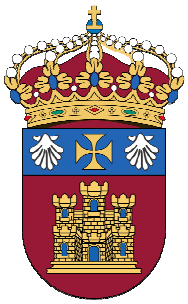
Asesoría y Consultoría TIC de Amazon



Universidad de Burgos

Autor del proyecto: *Dña. Virginia Elena Aguilar Arcos*
Tutor del proyecto: Prof. Miguel Ángel Davara Rodríguez
Directores del Magíster:
Dr. Emilio S. Corchado Rodríguez
Dr. Álvaro Herrero Cosio

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

UNIVERSIDAD DE BURGOS
II Edición. Burgos, Julio 2010.

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

ÍNDICE

1. INTRODUCCIÓN

1.1. CASO DE ESTUDIO

En este proyecto se ha llevado a cabo una asesoría y consultoría en nuevas tecnologías de la información y la comunicación de Amazon.com, Inc., una empresa estadounidense de comercio electrónico con sede en Seattle (Washington) y, actualmente, una de las primeras grandes compañías en vender bienes a través de Internet.

Esta firma se encuentra entre las 500 mayores empresas estadounidenses de capital abierto según la lista Fortune[1] y es un líder global en comercio electrónico. La empresa fue fundada como "Cadabra" por Jeff Bezos en 1994 y fue lanzada el 16 de julio de 1995. Comenzó como una librería online con más de 200.000 títulos que se podían pedir también por e-mail. Más tarde, Bezos se la bautizó Amazon, por el río más grande del mundo, ya que en ese momento circulaban listas ordenadas alfabéticamente y Amazon aparecería en los primeros lugares[2]. Desde el año 2000, logotipo de Amazon es una flecha que va desde la A a la Z, en representación de la satisfacción del cliente (ya que forma una sonrisa), el objetivo así era tener todos los productos por orden alfabético.

Hoy en día, esta empresa de venta al por menor ofrece de todo, desde libros y la electrónica hasta raquetas de tenis y joyas de diamantes. Está diversificada en diferentes líneas de productos, vendiendo DVDs, CDs de música, software, videojuegos, electrónica, muebles, comida, artículos de cocina, herramientas, artículos de césped y jardín, juguetes y juegos, productos para bebés, prendas de vestir, artículos deportivos, comida gourmet, libros, joyas, relojes, salud y artículos de cuidado personal, productos de belleza, instrumentos musicales, ropa, suministros industriales y científicos, etc.

Además de su extensa línea de productos, la compañía intenta por todos los medios personalizar la experiencia de compra del cliente. Cuando se llega a la página de Amazon, no sólo se pueden encontrar ofertas especiales y una amplia gama de productos, sino algunas recomendaciones que van dirigidas expresamente al que les visita. Una vez que uno se registra en Amazon con su nombre y algunos datos, el visitante es tratado de forma personal como si tuviera su propio vendedor asignado. Las técnicas de marketing usadas por Amazon para personalizar la experiencia del visitante, es quizá el mejor ejemplo del acercamiento que tiene la compañía a sus ventas. El seguimiento de clientes es uno de los puntos fuertes de Amazon. Si se permite que Amazon aloje una cookie en el ordenador, se reciben toda clase de consejos, como por ejemplo recomendaciones basadas en anteriores compras y listas de revisiones y guías de usuarios que ya han comprado el producto que andas buscando.

Otra característica que pone a Amazon en otros niveles, es la estrategia multi-nivel que realiza. Amazon permite vender casi cualquier cosa a cualquier persona dentro de su plataforma. Por tanto, se puede decir que Amazon es uno de los grandes, junto a eBay entre otros, que han hecho de la venta en Internet todo un fenómeno. Asimismo, tiene un programa de afiliación, con el que cualquiera puede recibir comisiones por medio de ventas en Amazon. Actualmente existen un programa que permite a dicho afiliados, o como les gusta ser llamados 'asociados', construir sus sitios Web enteramente basados en la plataforma de Amazon. Pueden literalmente crear pequeños sitios Web promocionando cualquiera de los productos que están alojados en la base de datos de Amazon, y usar también sus aplicaciones. Mientras que las ventas vayan a través de Amazon, se puede crear un sitio, poner productos directamente desde los servidores de Amazon, escribir tus propias guías y recomendaciones y percibir una parte de las ventas que generes. Este modelo ya siendo copiado por otras compañías de venta online.

La compañía ha establecido sitios web diferenciados para Canadá, el Reino Unido, Alemania, Austria, Francia, China (Joyo.com) y Japón para poder ofrecer los productos de esos países, tiene más de 20.000 empleados y más de 20 almacenes distribuidos por todo el mundo[3], aunque aún no posee uno para España. La firma también ha absorbido numerosas empresas, siendo algunas de sus adquisiciones: Audible (una empresa de audiolibros), BookSurge (dedicada a los libros de baja demanda), Mobipocket (que crea ebooks y dispositivos para libros electrónicos) o Fabric.com (una empresa de costura).

Asimismo, Amazon ha lanzado sus propios productos como el Kindle[4], un lector de libros electrónicos. También posee Alexa Internet, a9.com, Shopbop, Dpreview.com, Javari.co.uk, A2ZDevelopment, Amazon Web Services, Kongregate e Internet Movie Database (IMDb)[5]. Las páginas web Borders.com, Borders.co.uk, Waldenbooks.com, Virginmega.com, CDNOW.com y HMV.com redirigen a secciones de amazon.com o .co.uk, dependiendo del país, ya que están aliados. Igualmente, ofrece servicios web para gestionar las tiendas en línea de los locales y que éstos sólo se preocupen de la parte corporativa y apoya, pero no controla Shop@AOL, el servicio de AOL de ventas online.

Dada la amplitud de negocio de Amazon, este trabajo se centra únicamente en su modelo de negocio de venta por Internet y se hará el desarrollo de una simulación de implantación de una nueva oficina y almacén en España, así como la creación de la página web www.amazon.es. Su presencia en lengua española sería muy positiva ya que proporcionaría una mejora del servicio en el mercado español, ahorrando tiempo, costes de envío e impuestos y derechos de aduana que se imponen cuando el paquete procede de otro país, así se proporcionaría una mejor atención a los clientes. Además, España tiene una de las mayores industrias editoriales y abriría la competencia con El Corte Inglés, FNAC y la Casa del Libro, que llevan mucho tiempo vendiendo sus productos por Internet.

El estudio se realizará haciendo un recorrido por la legislación aplicable a las TIC (Tecnologías de la Información y Comunicaciones) que comprende los siguientes puntos:

1. Protección de datos de carácter personal.
2. Comercio electrónico.
3. Firma electrónica.
4. Propiedad intelectual e industrial
5. Nombres de dominio.
6. Contratación informática.
7. Fiscalidad electrónica.

En cada apartado se abordará la legislación aplicable y se empleará para el caso de la compañía, analizando la política que sigue o debería seguir para su implantación en

España, así como detectar posibles puntos de mejora. Este esfuerzo de auditoría y consultoría servirá para avanzar en la seguridad y confianza proporcionada por la plataforma de Amazon a la hora de realizar pagos, con el fin de mejorar la calidad del servicio y de atención al cliente y que esto repercuta en un mayor beneficio de la empresa.

1.2. LEGISLACIÓN APLICABLE

El resumen de las leyes y normativas de desarrollo que se abordarán a lo largo del proyecto incluye los siguientes apartados:

1.2.1. Protección de datos de carácter personal

En primer lugar, se examinará la legislación aplicable desde el punto de vista de la protección de datos de carácter personal para el negocio de Amazon. La legislación que se estudiará es la siguiente:

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (En adelante LOPD[6]).
- Real Decreto 1720/2007[7], de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.
- Instrucción 1/2006, de 8 de noviembre, de la Agencia Española de Protección de Datos, sobre el tratamiento de datos personales con fines de vigilancia a través de sistemas de cámaras o videocámaras (Inst. 1/06).

1.2.2. Comercio electrónico

A continuación, se estudiará la legislación concerniente al comercio electrónico, un área de vital importancia para Amazon:

- Ley 34/2002, de 11 de Julio, de servicios de la sociedad de la información y de comercio electrónico, más conocida como Ley de Comercio Electrónico[8] (En adelante LCE).

1.2.3. Firma electrónica

Serán tratados los aspectos relativos a la legislación sobre firma electrónica que vienen recogidos en la siguiente ley:

- Ley 59/2003, de 19 de diciembre, de firma electrónica (B.O.E. núm. 304, de 20 de diciembre). (Modificada por la Ley 56/2007).

1.2.4. Propiedad Intelectual

Los fundamentos de la propiedad intelectual estudiados son tratados en la siguiente ley:

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

1.2.5. Nombres de dominio

En este apartado, nos basaremos en las políticas de la ICANN. El 26 de agosto de 1999, aprobó una Política Uniforme de Solución de Controversias en materia de nombres de dominio, que podemos encontrar en su página Web en inglés, así como una traducción al español en la página Web de la OMPI.

1.2.6. Contratación Informática

La legislación aplicable en contratación informática que se analizará se muestra a continuación:

- Real Decreto legislativo 1/1996, de 12 de abril, por el que se aprueba el texto refundido de la Ley de Propiedad Intelectual, regularizando,

aclarando y armonizando las disposiciones legales vigentes sobre la materia.

- Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias (B.O.E. núm. 287, de 30 de noviembre)
- Orden ITC/1542/2005, de 19 de mayo, que aprueba el Plan Nacional de nombres de dominio de Internet bajo el código de país correspondiente a España («.es») (B.O.E. núm. 129, de 31 de mayo)
- Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información.
- Directiva 91/250/CEE, del Consejo, de 14 de mayo, sobre la protección jurídica de programas de ordenador (D.O. L 122, de 17 de mayo)
- Directiva 96/9/CE, del Parlamento Europeo y del Consejo, de 11 de marzo, sobre la protección jurídica de las bases de datos (D.O. L. 77, de 27 de marzo).

1.2.6. Administración electrónica

La legislación aplicable en administración electrónica incluye los siguientes puntos:

- Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Real Decreto 209/2003, de 21 febrero que regula los registros y las notificaciones telemáticas, así como la utilización de medios telemáticos para la sustitución de la aportación de certificados por los ciudadanos.
- Real Decreto 263/1996, de 16 de febrero, por el que se regula la utilización de técnicas electrónicas, informáticas y telemáticas por la Administración General del Estado.

- Real Decreto 772/1999, de 7 de mayo, por el que se regula la presentación de solicitudes, escritos y comunicaciones ante la Administración General del Estado, la expedición de copias de documentos y devolución de originales y el régimen de las oficinas de registro.

2. ESTUDIO DEL CASO

2.1. PROTECCIÓN DE DATOS

2.1.1. Conceptos básicos

Antes de analizar la actividad de Amazon en cuanto a su política de protección de datos, se ve necesario definir los términos más importantes en este área:

- **Datos de carácter personal:** Cualquier información concerniente a personas físicas identificadas o identificable (artículo 3 a LOPD).
- **Fichero:** Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso (artículo 3 b LOPD).
- **Soporte:** Objeto físico que almacena o contiene datos o documentos, u objeto susceptible de ser tratado en un sistema de información y sobre el cual se pueden grabar y recuperar datos (artículo 5.2. ñ R.D. 1720/2007).
- **Tratamiento de datos:** Cualquier operación o procedimiento técnico, sea o no automatizado, que permita la recogida, grabación, conservación, elaboración, modificación, consulta, utilización, modificación, cancelación, bloqueo o supresión, así como las cesiones de datos que resulten de comunicaciones, consultas, interconexiones y transferencias (artículo 5.1. t R.D. 1720/2007).
- **Afectado o interesado:** Persona física titular de los datos que sean objeto del tratamiento (artículo 5.1. a R.D. 1720/2007).
- **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 (Artículo 3 h LOPD).

- **Procedimiento de disociación:** Todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a persona identificada o identificable (artículo 3 f LOPD)

- **Responsable del fichero o tratamiento:** Persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente. Podrán ser también responsables del fichero o del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados (artículo 5.1. q R.D. 1720/2007).

- **Encargado del tratamiento:** La persona física o jurídica, pública o privada, u órgano administrativo que, solo o conjuntamente con otros, trate datos personales por cuenta del responsable del tratamiento o del responsable del fichero, como consecuencia de la existencia de una relación jurídica que le vincula con el mismo y delimita el ámbito de su actuación para la prestación de un servicio. Podrán ser también encargados del tratamiento los entes sin personalidad jurídica que actúen en el tráfico como sujetos diferenciados (Artículo 5.1. i R.D. 1720/2007).

- **Cesión o comunicación de datos:** Tratamiento de datos que supone su revelación a una persona distinta del interesado (artículo 5.1. c R.D. 1720/2007).

- **Fuentes accesibles al público:** Aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencias que, en su caso, el abono de una contraprestación. Tienen 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 (artículo 3 j LOPD).

- **Cancelación de datos:** Procedimiento en virtud del cual el responsable cesa en el uso de los datos. La cancelación implicará el bloqueo de los datos, consistente

en la identificación y reserva de los mismos con el fin de impedir su tratamiento excepto para su puesta a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento y sólo durante el plazo de prescripción de dichas responsabilidades. Transcurrido ese plazo deberá procederse a la supresión de los datos.

2.1.2. Consideraciones iniciales

Según recoge la página web www.davara.net[9], "La Protección de Datos es un derecho fundamental de los ciudadanos, es el amparo debido a los mismos frente a la utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento, para, de esta forma, confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad. Se trata de garantizar al titular de los datos que los terceros, bien se trate del sector público o del sector privado, utilizarán sus datos personales con el respeto debido al mismo, de forma que aquél pueda tener un control sobre los mismos, y en todo momento sepa qué va a hacer quien trata sus datos, para qué los recoge, cómo los trata y para qué los utiliza o a quién se los cede o comunica".

Según el artículo 1 del Título I (Disposiciones generales) de la LOPD, esta ley "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".

Su objetivo es, por tanto, regular el tratamiento de los datos y ficheros de carácter personal, independientemente del soporte en el cual sean tratados, los derechos de los ciudadanos sobre ellos y las obligaciones de aquellos que los crean o tratan, con el fin de garantizar su honor, intimidad y privacidad personal y familiar. Esta ley será aplicable a los datos de carácter personal registrados en soporte físico, y a todo tratamiento posterior.

Es una ley que define la protección de datos como un derecho fundamental de los ciudadanos. Es decir, protege a los mismos frente a la utilización por terceros, en forma no autorizada, de sus datos personales susceptibles de tratamiento, para, de esta forma,

confeccionar una información que, identificable con él, afecte a su entorno personal, social o profesional, en los límites de su intimidad. La Ley comprende un total de 49 artículos divididos en 7 Títulos y finaliza con una serie de disposiciones.

El tratamiento de datos según el artículo 3 de la LOPD es "cualquier operación y procedimiento técnico de carácter automatizado o no, que permita la recogida, grabación, conservación, elaboración, modificación, bloqueo y cancelación, así como la cesión de datos que resulten de comunicaciones, consultas, interconexiones y transferencias".

En el caso de Amazon, debemos distinguir dentro del organigrama de la compañía, la persona o entidades que van a tratar los datos de clientes del territorio español. Al tratarse de una gran multinacional con sede americana (Seattle), tiene dividida sus áreas de explotación por continentes. En el caso de Europa, la sede de las oficinas centrales se encuentra en Luxemburgo (65, Boulevard Grande-Duchesse Charlotte). En este trabajo, se va a contemplar la posibilidad de que la empresa establezca una oficina propia en España y también un almacén con los productos. La legislación española le será aplicable según se indica en el siguiente artículo:

Según el **artículo 2** referente al *Ámbito de aplicación*:

1. 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. Se regirá por la presente Ley Orgánica todo tratamiento de datos de carácter personal:

a) Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.

b) Cuando al responsable del tratamiento no establecido en territorio español, le sea de aplicación la legislación española en aplicación de normas de Derecho Internacional público.

c) Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, salvo que tales medios se utilicen únicamente con fines de tránsito.

El responsable del tratamiento para España sobre los datos de carácter personal de las personas físicas podría estar delegado en una persona que se encuentre en territorio español con la dirección:

Amazon España
C/ Barajas s/n
28006 Madrid, España
+34 91 568 96 22

2.1.3. Principios de la protección de datos

Los Principios de la Protección de Datos están recogidos en el Título II de la LOPD (son 9 artículos, del 4 al 12), y deben cumplirse por el responsable de los ficheros de Amazon:

- **Calidad de los datos:** Según el artículo 4 los datos deben ser adecuados, pertinentes, no excesivos, exactos y puestos al día de forma que respondan a la situación actual del afectado. Los datos deben ser tratados de forma leal, es decir, los interesados deben estar en condiciones de conocer la existencia de los tratamientos y, cuando los datos se obtengan de ellos mismos, contar con una información precisa y completa respecto a las circunstancias de dicha obtención. Los datos serán cancelados en un plazo máximo de 10 días cuando hayan dejado de ser necesarios para la finalidad para la cual hubieran sido recabados. Queda prohibida la recogida de datos por medios fraudulentos, desleales o ilícitos.

- **Información al interesado:** El artículo 5 establece que el interesado ha de ser informado de forma inequívoca de la existencia del fichero, finalidad, destinatarios, consecuencias y derechos. En todos los casos se deberá conservar el soporte en el que conste el cumplimiento, pudiendo utilizarse medios informáticos o telemáticos. Cuando los datos no hayan sido recabados del interesado, éste deberá ser informado excepto que una ley lo prevea. Algunas excepciones son para fines históricos, estadísticos o científicos, cuando exija esfuerzos desproporcionados o procedan fuentes accesibles al público.

- **Consentimiento:** Según el artículo 6 el interesado debe manifestar su voluntad de forma libre, inequívoca, específica, informada y consciente del tratamiento de datos de carácter personal que le conciernen. Siempre corresponderá al responsable del tratamiento la prueba de la existencia del consentimiento del afectado por cualquier medio de prueba admisible en derecho.

  Cuando se recaba el consentimiento para el tratamiento de datos, el consentimiento debe estar referido a un tratamiento o serie de tratamientos concretos, con delimitación de la finalidad para los que se recaba. Cuando se solicita el consentimiento para la cesión de datos, el afectado deberá ser informado de forma que conozca inequívocamente la finalidad a la que se destinarán los datos, el tipo de actividad desarrollada por el cesionario.

  El consentimiento también podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.

  No será preciso el consentimiento cuando los datos de carácter personal cuando los datos figuren en fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias, ni cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento.

  En estos casos no será preciso el consentimiento pero siempre será necesario el conocimiento, por tanto el responsable del fichero de Amazon España (el que recaba los datos) está obligado de informar al afectado.

El procedimiento recomendado a Amazon España para obtener el consentimiento del interesado es el siguiente:

1. Dirigirse al afectado cumpliendo con las obligaciones de información (artículo 5 de la LOPD y 12.2 del Reglamento).
2. Se concederá un plazo de treinta días para que manifieste su negativa al tratamiento.
3. Con advertencia de consentimiento tácito.

4. Control de devolución (gestión del consentimiento tácito).
5. Facilitar un procedimiento sencillo y gratuito para manifestar la negativa al tratamiento.
6. No será posible solicitar nuevamente el consentimiento respecto de los mismos tratamientos y para las mismas finalidades en el plazo de un año mediante este procedimiento.

Hay algunos casos en los que es necesario tratar el consentimiento de forma específica:

1. Consentimiento de los menores de edad: Será necesario el consentimiento de los padres para los menores de 14 años, y no se podrán obtener datos del menor que permitan obtener información sobre los demás miembros del grupo familiar. El responsable del tratamiento, articulará los procedimientos que garanticen que se ha comprobado la edad del menor y la autenticidad del consentimiento prestado en su caso por los padres, tutores o representantes legales.

   En su página web, Amazon indica que vende productos para niños y menores de edad, pero son los adultos quienes deben comprarlos. Si se tiene menos de 18 años, se podrá utilizar Amazón bajo la supervisión de los padres o tutores.

2. Si se solicitase el consentimiento del afectado durante el proceso de formación de un contrato para finalidades que no guarden relación directa con el mantenimiento, desarrollo o control de la relación contractual, deberá permitir al afectado que manifieste expresamente su negativa al tratamiento o comunicación de datos.

   El afectado podrá revocar su consentimiento a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento, y éste cesará en el tratamiento de los datos en el plazo máximo de 10 días a contar desde el de la recepción de la revocación del consentimiento.

   Amazon deberá conceder a los interesados un medio sencillo y gratuito para que puedan ejercer los derechos de acceso, rectificación y cancelación que son

independientes, de tal forma que no puede entenderse que el ejercicio de ninguno de ellos sea requisito previo para el ejercicio de otro.

Existen excepciones al consentimiento como por ejemplo cuando lo permita alguna norma con rango de Ley, cuando el interesado está dentro de una relación contractual, para proteger el interés vital del interesado o cuando los datos provienen de fuentes accesibles al público.

- **Datos especialmente protegidos:** El artículo 7 trata los datos relacionados con la ideología, afiliación sindical, religión, creencias y datos que hagan referencia al origen racial, salud y vida sexual. Exigen un consentimiento más exigente (expreso y por escrito) y un tratamiento distinto.

- **Datos relativos a la salud:** Se recogen en el artículo 8. Sin perjuicio de lo que se dispone en el artículo 11 respecto de la cesión, las instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

- **Seguridad de los datos:** El artículo 9 expone que el responsable o al encargado del tratamiento debe adoptar las medidas de seguridad del nivel adecuado. Es un principio destinado a proteger los datos personales de su pérdida o acceso por personas no autorizadas. Existen 3 niveles de seguridad (bajo, medio, alto) en función del tipo de dato que se esté protegiendo.

- **Deber de secreto:** En el artículo 10 se expone que el responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo.

El deber de secreto implica que, en la práctica, las personas que deban operar sobre los ficheros tienen que estar bajo normas severas de conducta para el mantenimiento del secreto y para poder prevenir el mal uso de los datos.

Las obligaciones que se desprenden del deber de secreto, durante el tratamiento, cualquiera que sea éste y después de finalizar sus relaciones con el titular del fichero o, en su caso, con el responsable del mismo, son:

- Secreto profesional respecto de los datos que traten,
- Deber de guardarlos y
- Obligación de observar normas severas de conducta para:
    - el mantenimiento del secreto,
    - poder prevenir el mal uso de los datos,
    - evitar el desvío de la información, mal intencionadamente o no, hacia sitios no previstos y garantizar su integridad.

- **Comunicación de datos:** Se encuentra en el artículo 11 y consiste en la revelación de datos del interesado a un tercero, para lo que requiere del consentimiento del interesado. Además, la cesión de datos debe estar justificada. Se indica que para la comunicación o cesión de datos en necesario el consentimiento del interesado excepto que una ley lo permita. No se considera cesión las fuentes accesibles al público, ciertas relaciones jurídicas, Defensor del Pueblo, el Ministerio Fiscal, Jueces o tribunales, el Tribunal de Cuentas o instituciones autonómicas análogas, fines históricos, estadísticos o científicos, urgencias sanitarias, etc.

- **Acceso a los datos por cuenta de terceros:** El artículo 12 establece que este acceso a datos debe estar justificado por la prestación del servicio y limitado por la finalidad. El interesado debe estar informado de cualquier dato que vaya a ser tratado por un tercero y no se considerará comunicación de datos el acceso de un tercero (encargado del tratamiento) a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento. Esta prestación deberá estar regulada en un contrato por escrito y al terminar la relación los datos deberán ser devueltos o destruidos a petición del responsable del fichero.

2.1.4. Derechos de la protección de datos

Los Derechos de la Protección de Datos están contemplados en el Título III de la LOPD (del artículo 13 al 19), corresponden a los interesados o afectados y son la garantía para que éstos puedan tener conocimiento de los tratamientos que se llevan a cabo y poder exigir el cumplimiento de todos los principios por parte de Amazon. Estos derechos son personalísimos, es decir, sólo podrán ser ejercidos por el afectado o su representante voluntario con la correspondiente acreditación. Además serán gratuitos, y podrán ejercerse mediante un procedimiento sencillo.

Los derechos que se reconocen al ciudadano, titular de los datos, en materia de protección de datos son:

- **Artículo 13. Derecho de impugnación de valoraciones:** faculta al interesado a impugnar aquellas decisiones que tengan efectos jurídicos y cuya base sea únicamente un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad. Ofrece la posibilidad de limitar el uso de técnicas que faciliten una información o perfil del interesado que vaya más allá de los datos por él facilitados.

- **Artículo 14. Derecho de consulta al Registro General de Protección de Datos (RGPD):** cualquier persona podrá proceder de forma gratuita a recabar información del RGPD de la AEPD u homólogos en las comunidades autónomas. La información que puede recabar es la relativa a conocer la existencia de tratamientos de los datos, la finalidad de los mismos y la identidad del responsable del fichero.

- **Artículo 15. Derecho de acceso:** el interesado podrá dirigirse al responsable del fichero con objeto de conocer qué datos figuran en el mismo, cuál es el origen de los datos y las comunicaciones que se hubieran realizado o que se prevean realizar en el futuro. Dicho derecho se ejercitará de forma gratuita a intervalos no inferiores a 12 meses, salvo que el interesado acredite un interés legítimo. La información podrá obtenerse mediante la mera consulta de los datos por medio de su visualización, o la indicación de los datos que son objeto de tratamiento

mediante escrito, copia, telecopia o fotocopia, certificada o no, en forma legible e inteligible, sin utilizar claves o códigos que requieran el uso de dispositivos mecánicos específicos.

- **Artículo 16. Derechos de rectificación y cancelación:** son derechos independientes. El primero ofrece al titular la posibilidad de corregir sus datos personales que figuran en un fichero, cuando éstos son inexactos o incompletos. El segundo otorga al titular la posibilidad de pedir que sus datos de carácter personal se cancelen, cuando hayan dejado del servir para el fin para el que fueron recogidos. La solicitud de rectificación debe indicar qué datos son erróneos, y la corrección que debe realizarse, y deberá ir acompañada de la documentación justificativa de la rectificación solicitada, salvo que la misma dependa exclusivamente del consentimiento del interesado.

  El responsable del fichero de Amazon responderá sobre la solicitud de rectificación o cancelación en el plazo máximo de diez días a contar desde la recepción de la solicitud. Transcurrido el plazo, sin que de forma expresa se responda a la petición, el interesado podrá interponer la reclamación prevista en el artículo 18 de la ley orgánica 15/1999, de 13 de diciembre. En el caso de que no disponga de datos de carácter personal del afectado, deberá igualmente comunicárselo en el mismo plazo.

  Si los datos rectificados o cancelados hubieran sido cedidos previamente, el responsable del fichero de Amazon deberá comunicar la rectificación o cancelación efectuada al cesionario, en idéntico plazo, para que éste, también en el plazo de diez días contados desde la recepción de dicha comunicación, proceda, asimismo, a rectificar o cancelar los datos.

  En todo caso, el responsable del fichero de Amazon informará al afectado de su derecho a recabar la tutela de la Agencia Española de Protección de Datos o, en su caso, de las autoridades de control de las Comunidades Autónomas, conforme a lo dispuesto en el artículo 18 de la Ley Orgánica 15/1999, de 13 de diciembre.

Artículo 6.4. Derecho de oposición: en los casos en los que no resulte necesario el consentimiento del interesado para el tratamiento de sus datos, y siempre que una Ley no disponga lo contrario, éste podrá oponerse al tratamiento de los mismos cuando existan motivos fundados y legítimos relativos a una concreta situación personal. Con relación a este derecho se pueden distinguir tres casos:

1. Que no sea necesario el consentimiento del interesado para el tratamiento y la oposición sea consecuencia de la concurrencia de un motivo legítimo y fundado, referido a su concreta situación personal, que lo justifique. En este caso, en la solicitud deberán hacerse constar los motivos fundados y legítimos, relativos a una concreta situación personal del afectado, que justifican el ejercicio de este derecho.

2. Que se trate de ficheros que tengan por finalidad la realización de actividades de publicidad y prospección comercial.

3. Que el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en un tratamiento automatizado de sus datos de carácter personal.

El responsable del fichero de Amazon resolverá sobre la solicitud de oposición en el plazo máximo de diez días a contar desde la recepción de la solicitud y deberá excluir del tratamiento los datos relativos al afectado que ejercite su derecho de oposición o denegar motivadamente la solicitud del interesado en el plazo previsto.

- **Artículo 19. Derecho a indemnización:** supone que aquellos interesados que sufran algún daño o lesión en sus bienes o derechos como consecuencia del incumplimiento de las obligaciones que tienen el responsable o el encargado del tratamiento, en su caso, en el tratamiento de sus datos de carácter personal, pueda ser indemnizado, debiendo acudir a la vía jurisdiccional competente para solicitar la oportuna indemnización.

2.1.4.1. Método para ejercer los derechos

En el ejercicio de los derechos anteriores y de acceso, rectificación, oposición o cancelación (derechos ARCO) hay que tener en cuenta que son derechos independientes, lo que significa que el ejercicio de cualquiera de ellos no debe ser requisito previo para el ejercicio de otro derecho; su ejercicio no conlleva ningún coste para el afectado por ser gratuitos; y, por último, dicho ejercicio deberá llevarse a cabo mediante solicitud escrita ante el responsable del fichero o tratamiento por cualquier medio que permita acreditar al afectado tanto el envío como su recepción por la empresa.

El responsable del tratamiento de Amazon deberá contestar la solicitud que se le dirija en todo caso, con independencia de que figuren o no datos personales del afectado en sus ficheros. En caso de que la solicitud no reúna los requisitos anteriormente expuestos, el responsable del fichero deberá solicitar la subsanación de los mismos.

2.1.5. Ficheros de datos de carácter personal

Los datos de carácter personal son, según el artículo 3 de la LOPD cualquier información concerniente a personas físicas identificadas o identificables. Estos datos podrán ser almacenados como ficheros que son un conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso. Al tratarse de una empresa privada, sus ficheros son de titularidad privada, y se regirán específicamente por las disposiciones del Título IV Capítulo II de la LOPD.

2.1.6. Creación de los ficheros de datos de carácter personal

Como primer paso, se deben crear los ficheros siempre que sea necesario para alcanzar alguna finalidad relacionada con el negocio de Amazon, tal como se indica en el siguiente artículo:

Artículo 25. *Creación*.

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 que esta Ley establece para la protección de las personas".

El responsable del fichero o tratamiento es una persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decide sobre la finalidad, contenido y uso del tratamiento, y es él quien decide qué ficheros se van a crear y con qué finalidad. En este caso, el responsable del fichero final será la propia empresa, en su cargo más alto. No obstante, en este caso, el fichero español se ha delegado a un responsable de la oficina española.

En primer lugar habría que identificar los ficheros de Amazon. La protección de datos tendría tres vertientes:

1. Protección de datos de la empresa (en sentido vertical, consistiría en la propia protección de datos de la empresa). Aquí entrarían los ficheros de:

- **Nómina de personal:** datos de las nóminas que se cobran y los conceptos por los que se cobran del personal de la empresa.
- **Nómina de proveedores:** datos de las nóminas que se cobran y los conceptos por los que se cobran de los proveedores de la empresa.
- **Personal:** datos personales de los empleados que estén trabajando en las oficinas o fábricas de Amazon.
- **Contabilidad:** datos sobre la contabilidad de la empresa, como pagos a proveedores, ventas, etc.
- **Proveedores:** Datos personales de los particulares o empresas que realicen la venta de productos, componentes o materias primas a Amazon.
- **Fichero de marketing:** para realizar el seguimiento de los clientes, uno de los puntos fuertes de Amazon. Este fichero tendrá datos sobre las

anteriores compras, listas de revisiones, guías de usuarios que ya han comprado un producto que otro cliente busque, recomendaciones, críticas y consejos que se hayan proporcionado, etc. Todo esto permite personalizar la experiencia del visitante.

- **Fichero de estudio de mercado:** contendrá datos sobre los comportamientos de los clientes de Amazon en España, los productos que más se solicitan, las épocas del año en las que se compra, etc.

2. Protección de datos hacia fuera: se referiría al de los clientes. Por tanto, habría un fichero de:

- **Clientes:** Datos personales de los particulares o empresas que se registren o realicen compras a través de la web de Amazon o alguno de sus distribuidores.

3. Protección de datos horizontal: En este caso tendríamos el fichero de:

- **Repartidores:** Datos personales de los particulares o empresas encargados de realizar los transportes y envíos de productos comprados a través del portal de Amazon (servicios de mensajería principalmente).

Una vez identificado cada fichero, habría que darle un contenido, en cada caso con la información necesaria para alcanzar la finalidad del negocio.

2.1.7. Inscripción de los ficheros de datos de carácter personal

El siguiente paso, una vez creados los ficheros, sería la inscripción de los mismos en el Registro de la Agencia Española de Protección de Datos (Artículo 26).

Artículo 26. *Notificación e inscripción registral.*

1. 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.

2. Por vía reglamentaria se procederá a la regulación detallada de los distintos extremos que debe contener la notificación, entre los cuales figurarán necesariamente el responsable del fichero, la finalidad del mismo, su ubicación, el tipo de datos de carácter personal que contiene, las medidas de seguridad, con indicación del nivel básico, medio o alto exigible y las cesiones de datos de carácter personal que se prevean realizar y, en su caso, las transferencias de datos que se prevean a países terceros.

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

4. El Registro General de Protección de Datos inscribirá el fichero si la notificación se ajusta a los requisitos exigibles. En caso contrario podrá pedir que se completen los datos que falten o se proceda a su subsanación.

5. Transcurrido un mes desde la presentación de la solicitud de inscripción sin que la Agencia Española de Protección de Datos hubiera resuelto sobre la misma, se entenderá inscrito el fichero automatizado a todos los efectos.

