los datos no serán utilizados o aplicados con un fin distinto al indicado.
    - Las medidas de seguridad que el encargado del tratamiento está obligado a implementar.

Como siempre, existen una serie de casos en los que no es necesario el consentimiento:

- En el caso de ceder los datos a entes públicos de la Administración o de ámbito jurídico.
- Si se ceden los datos debido a una emergencia médica.
- Si la transferencia de los datos está autorizada por la ley.

Destacar, que cualquiera que reciba los datos deberá atenerse a todas las disposiciones de la LOPD.

Derechos de la protección de datos

Derecho de impugnación de valoraciones

Consiste en la facultad que se concede a las personas para no verse sometidas a las decisiones con efectos jurídicos basadas exclusivamente en un tratamiento de datos destinado a evaluar determinados aspectos de su personalidad o definición de sus características. El afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizado en el tratamiento que sirvió para adoptar dicha decisión.

Derecho de consulta al Registro General de Protección de Datos

Con objeto de conocer la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento, para estar al tanto del uso de sus datos y controlar el perfil creado por estos, cualquier persona podrá consultar, pública y gratuitamente, el Registro General de Protección de Datos para obtener información a tal fin.

Derecho de acceso

Derecho que podrá ejercitar cualquier interesado para solicitar y obtener información gratuita sobre que datos están siendo tratados, el origen de éstos y las cesiones o comunicaciones realizadas o que se prevén realizar. Cuando el interesado sea menor de edad o incapacitado se comprobará que el derecho se ejerce a través de un representante legal.

Derechos de rectificación y cancelación

Otorgan la posibilidad al interesado de exigir al responsable del fichero que cumpla con el principio de calidad de datos, pudiendo solicitarle que rectifique aquellos datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la ley y, en particular, cuando éstos resulten inexactos o incompletos, y que los cancele cuando dejen de ser necesarios para el fin en el que hubieran sido registrados. Con esto se asegura que los datos se mantengan de forma adecuada y no excesiva en relación con el ámbito y finalidades legítimas para las que se recogieron. Los datos, totales o parciales, sobre los que se ejerciten los derechos de rectificación y cancelación podrán ser excluidos de un determinado fichero de datos personales, bien por ser erróneos o por negarse el titula a su tratamiento.

Derecho de oposición

Supone que en los casos en los que no se requiera el consentimiento de éste para el tratamiento de sus datos, y siempre que una ley no disponga lo contrario, pueda oponerse al tratamiento de los mismos cuando existan motivos fundados y legítimos.

Derecho a indemnización

Si los interesados han sufrido un daño o lesión en sus bienes o derechos como consecuencia del incumplimiento de lo dispuesto en la presente ley por el responsable o por el encargado del tratamiento, tienen derecho a ser indemnizados.

La responsabilidad patrimonial se reclamará por vía contencioso administrativa cuando se trate de los ficheros de titularidad pública, o bien ante los Tribunales ordinarios para los ficheros de titularidad privada.

Procedimiento del ejercicio de los derechos

Los derechos de acceso, rectificación, cancelación y oposición es la manera que dispone el interesado de corregir sus datos cuando estos sean inexactos, incompletos, inadecuados o excesivos. En estos supuestos, el titular de los datos puede comunicarse con el responsable del fichero para que éste rectifique los datos y registre los que correspondan o bien para que cancele sus datos y los elimine definitivamente del fichero.

- *Derecho de acceso.*
    - A través del derecho de acceso el interesado tiene derecho a obtener y solicitar información sobre sus datos personales, el origen de dichos datos, así como las cesiones realizadas o que el responsable del fichero prevé llevar a cabo de los mismos. El derecho de acceso sólo podrá ejercitarse a intervalos no inferiores a doce meses, salvo que el afectado acredite un interés legítimo al efecto, en cuyo caso podrá ejercitarlo antes. El responsable del tratamiento deberá resolver la petición de acceso en el plazo máximo de un mes, a contar de la recepción de la solicitud del afectado.
- *Derecho de rectificación.*
    - El ejercicio del derecho rectificación dará lugar a la sustitución de los datos erróneos por los datos correctos, adecuando el tratamiento a la situación real de la persona interesada. El plazo de satisfacción por el responsable del tratamiento es de diez días a contar desde el día siguiente al de la recepción de la solicitud del afectado.
- *Derecho de cancelación.*
    - El ejercicio del derecho de cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo los datos serán definitivamente eliminados de los ficheros. Al igual que ocurre con el

derecho de rectificación, el plazo de satisfacción por el responsable del tratamiento es de diez días.

- *Derecho de oposición.*
    - Mediante el derecho de oposición el afectado puede oponerse, previa petición y sin gastos, al tratamiento de sus datos. Ello sucede, por ejemplo, en los supuestos de tratamientos de datos del afectado con fines de publicidad y prospección comercial, en cuyo caso, a su simple solicitud, dichos datos serán dados de baja del tratamiento, cancelándose las informaciones que sobre el afectado figuren en el fichero.

Los derechos ARCO se ejercitarán ante el responsable del fichero donde se encuentran registrados los datos personales y puede realizarse utilizando dos métodos diferentes, bien utilizando los medios que el propio responsable del fichero disponga para ello (atención al cliente) o bien haciéndole llegar una comunicación por escrito con la información requerida en el artículo 25 del Real Decreto 1720/2007. En cualquier caso, el interesado deberá ejercer sus derechos utilizando una vía que, en caso de problemas, le permita demostrar que ha formulado la solicitud y que esta ha sido recibida por el responsable del fichero (sello del responsable del fichero, burofax, correo certificado etc.).

En el caso de que el ciudadano decida ejercer sus derechos a través de una comunicación por escrito, esta deberá contener la siguiente información (artículo 25 del Real Decreto 1720/2007):

- *Datos del interesado o de su representante.*
    - Se aportará el nombre y apellidos del interesado, acompañando fotocopia del DNI, Pasaporte, o documento válido que lo identifique. En caso de que el solicitante sea un representante del titular de los datos será necesario aportar su nombre, DNI y el documento que acredite la representación.
- *Petición en que se concreta la solicitud de rectificación.*
    - Si lo que se pretende es solicitar la rectificación de los datos, la solicitud deberá indicar a que datos se refiere y la corrección que haya de

realizarse y deberá ir acompañada de la documentación que justifique lo solicitado.

- *Petición en que se concreta la solicitud de cancelación u oposición.*
    - Si lo que se pretende es solicitar la cancelación u oposición de los datos, el interesado deberá indicar a qué datos se refiere, aportando si fuera necesaria la documentación que lo justifique.
- *Forma en la que se desea acceder a la información.*
    - Al ejercitar el derecho de acceso el ciudadano podrá optar por visualizar los datos directamente en pantalla u obtenerlos por medio de escrito, copia o fotocopia, telecopia, correo electrónico o cualquier otro sistema adecuado al tipo de fichero de que se trate.
- *Dirección a efectos de notificaciones, fecha y firma del solicitante.*
- *Documentos acreditativos de la petición que formula.*
    - Solamente cuando fueran necesarios.

En el caso de que la rectificación de los datos sea validada, se dará lugar a la sustitución de los datos erróneos por los datos que ha aportado el interesado al ejercer su derecho, logrando con ello que los datos sometidos a tratamiento respondan con veracidad a la situación real del titular de los datos.

Si se trata de una cancelación de datos, los datos no desaparecen del fichero de forma inmediata, cuando se otorga el derecho de cancelación los datos se bloquean impidiendo su tratamiento pero se mantienen registrados en los ficheros únicamente a disposición de las Administraciones públicas, Jueces y Tribunales hasta que prescriban las posibles responsabilidades nacidas del tratamiento. Cumplido el citado plazo los datos se suprimirán definitivamente del fichero.

Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero dispone de 10 días para comunicar la rectificación o cancelación efectuada al cesionario, para que este, en el plazo de diez días contados desde la recepción de la comunicación proceda a rectificar o cancelar los datos de que se trate

Sin embargo, el responsable del fichero podrá denegar el ejercicio de los derechos de rectificación, cancelación u oposición en los siguientes supuestos:

- Cuando quien solicite el ejercicio sea una persona distinta al titular de los datos y no haya quedado acreditado que actúe en representación de este.
- En los supuestos en que así lo prevea una Ley o una norma de derecho comunitario de aplicación directa o cuando éstas impidan al responsable del tratamiento revelar a los afectados el tratamiento de los datos a los que se refiera el acceso.
- En el caso del derecho de cancelación, el responsable del fichero podrá denegar el ejercicio del derecho cuando los datos deban ser conservados durante unos plazos determinados legalmente o bien porque no han finalizado las relaciones contractuales que justificaron el tratamiento de los datos entre el interesado y el responsable del fichero.

Tutela de Derechos y Sancionador

El interesado tiene un derecho de reclamación ante la Agencia de Protección de datos, en virtud del cual solicita la tutela de sus derechos y puede acudir a la Agencia para cualquier actuación contraria a la ley. Para ello, dispone de dos procedimientos:

Tutela de derechos

El procedimiento de tutela de derechos tiene como finalidad garantizar el ejercicio efectivo de los derechos de acceso, rectificación, cancelación y oposición del afectado. El procedimiento se divide en tres fases:

- *La fase de iniciación:*
  - El procedimiento se inicia mediante escrito del afectado expresando con claridad el contenido de la reclamación y los preceptos de la Ley Orgánica que se consideran vulnerados.
- *La fase de audiencia:*
  - Se dará traslado de la misma al titular del fichero para que en el plazo de quince días formule las alegaciones que estime pertinentes.
- *Fase de resolución:*
  - la Agencia de Protección de Datos resolverá la reclamación en el plazo máximo de seis meses dando traslado de la misma a las partes, una vez realizadas las acciones que estime pertinentes.

Procedimiento sancionador

Los responsables de los ficheros están sujetos al régimen sancionador establecido en la Ley Orgánica. Existe una serie de comportamientos que se califican como infracciones leves, graves y muy graves.

El procedimiento sancionador se iniciará siempre de oficio mediante acuerdo del Director de la Agencia de Protección de datos, bien por denuncia de un afectado o

afectados o por propia iniciativa. El régimen de infracciones y sanciones se enumeran en el anexo II (art. 44 y 45 de la Ley Orgánica).

Infracciones y sanciones

La LOPD establece un régimen sancionador al que se encuentran sujetos tanto los responsables de los ficheros como los encargados de los tratamientos. Este régimen fija tres niveles de infracción, clasificados en leves, graves y muy graves, los cuáles llevan asociadas la imposición de las correspondientes sanciones económicas.

Tipos de infracciones:

- *Leves:*
  - No atender la solicitud del interesado de rectificación o cancelación de los datos sujetos a tratamiento cuando proceda legalmente.
  - No proporcionar la información que solicite la Agencia de Protección de Datos en el ejercicio de las competencias que tiene legalmente atribuidas, en relación con aspectos no sustantivos de la protección de datos.
  - No solicitar la inscripción del fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando no sea constitutivo de infracción grave.
  - Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la LOPD.
  - Incumplir el deber de secreto establecido en el artículo 10 de la LOPD, salvo que constituya infracción grave.
- *Graves:*
  - Proceder a la creación de ficheros de titularidad pública o iniciar la recogida de datos de carácter personal para los mismos, sin autorización de disposición general.
  - Proceder a la creación de ficheros de titularidad privada o iniciar la recogida de datos de carácter personal para los mismos con finalidades

distintas de las que constituyen el objeto legítimo de la empresa o entidad.

- Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos de que éste sea exigible.
- Tratar los datos de carácter personal o usarlos posteriormente infringiendo los principios y garantías establecidos en la LOPD o con el incumplimiento de los mandatos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituye infracción muy grave.
- El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.
- Mantener datos de carácter personal inexactos o no efectuar las rectificaciones o cancelaciones de los mismos que legalmente procedan cuando resulten afectados los derechos de las personas que la LOPD ampara.
- La vulneración del deber de guardar secreto sobre los datos de carácter personal incorporados a ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda pública, servicios financieros, prestación de servicios de solvencia patrimonial y crédito, así como aquellos otros ficheros que contengan un conjunto de datos de carácter personal suficientes para obtener una evaluación de la personalidad del individuo.
- Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen.
- No remitir a la Agencia de Protección de Datos las notificaciones previstas en la LOPD o en sus disposiciones de desarrollo, así como no proporcionar en plazo a la misma cuantos documentos e informaciones deba recibir o sean requeridos por aquél a tales efectos.
- La obstrucción al ejercicio de la función inspectora.

- No inscribir el fichero de datos de carácter personal en el Registro General de Protección de Datos, cuando haya sido requerido para ello por el Director de la Agencia de Protección de Datos.
- Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de la LOPD, cuando los datos hayan sido recabados de persona distinta del afectado.

- *Muy Graves:*
  - La recogida de datos en forma engañosa y fraudulenta.
  - La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.
  - Recabar y tratar los datos de carácter personal a los que se refiere el apartado 2 del artículo 7 cuando no medie el consentimiento expreso del afectado; recabar y tratar los datos referidos en el apartado 3 del articulo 7 cuando no lo disponga una ley o el afectado no haya consentido expresamente, o violentar la prohibición contenida en el apartado 4 del artículo 7.
  - No cesar en el uso ilegítimo de los tratamientos de datos de carácter personal cuando sea requerido para ello por el Director de la Agencia de Protección de Datos o por las personas titulares del derecho de acceso.
  - La transferencia temporal o definitiva de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento, con destino a países que no proporcionen un nivel de protección equiparable sin autorización del Director de la Agencia de Protección de Datos.
  - Tratar los datos de carácter personal de forma ilegítima o con menosprecio de los principios y garantías que les sean de aplicación, cuando con ello se impida o se atente contra el ejercicio de los derechos fundamentales.
  - La vulneración del deber de guardar secreto sobre los datos de carácter personal a que hacen referencia los apartados 2 y 3 del artículo 7 (ver anexo I), así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.

- No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.
- No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

Tipos de sanciones:

- *Leves:*
  - 600 a 60000 €. Prescriben al año.
- *Graves:*
  - 60000 a 300000 €. Prescriben a los dos años.
- *Muy Graves:*
  - 300000 a 600000 €. Prescriben a los tres años.

Cuando cualquiera de las infracciones de estos tres niveles se cometan en ficheros cuyos responsables son las Administraciones públicas, el Director de la Agencia de Protección de Datos tomará las medidas oportunas para que cesen o se corrijan los efectos de la infracción, notificándolo al responsable del fichero, al órgano del que depende y a los afectados. Las sanciones aplicadas en este caso, serán las establecidas en la legislación sobre régimen disciplinario de las Administraciones públicas.

Medidas de seguridad

La LOPD establece que los datos de carácter personal que se encuentren bajo un tratamiento automatizado, deben ser protegidos con unas medidas de seguridad (tanto físicas como tecnológicas), que varían en función de la naturaleza de los datos, y que garantizan su seguridad y evitarán su alteración, pérdida, tratamiento o acceso no autorizado. Estas medidas pueden aplicarse en cualquier empresa y a cualquier clase de información, y varían de una a otra empresa, únicamente en función de su actividad, organización y dimensionamiento.

Las medidas de seguridad, establecidas en el Real Decreto 994/1999 y que afectan a los ficheros automatizados que contengan datos de carácter personal, se dividen en tres niveles, en función de la sensibilidad de los datos contenidos en el Fichero. Así, establece:

- Cuando se tratan datos de salud, ideología política o religiosa, el nivel de seguridad será el alto, debiendo tomar especiales precauciones.

- Cuando se traten datos relativos a la comisión de servicios financieros, hacienda pública, etc.., o cuando de los datos de carácter personal que contenga el fichero pueda obtenerse una evaluación de la personalidad del individuo, el nivel de seguridad será el medio.

- Todos los ficheros que contengan datos de carácter personal, deberán adoptar las medidas de seguridad calificadas como de nivel básico.

Es necesario que todas las empresas dispongan de los mecanismos básicos de seguridad para organizar sus propios procedimientos o políticas de seguridad de la información, y así proteger no sólo los Ficheros de Datos de Carácter Personal, sino cualquier información de la empresa. El establecimiento de estos procedimientos y garantías de seguridad frente a vulnerabilidades y amenazas, siempre actuará en beneficio de la propia empresa y su funcionamiento.

Niveles de seguridad

Dependiendo de la naturaleza de la información y del grado de necesidad de garantizar su confidencialidad e integridad, las medidas de seguridad se pueden clasificar en tres niveles, que son: básico, medio y alto. Estas medidas pueden ser técnicas u organizativas, pudiendo ser las técnicas de tipo físico o lógico.

Es importante saber que a todos los ficheros se aplican las normas de seguridad del nivel básico.

Las medidas de nivel alto contienen a su vez las medidas de nivel medio y básico

Las medidas de nivel medio contienen a su vez las de nivel básico.

Las medidas de nivel básico no contienen otras medidas, pero son las mínimas a cumplir para los datos de carácter personal, y la recomendación siempre será ampliar estas medidas.

Existen unos principios aplicables a todos los niveles de seguridad, y son:

- Cada uno de los niveles de seguridad suponen nada más que el mínimo exigible.
- Los accesos a través de redes supondrán un nivel de seguridad equivalente al exigido en los accesos en modo local.
- El tratamiento de datos fuera del local en el que se ubiquen los ficheros exigirá autorización expresa por parte del responsable del fichero, garantizándose en todo momento el nivel de seguridad que corresponda al tipo de fichero de que se trate.
- Incluso los ficheros de tipo temporal habrán de cumplir las medidas de seguridad que les corresponda con arreglo al presente reglamento.
- Todo fichero temporal será borrado una vez desaparezca el fin que motivó su creación.

Nivel básico

En el documento de seguridad, que el responsable de seguridad se encarga de elaborar e implantar, se deberá contemplar como mínimo, los siguientes aspectos:

- Su ámbito de aplicación, especificándose, detalladamente además, los recursos protegidos.
- Las medidas, normas, procedimientos, reglas y estándares, encaminados a garantizar el nivel de seguridad básico.
- Funciones y obligaciones del personal.
- Estructura de los ficheros y descripción de los sistemas de información que usen en su tratamiento.
- Procedimiento de notificación, gestión y respuesta ante las incidencias.
- Procedimientos de realización de copias de respaldo y de recuperación de datos.

El documento deberá estar actualizado en todo momento, a la vez que deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo.

Por otro lado, exige la normativa que el documento se adecúe, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

Nivel medio

Como hemos indicado anteriormente, el Reglamento ha establecido los niveles de seguridad de forma acumulativa; es decir, que al Nivel de seguridad Medio se aplicarán las medidas de seguridad del Nivel Básico y aquellas que se establecen en los arts.15 a 22 del Reglamento 994/1999.

Documento de seguridad

En el artículo 15 del reglamento se Establece que al contenido descrito por el art.8, deberá contener además el Documento de Seguridad lo siguiente:

- La identificación del/los responsables de seguridad.
- Los controles periódicos para verificar el cumplimiento de lo dispuesto en el Documento de Seguridad.
- Las medidas de seguridad para la reutilización/destrucción segura de soportes.

Fija el Reglamento que el Responsable del Fichero designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas de seguridad definidas en el Documento de Seguridad (art.15).

Podemos decir que el Responsable de Seguridad es la persona encargada de velar por el cumplimiento de las medidas, reglas y normas de seguridad establecidas por el Responsable del Fichero; en la mayoría de los casos, se trata del personal de los departamentos de sistemas/informática, por contar con conocimientos técnicos que deberán complementados con un conocimiento específico en materia de Protección de Datos de Carácter Personal. En otros casos, suele establecer varios responsables de seguridad que trabajan de forma coordinada en tres ámbitos dentro de la empresa: jurídico, informático y gestión de calidad.

Además de definirse al/los responsables de seguridad, deberá establecerse en el Documento de Seguridad las funciones y obligaciones del Responsable de Seguridad, entre las que podemos fijar las siguientes:

- Velar por el cumplimiento de las normas de seguridad contenidas en el Documento de Seguridad.
- Determinar y describir los recursos informáticos a los que se aplicará el Documento de Seguridad.

- Establecer y comprobar la aplicación del procedimiento de notificación, tratamiento y registro de incidencias.
- Establecer y comprobar la aplicación del procedimiento de realización de copias de respaldo y recuperación de datos y su periodicidad.
- Elaborar y mantener actualizada la lista de usuarios que tengan acceso autorizado al Sistema Informático, con especificación del nivel de acceso que tiene cada usuario.
- Establecer y comprobar la aplicación del procedimiento de identificación y autenticación de usuarios, así como la asignación, distribución y almacenamiento de las contraseñas de acceso.
- Establecer y comprobar la aplicación del procedimiento de cambio periódico de las contraseñas de los usuarios del sistema.
- Establecer y comprobar la aplicación de un sistema que limite el acceso de los usuarios únicamente a aquellos datos y recursos que precisen para el desarrollo de sus funciones.
- Establecer y comprobar la aplicación de los mecanismos necesarios para evitar que un usuario pueda acceder a datos o recursos con derechos distintos a los autorizados.
- Conceder, alterar, anular el acceso autorizado a los datos y recursos, de acuerdo con los criterios establecidos por el Responsable del Fichero.
- Velar por el cumplimiento de las normas de seguridad, comunicando al Responsable del Fichero las infracciones cometidas.
- Establecer los controles periódicos y auditorias necesarias para comprobar el nivel de cumplimiento del documento.

También establece expresamente el Reglamento, en el art.16, que en ningún caso el Responsable de Seguridad será responsable de las infracciones cometidas por el

incumplimiento de la normativa vigente en materia de protección de datos, puesto que la responsabilidad corresponde únicamente al responsable del fichero.

Auditoria

En materia de auditoria el Reglamento mediante su artículo 17 establece que los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.

Además, se establece que el Informe de Auditoría deberá dictaminar sobre el grado de adecuación y cumplimiento de las medidas de seguridad, identificar sus deficiencias y proponer las medidas correctoras necesarias.

Así, se establece la obligación de realizar una Auditoría cada 2 años, por personal propio o externo a la entidad debidamente cualificado, que deberá centrarse en la revisión de las Medidas de Seguridad implantadas y que deben reunir los ficheros automatizados, los equipos, los locales, centros de tratamiento y aplicaciones informáticas que tratan datos de carácter personal, así como en la revisión de los procedimientos, reglas y estándares organizativos y de seguridad, elaborados e implantados; elaborándose un Informe de Auditoría con el resultado de las deficiencias encontradas y las medidas correctoras propuestas, además de recogerse en el mismo todos los datos, hechos y observaciones en que se basen los dictámenes y recomendaciones propuestos.

En la realización de una Auditoría de Medidas de Seguridad para Ficheros automatizados de datos de nivel medio se analizarán, como mínimo:

- Los medios y procedimientos de identificación y autenticación.
- El control y registro de accesos, con determinación de perfiles de usuarios y privilegios.

- Los procedimientos de acceso y transmisión de datos a través de redes de telecomunicaciones.
- Los procedimiento de creación, conservación y borrado de ficheros temporales.
- Los procedimientos de Gestión y Notificación de Incidencias.
- Los procedimientos de realización de copias de respaldo y recuperación.
- Los procedimientos de Gestión y Distribución de soportes.
- Los procedimientos de cifrado de información sensible.
- Los procedimientos de borrado y destrucción de soportes.
- Los procedimientos de pruebas de nuevas aplicaciones/herramientas con datos reales.
- Los procedimientos de acceso, almacenamiento, conservación y destrucción de datos en formato papel.

Por último, establece el Reglamento que los Informes de auditoría serán analizados por el responsable de seguridad, quien elevará las conclusiones al responsable del fichero para que adopte las medidas correctoras adecuadas, quedando dichos Informes a disposición de la Agencia de Protección de Datos.

Identificación y autenticación

El Reglamento establece en su artículo 18, que para el Nivel Medio:

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

- Se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema.

Así, la medida descrita en el art.11 para el Nivel Básico se ve aumentada; es necesaria la identificación y autenticación de forma inequívoca y personalizada de todos los usuarios del sistema. Ello supone que cada usuario del sistema tendrá un nombre de usuario específico y una contraseña asociada al mismo, de uso personal e intransferible, siendo verificada su autorización cada vez que acceda al sistema.

Además, se establece por el Reglamento la obligación de adoptar medidas que impidan el intento reiterado de acceso no autorizado al sistema. Este bloqueo, que deberá operar tanto para accesos en modo local como en red, permite al responsable de seguridad evitar vulnerabilidades, estableciendo controles de seguridad para que usuarios no autorizados utilicen/averigüen contraseñas de acceso.

Estos procedimientos de identificación y autenticación, así como el de bloqueo y desbloqueo de cuentas de usuario, deberán recogerse en el Documento de Seguridad.

Control de acceso físico

Establece el Reglamento en su artículo 19, que exclusivamente el personal autorizado en el Documento de Seguridad podrá tener acceso a los locales en donde se encuentren ubicados los sistemas de información con datos de carácter personal. Este control de acceso físico deberá ser activado para los denominados Centros de Procesamiento de Datos o aquellas salas en las que se ubiquen los Servidores Centrales.

Aunque el Reglamento no establece que tipo de medidas de seguridad deberán ser implantadas para controlar el acceso físico, como mínimo, serán las siguientes:

- Acceso restringido a personal autorizado, mediante claves, llaves o tarjetas electrónicas.

- Sistemas redundantes de alimentación.

- Sistemas de refrigeración.
- Sistemas contra-incendios específicos para equipos electrónicos.
- Armarios ignífugos.

Además, deberá incorporarse al documento de Seguridad un listado, debidamente actualizado, de las personas autorizadas para acceder a este tipo de ubicaciones.

Gestión de Soportes.

Establece el Reglamento (artículo 20) que deberá de establecerse un sistema de registro de entrada de soportes informáticos que permita, directa e indirectamente, conocer el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción que deberá estar debidamente autorizada.

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

Así, incorporando estas medidas a las indicadas en el art.13 para los ficheros de Nivel Básico encontramos que deberán establecerse dos tipos de Registros para los soportes informáticos; uno de entrada y otro de salida. Esta medida supone la implantación por el responsable del fichero de nuevos procedimientos y normas de gestión y calidad, estableciendo un canal de autorizaciones para la entrada/salida de soportes informáticos que contengan datos de carácter personal de nivel medio.

El Registro de Entrada de soporte informáticos deberá permitir conocer:

- Tipo de soporte.
- Fecha y hora.

- Emisor.
- Número de soportes.
- Tipo de información que contienen.
- Forma de envío.
- Persona responsable de la recepción que deberá estar autorizada.

El Registro de Salida de soportes Informáticos deberá permitir conocer:

- Tipo de soporte.
- Fecha y hora.
- Destinatario.
- Número de soportes.
- Tipo de información que contienen.
- Forma de envío.
- Persona responsable de la entrega que deberá estar autorizada.

Estos Registros y el procedimiento de gestión y autorización de entrada/salida deberán quedar definidos en el Documento de Seguridad, incorporándose un modelo de autorización de entrada y salida de soportes como anexos, siendo las autorizaciones emitidas conservadas junto con toda la documentación relativa a los ficheros.

Además, el Reglamento establece en el apartado 3 del art.20 que cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario.

Cuando los soportes vayan a salir fuera de los locales en que se encuentren ubicados los ficheros como consecuencia de operaciones de mantenimiento, se adoptarán las medidas

necesarias para impedir cualquier recuperación indebida de la información almacenada en ellos; principalmente a través de mecanismos de cifrado de los datos.

Registro de Incidencias

El artículo 21 del reglamento expresa que en el registro regulado en el art.10 deberán consignarse, además, los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos han sido necesarios grabar manualmente en el proceso de su recuperación.

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

Pruebas con datos reales.

Establece el Reglamento, en su artículo 22 que las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

Antes de proceder a la migración de los datos tratados por una aplicación informática a otra nueva, se suelen realizar períodos de pruebas de la nueva aplicación con la finalidad de verificar, por un lado, su correcto funcionamiento y, por otro, que los usuarios tomen conocimiento de las nuevas funcionalidades que presenta. Durante la ejecución de estas pruebas, por regla general, no suelen utilizarse datos reales; pero, en caso de que se utilicen, deberán adoptarse e implantarse las medidas aplicables de acuerdo al nivel de los datos.

Nivel alto

Para el tratamiento de datos de carácter personal de nivel alto se establecen medidas de seguridad específicas dada la especial relevancia de esta tipología de datos (salud, creencias, filiación sindical, religión y sexo, principalmente). Estas medidas podemos resumirlas en:

- La utilización de mecanismos de encriptación y cifrado de los datos.
- El registro, control y almacenamiento de logs de accesos a los ficheros.
- El almacenamiento de copia de seguridad en ubicación distinta.

Distribución de soportes.

El artículo 23 regula que la distribución de los soportes que contengan datos de carácter personal se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que dicha información no sea inteligible ni manipulada durante su transporte.

La finalidad perseguida por esta medida es evitar que, ante cualquier incidencia que pueda producirse en la distribución de los datos (o en el soporte que los contiene), terceros no autorizados puedan acceder a la datos; recomendándose la utilización de mecanismos de encriptación.

