CONFEDERACIÓN DE EMPRESARIOS DE MÁLAGA

Cámara Málaga

Guía de Utilización de las Nuevas Tecnologías para la Pyme Malagueña

Guía para el empresario

ASELEX TECNOLOGÍA

Comité Permanente de Innovación del Tejido Productivo de la Provincia de Málaga

Unicaja

INDICE GENERAL

LA PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL.

LOS SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN.

6. ¿Qué deben hacer las empresas que realicen comunicaciones comerciales por vía electrónica? Información exigida; prohibiciones y derechos de los destinatarios.
7. La contratación electrónica: validez y eficacia de los contratos; prueba; intervención de terceros; obligaciones previas al inicio del procedimiento de contratación; información posterior a la celebración del contrato.
8. Protección de los consumidores.
9. Medios de pago
10. ¿Qué organismos administrativos tienen competencia e intervienen en estos procesos? Órganos de Información y Control.
11. La Seguridad del Comercio Electrónico.
12. Consejos para el empresario que tiene una página web.
13. Preguntas frecuentes.

LA FIRMA ELECTRÓNICA.

1. Elementos de seguridad y sus amenazas.
2. ¿Qué es la Firma Electrónica y cómo afecta a la empresa?
3. Reconocimiento jurídico de la Firma Electrónica.
4. ¿Por qué es útil la firma electrónica en las empresas? ¿Qué tipos de Firma Electrónica existen?
5. ¿Qué es un prestador de servicios de certificación?
6. ¿Qué es un certificado electrónico? Concepto, certificados de personas jurídicas, extinción de la vigencia de un certificado, suspensión de la vigencia de un certificado.
7. ¿Qué es un certificado electrónico reconocido? Concepto; obligaciones previas a su expedición; comprobación de la identidad; equivalencia internacional.

LA FACTURACION TELEMATICA

GLOSARIO DE TERMINOS

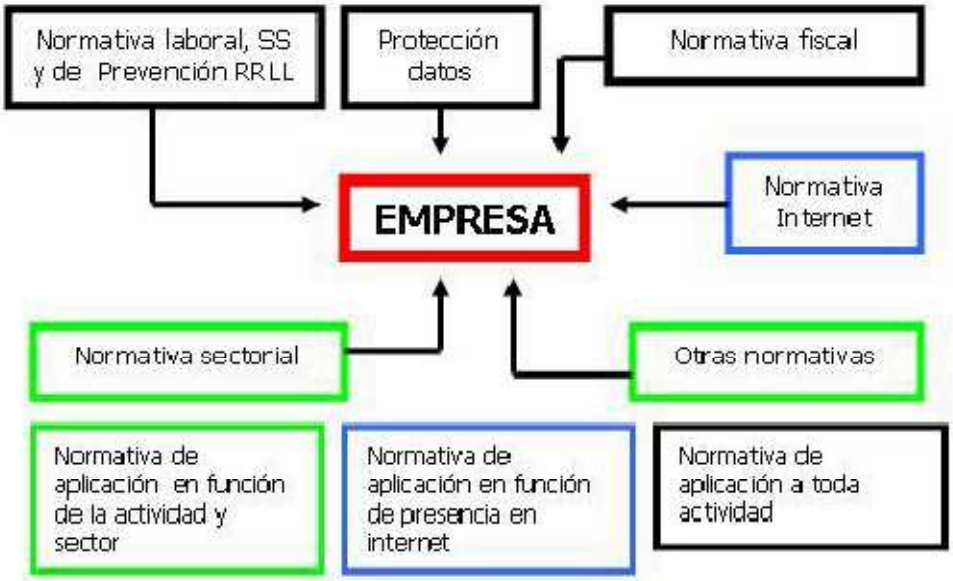
¿Qué es la Ley Orgánica de Protección de Datos y cómo afecta a la empresa?

El fundamento de este derecho de las personas lo podemos encontrar en el **artículo 18.4 de la Constitución Española**, que limita el uso de la informática para garantizar el honor, la intimidad personal y familiar de los ciudadanos, así como el legítimo ejercicio de sus derechos.

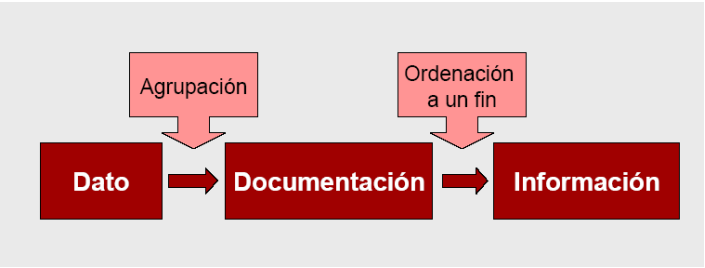
La **Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD)** adapta el régimen jurídico nacional de la protección de datos a las previsiones contenidas en la Directiva 95/46/CE, relativa a la protección de las personas físicas en lo que respecta al tratamiento de los datos personales y a la libre circulación de dichos datos. Esta Ley Orgánica establece los principios y los requerimientos mínimos necesarios e imprescindibles para realizar un tratamiento de información cuyo contenido esté formado por datos de carácter personal con independencia del sector de actividad. La LOPD se complementa y desarrolla por la normativa específica que desarrolló parte de la antigua LORTAD (la primera legislación española, ya derogada, sobre la materia), en este sentido, entre otras, por su interés y transcendencia debemos tener presente el **Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos (RLOPD)** que establece y desarrolla los requerimientos de seguridad técnicos y organizativos en función del tipo de datos que estemos tratando, tanto en papel, como de forma automatizada.

La empresa, cualesquiera que esa sea, dentro de sus peculiaridades, no se encuentra al margen de las obligaciones y derechos establecidos en la normativa de protección de datos como le ocurre respecto a la normativa laboral, de la Seguridad Social, de prevención de riesgos laborales, fiscal y demás normativa de aplicación general a toda actividad.

En este sentido, habrá que tener en cuenta la estructura y organización de cada empresa para poder determinar los ficheros existentes, sometidos a la LOPD, y las medidas que es necesario adoptar.



¿Qué datos deben ser protegidos?



La LOPD señala que **ha de protegerse toda información a través de la cual una persona física pueda ser identificada o identificable,** con independencia del soporte en donde se halle recogida y el formato en que se encuentre. En este sentido, no tendrá trascendencia si los datos se tratan en una aplicación específica, en una tabla Access o en un documento Word, en papel o en CPU, etc. Además, a todos los ficheros que contengan datos de carácter personal no se les aplicarán las mismas medidas de seguridad.

No obstante, hay que tener en cuenta los **ficheros excluidos** por la LOPD, como son los regulados en su artículo 2.2: los mantenidos por personas físicas en el ejercicio exclusivamente personal o doméstico, los ficheros relativos a materias clasificadas y los dedicados a la investigación del terrorismo y de otras formas graves de delincuencia organizada, y los ficheros regulados por sus normas específicas.

NIVELES DE SEGURIDAD	
	Básico: Todos los ficheros con datos personales.
	Medio: Infracciones advas. o penales, Hacienda Pública, servicios financieros y servicios de información solvencia patrimonial y crédito, evaluación personalidad.
	Alto: Datos especialmente protegidos y para fines policiales sin consentimiento de afectados.

¿Cómo se deben recabar los datos personales? Información y consentimiento del afectado.

El artículo 4 de la LOPD señala que sólo se podrán recoger para su tratamiento y posteriormente someterlo a dicho tratamiento, los datos de carácter personal **cuando sean adecuados, pertinentes y no excesivos** en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para los que se hayan obtenido. En base a ello, se desarrolla en el mismo artículo todo lo que se conoce como *principio de calidad de los datos*, prohibiéndose expresamente el uso de medios fraudulentos, desleales o ilícitos para recabar datos de los interesados.

La propia LOPD exige que en la recogida de datos, **los interesados deben ser previamente informados,** de modo expreso, preciso e inequívoco:

- ☑ De la existencia de un fichero, de la finalidad de la recogida y de los destinatarios de la información.
- ☑ Del carácter obligatorio o facultativo de la respuestas a las preguntas planteadas.
- ☑ De las consecuencias de la obtención de esos datos o de la negativa a facilitarlos.
- ☑ De la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición.
- ☑ De la dirección e identidad del responsable del fichero o tratamiento.

En el caso de que los datos de carácter personal no se recaben directamente del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca por el responsable del fichero, dentro de los tres meses siguientes al momento del registro de los datos de tal situación.

No se exigirá esa comunicación cuando los datos procedan de **fuentes accesibles al público** y se destinen a la actividad de publicidad o prospección comercial, siendo obligatorio

informar del origen de los datos, de la identidad del responsable del fichero y de los derechos que le asisten en cada comunicación que se dirija al interesado.

En este sentido, el art. 3 de la LOPD define fuente accesible 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 establecidos en 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 identificación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público, los Diarios y Boletines oficiales y los medios de comunicación".* (el subrayado es nuestro)

En relación al consentimiento del interesado en cuanto al tratamiento de sus datos de carácter personal, **se establece la regla general de requerir el consentimiento inequívoco salvo para los casos que la propia LOPD excepciona.**

Respecto a este consentimiento del interesado, la propia LOPD lo define en el artículo 3.h) como "*toda manifestación de voluntad, libre, inequívoca, específica e informada, mediante la que el interesado consienta el tratamiento de datos personales que le conciernen"*

¿Qué precauciones se deben tomar cuando se tratan datos personales?

- ☑ Los datos de carácter personal sólo pueden ser recogidos y tratados cuando sean **adecuados, pertinentes y no excesivos** en relación con el ámbito y finalidades determinadas, explícitas y legítimas para las que se hayan obtenido.
- ☑ Los datos de carácter personal objeto de tratamiento **no pueden usarse para finalidades incompatibles** a las que motivaron su recogida. No se considerará incompatible el tratamiento posterior de éstos para fines estadísticos, históricos o científicos.
- ☑ Los datos de carácter personal incorporados a un fichero han de **responder a la situación actual**, de manera que se recojan todas las modificaciones que hayan podido surgir en base a la necesidad de la exactitud de esos datos. De esta forma, si resultan ser inexactos o incompletos, en todo o en parte, han de ser cancelados o sustituidos de oficio por el responsable del fichero.
- ☑ Cuando se ha cumplido la finalidad para la que se recabaron los datos han de ser **cancelados o destruidos**, y en el caso de no ser posible han de ser bloqueados.
- ☑ No serán conservados en forma que permita la **identificación del interesado** por un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.
- ☑ Se prohíbe la recogida de datos por **medios fraudulentos, desleales o ilícitos.**
- ☑ Los interesados a los que se les soliciten datos personales deberán ser **previamente informados de modo expreso, preciso e inequívoco**: de la inclusión de los datos en un fichero, de su finalidad y su destinatario; de la obligatoriedad o no de dar esa información; de las consecuencias de la obtención de esos datos y de la negativa a suministrarlos; de la posibilidad de ejercer los derechos de acceso, rectificación, cancelación y oposición; de la identidad y dirección del responsable del tratamiento.
- ☑ Todas las advertencias deberán **recogerse en los cuestionarios o impresos** que se utilicen para la recogida de los datos.

  Además de estas medidas generales para todo tratamiento, deberemos tener en cuenta las medidas a adoptar en función del **nivel de seguridad** requerido para cada tratamiento. Así:

Medidas de seguridad para nivel BÁSICO	1. Documento de seguridad. 2. Régimen de funciones y obligaciones del personal. 3. Registro de incidencias. 4. Identificación y autenticación de usuarios. 5. Control de accesos. 6. Gestión de soportes. 7. Copias de respaldo y recuperación.

Medidas de seguridad para nivel MEDIO	1. Medidas de seguridad de nivel básico. 2. Responsable de seguridad. 3. Controles periódicos de verificación. 4. Auditoría bianual. 5. Medidas adicionales de identificación y autenticación. 6. Control de acceso físico. 7. Medidas adicionales de gestión de soportes. 8. Registro de incidencias. 9. Pruebas sin datos reales.

Medidas de seguridad para nivel ALTO	1. Medidas de seguridad de nivel bajo y medio. 2. Seguridad en la distribución de soportes. 3. Registro de accesos. 4. Medidas adicionales para copias de respaldo o recuperación. 5. Cifrado de la transmisión por redes de telecomunicaciones.

¿Se pueden comunicar datos personales a terceros?

Debemos tomar como premisa la **obligación de guardar secreto** establecida en la LOPD respecto al responsable del fichero y a quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal, obligación que subsiste después de finalizar sus relaciones con el titular del fichero.

La propia ley establece, como regla general, la **prohibición de ceder o comunicar datos si previamente no se ha obtenido el consentimiento informado del interesado.**

Como **excepciones** a esta regla general, la propia ley recoge entre otras las siguientes:

- ☑ Autorización expresa de una norma con rango legal.
- ☑ Datos procedentes de fuentes accesibles al público.
- ☑ Cesiones necesarias para el desarrollo de una relación jurídica que implique necesariamente la conexión de dicho tratamiento con ficheros de terceros.

¿Qué derechos tienen los titulares de los datos personales?
Acceso, cancelación, rectificación e indemnización.

Es muy importante tener siempre presente que los interesados o titulares de los datos tienen garantizado legalmente el derecho a decidir cuáles de sus datos van a ser objeto de tratamiento y si han de dejar de ser tratados.

Sin perjuicio del **derecho a indemnización** cuando el incumplimiento por parte del responsable del fichero suponga infligir un daño al interesado mediante acciones ante la jurisdicción ordinaria, los derechos que el interesado puede ejercitar frente al responsable del fichero, son:

- ☑ Derecho de acceso: El ejercicio de este derecho personalísimo permite al interesado obtener información exacta y veraz, y de manera gratuita de los datos personales sometidos a tratamiento, el origen de esos datos y las cesiones o comunicaciones que se realicen o se vayan a realizar.

  El artículo 15.1 de la LOPD reconoce el derecho del afectado a solicitar y obtener gratuitamente información de sus datos de carácter personal sometidos a tratamiento, el origen de dichos datos así como las comunicaciones realizadas o que se prevén hacer de los mismos.