Tal y como describe el artículo 26.2, cuando se notifique a la AEPD sobre los ficheros, se deberá incluir además la información indicada para cada uno de los mismos:

1. **Identidad del responsable del fichero:** Será el mismo para todos los ficheros: Amazon.
2. **Finalidad del fichero:** Dependerá de cada uno de ellos:
    - Nómina de personal: Poder pagar las nóminas de los trabajadores de la empresa.
    - Nómina de proveedores: Poder pagar a los proveedores de la empresa.
    - Personal: Poder tener la información necesaria de los trabajadores para pagar las nóminas, enviar notificaciones, etc.

- Contabilidad: Poder gestionar la contabilidad de la empresa, los pagos a proveedores y los de clientes, etc.
- Proveedores: Poder realizar compras de los productos que se van a vender posteriormente, así componentes y materias primas para productos de fabricación propia de Amazon, como Kindle.
- Fichero de marketing: Poder realizar el seguimiento de los clientes y personalizar su experiencia proporcionándole recomendaciones, guías de usuario, etc.
- Fichero de estudio de mercado: Poder analizar el mercado para decidir qué productos demandan los clientes y cuáles son los que más se compran.
- Clientes: Poder realizar ventas a los mismos, así como poder enviar publicidad siempre que nos haya dado su consentimiento.
- Repartidores: Poder enviar los productos a sus clientes.

3. **Ubicación de los ficheros:** Se abordará este tema en el punto de medidas de seguridad sobre dónde y cómo deben almacenarse los ficheros.
4. **Tipo de datos de carácter personal:** Se hablará de los datos a recabar en el punto de las fases del tratamiento de datos de carácter personal.
5. **Medidas de seguridad:** Se tratará el tema en el punto de niveles de seguridad que van a aplicarse para cada tipo de fichero.
6. **Cesiones de datos a terceros:** Se analizarán en el punto de las fases del tratamiento de datos de carácter personal.
7. **Transferencias de datos a otros países:** Se hablará de sobre las transferencias de datos en el punto de las fases del tratamiento de datos de carácter personal.

La AEPD comprobará que el fichero cumple con los requisitos exigibles y podrá pedir que se completen los datos si observa alguna anomalía. Al cabo de un mes, el fichero se entenderá como inscrito si la AEPD no se ha pronunciado. Asimismo, cualquier cambio que Amazon realice en el fichero, tanto en su finalidad, responsable como en su ubicación, deberá ser notificado a la AEPD para su actualización.

2.1.8. Niveles de seguridad en los datos de carácter personal

En materia de protección de datos, la seguridad debe ser extremada al máximo para impedir el acceso a los ficheros, en particular, y a los datos en general, a personas no autorizadas o para evitar el desvío de la información, mal intencionadamente o no, hacia sitios no previstos; pero la seguridad debe ser también tenida en cuenta para garantizar el tratamiento de datos dentro de los límites permitidos por la norma y con respeto a los derechos del afectado.

La obligación de adoptar las medidas de seguridad está prevista en la LOPD para el responsable del fichero, y para el encargado del tratamiento.

Según el artículo 9 de la LOPD, el responsable del fichero será responsable de asegurar que se cumplen ciertas medidas para garantizar la seguridad de los ficheros de datos de carácter personal. Cada fichero deberá ser clasificado según su nivel de seguridad.

> **Artículo 9.** *Seguridad de los datos.*
>
> 1. El responsable del fichero, y, en su caso, el encargado del tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.
>
> 2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su

integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas.

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

Asimismo, según el artículo 10 de la LOPD, los responsables del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal, aunque sólo sea de consulta, están obligados al deber de secreto.

Las medidas de seguridad vienen definidas en Título VIII del Real Decreto 1720/2007 por el que se aprueba el Reglamento de desarrollo de la ley orgánica 15/1999, de 13 de Diciembre de protección de datos de carácter personal.

En el artículo 80 del Real Decreto las medidas de seguridad las medidas de seguridad exigibles a los ficheros y tratamientos se clasifican en tres niveles: básico, medio y alto. Según el artículo 81, todos los ficheros o tratamientos de datos de carácter personal deberán tener un nivel de seguridad básico:

Artículo 81. *Aplicación de los niveles de seguridad*.

1. Todos los ficheros o tratamientos de datos de carácter personal deberán adoptar las medidas de seguridad calificadas de nivel básico.

2. Deberán implantarse, además de las medidas de seguridad de nivel básico, las medidas de nivel medio, en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los relativos a la comisión de infracciones administrativas o penales.

b) Aquellos cuyo funcionamiento se rija por el artículo 29 de la Ley Orgánica 15/1999, de 13 de diciembre.

c) Aquellos de los que sean responsables Administraciones tributarias y se relacionen con el ejercicio de sus potestades tributarias.

d) Aquéllos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.

e) Aquéllos de los que sean responsables las Entidades Gestoras y Servicios Comunes de la Seguridad Social y se relacionen con el ejercicio de sus competencias. De igual modo, aquellos de los que sean responsables las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

f) Aquéllos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

3. Además de las medidas de nivel básico y medio, las medidas de nivel alto se aplicarán en los siguientes ficheros o tratamientos de datos de carácter personal:

a) Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.

b) Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.

c) Aquellos que contengan datos derivados de actos de violencia de género.

4. A los ficheros de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y a los datos de localización, se aplicarán, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto contenida en el artículo 103 de este reglamento.

5. En caso de ficheros o tratamientos de datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual bastará la implantación de las medidas de seguridad de nivel básico cuando:

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

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

6. También podrán implantarse las medidas de seguridad de nivel básico en los ficheros o tratamientos que contengan datos relativos a la salud, referentes exclusivamente al grado de discapacidad o la simple declaración de la condición de discapacidad o invalidez del afectado, con motivo del cumplimiento de deberes públicos.

7. Las medidas incluidas en cada uno de los niveles descritos anteriormente tienen la condición de mínimos exigibles, sin perjuicio de las disposiciones legales o reglamentarias específicas vigentes que pudieran resultar de aplicación en cada caso o las que por propia iniciativa adoptase el responsable del fichero.

8. A los efectos de facilitar el cumplimiento de lo dispuesto en este título, cuando en un sistema de información existan ficheros o tratamientos que en función de su finalidad o uso concreto, o de la naturaleza de los datos que contengan, requieran la aplicación de un nivel de medidas de seguridad diferente al del sistema principal, podrán segregarse de este último, siendo de aplicación en cada caso el nivel de medidas de seguridad correspondiente y siempre que puedan delimitarse los datos afectados y los usuarios con acceso a los mismos, y que esto se haga constar en el documento de seguridad.

Por tanto, todos los ficheros de Amazon que contengan datos de carácter personal, deberán adoptar las medidas de seguridad de nivel básico. En el caso de los ficheros de las nóminas, este nivel sería suficiente.

Amazon no va a incluir ninguno de los siguientes tipos de datos en sus ficheros:

1. Relativos a ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
2. Datos recabados para fines policiales,
3. Aquéllos que contengan datos derivados de actos de violencia de género.

Por este motivo, según el punto 81.3, no será necesario adoptar medidas de seguridad de nivel alto para ningún fichero de datos de carácter personal. Tampoco habrá ningún dato relativo a la salud, discapacidad o invalidez de los clientes (81.6).

Asimismo, en el punto 81.2f del Real Decreto consta que deberán adoptarse medidas de nivel medio para todos aquellos ficheros que creen perfiles de las personas. En este caso, Amazon crea perfiles sobre sus clientes para ofrecer una mejora del servicio y obtener datos que puedan ser útiles a la compañía.

Hay que tener en cuenta que la LOPD en su artículo 9 establece que se han de cumplir las medidas de seguridad necesarias que garanticen la seguridad de los datos, por lo que aunque un fichero por su naturaleza pertenezca a una categoría pueden ser necesarias medidas de nivel superior o incluso medidas no incluidas en el reglamento. Por lo tanto, el responsable de los ficheros puede adoptar por propia iniciativa un nivel de seguridad mayor al mínimo exigible. En este caso la recomendación para el responsable de los ficheros de Amazon, sería adoptar las siguientes medidas de seguridad:

- Nómina de personal: nivel básico.
- Nómina de proveedores: nivel básico.
- Personal: nivel medio.
- Contabilidad: nivel medio.
- Proveedores: nivel medio.
- Fichero de marketing: nivel medio.
- Fichero de estudio de mercado: nivel medio.
- Clientes: nivel medio.
- Distribuidores: nivel medio.

De esta forma se combinan dos niveles de seguridad para proteger adecuadamente todos los diferentes tipos de ficheros de Amazon, unos ficheros con nivel de seguridad básico y otros con nivel de seguridad medio.

2.1.9. Documento de Seguridad de Amazon

Según el artículo 88, Capitulo II del Real Decreto 1720/2007, de 21 de diciembre, el responsable del fichero o seguridad de Amazon, deberá crear un documento de seguridad donde se recojan todas las medidas de seguridad de índole técnica y organizativa que se van a aplicar sobre los datos de carácter personal. El encargado del tratamiento, junto con el personal encargado deben comprometerse a cumplir las medidas de seguridad de acceso a datos previstas en dicho documento.

El documento de seguridad podrá ser único y comprensivo de todos los ficheros o tratamientos, o bien individualizado para cada fichero o tratamiento. También podrán elaborarse distintos documentos de seguridad agrupando ficheros o tratamientos según el sistema de tratamiento utilizado para su organización, o bien atendiendo a criterios organizativos del responsable. En todo caso, tendrá el carácter de documento interno de la organización.

En el caso de Amazon, se podría elaborar un documento de seguridad que incluya las especificaciones del nivel básico y del nivel medio. Se trataría de un documento que todo el personal de la empresa debe conocer según lo dicta la ley. Lo primero que deberá contener el documento son las funciones y obligaciones del personal, es decir, quién puede acceder a los datos.

El documento de seguridad, conforme al punto 3 del artículo 88, deberá contener como mínimo los siguientes aspectos:

a) Ámbito de aplicación del documento, que serán los ficheros españoles.
b) Medidas, normas, procedimientos de actuación, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este reglamento.
c) Funciones y obligaciones del personal en relación con el tratamiento de los datos de carácter personal incluidos en los ficheros.

d) Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
e) Procedimiento de notificación, gestión y respuesta ante las incidencias.
f) Los procedimientos de realización de copias de respaldo y de recuperación de los datos en los ficheros o tratamientos automatizados.
g) Las medidas que sea necesario adoptar para el transporte de soportes y documentos, así como para la destrucción de los documentos y soportes, o en su caso, la reutilización de estos últimos.

Además, como se adoptarán medidas de seguridad de nivel medio, el documento de seguridad, deberá contener:

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

Cuando exista un tratamiento de datos por cuenta de terceros, el documento de seguridad deberá contener la identificación de los ficheros o tratamientos que se traten en concepto de encargado con referencia expresa al contrato o documento que regule las condiciones del encargo, así como de la identificación del responsable y del período de vigencia del encargo. Según el punto 6, en aquellos casos en los que datos personales de un fichero o tratamiento se incorporen y traten de modo exclusivo en los sistemas del encargado, el responsable deberá anotarlo en su documento de seguridad.

Cuando tal circunstancia afectase a parte o a la totalidad de los ficheros o tratamientos del responsable, podrá delegarse en el encargado la llevanza del documento de seguridad, salvo en lo relativo a aquellos datos contenidos en recursos propios. Este hecho se indicará de modo expreso en el contrato celebrado al amparo del artículo 12 de la Ley Orgánica 15/1999, de 13 de diciembre, con especificación de los ficheros o tratamientos afectados. En tal caso, se atenderá al documento de seguridad del encargado al efecto del cumplimiento de lo dispuesto por este reglamento.

El punto 7 indica que el documento de seguridad deberá mantenerse en todo momento actualizado y será revisado siempre que se produzcan cambios relevantes en el sistema de información, en el sistema de tratamiento empleado, en su organización,

en el contenido de la información incluida en los ficheros o tratamientos o, en su caso, como consecuencia de los controles periódicos realizados. En todo caso, se entenderá que un cambio es relevante cuando pueda repercutir en el cumplimiento de las medidas de seguridad implantadas.

En el punto 8 se señala que el contenido del documento de seguridad deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal. A partir del siguiente modelo de la Agencia Española de Protección de Datos, se podría elaborar el documento de seguridad de Amazon (ver anexo 4.1.).

2.1.10. Medidas de seguridad sobre los datos de carácter personal

En el Real Decreto 1720/2007 están descritas las medidas de seguridad de distintos niveles aplicables a ficheros y tratamientos automatizados y no automatizados.

2.1.10.1. Medidas para ficheros y tratamientos automatizados

Amazon tendrá ficheros electrónicos y tratamientos automatizados. A continuación se resumen las medidas de seguridad de nivel básico que deben cumplir los ficheros y tratamientos automatizados de datos de carácter personal.

- **Funciones y obligaciones del personal (Artículo 89)**

  1. Las funciones y obligaciones de cada uno de los usuarios o perfiles de usuarios con acceso a los datos de carácter personal y a los sistemas de información estarán claramente definidas y documentadas en el documento de seguridad.
  También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

  2. El responsable del fichero o tratamiento adoptará las medidas necesarias para que el personal conozca de una forma comprensible las normas de seguridad que

afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

- **Registro de incidencias (Artículo 90)**

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

- **Control de Acceso (Artículo 91)**

  1. Los usuarios tendrán acceso únicamente a aquellos recursos que precisen para el desarrollo de sus funciones.
  2. El responsable del fichero se encargará de que exista una relación actualizada de usuarios y perfiles de usuarios, y los accesos autorizados para cada uno de ellos.
  3. El responsable del fichero establecerá mecanismos para evitar que un usuario pueda acceder a recursos con derechos distintos de los autorizados.
  4. Exclusivamente el personal autorizado para ello en el documento de seguridad podrá conceder, alterar o anular el acceso autorizado sobre los recursos, conforme a los criterios establecidos por el responsable del fichero.
  5. En caso de que exista personal ajeno al responsable del fichero que tenga acceso a los recursos deberá estar sometido a las mismas condiciones y obligaciones de seguridad que el personal propio.

- **Gestión de soportes y documentos (Artículo 92).**

  1. Los soportes y documentos deberán permitir identificar el tipo de información que contienen, ser inventariados y sólo accesibles por el personal autorizado.

2. La salida de soportes fuera de los locales de Amazon deberá estar autorizada, y deberán adoptarse medidas para evitar su robo.
3. Deberán adoptarse medidas de seguridad en la destrucción de documentos.
4. Siempre que vaya a desecharse cualquier documento o soporte que contenga datos de carácter personal deberá procederse a su destrucción o borrado.
5. La identificación de los soportes que contengan datos de carácter personal que la organización considerase especialmente sensibles se podrá realizar utilizando sistemas de etiquetado comprensibles y con significado que permitan a los usuarios con acceso autorizado a los citados soportes y documentos identificar su contenido, y que dificulten la identificación para el resto de personas.

- **Identificación y Autenticación (Artículo 93).**
    1. Se deberán adoptar medidas para garantizar la correcta identificación y autenticación de los usuarios que accedan a los sistemas de información.
    2. Se debe garantizar la confidencialidad de las contraseñas que se cambiaran con una periodicidad menor de un año.

- **Copias de respaldo y Recuperación (Artículo 94).**
    1. Deberán hacerse copias de respaldo como mínimo semanalmente.
    2. Se establecerán procedimientos para la recuperación de los datos en caso de pérdida.
    3. Se verificará cada 6 meses el correcto funcionamiento de los procedimientos de creación de copias de respaldo.

Además Amazon deberá cumplir estas medidas de seguridad de nivel medio:

- **Responsable de seguridad (Artículo 95).**

  Deberán designarse uno o varios responsables de seguridad para controlar las medidas definidas en el documento de seguridad.

- **Auditoría (Artículo 96).**

  Cada dos años, los sistemas de información deberán someterse a una auditoría interna o externa que verifique el cumplimiento del documento de seguridad. Asimismo dicha auditoría se realizará cuando haya un cambio sustancial en los sistemas de información.

  El informe de la auditoría será analizado por el responsable de seguridad que comunicará al responsable del fichero las medidas correctoras necesarias, y éstas quedarán a disposición de la AEPD.

- **Gestión y soporte de documentos (Artículo 97).**

  Deberá haber sistemas de registro de entrada y salida de soportes que permita conocer toda la información sobre los mismos.

- **Identificación y autentificación (Artículo 98).**

  Se establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

- **Control de acceso físico (Artículo 99).**

  Se restringirá el acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información.

- **Registro de incidencias (Artículo 100).**

  Se registrará todo proceso de restauración de datos. Será necesaria la autorización del responsable del fichero para la ejecución de los procedimientos de recuperación de los datos.

2.1.11. Plan de formación en protección de datos

Hay que tener en cuenta que Amazon está obligada a que todas las personas de la entidad que traten los datos (en los que se aplica la LOPD), deben estar formadas e informadas en protección de datos, por lo que se recomienda llevar a cabo un plan de formación en protección de datos.

La mejor manera de informar será en el contrato de trabajo, pero además, Amazon debe lograr que cada persona conozca cuáles son las obligaciones para cumplir con el documento de seguridad, por lo que se llevarán a cabo actividades complementarias.

El método de formación será a través de cursos online, que deberán realizarse y superarse de forma obligada por todos aquellos que traten datos. En el curso se ofrecerá información sobre la legislación que se aplica en la protección de datos, desde los principios hasta los derechos y se ofrecerán casos prácticos con ejemplos. En este plan se contemplarán dos niveles:

- **Formación de directivos:** se les formará e informará para que conozcan todos los aspectos que debe cumplir la compañía respecto a la protección de datos.

- **Formación de empleados:** se formará e informará a los empleados de Amazon que estén implicados en el tratamiento de datos de carácter personal.

2.1.12. Fases del tratamiento

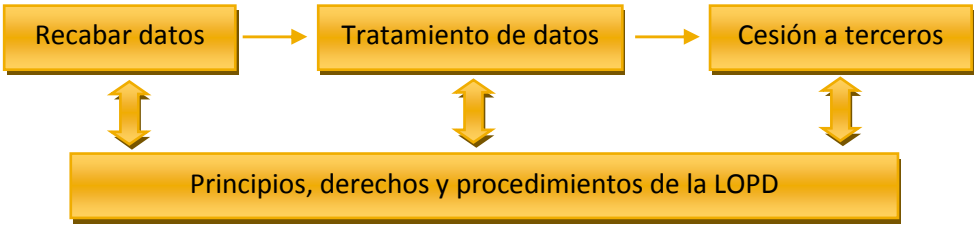
La auditoría a Amazon se tendría que realizar de acuerdo a las tres fases del tratamiento de los datos, que son las siguientes: recabar datos, tratamiento de los datos y cesión de datos.

1. El momento de **recabar los datos**, bien sea directamente del interesado o de un tercero, en el que tiene gran importancia su licitud y lealtad, con las características de conocimiento y, en su caso, consentimiento del afectado.

2. El momento del **tratamiento de los datos**, que pueden ser cruzados y relacionados junto con otros datos, buscando definir un perfil determinado del afectado que incluso él mismo llega a desconocer.

3. El momento de **la utilización y, en su caso, comunicación a terceros de los resultados del tratamiento**, conocida esta última como "cesión o comunicación de datos", en la que, al igual que en la recogida y en el tratamiento, se tendrá que considerar el conocimiento y consentimiento del titular.

El diagrama lógico sería el siguiente:



En cada una de las fases del tratamiento se deberá comprobar si se siguen los principios de la protección de datos (artículos 4 al 12 de la LOPD), los derechos de las personas (artículos 13 al 19 de la LOPD) y los procedimientos a tener en cuenta para posibilitar que el interesado ejerza sus derechos. Será a través del cumplimiento de esas disposiciones legales en cada una de las fases del tratamiento y, lo que es aún más importante, mediante el respeto al derecho fundamental a la protección de datos que se reconoce al titular de los mismos, como podrá garantizarse un tratamiento adecuado y conforme a la Ley Orgánica 15/1999 de Protección de Datos y con la normativa que la desarrolla

A continuación se detallan los pasos que habrá que seguir para cada fase:

2.1.12.1. Recabar los datos

Durante la fase de recabar los datos del cliente, tendremos en cuenta los principios de la protección de datos, y los derechos de las personas plasmados en la Ley Orgánica

15/1999 y la normativa que la desarrolla. Además deberemos conocer los procedimientos para ejercer los derechos del interesado.

Durante la primera fase, podremos recabar los datos, bien sea directamente del interesado o de un tercero siempre con licitud y lealtad. También es muy importante el conocimiento y consentimiento del afectado.

En esta primera fase, se deberán tener en cuenta los siguientes puntos:

- Comprobar que los datos son adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se hayan obtenido de acuerdo con el art 4 de la LOPD.

- Evitar la recogida de datos por medios fraudulentos, desleales o ilícitos (art 4 de la Calidad de los datos) y tendrá cuidado con las fuentes accesibles al público dada su posible falsedad.
- Comprobar que todos los ficheros están inscritos en el RGPD para no tener problemas si la AEPD hace una auditoría de nuestros ficheros.

- Según el artículo 5.1. en el impreso del formulario se deberá informar sobre:

    - La existencia de un fichero o tratamiento de datos de carácter personal, la finalidad de la recogida de éstos y los destinatarios de la información.

    - El carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.

    - Las consecuencias de la obtención de los datos o de la negativa a suministrarlos.

    - La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.

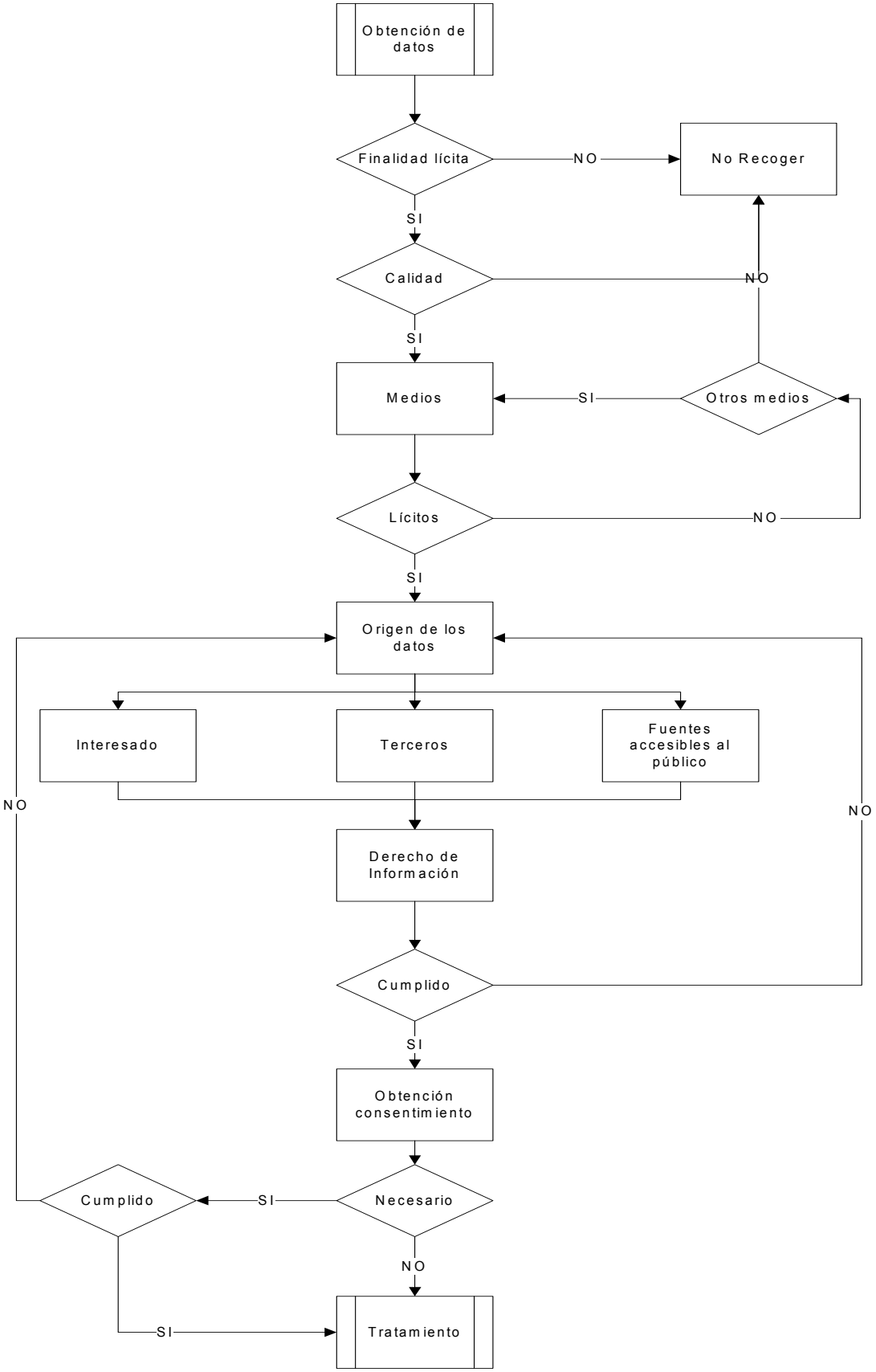
    - La identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

- Si la empresa cede los datos a terceros, deberá también informar de ello en el impreso, indicando el nombre de las empresas a las que se cederán y la finalidad.

- El interesado deberá poder ejercer sus derechos ARCO (acceso, rectificación, cancelación y oposición), por lo que la empresa debe poner a su disposición un procedimiento cumpliendo los plazos que indica la ley (Título III de la LOPD sobre derechos de las personas). Además también debe aplicar el de revocación del consentimiento del artículo 17 del reglamento. Estos servicios deben ser gratuitos para los interesados.

- La empresa debe dotar a sus ficheros de medidas de seguridad según lo establecido en el art. 9 y el Real Decreto 1720/2007. Tiene que indicar qué nivel de seguridad posee (alto, medio o bajo).

En la siguiente figura podemos ver el diagrama lógico de esta fase de recogida de datos.


Obtención de datos
Finalidad lícita
NO
No Recoger
SI
Calidad
NO
SI
Medios
SI
Otros medios
Lícitos
NO
SI
Origen de los datos
Interesado
Terceros
Fuentes accesibles al público
NO
NO
Derecho de Información
Cumplido
SI
Obtención consentimiento
Cumplido
SI
Necesario
NO
SI
Tratamiento

En el caso de Amazon se recogerán datos siguiendo ese esquema y respetando los puntos anteriormente indicados sobre los clientes, empleados, proveedores y distribuidores:

1. Clientes

   Se realiza un registro gratuito a través de la página web de Amazon, para lo que solamente es necesario un email y una contraseña. También existe una casilla para indicar la fecha de nacimiento, pero se señala que no es necesario dar ese dato. A la hora de hacer una compra o envío, se pide una dirección de entrega y los datos de la tarjeta de crédito (en Europa sólo Visa y MasterCard).

   Ya que la recogida de datos de los clientes se hace a través de Internet, hay que preparar un documento o proceso auditable para garantizar que el cliente ha sido informado de las condiciones del contrato (de la misma manera que en el medio offline), es decir garantizar que el cliente ha leído el impreso. Por tanto, se prepara la página web de manera que cuando se recaben datos de una persona no se pueda salir del ciclo de la información (de la pantalla) sin que pinche en la cláusula: "He leído y acepto las condiciones del contrato".

   Por otra parte, para garantizar que el cliente es quien dice ser, por lo que habría que emplear medios garantistas. En este caso no se ve viable que el cliente pase por las oficinas para firmar el contrato y recibir la clave, ni la necesidad de utilización de una firma electrónica avanzada o reconocida, ya que dificultaría demasiado el proceso de compra. Por tanto, en este caso se podría hacer rellenar la cláusula: "Me comprometo a que todos estos datos son verídicos".

   Entre los datos que se le vayan a solicitar habrá que diferenciar entre:

   - **Datos obligatorios**: (para la relación contraactual que se está realizando) como el Nombre, Apellidos, Dirección, DNI (para identificar a la persona inequívocamente) y tarjeta de crédito. En el caso online, llevarían un asterisco para indicar que hay que completar esos campos. Serían los siguientes:
     - Nombre y Apellidos
     - E-mail
     - Dirección

- Ciudad
- Código Postal
- Teléfono
- Contraseña

- **Datos no necesarios:** para los que hay que solicitar el consentimiento de la persona, se podría hacer a través de la pregunta: "¿Quiere usted recibir información sobre productos por e-mail?" El usuario podría marcar con una cruz en SÍ o NO, ya que es voluntario. En el caso online, estos datos no llevarían un asterisco.

2. Empleados

   Se realizará a través de un contrato, por lo que será más sencillo que para los clientes ya que se pueden tomar garantías más fácilmente para comprobar que la persona de la que se recibe los datos es quien dice ser, ya que estará en la oficina físicamente. En el caso de los contratos para empleados, serán suficientes los siguientes datos, que se introducirán en impresos firmados por los empleados:

   - Título
   - Nombre y Apellidos
   - DNI
   - Fecha de nacimiento
   - E-mail
   - Dirección
   - Ciudad
   - Código Postal
   - Teléfono
   - Número de cuenta bancaria
   - Número de la seguridad social
   - Estado civil
   - Titulación

3. Proveedores

   En el caso de los contratos para proveedores, al tratarse de otras empresas, solicitaremos el mismo tipo de datos, en impresos firmados por el representante de la empresa:

   - Nombre de la empresa
   - NIF
   - E-mail
   - Dirección
   - Ciudad
   - Código Postal
   - Teléfono
   - Número de cuenta bancaria

4. Distribuidores.

   Los datos que se recabarán de los distribuidores serán los mismos que de los proveedores.

2.1.12.2. Tratamiento de datos

En la fase del tratamiento de datos se crean perfiles de los usuarios ya que Amazon cruza datos y los relaciona con otros, obteniendo nuevas informaciones. Por tanto, habrá que tener en cuenta las siguientes consideraciones:

- Para poder realizar un tratamiento de los datos de carácter personal con una finalidad determinada, tendremos que recabar el consentimiento del interesado como condición indispensable, según se indica en el artículo 6.1. de la LOPD: "El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa".

a. En la página web redactaremos una declaración de privacidad, en la que se explique de manera clara y unívoca, que al registrarse, se está dando el consentimiento para tratar nuestros datos.

b. En los contratos, deberá redactarse un apartado en la que se especifique que nuestros datos van a pasar a formar parte de un fichero de datos de carácter personal, y que éste puede ser objeto de tratamiento.

- La empresa no podrá tratar los datos para fines diferentes a los expuestos en el momento de su obtención según el artículo 4 Calidad de los Datos.

  a. En el caso de los clientes de la página web, si se desea dar otro tratamiento, habrá que recabar el consentimiento del interesado con tal fin, mediante un checkbox.

  b. En los contratos, cualquier otra finalidad que no esté directamente relacionada con la propia relación contractual, deberá ser especificada claramente

- Según este mismo artículo, se deberán poner todos los medios posibles para que los datos que se traten sean exactos y puestos al día.

  a. Los clientes de la página web, deberán poder acceder a su perfil online y actualizar sus datos personales.

  b. En los contratos, una vez finalizados, se deberá habilitar algún procedimiento por medios electrónicos o no electrónicos, para cambiar los datos personales.

- El interesado podrá también ejercer sus derechos en el tratamiento de los datos, de modo que en cualquier momento puede revocar el consentimiento a que sus datos sean tratados (art 6 sobre Consentimiento).

- En el caso de datos especialmente protegidos será necesario el consentimiento expreso y por escrito para poder tratarlos (art. 8 datos especialmente protegidos).

- No se podrán comunicar datos de otros clientes, ya que estos son secretos, y sólo ellos mismos tendrán derecho a acceder a ellos.
- Los clientes tienen derecho a no verse sometidos a una decisión con efectos jurídicos, basada en un tratamiento automatizado de sus datos.
- Los clientes tendrán derecho a consultar al RGPD, el tratamiento de datos, sus finalidades y la identidad del responsable del fichero de Amazon.
- Los clientes tendrán derecho en intervalos no menores a 12 meses 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.

2.1.12.3. Cesión de datos

Después de que los datos hayan sido tratados, pueden ser utilizados y, en su caso, cedidos a terceros. La cesión de datos se muestra como un punto conflictivo en la ley ya que con la cesión se posibilita el cruce de los datos, aplicando con toda intensidad las posibilidades de tratamiento de la información que posee la informática y, además, la cesión facilita la utilización de los datos para un uso que no es el mismo para el que se habían recabado.

Es por ello que la cesión siempre necesitará del consentimiento del titular de los datos, del afectado, y solamente podrá utilizarse ese consentimiento, en el caso de que le otorgue su titular "para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario" salvo que la Ley prevea otra cosa, o se trate de datos recogidos de fuentes accesibles al público, o que exista previo consentimiento del afectado para realizar la cesión.

En el caso de Amazon, la cesión sólo será legítima en cuanto se limite a la finalidad que la justifique, o, en determinados casos, "cuando la cesión se produzca entre las Administraciones Públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos" o, por último, "cuando la cesión de

datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero".

Durante la fase de cesión de datos de Amazon, tendremos que tener en cuenta las siguientes consideraciones:

- Para que los datos de los clientes puedan ser cedidos a los distribuidores, será necesario recabar el consentimiento del interesado, si no se hizo durante la firma del contrato. Éste consentimiento, tendrá también un carácter revocable.
- Para que el consentimiento sea válido, deberá especificarse la finalidad a la que se destinarán los datos en la cesión.
- En el momento en que se efectúe la primera cesión de datos, se deberá informar de ello a los clientes, indicando, asimismo, la finalidad del fichero, la naturaleza de los datos que han sido cedidos y el nombre y dirección del cesionario.
- No se considerará cesión de datos cuando los datos de los clientes hayan sido obtenidos de fuentes accesibles al público.
- No se considerará cesión de datos, sino encargado de tratamiento, al acceso de datos por parte de los repartidores ya que son necesarios para la prestación del servicio. Este acceso deberá estar regulado mediante un contrato regulado en el artículo 12 de la LOPD en el que se restrinja el uso de estos datos.
- Es aconsejable especificar qué ocurrirá con los datos cuando el tratamiento haya finalizado. Para evitar problemas, los datos se deberían devolver al responsable del fichero.
- En caso de que los repartidores incumplan las condiciones del contrato, la responsabilidad recaerá sobre el responsable del tratamiento.
- Cuando exista la figura del encargado del tratamiento será necesario firmar un contrato según lo establecido en el artículo 12 de la ley y prestar especial atención al momento de indicar si los datos deben ser devueltos o destruidos, reservando siempre la decisión al responsable del fichero.