Para la encriptación de los datos pueden utilizarse mecanismos de cifrado de 40, 56, 128 bits o más, siendo el más recomendable para esta tipología de datos el cifrado de 128 bits.

El cifrado de los datos se realiza a través de algoritmos matemáticos. Actualmente, se están utilizando para la distribución de esta tipología de datos mecanismos de firma digital avanzada (claves públicas y claves privadas), que garantizan la autenticidad y confidencialidad de la información.

Registro de Accesos.

Esta medida impuesta por el Reglamento (artículo 24) conlleva problemas técnicos y económicos en su implantación en las empresas, dado que han de configurarse las aplicaciones destinadas al tratamiento de los datos para que guarden y almacenen un gran volumen de datos.

Establece el Reglamento que, de cada acceso, se guardarán como mínimo:

- La identificación del usuario,
- Fecha y la hora en que se realizó el acceso,
- Fichero accedido,
- Tipo de acceso: autorizado o denegado,
- Y en el caso que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.

Los mecanismos que permiten el registro de los datos detallados anteriormente estarán bajo el control directo del responsable de seguridad competente sin que se deba permitir, en ningún caso, la desactivación de los mismos.

El período mínimo de conservación de los datos registrados será de dos años. Dado que el volumen de los datos a conservar puede ser muy alto, muchas empresas utilizan para cumplir con esta medida copias de seguridad específicas donde almacenan estos registros.

Además, el Reglamento establece que el responsable de seguridad competente se encargará de revisar periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes. Estos informes deberán ser conservados junto con el Documento de Seguridad.

Copias de respaldo y recuperación.

El artículo 25 del Reglamento establece para los ficheros de datos de nivel alto que deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente a aquél en que se encuentran los equipos informáticos que los tratan cumpliendo, en todo caso, las medidas de seguridad exigidas.

El almacenamiento y conservación de juegos de copias de seguridad y de los procedimientos de restauración de datos fuera de la ubicación principal (por ejemplo, en cámaras de seguridad de bancos, que nos ofrecen altas medidas de seguridad) nos garantiza la continuidad de la actividad y la disponibilidad de la información ante cualquier incidencia grave o muy grave, sea física o lógica, que afecte a los equipos y servidores centrales (incendios, inundaciones, etc.).

Transmisión de datos por redes de telecomunicaciones.

El reglamento, en su artículo 26 establece que la transmisión de datos de carácter personal a través de redes de telecomunicaciones se realizará cifrando dichos datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Habitualmente se utiliza para transmitir archivos redes de telecomunicaciones que son abiertas, es decir, que no cifran los datos mientras se transmiten entre dos puntos, permitiendo que puedan ser interceptados por terceras personas. Con la finalidad de evitar que en la transmisión de datos de nivel alto a través de redes puedan producirse intercepciones/manipulaciones de los datos, deben utilizarse mecanismos de cifrado de los datos o su transmisión a través de redes privadas, que garantizan que la comunicación entre los dos puntos es segura y no podrá ser interceptada/manipulada.

Cuadro resumen

A continuación se muestra un cuadro resumen que recoge las distintas medidas de seguridad aplicables para cada nivel:

	NIVEL BÁSICO	NIVEL MEDIO	NIVEL ALTO
DOCUMENTO DE SEGURIDAD	- Ambito de aplicación. - Medidas, normas, procedimientos reglas y estándares de seguridad. - Funciones y obligaciones del personal. - Estructura y descripción de ficheros y sistemas de información. - Procedimiento de notificación, gestión y respuesta ante incidencias. - Proced. realización copias de respaldo y recuperación de datos.	- Identificación del responsable de seguridad. - Control periódico del cumplimiento del documento. - Medidas a adoptar en caso de reutilización o desecho de soportes.	
PERSONAL	- Funciones y obligaciones claramente definidas y documentadas. - Difusión entre el personal, de las normas que les afecten y de las consecuencias por incumplimiento.		
INCIDENCIAS	- Registrar tipo de incidencia, momento en que se ha producido, persona que la notificia, persona a la que se comunica y efectos derivados.	- Registrar realización de procedimientos de recuperación de los datos, persona que lo ejecuta, datos restaurados y grabados manualmente. - Autorización por escrito del responsable del fichero para su recuperación.	
IDENTIFICAIÓN Y AUTENTICACIÓN	- Relación actualizada de usuarios y accesos autorizados. - Procedimientos de identificación y autenticación. - Criterios de accesos. - Procedimientos de asignación y gestión de contraseñas y periodicidad con que se cambian. - Almacenamiento ininteligilble de contraseñas activas.	- Se establecerá el mecanismos que permita la identificación de forma inequívoca y personalizada de todo usuario y la verificación de que está autorizado. - Límite de intentos reiterados de accceso no autorizado.	
CONTROL DE ACCESO	- Cada usuario accederá únicamente a los datos y recursos necesarios para el desarrollo de sus funciones. - Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados. - Concesión de permisos de acceso sólo por personal autorizado.	- Control de acceso físico a los locales donde se encuenetren ubicados los sistemas de información.	
GESTIÓN DE SOPORTES	- Identificar el tipo de información que contienen. - Inventario. - Almacenamiento con acceso restringido. - Salida de soportes autorizada por el responsable del fichero.	- Registro de entrada y salida de soportes. - Medidas para impedir la recuperación posterior de información de un soporte que vaya a ser desechado o reutilizado. - Medidas que impidan la recuperación indebida de la información almacenada en un soporte que vaya a salir como consecuencia de operaciones de mantenimiento.	- Cifrado de datos en la distribución de soportes.
COPIAS DE RESPALDO	- Verificar la definición y aplicación de los procedimientos de copias y recuperación. - Garantizar la reconstrucción de los datos en el estado en que se encontraban en el momento de producirse la pérdida o destrucción. - Copia de respaldo, al menos semanal.		- Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos.
RESPONSABLE		- Uno o varios nombrados por el responsable del fichero. - Encargado de coordinar y controlar las medidas del documento. - No supone delegación de responsabilidad del responsable del fichero.	
PRUEBAS		- Solo se realizarán si se asegura el nivel de seguridad correspondiente al tipo de fichero tratado.	
AUDITORIA		- Al menos cada dos años, interna o externa. - Adecuación de las medidas y controles. - Deficiencias y propuestas correctoras. - Análisis del responsable de seguridad y conclusiones al responsable del fichero, - Adopción de las medidas correctoras adecuadas.	
REGISTRO DE ACCESOS			- Registrar usuario, hora, fichero, tipo acceso y registro accedido. - Control del responsable de seguridad. Informe mensual. - Conservación 2 años.
TELECOMUNICACIONES			- Transmisión de datos cifrada.

Documento de seguridad

El Real Decreto 1720/2007, Reglamento de desarrollo de la LOPD, establece las medidas de índole técnico y organizativo que los responsables de los los ficheros y los encargados de tratamiento han de implantar para garantizar la seguridad en los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de datos de carácter personal.
Entre estas medidas, se encuentra la elaboración de un documento que recogerá las medidas de índole técnica y organizativa acorde a la normativa de seguridad vigente que será de obligado cumplimiento para el personal con acceso a los datos de carácter personal.

El documento deberá contener, como mínimo, los siguientes aspectos:

- Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.
- Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.
- Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
- Procedimiento de notificación, gestión y respuesta ante las incidencias.
- Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.
- Las medidas que sea necesario 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 estos últimos.

En caso de que fueran de aplicación a los ficheros las medidas de seguridad de nivel medio o las medidas de seguridad de nivel alto, previstas en este título, el documento de seguridad deberá contener además:

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

Además cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo.

El documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización, en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

Obligaciones y responsabilidad del titular

A continuación se detallan una serie de deberes que la ley estipula que debe cumplir un titular de un fichero

Deber de inscripción en el Registro General de Protección de Datos (RGPD)

El Registro general de protección de datos es un órgano de la APD que tiene por objeto la inscripción de los ficheros de titularidad de las Administraciones Publicas, los ficheros de titularidad privada, las autorizaciones establecidas en la ley respecto de las transferencias internacionales de datos, los códigos éticos, así como los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición. La inscripción en el registro es declarativa a efectos del funcionamiento del tratamiento, simplemente es necesaria para cumplir la obligación legal y no incurrir en las correspondientes sanciones.

Derecho de uso de los datos una vez obtenido el consentimiento

Como ya se ha visto anteriormente, el responsable del tratamiento puede obtener los datos de carácter personal de dos tipos distintos de fuentes:

- Del propio interesado, de forma que en el mismo momento en que obtenga los datos debe obtener el consentimiento para incluirlos en un tratamiento.
- De cualquier otra fuente de información en cuyo caso debe informar al afectado del hecho de haber recibido la información, la procedencia de ésta y la finalidad de su tratamiento dentro de los tres meses siguientes o antes de realizar la primera cesión de los datos. La ley en este supuesto permite el tratamiento de los datos por el responsable sin otra obligación de la de informar en el plazo de tres meses desde que se inicio el tratamiento acerca de dicha circunstancia y la atención al derecho de cancelación para que pueda ejercerse por el interesado.

Deber de información sobre el tratamiento

En la recogida de los datos será requisito para la validez del consentimiento que de modo previo e inequívoco se advierta al interesado: de la existencia de un fichero automatizado, de la finalidad del mismo, de los destinatarios de la información, del carácter obligatorio o facultativo de sus respuestas a las preguntas planteadas, de las consecuencias de la obtención de los datos o de la negativa a suministrarlos, de la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición, de la identidad y dirección del responsable del fichero.

Cuando se utilicen cuestionarios u otros impresos para la recogida figurarán las advertencias señaladas en el párrafo anterior.

Obligaciones respecto de la calidad de los datos

La calidad de los datos exige que "*los datos sean adecuados, pertinentes y no excesivos en relación con el ámbito y finalidades legítimas para las que se hayan obtenido*". Esta obligación no permite que se puedan incluir en el tratamiento datos que no sean necesarios para atender a la finalidad a la que se autoriza.

La calidad de los datos establece una serie de obligaciones:

- Si los datos han dejado de ser necesarios o adecuados para la finalidad para la que han sido recogidos, nace la obligación de cancelar los datos innecesarios.
- Se establece en la ley la obligación de adecuación de los datos a la finalidad autorizada, es decir, a la actividad genérica a que se destinan los datos objeto de tratamiento. Sin embargo, no será incompatible que posteriormente se destinen a un tratamiento con fines históricos, estadísticos, o científicos
- Los datos deberán ser exactos y puestos al día respondiendo con veracidad a la situación actual del afectado. Si no son exactos o están incompletos deben ser cancelados o sustituidos por los correctos por efecto del deber de actualización y rectificación de los datos.

- En cuanto a las obligaciones de organización, se exige que los datos sean almacenados de forma que permitan el ejercicio del derecho de acceso. No se establece una organización concreta, se obliga a cualquiera que sea la estructura del tratamiento el afectado pueda ejercer su derecho de acceso.
- Por último se establece la prohibición de recogida de datos por medios fraudulentos, desleales o ilícitos.

Adopción de las medidas de seguridad

El responsable de los datos deberá adoptar las medidas necesarias para mantener la seguridad de los datos, al tiempo que está obligado a evitar la alteración, la pérdida y el acceso no autorizado.

Esta obligación legal se regula mediante el RD 1720/2007, El sistema de seguridad, como se ha visto anteriormente se estructura en tres niveles, nivel básico, nivel medio y nivel alto.

Deber de secreto

La obligación del deber de secreto afecta al responsable del fichero y demás personas que intervengan en cualquier fase del tratamiento de los datos de carácter personal, incluso después de haber finalizado la relación con el titular o el responsable del fichero.

Prohibición de la cesión de los datos

Sólo podrá realizarse la cesión de los datos con el consentimiento previo del afectado y para el cumplimiento de la finalidad previamente determinada del fichero. Será nulo el consentimiento cuando no conste la finalidad a la que se destinaran los datos o el tipo de

actividad de aquel a quien se pretendan comunicar. Además, el cesionario se obliga, por la sólo recogida de los datos, a cumplir todas las disposiciones de la Ley.

Hay una serie de excepciones a la exigencia del consentimiento previo:

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

Deber de comunicar la primera cesión de los datos

El responsable del fichero deberá informar de a los afectados de la primera cesión de los datos en cualquier supuesto indicando la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario. La doctrina ha criticado esta obligación, por entender que conforme a la Directiva debe cumplirse esta

obligación sólo en los casos en que el interesado no conozca la existencia del tratamiento.

Como excepción a esta obligación, están los casos de cesiones entre las Administraciones públicas y el destinatario sea el ministerio fiscal, jueces y tribunales, defensor del pueblo y tribunal de cuentas.

Derecho a la autonomía en la organización: el encargado del tratamiento.

La Ley no exige que sea el responsable del tratamiento el que realice dicho tratamiento. De modo que el responsable del tratamiento puede encargar a un tercero la gestión del tratamiento a través de un contrato de arrendamiento de servicios.

Inscripción de ficheros en la Agencia Española de Protección de Datos

Como ya se ha visto, una de las funciones que tiene el Registro General de Protección de Datos es realizar la inscripción de los ficheros públicos y privados.

Son objeto de inscripción en el Registro de Protección de Datos:

- Los ficheros de titularidad pública.
- Los ficheros de titularidad privada.
- Las autorizaciones a que se refiere la presente Ley.
- Los códigos tipo a que se refiere el artículo 32 de la presente Ley.
- Los datos relativos a los ficheros que sean necesarios para el ejercicio de los derechos de información, acceso, rectificación, cancelación y oposición.

El procedimiento de inscripción de los ficheros en el RGPD, tanto de titularidad pública como privada, está regulado por vía reglamentaria, así como también el contenido de la inscripción, su modificación, cancelación, reclamaciones y recursos contra las resoluciones correspondientes.

Para los ficheros de titularidad pública y según se expresa en el Artículo 20 referido a la creación, modificación o supresión de ficheros de titularidad pública, se debe hacer constar:

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

Para los ficheros de titularidad privada el Artículo 26, de notificación e inscripción registral, necesariamente se debe notificar previamente a la Agencia, haciendo constar los siguientes datos:

- Responsable del fichero.
- Finalidad del mismo.
- Ubicación.
- Tipos de datos de carácter personal que contiene.
- Medidas de seguridad con indicación del nivel (básico, medio o alto).
- Cesiones de datos de carácter personal que se prevean realizar.
- Transferencias de datos que se prevean realizar a países terceros.

Notificación de ficheros

La notificación de ficheros es el procedimiento a través del cual se informa a la » Agencia Española de Protección de Datos de la existencia de un fichero de datos de carácter personal para que, una vez comprobado que cumple con los requisitos legalmente establecidos, se acuerde su inscripción en el Registro General de Protección de Datos.

Los responsables de los ficheros tienen la obligación legal de inscribir en el Registro todos los ficheros de datos personales que posean en su organización para que cuando el ciudadano realice una consulta al Registro pueda localizar la información que necesita para ejercer sus derechos.

A la hora de determinar quién debe notificar la creación de un fichero y cuál es el momento para hacerlo, hay que diferenciar entre ficheros de titularidad pública y ficheros de titularidad privada debido a que la forma de crearlos es diferente en cada caso; mientras que los ficheros de titularidad privada se crean a partir de una simple decisión, los ficheros de titularidad pública se crean a partir de una norma o acuerdo de creación que debe ser publicado en el Diario Oficial que corresponda.

Los ficheros de datos de carácter personal de titularidad pública serán notificados por el órgano competente de la Administración responsable del fichero para su inscripción en el Registro General de Protección de Datos, en el plazo de treinta días desde la publicación de su norma o acuerdo de creación en el Diario Oficial correspondiente.

Los ficheros de titularidad privada serán notificados por la persona o entidad privada que pretenda crearlos antes de crear el fichero y comenzar el tratamiento de los datos personales.

Todo lo relacionado con el procedimiento de notificación e inscripción de ficheros se encuentra regulado en el Titulo V y en el título IX (capítulo V) del Real Decreto 1720/2007. Teniendo en cuenta lo dispuesto en dicho reglamento, podemos resumir el procedimiento de notificación e inscripción de ficheros de la siguiente manera:

- *Notificación del fichero.*

- La notificación del fichero se realiza cumplimentando un formulario electrónico gratuito que se denomina formulario electrónico de Notificaciones Telemáticas a la AEPD y que se descarga directamente desde la página web de la Agencia Española de Protección de Datos. Una vez cumplimentado dicho formulario, se debe enviar a la Agencia por cualquiera de las vías permitidas; a través de internet con firma electrónica, a través de internet sin firma electrónica o presentando la solicitud en soporte papel directamente en las oficinas de la Agencia.

- *Resolución de inscripción del fichero.*
  - Si la notificación contuviera la información preceptiva y se cumplieran las restantes exigencias legales, el Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, acordará, respectivamente, la inscripción del fichero, asignando al mismo el correspondiente código de inscripción.
- *Resolución denegando la inscripción.*
  - En el supuesto de que de los documentos aportados por el responsable del fichero se desprenda que la notificación no resulta conforme a lo dispuesto en la Ley Orgánica de Protección de Datos. El Director de la Agencia Española de Protección de Datos, a propuesta del Registro General de Protección de Datos, dictará resolución denegando la inscripción.
- *Plazo para resolver.*
  - El plazo máximo de que dispone la Agencia para dictar y notificar una resolución acerca de la inscripción será de un mes. Si en dicho plazo no se hubiese dictado y notificado resolución expresa, se entenderá inscrito, modificado o cancelado el fichero a todos los efectos.
- *Obligación de mantener actualizada la inscripción.*
  - Una vez inscrito el fichero, el responsable del mismo deberá mantenerlo actualizado comunicando a la Agencia de Protección de Datos la cancelación o supresión del fichero así los cambios que se produzcan en la finalidad del fichero, en su responsable y en la dirección de su ubicación. Es importante destacar, que la inscripción de un fichero en el

> Registro, únicamente acredita que se ha cumplido con la obligación de notificación dispuesta en el artículo 26 de la LOPD, sin que de esta inscripción se pueda desprender el cumplimiento por parte del responsable del fichero del resto de las obligaciones previstas en la Ley y demás disposiciones reglamentarias.

Es importante destacar, que la inscripción de un fichero en el Registro, únicamente acredita que se ha cumplido con la obligación de notificación dispuesta en el artículo 26 de la LOPD, sin que de esta inscripción se pueda desprender el cumplimiento por parte del responsable del fichero del resto de las obligaciones previstas en la Ley y demás disposiciones reglamentarias.

Transferencia internacional de datos

Según el art. 5.1.s. del RLOPD, una transferencia internacional de datos, es un tratamiento de datos que supone una transmisión de los mismos fuera del territorio del Espacio Económico Europeo (EEE), 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.

El exportador de datos es la persona física o jurídica, pública o privada, u órgano administrativo situado en territorio español que realiza una transferencia de datos de carácter personal a un país tercero (art. 5.1.j. RLOPD).

El importador de datos es 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, encargado del tratamiento o tercero. (art. 5.1.ñ. RLOPD).

Las comunicaciones de datos en el EEE constituyen cesiones de datos a efectos de la aplicación de la LOPD.

Una transferencia internacional de datos no excluye en ningún caso la aplicación de las disposiciones contenidas en la LOPD y en el RLOPD. Para que la transferencia internacional de datos pueda considerarse conforme a lo dispuesto en las citadas normas, será necesario:

- Autorización del Director de la Agencia Española de Protección de Datos, salvo:
    - Que los datos se transfieran a un país que ofrezca un nivel adecuado de protección.
    - Que se trate de supuestos legalmente excepcionados de la autorización del Director.

Es obligatoria la notificación de cualquier fichero que contenga datos personales que se encuentre en el ámbito de aplicación de la LOPD. En el caso de ficheros de contabilidad y facturación cuando sólo incluyen datos referidos a las personas previstas en los arts.

2.2 y 2.3 no tienen que inscribirse siempre que se ajusten a los términos previstos en los citados artículos: colectivos, tipos de datos y finalidades concretos. Si incluyen datos de otros colectivos, el DNI u otro tipo de datos no se excluyen de la aplicación de la LOPD y por lo tanto, si tienen que ser notificados.

Un fichero temporal creado para realizar un tratamiento ocasional a partir de un fichero existente no tiene que inscribirse, sin embargo sí tiene que estar inscrito el fichero de origen. Esto se debe tener en cuenta para ciertos casos como por ejemplo si se crea un fichero temporal para organizar las vacaciones del personal a partir del fichero de recursos humanos. Este último tendrá que estar inscrito el fichero de recursos humanos, el temporal no. Respecto a este fichero temporal de vacaciones tendrán que adoptarse las medidas de seguridad correspondientes. Un fichero creado para realizar tratamientos de datos periódicos, si que tendrá que inscribirse.

Normativa

La LOPD establece en sus artículos 33 y 34 la normativa a cumplir en materia de movimiento internacional de datos.

En el artículo 33 se recogen las normas generales:

- No podrán realizarse transferencias temporales ni definitivas de datos de carácter personal que hayan sido objeto de tratamiento o hayan sido recogidos para someterlos a dicho tratamiento con destino a países que no proporcionen un nivel de protección equiparable al que presta la presente Ley, salvo que, además de haberse observado lo dispuesto en ésta, se obtenga autorización previa del Director de la Agencia de Protección de Datos, que sólo podrá otorgarla si se obtienen garantías adecuadas
- El carácter adecuado del nivel de protección que ofrece el país de destino se evaluará por la Agencia de Protección de Datos atendiendo a todas las circunstancias que concurran en la transferencia o categoría de transferencia de datos. En particular, se tomará en consideración la naturaleza de los datos, la

finalidad y la duración del tratamiento o de los tratamientos previstos, el país de origen y el país de destino final, las normas de derecho, generales o sectoriales, vigentes en el país tercero de que se trate, el contenido de los informes de la Comisión de la Unión Europea, así como las normas profesionales y las medidas de seguridad en vigor en dichos países

En el artículo 34 vienen recogidas todas las excepciones a la norma general:

Lo dispuesto en el artículo anterior no será de aplicación:

- Cuando la transferencia internacional de datos de carácter personal resulte de la aplicación de tratados o convenios en los que sea parte España
- Cuando la transferencia se haga a efectos de prestar o solicitar auxilio judicial internacional
- Cuando la transferencia sea necesaria para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamiento médicos o la gestión de servicios sanitarios
- Cuando se refiera a transferencias dinerarias conforme a su legislación específica
- Cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista
- Cuando la transferencia sea necesaria para la ejecución de un contrato entre el afectado y el responsable del fichero o para la adopción de medidas precontractuales adoptadas a petición del afectado
- Cuando la transferencia sea necesaria para la celebración o ejecución de un contrato celebrado o por celebrar, en interés del afectado, por el responsable del fichero y un tercero
- Cuando la transferencia sea necesaria o legal-mente exigida para la salvaguarda de un interés público. Tendrá esta consideración la transferencia solicitada por una Administración fiscal o aduanera para el cumplimiento de sus competencias
- Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial

- Cuando la transferencia se efectúe, a petición de persona con interés legítimo, desde un Registro público y aquélla sea acorde con la finalidad del mismo
- Cuando la transferencia tenga como destino un Estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado

Transferencias según el país destino

Transferencias a países miembros de la UE o del EEE

La LOPD utiliza el término transferencia internacional de datos para referirse a la transmisión de datos de carácter personal fuera del territorio español sea cual sea el medio que se utilice para ello, estableciendo una serie de requisitos cuyo objetivo es evitar que se envíen datos personales obtenidos en España hacia países que no proporcionen un nivel de protección equiparable al que presta la propia LOPD. Sin embargo, desde que se constituyó el denominado Espacio Económico Europeo (formado por la Unión Europea, Islandia, Liechtenstein, y Noruega), y debido a que el nivel de protección de los datos personales es equivalente en todos los Estados Miembro, jurídicamente se considera como transferencia internacional de datos únicamente a las transmisiones de datos personales que se realizan fuera de las fronteras del Espacio Económico Europeo.

El Reglamento que desarrolla la LOPD ya define la transferencia internacional de datos como el 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

Transferencias a países declarados con un nivel adecuado de protección

La Comisión Europea ha declarado que se consideran países con nivel de protección adecuado al que presta al Ley Orgánica 15/1999: Suiza, Argentina, Guernsey, Isla de Man, Jersey, Canadá respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos y las entidades estadounidenses adheridas a los principios de “Puerto Seguro” (safe harbor).

Transferencias a terceros países

Cuando se trate de realizar transferencias a terceros países (países que no sean de la Unión Europea ni tengan un nivel adecuado de protección), se puede optar por realizar un contrato.

Cuando la transferencia internacional de datos tenga por objeto la realización de un tratamiento de datos por cuenta del responsable del fichero, la realización del tratamiento deberá estar regulada en un contrato, en que deberá hacerse constar la responsabilidad directa de la transmitente como consecuencia de cualquier incumplimiento de la Ley en que incurriera el destinatario.

El contrato, que deberá constar por escrito, establecerá expresamente que el destinatario únicamente tratará los datos conforme a las instrucciones del transmitente, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato y que adoptará las medidas de seguridad exigibles al transmitente conforme a las normas de protección de datos del Derecho español.

Además, deberá indicarse que una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al transmitente, al igual que cualquier soporte o documento en que conste algún dato de carácter personal objeto del tratamiento.

La receptora no podrá comunicar los datos, ni siquiera para su conservación, a otras personas.

En consecuencia, si la transmitente deseara que por parte de varias entidades distintas, situadas fuera del territorio español, se presten servicios de tratamiento, en los términos a que se refiere el artículo 12 de la LOPD, deberá contratar dichos servicios con cada una de las entidades, no siendo posible que la destinataria subcontrate esta segunda actividad con otra empresa, a menos que actúe en nombre y por cuenta del responsable del fichero.

En caso de que la transferencia se dirija a un destinatario situado en un Estado no miembro de la Unión Europea respecto del que no se haya declarado la existencia de un

nivel adecuado de protección o que no pertenezca al Espacio Económico Europeo, en el contrato deberán constar cautelas semejantes a las indicadas en la Norma Quinta en lo referente al régimen sancionador y de indemnización a los interesados, así como en lo relativo a las potestades de la Agencia de Protección de Datos, para el caso en que la destinataria emplee los datos para otra finalidad distinta de la que motivó la transferencia, los comunique o los utilice incumpliendo las estipulaciones del contrato.

Acuerdo de Puerto Seguro

El Acuerdo de puerto seguro (Safe Harbor) nace de una necesidad comercial entre los EEUU y la Unión Europea donde los principios de Protección de Datos difieren claramente tanto en su visión del sistema como en su protección.

La Directiva 95/46/CE restringe las transferencias internacionales de datos ya que establece que los Estados miembros pueden realizar transferencias de datos personales a un tercer país únicamente cuando el tercer país de que se trate garantice un nivel de protección adecuado y cuando con anterioridad a la transferencia se respeten las disposiciones legales de los Estados miembros adoptadas con arreglo a las demás disposiciones de dicha Directiva. Debido a esto la Unión Europea y EEUU han negociado y consensuado un sistema que permita las relaciones comerciales.

Esta negociación terminó con el Acuerdo de Puerto Seguro, adoptándose por parte de la Unión Europea la decisión de la comisión de 26 de julio de 2000 con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de Puerto Seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América.

Mediante este acuerdo, las empresas de los EEUU que se adhieran al mismo (sólo éstas y no sus filiales en otros países), tal y como lo establece la propia AGPD contarán con la “presunción de adecuación” al nivel de adecuación exigido por la Directiva. Es decir, es un sistema de adhesión y auto declaración, pero no por ellos obligados a su cumplimiento.

Por ello que las empresas de los EEUU se adhieran a este sistema auto declarativo, les salva el escollo de la transferencia internacional de datos establecido en la Directiva, si bien, no asegura un nivel adecuado de cumplimiento de la normativa.

El Acuerdo de Puerto Seguro sirve para controlar que los datos van a ser protegidos tal y como se obliga a las propias empresas del Estado.

Los principios de Puerto Seguro son siete: Notificación, Opción, Transferencia Ulterior, Seguridad, Integridad de los Datos, Acceso y Aplicación que, en términos de la Directiva harían referencia al derecho de información, consentimiento, comunicación a terceros, seguridad, calidad de datos, derecho de acceso y recursos, responsabilidad y sanciones, aunque con un contenido bastante más limitado.

Aunque los principios mencionados comprenden cuestiones importantes respecto a la protección de la vida privada de las personas en lo relativo a sus datos personales, éstos aún no logran resolver todos y cada uno de los supuestos que pueden presentarse en las operaciones específicas de Comercio Electrónico, y los datos que en relación a este circulan: tienen sus elementos característicos y también una problemática propia, pero lo cierto es que por desarrollarse en un ámbito transnacional la protección de los datos que por la red transitan e inherentes a la misma operación comercial de que se trate requieren de una normativa específica que ayude a preservar con seguridad la información contenida en tales datos.

Ficheros de Publicidad y Prospección Comercial

La LOPD regula los ficheros de Publicidad y Prospección comercial mediante el artículo 30. El Reglamento de desarrollo de la LOPD también posee un apartado para su regulación, como es el capítulo II del Título IV dedicado a las *"Disposiciones aplicables a determinados ficheros de titularidad privada"*, que comprende los artículos 45 a 51.