  El artículo 29 del Reglamento de Desarrollo de la LOPD, (RD 1720/2007), dispone que el responsable del fichero deberá resolver en el plazo de un mes acerca de la solicitud de acceso, y dispondrá desde este momento de DIEZ DÍAS para hacer efectiva la solicitud.

  Finalmente, el artículo 27 del mismo Real Decreto señala que la información comprenderá si los datos del titular están siendo objeto de tratamiento, la finalidad del tratamiento que, en su caso, se esté realizando, así como la información disponible sobre el origen de los datos y las comunicaciones realizadas o previstas.

- ☑ Derecho de rectificación, es otro derecho personalísimo, que concede al interesado la posibilidad de exigir al responsable del fichero la rectificación de los datos personales cuyo tratamiento no se ajuste a lo establecido en la LOPD.

Todo ello en cumplimiento del principio de calidad de los datos.

El plazo para hacer efectivo este derecho es de 10 días.

☑ Derecho de cancelación, también es un derecho personalísimo fundamentado en el principio de calidad de los datos, que concede al interesado la posibilidad de exigir al responsable del fichero el borrado físico de los datos personales cuyo tratamiento no se ajuste a los establecido en la LOPD.

El artículo 4.5 de la LOPD señala que:

"Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.
No serán conservados en forma que permita la identificación del interesado durante un período superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.
Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos."

El artículo 16 de la misma ley dispone que:

1. *El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.*
2. *Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.*
3. *La 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 deberá procederse a la supresión.*

4. *Si los datos rectificados o cancelados hubieran sido comunicados previamente, el responsable del tratamiento deberá notificar la rectificación o cancelación efectuada a quien se hayan comunicado, en el caso de que se mantenga el tratamiento por este último, que deberá también proceder a la cancelación.*
5. *Los datos de carácter personal deberán ser conservados durante los plazos previstos en las disposiciones aplicables o, en su caso, en las relaciones contractuales entre la persona o entidad responsable del tratamiento y el interesado.*

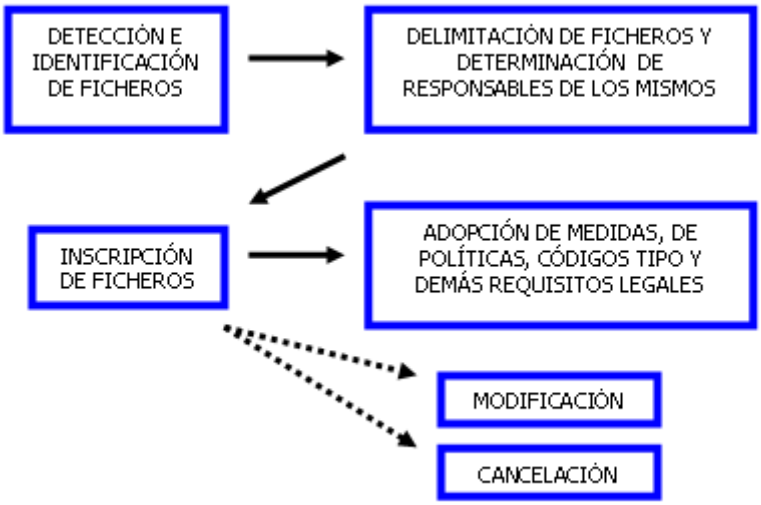
El plazo para hacer efectivo este derecho es de 10 días.

Si los datos rectificados o cancelados hubieran sido cedidos o comunicados con anterioridad al ejercicio de estos derechos, el responsable del fichero deberá notificar la rectificación o cancelación a los cesionarios.

☑ Derecho de oposición, en supuestos concretos legitima al interesado para los casos en que no sea necesario el consentimiento para el tratamiento de sus datos, a oponerse motivadamente al tratamiento de éstos.
Los titulares de los datos pueden instar la oposición al tratamiento automatizado de ese tipo de datos, de conformidad con lo revisto en el artículo 6.4 de la LOPD, que establece:

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

¿Qué debe hacer la empresa que trate datos personales?: creación, notificación e inscripción de ficheros.



Esquemáticamente,

Lo primero que tiene que hacer la empresa es la **detección e identificación de los posibles ficheros sometidos a dicha regulación** de entre la totalidad de sus ficheros y archivos, tanto en soporte informático como en soporte no informático.

Posteriormente, de entre esos posibles ficheros tendrá que **delimitar los campos y el contenido de los mismos,** sopesando sus necesidades y lo establecido por la normativa de aplicación, al tiempo que determina e identifica a los responsables de todos y cada uno de ellos.

Una vez que se conoce la existencia de los ficheros y se ha identificado a sus responsables, para el caso de que sean varios, **se inscribirán los ficheros en el Registro de la Agencia Española de Protección de Datos (RGPD)**. Registro que no podemos olvidar que sólo tiene efectos publicitarios y en ningún caso declarativos o constitutivos de legalidad y certeza de lo de allí inscrito.

Como señala la **Agencia Española de Protección de Datos (AEPD)**, están obligados a notificar la creación de ficheros para su inscripción en el RGPD, de acuerdo con lo dispuesto en la Ley Orgánica 15/99, aquellas personas físicas o jurídicas, de naturaleza pública o privada, u órgano administrativo, que procedan a la creación de ficheros que contengan datos de carácter personal.

La creación, modificación o supresión de los ficheros de las Administraciones Públicas sólo podrán hacerse por medio de ***disposición general*** publicada en el "Boletín Oficial del Estado" o diario oficial correspondiente.

Podrán crearse ficheros de titularidad privada que contengan datos de carácter personal cuando resulte necesario para el logro de la actividad u objeto legítimos de la persona, empresa o entidad titular y se respeten las garantías establecidas en la LOPD.

Toda persona o entidad que proceda a la creación de ficheros de datos de carácter personal lo notificará previamente a la Agencia Española de Protección de Datos.

Cualquier modificación posterior en el contenido de la inscripción de un fichero en el RGPD, deberá comunicarse a la Agencia Española de Protección de Datos, mediante una solicitud de modificación o de supresión de la inscripción, según corresponda. En ambos casos será necesario citar el Código de Inscripción asignado por el RGPD al fichero.

En el supuesto de ficheros y tratamientos no automatizados, creados con posterioridad a la fecha de entrada en vigor de la LOPD (14 de enero de 2000), los mismos deberán ser notificados para su inscripción en el RGPD.

La no notificación de la existencia de un fichero supondría una infracción leve o grave, tal y como señala el art. 44 de la LOPD, quedando sujeto al régimen sancionador previsto en esta Ley.

Como decimos, tal inscripción deberá estar en todo momento actualizada, por lo que en el supuesto en que se produzcan cambios en la estructura del fichero o deje de tener utilidad para la empresa habrá que notificarlo al Registro de la Agencia para que se proceda a la modificación o cancelación del mismo.

Recientemente, la AEPD ha puesto en uso el **Sistema de Notificaciones Telemáticas a la AEPD (NOTA)**, aprobado mediante Resolución de la Agencia Española de Protección de Datos de 12 de julio de 2006 (BOE núm. 181 de 31 de julio de 2006), permite a los responsables de ficheros con datos de carácter personal de titularidad pública y de titularidad privada:

- Cumplir con la obligación que la LOPD establece de notificar sus ficheros a la Agencia Española de Protección de Datos a través de una herramienta que le informa y asesora acerca de los requerimientos de la notificación.

- Presentar sus notificaciones a través de Internet con y sin firma electrónica.

- Presentar sus notificaciones en otros soportes: soporte informático o papel.

- Realizar notificaciones precumplimentadas de forma simplificada.

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

- Consultar el contenido completo de la inscripción de sus ficheros en la web de la Agencia.

Independientemente del procedimiento escogido para la solicitud de inscripción de ficheros (tradicional o telemáticamente), la empresa responsable del fichero **deberá implementar las medidas y procedimientos exigidos por la LOPD, y demás normativa de aplicación.**

¿Qué es La Agencia Española de Protección de Datos? ¿Qué funciones tiene?

La Agencia Española de Protección de Datos es un ente de derecho público, con personalidad jurídica propia y plena capacidad pública y privada, que actúa con plena independencia de las Administraciones Públicas en el ejercicio de sus funciones, entre otras:

- ☑ Velar por el cumplimiento de la legislación sobre protección de datos y controlar su aplicación.
- ☑ Dictar instrucciones para adecuar los tratamientos a los principios de la ley.
- ☑ Atender las peticiones y reclamaciones formuladas por personas afectadas por tratamientos.
- ☑ Requerir a los responsables y a los encargados de tratamiento, previa audiencia de éstos, la adopción de medidas para la adecuación de los tratamientos a la ley.
- ☑ Ejercer la potestad sancionadora.
- ☑ Velar por la publicidad de la existencia de los ficheros con datos de carácter personal.
- ☑ Iniciar, impulsar la instrucción y resolver los expedientes sancionadores referentes a los responsables de los ficheros privados.
- ☑ Instar la incoación de expedientes disciplinarios en los casos de infracciones cometidas en el ámbito del tratamiento de ficheros de titularidad pública.
- ☑ Autorizar la entrada en los locales en donde se encuentren los ficheros para llevar a cabo la acción inspectora.
- ☑ Otras funciones de gestión de la propia Agencia.

¿Qué es el Registro de Protección de Datos? ¿Qué funciones tiene?

El Registro General de Protección de Datos es el órgano de la Agencia Española de Protección de Datos al que le corresponde velar por la publicidad de la existencia de los ficheros automatizados de datos de carácter personal.

Las funciones a realizar por el Registro serán todas aquellas tendentes a facilitar a los ciudadanos el ejercicio de los derechos de información, acceso, rectificación y cancelación. Entre ellas podemos destacar:

- ☑ La inscripción de los ficheros de titularidad pública y privada.
- ☑ La inscripción de las autorizaciones de transferencia internacional de datos.
- ☑ La inscripción de los códigos tipo.
- ☑ Instruir los expedientes de inscripción de ficheros.
- ☑ Expedir certificaciones de los ficheros existentes.
- ☑ Publicar una relación anual de los ficheros notificados e inscritos.

Derecho de exclusión de las guías telefónicas.

De conformidad con el artículo 3.j de la LOPD, los datos telefónicos básicos que figuran en los repertorios telefónicos (tanto en papel como en soporte electrónico), constituyen una fuente que se considera como accesible al público, pudiéndose recabar tales datos sin el consentimiento expreso del interesado.

Concretamente, en los repertorios de abonados de servicios telefónicos, ya sean impresos en papel o disponibles por otros medios (Páginas Blancas, CD-ROM, etc.…), aparecen el nombre y apellidos así como la dirección y, salvo que se manifieste en sentido contrario exigiendo su exclusión, sus datos pueden ser consultados y utilizados por el público en general. La exclusión debe hacerse efectiva, en las guías formato papel, con la siguiente edición y, en las guías electrónicas, en el plazo de 10 días.

Frente a esta situación, y si no se quiere que los datos sean de dominio público, sería conveniente proceder a solicitar, con carácter preventivo, que se proceda gratuitamente a la exclusión total o parcial de los datos relativos a su persona que se encuentren en los repertorios telefónicos de abonados.

Derecho a no recibir publicidad no deseada.

Según dispone el artículo 30 de la LOPD, relativo a tratamientos con fines de publicidad y de prospección comercial:

1. *Quienes se dediquen a la recopilación de direcciones, reparto de documentos, publicidad, venta a distancia, prospección comercial y otras actividades análogas, utilizarán nombres y direcciones u otros datos de carácter personal cuando los mismos figuren en fuentes accesibles al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento.*
2. *Cuando los datos procedan de fuentes accesibles al público, de conformidad con lo establecido en el párrafo segundo del artículo 5.5 de esta Ley, en cada comunicación que se dirija al interesado se informará del origen de los datos y de la identidad del responsable del tratamiento, así como de los derechos que le asisten.*
3. *En el ejercicio del derecho de acceso los interesados tendrán derecho a conocer el origen de sus datos de carácter personal, así como del resto de información a que se refiere el artículo 15.*
4. *Los interesados tendrán derecho a oponerse, previa petición y sin gastos, al tratamiento de los datos que les conciernan, en cuyo caso serán dados de baja del tratamiento, cancelándose las informaciones que sobre ellos figuren en aquél, a su simple solicitud."*

Esta cuestión será tratada en la Parte II de esta Guía.

Derechos de los abonados y usuarios de servicios de telecomunicaciones.

Según dispone el art. 38.3 de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, los abonados y los usuarios a los servicios de telecomunicaciones, tienen los siguientes derechos:

- A que se hagan anónimos o se cancelen sus datos de tráfico cuando ya no sean necesarios a los efectos de la transmisión de una comunicación. Los datos de tráfico necesarios a efectos de la facturación de los abonados y los pagos de las interconexiones podrán ser tratados únicamente hasta que haya expirado el plazo para la impugnación de la factura del servicio o para que el operador pueda exigir su pago.
- A que sus datos de tráfico sean utilizados con fines comerciales o para la prestación de servicios de valor añadido únicamente cuando hubieran prestado su consentimiento informado para ello.
- A recibir facturas no desglosadas cuando así lo solicitasen (*).
- A que sólo se proceda al tratamiento de sus datos de localización distintos a los datos de tráfico cuando se hayan hecho anónimos o previo su consentimiento informado y únicamente en la medida y por el tiempo necesarios para la prestación, en su caso, de servicios de valor añadido, con conocimiento inequívoco de los datos que vayan a ser sometidos a tratamiento, la finalidad y duración del mismo y el servicio de valor añadido que vaya a ser prestado.
- A detener el desvío automático de llamadas efectuado a su terminal por parte de un tercero (*).
- A impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de su línea en las llamadas que genere.
- A impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de su línea al usuario que le realice una llamada (*).
- A impedir, mediante un procedimiento sencillo y gratuito, la presentación de la identificación de la línea de origen en las llamadas entrantes y a rechazar las llamadas entrantes en que dicha línea no aparezca identificada (*).

(*) *Estos derechos sólo están reconocidos por la LGT para los abonados a servicios de comunicaciones electrónicas.*

Derechos de los destinatarios de servicios de comunicaciones electrónicas.

Los arts. 21 y 22 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, establecen los siguientes derechos para los destinatarios de servicios de comunicaciones electrónicas:

- Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas. Éste precepto no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.