La información sobre los clientes es una parte importante del negocio. En la página web de Amazon en Francia (www.amazon.fr) se detallan los casos en los que las informaciones se comparten con terceros:

Afiliados

Amazon comparte esta información con Amazon.com, Inc.. filiales y Amazon. com, Inc. control y que cumplan con esta política o hagan cumplir las normas de protección como las que se describen en esta política, de acuerdo con lo que se describe a continuación en esta sección y para los fines establecidos en la presente política de protección de datos personales.

Afiliados que Amazon no controla

Trabajamos estrechamente con nuestros socios. En algunos casos, como el "Marketplace", estos socios pueden utilizar sus propios establecimientos o en venderle sus productos o servicios directamente a través del sitio Amazon.fr. En otros casos, la explotación de establecimientos, prestación de servicios o venden líneas de productos conjuntamente con estos socios, o por su cuenta. Para ver algunos ejemplos de las ofertas de marca compartida o conjunta las ofertas, haga clic aquí. Usted puede decir, cuando un tercero está implicado en sus transacciones. Podemos compartir con la información de terceros relativos a las operaciones con ese tercero.

Servicios de terceros

Nosotros utilizamos los servicios de otras empresas o personas independientes que prestan ciertos servicios en nuestro nombre. Los ejemplos incluyen el procesamiento de pedidos, envío de productos, envío de correo postal o por vía electrónica, la gestión de nuestras listas de clientes, análisis de nuestra base de datos, servicios de marketing, la provisión de los resultados de investigación y enlaces (incluidos los listados pagados y enlaces), procesamiento de pagos con tarjeta de crédito y servicios al cliente. Estos

proveedores tienen acceso a la información personal necesaria para realizar sus funciones y no se les permite utilizarla con otros fines. Por otra parte, están obligados a tratar dicha información de conformidad con la política y la aplicación de la legislación francesa sobre la información personal.

Ofertas

Con sujeción a su consentimiento, dado en su cuenta, en ocasiones se puede enviar ofertas a determinadas categorías de clientes Amazon.fr en nombre de otras empresas. En este caso, sólo se proporcionará a esas empresas a su nombre o dirección. Si el cliente ya no desea recibir tales ofertas, puede fácilmente y en cualquier momento cambiar sus preferencias al visitar su cuenta.

La transferencia de empresas o actividades

En el desarrollo del negocio de Amazon, y/o otras empresas controladas por Amazon.com, Inc.. pueden ser inducidos a vender o adquirir la totalidad o parte de las empresas, filiales o segmentos de negocio tales como ir de compras. En relación con dichas operaciones, la información del cliente es generalmente uno de los activos transferidos, dado que los compromisos políticos para la protección de la información, mientras que todavía se aplica (excepto, por supuesto, otro cliente de consentimiento). Por otra parte, en el improbable caso en que Amazon.com, Inc. o una de sus partes sustanciales sean adquiridos, la información del cliente será, evidentemente, también se suministren al comprador.

La protección de Amazon.com y otros

Nos revelará el contenido de las cuentas por cobrar y otra información personal cuando se requieran legalmente o si la revelación es necesaria para llevar a cabo y hacer cumplir nuestras Condiciones de Uso o cualquier otro acuerdo que tenemos con usted, o para proteger los derechos Amazon.com o los usuarios de los sitios de Amazon y

servicios. La información sobre nuestros clientes es una parte importante de nuestro negocio. Nuestro trabajo no es hacer que el comercio. Nosotros compartimos esta información con terceros si:

Anunciantes de terceros y enlaces a otros sitios web

Nuestro sitio puede incluir publicidad de terceros y enlaces a otros sitios web. En ningún caso se pasa información personal para identificar a nuestros clientes a estos anunciantes o los sitios web de terceros. Gracias, haga clic aquí para ver ejemplos e información sobre cómo ponerse en contacto con estas empresas para obtener más información o para la forma del traslado o de recogida de información.

Estos sitios web de terceros y el anunciante o empresas de publicidad en Internet que trabajan en su nombre, a veces utilizan la tecnología para enviar mensajes publicitarios que aparecen en nuestra página web directamente en su navegador. En este caso, reciben automáticamente su dirección IP. También puede utilizar cookies, Javascript, etiquetas, o imágenes de un pixel en formato GIF (gif de un solo píxel) y otras tecnologías para medir la efectividad de sus anuncios y para personalizar el contenido publicitario. Nosotros no tenemos acceso ni control sobre estas cookies u otras características que puede tener que utilizar. El uso de prácticas de información de los sitios web y anunciantes que no estén cubiertas nuestra política no proteger su información personal. Muchas gracias ponerse en contacto directamente con ellos para aprender más acerca de su política de protección de datos personales. Además, el "Network Advertising Initiative ofrece información útil sobre las empresas de publicidad de Internet (también llamada" red de anuncios "o" anunciante de la red "), incluyendo los procedimientos para el arranque o la recogida de información.

Amazon envía las páginas web de sus anuncios de banner sitio adaptado a los intereses del usuario. Aunque Amazon no comparte información de identificación personal de sus usuarios a los anunciantes de terceros, ellos (incluida la publicidad en línea las sociedades de inversiones) puede significar que los usuarios hacer clic en un vínculo o un anuncio que corresponde a los criterios utilizados para la exhibición publicidad (por ejemplo, los usuarios franceses a quienes les gusta la música clásica).

Otros casos

En los demás casos, se le notificará si los datos fueron transmitidos a terceros y usted tiene la oportunidad de dar su consentimiento. Si transferimos información personal a países fuera del Espacio Económico Europeo (EEE) con el fin de compartir información como el descrito anteriormente, Amazon se asegurará de que la información es transferida de conformidad con esta política y según la legislación vigente sobre datos personales. En el punto siguiente se desarrolla este último apartado.

2.1.13. Transferencia internacional de datos

En primer lugar decir que la Transferencia Internacional de Datos (TID) es un tipo de cesión de datos, en la que los datos salen del control del responsable del fichero, y pasan a ser accesibles por un tercero. Para analizar la licitud y legalidad de la transferencia internacional de datos, debemos analizar por un lado el país de destino de los datos y, por otro, la finalidad con que se realiza la TID.

Dentro del primer criterio, el país de destino, podemos diferenciar, a su vez, tres casos distintos:

1. Un país de la Unión Europea o del Espacio Económico Europeo.

2. Un país declarado con un nivel adecuado de protección.

3. Un tercer país.

En los dos primeros casos, la TID es libre, esto es, puede realizarse del mismo modo que las comunicaciones, o en su caso, prestaciones de servicios dentro del país comunitario origen de los datos.

En cuanto al criterio de la finalidad, ésta puede ser:

1. Una comunicación a un tercero.

2. Un encargo o prestación de servicios.

La Transferencia Internacional de Datos se encuentra en la última fase del tratamiento, en la que los datos salen del control del responsable del fichero. Por tanto, hay una comunicación de datos (art. 11 LOPD) o un acceso a los datos por cuenta de terceros (art. 12 LOPD). Al llevar a cabo un análisis jurídico de la regulación que en la LOPD se hace de la TID, hay que tener en cuenta que esta Ley prohíbe la transferencia de datos a terceros países que no proporcionen un nivel de protección equiparable al que presta la misma (art. 33 LOPD). Además es necesaria la obtención de autorización previa del Director de la Agencia Española de Protección de Datos (AEPD) que se otorgará con base en la concurrencia de garantías adecuadas y la evaluación del nivel de protección del país de destino (art. 33 LOPD).

Existen excepciones a esta norma general cuando el afectado haya dado su consentimiento inequívoco a la transferencia prevista (art. 34e LOPD), o cuando el país destino sea un estado miembro de la Unión Europea, o un Estado respecto del cual la Comisión de las Comunidades Europeas, en el ejercicio de sus competencias, haya declarado que garantiza un nivel de protección adecuado (art. 34k LOPD).

Al ser Amazon una multinacional americana que realiza su actividad de negocio en España, habrá cierta información sobre su actividad en España que deberá conocer la sede de EE.UU., dando lugar a la transferencia internacional de datos. Además los clientes particulares de Amazon en España dependen directamente de la sede en Luxemburgo, por lo que podemos asegurar que la totalidad de los datos de carácter personal de los clientes españoles van a viajar a Luxemburgo.

Por lo tanto, tenemos dos casos que analizaremos por separado:

- Una transferencia internacional de datos a un país miembro de la Unión Europea (Luxemburgo) con un nivel adecuado de protección de datos. Veremos qué principios, mecanismos y objetivos son necesarios para poder asegurar un nivel adecuado de protección de datos.

- Una transferencia internacional de datos a un país no comunitario que no tiene protección de datos (Estados Unidos). En relación a este país

tendremos que tener en cuenta la decisión 2000/520/CE, de 26 de Julio de 2000, de la Comisión, con arreglo a la Directiva 95/46/CE del Parlamento Europeo y del Consejo, sobre la adecuación de la protección conferida por los principios de puerto seguro para la protección de la vida privada y las correspondientes preguntas más frecuentes, publicadas por el Departamento de Comercio de Estados Unidos de América.

2.1.13.1. Nivel de protección adecuado

Para lograr un nivel de protección adecuado es necesario buscar una combinación de derechos para el sujeto de los datos y de obligaciones para aquellos que procesan los datos o que ejercen un control sobre dicho tratamiento. El nivel de protección adecuado no depende exclusivamente de la existencia de normas sobre protección de datos, sino que es necesario que esas normas se apliquen a la práctica. Por lo tanto son dos los elementos básicos para una protección adecuada: el contenido de las normas aplicables y los medios para garantizar su aplicación efectiva.

La Unión Europea ha adoptado la Directiva 95/46/CE que prohíbe la transferencia de datos personales a los países que, en su opinión, no otorgue una protección adecuada a la privacidad de los ciudadanos de la Unión Europea.

En primer lugar, la Directiva recoge como principios básicos los siguientes:

- **Principio de limitación del propósito:** Los datos deberán tratarse para un propósito específico y utilizarse o comunicarse posteriormente únicamente en la medida en que ello no sea incompatible con el propósito de la transferencia.

- **Calidad de los datos:** los datos deberán ser exactos y, cuando sea necesario, actualizados. Los datos deberán ser adecuados, relevantes y no excesivos con relación al objeto por el que se transfieren o se tratan.

- **Principio de transparencia:** deberá proporcionarse a los individuos información respecto al propósito del tratamiento y la identidad del

controlador de datos en el país tercero, así como cualquier otra información siempre que sea necesario para garantizar la equidad.

- **Principio de seguridad:** el controlador de los datos deberá adoptar medidas de seguridad técnicas y organizativas adecuadas a los riegos que presente el tratamiento. Cualquier persona que actúe bajo la autoridad del controlador de datos, incluidos los responsables del tratamiento, no deberán tratar los datos salvo por instrucción del controlador.

- **Derechos de acceso, rectificación y oposición:** El sujeto de los datos deberá tener derecho a obtener una copia de todos los datos relativos a él o ella que sean tratados, y un derecho a rectificar dichos datos cuando resulten inexactos. En determinadas situaciones el sujeto también deberá poder oponerse al tratamiento de los datos relativos a él o ella.

- **Restricciones a las transferencias sucesivas a otros países terceros:** las transferencias sucesivas de datos personales a partir del país tercero de destino a otro país tercero deberán permitirse únicamente cuando el segundo país tercero también garantice un nivel adecuado de protección.

En segundo lugar, la Directiva fija los mecanismos de procedimientos y de aplicación de las normas sobre protección de datos. El punto de partida es tratar de identificar los objetivos subyacentes de un sistema procedimental de protección de datos, y sobre esta base juzgar la variedad de diferentes mecanismos procedimentales judiciales y no judiciales que se utilizan en los países terceros, en términos de su capacidad para cumplir estos objetivos.

Por último, señala que los objetivos de un sistema de protección de datos son fundamentalmente los siguientes:

1. Proporcionar un buen nivel de cumplimiento de las normas. Un buen sistema se caracteriza generalmente por un elevado nivel de concienciación entre los controladores de datos respecto de sus obligaciones, y entre los sujetos de los datos respecto de sus derechos y su forma de ejercicio. La existencia de sanciones efectivas y disuasorias es importante para garantizar el respeto por las normas, así como los sistemas de

comprobación directa por parte de las autoridades, auditores o funcionarios independientes responsables de la protección de datos.

2. Proporcionar apoyo y ayuda a los sujetos de datos individuales en el ejercicio de sus derechos. Los individuos deberán ser capaces de ejercer sus derechos de forma rápida y eficaz, y sin costes prohibitivos. Para ello deberá existir algún tipo de mecanismo institucional que permita una investigación independiente de las denuncias

3. Proporcionar una reparación adecuada a las partes perjudicadas cuando no se cumplan las normas. Esto es un elemento clave que debe contar con un sistema de arbitraje independiente que permita pagar una compensación e imponer sanciones cuando sea oportuno.

2.1.13.2 El acuerdo de Puerto Seguro

Se encuentra en el artículo 25. Para asegurar que las diferentes políticas de privacidad en el mundo no impiden el flujo transfronterizo de datos en Internet, los EEUU han decidido involucrar a sus socios comerciales principales en discusiones para construir un soporte para soluciones desarrolladas por la industria a los problemas de privacidad y para los mecanismos dirigidos por el mercado para asegurar la satisfacción del consumidor sobre el manejo de sus datos privados. El Acuerdo de Puerto Seguro es fruto de las negociaciones de EEUU con la UE.

Los datos a los que se aplican los principios de Puerto Seguro son todos los datos personales recibidos desde la UE a partir del momento en que una entidad se adhiere a este sistema. Estos principios son:

- Notificación
- Opción
- Transferencia ulterior
- Seguridad
- Integridad de los datos
- Acceso
- Aplicación

Amazon deberá tener en cuenta estos principios para su sitio web español y deberá aplicarlos a los datos que reciba de sus clientes, empleados, proveedores y distribuidores de la Unión Europea.

Según se indica en la página web francesa, Amazon.com, Inc. y sus filiales en Estados Unidos (que controla Amazon.com, Inc.) ya participan en el programa de Puerto Seguro. Estas sociedades del grupo Amazon han certificado su adhesión a los principios concernientes a la protección de datos del Puerto Seguro, aceptados conjuntamente por los Estados Unidos y la Unión Europea. La página ofrece una dirección de correo electrónico para contactar con Amazon.com en lo referente a este programa: safeharbour@amazon.com como se puede ver en la imagen.

2.1.14. Publicidad

Para las actividades de publicidad es necesario, en todos los casos, y más en aquellas como la publicidad a través de Internet, una de cuyas ventajas es la personalización de los usuarios a los que va dirigida, el tratamiento de datos de carácter personal.En el artículo 30 de la LOPD se regulan los ficheros para publicidad y los dedicados a actividades de venta directa, que contemplan la actividad publicitaria, comercial y de marketing directo, permitiendo la utilización para esos fines, de 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, y siempre con el derecho de los ciudadanos a conocer el origen de sus datos de carácter personal y a no figurar en dichas listas si así lo solicitan:

Artículo 30. *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.

Por tanto, Amazon podrá beneficiarse del tratamiento de los datos con fines de publicidad, pero solamente podrá utilizar nombres y direcciones u otros datos de carácter personal cuando figuren en alguna fuente accesible al público o cuando hayan sido facilitados por los propios interesados u obtenidos con su consentimiento para finalidades determinadas, explícitas y legítimas relacionadas con la actividad de publicidad o prospección comercial, habiéndose informado a los interesados sobre los sectores específicos y concretos de actividad respecto de los que podrá recibir información o publicidad.

En el caso de los clientes, se podrá pedir el consentimiento de la persona a través de una cláusula que deberá marcar.

Si Amazon decide contratar a un tercero para la realización de una determinada campaña publicitaria de sus productos o servicios, encomendándole el tratamiento de determinados datos, se aplicarán las siguientes normas:

- Cuando los parámetros identificativos de los destinatarios de la campaña sean fijados por la entidad que contrae la campaña, ésta será responsable del tratamiento de los datos.

- Cuando los parámetros fueran determinados únicamente por la entidad o entidades contratadas, dichas entidades serán las responsables del tratamiento.

- Cuando en la determinación de los parámetros intervengan ambas entidades, serán ambas responsables del tratamiento.

Cuando intervengan las dos entidades en la determinación de los parámetros, la entidad que encargue la realización de la campaña publicitaria deberá adoptar las medidas necesarias para asegurarse de que la entidad contratada ha recabado los datos cumpliendo las exigencias establecidas en la LOPD. Se considerarán parámetros identificativos de los destinatarios las variables utilizadas para identificar el público objetivo o destinatario de una campaña o promoción comercial de productos o servicios que permitan acotar los destinatarios individuales de la misma.

Cuando los datos de carácter personal hayan sido recabados directamente del cliente a través de la página web, necesitaremos el consentimiento del mismo. Esto se puede implementar mediante una casilla que cuando se marque, acepte que Amazon le envíe publicidad. Cuando los datos de los clientes se obtengan a través de fuentes accesibles al público, habrá que informar en la publicidad que se envíe del origen de los datos y de la identidad del responsable de tratamiento.

En cualquiera de los casos anteriores, los clientes tendrán derecho a oponerse a recibir publicidad de forma gratuita.

2.1.14.1. Listas Robinson

Para las actividades de publicidad, es necesaria la utilización de los datos de carácter personal disponible y en muchos casos se realiza sin el consentimiento del titular de los datos, por lo que, para evitar la conculcación de derechos de las personas, se deben tomar unas medidas adicionales. Una de las primeras fue crear estas listas.

Además de los códigos éticos o las medidas de autorregulación que toman las empresas, especialmente en Internet, existe este mecanismo para proteger a los usuarios. Estos listados son gestionados por la Federación de Comercio Electrónico y Marketing Directo a las que pueden suscribirse las personas que no desean recibir publicidad.

Las listas Robinson no son de obligada consulta para las empresas, aunque su uso les puede suponer una serie de ventajas, sobre todo un ahorro económico. El problema es que al globalizarse el medio de transmisión de la publicidad, y al ser las listas en las que se pueden inscribir las personas de carácter local, el problema que nos podemos encontrar es el desconocimiento de la empresa que realiza la publicidad de la inserción de esa persona en alguna Lista Robinson. Además, los usuarios no pueden evitar completamente que les llegue publicidad, ya que no pueden poner barreras a que lleguen folletos que se buzonean indiscriminadamente o los mensajes publicitarios de las empresas de las que uno es cliente.

Por otra parte, estas listas funcionan básicamente para el entorno offline porque no se pueden aplicar técnicamente al entorno digital. Las denominadas Listas Robinson son una base de datos de direcciones de personas que, por propia voluntad, no quieren recibir publicidad directa de ninguna empresa. Representan uno de los medios para evitar que un tercero se pueda dirigir al afectado sin su consentimiento.

El Reglamento contempla el mantenimiento de estas listas Robinson incluso con la creación de ficheros comunes, de carácter general o sectorial, en los que sean objeto de tratamiento los datos de carácter personal que resulten necesarios para evitar el envío de comunicaciones comerciales a los interesados que manifiesten su negativa u oposición a recibir publicidad.

De esta forma, cuando el afectado manifieste ante un concreto responsable su negativa u oposición a que sus datos sean tratados con fines de publicidad o prospección

comercial, aquél deberá ser informado de la existencia de los ficheros comunes de exclusión generales o sectoriales, así como de la identidad de su responsable, su domicilio y la finalidad del tratamiento. El afectado podrá solicitar su exclusión respecto de un fichero o tratamiento concreto o su inclusión en ficheros comunes de excluidos de carácter general o sectorial.

De esta forma, Amazon deberá previamente consultar los ficheros comunes que pudieran afectar a su actuación, a fin de evitar que sean objeto de tratamiento los datos de los afectados que hubieran manifestado su oposición o negativa a ese tratamiento.

2.1.15. Ficheros sobre solvencia patrimonial y crédito

Existen otro tipo de ficheros que contienen datos de carácter personal, pero que no van a ser gestionados por el responsable del fichero de Amazon, son los denominados ficheros de solvencia patrimonial y crédito. Estos ficheros contendrán información crediticia sobre los clientes de Amazon.

Se pueden distinguir dos tipos de ficheros, por un lado los ficheros denominados popularmente como de "morosos" (cuyo responsable es ASNEF), y por otro los de información comercial o para evaluar la solvencia. Ambos ficheros se encuentran regulados con un régimen excepcional en este artículo 29, que distingue entre estos dos tipos de ficheros de acuerdo con la fuente de la que proceden los datos, esto es, de una parte, que los datos sean recabados de una fuente accesible al público o del afectado, y, de otra, que los datos sean recabados del acreedor:

> **Artículo 29.** *Prestación de servicios de información sobre solvencia patrimonial y crédito.*
>
> 1. Quienes se dediquen a la prestación de servicios de información sobre la solvencia patrimonial y el crédito sólo podrán tratar datos de carácter personal obtenidos de los registros y las fuentes accesibles al público establecidos al efecto o procedentes de informaciones facilitadas por el interesado o con su consentimiento.

2. Podrán tratarse también datos de carácter personal relativos al cumplimiento o incumplimiento de obligaciones dinerarias facilitados por el acreedor o por quien actúe por su cuenta o interés. En estos casos se notificará a los interesados respecto de los que hayan registrado datos de carácter personal en ficheros, en el plazo de treinta días desde dicho registro, una referencia de los que hubiesen sido incluidos y se les informará de su derecho a recabar información de la totalidad de ellos, en los términos establecidos por la presente Ley.

3. En los supuestos a que se refieren los dos apartados anteriores, cuando el interesado lo solicite, el responsable del tratamiento le comunicará los datos, así como las evaluaciones y apreciaciones que sobre el mismo hayan sido comunicadas durante los últimos seis meses y el nombre y dirección de la persona o entidad a quien se hayan revelado los datos.

4. Sólo se podrán registrar y ceder los datos de carácter personal que sean determinantes para enjuiciar la solvencia económica de los interesados y que no se refieran, cuando sean adversos, a más de seis años, siempre que respondan con veracidad a la situación actual de aquéllos.

Los ficheros de información comercial obtienen sus datos de fuentes accesibles al público o procedentes de informaciones facilitadas por el afectado o con su consentimiento y han sido recogidos y reconocidos en la primera parte del artículo. Por su parte, los ficheros de morosos recaban los datos del acreedor o de quien actúe por su cuenta o interés.

El acreedor o entidad financiera tendrá la obligación de informar al deudor en el momento en que se celebre el contrato y, en todo caso, al tiempo de efectuar el requerimiento previo de pago, que en caso de no producirse el pago en el tiempo previsto para ello y cumplirse los requisitos previos, los datos relativos al impago podrán ser comunicados a ficheros relativos al cumplimiento o incumplimiento de obligaciones dinerarias.

El responsable del fichero común deberá efectuar la notificación de la inclusión a través de un medio fiable, auditable e independiente de la entidad notificante, que permita acreditar la efectiva realización de los envíos, al tiempo que debe establecerse

un procedimiento para conocer si la notificación ha sido objeto de devolución por cualquier causa, en cuyo caso no podrá proceder al tratamiento de los datos referidos a ese interesado, no entendiéndose suficientes para que no se pueda proceder al tratamiento de los datos referidos a un interesado las devoluciones en las que el destinatario haya rehusado recibir el envío.

En caso de devolución de la notificación, el responsable del fichero común comprobará con la entidad acreedora que la dirección utilizada para efectuar esta notificación se corresponde con la contractualmente pactada con el cliente a efectos de comunicaciones, y no procederá al tratamiento de los datos si la mencionada entidad no confirma la exactitud de este dato.

En caso de que la contratación de productos o servicios financieros por vía telefónica, la información podrá realizarse de forma no escrita, correspondiendo al tercero la prueba del cumplimiento del deber de informar.

2.2. COMERCIO ELECTRÓNICO

2.2.1. Conceptos básicos

Antes de analizar la actividad de Amazon en cuanto a la legislación sobre comercio electrónico, se presentan a continuación los términos más importantes en este campo:

- **Código de conducta:** Acuerdo o conjunto de normas no impuestas por disposiciones legales, reglamentarias o administrativas de un Estado miembro, en el que se define el comportamiento de aquellos comerciantes que se comprometen a cumplir el código en relación con una o más prácticas comerciales o sectores económicos concretos (art. 2.f Directiva 2005/29/CE).

- **Comerciante:** Cualquier persona física o jurídica que, en las prácticas comerciales contempladas por la presente Directiva, actúe con un propósito relacionado con su actividad económica, negocio, oficio o profesión, así como cualquiera que actúe en nombre del comerciante o por cuenta de éste (art. 2.b Directiva 2005/29/CE).

- **Comercio Electrónico:** Intercambio de bienes y servicios, o establecimiento de relaciones jurídicas en el ámbito comercial, realizado a través de las tecnologías de la información y las comunicaciones, habitualmente con el soporte de plataformas y protocolos estandarizados.

- **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 la LCE, 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.

- **Condiciones generales de la contratación:** Cláusulas incorporadas unilateralmente por una de las partes con el fin de que rijan en todos los contratos que suscriba la misma, con independencia de la forma externa de las mismas, y sin perjuicio de que alguna de las cláusulas pueda haber sido negociada individualmente.

- **Consumidor:** Cualquier persona física que actúa con un propósito ajeno a su actividad económica, negocio o profesión (art. 2 e Directiva 2000/31/CE). Personas físicas que, en los contratos a distancia, actúan con un propósito ajeno a su actividad empresarial o profesional. (rt. 5 Ley 22/2007)

- **Consumidor y usuario:** Son consumidores o usuarios las personas físicas o jurídicas que actúan en un ámbito ajeno a una actividad empresarial o profesional (art. 3 R.D. 1/2007). Toda persona física que, en los contratos contemplados en la presente Directiva, actúe con un propósito ajeno a su actividad profesional (art. 2.2 Directiva 97/7/CE). Cualquier persona física que, en las prácticas comerciales contempladas por la presente Directiva, actúe con un propósito ajeno a su actividad económica, negocio, oficio o profesión (art. 2.a Directiva 2005/29/CE).

- **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.

- **Contrato a distancia:** Todo contrato entre un proveedor y un consumidor sobre bienes o servicios celebrado en el marco de un sistema de ventas o de prestación de servicios a distancia organizado por el proveedor que, para dicho contrato, utiliza exclusivamente una o más técnicas de comunicación a distancia hasta la celebración del contrato, incluida la celebración del propio contrato. (art. 2.1 Directiva 97/7/CE).

- **Destinatario del servicio:** Cualquier persona física o jurídica que utilice un servicio de la sociedad de la información por motivos profesionales o de otro tipo y, especialmente, para buscar información o para hacerla accesible (art. 2 d Directiva 2000/31/CE).

- **Prestador de servicios:** Cualquier persona física o jurídica que suministre un servicio de la sociedad de la información (art. 2 b Directiva 2000/31/CE).

- **Proveedor:** Toda persona física o jurídica que, en los contratos contemplados en la presente Directiva, actúe dentro del marco de su actividad profesional (art. 2.3 Directiva 97/7/CE). A efectos de esta norma es proveedor el empresario que suministra o distribuye productos en el mercado, cualquiera que sea el título o contrato en virtud del cual realice dicha distribución. (art. 7 R.D. 1/2007) Toda persona física o jurídica, privada o pública, que, en el marco de sus actividades comerciales o profesionales, presta un servicio financiero a distancia. A los efectos de esta Ley, se considera como proveedores a quienes intervengan por cuenta propia como intermediarios en cualquier fase de la comercialización. (art. 5 Ley 22/2007).

- **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 (aptdo. b) Anexo LCE).

- **Servicios de la sociedad de la información o servicios:** 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.º La contratación de bienes o servicios por vía electrónica.

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

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

4.º El envío de comunicaciones comerciales.

5.º El suministro de información por vía telemática.

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

2.º 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.º 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.º Los servicios de radiodifusión sonora

5.º El teletexto televisivo y otros servicios equivalentes como las guías electrónicas de programas ofrecidas a través de las plataformas televisivas (aptdo. a) Anexo LCE).

2.2.2. Consideraciones iniciales

Tal y como se indica en la página web de la asesoría jurídica de Davara&Davara, estar en Internet resulta hoy una necesidad. La viabilidad jurídica de las empresas y entidades en la red, en lo que se denomina comercio electrónico, pasa por cumplir los requisitos impuestos por la normativa específica y general, máxime teniendo en cuenta la cuantía de las sanciones aplicadas. Dada la importancia de las implicaciones del comercio electrónico en la actualidad, es necesario entender este tipo de negocio y sus muchas clases.

Por comercio electrónico podemos entender tanto la compra de productos o servicios por Internet, como la transferencia electrónica de datos entre operadores de un sector en un mercado, o el intercambio de cantidades o activos entre entidades financieras, o la consulta de información, con fines comerciales, a un determinado servicio, o un sinfín de actividades de similares características realizadas por medios electrónicos; pero, para no perdernos en ambigüedades, entenderemos, en un sentido amplio, que es comercio toda aquella actividad que tenga por objeto o fin realizar una operación comercial, y que es electrónico cuando ese comercio se lleva a cabo utilizando la herramienta electrónica de forma que tenga o pueda tener alguna influencia en la consecución del fin comercial, o en el resultado de la actividad que se está desarrollando.

No se trata solamente de compras por Internet, ya que podemos tratar cualquier tipo de intercambio de información, de entre los que destacamos, por parecer más propios de la contratación electrónica, el tema de las ofertas, sin realizar la transacción, y la publicidad; ofertas para el conocimiento de los productos y publicidad para conocer las novedades del mercado en un ámbito o sector determinado que, incluso, se adapten a los gustos y necesidades de cada consumidor, en una oferta, y conocimiento de los bienes ofertados o anunciados, que se puede considerar dinámica y flexible, de acuerdo

con el diálogo que se establezca entre ofertante, o en su caso, anunciante, y el consumidor.

El comercio electrónico viene impulsado por la extraordinaria expansión de las redes de comunicaciones y, en especial, de Internet como vehículo de transmisión en intercambio de todo tipo de información. Su incorporación dentro del modelo de negocio de Amazon ofrece innumerables ventajas, como la mejora de la eficiencia empresarial, el incremento de las posibilidades de compra de clientes, etc. Sin embargo, la implantación de Internet y las nuevas tecnologías tropieza con algunas incertidumbres jurídicas, que es preciso aclarar con el establecimiento de un marco jurídico adecuado, que genere en todos los actores intervinientes la confianza necesaria para el empleo de este nuevo medio.

Los fundamentos del comercio electrónico vienen recogidos en la **Ley 34/2002 de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico (LSSI)**, más conocida como Ley de Comercio Electrónico[10] (LCE). Esta ley es específica para los servicios de la sociedad de la información, pero, por un lado, el amplio concepto que la propia ley tiene de ellos y, por otro, su carácter subsidiario o necesitado de complemento por parte de la normativa específica que pueda aplicarse en muy distintas áreas (protección de datos, protección de los consumidores, fiscalidad....) conforman un amplio catálogo de normativa, si no dispar, de complicado manejo. Es importante dejar claro que la mera presencia en Internet, sin que tenga por qué realizarse contratación electrónica en sentido estricto, entraña la necesidad de adaptarse a lo especificado en la LCE.

2.2.3. Servicios de la sociedad de la información

La Ley de Comercio Electrónico establece una definición muy amplia, considerando como 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. De esto podemos concluir, en primer lugar, que no es necesario que el servicio sea oneroso para el destinatario, sino que represente un beneficio económico. Por otro lado, debe ser a distancia, es decir, sin la presencia física de los contratantes. En relación al medio, por vía electrónico puede ser a través de Internet u otras redes de

comunicaciones electrónicas. Por último, a petición individual del destinatario debe entenderse realizada mediante la solicitud de un destinatario.

2.2.4. Prestadores de servicios de la sociedad de la información

Son considerados prestadores de servicios de la sociedad de la información aquellas personas físicas o jurídicas, que proporcionan un servicio de la sociedad de la información. Según el artículo 7 de la ley de comercio electrónico, la prestación de servicios de la sociedad de la información no estará sometida a autorización previa:

> **Artículo 7.** *Principio de libre prestación de servicios.*
>
> 1. La prestación de servicios de la sociedad de la información que procedan de un prestador establecido en algún Estado miembro de la Unión Europea o del Espacio Económico Europeo se realizará en régimen de libre prestación de servicios, sin que pueda establecerse ningún tipo de restricciones a los mismos por razones derivadas del ámbito normativo coordinado, excepto en los supuestos previstos en los artículos 3 y 8.

En el caso de Amazon, sí realiza un servicio de la sociedad de la información ya que vende productos a través de su página web, por lo que le supone un beneficio y es una actividad que se realiza a distancia mediante vía electrónica. Por tanto, se le aplicaría esta ley.

La ley señala diferentes ámbitos de aplicación: prestadores de servicios establecidos en España, prestadores de servicios establecidos en otro Estado miembro de la Unión Europea o del Espacio Económico Europeo y Prestadores establecidos en un Estado no perteneciente a la Unión Europea o al Espacio Económico Europeo. Las oficinas centrales de Amazon en Europa están en un país miembro de la Unión Europea (Luxemburgo), pero además posee otra oficina en España. Por otra parte, presta un servicio de comercio electrónico dirigido a España a través de www.amazon.es. por lo que le será de aplicación la ley según el artículo 3:

Artículo 3. *Prestadores de servicios establecidos en otro Estado miembro de la Unión Europea o del Espacio Económico Europeo.*

1. Sin perjuicio de lo dispuesto en los artículos 7.1 y 8, esta Ley se aplicará a los prestadores de servicios de la sociedad de la información establecidos en otro Estado miembro de la Unión Europea o del Espacio Económico Europeo cuando el destinatario de los servicios radique en España y los servicios afecten a las materias siguientes:

a) Derechos de propiedad intelectual o industrial.

b) Emisión de publicidad por instituciones de inversión colectiva.

c) Actividad de seguro directo realizada en régimen de derecho de establecimiento o en régimen de libre prestación de servicios.

d) Obligaciones nacidas de los contratos celebrados por personas físicas que tengan la condición de consumidores.

e) Régimen de elección por las partes contratantes de la legislación aplicable a su contrato.

f) Licitud de las comunicaciones comerciales por correo electrónico u otro medio de comunicación electrónica equivalente no solicitadas.