Cuando una empresa requiere realizar un envío publicitario, necesita recopilar datos de clientes potenciales. Estos datos pueden ser captados de tres maneras distintas

- De fuentes accesibles al público
- Directamente del interesado con su consentimiento
- A través de un tercero con el previo consentimiento del titular de los datos.

Para los dos últimos supuestos, el RDLOPD detalla la forma en que deberán recogerse los datos y exige que la recogida sea para finalidades determinadas, explícitas y legítimas relacionadas con la actividad de publicidad o prospección comercial, y que se haya informado a los interesados sobre los sectores específicos y concretos de actividad respecto de los que podrá recibir información o publicidad.

Para cumplir con el deber de información regulado en el artículo 5 de la LOPD, en el supuesto de recogida de datos de fuentes accesibles al público, el artículo 45.2. del RDLOPD establece que la información que debe proporcionarse incluirá también la "indicación de ante quién podrán ejercitarse" los derechos que les corresponden.

En ese mismo artículo se dice que*: "A tal efecto, el interesado deberá ser informado de que sus datos han sido obtenidos de fuentes accesibles al público y de la entidad de la que hubieran sido obtenidos."*

Las campañas publicitarias son objeto de tratamiento particular. El artículo 46 establece las reglas especiales de las mismas que tienen como criterio determinante el de los *"parámetros identificativos"* esto es, *"las variables utilizadas para identificar el público objetivo o destinatario de una campaña o promoción comercial de productos o servicios que permitan acotar los destinatarios individuales de la misma."*

En relación con la depuración de datos personales el Reglamento dispone que cuando dos o más responsables de ficheros quieran constatar mediante un tratamiento cruzado de sus ficheros quiénes ostentan la condición de clientes de una u otra o de varios de ellos para poder así determinar los posibles destinatarios de la publicidad de sus productos o servicios, se entenderá que se está realizando una cesión de datos entre los distintos responsables, que requiere del consentimiento de los clientes.

Existen casos concretos del ejercicio de derechos dependiendo de las situaciones concretas que los tratamientos de datos con fines de publicidad plantean. Por ejemplo, se puede dar el caso que una tercera empresa se encargue de una campaña publicitaria. Para estos casos especiales la ley da relevancia al derecho de oposición que en estos tratamientos cobra especial importancia.

Los ficheros de exclusión para el envío de comunicaciones comerciales pueden ser, según el Reglamento, ficheros de exclusión individuales ó ficheros de exclusión comunes. Para los primeros, se establece que los responsables de los ficheros a los que el afectado haya manifestado su negativa a recibir publicidad, pueden crear un fichero en el que se conserven los datos mínimos imprescindibles para poder identificarlo. Respecto de los segundos, los ficheros comunes de exclusión, el artículo 49 prevé su creación e impone a los responsables de los ficheros que reciban la negativa u oposición de los afectados la obligación de informarles de la existencia de estos ficheros comunes de exclusión generales o sectoriales, así como de la identidad de su responsable, su domicilio y la finalidad del tratamiento.

Derechos de oposición

Como ya se ha comentado en el posterior apartado "Procedimiento del ejercicio de los derechos", en cualquier momento el interesado puede ejercer su derecho de oposición sobre los datos ante el responsable del fichero. En el caso de los ficheros de prospección comercial y publicidad existen unos ficheros de exclusión denominados Listas Robinson.

Listas Robinson

La Federación Española de Comercio Electrónico y Marketing Directo (FECEMD) es responsable de uno de los ficheros previstos en el artículo 49, el cual figura inscrito desde el año 2001 en el Registro General de Protección de Datos.

El Servicio de Listas Robinson tiene por objeto permitir a los consumidores eliminar su nombre y dirección de los listados de publicidad con el fin de reducir al mínimo la cantidad de publicidad que reciben en sus hogares en la forma de mailing dirigido personalmente a ellos. Los consumidores que deseen recibir menos publicidad en sus hogares, podrán solicitar el Servicio de Listas Robinson, y formar parte de manera gratuita de la Lista Robinson. Aquellas personas que por el contrario, estén interesadas en recibir más envíos publicitarios, y en particular, sobre algún tema determinado, también podrán solicitar el Servicio de Listas Robinson, y formar parte de manera gratuita, de la Lista de Preferencia.

Estas listas serán proporcionadas a las empresas miembros, quienes garantizarán que dichos nombres y direcciones dejan de figurar, o en su caso se incluyen, en los listados de consumidores que utilizan con fines de Marketing Directo. El Servicio de Listas Robinson será gestionado por la FECEMD, quién supervisará el correcto cumplimiento de las normas por parte de sus miembros.

El problema de las listas Robinson es que la consulta a dichas listas, no es obligatoria ya que cualquier entidad o persona puede crear un *"fichero común de exclusión de envío de comunicaciones comerciales"*. FECEMD no tiene ninguna exclusiva. El punto 1 del

artículo 49 del Real Decreto 1720/2007 dice que es posible la creación de estos ficheros, y que pueden ser *"de carácter general o sectorial"*. En ningún momento el Reglamento atribuye a ninguna entidad privada u organismo público en particular una gestión exclusiva. Por lo tanto cualquiera puede generar este tipo de listas y ofrecer sus servicios.

Por lo tanto, mientras no exista un único registro para estos ficheros de exclusión, este sistema no es completamente fiable para el afectado ya que la consulta por parte de las empresas encargadas de enviar publicidad no es de obligado cumplimiento.

Herramientas de publicidad

La publicidad es una forma destinada a difundir o informar al público sobre un bien o servicio a través de los medios de comunicación con el objetivo de motivar al público hacia una acción de consumo. En términos generales puede agruparse en (Above the Line) y (Below the Line), según el tipo de soportes que utilice para llegar a su público objetivo. Aunque no existe una clasificación globalmente aceptada, por ATL se entiende todo lo que va en medios de comunicación masivos: Televisión, Radio, Cine, Revistas, Prensa, Exterior e Internet, mientras que BTL agrupa acciones de Marketing Directo, Relaciones Públicas, Patrocinio, Promociones, Punto de Venta, Producto Placement, etc.

Nos vamos a centrar en las comunicaciones comerciales electrónicas más extendidas como son el envío de correos electrónicos y boletines electrónicos.

En primer lugar, hay que tener en cuenta que por comunicaciones comerciales se entiende, según el Anexo de la LSSI, "*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*". Por tanto, todo lo que sea publicidad u oferta de productos o servicios por estas entidades o personas entraría en este concepto, y no el envío de boletines de noticias o simplemente informativos, a menos que ofrezcan algún producto o servicio. Estos casos no entrarían dentro de lo que es "promoción", sino que se trataría de la simple prestación de un servicio de información al que se han suscrito voluntariamente los usuarios, aunque sea gratuito. No toda comunicación que se envíe a un grupo de usuarios tiene por qué ser comunicación comercial ni, por tanto, estar sujeta a los requerimientos de información y consentimiento que se indican en la Ley.

En segundo lugar, otro problema es la "promoción indirecta", que deja un margen de interpretación demasiado amplio. Se suele conocer por promoción indirecta al intercambio de enlaces o banners que suelen pactar algunas empresas y por el que en ocasiones se añaden contenidos ajenos, con ofertas de productos o servicios, en los mensajes de correo electrónico.

Hay que saber que un correo electrónico es un dato de carácter personal protegido por tanto por la LOPD, y ello supone que hay que aplicar una serie de medidas en cuanto al tratamiento de dicho tipo de información.

La LOPD no habla de forma expresa el dato del e-mail, pero la Agencia de Protección de Datos, máximo órgano administrativo sancionador en materia de protección de datos en España, estima que sí es un dato de carácter personal.

La publicidad debe presentarse como tal, de manera que no pueda confundirse con otra clase de contenido, e identificarse de forma clara al anunciante. Cuando la publicidad se envía por correo electrónico, incluirán al comienzo del mensaje la palabra "publicidad" o la abreviatura "publi".

Cuando se trate de ofertas promocionales, es decir, aquellas que incluyan regalos o premios o descuentos, y concursos o juegos promocionales, deben cumplir, además de lo anterior y de lo establecido en la normativa de ordenación del comercio minorista, con las siguientes obligaciones:

- Las ofertas, concursos o juegos deben aparecer claramente identificados como tales.
- Las condiciones de acceso y participación deben ser fácilmente accesibles y expresadas de forma clara e inequívoca.

Todo ello sin perjuicio de lo que disponga la normativa de las Comunidades Autónomas con competencias exclusivas sobre consumo, comercio electrónico o publicidad.

El mensaje publicitario deberá haber sido previamente solicitado o autorizado expresamente por el destinatario. No obstante, se permite el envío de comunicaciones comerciales a aquellos usuarios con los que exista una relación contractual previa, en cuyo caso el proveedor podrá enviar publicidad sobre productos o servicios similares a los contratados por el cliente.

En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales, tanto en el momento de recogida de

los datos como en cada una de las comunicaciones comerciales que se le dirijan. El prestador de servicios deberá establecer procedimientos sencillos y gratuitos a tal efecto.

Estas reglas son también aplicables al envío de mensajes publicitarios por otros medios de comunicación electrónica individual equivalente, como el servicio de mensajería de la telefonía móvil.

E-mail

Mediante mensajes de correo electrónico se puede enviar y recibir publicidad. Los envíos se hacen por parte de la empresa que quiere ofrecer sus productos y servicios y los reciben un grupo de potenciales clientes. No es lo mismo que el spam ya que el remitente no está oculto y es el mismo que la empresa que se publicita. Estas comunicaciones no suelen ser enviadas de forma masiva, sino que se selecciona a quien se envía. El contenido de estos mensajes es lícito

Boletines

Los boletines son una comunicación electrónica que reciben en el correo las personas que se den de alta e una lista de distribución con ese fin.

Estas comunicaciones contienen normalmente información relacionada con un tema concreto. Suelen venir acompañadas de publicidad relacionada con el tema que se trate (mediante banners, botones, links, etc…) con el fin de financiarse su mantenimiento.

Aplicación Práctica

LOGIBUR lleva a cabo una estricta política de protección de los datos personales que utiliza para su gestión y el cumplimiento de sus fines, de acuerdo con lo previsto en la LOPD y disposiciones de desarrollo.

La empresa necesita datos personales tanto de trabajadores, como de proveedores, clientes y cualquier otro organismo con el que se relacione y la relación requiera el tratamiento de datos personales.

En esta línea, sólo recaba los datos personales que son adecuados, pertinentes y no excesivos en relación con las finalidades para las que se obtienen y son tratados, e informa a los afectados de la existencia de ficheros automatizados que registran y tratan sus datos, en los términos previstos en el artículo 5 de la citada ley.

Los datos recabados en la empresa sirven a fines directamente relacionados con las competencias y funciones de LOGIBUR y en este sentido, recoge, procesa, almacena y utiliza sólo los datos necesarios para llevar a cabo las relaciones con trabajadores, proveedores, clientes y otras personas físicas, así como para desarrollar los servicios que pueda prestarles.

Derecho de Información

LOGIBUR necesita recoger información de sus clientes y proveedores. Esta información se recoge normalmente a través de formularios ya sean en soporte electrónico o en papel.

Cuando se utilicen formularios de recogida de datos, se incluye una leyenda que proporcione información, al menos, sobre la existencia de un fichero automatizado con datos de carácter personal y su finalidad, la identidad y dirección del responsable del tratamiento, así como acerca de la posibilidad de ejercer los derechos de acceso, rectificación y cancelación.

El texto informativo debe incluirse en el impreso correspondiente siempre que se realice una recogida de datos, salvo que al afectado ya se le haya informado previamente. En

este sentido, y para acreditar que se informó debidamente al interesado, la nota informativa se incluye siempre en impresos que firme éste y no es necesario repetirla en impresos posteriores, salvo que afecten además a interesados distintos.

En la empresa puede darse el caso de que no se utilicen formularios para la recogida de datos. Por ejemplo en encuestas de satisfacción tanto de trabajadores como de clientes. En estos casos los datos se recogen directamente en el fichero y la información requerida por el artículo 5 de la LOPD se incluirá en las normas reguladoras del procedimiento o servicio de que se trate, que deberán ser de público conocimiento, y a las que se dará la máxima difusión. Se puede colocar, por ejemplo, una referencia en la web, o se puede realizar la inclusión en convenios reguladores. Además, un extracto de dichas normas debe figurar en el documento de seguridad.

El Anexo I contiene un ejemplo texto informativo tipo que debe insertarse en los formularios de recogida de datos de empleados. Este texto debe figurar en las normas reguladoras de servicios, pantallas web que procedan, así como pliegos de cláusulas y contratos administrativos.

Consentimiento

De acuerdo con el Art. 6 de la LOPD, con carácter general el tratamiento de los datos de carácter personal por parte de LOGIBUR requiere del consentimiento inequívoco del afectado.

No obstante, como se ha visto en la teoría anterior, no será preciso el consentimiento para el tratamiento, entre otros, en los siguientes casos, por la especial incidencia que pueden tener en LOGIBUR:

- Cuando los datos se recojan para el ejercicio de funciones propias de la LOGBUR.
- Cuando se refieran a las partes de una relación laboral o administrativa y sean necesarios para su mantenimiento y cumplimiento.

- Cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por LOGIBUR o del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.

- Cuando una ley disponga otra cosa (es decir, excluya la necesidad del consentimiento expresamente).

Aunque no parezca necesario en un principio, la empresa puede necesitar recabar información acerca de la salud de sus empleados. Este tipo de datos de carácter personal sólo podrán ser recabados y tratados de forma automatizada cuando por razones de interés general así lo disponga una Ley, ó el interesado consienta expresamente.

Estos datos serían necesarios en el caso de realizarse una gestión de servicios sanitarios porque la empresa dispone de un servicio médico interno.

Conservación y cancelación de datos

Los datos de carácter personal son cancelados cuando dejan de ser necesarios o pertinentes para la finalidad para la cual han sido recabados o registrados.

Los datos de carácter personal son almacenados de forma que permiten el ejercicio del derecho de acceso, salvo que sean cancelados de acuerdo con lo previsto en la Ley.

Los plazos de conservación dependen de la vinculación existente entre LOGIBUR y el interesado, siendo conservados, con carácter general, mientras subsiste la relación y una vez concluida como máximo, por los plazos siguientes:

- Cinco años para los datos de clientes, proveedores o suministradores.

- Permanentemente para los datos de empleados o ex-empleados.

Mediante las cláusulas informativas que se insertan en los impresos de recogida de datos se puede especificar un plazo de conservación para finalidades también concretas, sin perjuicio del derecho de cancelación que asiste a los afectados.

Si los datos registrados son inexactos, en todo o en parte, o incompletos, son cancelados o sustituidos por los correspondientes datos rectificados o completados en el menor plazo de tiempo posible.

La cancelación de los datos se realiza de oficio por el responsable del fichero, al finalizar el plazo de conservación, o a petición del interesado en ejercicio de su derecho de cancelación. No se realiza la cancelación de los datos cuando ello pueda causar un perjuicio a intereses legítimos del interesado o de terceros, cuando existe una obligación legal de conservarlos, cuando existe una relación contractual, cuando es preciso su mantenimiento para gestiones de pagos o cobros o para el adecuado ejercicio de las funciones propias de LOGIBUR.

Derechos de acceso, rectificación y cancelación

Los empleados de LOGIBUR, proveedores y clientes pueden ejercitar estos derechos de acuerdo con lo dispuesto en la LOPD.

La normativa propia reguladora de estos derechos está pública en un apartado en la página web para facilitar el conocimiento por los interesados.

Los interesados pueden utilizar los modelos de solicitud establecidos en dicha normativa, que están disponibles en la página web de LOGIBUR ó mediante una solicitud por escrito dirigida al responsable del fichero de LOGIBUR.

Cesiones

Como empresa de logística que es, LOGIBUR puede necesitar realizar cesiones de datos como pueden ser de las direcciones postales de sus clientes a otras entidades subcontratadas.

LOGIBUR no realiza otras cesiones que las previstas en las leyes y otras normas de obligado cumplimiento, las que implican la prestación de los servicios que le soliciten, las necesarias para el cumplimiento de las finalidades que tiene encomendadas, así

como las cesiones necesarias a otras administraciones públicas para el ejercicio de las competencias propias de éstas sobre las mismas materias.

Todas estas cesiones están excluidas de la necesidad de consentimiento, según lo previsto en los arts. 11 y 21 de la LOPD.

La cesión de datos de carácter personal se efectúa en la forma y con las limitaciones y derechos que otorga la LOPD. En particular:

- No se ceden datos a terceros salvo que se cuente con el consentimiento del interesado o éste no sea preciso.
- En cualquier caso, los datos sólo pueden ser cedidos para fines relacionados con el ejercicio de funciones legítimas del cedente y del cesionario.

Las cesiones de datos previstas para cada fichero figuran en el documento de seguridad.

La cesión de datos a terceras empresas u organismos por parte de LOGIBUR que no precise consentimiento y no obedezca a procedimientos legales normalizados, se realiza previa advertencia al cesionario de la obligación de no utilizarlos para fines distintos de los que motivan la cesión, y de cumplir las previsiones de la LOPD en cuanto a medidas de seguridad y demás obligaciones legales, según la fórmula que figura en el anexo III.

Ejercitado el derecho de rectificación, cancelación o revocación del consentimiento, LOGIBUR debe comunicar a los cesionarios en el menor plazo de tiempo posible la rectificación de los datos efectuada o la obligación de cancelarlos.

Como ya se ha visto anteriormente, no será necesario recabar el consentimiento de los interesados en los siguientes casos:

- Cuando la cesión esté autorizada o prevista por una ley.
- Cuando se trate de datos recogidos de fuentes accesibles al público. No obstante, LOGIBUR no podrá ceder datos obtenidos de fuentes de acceso público a ficheros de titularidad privada salvo previo consentimiento del interesado o que una ley prevea otra cosa.

- Cuando el tratamiento responde a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros.

- Cuando la comunicación tiene por destinatario el Defensor del Pueblo, el Ministerio Fiscal, los Jueces o Tribunales o el Tribunal de Cuentas, e Instituciones Autonómicas análogas, en el ejercicio de las funciones que tienen atribuidas.

- Cuando la cesión se realice entre LOGIBUR y otra Administración Pública y tenga como objeto el tratamiento de los datos con fines históricos, científicos o estadísticos.

- Cuando la cesión de datos de salud es necesaria para solucionar una urgencia o para realizar los estudios epidemiológicos en los términos establecidos en la legislación estatal o autonómica sobre la materia.

- Si la cesión se realiza previo procedimiento de disociación de datos.

- Cuando los datos se recogen por LOGIBUR precisamente con destino a otras Administraciones Públicas o para el ejercicio por éstas de competencias sobre las mismas materias.

Procedimiento para efectuar las cesiones

En los procesos empresariales de LOGIBUR, existen diversos tipos de cesiones.

- Cesiones de datos que no requieren previo consentimiento del interesado.
    - Este tipo de cesiones ocurre cuando la cesión está prevista en un procedimiento legal o reglamentariamente establecido como por ejemplo las cesiones de datos sobre cotización al INSS, de retenciones a cuenta del IRPF a la Agencia Estatal de Administración Tributaria, y responda a alguno de los supuestos contenidos en los artículos 11 y 21 de LOPD.

- Este tipo de cesiones se llevan a cabo mediante la supervisión del responsable del fichero y se realizan de conformidad con las diferentes leyes aplicables, en el ejercicio de las funciones que tienen atribuidas los cesionarios.
- Entran dentro de esta categoría las cesiones que se realizan a petición expresa y puntual de datos concretos por parte de organismos judiciales o administrativos en procedimientos ordenados por ellos.

- Cesiones que no requieren el consentimiento del afectado, pero no responden a procedimientos normalizados, aunque están previstas en el documento de seguridad:
  - Cuando se trate de cesiones ya previstas en la disposición de creación del fichero que no requieren del consentimiento de los interesados y así consta en la misma, por tratarse de alguno de los casos del Art.11 o 21 de la LOPD, la cesión se realizará de la siguiente manera: Se realiza por el responsable del fichero. Al efectuar la cesión se acompaña un documento que debe ser devuelto firmado por la institución cesionaria en el que se le advierte de la obligación de no utilizar los datos para fines distintos de los que motivan la cesión, y de cumplir las previsiones de la LOPD en cuanto a medidas de seguridad y demás obligaciones legales. Un ejemplo puede ser el modelo que se encuentra en el anexo IV.
- Cesiones de datos que requieren el consentimiento:
  - No se tiene planeado este tipo de cesiones en LOGIBUR, pero en el caso de ser necesarios, es de suma importancia la obligación de respetar las previsiones de la LOPD.

Peticiones de datos realizadas dentro de procedimientos judiciales o administrativos

En caso de peticiones puntuales de cesión de datos concretos por parte de organismos judiciales y administrativos se tendrá en cuenta lo siguiente:

- La información sobre datos de carácter personal concretos obrantes en ficheros de LOGIBUR será comunicada a autoridades judiciales y administrativas, según el procedimiento que corresponda.

- Las peticiones deben tener un motivo y razón.

Pueden ser solicitados datos personales de LOGIBUR por jueces, organismos administrativos o por cuerpos y fuerzas de seguridad del Estado.

En el caso de que sean solicitados por mediación de un juez, los datos serán facilitados en el menor breve periodo de tiempo posible. Las informaciones solicitadas por órganos gubernativos en actuaciones relacionadas con procesos judiciales, serán facilitadas cuando conste claramente el órgano judicial que interviene.

En el caso de solicitudes de información por parte de los cuerpos y fuerzas de seguridad del Estado, debe mediar orden judicial para efectuar la cesión de datos.

En el caso de los organismos administrativos, se facilitarán los datos cuando

- La solicitud haya sido presentada por órganos o entidades de la Administración tributaria o recaudatoria estatal o local, en virtud de la normativa vigente en cada momento y siempre que la información solicitada tenga trascendencia tributaria.

- La solicitud sea presentada por el Instituto Nacional de la Seguridad Social o cualquiera de sus Agencias, en el ejercicio de las competencias que le son propias.

- La solicitud se formule por la autoridad laboral en el uso de las competencias que legalmente le corresponden.

- La solicitud de datos se presente basada en la Ley 12/1989, de 12 de mayo, sobre Función Pública Estadística para la elaboración de estudios de ese carácter.

Si se trata de datos relativos a la salud, se facilitarán cuando sea necesario para solucionar una urgencia, o para realizar estudios epidemiológicos en los términos

establecidos en la Ley 14/1986, de 25 de Abril, General de Sanidad, en la Ley 31/1995 de Prevención de Riesgos Laborales y en la normativa vigente en cada momento.

Cesión de datos personales a sindicatos

La cesión de datos personales de empleados a los representantes sindicales se realiza en los términos de la Ley Orgánica 11/1985, de 2 de Agosto de Libertad Sindical, y de la Ley 2/1991 de 7 de enero, sobre derecho de información de los representantes de los trabajadores en materia de contratación o normativa vigente en cada momento, y de acuerdo con las resoluciones de la Agencia Española de Protección de Datos sobre la materia.

Procedimiento de acceso a datos por un tercero para la prestación de servicios a LOGIBUR

El acceso de un tercero a los datos cuando sea necesario para la prestación de un servicio a LOGIBUR no requiere el consentimiento previo del interesado, pues de acuerdo con el artículo 12 de la LOPD no se considera cesión de datos. La ley denomina a ese tercero “encargado de tratamiento”.

La comunicación de datos en estos supuestos requiere la firma de un contrato, o documento escrito cuando no se requiera éste, entre LOGIBUR (responsable del tratamiento) y el encargado del tratamiento, mediante el cual éste se comprometa a:

- Tratar los datos conforme a las instrucciones del responsable del tratamiento.
- No utilizarlos para un fin distinto que el que figure en el documento.
- No comunicarlos a otras personas o entidades.
- Establecer las medidas de seguridad exigidas por la legislación.
- Destruir o devolver los datos tratados una vez concluido el servicio.

- Guardar confidencialidad

En el caso de que la prestación del servicio no esté recogida en un contrato administrativo por no ser necesario en aplicación de la legislación de contratos, el encargado de tratamiento firma igualmente documento de compromiso, según modelo anexo III.

Para todos los contratos que realice la empresa, debe incluirse en el contrato, como cláusula específica sobre protección de datos personales o como anexo, el modelo que se encuentra en los anexos V y VI respectivamente.

Ficheros.

Tanto la creación de ficheros, como sus posibles modificaciones y borrado corresponde al Presidente de LOGIBUR. Este se encarga de realizar la notificación a la Agencia Española de Protección de Datos en el plazo máximo de un mes desde que se realice la creación, modificación o supresión del fichero.

En un principio, LOGIBUR tiene pensado crear los siguientes ficheros para almacenar datos necesarios para el desempeño de su trabajo:

- Fichero Empleados
- Fichero Proveedores
- Fichero Clientes

La labor de creación del documento de seguridad es llevada a cabo por el responsable de los ficheros y el responsable de seguridad. El documento de seguridad debe complementarse con uno o varios textos que sirvan de manual informativo de dicho documento. Un esquema de un documento de seguridad adecuado puede verse en el anexo VII

Cuando alguno de los ficheros automatizados creados por LOGIBUR se modifique para incluir nuevos datos de carácter personal o se establezcan nuevas cesiones o impresos

de recogida de datos, el responsable del fichero es el encargado de analizar la necesidad de regularizar los ficheros ya declarados a la Agencia Española de Protección de Datos o de incluir textos informativos en los impresos, así como actualizar el documento de seguridad.

En la creación de nuevos ficheros y que contengan datos de carácter personal, el responsable de dichos ficheros es el encargado de encargar que su diseño implemente las medidas de seguridad. El responsable del fichero tiene como labor incluir los textos informativos que sean precisos en los impresos y procedimientos telemáticos de recogida de datos.

El documento de seguridad así como sus modificaciones es redactado conjuntamente por el responsable del fichero y el responsable de seguridad de LOGIBUR, Este último deberá prestar especial atención al apartado relativo a las especificaciones técnicas. El documento es aprobado por el Presidente de LOGIBUR. Las cuestiones técnicas referentes a la implantación de medidas de seguridad son llevadas a cabo por el responsable de seguridad de la empresa.

El documento de seguridad debe estar siempre actualizado, por lo que se tiene que incluir cualquier modificación relevante para la protección de datos personales desde el punto de vista técnico, organizativo o jurídico.

Debe constar en el documento de seguridad una copia de todas las comunicaciones que se envíen o reciban de la Agencia Española de Protección de Datos en lo referente a cada fichero.

El responsable de seguridad es el encargado de hacer cumplir el documento de seguridad.

El responsable de seguridad de la empresa ha creado un registro de incidencias para poder registrar en él cualquier incidencia que pueda suponer un peligro para la seguridad de los ficheros que contengan datos personales.

Cualquier usuario de la empresa que conozca hechos o circunstancias que puedan constituir una incidencia, especialmente si implica un riesgo respecto a la seguridad de

los datos automatizados de carácter personal, lo debe poner en conocimiento del responsable del fichero o del responsable de seguridad en menor periodo de tiempo posible. Ambos responsables deben trabajar conjuntamente para solucionar todas las posibles incidencias.

De igual manera, se lleva a cabo un riguroso control sobre la entrada y salida de soportes informáticos de la empresa mediante la utilización de un registro de entrada y salida de soportes.

El Presidente de LOGIBUR es el encargado de designar al responsable de todos los ficheros de LOGIBUR, éste a su vez designa a los responsables de sistemas y seguridad de los diferentes ficheros.

La relación actualizada de todos los responsables citados es incorporada al documento de seguridad de LOGIBUR y al manual informativo para el personal.

Todo el personal de LOGIBUR tiene el deber de conocer sus funciones y obligaciones en relación con el tratamiento y la protección de los datos de carácter personal, que se recogen y especifican en el documento de seguridad de la empresa y en un manual informativo de normas de seguridad y de gestión al que tiene acceso todo el personal. Debido a las actualizaciones en el documento de seguridad y por tanto, en los manuales informativos, es necesario informar a los usuarios de todo cambio que se realicen en dichos manuales.

En el contrato que se realiza a nuevo personal de LOGIBUR, se informa de la obligación de conocer el manual citado. Para mayor comodidad, este texto está accesible en la intranet de la empresa. Sería recomendable incluir clausulas en los contrato laborales que indiquen el compromiso de confidencialidad y cumplimiento de las normas.

Todo el personal de LOGIBUR que intervenga en alguna fase del tratamiento de datos personales o que de cualquier modo pueda tener acceso a ellos, está obligado al secreto profesional respecto de dichos datos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con la empresa. Por ese motivo, todos

los empleados de LOGIBUR deben firmar una cláusula de confidencialidad similar a la que se muestra en el anexo II.

Se realiza una auditoria interna de seguridad con una periodicidad anual. Esta auditoría es realizada por el responsable de seguridad de LOGIBUR. Con el fin de corregir vulnerabilidades y posibles fallos en los procedimientos no detectados en la auditoria interna, se lleva a cabo una auditoria externa cada dos años.