En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.

- El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente.

A tal efecto, los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado, y deberán facilitar información accesible por medios electrónicos sobre dichos procedimientos.

- Cuando los prestadores de servicios empleen dispositivos de almacenamiento y recuperación de datos en equipos terminales (*cookies*), informarán 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.

Lo anterior no impedirá el posible almacenamiento o acceso a datos con el fin de efectuar o facilitar técnicamente la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario.

Esta cuestión será tratada con profundidad en la Parte II de esta Guía.

¿Qué consecuencias tiene el incumplimiento de las normas relativas a la protección de datos? Infracciones y sanciones.

Al margen de las infracciones y sanciones recogidas en la LOPD, es muy importante tener en cuenta el coste en términos de desprestigio y pérdida de imagen frente a nuestros clientes y al resto de empresas, no sólo del sector sino de la totalidad del espectro comercial al que podamos llegar, potenciado por la deslocalización que conlleva el uso de las TIC.

No obstante, las infracciones recogidas en la LOPD son las que pasamos a enumerar.

Son infracciones leves:

a) No atender, por motivos formales, la solicitud del interesado de rectificación o cancelación de los datos personales objeto de tratamiento cuando legalmente proceda.

b) 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.

c) 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.

d) Proceder a la recogida de datos de carácter personal de los propios afectados sin proporcionarles la información que señala el artículo 5 de la presente Ley.

e) Incumplir el deber de secreto establecido en el artículo 10 de esta Ley, salvo que constituya infracción grave.

Son infracciones graves:

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

b) 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.

c) Proceder a la recogida de datos de carácter personal sin recabar el consentimiento expreso de las personas afectadas, en los casos en que éste sea exigible.

d) Tratar los datos de carácter personal o usarlos posteriormente con conculcación de los principios y garantías establecidos en la presente Ley o con incumplimiento de los preceptos de protección que impongan las disposiciones reglamentarias de desarrollo, cuando no constituya infracción muy grave.

e) El impedimento o la obstaculización del ejercicio de los derechos de acceso y oposición y la negativa a facilitar la información que sea solicitada.

f) 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 presente Ley ampara.

g) 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.

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

i) No remitir a la Agencia de Protección de Datos las notificaciones previstas en esta Ley 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.

j) La obstrucción al ejercicio de la función inspectora.

k) 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.

l) Incumplir el deber de información que se establece en los artículos 5, 28 y 29 de esta Ley, cuando los datos hayan sido recabados de persona distinta del afectado.

Son infracciones muy graves:

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

b) La comunicación o cesión de los datos de carácter personal, fuera de los casos en que estén permitidas.

c) 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 artículo 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.

d) 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.

e) 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.

f) 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.

g) 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, así como los que hayan sido recabados para fines policiales sin consentimiento de las personas afectadas.

h) No atender, u obstaculizar de forma sistemática el ejercicio de los derechos de acceso, rectificación, cancelación u oposición.

i) No atender de forma sistemática el deber legal de notificación de la inclusión de datos de carácter personal en un fichero.

Tipos de sanciones.

Las **infracciones leves** serán sancionadas con **multa de 601,01 € a 60.101,21 €**.

Las **infracciones graves** serán sancionadas con **multa de 60.101,21 € a 300.506,05 €**.

Las **infracciones muy graves** serán sancionadas con **multa de 300.506,05 € a 601.106,03 €**.

Las infracciones de las Administraciones Públicas respecto a sus ficheros tienen unas sanciones específicas y diferenciadas de las establecidas para los ficheros de titularidad privada.

Para mejor comprensión y relación de todo lo expuesto, incluimos la siguiente tabla.

RESPECTO AL DEBER DE INFORMACIÓN EN LA RECOGIDA DE DATOS: ▪ Necesidad de informar al usuario en el momento de la recogida de datos, entre otras cosas, de: ▪ El destino de los datos ▪ La finalidad ▪ Del carácter obligatorio o facultativo de las respuestas a las preguntas formuladas. ▪ De la consecuencia de la obtención de los datos o de la negativa a suministrarlos. ▪ Ante qué o quién cabe ejercer los Derechos de acceso, rectificación, cancelación y oposición. ▪ De la identidad y dirección del responsable del tratamiento.	**INFRACCIÓN LEVE** (Multa de 601,01 € a 60.101,21 €)

RESPECTO AL DEBER DE CALIDAD DE LOS DATOS: ▪ Los datos personales deberán ser adecuados, pertinentes y no excesivos en relación con la finalidad para la que se recogieron. ▪ No podrán usarse para finalidades distintas para las que se recogieron. ▪ Serán exactos y puestos al día ▪ Si resultaran inexactos, deberán ser cancelados y sustituidos de oficio ▪ Serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la que se recogieron	**INFRACCIÓN GRAVE** (multa de 60.101,21 € a 300.506,05 €)

RESPECTO AL DEBER DE CONSENTIMIENTO DEL AFECTADO PARA EL TRATAMIENTO DE SUS DATOS PERSONALES.	**INFRACCIÓN GRAVE** (Multa de 60.101,2 € a 300.506,05 €)

RESPECTO AL DEBER DE ENCARGADOS DE TRATAMIENTO La realización de tratamientos por cuenta de terceros deberá estar recogida en un contrato, con las debidas cláusulas y donde se estipulen unos determinados aspectos.	**INFRACCIÓN GRAVE** (multa de 60.101,21 € a 300.506,05 €)

RESPECTO AL DEBER DE SECRETO	**INFRACCIÓN GRAVE O MUY GRAVE ATENDIENDO A LA SENSIBILIDAD DE LOS DATOS DE QUE SE TRATEN** (Multa de 60.101,21 € a 601.106,03 €)

RESPECTO AL DEBER DE ESTABLECER PROCEDIMIENTOS QUE PERMITAN EL EJERCICIO EFECTIVO DE LOS DERECHOS DE ACCESO, RECTIFICACIÓN, OPOSICIÓN Y CANCELACIÓN POR LOS INTERESADOS.	**INFRACIÓN LEVE, GRAVE O MUY GRAVE, ATENDIENDO A LAS CIRCUNSTANCIAS DE CADA CASO** (Multa de 601,01€ a 601.106,03 €)
RESPECTO AL DEBER DE NOTIFICACIÓN E INSCRIPCIÓN DE LOS FICHEROS EN EL REGISTRO GENERAL DE LA AGENCIA DE PROTECCIÓN DE DATOS.	**INFRACCIÓN GRAVE** (Multa de 60.101,21 € a 300.506,05 €)
RESPECTO AL DEBER DE CUMPLIMIENTO DE LAS MEDIDAS DE SEGURIDAD APLICABLES A LOS NIVELES. SENSIBILIDAD DE LOS DATOS TRATADOS.	**INFRACCIÓN GRAVE** (multa de 60.101,21€ a 300.506,05 €)

Para entender el alcance del incumplimiento de la normativa relativa a la protección de datos sirva este **ejemplo**:

¿Cuál podría ser la sanción (aproximada) que la AEPD podría imponer a una PYME que no esté cumpliendo la LOPD?

Ficheros que puede tener la empresa (alrededor 25 empleados):

- nóminas.
- clientes.
- proveedores.

Los cálculos son los siguientes:

Infracciones leves (artículo 44.2):

- No solicitar la inscripción a la AEPD.
- Proceder a la recogida de datos sin proporcionar información a los afectados.

Infracciones graves (artículo 44.3)

- Tratar los datos de carácter personal con conculcación de los principios y garantías en la presente Ley…
- Mantener ficheros sin las debidas condiciones de seguridad.

Infracciones muy graves (artículo 44.4)

- No atender de forma sistemática el deber legal de notificación de ficheros.

Al contar con 3 ficheros, las infracciones leves se determinarían para los tres ficheros, al igual que el apartado de infracciones graves.

Según el artículo 45 las **sanciones** serían:

- Infracciones leves:

  Mínimo: 3(ficheros)*2 (infracciones)*601,01=3.606,06 €

  Máximo: 3(ficheros)*2(infracciones)*60.101,21 = 360.607,26 €

- Infracciones graves:

  Mínimo: [3(ficheros)*1(infracción -> 44.3.d) + 1(infracción->44.3.h)] * 60.101,21 = 240.404,84 €

  Máximo: [3(ficheros)*1(infracción -> 44.3.d) + 1(infracción->44.3.h)] * 300.506,05 = 1.202.024,2 €

- Infracciones muy graves:

  Mínimo: 1 infracción * 300.506,05 = 300.506,05 €

  Máximo: 1 infracción * 601.106,03 = 601.106,03 €

Total aproximado y sin tener en cuenta criterios de aplicabilidad del sistema sancionador:

Mínimo = 3.606,06 € + 240.404,84 € + 300.506,05 € = 544.516,95 €

Máximo = 360.607,26 € + 1.202.024,2 € + 601.106,03 € = 2.163.737,49 €

¿Es asegurable la responsabilidad empresarial en materia de protección de datos?

No puede incluirse dentro del objeto de un contrato de seguro.

¿Qué son los Códigos Tipo?

Son acuerdos sectoriales, convenios administrativos o decisiones de empresa, en los que los responsables de tratamiento o organizaciones en las que se agrupen, pueden formular establecer las condiciones de organización, el régimen de funcionamiento, los procedimientos aplicables, las normas de seguridad del entorno, programas o equipos, las obligaciones de las personas implicadas en el tratamiento y el uso de la información personal, así como las garantías, en su ámbito, para el ejercicio de los derechos de las personas con pleno respeto a lo establecido en la regulación relativa a la protección de datos.

Estos códigos tipo tendrán el carácter de **códigos deontológicos** o de **buenas prácticas profesionales** y deberán ser depositados en el Registro General de Protección de Datos.

Conclusiones y recomendaciones.

Las **conclusiones y recomendaciones** que para el empresario se resumen seguidamente:

1. Si no lo ha hecho, proceda a realizar una auditoría (interna o externa) de cumplimiento con la ley. El Apéndice I de esta Guía contiene un Auto diagnóstico muy simple que le permitirá determinar, en primera instancia, su grado de cumplimiento con la LOPD.

2. Si su empresa no está conforme a la ley proceda inmediatamente a su adecuación. Si usted no se encuentra animado o capacitado para hacerlo personalmente, contrate los servicios de algún buen equipo de profesionales (juristas y tecnólogos) con experiencia en la materia.

3. Una correcta adecuación a la LOPD le permitirá controlar, además, el flujo de información en su empresa, lo que le permitirá detectar fallos e inconsistencias que pueden estar haciéndole perder mucho dinero.

Preguntas frecuentes.

Seguidamente se plantean algunas de las preguntas más frecuentes que el empresario puede formular, incluyendo las respuestas que emanan de la doctrina de la AEPD.

¿Cómo se inscriben, modifican o suprimen los ficheros de mi empresa?

El concepto de fichero esta descrito en el artículo 3.b) de la Ley Orgánica 15/1999, de 13 de diciembre, según el cual, se define el fichero como 'todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso'.

En consecuencia, el empresario debe inscribir en el Registro General de Protección de Datos todos los ficheros que contengan datos de carácter personal (por ejemplo: fichero pacientes, fichero informes, fichero nóminas, fichero clientes, etc.), aunque contengan solamente el nombre y apellidos de la persona de contacto, el administrador o gerente de la empresa.

Dichos ficheros deben ser inscritos en el Registro General de Protección de Datos a nombre de cada uno de los responsables y conforme al formulario disponible de forma gratuita en la web de la Agencia.

Tanto para inscribir, como para suprimir o modificar la inscripción de un fichero en el Registro General de Protección de Datos, se deberá cumplimentar el modelo establecido en la Resolución de 12 de julio de 2006, de la Agencia Española de Protección de Datos, por la que se aprueban los formularios electrónicos a través de los que deberán efectuarse las solicitudes de inscripción de ficheros en el Registro General de Protección de Datos, así como los formatos y requerimientos a los que deben ajustarse las notificaciones remitidas en soporte informático o telemático.

El formulario electrónico de Notificaciones Telemáticas a la AEPD (NOTA) permite la presentación de notificaciones a través de Internet (con y sin certificado de firma electrónica reconocido), mediante soporte informático (disquete, CDROM) y en soporte papel. Dicho formulario interactivo, en formato PDF, se encuentra disponible en la página web de la Agencia (www.agpd.es).

Mediante este sistema de notificación se pueden realizar notificaciones de forma simplificada mediante notificaciones tipo precumplimentadas. Esta opción del formulario electrónico permite notificar de forma simplificada una serie de ficheros de titularidad privada relacionados con la gestión de comunidades de propietarios, clientes, libro recetario de las oficinas de farmacia, historial clínico, nóminas y recursos humanos.

Cualquier modificación posterior en el contenido de la inscripción de un fichero en el RGPD, deberá comunicarse a la Agencia Española de Protección de Datos, mediante la solicitud de modificación o de supresión de la inscripción, según corresponda.

Para modificar la inscripción de un fichero, previamente inscrito en el RGPD, deberá cumplimentar el formulario electrónico, la hoja de solicitud, el apartado de Modificación de la inscripción del fichero, indicando el código de inscripción asignado por la Agencia y señalando aquellos apartados que se modifican respecto a la notificación anterior, según las instrucciones que acompañan al modelo.

Los apartados señalados que pretendan modificar deben cumplimentarse por completo, indicando todos los datos y no sólo los modificados respecto a notificaciones previas, ya que esta notificación es sustitutiva a efectos de inscripción en el RGPD. Así mismo, únicamente se cumplimentarán los apartados que hayan sido señalados para su modificación en el apartado Modificación de la inscripción del fichero.

En el caso de que notifique la supresión de un fichero, deberá cumplimentar, del modelo de notificación, la hoja de solicitud y el apartado de Supresión, indicando el código de inscripción del fichero asignado por la Agencia. También deberá indicar el motivo de la supresión en el texto correspondiente, y el destino de la información en el siguiente campo. Si va a proceder a destruir el fichero, deberá indicar las previsiones adoptadas para ello.

La notificación de un nuevo fichero o tratamiento nunca invalida o sustituye a una inscripción previa. Si no se notifica una solicitud de supresión de la inscripción anterior se produciría un duplicado de la inscripción.