2. En todo caso, la constitución, transmisión, modificación y extinción de derechos reales sobre bienes inmuebles sitos en España se sujetará a los requisitos formales de validez y eficacia establecidos en el ordenamiento jurídico español.

3. Los prestadores de servicios a los que se refiere el apartado 1 quedarán igualmente sometidos a las normas del ordenamiento jurídico español que regulen las materias señaladas en dicho apartado.

4. No será aplicable lo dispuesto en los apartados anteriores a los supuestos en que, de conformidad con las normas reguladoras de las materias enumeradas en el apartado 1, no fuera de aplicación la ley del país en que resida o esté establecido el destinatario del servicio.

2.2.5. Obligaciones de Amazon como prestador de servicios

Las obligaciones de Amazon como prestador de servicios de la Sociedad de la Información aparecen reguladas en la sección I del capítulo II de la ley 34/2002 de Servicios de la Sociedad de la Información. Amazon posee una página web dinámica contractual, puesto que permite una interacción entre el individuo y la empresa, y además se llega a una contratación de manera electrónica, por lo que aquí se aplicaría una normativa de comercio y de los medios electrónicos.

En primer lugar, Amazon deberá comunicar el nombre o nombres de dominio de Internet que le correspondan al Registro Público en el que conste inscrito para la adquisición de personalidad jurídica o a los solos efectos de publicidad, con el fin de garantizar que los ciudadanos y la Administración Pública le vinculen con su establecimiento físico y su "establecimiento" o localización en la red, cumpliendo el nombre de dominio una función de identificador comercial del prestador de servicios en la red. A estos efectos el es-NIC, como entidad acreditada para el registro del dominio ".es", ha hecho público un modelo de comunicación que Amazon deberá presentar al Registro Mercantil para cumplir con esta obligación.

En segundo lugar, como se trata de una compañía que realiza comercio electrónico, según el artículo 10, está obligada a mostrar en su página web de forma permanente, fácil, directa y gratuita, los siguientes datos:

- ✓ Su nombre o denominación social.
- ✓ Residencia o domicilio, o la dirección de uno de sus establecimientos permanentes en España.
- ✓ Dirección de correo electrónico, teléfono o fax.
- ✓ Otros datos que permitan establecer una comunicación directa y efectiva.
- ✓ Datos de inscripción del nombre de dominio en el Registro en el que conste.
- ✓ Si se somete a autorización administrativa, los datos relativos a la misma y del órgano de supervisión: No aplica
- ✓ Si ejerce una profesión regulada, los datos que se refieran a la misma (art. 10d de la LCE): No aplica
- ✓ Número de identificación fiscal

- ✓ Precio del producto o servicio, indicando si se incluyen o no los impuestos y, en su caso, los gastos de envío.
- ✓ Códigos de conducta a los que esté adheridos, y la manera de consultarlos por vía electrónica. La LCE promueve el uso de instrumentos de autorregulación o códigos de conducta para que se adecuen los diversos preceptos de la Ley a las características específicas de cada sector.

La obligación de proporcionar esta información se considera cumplida si Amazon la incluye en su página de Internet en España. Por ejemplo, se ha comprobado que en la página francesa de Amazon (www.amazon.fr) sí que cumple con estas especificaciones.

2.2.6. Comunicaciones Comerciales

Las comunicaciones comerciales son "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". Las comunicaciones comerciales vienen reguladas por el siguiente artículo:

Artículo 19. *Régimen jurídico*.

1. Las comunicaciones comerciales y las ofertas promocionales se regirán, además de por la presente Ley, por su normativa propia y la vigente en materia comercial y de publicidad.

2. En todo caso, será de aplicación la Ley Orgánica 15/1999,de 13 de diciembre, de Protección de Datos de Carácter Personal, y su normativa de desarrollo, en especial, en lo que se refiere a la obtención de datos personales, la información a los interesados y la creación y mantenimiento de ficheros de datos personales.

Si Amazon envía publicidad por medios electrónicos, la empresa deberá cumplir con del título III de la Ley sobre Comunicaciones Comerciales por vía electrónica (artículos 20 al 22):

- ✓ Las comunicaciones comerciales por vía electrónica deberán ser claramente identificables como tales y el nombre de Amazon también deberá ser claramente identificable. En el caso de que las comunicaciones comerciales tengan lugar a través de correo electrónico u otro medio de comunicación electrónica equivalente incluirán al comienzo del mensaje la palabra «publicidad» o la abreviatura «publi».

- ✓ Deberán quedar perfectamente identificadas y explicadas las ofertas promocionales de Amazon que incluyan descuentos, premios y regalos, y de concursos o juegos promocionales.

- ✓ No se podrán enviar comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hayan sido solicitadas o expresamente autorizadas por los destinatarios de las mismas en la fase de registro de usuario o compra de productos y servicios (siempre que no haya una relación contractual previa).

- ✓ Amazon deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito.

- ✓ Cuando Amazon realice ofertas promocionales, que incluyan descuentos, premios, regalos, concursos o juegos promocionales, previa la correspondiente autorización, se deberá asegurar además, que queden claramente identificados como tales y que las condiciones de acceso y, en su caso, de participación sean fácilmente accesibles y se expresen de forma clara e inequívoca.

- ✓ El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad. A tal efecto, Amazon deberá habilitar algún procedimiento sencillo y gratuito para que los clientes puedan revocar el consentimiento que hubieran prestado. Asimismo, deberán facilitar información accesible por medios electrónicos sobre dichos procedimientos.

2.2.7. Contratación electrónica

Se entiende por comercio toda aquella actividad que tenga por objeto fin realizar una operación comercial, y es electrónico cuando ese comercio se lleva a cabo utilizando la herramienta electrónica de forma que tenga o pueda tener alguna influencia en la consecución del fin comercial, o en el resultado de la actividad que se está realizando. Dejando el concepto de comercio electrónico, y entrando en el de la contratación electrónica, diremos que entendemos por contratación electrónica aquella que se realiza mediante la utilización de algún elemento electrónico cuando éste tiene, o puede tener, una incidencia real y directa sobre la formación de la voluntad o el desarrollo o interpretación futura del acuerdo.

El eje de comercio y contratación electrónica de Amazon es su página web. Como se ha dicho anteriormente, dado que realiza una actividad bidireccional con los clientes que entran en ella, se puede clasificar de tipo dinámica. Además se puede catalogar como de tipo contractual, ya que a través de ella se puede celebrar un contrato por vía electrónica 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 comunicaciones.

Amazon deberá establecer un procedimiento auditable para garantizar que el cliente ha sido informado de las condiciones del contrato.

A la hora de hacer los contratos online, la empresa deberá proporcionar previamente en la página web la siguiente información según el título IV de contratación por vía electrónica:

- ✓ Los distintos trámites que deben seguirse para celebrar el contrato.
- ✓ Si el prestador va a archivar el documento electrónico en que se formalice el contrato y si éste va a ser accesible.
- ✓ Los medios técnicos que pone a su disposición para identificar y corregir errores en la introducción de los datos.
- ✓ La lengua o lenguas en que podrá formalizarse el contrato.
- ✓ Poner a disposición del destinatario las condiciones generales a que, en su caso, deba sujetarse el contrato, de manera que éstas puedan ser almacenadas y reproducidas por el destinatario.

La información posterior que Amazon estará obligada a ofrecer consistirá en confirmar la recepción de la aceptación mediante:

- ✓ Un acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente y en el plazo de 24 horas siguientes a las recepción de la aceptación.
- ✓ Un medio equivalente al utilizado en el procedimiento de contratación, tan pronto como el aceptante lo haya completado siempre que dicha confirmación pueda ser archivada por su destinatario.

2.2.7.1. Validez y eficacia

La celebración de contratos por vía electrónica no necesita la admisión expresa de la utilización de medios electrónicos, ni que las partes acuerden previamente la utilización de medios electrónicos. Los contratos se regirán, además de por la LCE, por lo dispuesto en el Código Civil y en el Código de Comercio, y demás normas específicas en concreto, sin olvidar especialmente, en su caso, las normas de protección de los consumidores.

Es decir, los contratos electrónicos se regirán, además de por la LCE, por lo dispuesto en el Código Civil y en el Código de Comercio y demás normas específicas, en concreto, sin olvidar especialmente, en su caso, las normas de protección de los consumidores.

El soporte electrónico tendrá validez siempre que la ley exija que cualquier contrato se celebre por escrito, y la firma electrónica que acompañe al contrato electrónico tendrá igual o mayor valor que la firma manuscrita que acompañe a un contrato escrito.

2.2.7.2. Prueba

En cuanto a la prueba de celebración de un contrato electrónico, cabe destacar que será admisible en juicio como prueba documental el soporte electrónico en el que se encuentre un contrato celebrado electrónicamente.

Para poder dar validez a estos documentos electrónicos es necesario establecer garantías respecto a la fiabilidad del contenido y a la seguridad de su almacenamiento, de este modo, los sistemas informáticos tendrán que ofrecer unas medidas de seguridad y de control ante el acceso no autorizado, así como garantizar la confidencialidad de la información en los casos en que sea exigible.

Estas medidas, junto con otras más avanzadas como la aplicación de técnicas criptográficas a documentos en soporte electrónico, los hacen más seguros e inaccesibles a su modificación y alteración que documentos en soporte papel.

Para lograr una mayor seguridad en las transacciones electrónicas, se podría pactar que un tercero archive en soporte informático las declaraciones que hubieran tenido lugar por vía electrónica y que integran los contratos electrónicos, consignando la fecha y la hora en que tuvieron lugar. El tercero archivará las declaraciones que hubieran tenido lugar por vía telemática entre las partes por un periodo estipulado no inferior a cinco años.

La intervención de estos terceros para archivar las declaraciones que por vía electrónica hayan tenido lugar entre las partes no podrá alterar ni sustituir las funciones que correspondan a las personas facultadas para dar fe pública.

2.2.7.3. Lugar y momento de la celebración

A efectos de determinar el régimen jurídico aplicable, y considerando que la contratación electrónica ofrece la posibilidad de celebrar contratos a distancia, se hacen necesarias unas reglas que determinen dónde ha de entenderse celebrado el contrato. En este caso, Amazon realizará comercio electrónico con clientes que son personas físicas (modelo B2C) con lo cual se entenderá que el contrato ha sido realizado en el lugar que el consumidor tenga su residencia habitual.

Respecto al momento en que se entienden celebrados los contratos, su importancia radica en que puede determinar el inicio de la producción de sus efectos, esto es el momento en el que las obligaciones de las partes comienzan a ser exigibles y deben ser cumplidas.

Los contratos electrónicos se caracterizan por celebrarse estando las partes contratantes en lugares diferentes. Este hecho resalta la importancia de determinar el momento en que se entiende que el contrato comienza a producir efectos.

La LCE dispone que en los contratos celebrados mediante dispositivos automáticos, hay consentimiento desde que se manifiesta la aceptación, lo que supone que el contrato comienza a producir efectos desde que se acepta.

2.2.7.4. Obligaciones específicas de Amazon como prestador de servicios que realiza contratación electrónica

Amazon deberá poner a disposición del destinatario las condiciones generales a que, en su caso, deba sujetarse el contrato, de manera que éstas puedan ser almacenadas y reproducidas por el destinatario. Deberá indicar la lengua en la que se realice el contrato, en este caso, será en español. En cuanto al plazo de validez de las ofertas o propuestas de contratación que se efectúen por vía electrónica, éstas serán válidas durante el periodo que fije Amazon. Si no se fijara plazo alguno, las ofertas serán válidas durante el tiempo que permanezcan accesibles a los destinatarios. Estos periodos de duración establecidos en la LCE se aplicarán sin prejuicio de lo establecido en la legislación específica.

2.2.7. Protección de los consumidores

La protección de los consumidores en el comercio electrónico puede y debe tener diversas manifestaciones. Sin embargo, en la actualidad, como consecuencia de la contratación y comercio masivos, ha aparecido y se ha asentado una manera de contratar

que adolece de la esencia de la contratación entre iguales, esto es, la negociación. Surge así una manera de contratar que, sobre todo en la esfera privada, sitúa al consumidor fuera de la posición de igualdad entre las partes.

El mecanismo en el que se plasma principalmente esta contratación son las Condiciones Generales de Contratación (CGC) que tienen una gran incidencia en el comercio masivo. Las CGC han sido objeto, desde su aparición, de una gran atención por parte de la doctrina jurídica. En este tipo de contratación entran en conflicto dos bienes jurídicos dignos de protección. Por un lado, está el tráfico mercantil, la libertad de la empresa, la competencia, etc. y, por otro, la libertad real de elección del consumidor, la protección del consumidor ante el desequilibrio entre las partes de la contratación.

2.2.7.1. Condiciones generales de contratación (CGC)

Antes de definir las condiciones generales de la contratación es necesario analizar el concepto de cláusula, ya que no son lo mismo que una condición general. Así, una cláusula es calificada como condición general cuando ha sido redactada unilateralmente por una de las partes de la contratación, de forma que ha sido predispuesta e incorporada a una pluralidad de contratos, sin que en ningún caso ello suponga necesariamente que se trate de una cláusula abusiva.

Sólo será cláusula abusiva aquella cláusula en contra de la buena fe que debe regir la contratación y a la que todo empresario o profesional está sujeto en virtud del Código de Comercio, que con carácter general dispone en su artículo 57 que los contratos de comercio se ejecutarán y cumplirán de buena fe, y resulta de aplicación en especial a la contratación en especial a la contratación efectuada entre aquellos y los consumidores.

La Ley 7/1998, de 13 de abril, de Condiciones Generales de la Contratación (en adelante, LCGC) define las condiciones generales de la contratación como "las cláusulas predispuestas cuya incorporación al contrato sea impuesta por una de las partes" (art. 1), por lo que nos encontramos ante una definición objetiva de condición general, ya que la ley no atiende "a la autoría material de las mismas, de su apariencia

externa, de su extensión y de cualesquiera otras circunstancias, habiendo sido redactadas con la finalidad de ser incorporadas a una pluralidad de contratos".

Las condiciones generales son cláusulas homogéneas redactadas de forma unilateral, sin negociación previa, por el empresario en las que deben ocurrir las siguientes condiciones:

a) Que la condición general forme parte del contrato

b) Que sean reconocidas, o en casos de contratación no escrita exista posibilidad real de ser conocidas,

c) Que hayan sido redactadas de forma transparente, con claridad, concreción y sencillez

d) Cuando se contrata con consumidores, que no sean abusivas.

Amazon cumple con estas condiciones ya que permite realizar compras a través de su sitio web, ofreciendo unas condiciones generales de contratación o cláusulas de adhesión. Ya que Amazon está aquí en una situación de privilegio, debe evitar realizar cláusulas abusivas que perjudiquen a los consumidores. Por tanto, las cláusulas de adhesión deben estar a disposición del usuario, y deben indicar los siguientes datos:

- ✓ Precio del producto.
- ✓ Si incluye impuesto o no.
- ✓ Garantías.
- ✓ Plazo de devolución.
- ✓ A quien corresponde pagar los gastos de envío o devolución.

Asimismo, las obligaciones de Amazon en la contratación electrónica deben cumplirse antes y después de haberse producido el contrato en cuestión:

- Deber de información previa
- Deber de confirmación documental

En la página web francesa de Amazon ya se incluyen las condiciones generales de contratación. Tales condiciones se aplican exclusivamente entre la sociedad Amazon

EU S.à.r.l., 5 rue Plaetis, L 2338 Luxemburgo y cualquier persona que visite o hacer una compra a través de www.amazon.fr. La creación de la página web para España debería seguir esas mismas condiciones generales de contratación. Tales condiciones de contratación incluyen los siguientes puntos:

Artículo 2. Contrato

2.1. Condiciones para efectuar un pedido: Usted declara ser mayor de 18 años y tener la capacidad jurídica o sea titular de permiso de los padres lo que le permite realizar un pedido en el sitio. Todos los pedidos realizados en el sitio debe cumplir con las necesidades normales de un hogar.

2.2 Pedido: Después de realizar su pedido, se le enviará un correo electrónico confirmando el mismo. Le informará también del envío de sus artículos. Usted tendrá todavía podrá cambiar su pedido hasta el envío de sus artículos.

Artículo 3. Precio, disponibilidad y entrega

Los precios exhibidos en el sitio están indicados en euros con impuestos franceses incluidos (IVA francés y otros impuestos), con exclusión de los gastos de envío, el coste de procesamiento de su pedido y el coste de la envoltura de regalos. Podemos aceptar sus pedidos dentro de los límites de las existencias disponibles. Le informamos de la disponibilidad de los artículos vendidos en el sitio en la página de información de cada artículo. Si elige pagar con cheque, su pedido será procesado a la recepción del mismo y los retrasos son los de la fecha de recepción del cheque. Si, a pesar de nuestros esfuerzos, los elementos no están disponibles, se lo notificaremos por correo electrónico con prontitud.

(i) En caso de indisponibilidad en el período indicado, nos reservamos el derecho de proponer a reemplazar una sección de una calidad e igual precio. En este caso, el coste de los rendimientos derivados del posible ejercicio del derecho de desistimiento será a costa nuestra. Si no fuera posible ofrecer un artículo de calidad y precio equivalentes o si usted no lo quiere, puede cancelar su solicitud.

(ii) En caso de falta de disponibilidad permanente, y si no le puede proporcionar un artículo de calidad y precio equivalentes, su orden será cancelada automáticamente. Le recordamos que tu tarjeta se carga en el momento del envío de su solicitud. Por lo tanto, si un artículo no está disponible y no hay ningún elemento de repuesto que no se puede entregar, la tarjeta no se le cobrará. A pesar de nuestros mejores esfuerzos, puede haber unos pocos entre los millones de artículos publicados en nuestro sitio que incluyan un error en el precio. Sin embargo llevamos a cabo la verificación de precios durante el proceso de enviar su artículo. Si el precio correcto es inferior al precio que aparece en el sitio, se aplicará el precio más bajo. Si el precio correcto es mayor que el precio que aparece en el sitio, se lo notificaremos y procederá a cancelar su pedido, a menos que usted opta por no aceptar el pedido al nuevo precio.

Si, a pesar de nuestra vigilancia, los elementos no están disponibles, se lo notificaremos por correo electrónico tan pronto como sea posible.

Artículo 4. Deberes

Cualquier pedido realizado en el sitio y entregado fuera de Francia estará sujeto a los impuestos y derechos de aduana que se imponen cuando el paquete llegue a su destino. Estos derechos e impuestos relacionados con la posible entrega de un artículo es su responsabilidad. No tenemos la obligación de verificar y de informarle de los derechos e impuestos. Para conocerlos, le recomendamos que consulte con las autoridades competentes de su país.

Artículo 5: Forma de pago

Usted puede pagar con tarjeta de crédito o cheque. Las tarjetas emitidas por bancos fuera de Francia deberán ser obligatoriamente tarjetas bancarias internacionales. Si paga con tarjeta de crédito, el importe del pedido se cobra en el momento del envío de tus artículos. Pago con cheque sólo se puede comprobar en euros emitidos por un banco domiciliado en Francia o en Mónaco. Al pagar con cheque, por lo que la operación de verificación se lleva a cabo tras la recepción del cheque.

El cheque debe ser pagadero a Amazon de Estados Unidos LLC, y enviados a la siguiente dirección:

Amazon.fr
En ICSB
240, avenue de Rosny
93106 Montreuil Cedex
Francia

Artículo 6: Devoluciones

Gracias por su amabilidad, lea nuestra política de devolución se aplica a los artículos que vendemos. Además de la posibilidad de beneficiarse de los treinta (30) días, de acuerdo con nuestra política de devoluciones, usted tiene el derecho a cancelar siete (7) días previsto por la ley para que podamos devolver la mercancía sin tener que justificar razón. Si la entrega de un bien es no conforme con su pedido o ha sido dañado durante el transporte, consulte nuestra política de devolución. Si aceptamos sustituir un producto dañado o no conforme con su pedido, necesita devolver el producto dentro de 30 días después de la fecha en la que hemos confirmado que se va a sustituir. El incumplimiento de su obligación de devolver el producto dañado o falta de conformidad dentro de esos 30 días, nos reservamos el derecho de cobrar la tarjeta de crédito que utilizó para su solicitud por un importe igual al precio (que se añade al IVA) del producto dañado o no conforme. En este caso, una segunda venta bajo la condición precedente se considerará como si hubiera sido hecha por nosotros. Esta condición se cumplirá si la expiración de los 30 días siguientes a la fecha en la que os hemos enviado un producto de reemplazo, el producto está dañado o no conforme, que no vuelven.

Artículo 7: Reserva de propiedad

La mercancía suministrada será de nuestra propiedad hasta que se envían a la entrega al transportista, una vez que han pagado el precio.

Artículo 8: Garantías y Responsabilidad

Se beneficia de las disposiciones de la garantía legal de vicios ocultos. El audio, video y multimedia pueden ser elegibles para la garantía establecida en los detalles del producto. En caso de avería durante el período de garantía, consulte al servicio del fabricante al cliente. Por nuestra parte, declinamos toda responsabilidad en caso de que el artículo entregado no cumpla con las leyes del país de destino distintos de Francia. Nos comprometemos a brindar todo el cuidado en el uso en la profesión para la aplicación de servicios al cliente. Sin embargo, nuestra responsabilidad no puede ser retenida en caso de incumplimiento de nuestras obligaciones contractuales debido a caso fortuito o fuerza mayor tal como se define por la jurisprudencia de los tribunales franceses. Nuestra responsabilidad no será responsable de cualquier retraso debido a la escasez de valores en el editor o el proveedor. Además, si las diferencias no sustanciales entre el cuadro presentado trabajos en nuestro sitio web, textos e ilustraciones y los puntos del pedido, nuestra responsabilidad no será comprometida.

Empleamos todos los medios a nuestro alcance para asegurar los objetos servicios de estos Términos de uso. Somos responsables de daños directos y previsibles en el momento de uso del sitio o de la celebración del contrato de venta entre nosotros y vosotros. En cualquier caso, no incurrirá en responsabilidad por la pérdida de beneficios comerciales, las pérdidas comerciales, pérdidas de datos o la pérdida de beneficios u otros daños consecuentes o no era previsible en el momento de la utilización del Sitio o la celebración del contrato de venta entre nosotros y vosotros.

La limitación de responsabilidad mencionadas anteriormente no es aplicable en los casos de negligencia grave por nuestra parte, por los daños y responsabilidad civil por productos defectuosos en caso de desalojo y en caso de incumplimiento (incluyendo por vicios ocultos).

Artículo 9: El acceso a la licencia del sitio

Le otorgamos una licencia limitada para acceder y usar el Sitio para su uso personal. En cualquier caso, usted no está autorizado a descargar o modificar total o

parcialmente este sitio sin nuestro consentimiento expreso por escrito. Esta licencia no le permite utilizar bajo ninguna circunstancia, la venta o para cualquier otro uso comercial, este Sitio o su contenido (lista de productos, descripciones, precios, descarga o copia de información en nombre de otro comerciante, con datos, software, clips de sonido, gráficos, imágenes, textos, fotografías, herramientas). Este sitio o cualquier porción de este Sitio no será en ningún caso podrá ser reproducido, copiado, vendido o explotado con fines comerciales sin nuestro permiso expreso por escrito.

No debe utilizar técnicas para copiar una marca, un logotipo u otra información (incluyendo imágenes, textos, modelos), de las que somos propietarios sin nuestro consentimiento expreso por escrito. Usted no debe utilizar ninguna etiqueta meta o cualquier otro "oculto" de texto que contiene nuestro nombre, nuestra marca o la de nuestros afiliados sin nuestro consentimiento expreso por escrito. Cualquier uso no autorizado dará por terminado la licencia que nos han concedido.

Le autorizamos, una licencia no exclusiva, revocable, para crear un hipervínculo a la página principal del sitio siempre dicho vínculo no puede crear o creamos contra empresas de nuestro grupo o de nuestros productos o servicios, una falsa, mendaz, injuriosos o que puedan hacernos daño. En cualquier caso, la creación de este hipervínculo no podrá ejercer nuestra responsabilidad, en cualquier condición sobre el contenido de su sitio. Cualquier uso en su enlace de nuestro logo, nuestra marca o nuestros gráficos sin nuestro consentimiento expreso por escrito.

Artículo 10: Los comentarios, opiniones, comunicaciones y otros contenidos

Los usuarios de este sitio puede responder a las críticas, comentarios u otro contenido; nosotros podemos presentar sugerencias, ideas, preguntas o cualquier otra información cuyo contenido no sea ilegal, obsceno, abusivo, amenazante, injurioso, difamatorio, en violación de los derechos de propiedad intelectual o en detrimento de otros y no es o no contiene virus de software, el activismo político, campañas de publicidad, envío masivo de correo, cadenas o cualquier otra forma de "spam". Usted no debe usar una dirección de correo electrónico falsa, hacerse pasar por otra persona o entidad, o falsificar el origen de contenido. Nos reservamos el derecho, a nuestra única discreción, eliminar o editar cualquier contenido, incluyendo, por razones técnicas

(capacidad de almacenamiento suficiente, los virus, la claridad de la página web) o jurídica (alrededor de un difamatorio, falso, racistas, obsceno o defender los crímenes contra la humanidad). Las razones mencionadas anteriormente son sólo un ejemplo y no deben interpretarse como exhaustivas.

Si usted nos envía el contenido, permite a Amazon la prestación de servicios, usted acepta conceder a empresas de nuestro grupo, el derecho, no exclusivo, término gratis y legal del derecho de autor operar, reproducir, modificar, adaptar, publicar, traducir, distribuir, sublicenciar y mostrar dicho contenido en todo el mundo en todos los medios de comunicación. Usted nos otorga para nuestros afiliados y nuestros licenciatarios el derecho a utilizar el nombre que nos da en la disposición de su contenido. Usted manifiesta y garantiza que posee o tiene los derechos necesarios en el contenido que usted transmita, como la fecha de transmisión de contenidos: (i) el contenido es exacto y veraz, (ii) el uso del contenido no viola no una de nuestras políticas y no infringe a ningún tercero (por ejemplo, el contenido no será difamatorio). Usted se compromete a indemnizar en cualquier acción contra nosotros a terceros, salvo en los casos en que puede ser la posible responsabilidad de Amazon buscado por no quitar el contenido que la ilegalidad habría sido notificada al que esta acción puede provocar que, la base o el origen de contenido que nos ha dado.

Artículo 11: Protección de datos personales

Nos comprometemos a proteger los datos que son personales. Todos los datos personales sobre usted que hemos recogido son tratados con la más estricta confidencialidad, de acuerdo con nuestra política de privacidad. Puede ver nuestra política de protección de sus datos personales.

Artículo 12: Derecho aplicable y jurisdicción

Estas condiciones generales de venta están sujetas a la legislación de Luxemburgo y la Convención de Viena sobre los Contratos de Compraventa Internacional de

Mercaderías. Todos los litigios relativos a la relación comercial entre usted y nosotros están sujetas a la jurisdicción exclusiva de los tribunales de Luxemburgo.

Artículo 13: Identificación

Amazon.fr es una marca comercial utilizada para identificar a EE.UU. y Amazon Amazon Services Europe SARL SARL. Este sitio web (excepto "Marketplace") es propiedad y está operado por la UE Amazon SARL. "Marketplace" está dirigido por Amazon Services Europe SARL.

Para visitar el sitio www.amazon.fr (con exclusión de "Mercado"):
Amazon SARL UE
5 rue Plaetis,
L 2338 Luxemburgo
Registrado en Luxemburgo con el número B-101818
Número de licencia: 104408
Número de IVA: LU 20260743

Para el Mercado:
Amazon Services Europe SARL
5 rue Plaetis,
L 2338 Luxemburgo
Registrado en Luxemburgo con el número B-93815
Número de licencia: 100416
Número de IVA: LU 19647148

El servicio de Amazon MP3 es proporcionado por la empresa Amazon de Estados Unidos Media LLC:
Media Amazon EE.UU. S.à.r.l.
5 rue Plaetis
L 2338 Luxemburgo
Registrado en Luxemburgo con el número B-112767

Número de licencia: 110001

Número de IVA: LU 20944528

Procedimiento de notificación y la obligación de presentar una denuncia por violación de los derechos

Amazon.fr es el nombre comercial de la UE para Amazon Sàrl y Amazon Services Europe SARL. Respondemos con prontitud a los titulares de los derechos de propiedad intelectual que completar y presentar un formulario de notificación (abajo) para comunicar sus preocupaciones acerca de una presunta violación de los derechos. Al recibir un formulario de notificación, podemos adoptar algunas medidas, incluida la retirada de cualquier información o elementos para los que puede haber aceptado la responsabilidad, sin perjuicio de los derechos, acciones o excepciones, todos los cuales están expresamente reservados.

Además, mediante la presentación de un Formulario de Notificación, usted otorga a Amazon.fr y sus afiliados el derecho a usar, reproducir, modificar, adaptar, publicar, traducir, crear trabajos derivados, y divulgar su contenido al mundo y en cualquier medio de comunicación. Esto incluye la transmisión de formulario de notificación a los interesados en la comunicación de contenidos infractores asumido. Usted acepta indemnizar a Amazon.fr y sus afiliados contra todas las reclamaciones presentadas por los contras tercera Amazon.fr o sus afiliados, que surjan de o en conexión con la presentación de un Formulario de Notificación.

En la página web de Amazon se deberá incluir una casilla en la que se acepten las condiciones generales de contratación anteriormente expuestas. Una vez celebrado el contrato, Amazon debe confirmar la contratación efectuada mediante la confirmación de la recepción de la aceptación a través de alguno de los medios que indica la LCE, y que pueden ser el correo electrónico u otro medio de comunicación electrónica equivalente indicado por el consumidor, dentro del plazo de 24 horas, o un medio equivalente al empleado para cumplimentar el procedimiento de contratación. La página web de

Amazon tendrá la obligación de conservar los datos de acceso tales como la IP, una marca de tiempo y cualquier dato relevante del cliente que inicio la contratación electrónica durante un plazo mínimo de un año y máximo de dos.

2.2.8. Pago-e

Los medios de pago en el comercio electrónico constituyen uno de los principales temas de estudio y análisis actualmente. El pago electrónico, entendido éste como cualquier operación tendente a realizar un pago a través de medios electrónico, constituye un pilar fundamental para la consolidación y desarrollo del comercio electrónico, puesto que el pago permite dar cumplimiento a la contraprestación económica surgida como consecuencia de la operación comercial realizada entre las partes.

2.2.8.1. Sistemas de pago-e

Cabe distinguir dos medios de pago en el comercio electrónico. En primer lugar, todos los mecanismos de pago electrónico que están sustentados por un sistema de prepago anterior que los avala, cualquiera que sea la materialización de estos medios de pago electrónico (tarjetas de débito o demás tarjetas de prepago, cheques electrónicos, sistemas electrónicos basados en "cupones" acumulados anteriormente). En este sistema, lo único que se produce es el reemplazamiento de una obligación de un deudor por la obligación de un tercero. También podríamos denominarlos instrumentos de pago electrónico basados en el prepago.

En segundo lugar, están todos los sistemas nuevos de dinero electrónico o dinero de Red. Estos sistemas no se basan en débitos, o incluso créditos, anteriormente fijados que se materializan en transferencias electrónicas posteriores, sino que se trata de la auténtica versión electrónica del dinero corriente. Son instrumentos de pago electrónico basados en un software de prepagado.

Amazon permite hacer compras en su página web utilizando los siguientes sistemas de pago:

- Tarjetas de crédito o débito
- Tarjetas regalo o códigos promocionales
- Amazon.com store card (monedero electrónico)
- Cuentas

2.2.9. Protocolos de seguridad

La seguridad en las transacciones electrónicas es uno de los aspectos que más preocupan en general pero también uno de los que más atención y estudio ha generado, e incluso más avances concretos, pues se deslinda un poco de los temas legislativos, y se centra en las aplicaciones tecnológicas disponibles para garantizar la referida seguridad de las transacciones. Además la utilización de herramientas como la firma electrónica, existen protocolos de seguridad como el SSL y el SET.

SSL o Secure Sockets Layer (Protocolo de Capa de Conexión Segura): es un protocolo de carácter general para conseguir comunicaciones electrónicas seguras. No exige ninguna capacidad específica en el servidor para el comerciante. Se encarga de proporcionar un canal seguro por el que se transmite la información de pago, pero carece de una estructura comercial integrada, pues el comerciante tiene que haber gestionado con la entidad financiera las compras. La facilidad en su implantación ha propiciado su éxito, pero adolece de ciertas deficiencias en cuanto a seguridad, y sobre todo dependiendo de los niveles de encriptación. El SSL no cubre aspectos como el de la relación tripartita en puntos, por lo que los comerciantes se arriesgan a que el número de tarjeta de crédito sea fraudulento y los compradores se arriesgan a que los comerciantes utilicen ilegítimamente su tarjeta. El SSL no hace uso de firmas electrónicas, por lo que la integridad no queda garantizada, y tampoco garantiza el repudio del envío del mensaje. Por todo ello se ha llegado a hablar del SSL como un protocolo de seguridad general, no un protocolo de pago seguro, aunque su utilización es masiva. Su uso es más apropiado para realizar diversas operaciones que impliquen pagos de poco valor.