Se realizan copias de seguridad de todos los ficheros que utiliza la empresa. Las copias de seguridad son almacenadas en una caja fuerte de un banco.

Todos los accesos a los servidores que contienen los datos de los ficheros se realizan mediante protocolo seguro SSL.

Existe un fichero de publicidad y prospección comercial cuyo objetivo es informar de nuestros servicios a los clientes y posibles clientes. Todas las comunicaciones comerciales que realice la empresa, se ajustaran a la Ley indicando en el asunto de los mensajes la palabra “publicidad”. En todas las comunicaciones se ofrece la posibilidad de cancelar el envío de publicidad mediante respuesta de correo electrónico con la palabra “baja” en el asunto. LOGIBUR procederá inmediatamente a la cancelación de envío de publicidad al usuario que así lo solicite.

Manuales y procedimientos.

Como ya se ha comentado es necesaria la creación de un documento de seguridad en el que se recojan las medidas de índole técnicas y organizativas que garanticen la seguridad de los datos personales.

Como complemento a este documento se recomienda la creación de unos manuales informativos que sean utilizados por los empleados de LOGIBUR. En el anexo VIII se puede ver un listado de manuales y procedimientos que sería recomendable redactar.

Comercio Electrónico

El comercio electrónico es cualquier transacción operativa realizada vía proceso digital o redes de trabajo.

Sin embargo, cuando se refiere al comercio electrónico, se habla de algo más que el simple mercado de productos o servicios vía Internet.

El comercio electrónico es una tecnología promocional que permite a las empresas incrementar la precisión y la efectividad en la realización de sus transacciones comerciales y una forma de intercambio de información entre organismos, clientes y comerciales para el beneficio de todos.

El comercio electrónico cambia la forma en que los productos, los servicios, incluso la información es presentada, vendida e intercambiada. También cambia la forma en que los organismos colaboran con los clientes y sus colaboradores.

El comercio electrónico vía Internet se infiltra en nuevos mercados, descubre o crea nuevos canales de ventas o se acerca a los clientes y colaboradores a través de nuevos canales de comunicación.

Tipos de Comercio Electrónico

Las empresas, organizaciones públicas y clientes pueden participar en el comercio electrónico. Las aplicaciones del comercio electrónico pueden ser clasificadas en cuatro categorías:

- Comercio electrónico de la Empresas a los Clientes (B2C).
- Comercio electrónico de los Clientes/Ciudadanos a las Instituciones Gubernamentales (C2G).
- Comercio electrónico de las Empresas a las Instituciones Gubernamentales.
- Comercio electrónico de las Empresas a las Empresas (B2B).

Comercio Electrónico de las Empresas a los Clientes (B2C)

Las aplicaciones B2C están dirigidas al consumidor medio. Este tipo de aplicaciones de comercio electrónico han sido desarrolladas durante los últimos años, principalmente como resultado del extendido uso de Internet y de la mejora de los servicios provistos por este medio. Internet es aplicable a este tipo de comercio electrónico, ya que es ampliamente disponible y puede promover productos efectivos y servicios entre todo tipo de posibles clientes.

Comercio electrónico de los Clientes/Ciudadanos a las Instituciones Gubernamentales (C2G).

Las aplicaciones C2G incluyen en su mayoría pago de impuestos, publicaciones de documentos oficiales, etc. A pesar de que no se puede definir las transacciones entre los clientes o ciudadanos con las instituciones gubernamentales como comercio electrónico, podemos ver suficientes aplicaciones C2G en el marco de transacciones que son realizadas más efectivamente y más eficientemente con el uso de sistemas de tecnología de comercio electrónico.

Comercio electrónico de las Empresas a las Instituciones Gubernamentales. (B2G).

Las aplicaciones B2G incluyen los impuestos, los suministros, y el control de aduanas para las importaciones y exportaciones, etc. Como en el caso de las aplicaciones de comercio electrónico entre consumidores e instituciones gubernamentales, las transacciones de las empresas a las instituciones gubernamentales no parecen tener una relación directa con lo que el mundo considera comercio electrónico. Sin embargo, el Estado está relacionado en casi todo tipo de transacción empresarial durante todo el ciclo comercial y por esta razón bastantes aplicaciones han sido desarrolladas con el fin de mejorar las transacciones B2G.

Comercio electrónico de las Empresas a las Empresas (B2B).

Las aplicaciones B2B tienen como objetivo la mejora y simplificación de varios procesos operativos en las empresas, así como el incremento de la eficiencia de las transacciones entre empresas colaboradoras.

Las empresas utilizan el sistema B2B para transacciones más rápidas sin faltas, para control de reservas, sustitución efectiva de productos, etc. Las empresas que desarrollan actividades B2B para comercio electrónico con sus colaboradores deben tener colaboración y coordinación. Una aplicación B2B implica normalmente a muchas personas individuales en muchas operaciones corporativas. Incluso si la mayor parte de la gente conoce ya las aplicaciones electrónicas de Empresas a consumidores y un gran número de Empresas pasa del comercio tradicional a los sistemas electrónicos de venta, la transacción más importante del comercio electrónico llevada a cabo es la del tipo B2B. Esto ocurre porque las aplicaciones B2B incluyen millones de transacciones, inversiones tremendas, así como la velocidad y la precisión pueden ser una gran ventaja competitiva.

Normativa

La regulación del comercio electrónico se manifiesta en la Ley 34/2002, de 11 de Julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSICE, LSSI o LCE).

La LSSI tiene por objeto incorporar al ordenamiento jurídico español la Directiva 200/31/CE, del Parlamento europeo y del Consejo, de 8 de Junio, relativa a determinados aspectos de los servicios de la sociedad de la información, en particular, el comercio electrónico en el mercado Interior. También incorpora parcialmente la Directiva 98/27/CE, del Parlamento europeo y del Consejo, de 19 de Mayo, relativa a las acciones de cesación en materia de protección de los intereses de los consumidores al regular una acción de cesación contra las conductas que contravengan lo dispuesto en la Ley.

El planteamiento de la Ley esta diseñado desde la perspectiva de englobar las actividades realizadas por medios electrónicos desarrollando unas normas que regulen lo que no está cubierto por otras legislaciones debido a la novedad.

La Ley afecta a todos aquellos para los cuales la prestación del servicio represente una actividad económica. De tal manera que se incluyen todos los servicios ofrecidos por los operadores de comunicaciones, los proveedores de acceso a Internet, los portales, los motores de búsqueda o cualquier otro sujeto que disponga de un sitio en Internet a través del que realice alguna de las actividades recogidas en la Ley, incluido el comercio electrónico.

Prestadores de servicios

Atendiendo a lo dispuesto en la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, entendemos por Prestador de Servicios de la Sociedad de la Información, todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario.

Dentro de este concepto se recogen igualmente servicios prestados gratuitamente, siempre que, constituyan una actividad económica para el prestador.

Por exclusión legal, no se consideran como tales, los servicios prestados por medio de telefonía, fax o télex, el intercambio de correos electrónico u otros de comunicación electrónica equivalente para fines ajenos a la actividad económica de quienes lo utilizan. Los servicios de radiodifusión televisiva o sonora, así como el teletexto televisivo y otros servicios equivalentes como las guías electrónicas de programas ofrecidas a través de las plataformas televisivas.

Por lo tanto, cualquier empresa que realice actividades económicas por Internet u otros medios telemáticos (correo electrónico, televisión digital interactiva...), es un prestador de servicios siempre que:

- La dirección y gestión de sus negocios esté centralizada en España o,
- Posea una sucursal, oficina o cualquier otro tipo establecimiento permanente situado en territorio español, desde el que se dirija la prestación de servicios de la sociedad de la información.

Se presumirán establecidos en España y, por tanto, sujetos a la Ley a los prestadores de servicios que se encuentren inscritos en el Registro Mercantil o en otro Registro público español en el que fuera necesaria la inscripción para la adquisición de personalidad jurídica.

La utilización de un servidor situado en otro país no será motivo suficiente para descartar la sujeción a la Ley del prestador de servicios. Si las decisiones empresariales

sobre el contenido o servicios ofrecidos a través de ese servidor se toman en territorio español, el prestador se reputará establecido en España.

Obligaciones y Régimen de responsabilidad

Obligaciones

El artículo 10 de la Ley indica que la información sobre el prestador de servicios y su actividad han de ponerse a disposición de los usuarios por medios electrónicos, de forma permanente, fácil, directa y gratuita. Cuando los servicios se prestan a través de una página en Internet, bastará con incluir en ella esa información de manera que ésta sea accesible en la forma indicada. Estas condiciones se cumplen cuando la información está contenida en la página de inicio del prestador de servicios o se inserta en páginas interiores relacionadas con el tipo de información de que se trate y a las que se pueda acceder a través de un enlace claramente visible, cuyo título aluda de forma inequívoca a la información de que se trate. Por ejemplo: para acceder a la información de identificación de la empresa, serviría una pestaña con el título “quiénes somos” o cualquier otro suficientemente expresivo del tipo de información a que se refiere.

La ley no solo trata de las comunicaciones por internet o el correo electrónico, sino que trata también sobre medios de comunicación electrónica equivalentes como aquéllos medios que permitan una comunicación individual entre el prestador y el destinatario de servicios, como, por ejemplo, los mensajes cortos (SMS) y los mensajes multimedia (MMS) dirigidos a terminales de telefonía móvil.

El artículo 27 de la Ley indica que la información previa a la contratación ha de ser clara, comprensible e inequívoca y debe ponerse a disposición del usuario de forma permanente, fácil y gratuita, mediante técnicas adecuadas al medio de comunicación utilizado.

La obligación de poner a disposición la información se dará por cumplida si el prestador la incluye en su página o sitio web.

Cuando a los servicios se acceda mediante dispositivos que cuenten con pantallas de formato reducido (ej. móviles) se dará por cumplida la obligación si se facilita la dirección de Internet donde se encuentre dicha información.

En el caso de que un prestador de servicios emplee dispositivos de almacenamiento y recuperación de datos en equipos terminales deberá informar a los destinatarios de manera clara y completa sobre su utilización y finalidad, ofreciéndoles la posibilidad de rechazar el tratamiento de los datos mediante un procedimiento sencillo y gratuito.

Los proveedores de acceso a Internet deberán informar a sus clientes de:

- Los medios técnicos que permitan la protección frente a las amenazas de seguridad en Internet (virus informáticos, programas espías, spam) y sobre las herramientas para el filtrado de contenidos no deseados.
- Las medidas de seguridad que apliquen en la provisión de sus servicios.
- Las posibles responsabilidades en que puedan incurrir por el uso de Internet con fines ilícitos.

Los prestadores de servicios de correo electrónico deberán informar a sus clientes sobre las medidas de seguridad que apliquen en la provisión de sus servicios.

Los prestadores de servicios de intermediación:

- No tienen obligación de supervisar los contenidos que alojan, transmiten o clasifican en un directorio de enlaces, pero deben colaborar con las autoridades públicas cuando se les requiera para interrumpir la prestación de un servicio de la sociedad de la información o para retirar un contenido de la Red.
- No son, en principio, responsables por los contenidos ajenos que transmiten, alojan o a los que facilitan acceso, pero pueden incurrir en responsabilidad si toman una participación activa en su elaboración o si, conociendo la ilegalidad de un determinado material, no actúan con rapidez para retirarlo o impedir el acceso al mismo.

Las obligaciones de los prestadores de servicios que realicen actividades económicas a través de Internet se concretan en dos grupos: obligaciones de información y obligaciones en relación con la contratación on-line. Por lo que se refiere a las obligaciones de información, la empresa debe incluir en su página web información

básica que permita a los usuarios identificar quién es el titular de dicha página. La información básica que se debe facilitar es:

- Su denominación social, NIF, domicilio y dirección de correo electrónico, así como cualquier otro dato que permita una comunicación directa y efectiva, como por ejemplo un teléfono o un número de fax.

- Datos de inscripción, en el caso de que la empresa esté registrada en el Registro Mercantil o en cualquier otro registro público.

- Información sobre el precio de los productos, indicando si incluye o no los impuestos aplicables, gastos de envío y cualquier otro dato que deba incluirse en cumplimiento de normas autonómicas aplicables.

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

- En los casos de que su actividad este sujeta a autorización previa o ejerza una profesión regulada, deberá informar a los usuarios sobre los siguientes aspectos:

    - Si ejerce alguna profesión regulada, los datos básicos que acrediten su derecho a ejercer dicha profesión (colegio profesional al que pertenece, número de colegiado, título académico, Estado de la Unión Europea en que se expidió el título académico y, en su caso, la correspondiente homologación).

    - Si su actividad estuviera sujeta a autorización administrativa, los datos de la autorización de que disponga y los identificativos del órgano encargado de su supervisión.

Además de la información básica señalada anteriormente, si la empresa realiza contratos en línea o por vía electrónica a través de su página web, deberá informar previamente al contrato de los pasos a realizar, lengua del contrato y condiciones generales. Una vez realizado el contrato, la empresa habrá de enviarle una confirmación sobre la recepción de su pedido.

Responsabilidades

En la LSSI se regula la responsabilidad de los prestadores de servicios de la sociedad de la información.

Los artículos 9 a 17 de la mencionada norma vienen a determinar cuando los prestadores de servicios, entendiéndose como toda persona o entidad que proporcione un servicio de la sociedad de la información son responsables por lo que suceda en dichos servicios.

Según el artículo 16 de la LSSI le exonera de responsabilidad al determinar que los prestadores de servicios de alojamiento o almacenamiento de datos no serán responsables por la información almacenada a petición del destinatario, siempre que:

- No tengan conocimiento efectivo de que la actividad o la información almacenada es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o

- Si lo tienen, actúen con diligencia para retirar los datos o hacer imposible el acceso a ellos.

La LSSI determina que *"Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el primer punto cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse"*.

Por lo tanto, el prestador de servicios de alojamiento no está obligado a realizar una investigación sobre la legalidad de los contenidos que aloja. Pero, si sospecha que un determinado contenido puede ser constitutivo de delito, debe poner en conocimiento del Juez de Instrucción más cercano el presunto hecho delictivo, de acuerdo con lo

dispuesto en la Ley de Enjuiciamiento Criminal. Si un órgano judicial o administrativo competente le ordena retirar el contenido o impedir el acceso al mismo, debe hacerlo inmediatamente.

El administrador del servidor no será responsable del contenido ilícito alojado en él si no tiene conocimiento efectivo de la ilicitud de las actividades que se llevan a cabo a través de ese canal. El "conocimiento efectivo" de su ilicitud puede obtenerse por cualquiera de estos tres medios destacados en la Ley:

- Conocimiento de una resolución dictada por órgano competente que declare la ilicitud del contenido y ordene su retirada o que se imposibilite el acceso al mismo.
- Recepción de una notificación enviada de conformidad con un procedimiento de detección y retirada de contenidos que el prestador de servicios haya suscrito.
- Otros que pudieran establecerse por norma jurídica o acuerdo entre las partes.

El apartado j del Anexo de definiciones de la LSSI define órgano competente como *"todo órgano jurisdiccional o administrativo, ya sea de la Administración general del Estado, de las Administraciones Autonómicas, de las Entidades locales o de sus respectivos organismos o entes públicos dependientes, que actúe en el ejercicio de competencias legalmente atribuidas"*

Comunicaciones comerciales

Por comunicaciones comerciales se entiende *"todas las formas de comunicación destinadas a proporcionar directa o indirectamente bienes, servicios o la imagen de una empresa, organización o persona con una actividad comercial, industrial, artesanal o de profesiones reguladas"*.

Las comunicaciones comerciales electrónicas no deseadas son comúnmente denominadas con los anglicismos "spam" o "spaming".

Según la Directiva 2000/31/CE, las comunicaciones comerciales deben estar claramente identificadas y no prestarse a equívocos (art. 6) con el fin de aumentar la confianza del consumidor y garantizar unas prácticas comerciales leales, mientras que las comunicaciones comerciales por correo electrónico deben ser reconocidas claramente por el destinatario desde su recepción.

Por otro lado, la Directiva sobre la privacidad y las comunicaciones electrónicas de 2002 prohíbe el envío de mensajes comerciales no solicitados (por correo electrónico, mensajes de texto o multimedia a terminales fijos o móviles) salvo que se haya obtenido previamente el consentimiento del abonado (régimen de consentimiento previo o del "opt-in")

En España, el envío de comunicaciones comerciales electrónicas está regulado principalmente por la LOPD y la LSSI.

La LOPD se refiere sólo al envío de comunicaciones comerciales a personas físicas y establece que en cada comunicación que se les dirija se les informará sobre el origen de los datos y de la identidad del responsable del tratamiento de los mismos, así como de los derechos que le asisten (art. 5), reconociéndose a los interesados el derecho a oponerse *"previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán datos de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud"* (art. 30). En todo caso, la LOPD exige el *"consentimiento inequívoco del afectado"* para el tratamiento de sus datos de carácter personal (art. 6).

En cambio, la LSSI regula el envío de comunicaciones comerciales tanto a las personas físicas como a las jurídicas y establece una serie de obligaciones en sus artículos 19 y siguientes (título III), que se enumeran a continuación.

En primer lugar, las comunicaciones comerciales realizadas por vía electrónica deberán ser claramente identificables como tales y deberán indicar la persona física o jurídica en nombre de la cual se realizan, además de incluir al comienzo del mensaje la palabra publicidad, en caso de que tengan lugar a través de correo electrónico u otro medio equivalente.

Las ofertas promocionales, como las que incluyan descuentos, premios y regalos, y de concursos o juegos promocionales, previa la correspondiente autorización, se deberá asegurar que queden claramente identificados como tales y que las condiciones de acceso y, en su caso, de participación se expresen de forma clara e inequívoca.

La LSSI prohíbe el envío de comunicaciones publicitarias o promocionales por correo electrónico y otro medio equivalente si previamente no se ha contado con el consentimiento expreso de los destinatarios, salvo que exista una relación contractual previa.

Además de las obligaciones mencionadas anteriormente, la LSSI reconoce a los destinatarios de las comunicaciones comerciales electrónicas la posibilidad de revocar en cualquier momento el consentimiento prestado a la recepción de dichas comunicaciones, simplemente notificándolo al remitente, debiendo habilitarse para ello procedimientos sencillos y gratuitos e informarlos de manera accesible por medios electrónicos.

El envío masivo de comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente o el envío, en el plazo de un año, de más de tres comunicaciones comerciales por los medios aludidos a un mismo destinatario, cuando en dichos envíos no se cumplan los requisitos establecidos en el artículo 21 de la LSSI, se considerará como una infracción grave, pasible de multa de multa de 30.001 hasta 1 50.000 euros, según establecen los artículos 38 y 39 de la LSSI.

Contratación electrónica

La Ley asegura la validez y eficacia de los contratos que se celebren por vía electrónica, aunque no consten en soporte papel. Se equipara la forma electrónica a la forma escrita y se refuerza la eficacia de los documentos electrónicos como prueba ante los Tribunales, resultando también éstos admisibles en juicio como prueba documental.

Pueden celebrarse por vía electrónica todo tipo de contratos, salvo los relativos al Derecho de familia y sucesiones, por ejemplo adopciones, matrimonio o testamento. Si los contratos deben ir seguidos del cumplimiento de ciertos requisitos formales, como su elevación a escritura pública o su inscripción en algún Registro, dichos requisitos seguirán siendo exigibles para que el contrato sea plenamente válido o eficaz.

El prestador de servicios de la sociedad de la información que lleve a cabo un proceso de contratación electrónica tendrá, en síntesis, las siguientes obligaciones:

Antes de iniciar el procedimiento de contratación, deberá poner a disposición del usuario, mediante técnicas adecuadas al medio de comunicación utilizado, de forma permanente, fácil y gratuita, información clara, comprensible e inequívoca sobre:

- Los trámites o pasos que debe seguir para celebrar el contrato.
- Si va a archivar el documento electrónico del contrato y si va ser accesible.
- Los medios técnicos que pone a su disposición para identificar y corregir los errores en la introducción de los datos, antes de confirmarlos.
- La lengua o lenguas en las que puede formalizarse el contrato.
- Las condiciones generales de contratación que, en su caso, rijan el contrato.

La obligación de poner a disposición la información anterior se dará por cumplida si el prestador la incluye en su página o sitio web.

Cuando a los servicios se acceda mediante dispositivos que cuenten con pantallas de formato reducido (ej. móviles) se dará por cumplida la obligación si se facilita la dirección de Internet donde se encuentre dicha información.

Una vez realizado el contrato, el prestador debe:

- Confirmar la recepción de la aceptación, ya sea por medio de un acuse de recibo por correo electrónico u otro medio de comunicación equivalente, ya sea a través de un medio equivalente al utilizado en el procedimiento de contratación.

Las anteriores obligaciones quedan exceptuadas en dos supuestos:

- Cuando hubiera un acuerdo entre las partes en tal sentido y ninguna de ellas tuviera la condición de consumidor, y
- Cuando el contrato se haya celebrado exclusivamente mediante el intercambio de correo electrónico u otro medio de comunicación electrónica equivalente.

La seguridad

La contratación por medios telemáticos plantea el problema de la seguridad de que se está contratando y con quien se esta haciendo (identificación). También existe el problema de saber que lo que se recibe es lo mismo que la otra parte ha querido enviar (autenticación) y que se ha recibido completo (integridad)

A pesar de que la mayoría de contratos pueden realizarse de forma electrónica , existen algunos contratos que exigen algún formalismo que impide completarlos de forma telemática.

Sin embargo, existe un instrumento que sirve para garantizar la seguridad de las compras a través de internet y que permite conocer la identidad de la persona o empresa que nos remite la información: la firma electrónica. Consiste en un conjunto de caracteres electrónicos que se unen al documento enviado y que confirman que el mensaje que se está recibiendo ha sido efectivamente emitido por la persona que lo envía. Esto se denomina firma electrónica, la cual también acredita que la información no ha sido modificada o alterada durante su recorrido. Posteriormente se tratará más en profundidad.

Conclusión del contrato

Es importante conocer cuando y donde queda concluido el contrato ya que hay que distinguir entre una contratación entre ausentes o entre presentes. De esta forma se puede saber que normativa aplicar o el juez competente en caso de discrepancias.

El Tratado de Bruselas considera que la legislación a aplicar es la del país de origen, aunque existen tendencias que dicen lo contrario, que se debería aplicar la legislación del país del consumidor. La ventaja de aplicar la legislación del país origen es que se aprovecha en gran medida la potencia de la contratación por internet, sin embargo tiene como desventaja que el consumidor tiene mas complicado realizar reclamaciones y el ejercicio de sus derechos.

Contratación en masa y consumidores

En muchos casos la contratación se lleva a cabo mediante ofertas genéricas que el comerciante realiza a través de la red. En estos casos se habla de contratos tipo de adhesión. Tienen el inconveniente de que el consumidor no puede discutir ninguna de las clausulas o condiciones del contrato.

Para regular este tipo de contratos, existe la Ley General para la defensa de los consumidores y usuarios, que ofrece una protección al consumidor al impedir las clausulas abusivas.

Ventajas e inconvenientes

El comercio electrónico posee ventajas sobre el comercio tradicional, y, por tanto, la contratación electrónica cuenta con esas mismas ventajas:

Eliminación de barreras geográficas.

- Contratos más ventajosos para las partes, ya que acceden a cualquier contrato sin necesidad de estar presentes en el mismo lugar físico.

- Posibilidad de realizar contratos internacionales al alcance de la mano.
- Ampliación de mercados, tanto a consumidores como a empresas.
- Ahorro considerable de tiempo y dinero en las gestiones.
- Contratación más flexible para las partes, produciendo iguales efectos jurídicos.
- Mayor rapidez y agilidad en la celebración de los contratos y en sus fases.

Y al igual que el comercio electrónico tiene con una serie de inconvenientes, la contratación electrónica tiene los mismos problemas:

- La seguridad en el modo de pago electrónico es una de las principales preocupaciones de los consumidores.
- El tratamiento de los datos personales proporcionados por los consumidores en el momento de la compra, es un aspecto negativo a tener en cuenta.
- La identificación de las partes, ya que al no encontrarse en el mismo lugar físico requiere otros métodos de autenticación algo más complicados.
- La logística y distribución de los servicios adquiridos continúa siendo un problema para los consumidores.
- Los gastos de envío de los productos adquiridos, según los consumidores, continúan siendo elevados.
- La ley aplicable en cada caso concreto es otro de los inconvenientes que los consumidores apuntan para llevar a cabo contratación por medios electrónicos.

Firma electrónica

La evolución tecnológica y la dimensión mundial de Internet han hecho necesario un planteamiento abierto a diferentes tecnologías y servicios de autenticación y en esta dirección ha surgido un sistema electrónico alternativo que sirve para sustituir a la firma manuscrita y que a la vez cumple sus mismas funciones, es decir, asegurar la identidad de las partes contratantes, y vincularlas en cuanto a las declaraciones de voluntad que realicen, o lo que es lo mismo, al contenido del contrato.

Esto se consigue gracias a la "firma electrónica" y a los proveedores de "servicios de certificación". Consiste en un instrumento generado por documento electrónico relacionado con la herramienta de firma en poder del usuario, y que es capaz de permitir la comprobación de la procedencia y de la integridad de los mensajes intercambiados y ofreciendo bases para evitar su repudio. Con ello se alcanza el vínculo contractual o la autenticidad de un documento al igual que si se tratara de una firma manuscrita.

La Directiva 1999/93/CE del Parlamento Europeo y del Consejo de la Unión Europea, creó un marco jurídico para la firma electrónica y para determinados servicios de certificación, con el fin de garantizar un adecuado funcionamiento del mercado comunitario y además formuló la necesidad de buscar acuerdos transfronterizos para garantizar la interoperabilidad a nivel mundial.

Esta Directiva pretende mantener un marco jurídico coherente en toda la Comunidad, conscientes de que ese marco claro aumentará la confianza en las nuevas tecnologías. Igualmente contribuye al uso y al reconocimiento legal de la firma electrónica. Es importante alcanzar el equilibrio entre las necesidades de los consumidores, de las empresas y de la propia administración y además de todo ello, para contribuir a la aceptación general de los métodos de autenticación electrónica, debe de garantizarse la admisibilidad de la firma electrónica como prueba en procedimientos judiciales de los estados miembros.

Para incrementar la confianza de los usuarios en sus comunicaciones y en el comercio electrónico, los proveedores de servicios de certificación deberán de observar las normativas sobre protección de datos y el respeto de la intimidad.

Esta Directiva entiende por firma electrónica *"los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación..."* (Artículo 2.1).

Igualmente distingue la firma electrónica de la denominada firma electrónica avanzada, un especie de firma electrónica cualificada, y la define como *"...la firma electrónica que cumple con los siguientes requisitos: estar vinculada al firmante de manera única; permitir la identificación del firmante; haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control; y estar vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable."* (artículo 2.2).

La firma electrónica avanzada comúnmente la conocemos como firma digital. Desde el punto de vista jurídico, esta distinción resulta importante, pues los efectos jurídicos de una firma electrónica serán equiparables a los de la firma manuscrita únicamente cuando se trate de una firma electrónica avanzada o firma digital artículo 5).La Ley española 59/2003, de firma electrónica, en su artículo 3, define igualmente la firma electrónica, cuyas características se detallan en el apartado *"Clases de firma electrónica"* de este trabajo

Funcionamiento de la firma electrónica

La firma electrónica se instrumenta mediante un sistema de "criptografía asimétrica".

La criptografía es la rama de las matemáticas que estudia el cifrado de información legible e información que no puede ser leída directamente, al tener que ser descifrada. La criptografía es el arte de cifrar y de descifrar los mensajes intercambiados entre un emisor y un receptor.

Los sistemas de criptografía utilizados en las tarjetas digitales, utilizan un algoritmo asociado a una llave para convertir un mensaje inicial en un mensaje codificado que no puede ser decodificado más que mediante un algoritmo de decodificación asociado a una llave de desencriptación.

Existen dos esquemas clásicos de encriptación:

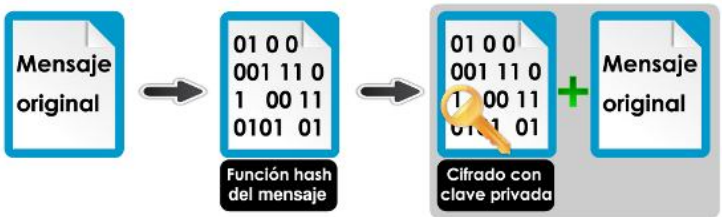
- *La encriptación simétrica.*
    - Obliga a al emisor y receptor del mensaje a utilizar la misma clave para encriptar y desencriptar el mismo (como por ejemplo el criptosistema DES, Data Encription Standard, desarrollado por IBM),
- *La encriptación asimétrica o criptográfica de claves públicas.*
    - Está basada en el concepto de pares de claves, de forma que cada uno de los elementos del par (una clave) puede encriptar información que solo la otra componente del par (la otra clave) puede desencriptar.

El par de claves se asocia con un solo interlocutor, así un componente del par (la clave privada) solamente es conocida por su propietario mientras que la otra parte del par (la clave pública) se publica ampliamente para que todo el mundo pueda verla (en este caso destaca el famoso criptosistema RSA cuyas iniciales son las de sus creadores: Rivest, Shamir y Adelman). Esta clave pública es dada por un tercero que es el conocido como "autoridad de certificación".