¿Debo obligatoriamente inscribir los ficheros manuales o en papel (listados, fichas, etc...)?

El soporte papel (como son los listados o las fichas) entra dentro de la definición de soportes físicos en general.

Los ficheros manuales (no automatizados), creados con posterioridad a la fecha de entrada en vigor de la LOPD (14 de enero de 2000), deberán ser notificados para su inscripción en el RGPD. Sin embargo, los ficheros manuales que ya existieran antes de la entrada en vigor de la LOPD, no será obligatoria la notificación para su inscripción hasta el 24 octubre de 2007, de conformidad con lo establecido en el último párrafo de la Disposición Adicional Primera.

¿Se aplica la LOPD a los empresarios individuales o autónomos? ¿Y a las personas jurídicas? ¿Y a los datos de personas ya fallecidas?

Con carácter general, el objeto de la Ley está regulado en los artículos 1 y 2.1 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, que expresamente establecen:

"*Artículo 1. Objeto:*
La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.
Artículo 2. Ámbito de aplicación:
La presente Ley Orgánica será de aplicación a los datos de carácter personal registrados en soporte físico que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado."

Por ello, no le es de aplicación la Ley Orgánica 15/1999:

1. A los datos de personas jurídicas.
2. A los datos de las personas fallecidas.

Por el contrario, sí le es de aplicación:

1. A los datos de los empresarios individuales - personas físicas (por ejemplo, autónomos).

2. A la grabación de datos de voz e imágenes, siempre que las mismas permitan la identificación de las personas que aparecen en dichas voces o imágenes y se hallen incorporadas a ficheros informáticos.

3. A los ficheros de empresas que tengan una relación de personas físicas de contacto, como Administradores, Gerentes, Directores Generales, Comerciales, etc.

¿Se considera dentro del ámbito de aplicación de la LOPD revelar datos de carácter personal en una página web?

De acuerdo con la definición de *tratamiento de datos* prevista en el artículo 3 c) de la LOPD, hacer referencia en una página web a una persona e identificarla por su nombre o por otros medios, como su número de teléfono o información relativa a sus condiciones de trabajo y a sus aficiones, constituye un tratamiento de datos de carácter personal, siendo necesario cumplir las previsiones establecidas en la Ley.

Lo que acaba de indicarse ha sido ratificado, en cuanto a la existencia de un tratamiento de datos de carácter personal por la Sentencia del Tribunal de Justicia de las Comunidades Europeas, de 6 de noviembre de 2003 (CASO LINDQVIST).

¿Qué países pueden considerarse con un nivel de protección equiparable a España?

Se consideran países con nivel de protección adecuado al que presta la Ley Orgánica 15/1999, los Estados Miembros de la Unión Europea, Islandia, Liechtenstein, Noruega y los Estados que la Comisión Europea ha declarado que garantizan un nivel de protección adecuado: Suiza, Argentina, Guernsey, Isla de Man, las entidades estadounidenses adheridas a los principios de «Puerto Seguro», Canadá respecto de las entidades sujetas al ámbito de aplicación de la ley canadiense de protección de datos y los datos personales incluidos en los registros de nombres de los pasajeros que se transfieren al Servicio de aduanas y protección de fronteras de los Estados Unidos de América.

¿Puede la empresa donde trabajo enviar datos de sus trabajadores a Estados Unidos?

En primer lugar indicar que cualquier empresa que pretenda realizar una transferencia internacional de datos, en este caso de sus empleados, que con anterioridad no venía realizando, deberá de cumplir, por una parte, con el derecho de información previsto en el artículo 5 de la Ley

Orgánica 15/1999, de Protección de Datos de Carácter Personal, debiendo informar de la transferencia internacional a cada una de las personas afectadas por los datos.

Por otra parte, tal y como se establece en el artículo 26 de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y en los artículos 65 a 70 del Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de Medidas de Seguridad de la LOPD, se deberá comunicar a la Agencia Española de Protección de Datos las transferencias internacionales que se vayan a realizar, dado que, con carácter general, todas las trasferencias internacionales necesitan de la autorización del Director de la Agencia, salvo que se den alguna de las excepciones previstas en el artículo 34 de la Ley Orgánica 15/1999.

Si los datos recogidos por una filial española de una multinacional alemana, cumpliéndose todos los requisitos de recogida de datos de la LOPD, se ceden a la matriz en Alemania, ¿Qué responsabilidad tiene la filial española si la matriz alemana utiliza los datos de forma fraudulenta de acuerdo a la legislación española?

En primer lugar, es necesario señalar que desde el momento en que se están recogiendo y tratando informáticamente en ficheros, cualquier tipo de datos de carácter personal por parte de empresas ubicadas en España, pertenezcan o no a multinacionales, dicho tratamiento está sometido a la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, y los ficheros de datos que se creen están sometidos al ámbito de aplicación de dicha Ley Orgánica, debiendo ser previamente comunicados al Registro General de Protección de Datos y adoptándose en ellos las medidas de seguridad correspondientes, de conformidad con lo previsto en el Reglamento de Desarrollo de la Ley Orgánica de Protección de Datos (RLOPD), aprobado mediante Real Decreto 1720/2007, de 21 de diciembre.

En segundo lugar, si dichos datos van a ser cedidos posteriormente a la central de la empresa multinacional con sede en Alemania, dicha cesión de datos deberá ser igualmente puesta en conocimiento de cada una de las personas afectadas por los datos y declarada a la Agencia Española de Protección de Datos al tratarse de una transferencia internacional en los términos previstos en los artículos 33 y 34 de la Ley Orgánica 15/1999.

Una vez realizada la transferencia internacional, de conformidad con las disposiciones anteriores, el tratamiento de datos que se realice en Alemania se regulara de conformidad con la legislación

alemana y no con la legislación española, aunque, al pertenecer ambos países a la Unión Europa, el nivel de protección será similar en base a la adaptación a la Directiva 95/46/CE del Parlamento Europeo y del Consejo de 24 de octubre de 1995, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos.

¿Qué autorizaciones y restricciones existen en la prestación de servicios mediante la sociedad de la información?

El principio que inspira esta legislación es el de **libre prestación de servicios**, es decir, no se somete a ningún tipo de autorización previa.

No obstante, este principio no alcanza a los regímenes de autorización que estén previstos en el ordenamiento y que no tengan por objeto específico y exclusivo la prestación por vía electrónica de los servicios concretos.

En todo caso, es posible que el órgano competente restrinja datos o interrumpa la prestación del servicio si atenta contra algunos de estos principios:

- ☑ La salvaguarda del orden público, la investigación penal, la seguridad pública y la defensa nacional.
- ☑ La protección de la salud pública o de las personas físicas que tengan la condición de consumidores o usuarios, incluso cuando actúen como inversores.
- ☑ El respeto a la dignidad de la persona y al principio de no discriminación por motivos de raza, sexo, religión, opinión, nacionalidad, discapacidad o cualquier otra circunstancia personal o social.
- ☑ La protección de la juventud y de la infancia.

¿Qué obligaciones tienen las empresas que prestan servicios utilizando la sociedad de la información? Registro de dominio; información; colaboración con los prestadores de servicios de intermediación; retención de datos electrónicos.

Básicamente y de forma muy esquemática podemos identificar las siguientes obligaciones:

- ☑ Informar sobre:
  - su nombre, NIF, datos de contacto, dirección de correo electrónico.
  - si están registrados su número de inscripción.
  - si la actividad está sujeta a autorización previa, sus datos.
  - Precio, impuestos y gastos de envío si los hubiere.
  - Códigos de conducta adheridos.

- ☑ Colaborar en la suspensión de los servicios ordenada por un órgano competente.

- ☑ Se respetarán los derechos a la intimidad personal y familiar, a la protección de los datos personales y a la libertad de expresión o de información.

- ☑ Retención de datos de conexión y tráfico de las comunicaciones para la localización del equipo empleado y el momento de la prestación del servicio, por el plazo legalmente establecido para ello.

¿Qué responsabilidad tienen las empresas que presten servicios en la Sociedad de la Información? Infracciones y Sanciones.

Las empresas que presten servicios a través de Internet responderán de los daños y perjuicios que causen al ejercer su actividad. Les serán aplicables las normas civiles sobre culpa contractual y extracontractual. Será el prestador de servicio a quien le corresponda demostrar que actuó con la diligencia debida.

No obstante, la propia LSSICE relaciona un paquete de infracciones y sanciones que pasamos a enumerar.

Obligación de información general Incumplimiento de la obligación de confirmar la recepción.	**LEVES** Multa de hasta 30.000 €

Obligación de información general No informar sobre los datos de inscripción en el registro que corresponda. No informar de la autorización administrativa cuando sea necesaria y del órgano competente para su supervisión. No informar de los datos correspondientes cuando se ejerza una profesión regulada. No informar del número de identificación fiscal. No informar de los códigos de conducta a los que esté adherido y la manera de consultarlos electrónicamente.	**LEVES** Multa de hasta 30.000 €

Obligación de información exigida sobre comunicaciones comerciales, ofertas promocionales y concursos	**LEVES** Multa de hasta 30.000 €
Obligación de no spam, salvo que constituya infracción grave	**LEVES** Multa de hasta 30.000 €
Obligaciones previas al inicio de la contratación De los trámites a seguir para celebrar el contrato. Si el prestador archivará el documento electrónico en que se formalice el contrato y si va a ser accesible. Medios para corregir errores en la introducción de datos. Lenguas en que podrá formalizarse el contrato.	**LEVES** Multa de hasta 30.000 €
Casos especiales de spam	**GRAVES** Multa de 30.001€ a 150.000 €
Obligación de información No dar información relativa a su nombre o denominación social; su domicilio; su dirección de correo electrónico y cualquier otro dato que permita establecer con él una relación directa y efectiva. No dar información clara y exacta sobre el precio del producto o servicio, los impuestos de aplicación y los gastos de envío.	**GRAVES** Multa de 30.001 € a 150.000 €

Obligaciones previas al inicio de la contratación No poner a disposición del destinatario del servicio las condiciones generales a que se sujete el contrato	**GRAVES** Multa de 30.001 € a 150.000 €
Obligaciones previas al inicio de la contratación Incumplimiento habitual de la obligación de confirmar la recepción.	**GRAVES** Multa de 30.001 € a 150.000 €
Resistencia, excusa o negativa a la actuación inspectora	**GRAVES** Multa de 30.001 € a 150.000 €
Incumplimiento de las órdenes dadas por un órgano administrativo respecto de restricciones a la libre prestación del servicio	**MUY GRAVE** Multa de 150.001 € a 600.000 € La reiteración en el plazo de tres años de dos o más infracciones muy graves, sancionadas con carácter firme y dependiendo de las circunstancias podrá dar lugar a la prohibición de actuación en España, durante un plazo máximo de dos años

Obligación del deber de colaboración de los prestadores de servicios de intermediación Incumplimiento de la obligación de suspender la transmisión, el alojamiento de datos, el acceso a la red y demás servicios equivalentes.	**MUY GRAVE** Multa de 150.001 € a 600.000 € La reiteración en el plazo de tres años de dos o más infracciones muy graves, sancionadas con carácter firme y dependiendo de las circunstancias podrá dar lugar a la prohibición de actuación en España, durante un plazo máximo de dos años
Obligación del deber de retener los datos de tráfico relativos a las comunicaciones electrónicas Incumplir la obligación de retener los datos de tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la sociedad de la información.	**MUY GRAVE** Multa de 150.001 € a 600.000 € La reiteración en el plazo de tres años de dos o más infracciones muy graves, sancionadas con carácter firme y dependiendo de las circunstancias podrá dar lugar a la prohibición de actuación en España, durante un plazo máximo de dos años

Obligación del deber de retener los datos de tráfico relativos a las comunicaciones electrónicas Utilizar los datos acumulados por el cumplimiento de la obligación de retener los datos relativos al tráfico para fines distintos de los que establece la ley	**MUY GRAVE** Multa de 150.001 € a 600.000 € La reiteración en el plazo de tres años de dos o más infracciones muy graves, sancionadas con carácter firme y dependiendo de las circunstancias podrá dar lugar a la prohibición de actuación en España, durante un plazo máximo de dos años

¿Qué deben hacer las empresas que realicen comunicaciones comerciales por vía electrónica? Información exigida; prohibiciones y derechos de los destinatarios.

Como punto de partida y en términos generales debemos señalar que **el *spam* está prohibido**, no obstante, y tras la modificación introducida a este respecto por la nueva ley de telecomunicaciones, podemos especificar que **si será posible enviar publicidad a través del email cuando exista una relación previa entre los sujetos y la publicidad se refiera al objeto de la relación comercial existente**.

Para los demás casos, será necesario:

- ☑ Identificación de las comunicaciones comerciales e indicación de la persona en cuyo nombre se hace. Además se deberá incluir la palabra publicidad en dichos correos electrónicos.

- ☑ Prohibición si no han sido previamente solicitadas o expresamente autorizadas por el destinatario.

- ☑ Procedimientos sencillos y gratuitos para la revocación del consentimiento.

La contratación electrónica: validez y eficacia de los contratos; prueba; intervención de terceros; obligaciones previas al inicio del procedimiento de contratación; información posterior a la celebración del contrato.

Los contratos formalizados por vía electrónica son contratos celebrados a distancia o sin que las partes –comprador y vendedor- estén presentes, que se realizan a través de equipos electrónicos de tratamiento y almacenamiento de datos.

En ningún caso se podrán celebrar a través de Internet los siguientes tipos de contratos:

- ☑ Compraventa de bienes inmuebles y creación de derechos sobre ellos.
- ☑ Actividades que exigen la intervención de tribunales, autoridades públicas, notarios o registradores.
- ☑ Contratos de crédito y caución.
- ☑ Contratos que regulan relaciones familiares y de sucesiones –herencias-.

En términos generales, **a los contratos electrónicos se les atribuye legalmente plena validez y eficacia,** otorgándoseles una equivalencia entre la "constancia por escrito" y el "soporte electrónico". Es más, se prevé su aceptación como prueba documental en juicio.