Por su parte, el **SET o Secure Electronic Transaction (Transacción Electrónica Segura):** es un protocolo transaccional orientado a las aplicaciones de comercio electrónico a través de tarjetas de crédito. A diferencia del SSL, su implantación requiere de unos requisitos tecnológicos específicos, por lo que se encuentra en un número de sitios muy inferior. Éste sí ofrece autentificación de todas las partes implicadas, confidencialidad e integridad, pues descansa sobre una Infraestructura de Clave Pública (PKI: Public Key Infraestructure). Sin embargo, estas ventajas conllevan problemas como son el funcionamiento de los Prestadores de Servicios de Certificación (PSC) que emiten los certificados necesarios o todos los trámites de funcionamiento de estos certificados, creando un conjunto de obstáculos cotidianos a la utilización de los mismos por los usuarios. El SET sí hace uso de firmas electrónicas y garantiza el no repudio al envío entre las partes. Sin embargo, resulta inadecuado para realizar un gran número de transacciones de poco valor.

Según se indica en la página web francesa de Amazon, esta empresa protege los datos de sus clientes durante las transferencias por medio de software SSL (Secure Sockets software Layer) que encripta la información que los clientes introducen antes de enviárnosla. Tras la confirmación de un pedido, nos revelan sólo los últimos cuatro dígitos de su tarjeta de crédito. Por supuesto, transmitimos el número completo de tarjeta de crédito a la tarjeta (de crédito Agrupación de Interés Económico) para procesar la solicitud.

Amazon también mantiene resguardos físicos, electrónicos de almacenamiento y los procedimientos relacionados con la recopilación y divulgación de la información personal de los clientes. Nuestros procedimientos de seguridad nos puede llevar a hacer una prueba de identidad antes de que podamos comunicar sus datos personales.

Es importante protegerse contra el acceso no autorizado a su contraseña ya su ordenador. Si comparte un equipo, debe cerrar la sesión después de cada uso.

2.3. FIRMA ELECTRÓNICA

2.3.1. Conceptos básicos

A continuación se detallan algunos conceptos básicos relativos a la firma electrónica:

- **Algoritmo de cifrado:** función matemática utilizada en combinación con una clave que se aplica a unos datos para garantizar su confidencialidad, integridad y autenticación.

- **Certificación de dispositivos seguros de creación de firma electrónica:** es el procedimiento por el que se comprueba que un dispositivo cumple los requisitos establecidos en esta ley para su consideración como dispositivo seguro de creación de firma (art. 27 Ley 59/2003).

- **Certificación de un prestador de servicios de certificación:** es el procedimiento voluntario por el que una entidad cualificada pública o privada emite una declaración a favor de un prestador de servicios de certificación, que implica un reconocimiento del cumplimiento de requisitos específicos en la prestación de los servicios que se ofrecen al público.

- **Certificado:** documento electrónico por el que se vinculan unos datos de verificación de firma a una persona –signatario- determinada y confirma su identidad.

- **Cifrado:** uso de algoritmos criptográficos para cifrar datos y evitar el acceso de personas no autorizadas al contenido que es objeto de transmisión.

- **Cifrado de clave asimétrica:** aquel en el que se utilizan dos claves, una para cifrar y otra para descifrar los datos a comunicar, la clave denominada pública, para descifrar, será conocida por todo el mundo, y otra privada para cifrar que estará en poder del remitente del mensaje y sólo será conocida por él.

- **Cifrado de clave simétrica:** aquel en el que se utiliza la misma clave para cifrar y para descifrar los datos que se van a comunicar, de forma que ambas partes,

emisor y receptor, deben conocer la clave utilizada teniendo que basar sus relaciones en cuestiones de total y absoluta confianza.

- **DNI electrónico:** es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos.

- **Encriptación:** técnica mediante la que se cifra la información y mensajes de forma que sólo el destinatario autorizado de los mismos pueda leerlos mediante la utilización de la clave o contraseña correspondiente.

- **Firma electrónica:** conjunto de datos en forma electrónica que sirve para identificar el autor del documento en que figuran.

- **Firma electrónica avanzada:** aquella firma electrónica que permite la identificación del signatario y que está vinculada únicamente al mismo de forma que sea detectable cualquier modificación posterior de los datos a los que se refiere.

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

2.3.2. Consideraciones iniciales

La firma electrónica es la traslación al entorno electrónico de lo que la firma manuscrita supone en el mundo que gira en torno al papel, sirviendo así como medio para determinar la autoría de cualquier documento electrónico que pueda ser transmitido a través de las redes de comunicaciones. Se constituye así en una solución tecnológica que permite dotar de seguridad jurídica a las transacciones electrónicas que se producen a través de redes abiertas, y en especial de Internet, fomentado de esta manera la confianza de los diferentes sujetos que pueden intervenir en una operación de comercio electrónico, no ya sólo del consumidor como destinatario final de los bienes y servicios objeto de contratación, sino también del propio prestador de servicios que procede al cobro o a la realización de las operaciones correspondientes (Davara & Davara).

La firma electrónica surge como respuesta a la necesidad de conferir seguridad a las comunicaciones por Internet debido al creciente desarrollo de la sociedad de la información y de las comunicaciones telemáticas. Es un instrumento capaz de permitir una comprobación de la procedencia y de la integridad de los mensajes intercambiados a través de redes de telecomunicaciones, ofreciendo las bases para evitar el repudio, si se adoptan las medidas oportunas basándose en fechas electrónicas.

La firma electrónica forma parte del negocio de Amazon de dos maneras. En primer lugar, los clientes de Amazon emplearán su tarjeta de crédito para realizar las compras. En segundo lugar, Amazon también empleará para gestionar sus relaciones con la administración española un certificado electrónico.

2.3.3. Clases de firma electrónica

El marco jurídico de la firma electrónica se encuentra actualmente constituido en el ordenamiento jurídico español por la Ley 59/2003, de 19 de diciembre, de firma electrónica (LFE), modificada por la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso a la Sociedad de la Información. Según el artículo 3 de esta misma ley se distinguen los siguientes tipos de firmas:

> **Artículo 3.** *Firma electrónica, y documentos firmados electrónicamente***.**
>
> 1. La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.
>
> 2. La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

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

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.

La firma electrónica sólo exige que los datos que la componen, el algoritmo de cifrado, permitan identificar al firmante. Por su parte, la firma electrónica avanzada introduce la necesidad de contar con un par de claves, es decir, tecnología de cifrado asimétrico o infraestructura de clave pública, pues se exige que esté vinculada al firmante de manera única y a los datos a que se refiere y que haya sido creada por medios que el firmante puede mantener bajo su exclusivo control, es decir, está claramente hablando de una clave privada que el firmante nunca hace pública.

La firma electrónica reconocida añade a la firma electrónica avanzada la necesidad de estar basada en un certificado reconocido, y haber sido generada mediante un dispositivo seguro de creación de firma.

2.3.4. Funciones de la firma electrónica

La firma electrónica tiene distintas funciones:

- **Identificación de las partes:** la firma tiene que garantizar que los intervinientes son quienes dicen ser. En todo caso, hay que tener presente que tan solo la firma electrónica avanzada y, en su caso reconocida, va a poder certificar esta característica plenamente.
- **Autenticación del contenido:** el contenido del mensaje tiene que ser el que las partes pusieron, es decir, que se asocia a sus autores, tal como ellos dispusieron.

- **Integridad del contenido:** el mensaje no puede haber sido modificado en el camino. Tiene que poder asegurarse que el contenido del mensaje transmitido no ha sido manipulado. Como simple mención técnica, la conocida función hash (o resumen) es la que garantizaría, al coincidir los resúmenes de emisor y receptor, que dicho mensaje no ha sido manipulado.

- **Confidencialidad:** el contenido debe ser secreto entre las partes.

- **No repudio:** se tiene que poder garantizar que ninguna de las partes puede negar haber enviado o recibido el mensaje. Esta posibilidad resulta de una importancia esencial a efectos de la conclusión y el perfeccionamiento de las relaciones jurídicas así formalizadas.

2.3.5. Validez probatoria de la firma electrónica

Tal y como se describe en el artículo 3, la firma electrónica reconocida tiene el mismo valor respecto a los documentos electrónicos como la firma manuscrita respecto a los datos en papel. Se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado.

El soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio. Si se impugnare la autenticidad de la firma electrónica reconocida con la que se hayan firmado los datos incorporados al documento electrónico se procederá a comprobar que se trata de una firma electrónica avanzada basada en un certificado reconocido, que cumple todos los requisitos y condiciones establecidos en esta Ley para este tipo de certificados, así como que la firma se ha generado mediante un dispositivo seguro de creación de firma electrónica.

2.3.6. Certificados electrónicos

El sistema de emisión de certificados por terceras partes de confianza es la solución técnica que se ha encontrado, a nivel UE y nacional, vinculando estos certificados de forma segura a unos datos de verificación de firma (una clave pública, en el caso de criptografía asimétrica) e indirectamente su correspondiente dato de creación de firma (clave privada) a una persona determinada.

En nuestro caso, Amazon utilizará un certificado que vinculará una clave pública a Amazon. El prestador de servicios de certificación es quien emite el certificado, pero antes llevará a cabo una serie de procedimientos de autenticación para asegurarse que el remitente es quien dice ser, y que la clave pública en el certificado pertenece realmente al remitente. En definitiva, la firma electrónica que autenticará las partes en una transacción, tiene que estar basada en un certificado. Con estos instrumentos, podrá firmar o cifrar documentos electrónicos para que sea posible comprobar su procedencia, integridad, y evitar el repudio.

El certificado es un documento electrónico que puede contener, entre otras, la siguiente información:

1. El nombre común de la empresa.
2. Información identificativa adicional.
3. La clave pública.
4. Fecha de prescripción de la clave pública.
5. Nombre del prestador de servicios de certificación que emite el certificado.
6. Un número de serie exclusivo.

El certificado se cifra con la clave privada del prestador de servicios de certificación, por lo tanto, si los usuarios finales confían en el prestador de servicios de certificación, y tienen su clave pública, pueden estar seguros de la legitimidad del certificado. Si además tenemos un certificado reconocido, éstos pueden incluir gran cantidad de información sobre Amazon en la cual pueden figurar los siguientes datos:

- Indicación de que son certificados reconocidos.
- El código identificativo único del certificado.

- La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.
- La firma electrónica avanzada del prestador de servicios de certificación.
- La identificación de la empresa por su denominación social y su código de identificación fiscal.
- Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.
- El comienzo y el fin del periodo de validez del certificado.
- Los límites de uso del certificado.
- Los límites del valor de las transacciones para las que puede utilizarse el certificado.
- 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.
- En caso de admitir una relación de representación, deberán dar una indicación del documento público que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente, y en caso de ser obligatoria la inscripción, también deberán figurar los datos registrales.

2.3.7. Intervinientes en el proceso de certificación electrónica

En la actualidad, para que pueda utilizarse una firma reconocida es necesaria una infraestructura de clave pública, basada en claves públicas y privadas y en certificados reconocidos por una autoridad de certificación. En este caso, Amazon deberá disponer de un par de claves (pública y privada) y un certificado asociado a su clave pública. Mediante determinadas aplicaciones, podrán firmar documentos, cifrarlos, etc.

Además de los usuarios finales, las otras partes intervinientes en una infraestructura de clave pública son:

- **El prestador de servicios de certificación:** es la encargada de emitir y revocar certificados. Es la entidad de confianza que da legitimidad a la relación de una clave pública con la identidad de un usuario o servicio.

- **La autoridad de registro:** es la responsable de verificar el enlace entre los certificados (concretamente, entre la clave pública del certificado) y la identidad de sus titulares.

- **La autoridad de validación:** es la encargada de comprobar la validez de los certificados digitales.

- **La autoridad de sellado de tiempo:** es la encargada de firmar documentos con la finalidad de probar que existían antes de un determinado instante de tiempo.

- **Los repositorios:** son las estructuras encargadas de almacenar la información relativa a la PKI. Los dos repositorios más importantes son el repositorio de certificados y el repositorio de listas de revocación de certificados. En una lista de revocación de certificados, se incluyen todos aquellos certificados que por algún motivo han dejado de ser válidos antes de la fecha establecida dentro del mismo certificado.

2.3.8. Prestadores de Servicios de Certificación

Un prestador de servicios de certificación es una persona física o jurídica que expide certificados electrónicos o presta otros servicios en relación con la firma electrónica. Es la entidad de confianza que da legitimidad a la relación de una clave pública con la identidad de un usuario o servicio.

Los prestadores de servicios de certificación deberán cumplir con una serie de obligaciones en materia de protección de datos que vienen especificadas en el artículo 17 de la ley 59/2003:

Artículo 17. *Protección de los datos personales.*

1. El tratamiento de los datos personales que precisen los prestadores de servicios de certificación para el desarrollo de su actividad y los órganos administrativos para el ejercicio de las funciones atribuidas por esta ley se sujetará a lo dispuesto en la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en sus normas de desarrollo.

2. Para la expedición de certificados electrónicos al público, los prestadores de servicios de certificación únicamente podrán recabar datos personales directamente de los firmantes o previo consentimiento expreso de éstos. Los datos requeridos serán exclusivamente los necesarios para la expedición y el mantenimiento del certificado electrónico y la prestación de otros servicios en relación con la firma electrónica, no pudiendo tratarse con fines distintos sin el consentimiento expreso del firmante.

3. Los prestadores de servicios de certificación que consignen un seudónimo en el certificado electrónico a solicitud del firmante deberán constatar su verdadera identidad y conservar la documentación que la acredite. Dichos prestadores de servicios de certificación estarán obligados a revelar la identidad de los firmantes cuando lo soliciten los órganos judiciales en el ejercicio de las funciones que tienen atribuidas y en los demás supuestos previstos en el artículo 11.2 de la Ley Orgánica de Protección de Datos de Carácter Personal en que así se requiera.

4. En cualquier caso, los prestadores de servicios de certificación no incluirán en los certificados electrónicos que expidan, los datos a los que se hace referencia en el artículo 7 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.

Asimismo, los prestadores de servicios que expidan certificados electrónicos deberán cumplir con las siguientes obligaciones:

Artículo 18. *Obligaciones de los prestadores de servicios de certificación que expidan certificados electrónicos.*

Los prestadores de servicios de certificación que expidan certificados electrónicos deberán cumplir las siguientes obligaciones:

a) No almacenar ni copiar los datos de creación de firma de la persona a la que hayan prestado sus servicios.

b) Proporcionar al solicitante antes de la expedición del certificado la siguiente información mínima, que deberá transmitirse de forma gratuita, por escrito o por vía electrónica:

1. Las obligaciones del firmante, la forma en que han de custodiarse los datos de creación de firma, el procedimiento que haya de seguirse para comunicar la pérdida o posible utilización indebida de dichos datos y determinados dispositivos de creación y de verificación de firma electrónica que sean compatibles con los datos de firma y con el certificado expedido.

2. Los mecanismos para garantizar la fiabilidad de la firma electrónica de un documento a lo largo del tiempo.

3. El método utilizado por el prestador para comprobar la identidad del firmante u otros datos que figuren en el certificado.

4. Las condiciones precisas de utilización del certificado, sus posibles límites de uso y la forma en que el prestador garantiza su responsabilidad patrimonial.

5. Las certificaciones que haya obtenido, en su caso, el prestador de servicios de certificación y los procedimientos aplicables para la resolución extrajudicial de los conflictos que pudieran surgir por el ejercicio de su actividad.

6. Las demás informaciones contenidas en la declaración de prácticas de certificación. La información citada anteriormente que sea relevante para terceros afectados por los certificados deberá estar disponible a instancia de éstos.

c) Mantener un directorio actualizado de certificados en el que se indicarán los certificados expedidos y si están vigentes o si su vigencia ha sido suspendida o extinguida. La integridad del directorio se protegerá mediante la utilización de los mecanismos de seguridad adecuados.

d) Garantizar la disponibilidad de un servicio de consulta sobre la vigencia de los certificados rápido y seguro.

En función del ámbito de actuación pueden distinguirse entre Prestador de Servicios de Certificación (PSC) públicos y privados. Así la Ley encomienda a la Fábrica Nacional de Moneda y Timbre-Real Casa de la Moneda, la prestación de los servicios de certificación necesarios para garantizar la seguridad, validez y eficacia de la emisión y recepción de comunicaciones y documentos a través de técnicas y medios electrónicos en el ámbito público de relaciones entre la administración pública y los ciudadanos, como de aquellas entre sí. Por tanto, Amazon deberá acudir a este PSC para solicitar su certificado.

2.3.9. Creación de la firma electrónica

La firma electrónica se crea de forma segura mediante un procedimiento de creación estandarizado, definido en el artículo 24 de la Ley 59/2003.

Artículo 24. *Dispositivos de creación de firma electrónica.*

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

2. Un dispositivo de creación de firma es un programa o sistema informático que sirve para aplicar los datos de creación de firma.

3. Un 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.

Amazon deberá crear una firma electrónica reconocida mediante un dispositivo seguro de creación de firma y basada en un certificado reconocido expedido por un prestador de servicios de certificación de confianza.

2.3.10. Verificación de la firma electrónica

Los documentos electrónicos firmados, se pueden verificar mediante dispositivos de verificación de firma electrónica, tal y como describe en el artículo 25 de la Ley 59/2003.

Artículo 25. *Dispositivos de verificación de firma electrónica.*

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

2. Un dispositivo de verificación de firma es un programa o sistema informático que sirve para aplicar los datos de verificación de firma.

3. Los dispositivos de verificación de firma electrónica garantizarán, siempre que sea técnicamente posible, que el proceso de verificación de una firma electrónica satisfaga, al menos, los siguientes requisitos:

a) Que los datos utilizados para verificar la firma correspondan a los datos mostrados a la persona que verifica la firma.

b) Que la firma se verifique de forma fiable y el resultado de esa verificación se presente correctamente.

c) Que la persona que verifica la firma electrónica pueda, en caso necesario, establecer de forma fiable el contenido de los datos firmados y detectar si han sido modificados.

d) Que se muestren correctamente tanto la identidad del firmante o, en su caso, conste claramente la utilización de un seudónimo, como el resultado de la verificación.

e) Que se verifiquen de forma fiable la autenticidad y la validez del certificado electrónico correspondiente.

f) Que pueda detectarse cualquier cambio relativo a su seguridad.

4. Asimismo, los datos referentes a la verificación de la firma, tales como el momento en que ésta se produce o una constatación de la validez del certificado electrónico en ese momento, podrán ser almacenados por la persona que verifica la firma electrónica o por terceros de confianza.

Amazon podrá comprobar la identidad de las personas físicas o jurídicas mediante los dispositivos de verificación de firma electrónica.

2.4. PROPIEDAD INTELECTUAL E INDUSTRIAL

2.4.1. Conceptos básicos

- **Agente de la Propiedad Industrial:** Persona inscrita como tal en el Registro de la Propiedad Industrial que, como profesional liberal, ofrece habitualmente sus servicios para aconsejar, asistir o representar a terceros para la obtención de las diversas modalidades de la Propiedad Industrial y la defensa ante el Registro de la Propiedad Industrial de los derechos derivados de la misma.

- **Autor:** Persona natural que crea alguna obra literaria, artística o científica (art. 5 RD 1/1996)

- **Distribución:** La puesta a disposición del público del original o copias de la obra mediante su venta, alquiler, préstamo o de cualquier otra forma (art. 19.1 RD 1/1996).

- **Divulgación de una obra:** Toda expresión de la misma que, con el consentimiento del autor, la haga accesible por primera vez al público en cualquier forma (art. 4 RD 1/1996).

- **Obra colectiva:** La creada por la iniciativa y bajo la coordinación de una persona natural o jurídica que la edita y divulga bajo su nombre y está constituida por la reunión de aportaciones de diferentes autores cuya contribución personal se funde en una creación única y autónoma, para la cual haya sido concebida sin que sea posible atribuir separadamente a cualquiera de ellos un derecho sobre el conjunto de la obra realizada (art. 8 RD 1/1996).

- **Obra compuesta:** La obra nueva que incorpore una obra preexistente sin la colaboración del autor de esta última, sin perjuicio de los derechos que a éste correspondan y de su necesaria autorización (art. 9.1 RD 1/1996)

- **Obra derivada:** Se entiendo por obra derivada la traducción y adaptación, las revisiones, actualizaciones y anotaciones, los compendios, resúmenes y

extractos, los arreglos musicales o cualesquiera transformaciones de una obra literaria, artística o científica.

- **Obra en colaboración:** Obra que sea resultado unitario de la colaboración de varios autores (art. 7 RD 1/1996).

- **Obra independiente:** La obra que constituya creación autónoma aunque se publique conjuntamente con otras (art. 9.2 RD 1/1996).

- **Organización Mundial de la Propiedad Intelectual (OMPI o WIPO):** Organización sin ánimo de lucro que, en lo relativo a los nombres de dominio, ha realizado una política de resolución de conflictos por medio del arbitraje, ateniéndose a las reglas de la ICANN (UPDR).

- **Programa de ordenador:** Toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación. A los mismos efectos, la expresión programas de ordenador comprenderá también su documentación preparatoria. La documentación técnica y los manuales de uso de un programa gozarán de la misma protección que este Título dispensa a los programas de ordenador (art. 96.1 RD 1/1996).

- **Publicación:** La divulgación que se realice mediante la puesta a disposición del público de un número de ejemplares de la obra que satisfaga razonablemente sus necesidades estimadas de acuerdo con la naturaleza y finalidad de la misma (art. 4 RD 1/1996).

- **Registro:** La entidad a la que se confía la organización, administración y gestión del dominio ".eu", incluido el mantenimiento de las bases de datos correspondientes y los servicios de información al público asociados, el registro de los nombres de dominio, el funcionamiento del Registro de nombres de dominio, la explotación de los servidores de nombres de dominio del Registro del dominio de primer nivel y la difusión de archivos de zona del dominio de primer nivel (art. 2.a Reglamento (CE) nº 733/2002).

2.4.2. Consideraciones iniciales

En la actual sociedad en que vivimos llamada "Sociedad de la Información", los bienes inmateriales han adquirido un gran valor en el ámbito empresarial, al lado o por encima de los bienes materiales. La nueva economía da más valor a los activos inmateriales que a los materiales. La información, el conocimiento, el fondo de comercio y el uso de la tecnología se han convertido en los puntales de la empresa moderna (Davara & Davara).

2.4.3. Bienes inmateriales

Todos los bienes que se encuentran en la sociedad son objeto de protección de un modo u otro, pero al contrario que los bienes materiales cuya protección resulta evidente para todo el mundo, con los bienes inmateriales no ocurre lo mismo. El pensamiento común es que cuando una creación intelectual ha sido puesta a disposición del público, ya pertenece a éste. En este sentido, mediante los derechos de propiedad intelectual e industrial es posible proteger estos bienes y asegurar las inversiones, no sólo creativas sino también económicas.

Entre los activos inmateriales cabe destacar los siguientes:

- **Los nombres de dominio:** Hasta ahora no se les había otorgado el valor que tienen, debido a que su existencia es bastante reciente. Haremos un amplio estudio de los nombres de dominio en el capítulo 2.5.

- **Creaciones del intelecto:** Cada vez tienen un mayor valor por el ahorro de costes que le permiten a la empresa, y por las posibilidades que abren.

En España, estas creaciones se protegen de dos formas:

- **Derechos de propiedad intelectual:** Protegen todas aquellas creaciones del ser humano con un carácter literario, científico o artístico, expresadas en un soporte tangible o intangible, y son de carácter moral o patrimonial.

- **Derechos de propiedad industrial:** Protegen el ejercicio de la actividad empresarial en general, y en particular todo lo que haga referencia a patentes, marcas, identificadores comerciales, etc.

Amazon tiene centros de desarrollo de software por todo el mundo. Aunque una gran parte de ellos está en Seattle, otras localizaciones incluyen Slough y Edinburgh (Reino Unido), Dublin (Irlanda), Bangalore, Chennai y Hyderabad (India), Cape Town (Sudáfrica), Iaşi (Rumanía), Shibuya, Tōkyō (Japón), Beijing (China) y Tempe, Arizona (Estados Unidos). Por tanto, los programas de ordenador que crea deben ser protegidos. Asimismo, deberá proteger los nombres de dominio y las bases de datos, que también son objeto de la propiedad intelectual.

2.4.4. Protección jurídica de los programas de ordenador

Podemos definir los programas de ordenador como toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación. También comprenderá su documentación preparatoria como la documentación técnica y los manuales de uso.

Con los programas de ordenador los derechos de la protección intelectual son fácilmente infringidos, ya que pueden ser fácilmente copiados y distribuidos mediante medios electrónicos, dándose el caso de que la copia puede ser de mayor calidad que el original al haberse realizado con medios tecnológicos más modernos. Los programas de ordenador son producto de una actividad creativa, con una gran carga de intelectualidad y están protegidos en Europa por las leyes de la propiedad intelectual.

Amazon tiene centros de desarrollo de software por todo el mundo y desarrolla diferentes programas de ordenador (aplicaciones para Kindle, Amazon S3 -Simple Storage Service-, Amazon EC2, Amazon web services, Amazon Virtual Private Cloud –VPC-, etc.) Por tanto, el conocimiento de la legislación en cuanto a la protección de su

software es un punto muy importante para la empresa y debe conocerlo a fondo para evitar las infracciones.

2.4.4.1. Objeto de protección de la propiedad intelectual

La propiedad intelectual está recogida en nuestra legislación como un tipo de propiedad especial centrada en el hecho de la intangibilidad del objeto sobre el que se desarrolla. Tal y como viene expuesto en el artículo 96 del Real Decreto Legislativo 1/1996 de 12 de abril, los programas de ordenador que sean propiedad de Amazon serán objeto de la propiedad intelectual, y la persona jurídica que goce de protección será Amazon.

Artículo 96. *Objeto de la protección.*

1. A los efectos de la presente Ley se entenderá por programa de ordenador toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un sistema informático para realizar una función o una tarea o para obtener un resultado determinado, cualquiera que fuere su forma de expresión y fijación.

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

2. El programa de ordenador será protegido únicamente si fuese original, en el sentido de ser una creación intelectual propia de su autor.

3. La protección prevista en la presente Ley se aplicará a cualquier forma de expresión de un programa de ordenador. Asimismo, esta protección se extiende a cualesquiera versiones sucesivas del programa así como a los programas derivados, salvo aquellas creadas con el fin de ocasionar efectos nocivos a un sistema informático.

Cuando los programas de ordenador formen parte de una patente o un modelo de utilidad gozarán, sin perjuicio de lo dispuesto en la presente Ley, de la protección que pudiera corresponderles por aplicación del régimen jurídico de la propiedad industrial.

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

Los derechos de protección que atribuye la legislación de propiedad intelectual se clasifican en dos tipos: derechos personales y derechos patrimoniales. Mientras los derechos personales son irrenunciables, e inalienables, los derechos patrimoniales son susceptibles de transmisibilidad. Se considerará el autor de la obra de propiedad intelectual a quien aparezca como tal en la obra, y gozará de protección de la ley.

2.4.4.2. Tipos de obras

Los tipos de obras, que se pueden aplicar a los programas de ordenador igual que a cualquier otro tipo de creación susceptible de protección como obra del intelecto, son las siguientes:

1. **Obra en colaboración:** Es aquella obra que sea resultado unitario de la colaboración de varios autores. Tiene las siguientes características:

    a. Los derechos de autoría corresponden a todos y cada uno de los autores.

    b. Para divulgar la obra así como para modificarla se necesita el consentimiento de todos los coautores.
    c. Una vez divulgada la obra, ningún coautor puede rehusar su consentimiento para su explotación en la forma en que se divulgó, salgo que lo haga de forma justificada.

d. Los coautores pueden explotar sus aportaciones de forma separada, salvo que causen prejuicio a la explotación común.
e. El hecho de haber realizado la obra en colaboración no supone que los derechos de la propiedad intelectual corresponden a los autores siempre en proporciones iguales, sino en la proporción que ellos mismos determinen.

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

3. **Obra compuesta:** Será la obra nueva que incorpore una obra preexistente sin la colaboración del autor de esta última, sin prejuicio de los derechos que a éste correspondan y de su necesaria autorización.

4. **Obra independiente:** Será la obra que constituya una creación autónoma, aunque dicha obra se publique conjuntamente con otras

En el caso de Amazon, los programas de ordenador que desarrolle serán de su propiedad. Se trata de obras colectivas ya que aunque la creación, en un principio, se entiende que es de varios autores, que serán los empleados de Amazon, se presume que se ha producido una transmisión desde el inicio de los derechos a Amazon ya que lo edita o divulga bajo su nombre.

La titularidad de los derechos viene expuesta en el artículo 97 del Real Decreto Legislativo.

Artículo 97. Titularidad de los derechos.

1. Será considerado autor del programa de ordenador la persona o grupo de personas naturales que lo hayan creado, o la persona jurídica que sea contemplada como titular de los derechos de autor en los casos expresamente previstos por esta Ley.

2. Cuando se trate de una obra colectiva tendrá la consideración de autor, salvo pacto en contrario, la persona natural o jurídica que la edite y divulgue bajo su nombre.

3. Los derechos de autor sobre un programa de ordenador que sea resultado unitario de la colaboración entre varios autores serán propiedad común y corresponderán a todos éstos en la proporción que determinen.

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

5. La protección se concederá a todas las personas naturales y jurídicas que cumplan los requisitos establecidos en esta Ley para la protección de los derechos de autor.

2.4.4.3. Ventajas de la protección de los programas de ordenador mediante los derechos de autor

Que el software es producto de una actividad creativa, con una gran carga de intelectualidad es algo que, en principio, nadie discute. También es un hecho la necesidad de implantar ese software en una máquina que permita su funcionamiento y que esa máquina encuentra su protección dentro de los derechos de propiedad industrial (patentes), es algo que tampoco se puede poner en duda. Sin embargo, no existe uniformidad respecto a la protección que se debe otorgar a los programas de ordenador,

y así nos encontramos con lugares (USA o Japón) donde se protegen mediante derechos de propiedad industrial (patentes), y otros (países de la UE) donde se protegen mediante los derechos de propiedad intelectual.

Aquí los programas de ordenador se encuadran bajo la figura jurídica de la propiedad intelectual, y de hecho esta es la fórmula adoptada por la Directiva Europea, y por nuestra vigente Ley de Propiedad Intelectual, sin embargo también podríamos considerar los programas de ordenador como una invención nueva que implique una actividad inventiva y sea susceptible de aplicación industrial con lo que nos inclinaríamos hacia su tratamiento mediante la protección específica de la legislación sobre patentes.

Sin embargo, en Europa, tanto por vía legislativa como jurisprudencial, el software ha sido excluido del ámbito de protección por el camino de las patentes, aceptándose, no obstante, la patentabilidad de un procedimiento completo en el que una parte del mismo sea desarrollada por un programa de ordenador.

La protección de los programas de ordenador bajo el ámbito de los derechos de autor, no siendo idónea, nos da las siguientes ventajas:

- El plazo de protección de los derechos de autor es de 70 años (50 años más largo que el plazo que otorgan las patentes). Sin embargo hay quien argumenta que el plazo de las patentes es suficiente dada la obsolescencia de estos elementos.

- La facilidad de copia de los programas de ordenador es el mayor problema con el que se encuentra un autor, y la protección otorgada mediante los derechos de autor protege bien este extremo, mientras que la protección por patentes tiene menor alcance.

- La protección mediante los derechos de autor no precisa de ningún requisito para surgir, sino que nace en el momento en que una persona crea una obra, por lo que evita trámites que posiblemente se desconocen y permite centrarse en la creación. La protección mediante patentes precisa de su inscripción registral para surtir efecto.

- El titular de los derechos de autor no necesita cumplir con ningún requisito adicional a la propia creación de la obra para encontrarse protegido por los derechos de autor, mientras que para la patentabilidad de un objeto, será necesario cumplir con una serie de requisitos.

2.4.5. Protección jurídica de las bases de datos

En el comercio electrónico es necesaria la utilización de la información para el desarrollo de la actividad, de una manera, además, lo más eficiente posible. Si las empresas consiguen tratar la información de una manera más eficiente que la competencia, tendrá una ventaja sobre ésta. Amazon gestiona muy bien las bases de datos de sus clientes y posee una tecnología muy avanzada, lo que hace posible una venta personalizada de sus productos y una mayor satisfacción de sus consumidores.

Las bases de datos son colecciones de obras, de datos, o de otros elementos independientes, dispuestos de manera sistemática o metódica y accesibles individualmente por medios electrónicos o de otra forma. Una base de datos es un "depósito" común de documentación, útil para diferentes usuarios y distintas aplicaciones, que permite la recuperación de la información adecuada, para la resolución del problema planteado en la consulta.

Todas las bases de datos deben partir de un fondo documental seleccionado, al que se somete a un proceso con objeto de que se pueda recuperar la información orientada a la solución de un problema. La base de datos contiene datos, pero debe contestar con información. Un dato se convierte en información cuando pasa de ser un dato abstracto en un conjunto de documentos que forman una base, a ser una información exacta y puntual que da respuesta, o ayuda a resolver el problema planteado en la consulta del usuario. Puesto que la base de datos está compuesta por un conjunto de documentos, éstos pueden ser objeto de propiedad de un tercero, y éste tener derechos sobre ellos.

Amazon posee diversas bases de datos, con información de clientes, proveedores, productos, etc. Estas bases de datos deberán estar protegidas por las leyes de la propiedad intelectual.

2.4.5.1. Forma de protección de las bases de datos

Las propias bases de datos, es decir, la estructura que contiene información, también se consideran obras de creatividad intelectual, ya que cuentan con una estructura organizada que permite su consulta de una forma rápida y fácil. Las bases de datos se protegen como obras de creatividad intelectual, ya que esta creatividad no se puede poner en duda en dos momentos distintos, tanto en el almacenamiento de información como en la recuperación de información, de acuerdo con la consulta planteada.

La copia o el acceso a las bases de datos se puede hacer a un coste sensiblemente inferior al de su creación y desarrollo, por lo que es preciso que la protección de estos productos sea lo más adecuada posible al bien objeto de protección. De forma análoga a como ocurría con los programas de ordenador, el objeto de protección no es solamente la recopilación de información, sino más bien todo el procedimiento de creación de una base de datos y el resultado del mismo.