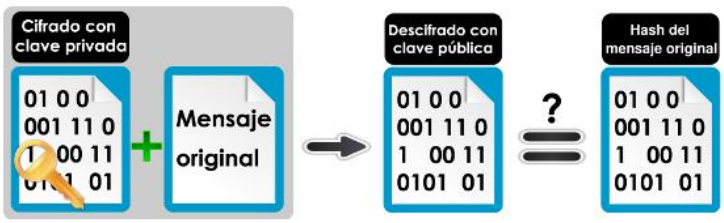
El sistema se compone de cuatro etapas:

- A cada usuario se le asigna una clave pública.
- Igualmente, cada usuario posee una clave privada que sólo él conoce, y que puede cambiar cuantas veces desee.
- Se crea un directorio de claves públicas accesibles al público general.
- El usuario de la red envía sus mensajes con la clave pública del destinatario encriptada con su clave privada. El destinatario sólo podrá abrir el mensaje con la clave pública junto con su clave privada.

Desde el punto de vista del emisor, el esquema de funcionamiento es:



Desde el punto de vista del receptor, el esquema que se sigue es:



Es un método que habitualmente se viene utilizando con total aceptación de los usuarios, ya que garantiza adecuadamente la seguridad y la confidencialidad de lo que se transmite.

Por tanto, la firma electrónica es un bloque de caracteres que se añade a un documento o fichero para acreditar quien es su titular (autenticación) y también para detectar que no haya habido ninguna manipulación subsiguiente de los datos (integridad). En la firma el titular utiliza el código personal que el solo conoce (criptografía asimétrica) y esto es lo que impide que después se pueda negar su autoría (no revocación o no repudio). De este modo el titular de la firma queda vinculado por el documento emitido e igualmente la validez de la firma podrá ser conocida por cualquier persona que disponga de la clave pública de titular.

Para la firma electrónica "escrita" se necesitará un pad o dispositivo de firma electrónica que sea capaz de capturar o registrar la firma escrita y todos sus aspectos, tales como tiempo, presión y trazado. También necesitará un programa capaz de codificar la firma electrónica de modo seguro y asimétrico en un documento electrónico con poder probatorio. El sistema que utilice habrá de ser capaz de captar la firma escrita

de modo que, en caso de juicio, y a pesar de tratarse de una firma electrónica, un grafólogo pueda verificar su autenticidad .Al realizar una firma electrónica, el sistema informático del titular introduce un algoritmo sobre el documento a firmar obteniendo un extracto de longitud determinada y específico para este documento de modo que si se produjere una mínima modificación posterior, se generaría un extracto totalmente diferente y por ello, no se correspondería con el original que firmó el titular. El extracto conseguido, cuya longitud oscila entre 128 y 160 bits, se somete seguidamente a un cifrado mediante la clase secreta del titular.

El algoritmo más utilizado en este procedimiento de encriptación asimétrica es el RSA. Con el se obtiene un extracto final cifrado con la clave privada del autor, que se añadirá al final del texto o mensaje para que se pueda verificar la autoría e integridad del documento por aquella persona interesada que disponga de la clave pública del autor.

Ahora, una vez realizada la firma electrónica habrá de determinarse su validez y para ello el software del receptor, previa introducción en el mismo de la clave pública de remitente (obtenida a través de una Autoridad de Certificación), descifrará el extracto cifrado del autor y a continuación calculará el extracto hash que le correspondería al texto del mensaje y, si el resultado coincide con el extracto anteriormente descifrado, se considera válida; en caso contrario significaría que el documento ha sufrido una modificación posterior y por tanto no es válido.

La firma electrónica conlleva una serie de claras ventajas:

- Mediante la firma electrónica se suprime el choque de medios, es decir, se evita la impresión en papel para la firma y se protegen adecuadamente los datos transmitidos.
- Se facilita la identificación tanto del emisor del mensaje como del receptor.
- Como la firma es intransferible, la firma electrónica escrita es una forma de identificación que al contrario que las contraseñas y llaves no se puede robar ni olvidar.
- La firma es sin duda un acto voluntario y además permite que el contenido de los mensajes lanzados a la red, sea irrevocable y no repudiable.

- La firma es un proceso reconocido por todos que da constancia de un acuerdo voluntario.
- El sujeto firmante no tiene que ser socio de ninguna compañía certificadora para poder utilizar la firma electrónica escrita.
- La firma capturada mediante la firma electrónica escrita puede ser examinada por expertos grafólogos (comparando, por ejemplo, la firma electrónica contra otra realizada sobre papel)

No obstante, este sistema también posee una serie de desventajas, como:

- El sistema por sí solo no es infalible y los riesgos no se pueden eliminar en su totalidad, y por ello es necesario utilizar un adecuado sistema de distribución de claves públicas.
- De otra parte, el sistema de distribución deberá estar debidamente protegido y debe ser administrado por una persona o entidad autorizada expresamente para ello

Clases de firma electrónica

Como ya se ha visto anteriormente, existen tres tipos de firma electrónica. En el Artículo 3 de la Ley de Firma Electrónica 59/2003.vienen recogidas las definiciones de los tipos de firma. En dicho artículo se expone que 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. Esto es la firma básica

La firma electrónica avanzada es 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.

Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. 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.

Certificados electrónicos

Para generar confianza en el usuario, el entorno internet ha de ser seguro. Es por eso que existe el concepto de "identidad digital". Esto es identificador digital único dentro de la red que permite a su poseedor ser identificado como tal dentro de la misma.

Los certificados electrónicos son dispositivos que posibilitan el almacenamiento de diversos datos relativos al propietario de los mismos (datos personales, claves, etc) y permiten identificarlo en la red, garantizando tanto la emisión de los datos, como su recepción, la integridad de la información transmitida, la confidencialidad y lo más importante, el no repudio de la transacción.

En el marco jurídico comunitario, los certificados de seguridad han sido expresamente definidos como: *"...la certificación electrónica que vincula unos datos de verificación de firma a una persona y confirma la identidad de ésta..."* (Artículo 2.9 de la Directiva 1999/93/CE).

La Ley 59/2003 de Firma Electrónica, en su artículo 6, ofrece el siguiente concepto: Un certificado electrónico es un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad. El firmante es 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.

Estos certificados deben ser emitidos por las autoridades de certificación, también conocidas con el nombre de proveedores de servicios de certificación. Al igual que existe una firma electrónica general y otra cualificada, en el caso de los certificados de seguridad se habla también de certificados ordinarios y certificados reconocidos. Éstos últimos son certificados que ofrecen mayores garantías, ya que reúnen una serie de requisitos que aumentan su seguridad:

El artículo 11 de la Ley de Firma Electrónica nos dice que como mínimo un certificado reconocido incluirá los siguientes datos:

- La indicación de que se expiden como tales.
- El código identificativo único del certificado.
- La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.
- La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.
- La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad o a través de un seudónimo que conste como tal de manera inequívoca y, en el supuesto 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.

Los certificados reconocidos podrán asimismo contener cualquier otra circunstancia o atributo específico del firmante en caso de que sea significativo en función del fin propio del certificado y siempre que aquél lo solicite. . Si los certificados reconocidos admiten una relación de representación incluirán una indicación del documento público que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales, de conformidad con el apartado 2 del artículo 13

Antes de la expedición de un certificado reconocido, los prestadores de servicios de certificación deberán cumplir las siguientes obligaciones:

- Comprobar la identidad y circunstancias personales de los solicitantes de certificados con arreglo a lo dispuesto en el artículo siguiente.
- Verificar que la información contenida en el certificado es exacta y que incluye toda la información prescrita para un certificado reconocido.
- Asegurarse de que el firmante está en posesión de los datos de creación de firma correspondientes a los de verificación que constan en el certificado.
- Garantizar la complementariedad de los datos de creación y verificación de firma, siempre que ambos sean generados por el prestador de servicios de certificación.

Servicios de Certificación

La identidad en la Red está basada en la existencia de las terceras partes de confianza, que son las entidades que verifican y dan fe de la identidad de los internautas. Los Servicios de certificación son entidades cuyo fin es el de verificar la identidad y otros datos relevantes de una persona para que ésta pueda identificarse en la Red.

Existen diferentes entidades de certificación que emiten certificados de seguridad para personas, para empresas, para colectivos, para colegios profesionales, para universidades o para entes públicos. Entre otros tenemos los siguientes prestadores:

- ANCERT (Agencia Notarial de Certificación), Banesto CA, CATCert, CERES (Fábrica Nacional de Moneda y Timbre), CICCP, Dirección General de la Policía y de la Guardia Civil, Firmaprofesional S.A., Izempe SA, Telefónica Empresas, etc.

Los certificados emitidos por cada prestador suelen estar vinculados a determinados colectivos de usuarios. Así, por ejemplo, un DNI electrónico emitido por la Policía será inicialmente aceptado para realizar trámites con la administración pública, mientras que un certificado emitido por un Colegio profesional será aceptado como instrumento electrónico que identifique al colegiado respecto a su actividad profesional.

Estas entidades, son la parte fiable que acredita la correspondencia entre una determinada clave y el usuario propietario de la misma. Actúan de forma similar a un notario electrónico que garantiza la veracidad de la información puesta en la red. En definitiva, son los órganos encargados de otorgar confianza en la infraestructura de las claves públicas, ya que resulta absolutamente necesario confiar en una tercera parte de toda solvencia que garantice la identificación de una persona física o jurídica a través de una clave pública.

Conforme al artículo 2.11 de la Directiva 1999/93/CE los Proveedores de Servicios de Certificación (PSCs), son *"...la entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica"* También son conocidos como prestadores de servicios de certificación o entidades de certificación.

El artículo 2 de la Ley 59/2003 los define como la persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica.

Los servicios de certificación podrán ser prestados tanto por instituciones públicas como privadas, sin que para ello deba solicitarse una licencia previa. No obstante, los servicios de certificación deberán cumplir con ciertos requisitos y obligaciones que se exponen en los siguientes apartados.

Obligaciones

Conforme a los artículos 17 a 21 de la Ley 59/2003, podemos clasificar las obligaciones a que están sujetos los prestadores de servicios de certificación, del siguiente modo:

- Obligaciones generales
    - Los PSCs que deseen emitir cualquier clase de certificado, deberán cumplir las siguientes obligaciones de carácter general:
    - Comprobar la identidad y demás datos personales del solicitante
    - Facilitar al signatario el dispositivo de creación y verificación de firma
    - No almacenar ni copiar los datos de creación de firma del solicitante
    - antes de la emisión del certificado, deberán informar al solicitante sobre el precio, condiciones de uso y limitaciones del certificado
    - Mantener un registro público de los certificados emitidos
    - En caso de cese de su actividad, deberán comunicarlo este hecho con la debida antelación (mínimo dos meses) a los titulares de los certificados
    - Estar inscritos en el Registro de Prestadores de Servicios de Certificación
- Obligaciones específicas: Además de las citadas obligaciones generales, los PSCs que emitan certificados reconocidos deberán cumplir las siguientes obligaciones específicas:
    - Indicar la fecha y hora de la expedición y/o revocación del certificado
    - Demostrar fehacientemente la fiabilidad de sus servicios
    - Garantizar rapidez y seguridad en la prestación de sus servicios
    - Contar con empleados cualificados para los servicios ofertados

- Utilizar sistemas y productos fiables que garanticen la seguridad técnica de la certificación
- Contar con medidas para prevenir la falsificación de certificados
- Utilizar sistemas fiables y seguros de almacenamiento
- Disponer de recursos económicos suficientes, que sirvan de garantía frente a una eventual responsabilidad por daños y perjuicios causados negligentemente
- Conservar durante un período de tiempo (generalmente 15 años) la información relativa al certificado emitido, para el caso de que dicha información pueda ser utilizada como prueba en algún procedimiento judicial o administrativo.

El conjunto de obligaciones citadas (generales y específicas) tiene como objetivo proporcionar seguridad y confianza en la prestación de los servicios de certificación y servir de garantía de calidad del servicio.

Responsabilidades

Conforme al artículo 23 de la Ley 59/2003, como principio de carácter general, los PSCs responden civilmente por los daños y perjuicios que pudieran causar a sus usuarios o a terceros cuando actúen con negligencia en el cumplimiento de sus obligaciones. Los PSCs son responsables, por tanto, no sólo frente al titular del certificado sino también frente a cualquier tercero que se vea perjudicado por actos u misiones de los PSCs. Se trata de una la responsabilidad subjetiva contractual y extracontractual.

Además, una vez revocado el certificado los PSCs seguirán estando sujetos a responsabilidad en cierta medida. No existe un criterio claro para esclarecer el alcance de esta responsabilidad. Por un lado, se considera que los PSCs deben estar sujetos a una responsabilidad limitada. Esto es, los PSCs responderían únicamente de los daños y perjuicios que causaran por el incumplimiento negligente de la obligación de publicar la revocación del certificado o de la obligación de inscribirlo en el registro de certificados

del PSC, con lo cual, el titular acabaría asumiendo todos los riesgos derivados de un posible robo o extravío de la clave. Por otro lado, se intenta extender la responsabilidad de los PSCs para que respondan también por las posibles utilizaciones ilegítimas de la clave de firma.

Entre los límites a la responsabilidad de los PSCs que admite la ley se encuentran los siguientes:

- Límites de uso:
    - Los PSCs podrán limitar su responsabilidad emitiendo el certificado únicamente para un uso determinado (ciertos ámbitos, transacciones, operaciones, etc). Con esta limitación, el PSC no será responsable cuando el certificado se utilice más allá de la finalidad para la cual fue expedido.
- Esta limitación debe establecerse de forma expresa, clara e inequívoca en el propio certificado, facilitando con ello que los terceros conozcan la limitación existente.
- Limites de cuantía:
    - Estos límites se dirigen a proteger a los PSCs, limitando su responsabilidad a un importe máximo relacionado con el valor de las transacciones realizadas utilizando el certificado.

Los PSCs pueden elegir el modo de utilizar sus certificados, en lo relativo a la cuantia de las transacciones:

- Establecer que el certificado sólo sea utilizado en transacciones que no excedan de una determinada cuantía. Por ejemplo, emisión de un certificado que sólo puede ser utilizado en operaciones cuyo monto no exceda de 24 millones de euros. El mayor problema es que el certificado puede ser utilizado en una gran cantidad de operaciones de distinto tipo, siempre que no se superaran los límites cuantitativos establecidos, por lo cual, la responsabilidad del PSC se incrementa.
- Establecer que el certificado sólo pueda utilizarse hasta una determinada cantidad máxima con independencia de las transacciones que se realicen. Por

ejemplo, un certificado válido hasta que se cubra la cantidad total de 24 millones de euros. El inconveniente que tiene es que si bien los derechos de los PSCs se encuentran más protegidos, ésta limitación perjudica los intereses de los usuarios de los certificados, pues éstos deberán estar controlando en todo momento el valor total de las operaciones realizadas con el certificado.

Firma electrónica de personas jurídicas

El caso de la firma electrónica de personas jurídicas, es un caso especial que presentó problemas en sus inicios ya que el el RDL 14/1999 negó inicialmente el reconocimiento de la firma electrónica a las personas jurídicas, pero el legislador de 2003 reconsideró dicha negativa inicial, y finalmente, ha terminado incorporándose al Ordenamiento jurídico la posibilidad de que la persona jurídica (así como la persona física) pueda ser titular directo, y no por medio de representante orgánico o voluntario, de un certificado de firma electrónica o digital. Así lo recoge el artículo 7.1 de la Ley 59/2003 al disponer que *"Podrán solicitar certificados electrónicos de personas jurídicas sus administradores, representantes legales y voluntarios con poder bastante a estos efectos"*. De igual manera también es recogido por el artículo 6.2 cuando señala que *"firmante es 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"*.

Con el reconocimiento legal de esta modalidad de firma de la persona jurídica realmente se está introduciendo en nuestro Ordenamiento un "poder al portador" a favor de quien solicita y custodia la firma electrónica.

Para actuar en la contratación, operar en la facturación electrónica o intervenir en el comercio electrónico, la persona jurídica puede valerse de dos mecanismos:

- Conferir a una persona física el poder para quedar obligado, dentro de los límites en el mismo atribuidos, por el uso de su firma electrónica como persona física representante
- Obligarse directamente mediante el uso del certificado de firma electrónica de persona jurídica de que es titular de forma propia e independiente de las personas que la representan o lo emplean.

La atribución a la persona jurídica de una firma electrónica es un hecho ficticio ya que la custodia y su empleo o aplicación práctica corresponde a la persona física que, en nombre y en representación de aquella, la ha solicitado. Así lo deja claro la Ley 59/2003 cuando dispone que *"La custodia de los datos de creación de firma asociados a cada*

certificado electrónico de persona jurídica será responsabilidad de la persona física solicitante, cuya identificación se incluirá en el certificado electrónico" (art. 7.2).

Cuando el firmante sea una persona jurídica, el solicitante del certificado electrónico asumirá la responsabilidad, y no la Autoridad de certificación expedidora del mismo, que se genere a la propia persona moral o a terceros de buena fe (art. 23.3 LFE), debida a su negligencia, descuido o mala fe en el cumplimiento de una serie de obligaciones que se resumen en:

- No haber proporcionado al prestador de servicios de certificación información veraz, completa y exacta sobre los datos que deban constar en el certificado electrónico o que sean necesarios para su expedición o para la extinción o suspensión de su vigencia, cuando su inexactitud no haya podido ser detectada por el prestador de servicios de certificación.
- La falta de comunicación sin demora al prestador de servicios de certificación de cualquier modificación de las circunstancias reflejadas en el certificado electrónico.
- Negligencia en la conservación de sus datos de creación de firma, en el aseguramiento de su confidencialidad y en la protección de todo acceso o revelación
- No solicitar la suspensión o revocación del certificado electrónico en caso de duda en cuanto al mantenimiento de la confidencialidad de sus datos de creación de firma.
- Utilizar los datos de creación de firma cuando haya expirado el período de validez del certificado electrónico o el prestador de servicios de certificación le notifique la extinción o suspensión de su vigencia.
- Superar los límites que figuren en el certificado electrónico en cuanto a sus posibles usos y al importe individualizado de las transacciones que puedan realizarse con él o no utilizarlo conforme a las condiciones establecidas y comunicadas al firmante por el prestador de servicios de certificación (art. 23.1 LFE).

Usos de la firma electrónica

El certificado de seguridad electrónico puede ser utilizado para muchas aplicaciones, desde la firma de documentos hasta la identificación dentro de una organización. Un certificado de seguridad es una identidad digital, y por tanto como identidad, sirve entre otros, para los siguientes usos:

- *Firma digital.*
    - El certificado de seguridad se utiliza para firmar todo tipo de documentos digitales, desde e-mails hasta contratos electrónicos. Esto implica garantía de no repudio, de conocimiento inequívoco de quien es el emisor del documento y de la integridad del documento, es decir, que el documento firmado es el original y que nadie ha modificado su contenido después de su firma. También es usado para firmar ciertas operaciones, como por ejemplo, formalizar una orden de transferencia que se pueda realizar en un home-banking, esto da la garantía a las partes de que dicha orden de transferencia sólo la puede realizar el titular, y la entidad bancaria guarda la prueba de dicha orden y capacidad.
- *Seguridad en la comunicación.*
    - El certificado sirve para codificar una comunicación entre dos personas, haciendo que toda la información transmitida sea confidencial. Con ello se garantiza que cualquier documento enviado por una persona a otra estará cerrado y sólo podrá ser abierto por su legítimo destinatario. A su vez es igualmente aplicable cuando el emisor o bien el receptor no son una persona sino un servidor de internet, y por tanto, la información enviada o recibida de este servidor estará codificada con el fin de que sólo el auténtico receptor pueda leerla.
- *Seguridad entre las partes:*
    - Un problema recurrente es la seguridad de saber que el receptor sea realmente quien dice ser y que por lo tanto el emisor posea dudas acerca de si enviar una información o no. Aquí es donde la autoridad de certificación que es la parte de confianza tiene un papel importante puesto que certifica a este como el auténtico receptor. Un caso específico

es el de los servidores web. La consulta del certificado digital que pueda tener la web nos va a certificar que realmente esta web pertenece a la empresa

- *Identificación ante un acceso restringido.*
    - Tradicionalmente se usa a la hora de entrar a un sistema digital restringido el par *login* + *password*, sistema con un nivel de seguridad muy bajo. El sistema de identificación más seguro es el certificado digital. En el momento de entrar en Intranets, accesos a una red local, a un servidor determinado, o incluso a aplicaciones específicas, la tecnología utilizada debería ser la del certificado de seguridad electrónico.
- *Firma de software.*
    - El certificado digital es utilizado para firmar software. Esto permite a la entidad que va a utilizar el software garantizar que este es el original, conocer quien lo ha creado, y muy importante, que con posterioridad a su firma, nadie lo ha modificado. Esto garantiza que dicho software no contiene virus, y si los contiene, es el propio creador del software quien los ha incorporado, pudiendo ir en contra de este con una prueba firmada.

Nombres de dominio

Internet es una red de redes de computadoras interconectadas a través de un protocolo de comunicación común, el TCP/IP (Transfer Control Protocol / Internet Protocol). El protocolo IP identifica a cada ordenador que se encuentre conectado a la red mediante su correspondiente dirección. Esta dirección es un número de 32 bit que debe ser único para cada Host, y normalmente suele representarse como cuatro cifras de 8 bit separadas por puntos, según el protocolo IP v4 actualmente utilizado. La dirección de Internet (IP Address) se utiliza para identificar tanto al ordenador en concreto como la red a la que pertenece, de manera que sea posible distinguir a los ordenadores que se encuentran conectados a una misma red.

Sin embargo, estas direcciones IP representadas por medio de cuatro grupos de tres cifras decimales, separadas por puntos (ej. 192.168. 0.1) son difíciles de memorizar, por lo que, a cada dirección IP se le asigna un nombre que sea más fácil de recordar. Esta complejidad en la navegación fue la causa de que apareciera la idea de implantar su reemplazo por nombres, y hacer conversiones de nombres a direcciones IP. Para ello, se utilizan los servidores DNS Domain Name Server, de modo que dada una dirección bajo un nombre, devuelven la IP que le corresponde. Es así como aparecen los nombres de dominio, que facilitan la navegación y que todos conocemos. En este sentido, los nombres de dominio vienen a ser direcciones de Internet fáciles de recordar y suelen utilizarse para identificar un sitio Web.

Todos los empresarios que buscan su presencia en Internet se plantean como objetivo inicial identificarse adecuadamente al público, mediante el registro de un nombre de dominio que, en líneas generales, coincidirá con el nombre comercial o marca de sus productos.

Así, en base a lo anterior, es posible distinguir dos enfoques distintos en los nombres de dominio. Desde un punto de vista informático, el nombre de dominio es una cadena de caracteres alfanuméricos, aceptados por las normas de sintaxis, utilizada como dirección de Internet asociada al código IP (Internet Protocol) y un nombre alfanumérico que identifica un ordenador o conjunto de ellos en Internet. Desde un punto de vista empresarial, el nombre de dominio es una dirección identificable desde cualquier

computadora y que es única y diferenciable en la Red. En este sentido, en el informe publicado por la OMPI (Organización Mundial de la Propiedad Intelectual) se define al nombre de dominio como la dirección fácilmente comprensible para el usuario, de un ordenador, normalmente en forma fácil de recordar o identificar.

Clases de dominio

Cuando se creó el Sistema de Nombres de Dominio en los años 80, el espacio de nombres se dividió en dos grandes grupos. El primero incluye los dominios, basados en los dos caracteres de identificación de cada territorio de acuerdo a las abreviaciones del ISO-3166. (Ej. *.es, *.fr) y se denomina ccTLD (Dominio de nivel superior de código de país ó Country Code Top level Domain), los segundos, incluyen un grupo de siete dominios de primer nivel genéricos, (gTLD), que representan una serie de nombres y multi-organizaciones: GOV, EDU, COM, MIL, ORG, NET e INT. Posteriormente, este grupo de dominios se ha ido ampliando.

Nombres de dominio de primer nivel

Son las extensiones de ámbito genérico, diferenciados por la finalidad del uso que se les dará. En éstos también están incluídos los ccTLD, los respectivos a los países como .es, .it o .fr para España, Italia y Francia respectivamente.

Nombres de dominio de primer nivel genéricos

Los Dominios Genéricos: (también son denominados dominios internacionales o globales), son los dominios básicos en Internet y los más utilizados a nivel mundial.

- .com: inicialmente previsto para empresas comerciales. Es el dominio más difundido en Internet.

- .org: inicialmente previsto para organizaciones sin ánimo de lucro, instituciones y fundaciones.
- .net: inicialmente previsto para empresas relacionadas con Internet.
- .info: esta terminación de dominio por regla general es utilizada por sitios web cuyo principal cometido es la difusión o publicación de contenidos informativos.
- .biz: esta terminación proviene de la abreviación de business (negocios en inglés) y su utilización está enfocada a la temática de los negocios. Es lo mismo que el .com, pero para la zona de Europa.
- .edu: los dominios con esta terminación son utilizados para fines educativos.
- .tv: Usados en empresas de vídeo, cine y televisión principalmente.
- .cc: Esta extensión tiene un especial interés para aquellos que pretenden conseguir un dominio global y no tienen posibilidad de conseguir el .com que desean.
- .ws: Las siglas .ws se identifican con Web Site, por lo que se trata de una magnífica opción para todo tipo de sitios web. Además, debido a su novedad, es mucho más probable conseguir el dominio deseado.
- .name: Proviene del inglés “name” que significa “nombre”, por lo que se trata de una opción totalmente nueva para registrar nuestro nombre propio o apodo.
- .pro: Para uso específico reservado a profesionales de determinadas categorías, agrupados en subdominios. Ejemplo: .med.pro (médicos). Deberán acreditar su pertenencia al colegio u organización profesional correspondiente.
- .aero: De uso restringido para la industria de los servicios aéreos: compañías aéreas, aeronáuticas, aeropuertos y servicios aéreos.
- .coop: Reservado a las cooperativas y hace falta demostrar la cualidad de cooperativa a través de las organizaciones locales correspondientes.
- .museum: Dominio de uso restringido para los museos. Permite en un segundo nivel el nombre del museo que se trate (prado.museum, picasso.museum).

Nombres de dominio de primer nivel de código de país

También denominados dominios territoriales ó dominios geográficos. Son los dominios mantenidos por cada país. Estos dominios territoriales son utilizados por las organizaciones y empresas que desean establecerse en Internet y proteger la identidad de su marca o su nombre comercial en un país concreto. Los dominios territoriales tienen sus terminaciones compuestas por 2 letras.

Algunos ejemplos de nombres de dominio territoriales son:

- .es, para servicios de España.
- .eu, para la región de Europa
- .cr para servicios de Costa Rica
- .ru para servicios de Rusia
- .fr para servicios de Francia
- .do para servicios de República Dominicana
- .gt para servicios de Guatemala
- .mx para servicios de México
- .sv para servicios de El Salvador

Nombres de dominio de segundo nivel

Son los nombres de dominio, lo que cualquier persona puede registrar en cualquier momento. El dominio de segundo nivel de la página de la Universidad de Burgos es “ubu”, y el de primer nivel el .es.

Para el caso de España, los dominios territoriales de 2º nivel “.es” pueden ser solicitados por:

- Las personas físicas españolas o extranjeras que residan en España.
- Las entidades con o sin personalidad jurídica constituidas conforme a la legislación española.

- Las primeras sucursales de sociedades extranjeras inscritas en el Registro Mercantil.
- Los Órganos Constitucionales, el Defensor del Pueblo, el Consejo de Estado y el Tribunal de Cuentas, las Administraciones Públicas españolas y las entidades de Derecho Público con personalidad jurídica propia, así como los Departamentos Ministeriales y Consejerías de las Comunidades Autónomas.
- Las embajadas y consulados extranjeros acreditados en España y las organizaciones internacionales a las que España pertenezca.

Nombres de dominio de tercer nivel

Se pueden registrar dominios de tercer nivel bajo los dominios de segundos nivel. Son extensiones de los dominios, o también llamados subdominios. Por ejemplo, '.com.es' está reservado para crear dominios de tercer nivel, como 'empresa.com.es'.

En el caso de España, existen dominios territoriales de 3er nivel .com.es - .nom.es - .org.es - .gob.es - .edu.es:

- **.**com.es: Pueden ser registrados por personas físicas o jurídicas y entidades sin personalidad que mantengan vínculos con España.
- **.**nom.es: Podrán solicitarlo las personas físicas que mantengan vínculos con España.
- .org.es: Podrán solicitarlo las entidades, instituciones o colectivos con o sin personalidad jurídica y sin ánimo de lucro que mantengan vínculos con España.
- .gob.es: Podrán solicitarlo las Administraciones Públicas españolas y las entidades de Derecho Público de ella dependientes.
- .edu.es: Podrán solicitarlo las entidades, las instituciones o colectivos con o sin personalidad jurídica que gocen de reconocimiento oficial y realicen actividades relacionadas con la enseñanza o la investigación en España.