No obstante, y previo pacto, una tercera parte podrá efectuar un archivo de las declaraciones de voluntad vertidas en el procedimiento precontractual y contractual, consignando fecha y hora de dichas comunicaciones

En los contratos electrónicos, la legislación aplicable será siempre la del país en el que se encuentra el consumidor, aunque será necesario tener en cuenta los convenios internacionales firmados entre países. La jurisdicción competente –es decir, el juez al que se someterán las partes, en caso de conflicto- también será el del país de origen. Se fomentará el arbitraje como vía para resolver conflictos de forma extrajudicial. No obstante, en los casos de B2B (business to business), es decir, transacciones entre empresas, se estará a los

términos pactados por las partes y en su defecto la del lugar de establecimiento del prestador de servicios.

En relación a las **obligaciones previas a la contratación**, debemos resaltar que serán necesarias observarlas, en todo caso cuando participe un consumidor y si no es así cuando no se haya pactado otra cosa o el contrato se hay celebrado expresamente mediante intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente. Por lo tanto, en el primer supuesto será necesario observar:

- ☑ De los trámites a seguir para celebrar el contrato.
- ☑ Si el prestador archivará el documento electrónico en que se formalice el contrato y si va a ser accesible.
- ☑ Medios para corregir errores en la introducción de datos.
- ☑ Lenguas en que podrá formalizarse el contrato.

Protección de los consumidores.

Es de aplicación la normativa general sobre protección de salud pública y derechos de los consumidores; Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios.

Medios de pago

Aquellas webs en las que sea necesaria la venta de productos deberá contar con un sistema de pago apropiado y que asegure al cliente la privacidad de sus datos y sea fiable, de forma que no suponga un obstáculo para el desarrollo de la actividad comercial.

Para ello debemos tener presente todas las nuevas formas de dinero y analizar cada una para determinar la de más interés en nuestra actividad, valorando sus costes y la seguridad. En este sentido, podemos distinguir varias formas de este nuevo dinero.

El nuevo dinero

- ☑ Red interbancaria
  - Del que compra y del que vende
- ☑ Tarjetas de crédito y de débito
  - Universales: Visa, MasterCard,…
  - Club privado: Grandes almacenes.
- ☑ Dinero electrónico y pago electrónico
- ☑ Escenarios transaccionales
  - Pago anticipado / aplazado (crédito)
  - Por consumo, por acceso, …
  - Suscripciones, bonos, puntos, …

Además hay que tener en cuenta los posibles fraudes de los que se puede ser víctima, e intentar evitarlos por todos los medios que estén a nuestro alcance, estableciendo un plan de previsión para el caso de que ello ocurra.

¿Qué organismos administrativos tienen competencia e intervienen en estos procesos? Órganos de Información y Control.

El órgano competente para conocer de la aplicación de la LSSICE es la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información del Ministerio de Industria, Turismo y Comercio.

La Seguridad del Comercio Electrónico.

De cara a garantizar la seguridad del tráfico en el comercio electrónico conviene tener en cuenta cuatro cuestiones que se contemplan de forma explícita o implícita en la norma en estudio, y que versan sobre los procedimientos de identificación plena de las partes contratantes, el almacenamiento de las declaraciones de voluntad expresadas por medios telemáticos, la adscripción a códigos deontológicos o de conducta y la resolución extrajudicial de conflictos.

La plena identificación de las partes contratantes

No debemos olvidar que la contratación electrónica se realiza entre partes físicamente alejadas, razón por la cual deben proveerse de todos los medios posibles para evitar suplantaciones que serían sin duda fuente de problemas posteriores.

Para dar cumplida respuesta a esta problemática concreta es conveniente acudir a las soluciones aportadas por la **firma electrónica** que veremos más adelante en esta Guía. Nos remitimos allí.

Almacenamiento de las declaraciones de voluntad

La LSSICE contempla la existencia de los llamados **Terceros de Confianza**, entidades de naturaleza jurídica pública o privada, que pueden encargarse de almacenar las declaraciones de voluntad de las partes contratantes a fin de mantenerlas accesibles a cualquier consulta posterior, incluso cuando así pueda ser requerido por un tribunal de justicia.

Los Códigos Deontológicos o de Conducta

Como se señala en su exposición de motivos, la LSSICE promueve la elaboración de códigos de conducta sobre las materias reguladas en esta Ley, al considerar que son un instrumento de autorregulación especialmente apto para adaptar los diversos preceptos de la Ley a las características específicas de cada sector.

Procedimientos extrajudiciales de resolución de conflictos

De forma análoga, la LSSICE, por su sencillez, rapidez y comodidad para los usuarios, potencia el recurso al **arbitraje** y a los procedimientos alternativos de resolución de conflictos que puedan crearse mediante códigos de conducta, para dirimir las disputas que puedan surgir en la contratación electrónica y en el uso de los demás servicios de la sociedad de la información. Se favorece, además, el uso de medios electrónicos en la tramitación de dichos procedimientos, respetando, en su caso, las normas que, sobre la utilización de dichos medios, establezca la normativa específica sobre arbitraje.

Consejos para el empresario que tiene una página web.

Si usted, empresario, mantiene una página web accesible al público lo más probable es que su sociedad esté comprendida en el concepto que se ha denominado *Prestador de Servicios de la Sociedad de la Información* y, por tanto, esté sujeta, como hemos visto, a una serie de deberes que, caso de incumplimiento, pueden acarrearle graves disgustos, entre ellos sanciones que podrían alcanzar los 600.000 euros y el precinto de su página web.

Como nuestra intención desde esta Guía no es asustarle sino, por el contrario, ayudarle a mejorar la situación de su negocio ante el desafío de la tecnología y de su regulación jurídica, nos proponemos en las líneas que siguen proporcionarle algunos consejos básicos para que pueda seguir utilizando los recursos que le brinda Internet sin ninguna preocupación.

La LSSICE regula la prestación de servicios de la sociedad de la información, habiendo entrado en vigor, a todos los efectos, el 12 de Octubre de 2002. Esta ley considera que **servicio de la sociedad de la información** es *"todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario"*, y añade, *"El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios."*

Como la ley no referencia ninguna otra, decíamos antes, que existe un error muy extendido que consiste en pensar que con el sólo cumplimiento de la antedicha norma ya se han satisfecho todas las exigencias de orden legal para constituirse en **Prestador de Servicios de la Sociedad de la Información**. Nada más lejos de la realidad.

Aun cuando la LSSICE precisa las exigencias legales que deben necesariamente satisfacer todas aquellas entidades (personas físicas o jurídicas) que estén involucradas en las diferentes formas de prestación de tales servicios (por ejemplo, y de forma no exhaustiva: contratación de bienes o servicios por vía electrónica, organización y gestión de subastas por medios electrónicos, gestión de compras en la red por grupos de personas, envío de comunicaciones comerciales, suministro de información por vía telemática, vídeo bajo demanda, gestión de juegos de azar, etc.), no es menos cierto que **existen otras normas** que, según en qué casos, deben ser cumplidas **además** de la propia LSSICE.

Pensemos, por ejemplo, en un Prestador de Servicios de la Sociedad de la Información que decide organizar vía Internet un servicio de juegos de azar, lotería, casino, bingo, etc. Aun cuando no cabe duda de que el artículo 6 de la LSSICE señala explícitamente que *"La prestación de servicios de la sociedad de la información no estará sujeta a autorización previa."* , no obstante, es bien conocido el hecho de que existen determinadas actividades que precisan, para su adecuado desarrollo, de alguna autorización o requisito previos, como es el caso que nos ocupa de Establecimientos de Juegos de Azar, y como también es el caso de los servicios financieros (seguros, reaseguros, créditos, servicios bancarios y de inversión, etc.) Estas excepciones a libre prestación de servicios de la sociedad de la información se subliman en la propia LSSICE del siguiente modo: *"Esta norma (referida a la no sujeción a autorización previa) no afectará a los regímenes de autorización previstos en el ordenamiento jurídico que no tengan por objeto específico y exclusivo la prestación por vía electrónica de los correspondientes servicios."*

Si bien la LSSICE trae causa inmediata en la exigencia de transposición impuesta por la Directiva 2000/31/CE, de 8 de junio de 2000, del Parlamento Europeo y del Consejo, sobre Aspectos Jurídicos de los Servicios de la Sociedad de la Información, en particular el Comercio Electrónico en el mercado interior, la razón última hay que buscarla en la enorme oferta de servicios que se ofrecen a través de Internet, servicios prestados a distancia y contratados utilizando procedimientos telemáticos, y en donde se exige del legislador elevar el nivel de protección del consumidor y propiciar, por ende, la utilización masiva de las Tecnologías de la Información y la Comunicación (TICs), que actualmente disponemos..

Sin embargo, y pese a su importancia capital, todo esto no debe hacernos creer que la LSSICE es la única norma que debe tenerse en cuenta. Muy al contrario. Existen otras normas cuya observancia –si se dan las condiciones que cada una de ellas impone- es, asimismo, de obligado cumplimiento. Algunos ejemplos son: El Código Civil y el de Comercio en lo tocante a los aspectos básicos de la actividad contractual; la Ley 26/1984, de 19 de julio, para la Defensa de los Consumidores y Usuarios; la Ley 7/1998, de 13 de abril, sobre Condiciones Generales de Contratación; el Real Decreto 1906/1999, de 17 de diciembre, relativo a la Contratación Telefónica y Electrónica con Condiciones Generales; la Ley 47/2002, de reforma de la Ley 7/1996, de Ordenación del Comercio Minorista, entre otras. Todos ellos cuerpos legales muy cambiantes, en virtud de lo modificable de la materia o del campo que intentan regular. Prueba de ello lo tenemos

en la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información, que ha venido a modificar gran parte de los anteriores textos legales.

Así pues, son tres (y no sólo una) las especialidades jurídicas que el empresario ha de tener en cuenta a la hora de publicitar su página web:

- Normativa general (como las que acabamos de mencionar).
- Normativa especial del producto o servicio ofertado (caso de que le sea de aplicación) y
- Normativa especial de servicios de la sociedad de la información, singularmente nuestra vieja conocida LSSICE.

Terminamos esta sección como habíamos empezado: ¿Tiene su empresa página web? ¿Cumple **todas** las legislaciones que le son aplicables? Asegúrese de ello. Le conviene por varios motivos: facilitará el acceso y la confianza de sus clientes, se distinguirá de su competencia y, si todo está bien hecho, le evitará cuantiosas sanciones. ¿No merece la pena?

Preguntas frecuentes.

Seguidamente, mencionamos algunas cuestiones que, de forma frecuente, han sido consultadas a través de la página web (www.lssi.es) que, a tales efectos aclaratorios, tiene habilitada el Ministerio de Industria, Turismo y Comercio (www.mityc.es).

¿Quiénes están sujetos a la Ley?

Las personas que realicen actividades económicas por Internet u otros medios telemáticos (correo electrónico, televisión digital interactiva...), 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.

Mi empresa tiene una página web con información sobre su actividad, productos y servicios que vende, pero éstos no pueden contratarse a través de la página web, ¿me afectan las obligaciones para los prestadores de servicios?

Sí. La Ley se aplica a toda actividad con trascendencia económica que se realice por medios electrónicos. En este caso, la empresa sólo está obligada a facilitar, a través de su página web, los datos de información general establecidos en el artículo 10, que se refieren principalmente a denominación, domicilio y actividad, y a asegurarse de que la publicidad de otras empresas que, en su caso, figure en la página web pueda distinguirse claramente del contenido propio de la página y esté identificado el anunciante.

Si la empresa está inscrita en un Registro público en el que sea necesaria la inscripción para la adquisición de personalidad jurídica o a efectos de publicidad, deberá comunicar al mismo el nombre de dominio o dirección de Internet que utilice habitualmente para su identificación en Internet.

¿Los servicios que se prestan de forma gratuita están dentro del ámbito de aplicación de la Ley?

El criterio para determinar si un servicio o página web está incluido dentro del ámbito de aplicación de la Ley es si constituye o no una actividad económica para su prestador. Todos los servicios que se ofrecen a cambio de un precio o contraprestación están, por tanto, sujetos a la nueva Ley.

Sin embargo, el carácter gratuito de un servicio no determina por sí mismo que no esté sujeto a la Ley. Existen multitud de servicios gratuitos ofrecidos a través de Internet que representan una actividad económica para su prestador (publicidad, ingresos de patrocinadores, etc.) y, por lo tanto, estarían incluidos dentro de su ámbito de aplicación. Ejemplos de estos servicios serían los habituales buscadores, o servicios de enlaces y directorios de páginas web, así como páginas financiadas con publicidad o el envío de comunicaciones comerciales.

¿Cuándo se entiende que una página web representa una "actividad económica" para su titular?

Cuando éste percibe ingresos directos (por las actividades de comercio electrónico que lleve a cabo a través de la página, etc.) o indirectos (por publicidad, patrocinio, etc.) derivados de su página web, con independencia de que éstos permitan sufragar el coste de mantenimiento de la página, igualen esa cantidad o la superen.

Dispongo de una página web personal, pero para financiar gastos tengo alojados "banners" u otros medios de publicidad. ¿En qué me afecta la nueva Ley?

La Ley es de aplicación a las páginas web que ofrezcan mensajes publicitarios por los que el titular de la página perciba algún ingreso. Sin embargo, los únicos requisitos que establece la Ley en cuanto al contenido de las páginas de Internet consisten en incluir una información básica en la página web del prestador. Para una página web personal, la información que debe facilitarse es la siguiente:

a. Su nombre

b. Domicilio (indicando, al menos, la localidad y provincia de residencia)

c. Dirección de correo electrónico.

d. NIF

e. Cualquier dato que permita establecer una comunicación directa y efectiva, como podría ser, por ejemplo, un teléfono o un número de fax.

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

La publicidad que se muestre en la página web deberá ajustarse a lo establecido en la Ley, la cual obliga a identificar al anunciante y a presentarla de manera claramente distinguible de los contenidos no publicitarios de la página. Así mismo, deberán respetarse las restantes normas sobre publicidad, recogidas en otras leyes.

¿Es necesaria alguna autorización para prestar servicios a través de Internet?