Se articula por tanto un doble ámbito de protección, de un lado, el que confiere el derecho de autor, y de otro lado, el derecho "sui generis", como figura jurídica creada de forma específica por la ley 5/1998, de 6 de marzo, al trasponer a nuestro ordenamiento jurídico la directiva 96/9/CE.

El derecho de autor requiere del requisito de originalidad, al igual que con el resto de obras que gozan de la protección conferida por los derechos de propiedad intelectual, en la selección o disposición de sus contenidos, y sin perjuicio de la protección que recaiga sobre éstos, ya que los mismo quedan excluidos de la protección conferida por esta norma remitiéndose, en su caso, a la norma específica que dote de protección a las mismas.

2.4.5.2. El derecho "Sui Generis"

El derecho "sui géneris" es un derecho del autor sobre la base de datos, y requiere del requisito de originalidad, al igual que el resto de obras que gozan de la protección conferida por las leyes de propiedad intelectual. Este derecho tiene por objeto la protección en una base de datos de la inversión sustancial evaluada cualitativa o

cuantitativamente realizada por su fabricante, de cualesquiera medios tales como tiempo, esfuerzo, energía u otros similares, para la obtención, verificación o presentación de su contenido y para prohibir la extracción o reutilización de la totalidad de la misma.

Asimismo, la protección conferida por el derecho "sui generis" también recaería sobre las modificaciones sustanciales posteriores que se produjeran en una base de datos, siempre que las mismas cumplan todos los requisitos para otorgar dicha protección a una base de datos. En consecuencia, el titular del derecho "sui generis", y por tanto beneficiario de la protección concedida por el mismo, no es sino el fabricante de la base de datos.

Este derecho, al igual que en la protección de autor, surge en el mismo momento en que finaliza el proceso de creación de la base de datos, y no con carácter previo al mismo, teniendo una duración de 15 años desde el día 1 de enero del año siguiente en que terminó dicho proceso.

Amazon tendrá que tener en cuenta la duración de los derechos para proteger, tanto sus programas de ordenador, como sus bases de datos.

2.5. NOMBRES DE DOMINIO

2.5.1. Consideraciones iniciales

Los nombres de dominio han pasado de ser un elemento casi desconocido dentro del ámbito del comercio electrónico a convertirse en un elemento básico para la identificación de una entidad en la red. Su evolución ha ido en paralelo con el desarrollo de la propia Internet.

En los orígenes de Internet no existía ningún motivo por el que fuera necesaria la identificación de las partes conectadas a la red mediante un sistema inteligible para todos puesto que el número de ordenadores implicados era muy pequeño. Tras el amplio desarrollo de la red, y la multiplicación de usuarios que accedían a la misma, se hizo necesario identificar a las partes intervinientes de forma inteligible para todos; para ello se ideó el sistema de nombres de dominio.

Al comprobarse que los nombres de dominio habían pasado de ser identificadores de ordenadores a ser identificadores comerciales de las entidades que los poseían, se empezó a comprender el verdadero valor que podían tener y, consecuentemente, comenzaron los conflictos referentes a estos nombres de dominio. Al no influir la localización geográfica del servidor en el que se encuentre alojada la dirección, el hecho de regular los nombres de dominio, en muchos casos, se queda en algo más que una declaración de intenciones.

Además, el hecho de que Internet, así como todas las entidades relacionadas con ella, tuvieran una clara vocación universal, dificultaba el control o la regulación de los nombres de dominio, que, por otra parte, se crearon cada uno con una concepción distinta, pero en la práctica, con una misma utilidad, lo que ha conducido a numerosas controversias producidas por la confusión entre direcciones.

Al no influir la localización geográfica del servidor en el que se encuentre alojada la dirección, el hecho de regular los nombres de dominio, en muchos casos se queda en una declaración de intenciones.

Los conflictos relacionados con los nombres de dominio son cada vez más numerosos, relacionados en la mayoría de los casos, con los derechos de la propiedad industrial, o con los de la propiedad intelectual

2.5.2. Origen de los nombres de dominio

Desde el comienzo de Internet, se crearon las direcciones IP (Internet Protocol), que identificaban a las máquinas de origen y destino de la información, y eran el sistema principal de intercomunicación dentro de Internet. Las direcciones IP están compuestas de 4 números, separadas por puntos, cada uno de ellos en un rango de entre 0 y 255, por lo que podríamos considerar que las direcciones de los ordenadores en este momento actuaban en forma similar a como lo hacían los números de teléfono.

Se desarrolló entonces lo que se denominó sistema de nombres de dominio, conocido popularmente como DNS (Domain Name System), que era un sistema que identificaba esas direcciones IP con unos términos que fueran comprensibles por las personas, y mucho más versátiles. Técnicamente, el sistema de nombres de dominio de Internet se apoya en una gran base de datos distribuida jerárquicamente por toda la red. Existen múltiples servidores que interactúan entre sí, para encontrar relación inequívoca de un nombre con una dirección numérica con la que poder efectuar la conversión deseada.

Este sistema de nombres de dominio divide la carga de gestión de un administrador central, repartiéndola entre distintos subadministradores, que a su vez pueden repetir el proceso si la dimensión del dominio así lo aconseja. De esta forma se pueden crear distintos niveles de dominios delegados, en los que cada administrador asigna nombres unívocos a su nivel.

El gran crecimiento del número de máquinas conectadas, y la expansión comercial que han visto las empresas en este nuevo medio de comunicación, provocaron el desarrollo de este sistema de nombres de dominio.

2.5.3. Clases de nombres de dominio

Los nombres de dominio se agrupan de la siguiente forma:

1. **Nombres de dominio de primer nivel:** lo constituyen un grupo de letras desde el final del nombre hasta el primer punto (se encuentran, en la escala de Internet, en el nivel más alto de la jerarquía)

    - **Genéricos (generic Top Level Domain, gTLD):** Pueden ser registrados por todo tipo de personas físicas y jurídicas de cualquier parte del mundo sin requerimientos especiales. Este tipo de dominios son económicos y de registro muy rápido. Ejemplos: .com, .net, .org, .edu

    - **Geográficos o de código de país (country-code Top Level Domain, ccTLD):** son los dominios mantenidos por cada país. Estos dominios territoriales son utilizados por las organizaciones y empresas que desean establecerse en Internet y proteger la identidad de su marca o su nombre comercial en un país concreto. Los dominios territoriales tienen sus terminaciones compuestas por 2 letras. Ejemplos. .es (España), .ie (Irlanda), .ar (Argentina), .in (India)

    - **Código Europeo:** el Parlamento Europeo y el Consejo han aprobado un Reglamento con fecha 22 de abril de 2002 por el que se regula la aplicación del dominio de primer nivel "eu". La aprobación de este dominio tiene como objetivo principal el de acelerar el comercio electrónico definido en la iniciativa eEurope aprobada por el Consejo europeo en su reunión de los días 23 y 24 de marzo de 2000 en Lisboa. Este dominio debe promover el acceso tanto de las redes como del mercado virtual basado en Internet.

2. **Nombres de dominio de segundo nivel (Second Level Domain, SLD):** es lo que estaría por debajo del dominio de primer nivel, y en este caso

inmediatamente a la izquierda de éste. Son los que habitualmente se equiparan a la marca o al nombre comercial. Estos nombres de dominio son los que las empresas u otras entidades quieren registrar, bajo otro nombre de dominio de primer nivel cualquiera, y es sobre los que realmente se producen los conflictos, por infringir derechos de propiedad intelectual, industrial o algunas normas de derecho de la competencia.

3. **Nombres de dominio de tercer nivel:** el Plan Nacional ha creado los indicativos de "com.es", "nom.es", "org.es", "gob.es" y "edu.es", bajo los que se pueden registrar nombres de dominio de tercer nivel. Estos dominios permitirán a los solicitantes ubicarse en un espacio adecuado a su actividad o al tipo de entidad que constituyan y a los usuarios, distinguir unas de otras de manera intuitiva.

Amazon contará con un nombre de dominio nuevo para operar en España y proteger la identidad de su marca en este país. La dirección será: www.amazon.es. El ".es" es un nombre de dominio de primer nivel de código de país.

2.5.4. Registro de un nombre de dominio

Para indicar los pasos a seguir para registrar un nombre de dominio, se deberán tener en cuenta dos conceptos:

1. El nombre de dominio a registrar será el de segundo nivel, bajo un nombre de dominio de primer nivel determinado.
2. Se deberá diferenciar si el nombre de dominio de primer nivel bajo el que se quiere registrar el de segundo nivel, es un nombre de dominio genérico o territorial.

   En el caso de Amazon, se trata de un nombre de dominio territorial.

2.5.4.1. Registro del dominio bajo ccTLD ".es"

Para registrar el dominio www.amazon.es habrá que acudir a la entidad pública que actualmente está a cargo de la asignación de nombres de dominio de segundo nivel en España que es “Red.es”.

Los nombres de dominio “.es” se pueden dividir en 2 tipos:

- **Nombres de dominio regulares**, son aquellos que se asignan conforme a las reglas establecidas en el plan nacional.
- **Nombres de dominio especiales**, son aquellos dominios de segundo nivel que la entidad pública empresarial Red.es puede asignar sin sujeción a las reglas establecidas en el Plan Nacional siempre que concurra un notable interés público. Red.es podrá someter la utilización del nombre de dominio especial a las condiciones que estime precisas para garantizar el mantenimiento de los requisitos que dieron lugar a su asignación.

Para registrar el dominio habrá que tener en cuenta los siguientes requisitos legales:

El registro de un nombre de dominio bajo ".es" solamente se podrá hacer por correo electrónico, y no se podrá transferir de una organización a otra. El registro del dominio se le otorgará siempre y cuando sea el primero en solicitarlo y cumpla una serie de requisitos establecidos en el Plan Nacional.

Estarán legitimados para adquirir un dominio .es, las personas físicas españolas o extranjeras que residan legalmente en España, las entidades con o sin personalidad jurídica constituidas conforme a la legislación española y las primeras sucursales, debidamente inscritas en el Registro Mercantil, de sociedades extranjeras legalmente constituidas.

Los requisitos establecidos en el Plan Nacional para la asignación de los nombres de dominio de segundo nivel bajo ".es" que se aplican al caso de Amazon son:

- No estar previamente asignado. Es el primer requisito, debe estar libre y no debe haber sido registrado por otro usuario.
- Cumplir las normas de sintaxis.
  - Los únicos caracteres válidos para su construcción serán las letras de los alfabetos de las lenguas españolas, los dígitos (0-9) y el guión.
  - El primero y el último carácter del nombre de dominio no puede ser el guión.
  - Los cuatro primeros caracteres del nombre de dominio no podrán ser "xn—"
  - La longitud mínima para un dominio de segundo nivel será de tres caracteres.
  - La longitud máxima admitida para un dominio de segundo nivel será de 63 caracteres.
- Cumplir las normas de derivación de nombres de dominio.
  - El nombre completo de la organización, tal como aparece en su norma de creación, escritura o documento de constitución o, en su caso, de modificación, sin que sea obligatoria la inclusión de la indicación o abreviatura de su forma social.
  - Un nombre abreviado del nombre completo de la organización que la identifique de forma inequívoca. En ningún caso podrán asignarse nombres abreviados que no se correspondan razonable e intuitivamente con el nombre completo de dicha organización.
  - Uno o varios nombres comerciales o marcas de los que sean titulares o licenciatarios y que se encuentren legalmente registrados en la Oficina Española de Patentes y Marcas o en la Oficina de Armonización del Mercado Interior.
  - A los solos efectos de la concesión de los nombres de dominio, se podrán equiparar a las marcas o nombres comerciales las denominaciones de origen cuando quien solicite su asignación sea su correspondiente Consejo Regulador.
- No estar comprendido dentro de las prohibiciones que se establecen en el Plan Nacional.
  - Coincidir con algún dominio de primer nivel.
  - Componerse exclusivamente de un topónimo o gentilicio.
  - Componerse exclusivamente de un término genérico o de su abreviatura.

- Asociarse de forma pública y notoria a otra organización o marca distintos de los del solicitante.
- Componerse exclusivamente de nombres propios o apellidos salvo que coincidan con la persona física solicitante.

Amazon estará legitimado para adquirir el dominio www.amazon.es al ser una entidad extranjera con personalidad jurídica, legalmente establecida en España. Además cumple con todas las obligaciones anteriores y no se ve afectado por ninguna de las prohibiciones.

Después de comprobar que se cumplen todas las normas que señala el Plan Nacional, el siguiente paso será enviar un Formulario de Solicitud Electrónica (FSE) de asignación de un nombre de dominio, que se puede obtener en la dirección del ES-NIC. El formulario solamente se puede enviar por medio de correo electrónico, a la dirección domreg@nic.es, incluyéndolo en el cuerpo principal del mensaje, no en un archivo adjunto ni comprimido.

Cuando se haya procesado la solicitud, el resultado positivo o negativo le será comunicado al remitente. Si la solicitud fuera positiva, se enviará por correo postal la factura a la persona de contacto. A la recepción de la factura se debe enviar el formulario de manera que quede constancia de la solicitud con la firma de la persona responsable, y el Justificante de Pago (JP) de abono de las tasas correspondientes.

2.5.5. Derechos de Amazon sobre sus dominios

Amazon tendrá los siguientes derechos sobre sus dominios registrados:

- Derecho a utilizar el nombre de dominio a efectos de direccionamiento en el sistema de nombres de dominio.

  El derecho a la utilización del nombre de dominio estará condicionado al respeto a las normas comunes para la asignación del mismo y al mantenimiento de las condiciones que permitieron su asignación.

Este cumplimiento podrá ser comprobado por la autoridad de asignación de oficio o a instancia de parte, si se mantienen las condiciones que permitieron la asignación de un nombre de dominio instando, en su caso, al beneficiario del nombre de dominio para que subsane los defectos detectados.

El incumplimiento de las condiciones que permitieron la asignación de un nombre de dominio o de las recogidas con carácter general en el apartado decimoséptimo determinará su cancelación por la autoridad de asignación, previa audiencia del interesado.

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

2.5.6. Deberes de Amazon sobre sus dominios

Amazon tendrá los siguientes deberes sobre su nuevo dominio registrado:

1. Facilitar sus datos identificativos siendo responsables de su veracidad y exactitud.
2. Respetar las reglas y condiciones técnicas que pueda establecer la autoridad de asignación para el adecuado funcionamiento del sistema de nombres bajo el ".es".
3. Informar inmediatamente a la autoridad de asignación de todas las modificaciones que se produzcan en los datos asociados al registro del nombre de dominio.

La responsabilidad del uso de un nombre de dominio, así como del respeto a los derechos de propiedad intelectual e industrial, corresponde a la persona u organización para la que se haya registrado dicho nombre de dominio en los términos establecidos en la Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico.

2.5.7. Protección de las marcas famosas y notoriamente conocidas

La protección especial de las marcas famosas y notoriamente conocidas está reconocida en dos tratados multilaterales, que son el Convenio de París para la Protección de la Propiedad Industrial, y el Acuerdo sobre los Aspectos de los Derechos de la Propiedad Intelectual relacionados con el comercio. El convenio de París establece un tipo de protección a las marcas notoriamente conocidas del que podemos extraer las siguientes cuestiones:

1. La protección concedida es una protección contra el registro y el uso de la marca famosa y notoriamente conocida.
2. La protección se aplica únicamente a las marcas de fábrica, y no se extiende a las marcas de servicio.
3. La protección se extiende al registro o uso de productos idénticos o similares.
4. Determinar qué marca es notoriamente conocida dependerá de cada Estado donde se presenta el uso ilegítimo.

En España, respecto a estas marcas famosas y notoriamente conocidas, existe la protección del denominado "riesgo de confusión en el mercado", propiciando que el usuario de una marca anterior notoriamente conocida en España por los sectores interesados pueda reclamar ante los tribunales la anulación de una marca registrada para productos idénticos o similares que pueda crear confusión con la marca notoria.

Los dos requisitos que deben concurrir para que se produzca este riesgo de confusión serán:

1. Identidad de los signos en conflicto.
2. Similitud o identidad de los productos a que se refiere

El primero de los elementos se da con frecuencia, sin embargo el segundo es mucho más difícil que se dé, puesto que la persona que está infringiendo el derecho de marcas puede dedicarse a otra actividad, y utilizar la confusión del nombre de dominio solamente para captar la atención de la gente.

Para evitar este problema se ha acuñado un segundo término de "riesgo de asociación", es decir, ya no se trata tanto de que se confundan los productos, cuanto de que se asocien los productos, con su correspondiente efecto perjudicial para el verdadero propietario de la marca quien ve como una persona ajena se aprovecha de su reputación.

2.5.8. Conflictos entre los nombres de dominio

Los nombres de dominio, desde el momento en que pasaron a ser identificadores comerciales, se convirtieron en objeto de prácticas predatorias por parte de aquellas personas que vieron en ellos una posibilidad de negocio, aunque fuera a costa de vulnerar los derechos de otras partes. Al realizarse estas acciones sobre un elemento de ámbito universal surge la dificultad de la falta de legislación en Internet, y de la falta de un órgano central de autoridad y control de la Red, agravada por tratarse Internet del prototipo de las libertades y de autorregulación del mercado, basado en una política de "first come, first served".

Sin embargo, al aumentar exponencialmente el tráfico de datos a través de la Red, se fue observando la necesidad de regular, de alguna manera, el registro y la utilización de los nombres de dominio. Así surgieron las Normas de Resolución de Conflictos sobre los nombres de dominio para los gTLD y aquellos ccTLD que las hayan aprobado como medio para dirimir sus controversias, y se crean una serie de órganos arbitrales de resolución de estas controversias.

Uno de los casos más comunes es la utilización como propio de un nombre de dominio de una marca ajena, que se encuentre válidamente registrada, bien sea en el mismo país como en otro país distinto. La OMPI (Organización mundial de la propiedad intelectual) propone, para terminar con este problema, un mecanismo de exclusión por el que el titular de una marca famosa o notoriamente conocida pudiera obtener dicha exclusión, que prohibiera a terceros registrar la marca como nombre de dominio.

La exclusión consiste en que la OMPI constituye una presunción probatoria en la que la carga de la prueba recaería sobre el titular del nombre de dominio, respecto a demostrar que tiene interés legítimo en ese nombre.

Los problemas de competencia desleal se pueden observar, con respecto a los nombres de dominio, por cuanto pueden existir empresas que se aprovechen de otras utilizando sus nombres de dominio para hacer competencia desleal. En la legislación española sobre competencia desleal no se configura como requisito para el ejercicio de las acciones que contiene el que las partes en conflicto se encuentren en una situación de competencia.

Así puede ser alegada esta norma en los casos en que un nombre de dominio coincida con un signo distintivo ajeno, aunque los ámbitos de actividad de las empresas no coincidan. Esto querrá decir que igualmente se podrá aplicar cuando los productos o servicios que se oferten sean distintos. Dentro de este punto podríamos considerar, incluso, como un acto de competencia desleal el registro de un nombre que se asocie claramente a servicios que presta otra persona, aunque el nombre de dominio no sea idéntico, y por descontado, podría considerarse competencia desleal el uso de un signo distintivo ajeno como nombre de dominio. Esto será así porque incluso en el primero de los casos, que podría parecer excesivo, se puede generar el riesgo de asociación en el mercado y fundamentar la deslealtad.

Otra práctica prohibida por la legislación sobre marcas sería la explotación de la reputación ajena. Ya no estamos hablando del riesgo de confusión, sino de cerrar las posibilidades de promocionarse en el medio Internet con la marca de que se es titular, lo cual es de especial trascendencia de acuerdo con esta legislación sobre competencia desleal. Todos estos derechos, que se encuentran regulados en otros ámbitos, tienen una gran dificultad en su aplicación en internet, y en el sistema de nombres de dominio en especial, debido a las características de este entorno y su escasa regulación. La falta de control a priori para el registro de nombres de dominio ha producido este efecto nocivo.

La cuestión esencial consiste en determinar si el mero hecho de inscribir un nombre de dominio sin proceder a usarlo efectivamente constituye un uso relevante para el Derecho de la Competencia Desleal. Habría que comprobar el aprovechamiento indebido de la reputación ajena en este caso.

En este sentido podría ser razonable que aun cuando no se vincule el nombre de dominio a determinados productos o servicios, el mero registro del nombre de dominio, con objeto de vendérselo al titular de la marca, constituiría una finalidad lucrativa por parte de quien la registra, por lo que conformaría un uso capaz de generar un aprovechamiento ilícito en el sentido que marca la ley.

Las prácticas predatorias y parasitarias que se han llevado a cabo han aprovechado la falta de conexión entre los fines propios del sistema de nombres de dominio y aquellos propios de los derechos de propiedad industrial o derecho de la competencia. Como ya hemos indicado, la práctica principal la constituye el registro deliberado y de mala fe de un nombre de dominio que coincida con una marca ajena, con la esperanza de revender esos nombres por una cantidad de dinero mayor.

Estas prácticas han llegado a ser tan importantes que se han inventado los términos "cibersquatting" o "warehousing" para describirlas. El "cibersquatting " o ciberocupación lo podríamos entender como el registro deliberado, de mala fe y abusivo de nombres de dominio, y el "warehousing" como la acumulación de una gran cantidad de nombres de dominio de marcas con objeto de una venta posterior.

En el caso de Amazon.es, no se ha detectado ninguna práctica de competencia desleal, en www.whois.org aparecen 1000 nombres de dominio que contienen la palabra "amazon" (ver anexo 4.2.), pero no existe aún www.amazon.es, por lo que no ha habido ningún problema para su reserva. No obstante, a continuación se explica el procedimiento que debería llevar a cabo Amazon para recuperar su nombre de dominio en España, si éste hubiera sido ciberocupado.

2.5.9. Procedimientos de resolución de conflictos con relación a nombres de dominio

A la vista del panorama expuesto respecto a los conflictos entre los nombres de dominio y determinados derechos, y las dificultades de aplicación de las legislaciones nacionales en este ámbito, en la entidad encargada del registro y asignación de nombres

de dominio (ICANN) se decidió promulgar una serie de normas de obligado cumplimiento para todas aquellas personas usuarias de algún gLTD y para aquellos ccTLD que se quisieran adherir a ellas, mientras que en la mayoría de países se dictaban normas de registro y protección de sus propios dominios.

La ICANN aprobó, el 26 de agosto de 1999, una Política Uniforme de Solución de Controversias en materia de nombres de dominio, que podemos encontrar en su página Web en inglés, y una traducción al español en la página Web de la OMPI. Esta política está en vigor y se aplica para la solución de controversias relacionadas con los gTLD, incluso con efectos retroactivos.

Establece las cláusulas y condiciones en relación con una controversia que surja entre la persona que registró un dominio y cualquier otra parte distinta al propio registrador sobre el registro y utilización de un nombre de dominio de Internet registrado por esa persona, y el procedimiento lo establece en el "Reglamento de la Política Uniforme de solución de controversias en materia de nombres de dominio" y el Reglamento Adicional del proveedor del servicio de solución de controversias administrativas seleccionado.

Las fases en las que se divide el procedimiento son las siguientes:

- **Iniciación del procedimiento**

  Cualquier persona o entidad podrá iniciar un procedimiento administrativo presentando una demanda a cualquier proveedor aprobado por la ICANN de conformidad con la política y el Reglamento. Se deberá presentar de manera electrónica, y se deberán efectuar las solicitudes y especificar la forma preferida para efectuar las comunicaciones al demandante. El demandado estará obligado a someterse a un procedimiento administrativo en caso de que un tercero sostenga ante el proveedor competente, en cumplimiento del Reglamento, que:

  a. El demandado posee un nombre de dominio idéntico o similar hasta el punto de crear confusión con respecto a una marca de productos o de servicios sobre la que el demandante tiene derechos.

b. El demandado no tiene derechos o intereses legítimos respecto del nombre de dominio. El demandado posee un nombre de dominio que ha sido registrado y se utiliza de mala fe.

- **Legislación adicional**

Si las dos partes son del mismo país se podrán aplicar por parte del árbitro normas del país en cuestión para dirimir la controversia.

- **Pruebas**

La carga de la prueba estará siempre del lado del demandante, que será quien tenga de demostrar los aspectos antes mencionados.

Los tres aspectos señalados en la iniciación se deberán demostrar por parte del demandante, de manera independiente, y todos ellos. Si el demandante no es capaz de probar uno solo de ellos, el nombre de dominio seguirá siendo utilizado por el demandado. Con objeto de facilitar la solución de la controversia, las UDRP indican una serie de factores que servirían para demostrar o no el derecho del demandante a la utilización del nombre, y la mala fe del mismo en el momento del registro o de la utilización del nombre de dominio.

- **Pruebas del registro y utilización de mala fe**

Las circunstancias siguientes, entre otras, constituirán la prueba del registro y utilización de mala fe de un nombre de dominio, en caso de que el grupo de expertos constate que se hallan presentes.

a. Circunstancias que indiquen que el demandado ha registrado o adquirido el nombre de dominio fundamentalmente con el fin de vender, alquilar o ceder de otra manera el registro del nombre de dominio al demandante que es el titular de la marca de productos o

de servicios o a un competidor de ese demandante, por un valor cierto que supera los costos diversos documentados que están relacionados directamente con el nombre de dominio.

b. El demandado ha registrado el nombre de dominio a fin de impedir que el titular de la marca de productos o de servicios refleje la marca en un nombre de dominio correspondiente, siempre y cuando usted haya desarrollado una conducta de esa índole.

c. El demandado ha registrado el nombre de dominio fundamentalmente con el fin de perturbar la actividad comercial de un competidor.

d. Al utilizar el nombre de dominio, el demandado ha intentado de manera intencionada atraer con ánimo de lucro, usuarios de internet a su sitio Web o a cualquier otro sitio en línea, creando la posibilidad de que exista confusión con la marca del demandante en cuanto a la fuente, patrocinio, afiliación o promoción de su sitio Web o de su sitio en línea o de un producto o servicio que figure en su sitio Web en su sitio en línea.

Por lo tanto, si se da alguna de estas condiciones, sólo una de ellas es suficiente, se entenderá que ha existido mala fe por parte de la persona que registró el nombre de dominio.

La mala fe, sin embargo, la deberemos demostrar en dos momentos, en el momento del registro del nombre de dominio, y en el momento de la utilización de ese nombre de dominio.

- **Cómo demostrar sus derechos y sus legítimos intereses sobre el nombre de dominio al responder una demanda**

El demandado podrá probar su interés legítimo sobre el nombre de dominio objeto de controversia de alguna de las siguientes maneras:

a. Antes de haber recibido cualquier aviso de la controversia, el demandado ha utilizado el nombre de dominio, o ha efectuado preparativos demostrables para su utilización, o un nombre correspondiente al nombre de dominio en relación con una oferta de buena fe de productos o servicios.

b. El demandado ha sido conocido corrientemente por el nombre de dominio, aun cuando no haya adquirido derechos de marcas de productos o de servicios.

c. El demandado hace un uso legítimo y leal o no comercial del nombre de dominio, sin intención de desviar a los consumidores de manera equívoca o de empañar el buen nombre de la marca de productos o de servicios en cuestión con ánimo de lucro.

Con probar uno solo de los aspectos señalados, el demandado demostrará su interés legítimo en el nombre de dominio, y desvirtuará toda posibilidad de traspaso al demandante.

- **Resolución y costas del procedimiento.**

Las costas de procedimiento serán siempre de parte del demandante, y la solución que decida el órgano administrativo no podrá determinar nada en cuanto a las costas, sólo podrá decidir acerca del nombre de dominio:

a. Que siga utilizándolo el demandado, cuando entienda que no se han cumplido los tres puntos antes señalados.

b. Que pase al demandante, cuando entienda que tiene derecho a ello, que el demandado no tiene derecho, y que lo registró y lo utiliza de mala fe.

c. Que se cancele el nombre de dominio, cuando el nombre de dominio pueda resultar ofensivo para el demandante, por lo que él no lo querrá, pero sí querrá que se retire del mercado.

Las únicas costas que pueden ser parte del demandado serán aquellas que hagan referencia a la intención de éste (demandado) de ampliar el número de árbitros a tres, por lo que pagará las costas de diferencia. En la actualidad las costas por iniciar un procedimiento en que se dirima de uno a cinco nombres de dominio en la OMPI son de $1500.

- **Recursos**

  Contra la resolución del órgano administrativo se pueden interponer recursos antes de iniciar el procedimiento administrativo o después de su conclusión.El registrador esperará a conocer si se ha iniciado alguna vía judicial de resolución de esa controversia antes de ejecutar la decisión que haya tomado el panel de expertos.

- **Resumen**

  La persona, física o jurídica, que considere que tiene derecho a un nombre de dominio que haya registrado otra persona podrá interponer una demanda ante uno de los órganos administrativos seleccionados por la ICANN. Sobre el demandante recaerá la carga de la prueba de todos los elementos necesarios para el traspaso de un nombre de dominio.

Tras la demanda y la contestación, el árbitro decidirá acerca de la situación en que debe quedar el nombre de dominio. Las costas serán siempre de parte del demandante, salvo que el demandado solicite la ampliación del Panel de árbitros a tres, en cuyo caso pagará la diferencia. Contra esta resolución administrativa cabe la interposición de recursos ante la jurisdicción ordinaria, que paralizarían la ejecución de

la resolución, o que impedirían la transmisibilidad del nombre de dominio, a fin de facilitar las cosas al órgano juzgador posterior.

Respecto a los dispuesto en la Disposición adicional segunda del Plan Nacional de nombres de dominio, la autoridad de asignación podrá establecer un sistema de resolución extrajudicial de conflictos sobre la utilización de nombes de dominio, incluidos los relacionados con los derechos de propiedad industrial, sin perjuicio de las eventuales acciones judiciales que las partes puedan ejercitar. Sin embargo, si una persona considra que se está utilizando, si derecho a ello, un nombre de dominio que le pertenece , debe interponer un recurso basándose en la infracción de la Ley de Marcas o de las Normas de Competencia Desleal, y reclamando daños y perjuicios. Incluso ha habido algún caso que ha acudido a la vía penal por estafa, pero es algo muy excepcional, y lo habitual es acudir a la vía civil para dirimir las posibles controversias.

2.6. CONTRATACIÓN INFORMÁTICA

2.6.1. Conceptos básicos

A continuación se describen algunos conceptos importantes de esta sección:

Bienes informáticos: todos aquellos elementos que forman el sistema (ordenador) en cuanto al hardware, ya sea la unidad central de proceso o sus periféricos, y todos los equipos que tienen una relación directa de uso con respecto a ellos y que, en su conjunto, conforman el soporte físico del elemento informático, así como los bienes inmateriales que proporcionan las órdenes, datos, procedimientos e instrucciones, en el tratamiento automático de la información y que, en su conjunto, conforman el soporte lógico del elemento informático (software).

Contrato de licencia de uso: un contrato en virtud del cual el titular de los derechos de un programa de ordenador cede su uso a un tercero conservando el cedente la propiedad del software.

Contrato de licencia de uso personalizado: el cliente es normalmente una empresa que adquiere software para sus necesidades concretas y determinadas. Se adapta a las necesidades y lleva anejos servicios de parametrización, formación y mantenimiento.

Contrato Informático: contrato que tiene por objeto bienes o servicios informáticos.

Escrow: contrato de depósito cuyo objeto es el Código Fuente de un programa de ordenador.

Hardware: todo aquello que, físicamente, forme parte del equipo, considerando como tal, también, a los equipos de comunicaciones u otros elementos auxiliares necesarios para el funcionamiento del sistema que se va a implementar.

Hosting: contrato en virtud del cual, un usuario de Internet que no puede o no quiere mantener, por razones técnicas o económicas, su propio servidor, alquila éste a un tercero. Así, el proveedor pone a disposición del cliente un espacio en su disco duro, para que éste pueda almacenar su información.

Housing: contrato en virtud del cual una de las partes se compromete a ubicar en sus instalaciones un determinado Hardware y a prestar al cliente una serie de servicios además del alojamiento del Hardware.

Interfaces: partes del programa que establecen la interconexión e interacción entre los elementos de software y hardware.

Interoperabilidad: la capacidad de los programas de ordenador para intercambiar información y utilizar mutuamente la información así intercambiada.

Leasing: contrato en virtud del cual una parte adquiere un bien a petición de otra para cederle el uso, por tiempo irrevocable y renta periódica a cuyo fin el arrendatario deberá devolverlo o adquirirlo pagando por ello un precio residual.

Licencia de uso: contrato en virtud del cual el titular de los derechos de un programa de ordenador cede su uso a un tercero conservando el cedente la propiedad del software.

Mantenimiento: pacto entre las partes contratantes para asegurar la perfecta utilización del bien adquirido, realizar las adaptaciones que sean precisas según las circunstancias e introducir mejoras que se consideren oportunas.

Outsourcing: la cesión de la gestión de los sistemas de información de una entidad a un tercero que, especializado en esta área, se integra en la toma de decisiones y desarrollo de las aplicaciones y actividades propias de la referida gestión, con la finalidad de la optimización de los resultados de la misma, al tiempo que permite a la entidad el acceso a nuevas tecnologías y la utilización de recursos especializados de los que no dispone.

2.6.2. Consideraciones iniciales

Por contratación informática entendemos la contratación de bienes o servicios informáticos, y bajo el nombre de "contratación por medios electrónicos e informáticos" a la contratación que, sea cual fuere el objeto, se realice por medio de ordenadores, elementos informáticos o cualquier otro electrónico, incluso unido a las comunicaciones

en la conocida telemática. No debe confundirse con la contratación por medios electrónicos cuyo objeto no tiene porqué ser informático.

Los contratos informáticos, sin perjuicio de su propio concepto, son contratos y como tales su primera definición deriva del artículo 1254 del Código Civil, en adelante Cc, que indica que "El contrato existe desde que una o varias personas consienten en obligarse respecto de otra u otras, a dar alguna cosa o prestar algún servicio".

La contratación informática es un negocio jurídico de suma importancia hoy en día. Sin embargo, y debido, en gran parte, al desconocimiento de los usuarios de las posibilidades y límites de la informática, este negocio no se puede basar únicamente, en términos generales, en el principio de la autonomía de la voluntad de los contratantes.