Registro de nombres de dominio

El registro de dominios es el proceso por el cual una persona pasa a tener el control sobre un nombre de dominio a cambio de pagar una cierta cantidad de dinero a un registrador.

Hay que saber que el nombre de dominio a registrar será el de segundo nivel, bajo un nombre de dominio de primer nivel.

El nombre de dominio de primer nivel bajo el que se quiere registrar el de segundo nivel puede ser un nombre de dominio genérico o territorial.

Registro de nombres de dominio bajo un gTLD

Desde el mes de octubre de 1998, el registro y asignación de los nombres de dominio de primer nivel genéricos ha sido atribuido al ICANN -The Internet Corporation for Assigned Names and Numbers. De acuerdo con sus estatutos, la principal función de la ICANN es la coordinación de la explotación y desarrollo del DNS.

Por ello, para registrar un nombre de dominio, el primer paso es buscar un registrador acreditado por la ICANN. Esta búsqueda puede realizarse en la página web de la ICANN.

El segundo paso, ya una vez dentro de la página web de la entidad registradora, es rellenar el impreso de solicitud de registro del nombre de dominio y abonar las tasas de dicho registro.

La solicitud del registro no conlleva ningún tipo de control sobre los datos de la solicitud ni sobre los derechos que se tenga sobre el nombre de dominio.

Los registradores tienen como política, el principio de “first come, first served”. De esta forma evitan pronunciarse sobre la licitud o no del registro. El único control que se lleva a cabo es que el nombre tenga una sintaxis correcta. Así se consigue una gran rapidez en la creación de nombres de dominio.

El tercer y último paso es esperar la confirmación de solicitud por parte de la entidad registradora.

A partir del registro de un nombre de dominio, se pasa a formar parte de una base de dato común de acceso libre n la que se indican los dominios registrados, el nombre de la entidad registradora y los datos del titular. Esto se hace para:

- Que cualquier persona pueda saber si un nombre de dominio se encuentra ya registrado o no.
- Que si existen problemas de controversia con el nombre de dominio, la persona que quiera realizar alguna acción ante los órganos de arbitraje, sepa contra quien debe hacerlo.

Registro de nombres de dominio bajo '.es'

El registro se debe hacer a través del órgano delegado de InterNIC. En España, es el ES-NIC.

La norma que regula la asignación de nombres de dominio bajo el ccTLD .es es el Plan Nacional de nombres de dominio de Internet bajo el código de país correspondiente a España. (.es).

Requisitos para la asignación de un nombre de dominio bajo .es

El registro de un nombre de dominio bajo .es solamente se podrá realizar mediante correo electrónico. Para poder registrar un nombre de dominio, se deben cumplir las reglas indicadas en el Plan Nacional.

No se puede transferir un nombre de dominio de una organización a otra. Para poder obtener el nombre de dominio de otra persona, se debe enviar el Formulario de Solicitud Electrónica (FSE) de baja de esa persona y posteriormente enviar el FSE de alta del

solicitante. Esto se hace para poder comprobar los derechos que la nueva persona tiene para la obtención del nombre de dominio. De esta forma se evitan fraudes.

Siempre que una persona tenga derecho a registrar un nombre de dominio y cumpla las normas del plan Nacional, el registro se le otorgara si es el primero que lo solicita. Si alguien posteriormente, también quiere registrar el mismo nombre de dominio, aunque tenga derechos sobre el nombre de dominio, no lo puede hacer.

Es un requisito el cumplimiento de las normas de sintaxis. El nombre debe construirse con letras de alfabetos de lenguas españolas, los dígitos y el guión.

También es un requisito el cumplimiento de las normas de derivación de nombres de dominio. Estas normas vienen recogidas en el apartado 8 del Plan Nacional, en el que se dice principalmente, que pueden ser:

- El nombre completo de la organización
- Un nombre abreviado y significativo del nombre completo de la organización.
- Uno o varios nombres comerciales o marcas de los que sean titulares o licenciatarios.

Derechos y deberes de los titulares de los nombres de dominio

Los derechos de los titulares de nombres de dominio son:

- Derecho a utilizar el nombre de domino a efectos de direccionamiento en el sistema de nombres de dominio.
    - Este derecho está condicionado al respeto de las nomas comunes para ala asignación de los mismo y al mantenimiento de las condiciones que permitieron su asignación
    - El cumplimiento puede ser comprobado por la autoridad de asignación de oficio o a instancia de parte.
    - El incumplimiento de las condiciones conlleva la cancelación por la autoridad de asignación, previa audiencia del interesado.

- Derecho a la continuidad y calidad del servicio que presta la autoridad de asignación.

Los deberes de los titulares de nombres de dominio son:

- Facilitar sus datos identificativos siendo responsables de su veracidad y exactitud.
- Respetar las reglas y condiciones técnicas que establezca la autoridad de asignación.
- Informar inmediatamente a la autoridad de asignación de todas las modificaciones que se produzcan en los datos asociados al registro del nombre de dominio.

Procedimiento para el alta del nombre de dominio bajo '.es'

El primer paso será comprobar que el nombre de dominio cumple las normas que señala el Plan Nacional. A continuación se envía el Formulario de Solicitud Electrónica (FSE) de asignación de un nombre de dominio. El envío del formulario implica el conocimiento de las normas y procedimientos, de las tarifas y de los requisitos técnicos necesarios.

Una vez enviado por correo electrónico el formulario, se deberá esperar a recibir un correo de confirmación en el que viene indicado un número de ticket.

Cuando la solicitud es aprobada, se envía por correo postal la factura. Es entonces cuando se debe enviar el formulario de Solicitud Firmado (FSF) para que quede constancia de la solicitud y del justificante de pago.

En el caso de que la solicitud sea rechazada, el interesado puede formular alegaciones y en el caso de que estas sean desestimadas, se puede interponer un recurso de alzada antes el Presidente de la Entidad Publica Empresarial Red.es.

Aspectos de interés a la hora de registrar los dominios

Hay que tener en cuenta que se puede elegir la forma de registrar un dominio:

- *Nombre de dominio delegado:*
  - El nombre de dominio estará activo desde el momento en que se conceda y es apto para su utilización desde ese mismo momento.
- *Nombre de dominio reservado:*
  - El nombre de dominio se reserva para un uso futuro. Nadie más puede utilizarlo ni reservarlo. El titular puede activarlo en cualquier momento.
- *Nombre de dominio MX:*
  - Hace referencia a aquel que quedara activo en el DNS con la información de encaminamiento de correo electrónico en Internet.

A la hora de completar el FSE, en la sección relativa a la organización usuaria del nombre de dominio, se deberá rellenar con los datos del usuario final del nombre de dominio, no con los datos del proveedor de servicio.

La persona de Contacto Administrativo es aquella persona que tenga la autoridad y responsabilidad última sobre el nombre de dominio objeto de registro.

La persona de Contacto Técnico es la persona que el ES-NIC contactará en caso de que sea necesario tratar remas técnicos relacionados con un dominio operativo. Este apartado puede dejarse en blanco en el supuesto que el dominio se haya solicitado como Reservado.

La persona de contacto de facturación es la persona a la que el ES-NIC enviará as facturas de alta y mantenimiento anual del dominio registrado, así como los avisos por impago.

Conflictos de nombres de dominio

Los nombres de dominios no son signos distintivos porque la ley no les otorga tal categoría, sin embargo son cumplen las mismas funciones y tienen las mismas características. La forma de adquirir los derechos sobre los Nombres de Dominio está regulada por normas de carácter técnico expedidas por la ICANN. Las entidades que se encargan de registrar los Nombres de Dominio no ejercen ningún tipo de control o vigilancia a efectos de impedir que con el registro de dominios se violen derechos de propiedad industrial, y advierten que en el supuesto de cometerse alguna infracción con el registro y uso del dominio el único responsable será el solicitante del registro. Es normal por tanto que esta falta de control lleve frecuentemente a la violación de la legislación sobre propiedad industrial y sobre competencia desleal.

Los conflictos entre las marcas y los nombres de dominio se detectan en el momento en que, empresas con derechos exclusivos sobre marcas preestablecidas lícitamente en el mercado tradicional o real, no pueden utilizarlas como nombres de dominio, porque terceras personas con derechos anteriores o sin ellos, habían llegado primero.

En el caso que estuviese provocada por actos de mala fe y con fines de lucro, se trataría del denominado Cybersquatting, práctica donde surgen litigios y enfrentamientos, especialmente respecto de empresas con un cierto prestigio o una cierta relevancia, ya sea en el ámbito regional, nacional o internacional, frente a aquellos particulares que se adelantaron y registraron nombres de dominio ajenos con la intención de revenderlos a sus titulares y poder obtener de ello un beneficio económico. La propia ICANN ha elaborado una Política Uniforme de Resolución de Controversias respecto de los nombres de dominio de nivel superior genéricos, sin perjuicio de poder acudir al arbitraje o, incluso, a los órganos judiciales como se verá mas extensamente en el siguiente apartado.

Otra de las situaciones que genera conflictos es el denominado “domain grabbing” o “domain piracyng”. Se trata de la piratería que realiza una persona que solicita el registro de un nombre de dominio que incluye, deliberadamente una marca o una expresión semejante a ella, con la finalidad de transmitir posteriormente los derechos a cambio de un precio.

Sin embargo, lo más común es el denorminado cybersquatting o cyberocupismo, los cuales se pueden definir como el registro de mala fe de los nombres de dominio. Esta mala fe se manifiesta, fundamentalmente, en la especulación o en el objetivo de atraer visitantes. En el primer supuesto, el objetivo principal del titular del nombre de dominio se centra en especular o negociar con el titular legítimo de la marca, con el objetivo de pactar una transferencia del dominio en contraprestación de un precio por encima del inicialmente pagado. El titular suele asignar al dominio una página en blanco o una redirección a una página Web con contenidos pornográficos u ofensivos, normalmente con el fin de forzar o agilizar la negociación.

En el segundo supuesto, el titular del nombre de dominio pretende atraer visitantes a su página Web, mediante la confusión de los internautas que verdaderamente busquen la página Web o blog del titular de la marca afectada. El beneficio obtenido queda patente en el incremento considerable del número de visitas en forma de ganancia económica, por ejemplo incluyendo publicidad.

En cualquier caso, es conveniente no confundir estos actos ilegales con otras prácticas ancladas dentro de los parámetros de la ley, como las llevadas a cabo por los denominados “Domainers”, es decir, aquella persona que dedica su tiempo y su dinero a la inversión en dominios con el ánimo de revenderlos, alquilarlos o destinarlos a cualquier otro uso. Se denomina también “warehousing” a la práctica de registro en serie de nombres de dominio correspondientes a marcas. Muchas veces, el titular de dicho nombre de dominio ni siquiera lo utiliza, simplemente lo tiene a su nombre.

En resumen, el cyberocupismo es el robo de una marca registrada con el objeto de impedir el registro del nombre de dominio por el titular de la misma, bien porque se han olvidado de renovar el mismo o, bien porque hay una nueva extensión TLD disponible y el propietario de la marca se ha descuidado.

Una variante del robo de dominios o cybersquatting es el denominado typosquatting. Esta práctica fraudulenta consiste en el registro de aquellos nombres de dominio que hacen referencia a expresiones gramaticalmente parecidas a los diferentes tipos de marca registradas, que inevitablemente se producen cuando tecleamos mal una dirección, fruto de un error o una equivocación. Por ejemplo teclear “diarideburgs.com”

o cualquier otra expresión similar cuando se quiere escribir “diariodeburgos.com”. Por ello, es conveniente que se registren no sólo los punto com, sino los punto net, org, y el propio del país, además de redireccionarlos al dominio correcto.

El cybersquatting es una práctica que aprovecha numerosos vacíos legales relacionados con los nombres de marca en la red. El principio ya comentado del “first come, first served”, permite registrar un nombre de dominio a la primera persona en llegar sin comprobar si realmente pertenece a la organización. Esta práctica puede afectar gravemente a la identidad y reputación en Internet en el contexto de “sitios Web clonados”. Alguien reproduce fielmente la imagen corporativa, diseño y contenidos del sitio Web original, los copia para crear un sitio Web clonado que además tendrá un nombre de dominio muy parecido, el internauta puede llegar a interactuar con el sitio Web falso pensando que se trata de original.

Procedimiento de resolución de conflictos de la ICANN

La ICAAN tiene una Política Uniforme de Solución de Controversia en materia de nombres de dominio desde Agosto de 1999. Esta política establece clausulas y condiciones en relación con una controversia que surja entre la persona que registre un dominio y cualquier otra parte.

Iniciación del procedimiento

Cualquier persona o entidad puede iniciar el procedimiento presentando una demanda a cualquier proveedor aprobado por la ICANN. La demanda se presenta de manera electrónica y el demandado está obligado a someterse a un procedimiento administrativo en caso de que un tercero sostenga ante el proveedor competente que:

- El demandado tiene un nombre de dominio parecido y que crea confusión con marcas y productos que el demandante tenga derechos
- El demandado no tiene derechos o intereses legítimos respecto del nombre de dominio.
- El demandado posee un nombre de dominio registrado y utilizado de mala fe.

Pruebas del demandante

El demandante debe demostrar los tres puntos señalados anteriormente. Si el demandante no puede probar uno solo de ellos, el nombre de dominio seguirá siendo utilizado por el demandado.

La política de solución de controversia indica unos factores que son los que demuestran o no el derecho sobre el nombre de dominio.

Se debe demostrar la mala fe. Esto es que el demandado haya registrado el nombre de domino con el fin e vender, alquilar o ceder el registro a un tercero (normalmente el demandante), o que lo haya registrado para causar un daño en un competidor.

Se debe demostrar el interés legítimo del nombre de dominio. El demandado puede probarlo si este es conocido corrientemente por el nombre de dominio, si ha utilizado el nombre de domino anteriormente o ha efectuado preparativos para su utilización, etc…

Escrito de contestación por parte del demandado

En el plazo de veinte días naturales a partir de la fecha de comienzo del procedimiento, el Demandado debe enviar un escrito de contestación impreso ó en formato electrónico (excepto aquellos anexos que no estén disponibles en este formato), al Proveedor y al Demandante simultáneamente.

En ese escrito, el demandado debe responder a las declaraciones y alegaciones que figuran en la Demanda y debe incluir todas las razones por las que considera que debe mantener la titularidad del nombre de dominio objeto de la controversia.

Puede incluir cualquier tipo de prueba documental sobre las que se base el escrito de contestación, en especial aquellas que acrediten que no se ha producido el registro de nombre de dominio de carácter especulativo o abusivo o aquellas que puedan desvirtuar los derechos previos alegados por el demandante.

Deberá incluir en el escrito de contestación una declaración responsable de que la información contenida en la misma, a su leal saber y entender, es completa y exacta, y que el escrito de contestación no se presenta de forma abusiva.

En caso de que el demandado no presente escrito de contestación, el experto resolverá la controversia basándose en la demanda.

Nombramiento del grupo de expertos y plazo de resolución

Si las partes no se ponen de acuerdo en un grupo de expertos de tres miembros, el proveedor nombrará un experto elegido entre los que figuren en su relación de expertos,

valorando su disponibilidad y los conocimientos requeridos para resolver el procedimiento.

El nombramiento se efectuará en el domicilio del proveedor en el plazo de cinco días naturales a partir de la recepción del escrito de contestación de la demanda.

Una vez que haya sido nombrado el experto, el proveedor le remitirá el expediente y notificará el nombre y la dirección electrónica de contacto del experto a las partes y a Red.es.

Las facultades de este experto son las siguientes:

- El experto dirigirá el procedimiento en la forma que estime más apropiada para su adecuada tramitación con arreglo al reglamento. El experto garantizará la igualdad de trato para las partes.
- El experto decidirá sobre la admisibilidad de las pruebas.
- El experto podrá solicitar a las partes, cuando lo considere pertinente, que aporten aclaraciones o documentos adicionales a la demanda o el escrito de contestación.
- El experto resolverá sobre la admisibilidad de las aclaraciones o documentos adicionales que las partes estén interesadas en aportar al procedimiento en cualquier fase del mismo.

Costes del procedimiento y resolución

El demandante debe responder de las costas del procedimiento. La resolución que decida el órgano administrativo puede decidir lo siguiente acerca del nombre de dominio:

- Que siga utilizándolo el demandado porque no se han demostrado los tres puntos antes señalados.

- Que pase al demandante porque se ha demostrado que el demandado no tiene derechos y tiene mala fe.
- Que se cancele el nombre de dominio, cuando el nombre de dominio sea ofensivo para el demandante.

Recursos

Contra la resolución del órgano administrativo, tanto el demandante como el demandado, pueden interponer recursos.

El registrador espera a conocer si se ha iniciado alguna vía judicial de resolución de la controversia antes de ejecutar la decisión que haya tomado el panel de expertos.

Aplicación Práctica

La generalización del uso de Internet en cada vez más áreas de negocio y en la vida cotidiana ha supuesto un gran cambio económico. Las reglas de negocio son diferentes a las de la economía tradicional y se hace imprescindible revisar antiguos esquemas y estrategias de negocio.

El funcionamiento de la economía y del comercio conlleva el movimiento de información (virtual) y de bienes físicos. Estas dos realidades deben coordinarse para el correcto funcionamiento del comercio.

El comercio electrónico ha conllevado un gran reto para la logística, pero a su vez ha sido una gran herramienta. La revolución tecnológica que ha presentado el uso de internet ha dado una gran amplitud al comercio, obligando a éste al uso de fórmulas como la integración en la cadena de suministros, el just in time, producción ajustada, etc…

Los aspectos logísticos que utilizan las posibilidades del comercio electrónico, internet y las nuevas tecnologías de la información han sido bautizados con el nombre de “e-logistics”.

La naturaleza del funcionamiento del comercio electrónico conlleva un gran cambio en la forma de vender los productos, pero también en la forma de entregarlos.

El uso del comercio electrónico tiene unas características específicas y esto origina unas necesidades logísticas especiales que las empresas que utilicen el comercio electrónico deben satisfacer si desean tener éxito.

Se puede decir que la logística del comercio electrónico es una variante de la logística tradicional con finalidad propia. Esta finalidad es realizar de forma más eficiente todas las actividades logísticas necesarias para satisfacer los requerimientos específicos procedentes del comercio electrónico.

En la siguiente tabla se pueden ver las diferencias entre la logística tradicional y la logística del comercio electrónico.

	Logística Tradicional	Logística comercio electrónico
Tipo de Envío	Masivo: camión, contenedor.	Paquete
Cliente	Estratégico	Desconocido
Estilo demanda	Empujar (push)	Tirar (pull)
Flujo de mercancías	Unidireccional	Bidireccional
Valor medio pedido	Mas de 1.200 €	Menos de 100 €
Puntos de destino	Concentrados	Dispersos
Demanda	Estable	Estacional
Información	Escasa	Toda la cadena de suministro

El comercio electrónico requiere nuevas formulas y cambios en los métodos logísticos tradicionales.

Es importante destacar el auge del comercio electrónico en los últimos años y el la tendencia de crecimiento de empresas de comercio electrónico que subcontratan servicios logísticos.

LOGIBUR nace como una empresa con el ímpetu de aprovechar la oportunidad de negocio que supone el auge del comercio electrónico.

LOGIBUR pretende ser una empresa que opere en el ámbito del B2B y del B2C. El gran número de tiendas virtuales que existen en internet requiere de empresas de logística flexibles como LOGIBUR. De igual modo, los mercados electrónicos inter-empresariales (B2B market places) necesitan asociarse con una empresa que proporcione servicios logísticos.

Asociándose a una empresa como LOGIBUR se consiguen grandes ahorros logísticos que son determinantes para cualquier empresa.

El buen hacer de LOGIBUR es fruto de la especialización y el amplio conocimiento en gestión logística. La calidad del servicio resulta imprescindible para conseguir la confianza de los clientes y garantiza que dichos clientes repetirán la visita y la compra.

El registro de dominios es un factor realmente importante para adquirir una presencia verdadera y consolidada en Internet, importancia que en el caso de las empresas o negocios asciende a niveles altísimos, convirtiéndose actualmente en parte imprescindible de su identidad corporativa e incluso en la parte fundamental de la misma.

El nombre de LOGIBUR ha sido elegido durante el proceso de planificación y creación de la empresa y uno de los factores determinantes para su elección ha sido que el nombre de dominio se encuentra disponible.

En principio, la empresa esta interesada en utilizar un nombre de dominio que coincida con su nombre comercial o marca. Esto se hace para que los usuarios y clientes identifiquen la empresa de forma rápida en la red. De este modo, se puede observar que los nombres de dominios, constituyen, junto con las marcas y patentes un activo muy valioso. Se puede decir que registrar un nombre de dominio es una nueva forma de uso de las marcas.

Por esta razón, una tarea básica es comprobar si el nombre de dominio se encuentra libre. Para realizar la comprobación hay que acudir a la página web de nic.es e introducir LOGIBUR en la sección de buscador de dominios. Se comprueba que el dominio está libre y se procede a registrar todos los dominios posibles (con el fin de evitar problemas en el futuro) con cualquiera de los agentes registradores disponibles

Posteriormente se alojará la página web en uno de los servidores de LOGIBUR y todos los dominios registrados apuntaran al mismo sitio.

Como se ha visto en el apartado anterior “Usos de la firma electrónica”, el certificado electrónico puede ser utilizado en diversos campos como la firma de e-mails y contratos electrónicos, dar seguridad a las comunicaciones, dar seguridad a las partes, identificar accesos o firmar software.

Se ha decidido solicitar un certificado electrónico que permita realizar algunas de las tareas anteriormente citadas. Para ello se ha utilizado la entidad acreditadora Fábrica Nacional de Moneda y Timbre (FNMT).

El primer paso es entrar en la web de la Fábrica Nacional de Moneda y Timbre y pulsar sobre el enlace “Obtenga su Certificado”

En la siguiente ventana se debe ir al apartado “Empresas”, subapartado “Cert. Persona jurídica”. En esa pantalla pulsar sobre “Solicitud vía Internet de su certificado”.

En la nueva ventana se tecleará el NIF y se podrá escoger entre longitud de clave Grado Medio (longitud de clave 1024) “Grado Alto” (longitud de clave 2048). Se elegirá esta última opción por ser más segura. Posteriormente, se pulsará sobre el botón “Enviar petición

Es importante saber que existen unos procesos de seguridad (para evitar la obtención de la firma digital por terceros) y que solo se puede recoger la firma desde el mismo ordenador que se ha solicitado.

Una vez aceptado el certificado que obliga a instalar la FNMT, aparece una ventana con un código que debe ser apuntado o imprimido.

El último paso es acudir a una oficina de registro para completar la solicitud como por ejemplo, una oficina de Hacienda con el NIF del representante, el código de solicitud, el CIF de la empresa, el certificado de estar de alta en el Registro Mercantil y toda aquella documentación que nos sea solicitada.

Una vez validada la identidad, se expide el certificado electrónico, el cual se puede descargar desde la propia página de CERES en el apartado “Descarga del Certificado”.

Una vez descargado el certificado se procederá a realizar alguna copia de seguridad.

Propiedad industrial

La propiedad industrial entiende por invención "*toda idea, creación del intelecto humano capaz de ser aplicada en la industria*". La propiedad industrial es la propiedad que adquiere por sí mismo el inventor o descubridor con la creación o descubrimiento de cualquier invención relacionada con la industria; y el productor, fabricante o comerciante con la creación de signos especiales con los que distinga de los demás de la misma categoría.

La propiedad industrial ampara la protección de la creatividad, la invención e ingenio que son las pertenencias más valiosas de cualquier persona, empresa y sociedad. Por otra parte, el interés general exige que las concesiones exclusivas de propiedad industrial no sean perpetuas, y ello determina que las leyes concedan a los derechos citados un tiempo de duración distinto según las distintas modalidades que discriminen esta propiedad especial y temporal.

La propiedad industrial es una rama de la propiedad Intelectual. La propiedad intelectual tiene que ver con las creaciones de la mente: las invenciones, las obras literarias y artísticas, los símbolos, los nombres, las imágenes, los dibujos y modelos utilizados en el comercio.

La propiedad intelectual se divide en dos categorías:

- *El Derecho de Autor*
    - Es la protección jurídica que se otorga al titular del derecho de una obra original del que es inventor. Se trata del derecho patrimonial oponible al público que confiere a su titular un monopolio exclusivo de explotación sobre un objeto no tangible pero dotado de un valor económico. El derecho de autor comprende dos categorías principales de derechos: los derechos patrimoniales y los derechos morales.
        - *Derechos patrimoniales*

- Son los derechos de reproducción, radiodifusión, interpretación y ejecuciones públicas, adaptación, traducción, recitación pública, exhibición pública, distribución, entre otros.

▪ *Derechos morales*

- Es el derecho del inventor a oponerse a cualquier deformación, mutilación o modificación de su obra que pueda ir en detrimento de su honor y reputación.

- *La Propiedad Industrial*

o Abarca las invenciones, los diseños industriales, las marcas, los lemas, las denominaciones comerciales, incluye también la represión a la competencia desleal, las patentes, la creación técnica de las invenciones aplicables a la industria, los diseños industriales, los descubrimientos, así como también los signos distintivos, incluida las marcas de fabrica, de comercio y de agricultura, las denominaciones de origen los nombres y lemas comerciales. En otras palabras la propiedad industrial abarca:

▪ Los derechos de patentes y

▪ El derecho marcario el cual tiene por objeto la producción comercial.

Entre estas dos ramas de la propiedad intelectual podemos notar las siguientes diferencias:

- En la propiedad industrial el diseño debe ser registrado para su protección legal; mientras en el derecho de autor la obra queda protegidas sin ninguna formalidad.

- En la propiedad industrial los derechos concedidos a través del registro son eminentemente territoriales, salvo algunas excepciones; mientras en el derecho de autor las obras pueden ser protegidas de manera automática en todos los

países miembros del Convenio de Berna, sin cumplimiento de ninguna formalidad.

- En la propiedad industrial el derecho sobre el diseño es mas limitado pues solo se circunscribe al de excluir a terceros de la fabricación, importación, oferta; mientras en el derecho de autor, el derecho patrimonial comprenderá el exclusivo de realizar, autorizar o prohibir todo uso de la obra, por cualquier medio o procedimiento conocido o por conocerse, salvo excepción legal expresa, sin importar que su uso este vinculado o no a la presentación de un producto.

- En el ámbito de la propiedad industrial el periodo de protección del diseño es mucho menor, ya que puede girar entre los cinco y diez años a partir de la solicitud; mientras en el derecho de autor el plazo mínimo de protección de las obras de arte aplicado es de veinticinco años contados a partir de su realización, pero en la mayoría de las legislaciones nacionales han extendido esta duración equiparándola a la de las obras literarias y artísticas por cincuenta años.

- En la propiedad industrial, no son registrables los diseños que sean contrarios a la moral, al orden público o a las buenas costumbres; por el contrario en el derecho de autor no se conoce figura de la legalidad, es decir, la obra queda protegida aunque eventualmente sean contrarios a la moral y a las buenas costumbres.

Clases de protección

Existen dos clases de protección: los derechos de propiedad industrial (creaciones con protección distinta a la de los derechos de propiedad intelectual) y la protección de los signos distintivos de empresas (marcas).

Creaciones del intelecto aportadas a la industria

Patentes

Una patente es un título que reconoce el derecho de explotar en exclusiva la invención patentada, impidiendo a otros su fabricación, venta o utilización sin consentimiento del titular. Como desventaja, la patente se pone a disposición del público para general conocimiento.

El derecho otorgado por una patente no es tanto el de la fabricación, el ofrecimiento en el mercado y la utilización del objeto de la patente (que siempre tiene y puede ejercitar el titular), sino, "el derecho de excluir a otros" de la fabricación, utilización o introducción del producto o procedimiento patentado en el comercio.

La patente puede referirse a un procedimiento nuevo, un aparato nuevo, un producto nuevo o un perfeccionamiento o mejora de los mismos.

La duración de la patente es de veinte años a contar desde la fecha de presentación de la solicitud. Para mantenerla en vigor es preciso pagar tasas anuales a partir de su concesión.

Modelos de utilidad

El modelo de utilidad protege invenciones con menor rango inventivo que las protegidas por Patentes, consistentes, por ejemplo, en dar a un objeto una configuración o estructura de la que se derive alguna utilidad o ventaja práctica.

El dispositivo, instrumento o herramienta a proteger por el modelo de utilidad se caracteriza por su utilidad y practicidad y no por su estética como ocurre en el diseño industrial.

El alcance de la protección de un modelo de utilidad es similar al conferido por la patente.

La duración del modelo de utilidad es de diez años desde la presentación de la solicitud. Para el mantenimiento del derecho es preciso el pago de tasas anuales.

Modelos y dibujos industriales y artísticos

Un diseño industrial otorga a su titular un derecho exclusivo (a utilizarlo y a prohibir su utilización por terceros sin su consentimiento), sobre la apariencia de la totalidad o de una parte de un producto, que se derive de las características de, en particular, las líneas, contornos, colores, forma, textura o materiales del producto en sí o de su ornamentación.