La prestación de cualquier servicio a través de Internet u otros medios electrónicos puede realizarse libremente y no requiere ninguna autorización específica. Sin embargo, aquellas actividades o servicios que estén sujetos a autorización administrativa o a cualquier otro requisito estarán sometidos al régimen general que les sea aplicable por razón de las leyes y normas ya existentes, con independencia de que se presten a través de Internet. Por ejemplo: la autorización general de tipo C necesaria para prestar servicios de acceso a Internet seguirá siendo exigible a los proveedores de acceso a Internet y las autorizaciones precisas para la apertura de determinado tipo de establecimientos, como las farmacias, o la necesidad de colegiarse para ejercer ciertas profesiones no resultan afectadas por esta Ley.

¿Deben los prestadores de servicios de la sociedad de la información inscribirse en algún registro?

Al igual que para prestar servicios a través de Internet no se requiere ninguna clase de autorización administrativa, no existe ningún Registro en el que deban inscribirse los prestadores de servicios por el hecho de utilizar medios electrónicos para realizar su actividad.

¿De qué forma ha de mostrarse la información básica sobre el prestador de servicios señalada en el artículo 10 de la Ley?

El artículo 10 de la Ley indica que la información sobre el prestador de servicios y su actividad ha 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.

En el servidor que dirijo, se ha registrado un canal de contenido sospechoso. ¿Qué debo hacer? ¿Se me considerará responsable si la información disponible en el canal resultara ser ilícita o delictiva?

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 (o canal) puede ser constitutivo de delito, debe poner en conocimiento del Juez de Instrucción más cercano el presunto hecho delictivo, o del las Fuerzas y Cuerpos de Seguridad del Estado, si fuera necesario, 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.

¿Qué implica la presunción sobre el lugar de celebración del contrato electrónico establecida en el artículo 29 de la Ley?

La presunción establecida en el artículo 29 es simplemente una regla interpretativa para facilitar la concreción del lugar de celebración del contrato, cuando éste se formaliza por medios electrónicos. Al tratarse de una presunción, las partes pueden fijar, como lugar de celebración del contrato, un lugar distinto del señalado en la Ley.

La presunción establecida sobre el lugar de celebración del contrato no es un criterio de jurisdicción que sirva para determinar ante qué Tribunales pueden demandar las empresas a los consumidores o viceversa. Las normas para determinar la jurisdicción competente para conocer de los litigios en materia contractual están contenidas en los Tratados internacionales y en las normas de la Unión Europea sobre competencia judicial, reconocimiento y ejecución de resoluciones judiciales, en la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial y en la Ley 1/2000, de 7 de enero, de Enjuiciamiento Civil.

¿Se aplica la legislación española si un consumidor residente en España compra un producto o contrata un servicio a una tienda on-line extranjera?

La normativa española se aplicará a los contratos que los consumidores celebren con prestadores establecidos en España. El lugar de establecimiento en España de un prestador de servicios debe estar indicado en su página web y puede comprobarse mediante consulta al Registro Mercantil u otro en que el prestador esté inscrito.

También se aplicará la Ley española a las compras que efectúen a prestadores de servicios establecidos en otro Estado de la Unión Europea o del Espacio Económico Europeo (países de la Unión Europea más Noruega, Islandia y Liechtenstein), siempre que la normativa española sea más beneficiosa para el consumidor que la legislación del país en que resida el prestador de servicios.

Si la compra o la contratación del servicio se realiza a un prestador de servicios establecido en un país que no pertenezca al Espacio Económico Europeo, la legislación española sólo será aplicable si los consumidores españoles compran en tiendas virtuales que dirijan su actividad al mercado español o se hayan puesto en contacto con el consumidor a través de correo electrónico.

Si tengo algún problema con la compra realizada por Internet o correo electrónico con un prestador de otro país, ¿puedo acudir a los tribunales españoles?

Para determinar la jurisdicción competente para la resolución de conflictos en materia contractual cuando un consumidor intervenga como parte en el contrato, es preciso acudir a las normas de Derecho Internacional privado, las cuales tienen en cuenta distintos puntos de conexión para fijar la extensión de la jurisdicción de los jueces y tribunales.

Con carácter general, un consumidor residente en España que haya celebrado un contrato on-line con un prestador establecido fuera de España sólo podrá ser demandado ante los tribunales españoles y podrá, a su vez, demandar al prestador ante los tribunales españoles cuando el contrato se haya celebrado gracias a una oferta que el prestador le hubiera dirigido personalmente (correo electrónico) o que hubiera dirigido al mercado español o a varios mercados, incluido el español.

En los demás casos, si un consumidor residente en España quisiera demandar a una empresa establecida fuera de nuestro país por el incumplimiento de un contrato celebrado por vía electrónica, sería necesario alegar otras circunstancias, por ejemplo, que la obligación que da lugar a la demanda debía cumplirse en España, para fundar la competencia de los tribunales españoles.

Como se ve, en la contratación transfronteriza, no siempre puede asegurarse que los jueces y tribunales españoles sean competentes para conocer de la demanda. Por eso, la Ley potencia los mecanismos de resolución extrajudicial de conflictos, y, en especial, aquéllos que se basen en la utilización de medios electrónicos y sean reconocidos en otros Estados.

¿En qué condiciones está permitido el envío de comunicaciones comerciales por medios electrónicos?

La Ley permite la realización de comunicaciones comerciales mediante el uso de Internet u otros medios electrónicos, siempre que puedan identificarse como tales y a la persona o empresa en nombre del cual se realizan o anunciante.

Se permite el envío de mensajes publicitarios o comerciales por correo electrónico a aquellos usuarios que previamente lo hubieran autorizado o lo hubieran solicitado de forma expresa. 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 le dirija.

La Ley obliga, además, a los prestadores de servicios a habilitar procedimientos sencillos y gratuitos para que los destinatarios puedan revocar el consentimiento que hubieran prestado, así como a facilitar información accesible por vía telemática sobre dichos procedimientos.

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.

¿A qué se refiere la Ley cuando alude a medios de comunicación electrónica equivalentes al correo electrónico?

Se refiere a aquéllos 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.

¿Qué se entiende por "consentimiento o autorización expresa"?

La prestación de consentimiento expreso exige la manifestación de una voluntad libre, informada, específica e inequívoca (que no deje lugar a duda) de aceptación del envío de comunicaciones comerciales realizadas por correo electrónico u otro medio de comunicación individual equivalente. Este requisito se entendería cumplido por ejemplo, si el prestador de servicios, después de informar al usuario sobre el uso al que destinará su dirección o número de teléfono, le ofrece la oportunidad de manifestar su conformidad con el envío de comunicaciones comerciales haciendo "clic" en una casilla dispuesta al efecto.

Este requisito no se cumple cuando, sin haber autorizado de forma expresa la recepción de comunicaciones comerciales, el destinatario tolera o no se opone a su envío, cuando no responde a los mensajes por los que se solicita su consentimiento y, por supuesto, cuando se ha opuesto a su recepción.

¿De qué forma se puede recabar el "consentimiento expreso" del destinatario para la recepción de comunicaciones comerciales por correo electrónico?

El consentimiento expreso del destinatario puede recabarse, en particular, de las siguientes maneras:

• En el marco de un procedimiento de contratación o suscripción a algún servicio que tenga lugar vía web y en el que el destinatario deba facilitar su dirección de correo electrónico, incluyendo en las condiciones generales de contratación una cláusula sobre el consentimiento del destinatario a la recepción de comunicaciones comerciales y solicitando su aceptación junto con el contrato, o bien formulando una pregunta concreta al usuario sobre si acepta el envío de comunicaciones comerciales.

• Ofreciendo a los usuarios la posibilidad de facilitar su dirección de correo electrónico para recibir información sobre los productos o servicios ofrecidos por la empresa mediante un mensaje y un formulario tipo incluido en su página de Internet.

Si recibo comunicaciones comerciales no deseadas por medios electrónicos, ¿qué medidas puedo adoptar?

- Ponerse en contacto con el proveedor de acceso a Internet para conocer las medidas que estén implantando al respecto.
- Poner filtros que eviten la recepción de comunicaciones comerciales no deseadas.
- Si considera que se ha cometido una infracción contra la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, diríjase a la Agencia Española de Protección de Datos (www.agpd.es).

Elementos de seguridad y sus amenazas.

Una de las cuestiones más trascendentales para lograr la plena utilización de las redes de telecomunicaciones –y, en concreto, **Internet**- es garantizar que la comunicación a través de la red está **protegida**; esto es, que nadie distinto del emisor y del receptor pueden tener acceso a la información contenida en dicha comunicación.

Para alcanzar este objetivo la tecnología dispone de solución: se trata del cifrado o encriptación de los datos.

Un segundo elemento, quizás el de mayor importancia en las transacciones comerciales habituales, es garantizar la **identidad** de los participantes. Es crucial que el comprador sepa que el comercio al que acude –el *sitio web* que está apareciendo en la pantalla de su ordenador- *es* precisamente quien dice ser y no un impostor que pudiera estar haciéndose pasar por él. Para el comerciante, por su parte, la garantía de que el comprador es quien dice ser es también especialmente importante, sobre todo cuando la entrega del producto o servicio adquirido tiene lugar a través de la propia red (*comercio electrónico directo*).

Para alcanzar este objetivo la tecnología también dispone de solución: la **autenticación de los partícipes**.

Por otro lado, ambas partes deben tener la certeza de que los mensajes que han intercambiado han llegado al otro sin alteración alguna; eso es, que el mensaje que llega al receptor es exactamente el mismo -sin ningún tipo de adición, supresión o modificación- que el que salió del emisor. Este elemento de la seguridad, llamado **integridad**, también es alcanzable, como veremos, con determinados procedimientos tecnológicos.

No basta, sin embargo, con verificar la identidad del que se halla al otro extremo; es necesario, en muchas ocasiones, que cada una de las partes involucradas sepa fehacientemente si la otra parte es confiable, es decir: si está **autorizada** para actuar de la manera que lo está haciendo. Piénsese, por ejemplo, en el caso de la formalización de un contrato celebrado telemática o electrónicamente. Para cada parte será especialmente importante saber que la contraparte goza de la autoridad (*autoritas*) para comportarse como lo está haciendo; si tiene los poderes requeridos, si está legitimado en definitiva para obligarse.

La tecnología, una vez más, dispone de solución para alcanzar este objetivo. Se trata de los **procedimientos de confiabilidad**.

Por último, habiendo asegurado previamente la privacidad de la transmisión, la identidad y autoridad de las partes que intervienen, se hace preciso responder a la siguiente pregunta: "¿Qué hacemos si, a pesar de todo, tenemos un problema? ¿Cómo demostrar que la transacción ha tenido lugar y de qué forma?"

Nos encontramos en este caso con lo que se ha dado en llamar una cuestión de trazabilidad de la transacción. Trazar una transacción no es más que poseer una auditoría que permita conocer a un tercero –a un árbitro o a un juez, por ejemplo- que aquello ha tenido lugar de determinada forma; esto es, probar la existencia de tal transacción. Posibilitar esta opción es tanto como dotar al sistema transaccional de unas características tecnológicas de **no-repudio** donde ninguno de los partícipes podrá desdecirse de lo que ha hecho.

Así pues, se han identificado los cuatro elementos en los que podemos fundamentar lo que hemos definido como confianza y seguridad en las redes: privacidad, autenticación, autorización y auditoría. Estos cuatro elementos, lo veremos más adelante, constituyen el fundamento y el objetivo de la firma electrónica.

Todo esto es preciso porque muchas y variadas son las amenazas que se ciernen sobre una red de telecomunicaciones. Algunas de ellas son meras transposiciones de lo que ocurre en el mundo presencial pero otras, sin embargo, son exclusivas de este nuevo canal de relaciones.

Tales amenazas existen cuando aparece lo que se ha dado en llamar las vulnerabilidades de las redes de telecomunicaciones. Tres son las más evidentes:

- Su complejidad. Es sobradamente conocido el hecho de que cuantos más elementos distintos posea un sistema –de la naturaleza que sea- tanto más fácil será encontrar huecos de seguridad.

- El número de puntos de acceso. La cantidad de puntos de acceso a cualquier red multiplican geométricamente su vulnerabilidad.

- La falta de un compromiso formal con la seguridad por parte de empresas y usuarios.

Respecto de las amenazas propiamente dichas, se han descrito de dos tipos, a saber:

- Amenazas pasivas. Aquellas que atentan contra la confidencialidad de la información, sin alterarla. El caso más frecuente es la interceptación de canales de comunicación o, lo que es lo mismo, la pérdida de privacidad entre emisor y receptor; y también la recogida de información no autorizada. Tales amenazas son las de más difícil detección, constituyendo la gestión de sus riesgos una actividad de enorme importancia.

- Amenazas activas. Aquellas que sí producen alteraciones en la información o en los elementos del sistema de comunicaciones (emisor, canal o receptor), siendo las más habituales:

    - La interrupción o bloqueo de un determinado servicio electrónico.
    - La modificación fraudulenta del contenido de los mensajes.
    - La generación de mensajes falsos, por ejemplo la que tiene lugar cuando ocurre una suplantación en origen o en destino.

En los próximos apartados nos centraremos en examinar las soluciones que la tecnología ha puesto a nuestro alcance para evitar –o paliar, al menos- las amenazas enumeradas.

¿Qué es la Firma Electrónica y cómo afecta a la empresa?

La Firma Electrónica es el resultado de un procedimiento **reconocido legalmente** (en virtud de Ley 59/2003, de 19 de diciembre, de Firma Electrónica que incluimos en el Anexo IV de esta Guía) y **sustentado en equipamientos informáticos** que permite, esencialmente, dos cuestiones:

1. **Firmar documentos electrónicos** (correos electrónicos, textos, facturas, documentos, formularios, gráficos, imágenes, etc.) y remitirlos o entregarlos firmados a su(s) destinatario(s), garantizando:

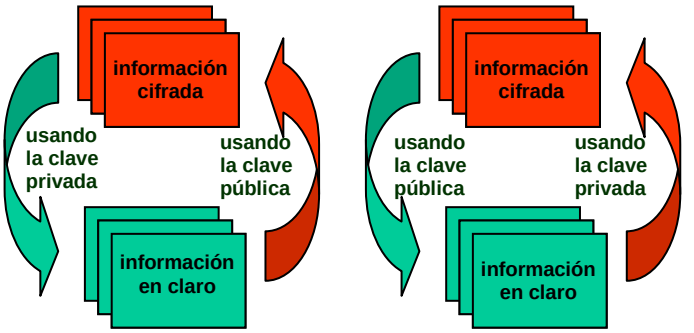
   - La **autenticación** del emisor del documento. Es decir, la completa seguridad de que quien firma tal documento electrónico es efectivamente quien dice ser.
   - La **integridad** (no alteración) del documento. Es decir, la garantía que nos permite asegurar que el documento electrónico que lee o recibe su destinatario es exactamente igual que el que fue producido o enviado por el emisor.
   - La **confidencialidad** del mismo. Es decir, que nadie ajeno al emisor del documento electrónico y a su destinatario podrá tener acceso a la información que contiene tal documento.
   - El **no-repudio** de la transacción efectuada. Es decir, que la garantía de que si emisor y receptor intercambian sus declaraciones de voluntad firmadas electrónicamente ninguno de ellos podrá desdecirse de sus actuaciones.