En todo caso, hay que tener presente que los contratos informáticos están formados por elementos dispares que exigen la mezcla o unión de dos o más tipos de contratos para poder configurar sus características.

Amazon vende bienes informáticos, por tanto será la parte que ofrece bienes y servicios informáticos a sus clientes, o que le otorga una situación ventajosa debido a que conoce muy bien las cualidades y limitaciones de sus productos. No obstante, no deberá aprovecharse de esta posición ventajosa, y deberá cubrir fielmente en el contrato informático todos los puntos conflictivos para la seguridad de ambas partes.

2.6.3. Bienes y servicios informáticos

Bienes informáticos son todos aquellos elementos que forman el sistema ordenador en cuanto al hardware, ya sea la unidad central de proceso o sus periféricos, y todos los equipos que tienen una relación directa de uso con respecto a ellos y que, en su conjunto, conforman el soporte físico del elemento informático, así como los bienes inmateriales que proporcionan las órdenes, datos, procedimientos e instrucciones, en el tratamiento automático de la información, y que, en su conjunto conforman el soporte lógico del elemento informático.

Amazon, ofrecerá principalmente los siguientes bienes informáticos de tipo hardware: ordenadores de sobremesa, portátiles, netbooks, monitores, componentes y

accesorios de ordenador, software, juegos de ordenador, impresoras y cartuchos de tinta, productos de oficina, discos duros y otros periféricos y consumibles.

Servicios informáticos son todos aquellos que sirven de apoyo y complemento a la actividad informática, en una relación de afinidad directa con ella. Más concretamente los definiremos como aquellos que tengan por su propia naturaleza, una identidad particular unida al tratamiento automático de la información. En este caso, Amazon no ofrece servicios informáticos.

2.6.4. eAdministración de Amazon

Al hablar de administración electrónica nos estamos refiriendo al uso de técnicas y medios electrónicos, informáticos y telemáticos en el desarrollo de las actividades y procedimientos que competen a Amazon. Uno de los aspectos que aparece detrás del concepto de Administración Electrónica es el cambio de los procedimientos tradicionales en papel a procedimientos electrónicos automatizados.

Los clientes, al interactuar con Amazon electrónicamente, percibirán una mayor transparencia y control sobre el estado de tramitación de cualquier procedimiento por ellos iniciado. Asimismo percibirán, sin duda, una mejora sustancial en la calidad del servicio que les presta. Además habrá otra serie de ventajas entre las que podemos destacar:

- Conocimiento por medios electrónicos del estado de tramitación de los procedimientos con los clientes así como la obtención de copias electrónicas de los documentos electrónicos de dichos procedimientos.
- Conservación en formato electrónico de los datos electrónicos que formen parte del expediente de un cliente.
- Uso del sistema de firma electrónica, o de métodos de identificación electrónicos en las comunicaciones.
- Garantía de seguridad y confidencialidad en los datos que figuran en los ficheros, sistemas y aplicaciones de Amazon.

- Se garantiza el acceso al mismo a todos los ciudadanos, con independencia de sus circunstancias personales, medios o conocimientos. Tan sólo se exigirá un canal telemático que será bien el portal de Amazon o un servicio de atención telefónico.

- Creación de registros electrónicos automáticos que permiten ver el historial completo de interacción del cliente.

- Creación de un perfil electrónico que contenga toda la información relevante del cliente así como entre la que se incluye su historial completo de interacción.

- Pago electrónico a través de tarjetas de crédito, transferencias u otros medios electrónicos.

- Descarga de aplicaciones, soporte técnico etc.

La administración electrónica se realizará a través del portal web, que es la parte de mayor interés para el negocio de Amazon, ya que todas sus ventas se canalizan por esta vía. Los clientes que accedan a dicho portal, se identificarán mediante un usuario y una contraseña que les dará acceso a su perfil desde el cual podrán interactuar con todos los servicios disponibles.

Amazon tiene responsabilidad jurídica sobre todos los trámites hechos a través de su sede electrónica, y esta responsabilidad vendrá recogida en cada uno de los contratos electrónicos como veremos en los siguientes apartados.

2.6.5. Características de los contratos informáticos

Los contratos informáticos carecen de regulación específica en nuestro derecho, son atípicos, por lo que su estudio implica el examen de una diversidad de normas que inciden en los mismos. Este carácter atípico de los contratos informáticos no se salva con la aplicación del principio de la autonomía de la voluntad recogida en el artículo 1255 Cc que indica: “Las partes contratantes pueden establecer los pactos, cláusulas y

condiciones que tengan por conveniente, siempre que no sean contrarios a las leyes, a la moral, ni al orden público". Es necesario tener en cuenta las peculiaridades de la contratación informática y estudiar su régimen jurídico extrayéndolo de una pluralidad de normas.

Las principales características de los contratos informáticos son:

- **Son contratos atípicos:** no tienen una regulación expresa en nuestro Derecho.
- **Su objeto es complejo:** está compuesto, generalmente, por una pluralidad de prestaciones. Esta diversidad proviene en gran medida del carácter ampliamente técnico de los objetos de los contratos informáticos.
- **Las partes contratantes no se encuentran en la misma posición de conocimiento**, lo que puede provocar una inseguridad jurídica. El gran desconocimiento, en términos generales, de la informática por el usuario y la posición dominante del proveedor, en algunos casos grandes multinacionales del sector, hace que el usuario contrate el servicio o el bien informático y no sepa realmente su contenido exacto, todas sus prestaciones, o si la solución ofrecida es la más adecuada para sus necesidades.
- **Necesidad de observar la normativa sobre protección de los consumidores**, y en particular la aplicación del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias. Publicado en el Boletín Oficial del Estado número 287, del 30 de noviembre.

Para poder obviar los problemas que plantean los contratos informáticos, podemos pensar que la contratación de un bien o servicio informático se hace siempre bajo la fórmula del resultado; esto es, mediante un contrato de los denominados de resultado, en el que salvaríamos el desconocimiento del usuario fijando, claramente, el resultado que queremos obtener. Sin embargo, la propia naturaleza de determinados objetos de la contratación informática impide utilizar rígidamente la teoría del resultado. Por otra parte, la aplicación de esta teoría traería la consecuencia de cargar todas las

responsabilidades y riesgos sobre Amazon, lo cual no beneficiaría al proveedor del bien o servicio informático.

Además, hay que tener en cuenta que el tratamiento de un equipo con determinados programas, es, en muchas ocasiones, una tarea dinámica que exige un alto grado de iniciativa e incluso de creatividad por parte del usuario. Por eso es muy probable que se den situaciones en que no se dé un tratamiento adecuado a la información, y se obtengan errores que no se pueden achacar al suministrador ya que el manejo del sistema está en manos de usuario.

2.6.6. Tipos de contratos informáticos

Podemos atender a dos tipos de clasificaciones de contratos informáticos:

Por el objeto, se distinguen los siguientes contratos:

- **Contratos de hardware:** todo aquello que físicamente forme parte del equipo, considerando como tal, también los equipos de comunicaciones u otros elementos auxiliares necesarios para el funcionamiento del sistema que se va a implementar.

- **Contratos de software:** tanto el software de base como de sistema y el de utilidad responden a unas características generales que son las del propio sistema o las de la utilidad a la que sirven y es un producto ya conformado de antemano que no se somete a peticiones del usuario, aunque hay que adecuar el de usuario al de base y utilidad.

- **Contratos de instalación llave en mano:** en los que irán incluidos tanto el software como el hardware, así como servicios de mantenimiento y de formación del usuario.

- **Contratos de servicios auxiliares:** o complementarios, como el mantenimiento de equipos y programas o la formación de personas que van a utilizar la aplicación.

Desde el punto de vista jurídico, Amazon realizará contratos de hardware y de software, pero no de servicios auxiliares (cobertura de asistencia técnica de hardware, servicios de soporte online, etc.).

Por el negocio jurídico, existirán tantos tipos de contratos como negocios jurídicos se realicen sobre este objeto. Algunos de los más utilizados son los siguientes:

- **De venta:** el suministrador, o vendedor en este caso, se obliga a entregar una cosa determinada y la otra parte, el consumidor, a pagar por ella un cierto precio.

- **De arrendamiento financiero:** o leasing, mediante el que se requiere que participen tres partes aunque en dos contratos diferentes, el suministrador del equipo informático, una entidad o intermediario financiero que comprará el bien y el usuario del bien.

- **De alquiler:** el suministrador o dueño se obliga a dar al usuario el goce o uso de un bien informático durante un tiempo determinado y por un cierto precio.

- **De opción a compra:** mediante la cual en cualquier momento se debe conceder la decisión unilateral de la realización unilateral de opción de compra del bien, por un precio determinado.

- **De mantenimiento:** puede ser tanto de equipos como de programas, o incluso, mantenimiento integral en el que se puede incluir un servicio de formación, asesoramiento y consulta.

- **De prestación de servicios:** en el que se incluyen análisis, especificaciones, horas máquina, tiempo compartido, programas, etc. Se da cuando una parte se obliga con la otra a prestarle unos determinados servicios, con independencia del resultado que se obtenga mediante esa prestación.

- **De arrendamiento de obra:** consistente en el compromiso de una parte a ejecutar una obra, y de la otra parte a realizar una contraprestación en pago por la obra realizada.

- **De préstamo:** una parte entrega a otra el bien informático para que use de él durante un tiempo determinado y le devuelva una vez cumplido ese tiempo.

- **De depósito:** desde que una persona recibe una cosa ajena con la obligación de guardarla y restituirla.

2.6.7. Contratos informáticos como contratos de adhesión

Los contratos informáticos, en muchas ocasiones, son contratos de adhesión, en los que una de las partes fija las cláusulas del contrato y la otra parte se adhiere a las mismas, sin tener posibilidad de modificar ninguna de ellas. Por tanto, en este apartado habría que tener en cuenta lo señalado en las Condiciones Generales de Contratación vistas previamente.

Los contratos de adhesión son producto de la contratación en masa que, con frecuencia, violan los derechos de los consumidores de bienes y servicios informáticos por el gran desequilibrio que se produce al faltar la emisión libre de voluntad por una de las partes en la fijación de las cláusulas del contrato.

Este tipo de contratos implican, al menos, un debilitamiento de la autonomía de la voluntad de los contratantes, ya que son contratos en los que existe una voluntad fuerte y predominante de una parte, en contraposición a una voluntad debilitada que se manifiesta por la mera adhesión del usuario. La situación de desequilibrio típica en este tipo de contratos se agrava en el caso de la contratación informática, debido al desconocimiento que el usuario, una de las partes tiene de las técnicas informáticas en general, y de los detalles del funcionamiento e implementación de una determinada máquina con unos determinados programas en particular.

Los contratos que Amazon ofrece a sus clientes son casi en su totalidad contratos de adhesión, ya que las condiciones de contratación están estipuladas y no varían de un producto a otro. Además el hecho de que toda la contratación de bienes informáticos a Amazon se realice por medios electrónicos favorece que el tipo de contratos sea de adhesión, ya que las condiciones de contratación no se pueden negociar a través de dichos medios.

No obstante sí que se ofrecerá al usuario la opción de elegir entre tres tipos distintos de duración del soporte técnico al usuario sobre el producto. Esta opción ofrece una cierta flexibilidad en el contrato pero implica un aumento del precio final del producto, por lo que podemos seguir considerando que los contratos que realiza Amazon son puramente de adhesión. Es necesario decir que, dada la posición ventajosa de la compañía en la realización de los contratos, éste no debe abusar de esta situación, y debe elaborar un contrato lo más beneficioso posible para ambas partes.

2.3.1. Compraventa informática

Este contrato es un contrato tradicional de compraventa con la especialidad de que su objeto es un bien informático de Hardware. La compraventa es "contrato por el que una parte se obliga a entregar una cosa determinada y la otra a pagar por ella un precio cierto, en dinero o signo que lo represente", según se indica en el artículo 1445 del Código Civil.

El vendedor tiene la obligación de entregar la cosa comprada en el estado en que estuviese al perfeccionarse el contrato y la de facilitar al comprador toda la información necesaria para que conozca las posibilidades y utilidades del bien informático adquirido. Esto incluye las obligaciones de prevenir y aconsejar la mejor y más útil adquisición para el comprador.

Por su parte el comprador está obligado a pagar el precio de la cosa vendida en el tiempo y lugar fijados por el contrato y a colaborar con el vendedor debiendo seguir las instrucciones de este último en cuanto a la preparación de los locales, la utilización del bien y los cuidados que precise.

En un contrato de compraventa informática Amazon deberá incluir, entre otras, las siguientes cláusulas contractuales: objeto del contrato, precio, determinar el lugar y la fecha de la entrega del bien, la garantía, obligaciones de las partes, resolución del contrato, resolución de conflictos y reserva del dominio.

2.6.9. Contrato de arrendamiento financiero o leasing informático

Es el contrato mercantil por el que una de las partes, mediante precio determinado, se obliga a adquirir una cosa cierta y ceder su uso a la otra parte, por un período de tiempo y por el pago de unas cuotas tasadas según la amortización del bien. Transcurrido el plazo previsto deberá devolver el bien o, a su elección, comprarlo por un precio adicional que coincidirá con el denominado valor residual.

Las características que tiene este contrato son las siguientes:

1. Incluir necesariamente una opción de compra por el valor residual del bien que previamente se haya pactado.

2. Inscribir el contrato en una sección especial del Registro de bienes de venta a plazos del Registro Mercantil.

3. Tener necesariamente como parte contratante a una empresa de leasing o entidad de crédito y como objeto la cesión de uso de un bien mueble o inmueble con una opción de compra del mismo por un valor residual.

4. Su duración es la pactada por las partes y tiene como regla general la de 2 años para bienes muebles y 10 para bienes inmuebles.

5. Su precio consiste en cuotas compuestas de una parte destinada a la recuperación del bien siempre creciente o constante y otra parte destinada a los intereses.

2.6.10. Contrato de software de aplicación a medida

Se trata del contrato a través del cual se acuerda la realización de un producto de software ajustado a las necesidades del cliente. El producto resultante no es sólo una serie de código realizado en un lenguaje de programación, sino que también incluye sus manuales, las ayudas en línea, el software de apoyo, la documentación de diseño, el código fuente, los planes de prueba, los programas ejecutables, la documentación de estándares seguidos, la propiedad sobre derechos de autor y demás información extra que lo componga.

Estos proyectos conllevan generalmente cuantiosas inversiones y un largo período de formación (de 5 a 10 años) y además implican decisiones estratégicas y tecnológicas ya que las empresas contratantes están en continua evolución. Al ser un programa a medida, está destinado a integrarse en la vida laboral de las personas; debe ser construido pensando en el cumplimiento del trabajo, enfocado en una organización específica, de modo que se tengan en cuenta las reglas del negocio, políticas, procedimientos, misión y visión de la organización para la cual se desarrolla.

2.6.11. Contrato de Licencia de uso

Es un contrato en virtud del cual el titular de los derechos de un programa de ordenador cede su uso a un tercero conservando el cedente la propiedad del software. Con cede una licencia de uso con carácter no exclusivo, intransferible y por tiempo indefinido salvo pacto en contrario.

Los contratos de licencia de usos pueden ser:

1. **No personalizado:** es el software de masas que tienen iguales características y precio para todos.

2. **Personalizado:** el cliente es normalmente una empresa que adquiere software para sus necesidades concretas y determinadas. Se adapta a las necesidades y lleva anejos servicios de parametrización, formación y mantenimiento.

3.

Las licencias por su parte pueden clasificarse en:

1. **Licencia individual:** existe una licencia por cada PC.
2. **Licencia múltiple:** existe una licencia para varios PC.
3. **Licencia cliente servidor:** pueden ser simultáneas o concurrentes.
4. **Licencia Up-grade:** se dan en función de la potencia de la máquina y se cobra en función del rendimiento que se está sacando del software.
5. **Licencia de código abierto u opencode:** se licencia de forma gratuita, es el software libre, tiene una condición y es que el software que se integre sea también libre.
6. **Licencia de estructura cliente servidor:** es la licencia para un programa instalado en un servidor o host, que es utilizado por los ordenadores clientes de red.

2.6.12. Contrato de Escrow o de depósito de código fuente

Es un contrato de depósito cuyo objeto es el código fuente de un programa de ordenador. El artículo 1758 CC dispone que "se constituye depósito desde que uno recibe la cosa ajena con la obligación de guardarla y restituirla". Y por código fuente entendemos el núcleo formal del programa de ordenador que expresa la secuencia de instrucciones u órdenes en lenguaje de programación estructuradas para que se logre el fin deseado.

Consiste en la constitución de un depósito sobre el "know-how" de una empresa en manos de persona distinta a los clientes-licenciatarios de la misma, con el fin de que éstos puedan acceder a dicho "know-how" si se cumplen determinadas circunstancias, expresadas en el propio contrato de Escrow. el contenido de este depósito es el siguiente: el código fuente, el compilador en caso de que sea propietario, el manual de usuario y el código objeto.

Puede constituirse como un contrato independiente o como una cláusula de un contrato de licencia de uso. El contrato de depósito tiene carácter gratuito a menos que

se pacte lo contrario y el "Escrow" es un pacto en este sentido que se caracteriza por ser retribuido. Se pacta una cantidad fija o periódica a favor del depositario. Esta remuneración suele ser repercutida al licenciatario mediante pacto expreso al respecto.

Los objetivos principales de este contrato son:

1. Acceder al código fuente en los supuestos pactados por las partes.
2. Probar la titularidad del programa, porque se deposita en el protocolo del Notario.
3. Probar la preexistencia y originalidad frente a terceros.

2.6.13. Contrato de Outsourcing

Consiste en la cesión de la gestión de los sistemas de información de una entidad a un tercero que, especializado en este área, se integra en la toma de decisiones y desarrollo de las aplicaciones y actividades propias de la referida gestión, con la finalidad de la optimización de los resultados de la misma, al tiempo que permite a la entidad el acceso a nuevas tecnologías y la utilización de recursos especializados de los que no dispone.

Es un contrato que se caracteriza por ser complejo en su elaboración dado que implica una cesión de responsabilidad del que solicita el servicio al que lo presta y por lo tanto será necesaria la delimitación detallada de la asunción de responsabilidad por este último. Su duración es de medio a largo plazo y su alcance puede ser total, de transferencia de toda la gestión de los sistemas de información, o parcial, alcanzando a una parte concreta de esa gestión.

2.6.14. Contratos informáticos en el ámbito de Internet

En la Red son muchos los contratos que van surgiendo para cubrir distintas necesidades que con su uso se van creando. En el entorno de Internet, surge la necesidad

de extremar las medidas de seguridad para que las transacciones que a través de ella se realizan lo san en un entorno seguro. Algunas de las posibilidades de seguridad que se ofrecen son la firma electrónica y los certificados digitales de firma.

Dentro de los contratos de este tipo se encuentran:

1. Contratos de acceso a Internet: por estos contratos se solicita acceso a la Red a cambio de un precio.

2. Contrato de correo electrónico: para poder utilizar este medio de comunicación es necesario darse de alta como usuario de correo electrónico que puede tener por objeto comunicaciones internas dentro de una misma empresa así como con el exterior.

3. Contrato de creación de página web: este contrato de carácter técnico y de diseño busca revestir el alojamiento de un sitio web en la red.

4. Contrato de nombres de dominio: por el que se registra un nombre de dominio y se adquiere derecho a utilizarlo con exclusividad en Internet.

5. Contrato de housing: una de las partes se compromete a ubicar en sus instalaciones un determinado hardware y a prestar al cliente una serie de servicios además del alojamiento del hardware. Es un contrato de servicios de una empresa de tecnología a un cliente permitiéndole alcanzar mayor nivel de competitividad sin necesidad de realizar inversiones en equipamiento tecnológico o en formación del personal informático propio.

6. Contrato de hosting: es aquel contratoo en virtud del cual, un usuario de Internet que no puede mantener, por razones técnicas o económicas, su propio servidor, alquila éste a un tercero. Así, el proveedor pone a disposición del cliente, un espacio en su disco duro, para que éste pueda almacenar su información, normalmente una página o sitio web.

2.6.15. Cláusulas tipo de un contrato informático

A continuación se van a exponer las principales cláusulas tipo que deberemos incluir en todos los contratos de Amazon:

1. **Objeto del contrato:** En muchas ocasiones, el desequilibrio existente y la posición predominante de una de las partes es consecuencia de no haber descrito con claridad el objeto del contrato.

2. **Precio:** Es conveniente hacer constar que el precio no estará sujeto a variaciones de ningún tipo, excepto si se pacta algo en contra expresamente; con esto se logra que quede bien definido en el contrato, sin riesgo de sorpresas, desmenuzándose las diferentes partidas y a qué corresponde cada una de ellas, de manera que no pueda haber algún lugar por donde colarse una variación.

3. **Pago:** Siempre que sea posible, y si no se pacta nada en contra, el precio se pagará después de la aceptación del trabajo o del equipo o servicio contratado y no cuando se efectúe la entrega. Esto no excluye lógicamente, que se pueda pactar cantidades adelantadas a cuenta; pero, la parte fuerte, incluso una de garantía, deberá ser pagada después de la aceptación y del periodo de implementación en el circuito de información del usuario.

4. **Plazos:** El suministrador deberá fijar los plazos de entrega del material y de los programas o de realización de servicios, u obras encargados. Estos plazos no podrán en ningún caso, incidir sobre el resto de cumplimiento de las obligaciones, de forma que, mediante cláusulas de penalización, se forzará el cumplimiento, ya que hay que tener en cuenta que, en este tipo de contratación, todas las partes están tan íntimamente ligadas que un retraso en un plazo puede incidir sobre el resto de la contratación, llegando a poder ser un elemento de fuerza o presión por el daño que cause. Los plazos estarán suficientemente asegurados o garantizados con cláusulas de penalización.

5. **Preparación del local o locales:** Se especificará en su caso, a cargo de quién corre la preparación de los locales, indicando cuáles son éstos y las necesidades de adaptación , así como el plazo, con su correspondiente penalización, en el que se realizarán las adaptaciones y estarán disponibles los locales; para el mejor cumplimiento

de los plazos y obligaciones del contrato, quien corresponda deberá permitir y facilitar el acceso a los locales, en las condiciones y fechas que se establezcan en el contrato.

6. **Entrega en instalación:** Fijar las condiciones de esa entrega e instalación de común acuerdo. Es importante que las partes queden obligadas por contrato a realizar las actividades necesarias o proporcionar los medios para que se pueda llevar a cabo esa entrega a total satisfacción. Por otra parte, si el usuario no proporciona los medios, o no da facilidades para que se realice esta entrega e instalación del equipo, se pueden retrasar los plazos del suministrador, con el consiguiente prejuicio. Es importante, por tanto, que ambas partes fijen sus obligaciones contractualmente, respecto a actividades o medios a proporcionar, para que se realice la entrega y la instalación.

7. **Pruebas de aceptación:** El contrato llevará un anexo en el que, por acuerdo de las partes, se especifiquen las pruebas de aceptación que se deberán realizar para poder considerar que el sistema y los programas cumplen con los requisitos y especificaciones que se han contratado. Estas pruebas tendrán que ser satisfactorias respecto al tratamiento de la información y al resultado, en su caso, que se había especificado como objeto de la contratación.

8. **Retención en precio como garantía:** Es conveniente pactar una retención de una parte del precio, durante tiempo, con aval o garantía suficiente. Esto permitirá entrar en un periodo de prueba y rodaje de los programas, su implementación con el sistema y con el circuito de información del usuario.

9. **Repuestos:** Se deberá fijar un tiempo mínimo, que será suficiente con 10 años debido a la práctica comercial al uso, durante el que el usuario tendrá, sujeto a penalizaciones y responsabilidades del suministrador, los repuestos del equipo.

10. **Mantenimiento:** Deberá existir un compromiso de tiempo en el que el suministrador garantizará prestar ese mantenimiento. Este periodo de tiempo deberá ser de al menos 10 años.

11. **Software:** Debido a la existencia de la figura jurídica de los derechos de autor, en caso de estar incluido en la contratación, será necesario especificar, además de a quien corresponden todos los derechos patrimoniales de los programas especificados y

contratados, los plazos de entrega, su implementación en el sistema, así como las responsabilidades de compatibilidad.

12. Compatibilidad: Se debe fijar en el clausulado la adecuación operativa del sistema con el software, tanto de base como de utilidad y de usuario. Además, el software y los equipos, deben compatibilizarse con las interfaces y con otros equipos y programas que disponga el usuario y con los que deba trabajar; para lograr esto debe especificarse en el contrato cuales serán esos equipos y programas y desarrollar una cláusula al respecto para que se obligue al cumplimiento de su compatibilización. Los manuales y la documentación deben estar orientados en un doble sentido; de una parte, los manuales deben ser suficientes para cumplir con las necesidades de manejo y operativa del equipo y de los programas, además de estar confeccionados de forma que permitan realizar un mantenimiento preventivo. De otra parte, los manuales y la documentación deben proporcionar información para que el usuario pueda reaccionar ante situaciones anómalas; para que pueda ser autosuficiente, tanto en los errores como en los fallos del sistema.

13. Entrenamiento y soporte del sistema: La formación del personal del usuario, en número razonable para que se ejerciten y puedan llevar a cabo las actividades propias del funcionamiento y del mantenimiento de los equipos y de los programas, es cláusula normal a introducir en este tipo de contratos. Esta formación, suficiente en calidad y cantidad para el buen uso y óptimo manejo del sistema, debe ser controlada sin coste adicional alguno. Es conveniente fijar en el contrato unas obligaciones del suministrador, respecto a los cursos necesarios al personal del usuario, para que se pueda operar el sistema, en condiciones óptimas de trabajo, desde que se haya realizado la entrega. También es frecuente introducir en el contrato una cláusula en la que el suministrador se comprometa, con o sin coste adicional, a proporcionar un sistema de apoyo y reciclaje en la formación para el personal del usuario. Todo ello deberá quedar claramente especificado en el contrato con indicación de personas, cualificaciones y coste, así como plazos y condiciones, en su caso de la formación, respecto a horarios y lugar.

14. Periodo contractual de garantía: Independientemente de la garantía normal de cualquier tipo de producto, esta contratación exige una garantía complementaria que

incluya, además de los equipos, los programas y la implementación de ambas cosas en el circuito de información del usuario. Esto es, al tener que integrar este producto en una forma de trabajo y tratamiento de la información, es posible que no se puedan comprobar todas las situaciones de tratamiento que garanticen el buen funcionamiento del sistema. Es por ello que el suministrador estará obligado a garantizar durante un tiempo mínimo, que deberá ser por lo menos 18 meses, la integración de equipos y programas en el tratamiento de la información previsto. Este tiempo es suficiente para que se hayan podido dar ya todas las circunstancias por las que debe pasar y funcionar el sistema. Si durante el mismo se detectara una anomalía en el funcionamiento, o que el programa y equipos no reaccionan de una forma determinada ante una circunstancia o evento que se produzca, el suministrador, sin coste alguno adicional, deberá adaptar el programa o los equipos al modo de trabajo que garantice el tratamiento correcto de la información. En el caso de que se detecte un error mediante el que el sistema esté sin funcionar, o provoque una situación de no tratamiento adecuado de la información, durante un tiempo determinado, y haya que adaptar equipos y programas para poder volverlo a poner en marcha, la garantía comenzará a correr por el tiempo pactado completo, nuevamente y a partir de que se dé esa circunstancia.

15. Transmisión de derechos: La transmisión de cualquier derecho sobre el contrato (cesión, subarriendo u otro) o sobre alguna parte del mismo, ya sea de propiedad intelectual o industrial, deberán quedar sometidos mediante acuerdo contractual, al consentimiento de la otra parte, de forma que, a no ser que exista consentimiento expreso y escrito, ninguna de las partes podrá ceder los derechos del contrato, ni sobre una parte del mismo, a ninguna otra persona, de ninguna forma. Esto incluye a los derechos que correspondan al suministrador y al usuario conjuntamente sobre el producto final. Todo ello salvo los derechos que, de forma individual puedan corresponder a suministrador, usuario o a un tercero sobre los programas o equipos que se contratan.

16. Propiedad: Deberán quedar claros los derechos de propiedad que, sobre el equipo o sobre los programas, queden al perfeccionarse el contrato o, en su caso, con el pago total de la cantidad pactada. Para ello, se especificará en la cláusula correspondiente a quien corresponderá la propiedad del equipo, o de cada una de las partes, y de los programas, o, en su caso, el régimen jurídico por el cual se legitima al usuario para poder utilizarlos en régimen de arrendamiento, cesión de uso o cualquier

otro, especificando de quién es la propiedad en estos casos y los correspondientes derechos de autor.

17. Seguro: En este tipo de contrato se deben fijar dos tipos de seguros. Uno de ellos es el de la pérdida, deterioro o cualquier otro daño que sea asegurable y que afecte patrimonialmente a equipos y programas. Este seguro pasará por tres fases: la primera fase, respecto al periodo que va desde la contratación hasta la aceptación definitiva, en que la responsabilidad por los daños que se puedan causar a los equipos o programas objeto del contrato serán de único riesgo del suministrador. En la cantidad en que éste considere que se van realizando los adelantos hacia la entrega definitiva, deberá tener cubierto un seguro en beneficio de ambos, ya que, aunque se pacte que el suministrador corra con toda la responsabilidad mientras no exista aceptación definitiva, el daño que se puede causar al usuario, representa un perjuicio patrimonial importante y habrá que considerarlo. En una segunda fase, realizada ya la aceptación definitiva, el suministrador pactará con el usuario que éste corra con un seguro, al menos por la cantidad que quedará aplazada o pendiente de cobrar por la causa que fuere. Los riesgos en este caso del daño o deterioro del bien informático contratado correrán a cargo del usuario pero el suministrador tiene que tener cubierto su riesgo y, por ello, la necesidad del seguro. En una tercera fase, se realizará un seguro ya solamente a favor del usuario que así cubrirá el posible daño que por causas no determinadas puedan sufrir los bienes informáticos contratados en el caso de que sean todos de su propiedad. En el caso de que alguno de ellos esté arrendado, o de cualquier otra forma en la que la propiedad no sea del usuario, el seguro se realizará poniendo como beneficiario a la persona perjudicada por la pérdida o deterioro del equipo.La otra clase de seguro es de mantenimiento de equipos y programas, que garantice la adaptación, arreglo y atención a cualquier tipo de eventualidad que pueda ocasionarse. En este seguro nos referimos principalmente, a adaptaciones por errores o fallos de programas en el caso de producirse después de la aceptación definitiva y sin estar contemplados en la relación contractual.

18. Confidencialidad: Se pactará una total y absoluta confidencialidad respecto a la información que haya podido conocerse como consecuencia de la relación contractual. Hay que tener en cuenta que el suministrador puede, en ocasiones, tener acceso a la cadena de información del usuario para poder desarrollar la aplicación. La

confidencialidad se hará también extensiva al secreto de la información sobre el objeto del contrato, de forma que sea el usuario, si así lo considera oportuno, el que pueda dar a la luz y publicidad del equipo y programas que ha contratado y las posibilidades que ofrecen en el tratamiento de la información.

19. Definición de términos y conceptos: Como comienzo de toda exposición, es conveniente que exista, a modo de glosario de términos a emplear en el contrato, una descripción aclarativa de todos los términos utilizados que se puedan prestar a una interpretación confusa o que necesiten una explicación. Una definición de estos términos en la parte expositiva del contrato, con el alcance de su contenido y su vinculación por las partes, es de gran interés.

20. Otras: además de las cláusulas anteriormente citadas, deberán incluirse todas aquellas normales de un contrato, como son las que hacen referencia a duración, rescisión, responsabilidades, etc. Existen además una serie de eventualidades, o circunstancias particulares, que se pueden dar en una contratación informática que algunos, en el momento de redacción del contrato, olvidan, para después, más tarde, cuando se producen, considerarlas como un riesgo extraordinario producido. Algunos de estos riesgos pueden y deben ser previstos en la contratación. Son por ejemplo, los riesgos de pérdida o dispersión de información o aquellos producidos por la falta de seguridad. Estos riesgos que se deben tener previstos, pueden traer como consecuencia errores en el tratamiento de la información o pérdida de la misma, así como otras graves consecuencias.

2.7. FISCALIDAD ELECTRÓNICA

2.7.1. Consideraciones iniciales

Los sistemas tributarios tienen y han tenido tradicionalmente un carácter nacionalista. Con la llegada de la globalización, se pone en cuestión la eficiencia de los sistemas jurídicos basados en la soberanía nacional y por eso las organizaciones internacionales juegan un papel muy relevante en la solución fiscal a los problemas de la internacionalización. Los sistemas tributarios actuales no están adaptados a los cambios que requiere la globalización. A medida que las restricciones normativas desaparecen, los obstáculos fiscales persistentes, cada vez son más patentes y la fiscalidad resulta uno de los ámbitos más relevantes en los que el mercado único no llega a implantarse.

El comercio electrónico representa un reto para la fiscalidad ya que resulta muy difícil conocer la identificación del contribuyente, así como controlar su información tributaria. Es necesaria la cooperación internacional para diseñar acuerdos internacionales sobre imposición que ayuden a solucionar los problemas de fiscalidad electrónica que puedan aparecer en el comercio electrónico entre distintos países.

En nuestro caso, Amazon al ser una multinacional con presencia en numerosos países, deberá conocer distintos sistemas tributarios para no tener que enfrentarse a posibles problemas de fiscalidad electrónica.

2.7.2. Imposición directa

Todos los impuestos directos, en general los que gravan las rentas de las personas físicas y jurídicas se ven afectados por la generalización del comercio electrónico ya sea por problemas de identificación de los intervinientes, de calificación de las rentas o de localización geográfica.

2.7.3. Impuesto sobre la renta de las personas físicas (IRPF)

Este impuesto no va a verse especialmente afectado por el desarrollo del comercio electrónico, pero el principal problema que se va a encontrar está en la localización de las rentas, es decir, en la distinción de la presencia física de una persona en un determinado territorio, a efectos de determinar el estado de residencia del sujeto pasivo que tributa por ese concepto.