Los diseños podrán ser bidimensionales o tridimensionales.

La duración de la protección conferida por los diseños industriales es de cinco años contados desde la fecha de presentación de la solicitud de registro, y podrá renovarse por uno o más períodos sucesivos de cinco años.

Protección de los signos distintivos

La idea principal es que en un sistema de economía de mercado es imprescindible que existan signos distintivos que permitan diferenciar a las empresas y a sus productos.

La normativa relativa a la protección de los signos distintivos de la empresa está dirigida a conseguir que los clientes potenciales puedan identificar y distinguir en el mercado los diversos productos y servicios que ofrecen, los empresarios y sus establecimientos. Para éstos el requisito fundamental e indispensable que han de presentar es la aptitud diferenciadora, que permita distinguirlos e individualizarlos en el mercado.

Marcas

Una marca es el derecho exclusivo de utilizar un signo o medio material, sea cual sea su clase y forma, que sirve para distinguir un producto o servicio en el mercado, de manera que el público pueda reconocer y distinguir.

Pueden ser marcas las palabras o combinaciones de palabras, imágenes, figuras, símbolos, gráficos, letras, cifras, formas tridimensionales (envoltorios, envases, formas del producto o su representación).

Nombre comercial y rótulo de establecimiento

Un nombre comercial es un titulo que concede el derecho exclusivo a utilizar cualquier signo o denominación como distintivo de una empresa. Los nombres comerciales son independientes de los nombres de las sociedades inscritas en el Registro Mercantil.

El rótulo de establecimiento es un signo o denominación que sirve para darlo a conocer al público y diferenciarlo de otros destinados a actividades idénticas o similares.

Protección jurídica del software

Uno de los bienes a proteger desde el punto de vista jurídico en la sociedad de la información son los programas de ordenador o software.

La protección jurídica del software se garantiza mediante lo dispuesto en la Ley de Propiedad Intelectual y convenios y normativa internacional aplicables.

El ámbito de protección de software que es protegido por la Ley engloba tres realidades distintas: el programa fuente, el programa objeto y los manuales explicativos.

La Ley expone que la originalidad y creatividad de un programa de ordenador es un requisito de base para protegerlo jurídicamente.

Existe una problemática a la hora de definir la autoría de un programa de ordenador. Según la Ley, sólo la persona física es autor o creador de una obra literaria, artística o científica. Esta afirmación se reafirma con el Derecho de autor como un derecho personalísimo.

Sin embargo, el art. 5 de la LPI introduce una excepción al principio general de atribución de derechos exclusivamente personas físicas. La Ley prevé que las obras puedan tener como autor una persona jurídica pero con carácter restrictivo.

La obra en colaboración es aquella que resulta de la incorporación de distintas aportaciones de los autores cada una de las cuales son objetivamente identificables entre sí. El art. 97.3 LPI indica que cuando el software tenga como origen de creación la colaboración de varias personas, los derechos de propiedad intelectual sobre el software pertenecerán a todas las personas en la proporción que ellos determinen. Hay que destacar que, a falta de pacto en contrario, y, según el art. 7 de la Ley, si nada se pacta sobre la proporción de derechos de cada uno, éstos pertenecerán por partes iguales a todos ellos.

Una vez divulgada la obra de este tipo, ningún autor podrá rehusar injustificadamente su consentimiento para su explotación en la forma en que se divulgó.

Pero existe otro modo de creación de un programa informático más común, esto es la obra creada por el autor asalariado.

La LPI 97.4 expresa que los *derechos de explotación* sobre el programa informático pertenece al empresario o empleador, salvo que se establezca por pacto lo contrario y según los siguientes puntos:

- El empresario no podrá utilizar la obra o disponer de ella para un sentido o fines diferentes de los que se puedan deducir que constituyen el núcleo necesario de la actividad habitual del empresario.
- Se ceden en exclusiva al empresario los derechos de explotación con el alcance necesario para el ejercicio de su actividad habitual en el momento de la entrega de la obra.

La titularidad de los derechos de explotación sobre la obra pertenece al empleador siempre que se cumplan los tres puntos siguientes:

- Cuando el programa informático se cree por el trabajador en el ámbito usual y pactado del contrato de trabajo.

- Cuando el programa informático se haya creado en el ejercicio de las funciones confiadas por el empresario al trabajador
- Cuando el trabajador haya creado el software siguiendo las instrucciones expresas del empresario

Existe otro modo de creación de programas informáticos, la obra colectiva. La obra colectiva se define en el art. 8 de la LPI. A diferencia de la obra en colaboración, la obra colectiva se caracteriza por que en ella existe una persona, física o jurídica, que la edita y divulga. Esta persona asume la responsabilidad en la creación misma de la obra colectiva, en la medida en que toma la iniciativa de la creación y de la coordinación de su desarrollo creativo. La obra es concebida como una creación autónoma y distinta en la que se fusionan diferentes aportaciones de autores individuales.

De acuerdo con lo dispuesto en el art. 97.2, el autor de una obra colectiva, es la persona jurídica o física que la edite y divulgue bajo su nombre.

La cesión de derechos que ha planificado la Ley respecto a este tipo de obras tipo de obras tiene como resultado que el editor aparezca como autor a todos los efectos y que, las facultades morales sobre la obra sean titularidad suya. Si los autores colaboradores pretenden una porción de los derechos sobre la obra colectiva, entonces deberán preverlo expresamente mediante cláusula al efecto.

Protección jurídica de las bases de datos

Las bases de datos son creaciones originales, y como tales, están protegidas por la LPI. La protección no sólo afecta a la colección de datos, obras, y demás materiales ordenados, sino también al material electrónico necesario para el funcionamiento de la misma, por ejemplo, su diccionario, índice o sistema de consulta o presentación de la información. La Ley expresa que el autor de la base de datos tiene un derecho exclusivo de explotación de la misma durante toda su vida más sesenta años después de su muerte. Esta protección conlleva que, aunque la base de datos se actualice, o se hagan cambios de poca importancia en su contenido o estructura, la base de datos permanece sustancialmente la misma, y por tanto, los derechos permanecen intactos

La reproducción o distribución de la obra sin la autorización del titular de sus derechos de explotación, son acciones delictivas en España. En el caso de que el delito se realice desde un país extranjero, la obra estará igualmente protegida gracias al convenio de Berna. Este convenio internacional sirve de protección de las obras artísticas y literarias. El convenio, al cual pertenecen España y otros ciento once países, ofrece protección a *"las colecciones de obras literarias o artísticas tales como las enciclopedias y antologías, que por la selección o disposición de las materias, constituyan creaciones intelectuales"*. Dentro de esta categoría se incluyen las bases de datos.

En la vida de una base de datos, ésta puede modificarse redefiniendo campos y asociaciones de manera que la estructura de la base de datos original se modifique sustancialmente .En estos casos puede surgir una base de datos distinta que origina que los periodos de protección comiencen a contabilizarse de nuevo.

El artículo 133. 1 de la LPI establece: *"El derecho sui generis sobre una base de datos protege la inversión sustancial, evaluada cualitativa o cuantitativamente, que realiza su fabricante ya sea de medios financieros, empleo de tiempo, esfuerzo, energía u otros de similar naturaleza, para la obtención, verificación o presentación de su contenido"*.

La protección por tanto es a raíz de la inversión y el esfuerzo realizado por el fabricante.

Aplicación práctica

El registro de la marca "LOGIBUR" proporcionará a la empresa el derecho exclusivo a impedir que terceros comercialicen servicios similares con la misma marca o utilizando una marca tan similar que pueda crear confusión.

Es importante registrar la marca para poder obtener éxito en el mercado. De no hacerlo, empresas de la competencia puede ofrecer servicios similares utilizando la misma marca o similar. Este hecho conllevaría una disminución en los ingresos de LOGIBUR y un daño en la reputación y en la imagen de la empresa.

Si la marca goza de buena reputación entre los clientes, también podría emplearse para obtener financiación de instituciones financieras.

Se puede observa que el registrar la marca LOGIBUR, conlleva claras ventajas:

- Garantiza que los clientes distingan los servicios respecto a otras empresas del sector
- Permite a LOGIBUR diferenciar sus servicios
- Proyecta la imagen y la reputación de la empresa
- Posibilidad de concesión de licencias y obtención de ingresos a través de regalías
- Representa un importante activo comercial
- Útil para obtener financiamiento.

Para la protección jurídica de los Signos Distintivos, la OEPM concede Marcas de productos o servicios y Nombres Comerciales. Los Rótulos de establecimiento ya no pueden ser registrados.

Para realizar los trámites, LOGIBUR contratará los servicios de un Agente de la Propiedad Industrial que, según la Ley 17/2001, de Marcas , son: *"las personas físicas inscritas como tales en el Registro de la Propiedad Industrial que, como profesionales liberales, ofrecen habitualmente sus servicios para aconsejar, asistir o representar a terceros para la obtención de las diversas modalidades de la Propiedad Industrial y la defensa ante el Registro de la Propiedad Industrial de los derechos derivados de las mismas."*

Es importante saber que la duración de la protección conferida es de diez años a partir de la fecha del depósito de la solicitud y se puede renovar indefinidamente. Para el mantenimiento en vigor de la marca es preciso el pago de tasas.

En la página web de la Oficina Española de Patentes y Marcas se puede consultar un listado de los Agentes de la Propiedad Industrial, así como información, formularios de solicitud y tasas sobre los distintos derechos de propiedad industrial concedidos por organizaciones supranacionales con efectos a nivel comunitario o internacional. Debido

a que LOGIBUR operará a nivel internacional, será necesario registrar la marca y el nombre comercial de la empresa mediante la vía internacional, de esta forma se obtiene protección en hasta 78 países (entre ellos España) depositando una única solicitud en la OEPM para su traslado a la Oficina Internacional de OMPI, teniendo el registro los mismos efectos que si la solicitud hubiese sido presentada en cada uno de los países designados. Cada país puede conceder o denegar la protección. Se trata de una solicitud única pero que, una vez registrada en todos los países designados, da lugar a un conjunto de registros nacionales igual que si se hubieran solicitado país por país.

Protección jurídica del software y de las bases de datos

LOGIBUR necesitará del uso de software de diverso tipo para el correcto funcionamiento de la empresa.

Por una parte contará con diversos programas adquiridos mediante contratos de licencia. De esta manera, tan solo se tiene el derecho legal de ejecutar el software, y el licenciante mantiene todos los secretos intrínsecos del software e incluso la facultad de poder otorgar otros permisos. Dentro de esta categoría se encontraran los sistemas operativos (tanto de ordenadores personales como de servidores), paquetes ofimáticos, sistemas gestores de bases de datos, etc.

Por otro parte, LOGIBUR, como empresa de logística necesitará software concreto para el desempeño de su labor. Un ejemplo de este tipo de software son los programas de planeación de rutas. Existen multitud de programas de planificación de rutas e itinerarios para vehículos. Este tipo de software sirve para administrar eficazmente la flota de vehículos, reduciendo los costes de transporte, mejorando la atención al cliente y el control del transporte. Se consigue disminuir los plazos de entrega y una mayor capacidad de respuesta ante las exigencias de los clientes.

Primeramente se plantean las características que serán necesarias en el software:

- Planificación de rutas e itinerarios
- Gestión de flotas centralizada

- Calculo de rutas e itinerarios
- Planificación diaria del transporte
- Planificación estratégica
- Seguimiento y reprogramación de rutas para flotas en tiempo real
- Gestión de múltiples usuarios combinando panificación central con control local

Una vez estudiadas las características del software que se encuentra en el mercado, y observando la necesidad de contar con un software específico, LOGIBUR ha decidido optar por contratar un software a medida. El programa será encargado a una empresa informática y será una obra colectiva protegida por la LPI. El presidente de LOGIBUR será el titular de los derechos morales y patrimoniales

Por su parte, la base de datos de LOGIBUR se encontrara protegida por el derecho sui generis y la Propiedad intelectual.

Contratación Informática

Se entiende por contrato informático: aquel contrato que tiene por objeto bienes y servicios informáticos.

Los bienes informáticos comprenden tanto los elementos materiales que constituyen el soporte físico o hardware, su unidad central de procesamiento, periféricos, complementos, en definitiva todos los otros equipos que componen el soporte físico del elemento informático; como los bienes inmateriales o software que proporcionan las órdenes, los datos, los procedimientos y las instrucciones en el tratamiento automático de información, cuyo conjunto constituye el soporte lógico del elemento informático.

En cambio, los servicios informáticos abarcan todos aquellos servicios que se relacionan con el tratamiento automatizado de la información y sirven de apoyo a la informática, tales como el diseño, el análisis y el mantenimiento del sistema.

Características de los contratos informáticos

Debido a su naturaleza, este tipo de contratos cuenta con una serie de características que lo diferencian de otros contratos:

Son contratos atípicos ya que no están regulados mediante ninguna Ley o Reglamento. La regulación se encuentra en la autonomía de la voluntad de las partes y en las normas especiales que puedan ser aplicables.

Su objeto está compuesto normalmente por varias prestaciones y es debido al carácter técnico. Esto provoca que haya varias normas de aplicación.

Las partes contratantes poseen distinto grado de conocimiento. Esto provoca inseguridad jurídica y que en la negociación sea necesario la intervención de abogados y técnicos informáticos. Estos deben trabajar en equipo para conseguir una precisa redacción del contrato, especialmente de sus anexos.

Debido a su complejidad, los contratos pueden incluir diversas prestaciones propias de contratos tipificados. Esto hace que puedan ser calificados como contratos híbridos entre varios.

Otra característica importante de este tipo de contratos es la larga gestación de los mismos ya que en muchas ocasiones es necesaria una larga negociación entre las partes.

Partes de un contrato informático

En la contratación informática se ven involucrados varios elementos, a los que podemos denominar complementarios, que sé interrelacionan entre sí. Así, distinguiremos entre: sujetos, parte expositiva, clausulas o pactos y anexos, que se analizan a continuación.

Los sujetos

No es lo mismo la contratación informática realizada entre profesionales de la informática, que la contratación informática realizada entre un profesional de la informática y un tercero.

Por ello, la identificación y la situación profesional de los intervinientes reviste gran importancia, debiendo fijar, no solamente quien adquiere cada responsabilidad proveniente de la contratación y a quien representa, sino también que conocimientos o formación profesional, todo esto se da para determinar una buena fe, de informar correctamente a la otra parte y de proporcionar claridad a las cláusulas y obligaciones del contrato.

Cuando hablamos de contratos informáticos no debemos olvidarnos que en muchos casos estamos en presencia de contratos de adhesión, en los cuales, la mayoría de las cláusulas se encuentran predispuestas.

Parte expositiva

En esta parte se expone, de forma clara y concreta, el por qué y el para qué del contrato. Es importante señalar que dentro de los contratos informáticos es imprescindible fijar de forma sencilla, por que se realiza el contrato y cuales han sido los condicionantes o circunstancias que han movido a las partes a unirse mediante esta relación contractual.

Para ello, se fijaran los intereses de cada cual, especificando las necesidades de uno y la oferta del otro; dejando bien claro que es lo que ofrece una parte y que es lo que acepta la otra y debiendo existir una coincidencia real sobre el objeto, o concepto que de el y de su utilidad respecto al fin perseguido, tienen cada una de las partes.

Por otro lado es de especial interés establecer claramente el negocio jurídico en el cual luego, de acuerdo con la teoría general para ese negocio en el ordenamiento, se pueda subsumir el caso e interpretar el contrato.

Clausulas

Partimos del principio de buena fe (tanto creencia como lealtad), y establecemos una obligación de colaboración en ambos sentidos, el suministrador debe colaborar con el usuario y el usuario debe colaborar con el suministrador.

El usuario debe respetar y seguir las directivas que le indique el suministrador y utilizar el equipo informático o los programas, siguiendo las instrucciones que, para su óptima utilización, le señale. El suministrador se exonera de responsabilidad en el caso en que exista una anomalía consecuencia del incumplimiento por parte del usuario de estas instrucciones de funcionamiento o manejo.

Estas cláusulas o pactos han de cumplir los siguientes requisitos:

- Obligaciones de las partes
- El deber de asesoramiento
- El cumplimiento del plazo

- Prohibición de subarrendar
- Definición de términos o conceptos obscuros
- Cláusula de garantía

Anexos

Es fundamental que los contratos informáticos vayan acompañados de unos Anexos que incorporados a ellos, contengan diferentes desarrollos de elementos que forman parte sustancial del contrato.

Entre los Anexos tipo, que ayudan a describir el objeto y que siempre deben figurar, en un contrato informático destacan:

- Especificaciones del sistema a contratar.
- Especificaciones de los programas a desarrollar
- Pruebas de aceptación
- Resultados a obtener
- Análisis

Tipos de contratos informáticos

Los contratos informáticos se pueden clasificar en dos grupos:

- *Respecto al objeto:*
    - *Contratos de hardware:*
        - En los que se trata la parte física de los equipos.
    - *Contratos de software:*

        - Los contratos que tratan de la parte lógica de los sistemas. Pueden ser software base o de sistema o software de utilidad.
    - *Contratos de instalación llave en mano:*
        - Incluyen el hardware, el software, el mantenimiento y la formación a usuarios.
    - *Contratos de servicios auxiliares:*
        - Los que traten de servicios complementarios.
- *Respecto al negocio jurídico:*
    - Existen tantos tipos de contrato s como negocios jurídicos se realicen sobre este objeto. En los contratos informáticos, los mas utilizados son los siguientes:
        - De venta
        - De arrendamiento financiero
        - De alquiler
        - De opción a compra
        - De mantenimiento:
        - De prestación de servicios
        - De arrendamiento de obra
        - De préstamo
        - De deposito

Algunos de los contratos informáticos más usuales se detallan a continuación:

- *Contrato de Diseño de Sistemas de Información.*
    - Tiene por objeto la toma de datos, análisis, valoración y selección de sistemas de información (software y plataforma) con el fin de ajustarlo a las necesidades del cliente. En este tipo de contratos hay que tener muy en cuenta la existencia de equipo humano técnicamente capacitado para la ejecución del trabajo. También hay que tener en consideración la existencia de Consultores Homologados por Instituciones de reconocido prestigio. Algunas de las clausulas específicas a tener en cuenta son:
        - Fases de desarrollo.
        - Plazos: Cronograma de ejecución.

        - Documentación: Informe final.
        - Confidencialidad
        - Cesión de contrato y subarriendo.

- *Contrato de Dirección y Ejecución de Proyectos.*
    - Tiene por objeto la dirección y supervisión de la ejecución de trabajos establecidos en una Oferta o Consultoría previas. Del correcto funcionamiento del Comité de Control y Seguimiento dependerá en gran medida el éxito del proyecto. Es importante también la implicación del comité en la redacción de hitos y pruebas de aceptación con descargo del Director aclarando términos y conceptos técnicos. Algunas cláusulas específicas de este tipo de contrato son:
        - Pago.
        - Plazos.
        - Garantías.
        - Confidencialidad.
        - Cambios y modificaciones.
- *Contrato de Montaje y Certificación de Redes.*
    - Tiene por objeto la ejecución de trabajos de tendido de cableado y conexión de los elementos físicos necesarios para lograr el correcto medio de transmisión de los datos que deberá soportar el sistema. Puede tratarse de diversos tipos de redes (local, extensa, privada, virtual, etc.).Hay que tener en cuenta el correcto cumplimiento de especificaciones técnicas (Normas ISO-UNE), la certificación de la instalación según categoría y exigir la presentación de documentación acreditativa de la condición laboral del instalador de la proveedora. Clausulas específicas a tener en cuenta:
        - Preparación de locales.
        - Entrega e instalaciones.
        - Pruebas de aceptación.
        - Mantenimiento.
        - Manual y Documentación.
        - Garantías.

        - Cesión de contrato y subarriendo.
        - Seguridad e higiene en el trabajo.
        - Seguridad Social.

- *Contrato de adquisición de equipos informáticos.*
    - Tiene por objeto la entrega de elementos físicos (hardware) que soportan los datos de una determinada instalación, señalándose como contraprestación la entrega de un precio. No se diferencia en este caso los modos de adquisición. Los equipos deberán ser los adecuados para la aplicación, no por tratarse de equipos de "ultima generación" serán, ni los necesarios, ni los que mejor cumplan su cometido. Algunas clausulas específicas a desarrollar son:
        - Cláusulas específicas:
        - Precio.
        - Pago.
        - Repuestos.
        - Garantías.
        - Compatibilidad.
        - Manuales y Documentación.
        - Propiedad.
- *Contrato de adquisición de Sistemas Operativos.*
    - Tiene por objeto la adquisición de la licencia para la utilización de los programas necesarios para que funcione el software de aplicación. Tratándose de un producto normalmente conformado de antemano, se suele contemplar como contrato de adhesión. No hay que olvidar que es la base del funcionamiento del sistema, por ello debe ser capaz de soportar y compatibilizarse con prácticamente la totalidad de aplicaciones existentes en el mercado. La apertura del paquete puede suponer la aceptación tácita de las condiciones contractuales. Cláusulas específicas a tener en cuenta:
        - Derechos.
        - Manual y documentación.
        - Entrenamiento y formación.

- Compatibilidad.
- Soporte.
- Transmisión de Derechos.
- Propiedad.

- *Contrato de implementación de Sistemas Operativos.*
  - Tiene por objeto los servicios de instalación, parametrización, configuración, implantación y puesta en marcha del sistema operativo (monopuesto o redes). Puede tener múltiples niveles: perfiles de usuario, seguridad, planes de emergencia, auditorias, servicios de acceso remoto, etc. Algunas clausulas específicas de estos contratos son:
    - Manual y documentación.
    - Entrenamiento y formación.
    - Pruebas de aceptación
    - Confidencialidad.
    - Soporte.
    - Seguros.
    - Definición de términos y conceptos.
    - Cambios y modificaciones.
- *Contrato de adquisición de Software Vertical*
  - Tiene por objeto la adquisición de aplicaciones que, conjuntadas con el equipo físico, dan solución a las necesidades específicas de un sector o grupo determinado (Gestión integrada de Empresas Industriales, Económico-Financiero, etc...). La aplicación base objeto del contrato suele ser adaptable a las necesidades del cliente dando lugar con ello al tipo de contrato más habitual dentro de los contemplados, y cargado de las implicaciones de la llamada teoría del contrato de resultado. Clausulas específicas de este tipo de contratos
    - Todas las contempladas en el apartado de clausulas.
    - Destacar la importancia del mantenimiento futuro.
- *Contrato de Adquisición de Software Horizontal.*
  - Tiene por objeto la adquisición de aplicaciones, que sin precisar alteración alguna, conjuntadas con el equipo físico, dan solución a

necesidades de la generalidad de los usuarios (procesador de texto, hoja de cálculo, agenda, tratamiento de imágenes, etc.). Tratándose de un producto cerrado, se suele configurar como un contrato de adhesión. Algunos puntos a tener en cuenta son: la implantación, la formación de usuarios, el mantenimiento (revisión), las licencias OEM y precargadas, y que la apertura del paquete puede suponer la aceptación tácita de las condiciones contractuales. Algunas clausulas específicas son las siguientes:

- Precio.
- Mantenimiento (actualizaciones).
- Derechos sobre el software.
- Compatibilidad.
- Manual y documentación.
- Entrenamiento y formación.
- Soporte.
- Garantías.
- Transmisión de derechos.
- Propiedad.

- *Contrato de Servicios de Análisis, Diseño y Programación a Medida.*
  - Tiene por objeto la prestación de servicios de programación, propiamente dicha, de una aplicación diseñada específicamente para un cliente. Generalmente se componen de tareas de análisis, diseño y programación, pudiendo diferenciarse tres objetos distintos. Los problemas surgen sobre la titularidad, compartida o no, de los derechos de propiedad intelectual. Hay que prestar atención especial al modo de cesión de derechos y que la titularidad de los mismos esté suficientemente probada. Las cláusulas especificas de este tipo de contratos son:
    - Todas las contempladas en el apartado de clausulas.
    - En especial:
      - Derechos sobre el software.
      - Propiedad

- Cambios y modificaciones.

- *Anexos de mantenimiento*
    - Deberán figurar en Anexos al Contrato los elementos a mantener, hay que especificar si se incluye asistencia técnica, soporte a usuarios y actualizaciones. Es necesario prestar atención a la documentación que deberá acompañarse con el envío de actualizaciones, a la cláusula de revisión de precios, a las cláusulas de resolución y rescisión y a las penalizaciones por incumplimiento. Los tipos de anexos de mantenimiento pueden ser:
        - Redes y Sistemas Operativos.
        - Equipos Informáticos.
        - Software.
        - Sistemas Gestores de Base de Datos.

Aplicación Práctica

LOGIBUR contará con un departamento informático encargado de gestionar y administrar todos los sistemas informáticos que posea la empresa. No obstante, será necesaria la participación de terceras empresas para garantizar el correcto despliegue y mantenimiento de los sistemas.

La infraestructura informática que será necesaria implicará firmar uno o varios contratos de montaje y certificación de redes, contratos de adquisición de equipos informáticos, contratos de adquisición de Sistemas Operativos, contratos de adquisición de software (tanto vertical como horizontal), contratos de mantenimiento, etc…

El departamento informático será el encargado de realizar un estudio previo en el que se determinen de manera precisa las necesidades informáticas de LOGIBUR, así como de los objetivos que se pretenden cubrir. Para ello el departamento informático deberá informarse adecuadamente de los tipos de servicios que ofrecen las distintas empresas y deberá formar parte de la negociación de dichos contratos por lo que es importante recabar información acerca de las implicaciones que conlleva la firma de cada contrato.

La Administración Electrónica

La administración electrónica se refiere al uso de técnicas y medios electrónicos, informáticos y telemáticos en el desarrollo de las actividades y procedimientos que competen a la Administración. Ya en la Ley 30/1992 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común(LRJPAC) se impulsaba el empleo de estos medios, si bien la puesta en marcha de los mismos no se planteaba como una obligación para las distintas Administraciones, sino que era potestativa.

El gran salto en el desarrollo de una administración electrónica avanzada tiene su origen en la publicación de la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP). Esta Ley reconoce el *"derecho de los ciudadanos a relacionarse con las Administraciones Publicas por medios electrónicos"* y, junto a ello, establece la *"obligación de las Administraciones Públicas de rediseñar sus procedimientos y dotarse de los medios técnicos necesarios para que el ejercicio del nuevo derecho sea plenamente efectivo"*.

La LAECSP supone una transformación de las Administraciones Públicas, ya que deberán articular los mecanismos necesarios para que la iniciación, tramitación y terminación de los procedimientos pueda realizarse por medios electrónicos, con plena validez y en plenas condiciones de seguridad jurídica.

Uno de los aspectos que aparece detrás del concepto de Administración Electrónica es el cambio de los procedimientos tradicionales en papel a procedimientos electrónicos. El interesado, al interactuar con la Administración electrónicamente, percibe una mayor transparencia y control sobre el estado de tramitación de cualquier procedimiento por él iniciado. Esto hace que el servicio prestado por la Administración sea de mayor calidad.

Derechos de los ciudadanos

Los ciudadanos tienen el derecho de relacionarse con las Administraciones públicas utilizando medios electrónicos para el ejercicio de los derechos previstos en el artículo

35 de la LRJPAC. También puede utilizar dichos medios para realizar consultas y alegaciones, formular solicitudes, manifestar consentimiento, entablar pretensiones, efectuar pagos, realizar transacciones y oponerse a las resoluciones y actos administrativos.

El artículo 35 prevé los siguientes derechos:

- El derecho a conocer el estado de la tramitación de los procedimientos en los que tengan la condición de interesados, y obtener copias de documentos contenidos en ellos.
- El derecho a identificar las autoridades y al personal al servicio de las Administraciones Públicas bajo cuya responsabilidad se tramiten los procedimientos.
- El derecho a obtener una copia sellada de los documentos que presenten, así como a la devolución de los originales salvo cuando los originales deban obrar en el procedimiento.
- El derecho a utilizar la lengua oficial del territorio de la Comunidad Autónoma.
- El derecho a formular alegaciones y a aportar documentación en cualquier fase del procedimiento anterior al trámite de audiencia. Esta documentación deberá ser tomada en cuenta por el órgano competente.
- El derecho a no presentar documentos no exigidos por las normas aplicables al procedimiento de que se trate o que ya se encuentran en poder de a Administración actuante.
- El derecho a obtener información y orientación sobre los requisitos jurídicos o técnicos que las disposiciones vigentes impongan a los proyectos, actuaciones o solicitudes que se quieren realizar.
- El derecho a acceder a los registros y archivos de las Administraciones Publicas en los términos previstos en la Constitución u otras leyes.
- El derecho a ser tratado con respeto por las autoridades y funcionarios.
- El derecho a exigir responsabilidades de las Administraciones Públicas y del personal a su servicio, cuando así corresponda legalmente.
- Los derechos que reconozca la Constitución u otras leyes.