2. Incorporar **mecanismos de seguridad fuerte** a los sistemas de información de las empresas. Es decir, posibilitar el acceso y la identificación seguro a los ordenadores o redes de la empresa, a sus comunicaciones, a sus instalaciones, etc.

Así pues, y por las sustanciales ventajas que incorpora, la firma electrónica es una herramienta que puede (y debe) ser usada plenamente por todas las empresas, cualquiera que sea su sector.

Tradicionalmente, la seguridad en el tratamiento de la información descansa en la disciplina conocida como **criptografía** o **cifrado de datos,** técnica que estudia los principios, métodos y herramientas para ocultar el significado de un mensaje. Como técnica ancestral de ocultación de la información, veremos cómo puede contribuir decisivamente a solventar algunas de las

amenazas que hemos enumerado antes, especialmente aquellas derivadas de la pérdida de privacidad en las comunicaciones. En concreto, la firma electrónica se debe al desarrollo de la llamada **criptografía asimétrica**. Este método se fundamenta en la utilización de **una pareja de claves**, llamadas *pública* y *privada*, que poseen la siguiente peculiaridad: Un mensaje que sea cifrado con la clave pública sólo podrá ser leído con la correspondiente clave privada y viceversa.



Protegiendo la información **Firmando la información**

Reconocimiento jurídico de la Firma Electrónica.

Decimos que la Firma Electrónica es un mecanismo **reconocido legalmente** porque así lo está en gran parte de los estados de todo el mundo y, en lo que más nos concierne a nosotros, avalada por la **Directiva Europea 1999/93/CE para la firma electrónica** y, en nuestro país, por la **Ley 59/2003, de Firma Electrónica** y múltiples Órdenes Ministeriales concretando su utilización en los distintos departamentos (Economía, Hacienda, Sanidad, etc.), Comunidades Autónomas y Corporaciones Locales.

Quizás el argumento indiscutible del uso, validez y reconocimiento de la firma electrónica lo encontremos en el artículo 3.4 de la Ley de Firma Electrónica, que señala:

> *Artículo 3.4.*
> *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.*

Se consagra aquí, por consiguiente, el valor jurídico de la firma electrónica.

¿Por qué es útil la firma electrónica en las empresas? ¿Qué tipos de Firma Electrónica existen?

La Firma Electrónica es muy útil para las empresas por varios motivos:

1. Porque **agiliza y simplifica** la **gestión interna**, esto es, las relaciones de los departamentos y empleados de la empresa, y la **gestión externa**, esto es, las relaciones de la empresa con sus clientes, sus proveedores, las Administraciones Públicas y con otras organizaciones.

2. Porque garantiza la **validez y eficacia legal de los actos.**

3. Porque **ahorra costes de gestión y envío de documentación y favorece el ROI** (retorno de la inversión realizada).

4. Porque **facilita el control sobre la seguridad** de los Sistemas e Instalaciones Físicas (edificios, recintos, despachos,…) y Lógicas (Sistemas de Información, informática y comunicaciones) de la organización.

Existen varios **tipos de firma electrónica**, tal y como se recoge en al artículo 3 de la Ley 59/2003, a saber:

Firma electrónica ordinaria: Que 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.

Firma electrónica avanzada: Que 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.

Firma electrónica reconocida: Que es la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

Lo más importante de todo ello es que, como señala la ley, **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.**

¿Qué es un prestador de servicios de certificación?

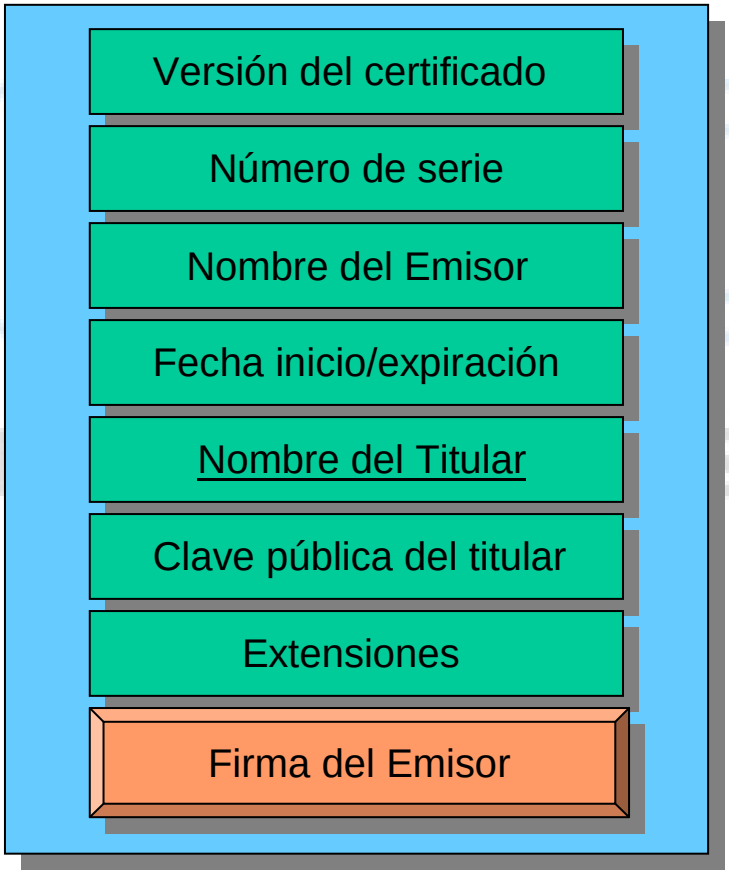
Las organizaciones que se encargan de dar fe de la autenticidad de las claves públicas se las denomina **Prestadores de Servicios de Certificación** (también llamadas *Autoridades de Certificación*) toda vez que certifican –mediante un instrumento especial que veremos más adelante llamado *certificado electrónico*- la identidad y correspondencia entre un determinado titular y su clave pública. De esta manera, cuando un tercero tiene acceso a la clave pública de una persona que le ha enviado un mensaje firmado, podrá comprobar quien está avalando tal correspondencia, tal identificación. De ahí la enorme importancia que tiene que tal Autoridad de Certificación sea capaz de generar la mayor **confianza** posible entre los usuarios.

Se muestra seguidamente una lista no exhaustiva de los Prestadores de Servicios de Certificación más significativos que operan en nuestro país.

Camerfirma
Fábrica Nacional de Moneda y Timbre
Agencia Notarial de Certificación
Agencia Catalana de Certificación
Firma Profesional
Generalitat Valenciana
Consejo General de la Abogacía
Dirección General de la Policía

¿Qué es un certificado electrónico? Concepto, certificados de personas jurídicas, extinción de la vigencia de un certificado, suspensión de la vigencia de un certificado.

Para firmar electrónicamente documentos electrónicos (y, sobre todo, para validar firmas electrónicas) es necesario disponer de un **equipo físico** (ordenador, PDA o teléfono móvil) y, esencialmente, un **certificado digital** (que no es más que un pequeño fichero que asocia una clave a su titular para propósitos de identificación) que puede estar contenido en el disco duro del ordenador, en una tarjeta inteligente, en un *tokken* de almacenamiento externo, en un pen-drive, en la memoria de una PDA, la memoria de un teléfono móvil, etc. Esto hace que sea posible firmar electrónicamente documentos sin tener que estar supeditados a un dispositivo concreto.



Cuando se utiliza una **tarjeta inteligente** puede usarse este dispositivo tanto para firmar electrónicamente documentos como para realizar **pagos electrónicos**, según el modelo de *Visa* o *Master Card*. Así, por ejemplo, la combinación de tarjetas inteligentes y dispositivos tales como las PDA's (agendas electrónicas) permitirían generar pedidos en tiempo real y ser pagados por el cliente.

En los términos de la Ley 59/2003 podemos decir que:

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.

La Ley también contempla los **certificados electrónicos de personas jurídicas**, señalando:

1. Podrán solicitar certificados electrónicos de personas jurídicas sus administradores, representantes legales y voluntarios con poder bastante a estos efectos.
Los certificados electrónicos de personas jurídicas no podrán afectar al régimen de representación orgánica o voluntaria regulado por la legislación civil o mercantil aplicable a cada persona jurídica.

2. 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.

3. Los datos de creación de firma sólo podrán ser utilizados cuando se admita en las relaciones que mantenga la persona jurídica con las Administraciones públicas o en la contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario.

Asimismo, la persona jurídica podrá imponer límites adicionales, por razón de la cuantía o de la materia, para el uso de dichos datos que, en todo caso, deberán figurar en el certificado electrónico.

Por otro lado, son causas de **extinción de la vigencia** de un certificado electrónico:

a) Expiración del período de validez que figura en el certificado.

b) Revocación formulada por el firmante, la persona física o jurídica representada por éste, un tercero autorizado o la persona física solicitante de un certificado electrónico de persona jurídica.

c) Violación o puesta en peligro del secreto de los datos de creación de firma del firmante o del prestador de servicios de certificación o utilización indebida de dichos datos por un tercero.

d) Resolución judicial o administrativa que lo ordene.

e) Fallecimiento o extinción de la personalidad jurídica del firmante; fallecimiento, o extinción de la personalidad jurídica del representado; incapacidad sobrevenida, total o parcial, del firmante o de su representado; terminación de la representación; disolución de la persona jurídica representada o alteración de las condiciones de custodia o uso de los datos de creación de firma que estén reflejadas en los certificados expedidos a una persona jurídica.

f) Cese en la actividad del prestador de servicios de certificación salvo que, previo consentimiento expreso del firmante, la gestión de los certificados electrónicos expedidos por aquél sean transferidos a otro prestador de servicios de certificación.

g) Alteración de los datos aportados para la obtención del certificado o modificación de las circunstancias verificadas para la expedición del certificado, como las relativas al cargo o a las facultades de representación, de manera que éste ya no fuera conforme a la realidad.

h) Cualquier otra causa lícita prevista en la declaración de prácticas de certificación.

¿Qué es exactamente un certificado electrónico reconocido? Concepto; obligaciones previas a su expedición; comprobación de la identidad; equivalencia internacional.

Se llaman **certificados electrónicos reconocidos** los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en la Ley 59/2003 en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.

Los certificados reconocidos incluirán, al menos, los siguientes datos:

a) La indicación de que se expiden como tales.

b) El código identificativo único del certificado.

c) La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.

d) La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.

e) 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.

f) Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.

g) El comienzo y el fin del período de validez del certificado.

h) Los límites de uso del certificado, si se establecen.

i) 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, los prestadores de los servicios de certificación comprobarán, además de los datos relativos a la constitución y personalidad jurídica, la extensión y vigencia de las facultades de representación del solicitante mediante los documentos públicos que sirvan para acreditar los extremos citados de manera fehaciente, y su inscripción en el correspondiente registro público, si es exigible, tal y como expresa el apartado 2 del artículo 13, de la citada Ley 59/2003.

Por otro lado, **antes de la expedición** de un certificado reconocido, los prestadores de servicios de certificación deberán cumplir las siguientes **obligaciones**:

a) Comprobar la identidad y circunstancias personales de los solicitantes de certificados con arreglo a lo dispuesto en el artículo siguiente.

b) Verificar que la información contenida en el certificado es exacta y que incluye toda la información prescrita para un certificado reconocido.

c) 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.

d) Garantizar la complementariedad de los datos de creación y verificación de firma, siempre que ambos sean generados por el prestador de servicios de certificación.

Además, la **identificación de la persona física** que solicite un certificado reconocido exigirá su personación ante los encargados de verificarla y se acreditará mediante el documento nacional de identidad, pasaporte u otros medios admitidos en derecho. Podrá prescindirse de la personación si su firma en la solicitud de expedición de un certificado reconocido ha sido legitimada en presencia notarial.

El régimen de personación en la solicitud de certificados que se expidan previa identificación del solicitante ante las Administraciones públicas se regirá por lo establecido en la normativa administrativa.

Respecto de la **equivalencia internacional de certificados reconocidos** hay que decir, como señala la ley, que los certificados electrónicos que los prestadores de servicios de certificación establecidos en un Estado que no sea miembro del Espacio Económico Europeo expidan al público como certificados reconocidos de acuerdo con la legislación aplicable en dicho Estado se considerarán equivalentes a los expedidos por los establecidos en España, siempre que se cumpla alguna de las siguientes condiciones:

a) Que el prestador de servicios de certificación reúna los requisitos establecidos en la normativa comunitaria sobre firma electrónica para la expedición de certificados reconocidos y haya sido certificado conforme a un sistema voluntario de certificación establecido en un Estado miembro del Espacio Económico Europeo.

b) Que el certificado esté garantizado por un prestador de servicios de certificación establecido en el Espacio Económico Europeo que cumpla los requisitos establecidos en la normativa comunitaria sobre firma electrónica para la expedición de certificados reconocidos.

c) Que el certificado o el prestador de servicios de certificación estén reconocidos en virtud de un acuerdo bilateral o multilateral entre la Comunidad Europea y terceros países u organizaciones internacionales.

La facturación telemática.

Con toda probabilidad, además del correo electrónico y la firma electrónica de documentos, una de las aplicaciones más significativas del uso de la firma electrónica en las empresas es la facturación telemática, es decir, la posibilidad de enviar (y recibir) facturas sin necesidad de acudir a la tradicional forma del envío postal.