Esto deberá tenerlo en cuenta Amazon para generar las nóminas de sus empleados, ya que el tipo de impuesto a aplicar sobre las mismas variará dependiendo del país de trabajo de las personas físicas.

2.7.4. Impuesto sobre Sociedades (IS)

En relación a este impuesto, hay que atender a los problemas generados por la calificación de las rentas, la localización de los sujetos, y el concepto de establecimiento permanente. La calificación de las rentas obtenidas cuando se produce una compraventa electrónica plantea dos supuestos diferenciados. De un lado, en el comercio electrónico directo, esto es, la transmisión de bienes y servicios digitalizados puede consistir sólo en un derecho de uso o una compraventa de estos productos que sólo difiere de la compraventa de bienes físicos en el soporte utilizado.

En términos tributarios, la cesión de uso puede entenderse que genera un canon cuya renta se considera obtenida en España, o puede entenderse como una compraventa internacional que se somete a tributación en el Estado de residencia del proveedor.

Las rentas se pueden calificar en beneficio empresarial, canon y otras rentas. Como reglas generales los beneficios empresariales se gravan en el estado de residencia que los obtiene, por lo que el establecimiento permanente es de gran importancia, ya que la parte de la renta imputable a este establecimiento permanente será gravada en el país de localización del mismo. Los cánones se gravan en el país de residencia del beneficiario y afectan a gran cantidad de bienes como los que se encuadran en la propiedad industrial o intelectual. Las otras rentas, con carácter general tributan en el país de residencia del transmitente del bien.

Los problemas de localización de los sujetos intervinientes crean graves conflictos en la tributación directa. En principio, prevalece el Estado de residencia sobre el Estado de la fuente. En el caso de Amazon, al tener un establecimiento en España, no habrá duda sobre el lugar de aplicación del impuesto.

2.7.5. Impuesto sobre la Renta de No Residentes

La ley de renta de no residentes requiere que exista un lugar fijo de negocios para permitir el gravamen de las rentas generadas en este lugar fijo. Este concepto puede llegar a constituir un concepto jurídico indeterminado cuya interpretación amplíe o disminuya la obligación de tributar, por lo que, una vez que se determina la existencia de este lugar fijo de negocios, se necesita asimismo que la actividad desarrollada tenga cierta importancia, y por ende, cierta independencia logística y en términos de beneficios, de la casa matriz.

Este concepto ya parte del Modelo de Convenio de la OCDE según el cual el establecimiento permanente es un lugar fijo de negocios mediante el cual una empresa desarrolla toda o parte de su actividad. El comercio electrónico aumenta en gran medida los problemas de determinación efectiva del establecimiento permanente, y que si atendemos a la definición del Modelo de Convenio de la OCDE, la falta de presencia física elimina la posibilidad de reconocer un establecimiento permanente en un país.

Además el modelo de tributación de los establecimientos permanentes, por diferencia entre ingresos y gastos, dificulta también la adjudicación de los mismos a un establecimiento permanente concreto que los genera por sus operaciones electrónicas que a la vez incluyen a diversos agentes en su desarrollo a los que serán imputables proporcionalmente los gastos e ingresos generales.

2. 7.6. Imposición indirecta

La imposición indirecta constituye una de las fuentes más antiguas de ingresos gubernamentales. Son impuestos que recaen sobre determinadas transacciones, bienes o servicios. También se ve afectada por las transacciones comerciales electrónicas.

El Impuesto sobre el Valor Añadido (IVA) también tiene su versión en el entorno electrónico. Las mercancías materiales compradas por consumidores privados por vía electrónica, pero suministrados por vía tradicional, a efectos de IVA se tratan de la misma forma que cualquier otra forma de venta a distancia, es decir, las mercancías compradas en países terceros se gravan a la importación, las exportadas son a tipo cero y las ventas intracomunitarias se gravan en el país del vendedor o del comprador dependiendo en gran medida del volumen de transacciones realizadas por el vendedor.

Si el IVA grava dos hechos imponibles, las entregas de bienes y las prestaciones de servicios, tratar una transacción de una manera u otra tiene sus consecuencias impositivas, pues en el caso de las entregas de bienes se localizan en el lugar donde el cliente dispone efectivamente del bien, y las prestaciones de servicios hay que localizarlas en el país de sede efectiva del prestador de servicios.

El IVA se ve amenazado por el creciente número de servicios internacionales que gracias a las nuevas tecnologías sitúan las transacciones imponibles fuera del ámbito territorial de aplicación del sistema común del IVA, a la vez que las divergencias entre las normativas nacionales favorecen cada vez más la evasión fiscal. Los prestadores de servicios establecidos en terceros países tendrán que aplicar y declarar el IVA en las ventas a consumidores finales establecidos en la UE.

Amazon debe tener en cuenta distintos aspectos para tomar una decisión correcta en cuanto a la fiscalidad aplicable: La situación fiscal del cliente, es decir, si el comprador está registrado a efectos de IVA o si es un consumidor privado. Si se trata de un consumidor privado establecido fuera de la UE, se deberá determinar la jurisdicción competente, siendo el objetivo verificar el lugar de consumo, y el tipo de impuesto aplicable a la transacción siendo en las ventas a consumidores en la UE el IVA del Estado miembro en el que esté registrado el prestador de servicios.

La localización de los activos a efectos fiscales resulta de extraordinaria importancia respecto de multitud de impuestos, destacando sobre manera impuestos como el IVA en el que la localización de los bienes en cuestión puede determinar su aplicabilidad, esto es, el IVA solo se paga si el suministro de los productos se realiza en un país sujeto a IVA. En definitiva, en toda transacción a efectos de IVA tendrá que determinarse su calificación como entrega de bien o prestación de servicios.

3. CONCLUSIONES

El presente trabajo ha consistido en una asesoría y consultoría en las tecnologías de la información y la comunicación de la empresa estadounidense Amazon, así como su aplicación en una implantación imaginaria en España. Para realizar este estudio, se ha partido de la legislación vigente en cada una de los puntos analizados con el objetivo de adecuar su negocio a la legislación española, así como detectar los aspectos más importantes para Amazon y las posibles áreas de mejora.

Amazon es un referente en comercio electrónico a nivel mundial, por lo que la aplicación de la legislación en este ámbito también debería ser su objetivo, con el fin de convertirse en una empresa modelo en cuanto a la protección de datos de sus clientes. No obstante, nos encontramos en un contexto en el que la proliferación de las redes de información y comunicaciones está produciendo un gran impacto en el desarrollo económico y en el comercio mundial. La globalización hace que los datos personales sean cada día más vulnerables, siendo necesaria la aplicación de medidas de seguridad y procedimientos técnicos y legales para la protección de los datos.

El reto de esta compañía es ofrecer una venta personalizada, pero respetando fielmente los datos de los clientes y garantizando la máxima seguridad en las transacciones que realicen. Hay que tener en cuenta que a los consumidores no les gusta no tener control o ser observados por las empresas, aunque sí les puede resultar interesante o de utilidad ser asesorados por una fuente de confianza como Amazon. Por tanto, la empresa debe encontrar un equilibrio, para no obstaculizar el comercio electrónico y al mismo tiempo evitar un tratamiento no autorizado de datos de carácter personal.

Con el establecimiento de reglas claras y la tutela de los derechos fundamentales se incrementará la confianza de los consumidores en las nuevas tecnologías, convirtiéndose en una condición para el desarrollo del sector y en particular del comercio electrónico.

4. ANEXOS

4.1. DOCUMENTO DE SEGURIDAD

Para elaborar el documento de seguridad de Amazon se podría tomar como modelo el siguiente documento que recoge la Agencia Española de Protección de datos:

El presente Documento y sus Anexos, redactados en cumplimiento de lo dispuesto en el Reglamento de Medidas de Seguridad (Real Decreto 994/1999 de 11 de Junio), recogen las medidas de índole técnica y organizativas necesarias para garantizar la protección, confidencialidad, integridad y disponibilidad de los recursos afectados por lo dispuesto en el citado Reglamento y en la Ley Orgánica 15/1999 de 13 de diciembre, de Protección de Datos de Carácter Personal.

El contenido principal de este Documento queda estructurado como sigue:

I. Ámbito de aplicación del documento.

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

III. Procedimiento general de información al personal.

IV. Funciones y obligaciones del personal.

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

VI. Procedimientos de revisión.

VII. Consecuencias del incumplimiento del Documento de Seguridad.

Anexo I. Aspectos específicos relativos a los diferentes ficheros.

Anexo I a. Aspectos relativos al fichero Amazon España

Anexo I b. Aspectos relativos al fichero Amazon España

Anexo II. Nombramientos

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

Anexo IV. Inventario de soportes <si se gestiona en papel>

Anexo V. Registro de Incidencias <si se gestiona en papel>

Anexo VI. Contratos o cláusulas de encargados de tratamiento <si existen, de

acuerdo con lo indicado en el artículo 12 de la LOPD>.

Anexo VII: Registro de entrada y salida de soportes

Este Documento deberá mantenerse permanente actualizado. Cualquier modificación relevante en los sistemas de información automatizados o no, en la organización de los mismos, o en las disposiciones vigentes en materia de seguridad de los datos de carácter personal conllevará la revisión de la normativa incluida y, si procede, su modificación total o parcial.

CAPÍTULO I: ÁMBITO DE APLICACIÓN DEL DOCUMENTO

El presente documento será de aplicación a los ficheros que contienen datos de carácter personal que se hallan bajo la responsabilidad de Amazon España, incluyendo los sistemas de información, soportes y equipos empleados para el tratamiento de datos de carácter personal, que deban ser protegidos de acuerdo a lo dispuesto en normativa vigente, las personas que intervienen en el tratamiento y los locales en los que se ubican.

Las medidas de seguridad se clasifican en tres niveles acumulativos (básico, medio y alto) atendiendo a la naturaleza de la información tratada, en relación con la menor o mayor necesidad de garantizar la confidencialidad y la integridad de la información.

Nivel básico: Se aplicarán a los ficheros con datos de carácter personal.

Nivel medio: Ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, (en estos dos casos, deberán ser de titularidad pública), servicios financieros y los que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia y crédito).

Nivel alto: Ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual o los recabados para fines policiales sin consentimiento (en este último caso, también deberán ser de titularidad pública). En concreto, los ficheros sujetos a las medidas de seguridad establecidas en este documento, con indicación del nivel de seguridad correspondiente, son los siguientes:

- Nómina de personal: nivel básico
- Nómina de personal: nivel básico.
- Nómina de proveedores: nivel básico.
- Personal: nivel medio.
- Contabilidad: nivel medio.
- Proveedores: nivel medio.
- Fichero de marketing: nivel medio.

- Fichero de estudio de mercado: nivel medio.
- Clientes: nivel medio.
- Distribuidores: nivel medio.

En el Anexo I se describen detalladamente cada uno de los ficheros o tratamientos, junto con los aspectos que les afecten de manera particular.

CAPÍTULO II: MEDIDAS, NORMAS PROCEDIMIENTOS, REGLAS Y ESTÁNDARES ENCAMINADOS A GARANTIZAR LOS NIVELES DE SEGURIDAD EXIGIDOS EN ESTE DOCUMENTO

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

<Especificar las normativas de identificación y autenticación de los usuarios con acceso a los datos personales. Si la autenticación se realiza mediante contraseñas, detallar el procedimiento de asignación, distribución y almacenamiento e indicar la periodicidad con la que se deberán cambiar. También es conveniente incluir los requisitos que deben cumplir las cadenas utilizadas como contraseña >

#nivel medio#

En los ficheros <indicar los nombres de los ficheros de nivel medio y alto> la identificación de los usuarios se deberá realizar de forma inequívoca y personalizada, verificando su autorización. <cada identificación debe pertenecer a un único usuario>. Asimismo, se limitará la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Control de acceso

El personal sólo accederá a aquellos datos y recursos que precise para el desarrollo de sus funciones. Exclusivamente el < persona autorizada (o denominación de su puesto de trabajo) para conceder, alterar o anular el acceso autorizado > está autorizado para conceder, alterar o anular el acceso autorizado sobre los datos y los recursos, <nota: si la persona es diferente en función del fichero, incluir el párrafo en la parte del Anexo I correspondiente>. <Especificar los procedimientos para solicitar el alta, modificación y baja de las autorizaciones de acceso a los datos, indicando que persona (o puesto de trabajo) concreta tiene que realizar cada paso. Incluir y detallar los controles de acceso a los sistemas de información >

En el Anexo I, se incluye la relación de usuarios actualizada con acceso autorizado a cada sistema de información. Asimismo, se incluye el tipo de acceso autorizado para

cada uno de ellos. Esta lista se actualizará < Especificar procedimiento de actualización.>

#nivel medio# Control de acceso físico

Exclusivamente el personal que se indica a continuación, podrá tener acceso a los locales donde se encuentren ubicados los sistemas de información correspondientes a

- personal
- Contabilidad
- Proveedores
- Fichero de marketing
- Fichero de estudio de mercado
- Clientes
- Distribuidores

Gestión de soportes

Los soportes que contengan datos de carácter personal deben ser etiquetados para permitir su identificación, inventariados y almacenados en la oficina de ficheros de Amazon, lugar de acceso restringido al que solo tendrán acceso las personas con autorización que se relacionan a continuación: Virginia Aguilar Arcos, responsable de protección de datos.

Los soportes informáticos se almacenarán de acuerdo a las siguientes normas: <Indicar normas de etiquetado de los soportes. Especificar el procedimiento de inventariado y almacenamiento de los mismos. El inventario de soportes puede anexarse al documento o gestionarse de forma automatizada, en este último caso se indicará en este punto el sistema informático utilizado>.

La salida de soportes informáticos que contengan datos de carácter personal, fuera de los locales en donde esté ubicado el sistema de información, únicamente puede

ser autorizada por el responsable del fichero o aquel en que se hubiera delegado de acuerdo al siguiente procedimiento <detallar el procedimiento a seguir para que se lleve a cabo la autorización. Tener en cuenta también los ordenadores portátiles y el resto de dispositivos móviles que puedan contener datos personales>.

En el Anexo III se incluirán los documentos de autorización relativos a la salida de soportes que contengan datos personales.

#nivel medio# Registro de Entrada y Salida de Soportes.

Las salidas y entradas de soportes correspondientes a los ficheros <indicar los nombres de los ficheros de nivel medio y alto>, deberán ser registradas de acuerdo al siguiente procedimiento: <Detallar el procedimiento por el que se registrarán las entradas y salidas de soportes>.

El registro de entrada y salida de soportes se gestionará mediante un modo informático y en el que deberán constar el tipo de soporte, la fecha y hora, el emisor, el número de soportes, el tipo de información que contienen, la forma de envío y la persona responsable de la recepción, y en el caso de las salidas, el tipo de soporte, la fecha y hora, el destinatario, el número de soportes , el tipo de información que contienen, la forma de envío y la persona responsable de la entrega> <En caso de gestión automatizada se indicará en este punto el sistema informático utilizado>.

#nivel medio# Medidas adicionales para los soportes con datos de nivel medio

Los soportes correspondientes a personal, contabilidad, proveedores, fichero de marketing, fichero de estudio de mercado, clientes, distribuidores, que vayan a ser desechados o reutilizados, deberán ser previamente <detallar procedimiento a realizar para impedir cualquier recuperación de la información almacenada en ellos> de forma que no sea posible recuperar la información almacenada en ellos. Si los soportes con datos de los mencionados ficheros van a salir fuera de los locales en que se encuentren ubicados, como consecuencia de operaciones de mantenimiento, se adoptarán las siguientes medidas con el fin de impedir cualquier recuperación indebida de la información almacenada en ellos.

Acceso a datos a través de redes de comunicaciones

Las medidas de seguridad exigibles a los accesos a los datos de carácter personal a través de redes de comunicaciones deberán garantizar un nivel de seguridad equivalente al correspondiente a los accesos en modo local.

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

La ejecución de tratamiento de datos de carácter personal fuera de los locales de la ubicación del fichero deberá ser autorizada expresamente por el responsable del fichero y, en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado. <detallar el procedimiento de autorización>

Ficheros temporales

Los ficheros temporales deberán cumplir el nivel de seguridad que les corresponda con arreglo a los criterios expresados en el Reglamento de medidas de seguridad, y serán borrados una vez que hayan dejado de ser necesarios para los fines que motivaron su creación.

Copias de seguridad

Es obligatorio realizar copias de respaldo de los ficheros automatizados que contengan datos de carácter personal. Los procedimientos establecidos para las copias de respaldo y para su recuperación garantizarán su reconstrucción en el estado en que se encontraban al tiempo de producirse la pérdida o destrucción.

En el Anexo I se detallan los procedimientos de copia y recuperación de respaldo para cada fichero.

#nivel medio# Las recuperaciones de datos de los ficheros de personal, contabilidad, proveedores, fichero de marketing, fichero de estudio de mercado, clientes y distribuidores deberán ser autorizadas por escrito por el responsable del fichero, según el procedimiento indicado en el Capítulo V.

#nivel medio# Responsable de seguridad

El responsable del fichero designará a <indicar si existen uno o varios responsables de seguridad>, que con carácter general se encargará de coordinar y controlar las medidas definidas en este documento de seguridad.

En ningún caso, la designación supone una delegación de la responsabilidad que corresponde a <denominación responsable del fichero> como responsable del fichero de acuerdo con el Reglamento de medidas de seguridad.

El responsable de seguridad desempeñará las funciones encomendadas durante el periodo de <indicar periodo de desempeño del cargo>. Una vez transcurrido este plazo <denominación responsable del fichero> podrá nombrar al mismo responsable de seguridad o a otro diferente. <Si existiera un responsable de seguridad diferente para cada fichero, indicarlo en la parte correspondiente del Anexo I>

En el Anexo II se encuentran las copias de los nombramientos de responsables de seguridad.

#nivel medio# Pruebas con datos reales

Las pruebas anteriores a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal, no se realizarán con datos reales, salvo que se asegure el nivel de seguridad correspondiente al fichero tratado.

CAPÍTULO III. PROCEDIMIENTO GENERAL DE INFORMACIÓN AL PERSONAL

Las funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y a los sistemas de información están definidas de forma general en el

Capítulo siguiente y de forma específica para cada fichero en la parte del Anexo I correspondiente.

Para asegurar que todas las personas conocen las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias del incumplimiento de las mismas, serán informadas de acuerdo con siguiente procedimiento: <indicar el procedimiento por el cual se informará a cada persona, en función de su perfil, de las normas que debe cumplir y de las consecuencias de no hacerlo. Puede ser conveniente incluir algún sistema de acuse de recibo de la información> <Si se estima oportuna, la remisión periódica de información sobre seguridad: circulares, recordatorios, nuevas normas, indicar aquí el procedimiento y las personas autorizadas para hacerlo>

CAPÍTULO IV. FUNCIONES Y OBLIGACIONES DEL PERSONAL

Funciones y obligaciones de carácter general.

Todo el personal que acceda a los datos de carácter personal está obligado a conocer y observar las medidas, normas, procedimientos, reglas y estándares que afecten a las funciones que desarrolla. Constituye una obligación del personal notificar al <responsable del fichero o de seguridad en su caso> las incidencias de seguridad de las que tengan conocimiento respecto a los recursos protegidos, según los procedimientos establecidos en este Documento, y en concreto en su Capítulo V. Todas las personas deberán guardar el debido secreto y confidencialidad sobre los datos personales que conozcan en el desarrollo de su trabajo.

Funciones y obligaciones de <incluir un punto con las obligaciones detalladas de los perfiles que afectan a todos los ficheros, como por ejemplo, administradores de los sistemas, responsables de informática, responsable/s de seguridad si existe/n, responsables de seguridad física, etc. Es importante que se concrete la persona o cargo que corresponde a cada perfil. También deben contemplarse los procedimientos de actuación o delegación de funciones para casos de ausencia. Este apartado se propone principalmente como un recopilatorio que agrupe las medidas que en el resto del Documento se asignan a perfiles concretos>

CAPÍTULO V. PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE LAS INCIDENCIAS.

Se considerarán como "incidencias de seguridad", entre otras, cualquier incumplimiento de la normativa desarrollada en este Documento de Seguridad, así como a cualquier anomalía que afecte o pueda afectar a la seguridad de los datos de carácter personal de <denominación del responsable del fichero>. El procedimiento a seguir para la notificación de incidencias será < especificar concretamente los procedimientos de notificación y gestión de incidencias, indicando quien tiene que notificar la incidencia, a quien y de qué modo, así como quien gestionará la incidencia>.

El registro de incidencias se gestionará mediante <indicar la forma en que se almacenará el registro, que puede ser manual o informático, y en el que deberán constar, al menos, el tipo de incidencia, el momento en que se ha producido, la persona que realiza la notificación, a quién se comunica y los efectos que se hubieran derivado de la

misma. En caso de gestión automatizada se indicará en este punto el sistema informático utilizado>.

#nivel medio# En el registro de incidencias se consignarán también los procedimientos de recuperación de datos que afecten a los ficheros <relacionar los ficheros de nivel medio y alto>, del modo que se indica a continuación <detallar el procedimiento para registrar las recuperaciones de datos, que deberá incluir la persona que ejecutó el proceso, los datos restaurados y, en su caso, que datos ha sido necesario grabar manualmente en el proceso de recuperación. En caso de gestión automatizada, se deberá prever la existencia de un código específico para recuperaciones de datos, en la información relativa al tipo de incidencia>.

#nivel medio# Para ejecutar los procedimientos de recuperación de datos en los ficheros mencionados en el párrafo anterior, será necesaria la autorización por escrito del responsable del fichero.

En el Anexo III se incluirán los documentos de autorización por parte del responsable del fichero relativos a la ejecución de procedimientos de recuperación de datos.

CAPÍTULO VI PROCEDIMIENTOS DE REVISIÓN

Revisión del Documento de Seguridad.

< Especificar los procedimientos previstos para la modificación del documento de seguridad, con especificación concreta de las personas que pueden o deben proponerlos y aprobarlos, así como para la comunicación de las modificaciones al personal que pueda verse afectado.

El documento deberá mantenerse en todo momento actualizado y deberá ser revisado siempre que se produzcan cambios relevantes en el sistema de información o en la organización del mismo. Asimismo, deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal >

#nivel medio# Auditoría

< Indicar los procedimientos para realizar la auditoría interna o externa que verifique el cumplimiento del Reglamento de Seguridad según lo indicado su artículo 17, y que debe realizarse al menos cada dos años. El informe analizará la adecuación al Reglamento de las medidas y controles, identificará las deficiencias y propondrá las medidas correctoras o complementarias necesarias. Los informes de auditoría han de ser analizados por el responsable del fichero, y quedar a disposición de la Agencia Española de Protección de Datos >

CAPÍTULO VII: CONSECUENCIAS DEL INCUMPLIMIENTO DEL DOCUMENTO DE SEGURIDAD

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el presente documento por el personal afectado, se sancionará conforme a <indicar la normativa sancionadora aplicable>

ANEXO I a. ASPECTOS RELATIVOS AL FICHERO <nombre del fichero a>

Actualizado a: < fecha de la última actualización del anexo > <Se incluirá un anexo de este tipo por cada fichero incluido en el ámbito del documento de seguridad, podrían denominarse ANEXO I b, c, etc.>

• Nombre del fichero o tratamiento: <rellenar con nombre del fichero>

• Unidad/es con acceso al fichero o tratamiento: <especificar departamento o unidad con acceso al fichero, si aporta alguna información>

• Identificador y nombre del fichero en el Registro General de Protección de Datos de la

Agencia Española de Protección de Datos: <rellenar los siguientes campos con los datos relativos a la inscripción del fichero en el Registro General de Protección deDatos (RPGD)> o Identificador: <código de inscripción> o Nombre: <nombre inscrito> o Descripción: <descripción inscrita>

• Nivel de medidas de seguridad a adoptar: <básico, medio o alto>

• #nivel medio# Responsable de seguridad: <Persona designada por el responsable del fichero al objeto de coordinar y controlar las medidas incluidas en este documento>.

• Administrador: <Persona designada para conceder, alterar, o anular el acceso autorizado a los datos>.

• Leyes o regulaciones aplicables que afectan al fichero o tratamiento <si existen>

• Código Tipo Aplicable: <se indicará aquí si el fichero esta incluido en el ámbito de alguno de los códigos tipo regulados por el articulo 32 de la LOPD>.

• Estructura del fichero principal: <Incluir los tipos de datos personales incluidos, con especificación de los que, por su naturaleza, afectan a la diferente calificación del nivel de medidas de seguridad a adoptar, según lo indicado en el artículo 4 del Reglamento de Seguridad>.

• Información sobre el fichero o tratamiento

o Finalidad y usos previstos:

o Personas o colectivos sobre los que se pretenda obtener o que resulten

obligados a suministrar los datos personales:

o Cesiones previstas:

o Transferencias Internacionales: <relacionar las transferencias internacionales, especificando si ha sido necesaria la autorización del Director de la Agencia Española de Protección de Datos>

o Procedencia de los datos: <indicar quien suministra los datos>

o Procedimiento de recogida: <encuestas, formularios en papel, Internet, ...>

o Soporte utilizado para la recogida de datos: <papel, informático, telemático, ...>

• Servicio o Unidad ante el que puedan ejercitarse los derechos de acceso, rectificación, cancelación y oposición: <indicar la unidad y/o dirección. Deben preverse además, los procedimientos internos para responder a las solicitudes de ejercicio de derechos de los interesados>

• Descripción del sistema de información: <Describir los sistemas de información automatizados o no en los que se realiza el tratamiento de los datos. En el caso de ficheros automatizados, incluir los equipos físicos>.

• Descripción detallada de las copias de respaldo y de los procedimientos de recuperación <En el caso de sistemas automatizados. Especificar la periodicidad de las copias (que debe ser al menos semanal). Si se trata de ficheros manuales y tienen prevista alguna medida en este sentido, detallarla>.

• Información sobre conexión con otros sistemas: <Describir las posibles relaciones con otros ficheros del mismo responsable>.

• Funciones del personal con acceso a los datos personales: <Especificar las diferentes funciones y obligaciones de cada una de las personas con acceso a los datos de carácter personal y sistema de información específicos de este fichero>.

• Descripción de los procedimientos de control de acceso e identificación: <Cuando sean específicos para el fichero>.

• Relación actualizada de usuarios con acceso autorizado: <Relacionar todos los usuarios que acceden al fichero, con especificación del tipo o grupo de usuarios al que pertenecen, su clave de identificación, nombre y apellidos, unidad, fecha de alta y fecha de baja>.

<Si la relación se mantiene de forma informatizada, indicar aquí cual es el sistema utilizado y la forma de obtener el listado. No obstante, siempre que sea posible, es conveniente imprimir la relación de usuarios y adjuntarla periódicamente a este Anexo>.

• Terceros que acceden a los datos para la prestación de un servicio: <Relacionar las empresas de mantenimiento, de servicios, etc., que tienen acceso a los datos. Cuando sea necesario realizar un contrato escrito según lo dispuesto en el artículo 12 de la LOPD, se incluirá una copia del mismo o de las cláusulas al efecto en el Anexo VI del documento>.

• Relación de actualizaciones de este Anexo: <incluyendo fecha, resumen de aspectos modificados y motivo>

ANEXO II NOMBRAMIENTOS

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

ANEXO III AUTORIZACIONES SALIDA O RECUPERACIÓN DE DATOS

<Adjuntar original o copia de las autorizaciones que el responsable del fichero ha firmado para la salida de soportes que contengan datos de carácter personal, así como aquellas relativas a la ejecución de los procedimientos de recuperación de datos >

ANEXO IV INVENTARIO DE SOPORTES

<Si el inventario de soportes se gestiona de forma no automatizada recoger en este anexo la información al efecto, según lo indicado en el Capítulo II, punto "Gestión de soportes" de este documento. Los soportes deberán permitir identificar el tipo de información, que contienen, ser inventariados y almacenarse en un lugar con acceso restringido al personal autorizado para ello en este documento >

ANEXO V: REGISTRO DE INCIDENCIAS.

<Si el registro de incidencias se gestiona de forma no automatizada, recoger en este anexo la información al efecto, según lo indicado en el Capítulo V, "Procedimiento de notificación, gestión y respuesta ante las incidencias" de este documento>

ANEXO VI: ENCARGADOS DE TRATAMIENTO

<Cuando el acceso de un tercero a los datos del responsable del fichero sea necesario para la prestación de un servicio a este último, no se considera que exista comunicación de datos. Recoger aquí el contrato que deberá constar por escrito o de alguna otra forma que permita acreditar su celebración y contenido, y que establecerá expresamente que el encargado de tratamiento tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizara con fin distinto al que figure en dicho contrato, ni los comunicarán ni siquiera para su conservación a otras personas. El contrato estipulará las medidas de seguridad a que se refiere el artículo 9 de la LOPD que el encargado del tratamiento está obligado a implementar>

ANEXO VII REGISTRO DE ENTRADA Y SALIDA DE SOPORTES

<Si el registro de entrada y salida de soportes al que se refiere el Capítulo II, punto "Gestión de soportes", y que es obligatorio a partir del nivel medio, se gestiona de forma no automatizada, recoger en este anexo la información al efecto, según lo indicado los artículos 20.1 y 20.2 del Reglamento de Seguridad.>

4.2. EJEMPLO DE INFORMACIÓN DE AMAZON EN WHOIS.ORG

WHOIS information for **amazon.com** :

```
[Querying whois.verisign-grs.com]
[whois.verisign-grs.com]

Whois Server Version 2.0

Domain names in the .com and .net domains can now be registered
with many different competing registrars. Go to
http://www.internic.net
for detailed information.

   Domain Name: AMAZON.COM
   Registrar: NETWORK SOLUTIONS, LLC.
   Whois Server: whois.networksolutions.com
   Referral URL: http://www.networksolutions.com
   Name Server: PDNS1.ULTRADNS.NET
   Name Server: PDNS2.ULTRADNS.NET
   Name Server: PDNS3.ULTRADNS.ORG
   Name Server: PDNS4.ULTRADNS.ORG
   Name Server: PDNS5.ULTRADNS.INFO
   Name Server: PDNS6.ULTRADNS.CO.UK
   Name Server: UDNS1.ULTRADNS.NET
   Status: clientDeleteProhibited
   Status: clientTransferProhibited
   Status: clientUpdateProhibited
   Updated Date: 25-jun-2010
   Creation Date: 01-nov-1994
   Expiration Date: 31-oct-2019

<<

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the
registry is
currently set to expire. This date does not necessarily reflect the
expiration
date of the domain name registrant's agreement with the sponsoring
registrar.  Users may consult the sponsoring registrar's Whois
database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
database through the use of electronic processes that are high-volume
and
automated except as reasonably necessary to register domain names or
modify existing registrations; the Data in VeriSign Global Registry
Services' ("VeriSign") Whois database is provided by VeriSign for
information purposes only, and to assist persons in obtaining
information
about or related to a domain name registration record. VeriSign does
not
```

guarantee its accuracy. By submitting a Whois query, you agree to abide
by the following terms of use: You agree that you may use this Data only
for lawful purposes and that under no circumstances will you use this Data
to: (1) allow, enable, or otherwise support the transmission of mass
unsolicited, commercial advertising or solicitations via e-mail, telephone,
or facsimile; or (2) enable high volume, automated, electronic processes
that apply to VeriSign (or its computer systems). The compilation,
repackaging, dissemination or other use of this Data is expressly
prohibited without the prior written consent of VeriSign. You agree not to
use electronic processes that are automated and high-volume to access or
query the Whois database except as reasonably necessary to register
domain names or modify existing registrations. VeriSign reserves the right
to restrict your access to the Whois database in its sole discretion to ensure
operational stability. VeriSign may restrict or terminate your access to the
Whois database for failure to abide by these terms of use. VeriSign
reserves the right to modify these terms at any time.

The Registry database contains ONLY .COM, .NET, .EDU domains and
Registrars.

5. BIBLIOGRAFÍA

[1] http://money.cnn.com/magazines/fortune/mostadmired/2010/snapshots/10810.html Consultado el 21 de mayo de 2010

[2] http://es.wikipedia.org/wiki/Amazon.com Consultado el 21 de mayo de 2010

[3] http://www.amazon.com/Careers-Homepage/b/ref=amb_link_6001432_3?ie=UTF8&node=239364011&pf_rd_m=ATVPDKIKX0DER&pf_rd_s=center-2&pf_rd_r=1507VKG6VFP5QVC1DQBW&pf_rd_t=101&pf_rd_p=434481001&pf_rd_i=203348011 Consultado el 21 de mayo de 2010

[4] http://www.amazon.com/dp/B0015T963C/?tag=gocous-20&hvadid=4139604977&ref=pd_sl_7caym1p0x_e

[5] http://es.wikipedia.org/wiki/Amazon.com

[6] Ley Orgánica 15/1999. http://www.boe.es/aeboe/consultas/bases_datos/doc.php?coleccion=iberlex&id=1999/23750

[7] Real Decreto 1720/2007

http://www.boe.es/aeboe/consultas/bases_datos/doc.php?coleccion=iberlex&id=2008/00979

[8] Ley De Comercio Electrónico

http://www.boe.es/boe/dias/2002/07/12/pdfs/A25388-25403.pdf

[9] http://www.davara.net/c/mac-tic/pagina_centro_proteccion_generalidades.asp

[10] Ley De Comercio Electrónico

http://www.boe.es/boe/dias/2002/07/12/pdfs/A25388-25403.pdf

- Documentación ofrecida durante el curso del Máster en Asesoría y Consultoría en Tecnologías de la Información y las Comunicaciones (MAC-TIC).

  Davara&Davara asesores jurídicos.

- Factbook comercio electrónico (2004). Editorial Aranzadi.

  Miguel Ángel Davara Rodríguez

- Página web del ministerio de industria y comercio

  www.mityc.es

- Página de la Agencia Española de Protección de Datos

  www.agpd.es

- Página web de WHOIS

  www.whois.org