Los ciudadanos, en relación con la utilización de medios electrónicos y la Administración Pública, cuentan con los siguientes derechos previstos en la Ley:

- A elegir el canal a través del cual relacionarse por medios electrónicos con las Administraciones Públicas, siempre que se encuentren disponibles (presencial, teléfono, SMS, TDT, …).
- Derecho a no aportar los datos y documentos que obren en poder de las Administraciones Públicas. Estas deberán utilizar medios electrónicos para recabar dicha información siempre que, en el caso de daos de carácter personal, se cuente con el consentimiento de los interesados en los términos establecidos por la LOPD, o cuando una norma con rango de Ley así los determine, salvo que existan restricciones conforme a la normativa de aplicación a los datos y documentos recabados. El citado consentimiento podrá emitirse y recabarse por medios electrónicos.
- Derecho a la igualdad en el acceso electrónico a los servicios de las Administraciones Públicas. Se debe poder elegir el medio de comunicación que se desee. La utilización de medios no electrónicos no debe suponer una discriminación.
- A conocer por medios electrónicos el estado de tramitación de los procedimientos en los que sean interesados, salvo en los supuestos en que la normativa de aplicación establezca restricciones al acceso a la información sobre aquellos.
- A obtener copias electrónicas de los documentos electrónicos que formen parte de los procedimientos en los que tengan la condición de interesado.
- A la conservación por parte de las Administraciones Públicas de los documentos electrónicos que formen parte de un expediente. Los medios o soportes en que se almacenen documentos deberán contar con medidas de seguridad que permitan garantizar la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados.
- A obtener los medios de identificación electrónica necesarios, pudiendo las personas físicas utilizar los sistemas de firma electrónica del Documento

Nacional de Identidad para cualquier trámite electrónicos con cualquier Administración Pública.

- A la utilización de otros sistemas de firma electrónica admitidos en el ámbito de las Administraciones Públicas.
- A la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.
- A la garantía del principio de responsabilidad y calidad en la veracidad y autenticidad de las informaciones y servicios ofrecidos por las Administraciones Públicas a través de medios electrónicos
- A elegir las aplicaciones o sistemas para relacionarse con las Administraciones Públicas siempre y cuando utilicen estándares abiertos o aquellos que sean de uso generalizado por los ciudadanos (neutralidad tecnológica).

Régimen jurídico

El título II de la Ley de Acceso recoge la regulación del régimen jurídico de la Administración electrónica.

La sede electrónica

En el capítulo I se define la sede electrónica. La sede electrónica es la dirección electrónica cuya gestión y administración corresponde a una Administración Pública funcionando con pena responsabilidad respecto de la integridad, veracidad .y actualización de la información y los servicios a los que puede accederse a través de ella.

En la sede electrónica se podrán publicar Diarios o Boletines Oficiales con los mismos efectos que la publicación en papel

Identificación y Autentificación

En el capitulo segundo se recogen las formas de realizar la identificación y autenticación. La identificación y autenticación es doble; tanto el ciudadano como la Administración es necesario que se autentiquen como garantía y seguridad. Esta basado en la firma electrónica. La ley de Acceso promueve el uso del DNI electrónico frente otros sistemas, aunque también sean aceptados otros sistemas.

La firma electrónica incorporada en el DNIe permite la identificación y autenticación del ciudadano, así como la identificación y autenticación de sus documentos.

Los certificados electrónicos reconocidos serán admitidos por las Administraciones Públicas como validos para relacionarse con las mismas, siempre que el prestador de servicios de certificación ponga a su disposición la información precisa en condiciones tecnológicamente viables sin que suponga un coste.

Los registros, las comunicaciones y las notificaciones electrónicas

En el capítulo tercero se dice que los ciudadanos pueden elegir en todo momento la manera de comunicarse con las Administraciones Públicas (con medios electrónicos o no). Las comunicaciones electrónicas serán validadas siempre que exista constancia de la transmisión y recepción de sus fechas, del contenido íntegro de las comunicaciones y se identifique inequívocamente al remitente y al destinatario de las mismas.

Las notificaciones de las Administraciones Públicas por medios electrónicos se realizarán cuando el ciudadano haya señalado dicho medio como preferente o haya consentido su utilización.

Los documentos y los archivos electrónicos

En el capítulo cuarto vienen recogidas las condiciones de validez de los documentos y archivos electrónicos.

La Ley define el expediente electrónico como el conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contengan.

Las copias de los documentos electrónicos emitidas por el propio interesado o por las Administraciones Públicas tienen consideración de copias autenticas siempre que el documento electrónico original se encuentre en poder de la Administración y que la información de la firma electrónica y, en su caso, de sellado de tiempo, permitan comprobar la coincidencia entre documentos.

Las Administraciones Públicas pueden obtener imágenes electrónicas de documentos aportados por los ciudadanos mediante procesos de digitalización que garanticen la autenticidad, integridad y la conservación del documento imagen.

Los documentos electrónicos deben almacenarse en soportes que cuenten con medidas de seguridad que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados. Se debe asegurar la

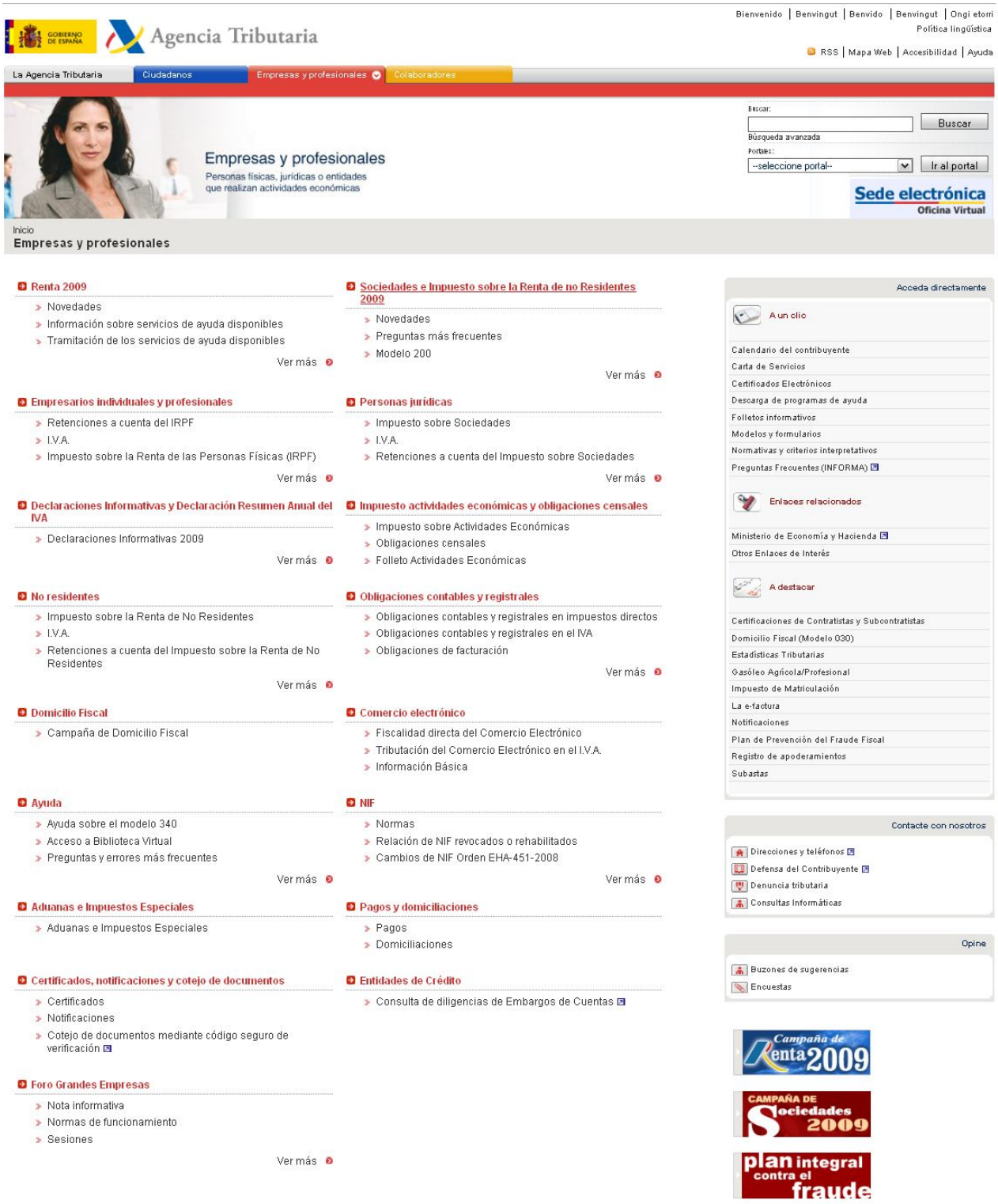
identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos.

Aplicación práctica

LOGIBUR aprovechará los beneficios que aporta la Administración Electrónica, con el uso de los servicios administrativos electrónicos que conllevaran a generar ganancias de productividad y competitividad. Estas ganancias son debidas a la reducción de los costes de los propios servicios públicos y también de los costes de transacción para la empresa (tiempo y esfuerzo).

Para poder operar con la Administración Electrónica, LOGIBUR utilizará el certificado electrónico creado con la Fabrica Nacional de Moneda y Timbre. Se deberá ingresar en la página de la Agencia Tributaria en la sección de Empresas y Profesionales.

Actualmente, la Administración Electrónica permite a las empresas llevar a cabo por Internet los trámites que se muestran en la siguiente imagen.



Agencia Tributaria

Bienvenido | Benvingut | Benvido | Benvingut | Ongi etorri
Política lingüística
RSS | Mapa Web | Accesibilidad | Ayuda

La Agencia Tributaria | Ciudadanos | Empresas y profesionales | Colaboradores

Empresas y profesionales
Personas físicas, jurídicas o entidades que realizan actividades económicas

Buscar: Buscar
Búsqueda avanzada
Portales: --seleccione portal-- Ir al portal

Sede electrónica
Oficina Virtual

Inicio
Empresas y profesionales

Renta 2009
- Novedades
- Información sobre servicios de ayuda disponibles
- Tramitación de los servicios de ayuda disponibles

Ver más

Sociedades e Impuesto sobre la Renta de no Residentes 2009
- Novedades
- Preguntas más frecuentes
- Modelo 200

Ver más

Empresarios individuales y profesionales
- Retenciones a cuenta del IRPF
- I.V.A.
- Impuesto sobre la Renta de las Personas Físicas (IRPF)

Ver más

Personas jurídicas
- Impuesto sobre Sociedades
- I.V.A.
- Retenciones a cuenta del Impuesto sobre Sociedades

Ver más

Declaraciones Informativas y Declaración Resumen Anual del IVA
- Declaraciones Informativas 2009

Ver más

Impuesto actividades económicas y obligaciones censales
- Impuesto sobre Actividades Económicas
- Obligaciones censales
- Folleto Actividades Económicas

No residentes
- Impuesto sobre la Renta de No Residentes
- I.V.A.
- Retenciones a cuenta del Impuesto sobre la Renta de No Residentes

Ver más

Obligaciones contables y registrales
- Obligaciones contables y registrales en impuestos directos
- Obligaciones contables y registrales en el IVA
- Obligaciones de facturación

Ver más

Domicilio Fiscal
- Campaña de Domicilio Fiscal

Comercio electrónico
- Fiscalidad directa del Comercio Electrónico
- Tributación del Comercio Electrónico en el I.V.A.
- Información Básica

Ayuda
- Ayuda sobre el modelo 340
- Acceso a Biblioteca Virtual
- Preguntas y errores más frecuentes

Ver más

NIF
- Normas
- Relación de NIF revocados o rehabilitados
- Cambios de NIF Orden EHA-451-2008

Ver más

Aduanas e Impuestos Especiales
- Aduanas e Impuestos Especiales

Pagos y domiciliaciones
- Pagos
- Domiciliaciones

Certificados, notificaciones y cotejo de documentos
- Certificados
- Notificaciones
- Cotejo de documentos mediante código seguro de verificación

Entidades de Crédito
- Consulta de diligencias de Embargos de Cuentas

Foro Grandes Empresas
- Nota informativa
- Normas de funcionamiento
- Sesiones

Ver más

Acceda directamente

A un clic
- Calendario del contribuyente
- Carta de Servicios
- Certificados Electrónicos
- Descarga de programas de ayuda
- Folletos informativos
- Modelos y formularios
- Normativas y criterios interpretativos
- Preguntas Frecuentes (INFORMA)

Enlaces relacionados
- Ministerio de Economía y Hacienda
- Otros Enlaces de Interés

A destacar
- Certificaciones de Contratistas y Subcontratistas
- Domicilio Fiscal (Modelo 030)
- Estadísticas Tributarias
- Gasóleo Agrícola/Profesional
- Impuesto de Matriculación
- La e-factura
- Notificaciones
- Plan de Prevención del Fraude Fiscal
- Registro de apoderamientos
- Subastas

Contacte con nosotros
- Direcciones y teléfonos
- Defensa del Contribuyente
- Denuncia tributaria
- Consultas Informáticas

Opine
- Buzones de sugerencias
- Encuestas

Campaña de Renta 2009

CAMPAÑA DE Sociedades 2009

plan integral contra el fraude

ANEXO I. Texto Informativo Tipo (Inclusión en Fichero de Empleados)

Estos datos serán incorporados al fichero automatizado de Empleados de esta Empresa, cuya finalidad es la elaboración de nóminas y seguros sociales y cualquier otra cuestión derivada de la relación entre la empresa y el trabajador. De acuerdo con la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, los derechos de acceso, rectificación y cancelación podrán ejercitarse mediante solicitud escrita acompañada de copia del DNI, dirigida al responsable del fichero de LOGIBUR, Avda. Burgos s/n 09005, Burgos, mediante correo certificado.

ANEXO II. Texto Informativo Tipo (Deber de Secreto)

El trabajador se compromete a guardar secreto sobre las informaciones confidenciales y los datos de carácter personal de los que tenga conocimiento en el ejercicio de las funciones que le sean encomendadas, de conformidad con lo establecido en el artículo 10 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, incluso tras haber finalizado su relación profesional con la Administración Pública contratante.

Igualmente, el trabajador estará obligado a atender las instrucciones relativas a la seguridad de los datos de carácter personal contenidas en las políticas de seguridad y en el documento de seguridad y difundidas, en su caso, por el responsable del fichero o el responsable de seguridad, de conformidad con lo establecido en el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13-12-1999, de protección de datos de carácter personal.

ANEXO III. Modelo de Documento de Compromiso en Cesiones de Datos.

Fichero al que afecta: [Fichero al que afecta]:

Fecha: [Fecha]

La cesionaria [Nombre del organismo público o denominación social] (en adelante la cesionaria;) de datos de carácter personal incluidos en el fichero arriba referenciado asume los siguientes compromisos en virtud del presente documento:

1. Deberá tratar los datos con la finalidad exclusiva de [introducir finalidad].

2. Ejercitado el derecho de rectificación o de cancelación de datos por parte de los interesados, revocado el consentimiento, o cuando LOGIBUR lo estime oportuno y así lo comunique a la cesionaria, ésta deberá rectificar los datos o, en su caso, cesar de inmediato en el tratamiento de los datos, que serán cancelados procediéndose al borrado de los mismos.

3. La cesionaria deberá cumplir con la normativa vigente en materia de protección de datos de carácter personal y en particular con las medidas de seguridad correspondientes a sus ficheros, así como exigir la confidencialidad de aquellos de sus empleados que traten los datos de carácter personal que se ceden.

4. No comunicará los datos a terceras personas, ni siquiera para su conservación.

5. El incumplimiento de los compromisos adoptados será responsabilidad exclusiva de la cesionaria, que responderá de los daños y perjuicios que pudieran generarse.

Recibí y conforme

Fdo: D…

Representante de la cesionaria

ANEXO IV. Documento de Comunicación o compromiso en tratamiento de datos por terceros

Se trata de una notificación que deberá remitirse a la empresa y que ésta devolverá un recibí firmado. Se enviará una sola vez pero será válida para todos los servicios que, a petición del responsable fichero, se realicen. Su utilización será frecuente en caso de que sea necesaria la contratación de un servicio de mantenimiento de ficheros informáticos.

(En supuestos en los que no exista contrato)

En relación con la prestación de servicios de [Descripción de los servicios encargados] en relación con el fichero [Nombre del fichero] que por parte de esa empresa se viene desarrollando, y para dar cumplimiento a lo previsto en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal, le comunico lo siguiente:

1º LOGIBUR facilitará a la empresa acceso al fichero mencionado, que contiene datos de carácter personal, con la finalidad exclusiva de realizar [Descripción de los servicios encargados] que en cada momento se le encarguen.

2º La empresa hará guardar a su personal la debida confidencialidad.

3º Deberá tratar el fichero únicamente con la finalidad descrita y no comunicará los datos personales a terceros (art 12.2 de la Ley 15/1999).

4º Deberá tomar las medidas de índole técnica y organizativas necesarias que eviten cualquier posible uso no legítimo de los datos personales, su revelación o alteración."

5º. El incumplimiento de los compromisos adoptados será responsabilidad exclusiva de la empresa, que responderá de los daños y perjuicios que pudieran generarse.

Recibí y conforme

Fdo: D...

Representante de la empresa

ANEXO V. Clausula a insertar en el contrato

Cláusula xx

Protección de datos personales (artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal)

1. Para la realización exclusiva de los servicios contratados, LOGIBUR facilitará a [Nombre de la Empresa], en adelante Empresa, el acceso al fichero [Nombre del fichero] con el fin de que por la citada empresa se gestione [Definición del servicio y finalidad], previas las operaciones de tratamiento de datos que sean precisas.

2. Que el fichero [Nombre del fichero] contiene datos personales de acuerdo con el concepto de tales señalado en el artículo 3 a) de la Ley Orgánica citada en el encabezamiento de este documento.

3. Que la Empresa actúa en calidad de encargado del tratamiento, en los términos previstos en el artículo 12 de la Ley Orgánica antedicha, no siendo por tanto [el acceso a datos personales por parte de la Empresa / el suministro de datos personales por parte de LOGIBUR] una cesión de datos a los efectos de la Ley.

4. La Empresa se compromete a respetar las siguientes condiciones:

4.1 El tratamiento de datos del fichero de [Nombre del fichero] de LOGIBUR por la Empresa tiene como finalidad exclusiva la [Definición de la finalidad del servicio].

4.2 La Empresa se compromete a tratar únicamente los datos conforme a las instrucciones de LOGIBUR, no aplicarlos o utilizarlos con fin distinto que el descrito y no comunicarlos, ni siquiera para su conservación, a otras personas (art. 12.2 de la Ley 15/1999).

4.3 La Empresa se compromete a 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, exigidas por el artículo 9 de la Ley 15/1999 y de manera especial por el RD 994/1999 por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, así como las que la legislación vigente imponga en cada momento.

De manera especial, la Empresa exigirá la confidencialidad expresa de aquéllos de sus empleados que tengan acceso a los datos personales.

4.4 Una vez cumplida la prestación pactada, los datos de carácter personal serán destruidos o devueltos a LOGIBUR, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento (art. 12.3 de la Ley 15/1999).

5. El incumplimiento de los compromisos adoptados será responsabilidad exclusiva de la empresa, que responderá por los daños y perjuicios que se pudieran causar.

ANEXO VI. Documento anexo al contrato en tratamiento de datos personales por terceros.

DOCUMENTO REGULADOR DEL TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL DEL FICHERO AUTOMATIZADO DE "[Nombre del fichero]"

DE LOGIBUR POR LA EMPRESA [NOMBRE DE LA EMPRESA].

Anexo al contrato firmado [Fecha de la firma]

(Artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal)

De una parte, D. Héctor Alonso García, Presidente de LOGIBUR, en nombre y representación de la misma.

De otra parte [Nombre de la Empresa] con C.I.F.: [CIF], Número de Inscripción en el Registro Mercantil: [Número de Inscripción en el Registro Mercantil] y con domicilio social en [Domicilio Social], en adelante la Empresa y en su nombre D. [Nombre del representante de la empresa] con D.N.I.: [DNI] y cargo: [Nombre del cargo desempeñado], como representante legal de la misma,

MANIFIESTAN

Primero: que LOGIBUR facilitará a la Empresa el acceso al fichero [Nombre del fichero] con el fin de que por la citada empresa se gestione [Descripción del servicio y finalidad], descrito con mayor detalle en el contrato indicado, previas las operaciones de tratamiento de datos que sean precisas.

Segundo: que dicho fichero contiene datos personales de acuerdo con el concepto de tales señalado en el artículo 3 a) de la Ley Orgánica citada en el encabezamiento de este documento.

Tercero: que la Empresa actúa en calidad de encargado del tratamiento, en los términos previstos en el artículo 12 de la Ley Orgánica antedicha, no siendo por tanto ["el acceso a datos personales por parte de la Empresa" / "el suministro de datos personales por parte de LOGIBUR"] una cesión de datos a los efectos de la Ley.

Cuarto: La Empresa se compromete a respetar las siguientes condiciones:

1º El tratamiento de datos del fichero de [Nombre del Fichero] de LOGIBUR por la Empresa tiene como finalidad exclusiva la [Finalidad del servicio].

2º La Empresa se compromete a tratar únicamente los datos conforme a las instrucciones de LOGIBUR, no aplicarlos o utilizarlos con fin distinto que el descrito y no comunicarlos, ni siquiera para su conservación, a otras personas (art. 12.2 de la Ley 15/1999).

3º La Empresa se compromete a 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, exigidas por el artículo 9 de la Ley 15/1999 y de manera especial por el RD 994/1999 por el que se aprueba el Reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, así como las que la legislación vigente imponga en cada momento.

De manera especial, la Empresa exigirá la confidencialidad expresa de aquéllos de sus empleados que tengan acceso a los datos personales.

4º Una vez cumplida la prestación pactada, los datos de carácter personal serán destruidos o devueltos a LOGIBUR, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento (art. 12.3 de la Ley 15/1999).

Quinto: el incumplimiento de los compromisos adoptados será responsabilidad exclusiva de la empresa, que responderá por los daños y perjuicios que se pudieran causar.

[Lugar de Firma del Contrato], a [Fecha de firma]

POR LOGIBUR

El Presidente,

Fdo.: [Firma]

POR <EMPRESA>

Fdo: [Firma]

D.N.I.: [DNI]

CARGO.: [Cargo]

Anexo VII. Propuesta de Índice del Documento de Seguridad.

Nota: Los artículos mencionados son del Reglamento de Medidas de Seguridad de Ficheros Automatizados con datos de carácter personal (Real Decreto 994/1999).

Nivel Bajo: Texto Negro (del artículo 5 al 14)

Nivel Medio (M): Texto Azul cursiva (de artículo 15 al 22)

Nivel Alto (A): Texto Rojo subrayado (del artículo 23 al 26)

1. Política de seguridad, ámbito de aplicación y recursos protegidos

- Política de seguridad y objeto del documento
- Ámbito de aplicación de este Documento de Seguridad (Art. 8)
- Servicio ante el cual pueden ejercerse los derechos de Acceso, Rectificación o Cancelación
- Estructura de los ficheros protegidos (Art. 8)
- Descripción de los Sistemas de Información (Art. 8)
- Locales de ubicación de los Ficheros
- Almacenes de soportes con datos
- Inventario de activos hardware, software y red de comunicaciones

2. Difusión, actualización y cambios de la normativa de seguridad (Art. 8 y 9)

- 2.1. Difusión de este Documento de Seguridad
- 2.2. Cambios en este Documento de Seguridad
- 2.3. Procedimiento de creación de nuevos ficheros, cambios de las inscripciones actuales en el RGPD y baja de las mismas

3. Nombramientos, funciones y obligaciones del personal (Art.8 y 9)

- 3.1. Obligaciones y consecuencias de incumplimiento generales
- 3.2. Estructura para la Seguridad Informática de datos personales
- 3.3. Responsable de los Ficheros
- 3.4. Gestor de Fichero
- 3.5. Usuario de Fichero
- 3.6. Junta de Seguridad
- 3.7. Responsable de Seguridad (Art. 15 y 16 nivel Medio)
- 3.8. Administradores de sistemas informáticos
- 3.9. Encargado de Almacén e Inventario de soportes
- 3.10. Encargado de Local de acceso restringido

4. Protección física y del entorno

- 4.1. El puesto de trabajo
- 4.2. Protecciones adicionales de ordenadores portátiles
- 4.3. Mantenimiento y reparaciones
- 4.4. Protección ante software malicioso
- 4.5. Controles de red
- 4.6. Locales de ubicación con Acceso Restringido (Art. 19, nivel medio)
- 4.7. Trabajo fuera de los locales de ubicación de un Fichero (Art. 6)

5. Controles de acceso a los Sistemas de Información

- 5.1. Control de acceso lógico a los Sistemas de Información, identificación y autenticación (Art. 11, 12 y 18)
- 5.2. Asignación de permisos y Lista de Usuarios Autorizados (Art. 11 y 12)
- 5.3. Normas para los códigos de usuario y contraseñas
- 5.4. Pruebas con datos reales (Art. 22, nivel Medio)
- 5.5. Registro de accesos a Ficheros (Art. 24, nivel Alto)

6. Gestión de soportes informáticos, transmisiones y copias de datos protegidos

- 6.1. Política de control de soportes
- 6.2. Identificación de soportes (Art. 13)
- 6.3. Inventario de soportes (Art. 13 Nivel Básico)
- 6.4. Almacén de soportes (Art. 13)
- 6.5 Desecho y reutilización de soportes (Art. 15 y 20, nivel medio)
- 6.6. Autorizaciones y Registro de entradas y salidas de soportes y transmisiones (Art. 13 Nivel Básico, Art. 20 nivel Medio y Art. 23 y 26, Nivel Alto)
- 6.7. Copias o Ficheros temporales con datos de carácter personal (Art. 7)

7. Copias de respaldo

- 7.1. Método de obtención de copias de respaldo (Art.14 Básico)
- 7.2. Custodia de copias de respaldo y del procedimiento (Art.13.1 Básico, Art. 25 Alto)
- 7.3. Método de Recuperación de datos (Art.14 Básico y Art. 21 nivel Medio)

8. Tratamiento de incidencias

- 8.1. Definición de incidencia (Art.8 y 10 nivel Básico)
- 8.2. Notificación de incidencias (Art.8 y 10 nivel Básico)
- 8.3. Registro de incidencias (Art.10 Básico y Art. 21 nivel Medio)

9. Normas generales de uso de Internet y del correo electrónico

- 9.1. Política de uso de Internet y del correo electrónico
- 9.2. Procedimiento de uso de Internet y del correo electrónico
- 9.3. Privacidad, seguridad de los servicios y bloqueo de contenidos
- 9.4. Cancelación de los servicios

10. Controles e informes periódicos de evaluación de la normativa de seguridad (Art.15 y 17, nivel medio)

- 10.1.- Política de evaluación
- 10.2.- Informe mensual del Responsable de Seguridad
- 10.3.- Revisiones anuales

Anexo VIII. Propuesta de Manuales y Procedimientos a redactar

Manuales

- Documento de Seguridad LOPD
- Documento de Seguridad LOPD (anexos)
- Política de Seguridad de la información
- Política de Gestión de copias de seguridad
- Política de uso de Internet
- Política de gestión de contraseñas
- Política de uso del correo electrónico
- Política de Antivirus
- Política de Conexión de Recursos a la Red de LOGIBUR
- Política de Publicación de Máquinas y Servicios en una DMZ
- Política de Seguridad para Usuarios
- Política de Validación de la Seguridad en aplicaciones
- Política de Seguridad para el uso de Ordenadores portátiles y otros dispositivos móviles

Procedimientos

- Procedimiento de copias de seguridad
- Procedimiento Alta / Baja de Usuarios en los sistemas
- Procedimiento de Gestión y Uso del Almacenamiento Corporativo
- Procedimiento de Clasificación y Manejo de la Información
- Procedimiento en caso de incumplimiento de la normativa de seguridad de la información
- Procedimiento de Cifrado de Información en Ordenadores
- Establecimiento de conexiones desde el exterior a la red de LOGIBUR
- Incorporación de Servidores en DMZ

Bibliografía

- Documentación del Magíster Asesoría y Consultoría en Tecnologías de la Información y las Comunicaciones.

  Davara & Davara Asesores jurídicos

- Análisis del Real Decreto 1720/2007, Editorial DaFema

  Miguel Ángel Davara Rodríguez

- Manual del Derecho Informático. Editorial ARANZADI

  Miguel Ángel Davara Rodríguez

- Factbook Comercio Electrónico. Editorial ARANZADI

  Miguel Ángel Davara Rodríguez

- Página web de la Agencia Española de Protección de Datos

  https://www.agpd.es

- Página web de la Organización Mundial de la Propiedad Intelectual

  http://www.wipo.int/portal/index.html.es

- Página web de Red.es

  http://www.red.es

- Pagina web de nic.es

  http://www.nic.es

- Página web de la Internet Corporation for Assigned Names and Numbers

  http://www.icann.org

- Pagina web de la Fábrica Nacional de Moneda y Timbre (FNMT).

  http://www.fnmt.es

- Pagina web del ministerio de Industria y Comercio

  http://www.mityc.es

- Página web de la Oficina Española de Patentes y Marcas

http://www.oepm.es

- Página web de la Agencia tributaria

  http://www.agenciatributaria.es