La entrada en vigor de la ley 59/2003, de 19 de diciembre, de Firma Electrónica, ha supuesto un importante paso adelante en el camino de la utilización de las nuevas tecnologías en el ámbito empresarial con validez y eficacia jurídicas plenas. La posibilidad que abre la citada norma a la firma electrónica de documentos por parte de personas jurídicas o por parte de personas físicas, administradores de tales empresas o representantes legales o voluntarios con poder bastante, ha hecho que sea posible incorporar la firma electrónica a los esquemas de gestión empresariales en una de las áreas tradicionalmente tan costosas, rutinarias y molestas como inexcusables: la facturación.

Todo empresario sabe bien, especialmente si es él mismo quien administra o gerencia su propia empresa (pyme o micropyme), el importante coste económico que supone para la empresa la gestión tradicional de sus facturas.

Dejando a un lado por el momento otros inconvenientes que este modelo tradicional conlleva, tales como la **larga tramitación en el tiempo** (los diferentes pasos del trámite hacen que sean necesarios, al menos, uno o dos días para concluir el procedimiento), los **problemas de espacio** (la obligación legal de la conservación de las facturas puede convertirse en un grave problema de espacio físico para aquellas empresas con un alto volumen de facturas emitidas) y la **inseguridad** inherente a los canales de comunicaciones tradicionales, recientes estudios desarrollados por Confederaciones de Empresarios han estimado la suma de los antedichos **costes** en un rango que oscila **entre los 3 y los 5 euros por factura emitida y recibida.** He aquí el problema que podemos resolver con el adecuado uso de la legal y reconocida firma electrónica.

En efecto, el 29 de noviembre de 2003 se publicaba en el B.O.E. el Real Decreto 1496/2003, de 28 de noviembre, por el que se aprueba el *Reglamento por el que se regulan las obligaciones de facturación, y se modifica el Reglamento del Impuesto sobre el Valor Añadido.* Los artículos 17, 18, 20 y 21 de esta norma concretan la posibilidad de la facturación telemática, contemplando, en

esencia, dos exigencias: el consentimiento expreso por parte del receptor del medio electrónico usado y la utilización de un procedimiento tecnológico que asegure la *calidad* de la factura emitida y su conservación. En concreto, el artículo 17 de esta norma, allí donde habla de las *Formas de remisión de las facturas*, señala textualmente: *"La obligación de remisión de facturas o documentos sustitutivos podrá ser cumplida por cualquier medio y, en particular, por medios electrónicos, siempre que en este caso el destinatario haya dado su consentimiento de forma expresa y los medios electrónicos utilizados en la transmisión garanticen la autenticidad del origen y la integridad de su contenido."*

Por otro lado, el artículo 18, versando sobre la *Remisión electrónica de las facturas*, señala: *"1. A efectos de lo dispuesto en el artículo 17, la garantía de la autenticidad del origen y de la integridad del contenido de las facturas o documentos sustitutivos que se hayan remitido por medios electrónicos se acreditará por alguna de las siguientes formas: a) Mediante una* ***firma electrónica avanzada****…"*

Finalmente, en los artículos 20 y 21, en lo referente a la obligatoria *Conservación de las facturas* y en las *Formas de conservación de las facturas*, se posibilita que tal obligación sea tenida como cumplida si la referida conservación se realizara en soporte electrónico, siempre que sea posible asegurar su legibilidad en un momento dado.

Este Reglamento ha sido desarrollado recientemente con la publicación de la ORDEN EHA/962/2007, de 10 de abril, por la que se desarrollan determinadas disposiciones sobre facturación telemática y conservación electrónica de facturas.

La Cámara de Comercio de Madrid (White Paper, AC-Camerfirma) ya ha expresado con precisión las peculiaridades e inconvenientes de la facturación tradicional frente a la facturación telemática. Así tenemos que la operativa de emisión de facturas por el método tradicional de emisión en soporte papel se resume en cuatro pasos fundamentales:

1. Creación de la factura e impresión (o trascripción manuscrita) en soporte papel.

2. Envío de la factura por medio de correo ordinario u otros medios de mensajería tradicionales.

3. Recepción y archivado físico de las facturas.

4. Entrega personal de las copias ante el órgano tributario, cuando es requerida.

Los inconvenientes que puede ocasionar este sistema a la empresa son muy variados, pero destacamos los siguientes:

1. **Excesivos gastos para la empresa**: dentro de éstos debemos incluir entre otros los de papel, tinta, gastos de almacenaje, personal y envíos.

2. **Tramitación larga en el tiempo**: los diferentes pasos de la tramitación hacen que sean necesarios al menos uno o dos días para concluir el procedimiento.

3. **Problemas de espacio**: fundamentalmente en empresas grandes con un alto volumen de facturación la obligación de conservación de las facturas puede convertirse en un grave problema de espacio físico.

4. **Falta de seguridad**: este sistema de facturación carece de cualquier medida de seguridad que garantice la autenticación del emisor y la integridad de la factura. Además las facturas son intercambiadas por medios no seguros.

Con la entrada en funcionamiento de los nuevos medios telemáticos y electrónicos de facturación, surgen nuevos esquemas y se simplifican los trámites. Básicamente se sigue el mismo patrón de generación, envío-recepción, almacén y presentación, pero esta vez, emisor y receptor podrán realizar toda la tramitación de forma cómoda, inmediata, segura y con bajo coste.

La operativa telemática se sustenta en la creación de una aplicación informática capaz de generar y autenticar las facturas electrónicas, posibilitando a su vez a la otra parte a su visualización y ratificación de la autenticidad e integridad factura recibida. En puridad, la generación de la factura por medios electrónicos no supone una novedad, ya que en la actualidad prácticamente todas las empresas emplean ordenadores para realizar estos procesos, sin embargo, llama la atención que una vez realizados tengan que ser pasados de soporte digital a papel.

Los pasos a seguir son los siguientes:

1. Creación y firma digital de la factura.
2. Envío y recepción telemática del documento autenticado.
3. Conservación en soporte digital.
4. Envío telemático a la Administración cuando sea requerido.

Los beneficios del empleo de este sistema surgen como contrapartida lógica a los inconvenientes de la operativa tradicional:

1. **Recorte de gastos** para la empresa: con el ahorro de papel, gastos de envío y gastos de almacenamiento se reducen drásticamente los gastos de la empresa

2. **Agilidad en la tramitación**: los diferentes pasos de la tramitación se pueden realizar en pocos minutos y cómodamente, sin necesidad de desplazamiento alguno.

3. **Ahorro de espacio**: los documentos generados pueden ser almacenados fácilmente en medios de almacenamientos magnéticos u ópticos. Se suprimen las pilas y archivadores de papel.

4. **Procedimiento seguro**: mediante el empleo de certificados y firmas digitales se garantiza en todo momento la autenticidad, la integridad y el no repudio de los documentos. Además el envío de documentos mediante canales seguros basados en el protocolo SSL aseguran la confidencialidad de todo el proceso.

Normativa habilitante

Podemos encontrar la normativa legal que posibilita el uso de la firma electrónica en la remisión y recepción de facturas electrónicas en el Real Decreto 1496/2003, de 28 de noviembre, por el que se aprueba el *Reglamento por el que se regulan las obligaciones de facturación, y se modifica el Reglamento del Impuesto sobre el Valor Añadido.*

Su utilización impone una serie de exigencias*:*

- Consentimiento expreso por parte del receptor, del medio electrónico usado.
- Procedimiento de emisión que garantice la autenticidad del emisor y la integridad del documento, es decir, la firma electrónica.
- Conservación fidedigna en soporte electrónico.

Es nuestro deber señalar, por último y a modo de conclusión, que el uso de la firma electrónica en las empresas es ya una realidad imparable. Su **facilidad de uso**, el **pleno reconocimiento jurídico** que posee y –quizás lo definitivo- el **importante ahorro de costes** que comporta, hacen que sean más cada día las empresas e instituciones de todo tipo que están incorporando la firma electrónica a sus procesos de negocio y a sus relaciones internas y externas. Desde esta guía animamos a los empresarios, si todavía no lo están haciendo, a tomar muy en consideración su utilización inmediata.

Protección de Datos:

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

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

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

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.

Afectado o interesado: persona física titular de los datos que sean objeto del tratamiento a que se refiere el apartado c) del presente artículo.

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

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

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

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

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

Sistema de información**:** Conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.

Usuario: Sujeto o proceso autorizado para acceder a datos o recursos.

Recurso: Cualquier parte componente de un sistema de información.

Accesos autorizados: Autorizaciones concedidas a un usuario para la utilización de los diversos recursos.

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

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

Control del acceso: Mecanismo que en función a la identificación ya autenticada permite acceder a datos o recursos.

Contraseña: Información confidencial, frecuentemente constituida por una cadena de caracteres, que puede ser usada en la autenticación de un usuario.

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

Soporte: Objeto físico susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar o recuperar datos.

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.

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

Servicios de la Sociedad de la Información:

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.

El concepto de servicio de la sociedad de la información comprende también los servicios no remunerados por sus destinatarios, en la medida en que constituyan una actividad económica para el prestador de servicios.

Son servicios de la sociedad de la información, entre otros y siempre que representen una actividad económica, los siguientes:

1.° La contratación de bienes o servicios por vía electrónica.

2.° La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.

3.° La gestión de compras en la red por grupos de personas.

4.° El envío de comunicaciones comerciales.

5.° El suministro de información por vía telemática.

6.° El vídeo bajo demanda, como servicio en que el usuario puede seleccionar a través de la red, tanto el programa deseado como el momento de su suministro y recepción, y, en general, la distribución de contenidos previa petición individual.

No tendrán la consideración de servicios de la sociedad de la información los que no reúnan las características señaladas en el primer párrafo de este apartado y, en particular, los siguientes:

1.° Los servicios prestados por medio de telefonía vocal, fax o télex.

2.° El intercambio de información por medio de correo electrónico u otro medio de comunicación electrónica equivalente para fines ajenos a la actividad económica de quienes lo utilizan.

3.° Los servicios de radiodifusión televisiva (incluidos los servicios de cuasivídeo a la carta), contemplados en el artículo 3.a) de la Ley 25/1994, de 12 de julio, por la que se incorpora al ordenamiento jurídico español la Directiva 89/552/CEE, del Consejo, de 3 de octubre, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva, o cualquier otra que la sustituya.

4.° Los servicios de radiodifusión sonora.

5.° El teletexto televisivo y otros servicios equivalentes como las guías electrónicas de programas ofrecidas a través de las plataformas televisivas.

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

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

Prestador de servicios: persona física o jurídica que proporciona un servicio de la sociedad de la información.

Destinatario del servicio: persona física o jurídica que utiliza, sea o no por motivos profesionales, un servicio de la sociedad de la información.

Consumidor: persona física o jurídica en los términos establecidos en el artículo 1 de la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios.

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

A efectos de esta Ley, no tendrán la consideración de comunicación comercial los datos que permitan acceder directamente a la actividad de una persona, empresa u organización, tales como el nombre de dominio o la dirección de correo electrónico, ni las comunicaciones relativas a los bienes, los servicios o la imagen que se ofrezca cuando sean elaboradas por un tercero y sin contraprestación económica.

Profesión regulada: toda actividad profesional que requiera para su ejercicio la obtención de un título, en virtud de disposiciones legales o reglamentarias.

Contrato celebrado por vía electrónica o contrato electrónico: todo contrato en el que la oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones.

Ámbito normativo coordinado: todos los requisitos aplicables a los prestadores de servicios de la sociedad de la información, ya vengan exigidos por la presente Ley u otras normas que regulen el ejercicio de actividades económicas por vía electrónica, o por las leyes generales que les sean de aplicación, y que se refieran a los siguientes aspectos:

1.° Comienzo de la actividad, como las titulaciones profesionales o cualificaciones requeridas, la publicidad registral, las autorizaciones administrativas o colegiales precisas, los regímenes de notificación a cualquier órgano u organismo público o privado.

2.° Posterior ejercicio de dicha actividad, como los requisitos referentes a la actuación del prestador de servicios, a la calidad, seguridad y contenido del servicio, o los que afectan a la publicidad y a la contratación por vía electrónica y a la responsabilidad del prestador de servicios.

No quedan incluidas en este ámbito las condiciones relativas a las mercancías y bienes tangibles, a su entrega ni a los servicios no prestados por medios electrónicos.

Órgano competente: 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.

Firma electrónica:

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.

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.

Firma electrónica reconocida: es la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

Documento electrónico: se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según el formato determinado y susceptible de identificación y tratamiento diferenciado.

Los documentos electrónicos podrán ser soporte de:

a) Documentos públicos, por estar firmados electrónicamente por funcionarios que tengan legalmente atribuida la facultad de dar fe pública, judicial, notarial o administrativa, siempre que actúen en el ámbito de sus competencias con los requisitos exigidos por la ley en cada caso.

b) Documentos expedidos y firmados electrónicamente por funcionarios o empleados públicos en el ejercicio de sus funciones públicas, conforme a su legislación específica.

c) Documentos privados.

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.

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.

Certificado reconocido: es el certificado electrónico expedido por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.

Datos de creación de firma: son los datos únicos, como códigos o claves criptográficas privadas, que el firmante utiliza para crear la firma electrónica.

Dispositivo de creación de firma: es un programa o sistema informático que sirve para aplicar los datos de creación de firma.

Dispositivo seguro de creación de firma: es un dispositivo de creación de firma que ofrece, al menos, las siguientes garantías:

a) Que los datos utilizados para la generación de firma pueden producirse sólo una vez y asegura razonablemente su secreto.

b) Que existe una seguridad razonable de que los datos utilizados para la generación de firma no pueden ser derivados de los de verificación de firma o de la propia firma y de que la firma está protegida contra la falsificación con la tecnología existente en cada momento.

c) Que los datos de creación de firma pueden ser protegidos de forma fiable por el firmante contra su utilización por terceros.

d) Que el dispositivo utilizado no altera los datos o el documento que deba firmarse ni impide que éste se muestre al firmante antes del proceso de firma.

Datos de verificación de firma: son los datos, como códigos o claves criptográficas públicas, que se utilizan para verificar la firma electrónica.

Dispositivo de verificación de firma: es un programa o sistema informático que sirve para aplicar los datos de verificación de firma.