6. SISTEMAS DE SEGURIDAD Y ASPECTOS LEGALES

"El único sistema seguro es aquel que está apagado en el interior de un bloque de hormigón, protegido en una habitación sellada rodeada por guardias armados".

Gene Spafford

A lo largo de este curso, hemos comentado que uno de los grandes obstáculos a la hora de realizar compras a través de Internet es la seguridad. Como refleja la cita, es imposible encontrar un sistema infranqueable, ya que tanto en los negocios vía Internet como también en los negocios físicos siempre existirá una pequeña sombra de

duda. Pero eso no puede suponer una excusa para caer en el inmovilismo y rechazar todos los avances que las nuevas tecnologías ofrecen.

Lo primero que debe hacerse es concienciar a los clientes de que los sistemas y medidas de seguridad son cada día más eficientes. Para garantizar la seguridad del usuario se implantan protocolos de seguridad (o protocolos criptográficos), que constituyen una serie de normas comunes para establecer una comunicación protegida a través de Internet. Estos protocolos describen la forma en que deben usarse las diferentes estructuras de datos y contribuyen al buen funcionamiento en lo que al transporte de datos se refiere. Además de estos protocolos, nos encontramos con toda una serie de normas y aspectos legales cuya finalidad es la de proteger los datos de los usuarios, con el fin de que su información personal quede protegida y no pueda ser accesible por nadie.

De este modo en este capítulo vamos a hablar tanto de los sistemas de seguridad, con el fin de hacernos con la confianza de los consumidores, así como de toda una serie de aspectos legales que debemos tener en cuenta al trabajar con los datos personales de terceros.

6.1. PROTOCOLO TLS

Uno de los protocolos más habituales es el protocolo TLS (Transport Layer Security o Seguridad de la Capa de Transporte). Se trata de un protocolo criptográfico que nos permite una conexión segura a través de la red por medio de un canal cifrado que garantiza un transporte de información privado y seguro. El TLS supone una evolución de una versión anterior conocida como SSL (Secure Sockets Layer o Capa de Conexiones Seguras).

El protocolo TLS identifica únicamente el servidor, es por ello que el cliente se mantiene sin identificar. Estos sistemas permiten introducir información personal a diferentes webs sin peligro, y pueden prevenir escuchas secretas conocidas como *Eavesdropping* o falsificaciones de identidad. Se trata del sistema más utilizado en tiendas online, bancos y todo aquel negocio que implique contraseñas y datos personales. No obstante, debemos tener en cuenta que no todas las webs utilizan este

sistema, así que debemos ser muy cuidadosos con nuestra información personal y nuestras contraseñas:

"Las contraseñas son como la ropa interior. No puedes dejar que nadie la vea, debes cambiarla regularmente y no debes compartirla con extraños".

Chris Pirillo

6.1.1 Conceptos y funcionamiento

Antes de profundizar en el funcionamiento del TLS, conviene repasar algunos conceptos que nos ayudarán a entender cómo se desarrolla este sistema de seguridad:

- El cifrado: es el proceso por medio del cual se convierte una información para que sólo determinados usuarios puedan entender. Para ello se utiliza lo que se denomina "clave", y sólo aquel que posea esa clave puede descifrar la información.
- Firma digital: igual que sucede con la firma física, la firma digital es un elemento personal que permite nuestra identificación. Se utiliza una clave única y privada de la persona que firma.
- Autoridad Certificadora (CA, Certification Authority): se trata de entidades que identifican los certificados digitales y garantizan que sus poseedores son realmente quien dicen ser.
- HTTPS: es el resultado de aunar el protocolo HTTP y el TLS (o SSL) para realizar comunicaciones cifradas en los sitios web.
- Certificado digital TLS: consiste en un documento que certifica la vinculación entre una entidad y su clave. En ella encontramos los datos personales del usuario y la información de la clave como el número de serie, su autoridad certificadora, periodo de validez, firma digital, etc.

El protocolo se desarrolla con una primera fase en la que se inicia la comunicación segura en la que el cliente y el servidor negocian los algoritmos criptográficos con los que se cifrarán los datos y se autentificarán. Se envían todos los datos sobre el protocolo que soportan y los parámetros requeridos para la conexión.

En la siguiente fase, las dos partes implicadas intercambian las claves y se autentifican por medio de certificados digitales, intercambiando los códigos necesarios para llevar a cabo el tráfico de información. Se verifica la integridad del certificado, su vigencia y quién es el emisor.

Finalmente, servidor y navegador pueden iniciar la comunicación cifrada, ya autentificada y verificada.

El funcionamiento del protocolo TLS pasa por varias etapas de intercambio de datos:

1. En primer lugar, el navegador pide que el servidor web se identifique.
2. El servidor presenta una copia de su certificado TLS (o SSL) para probar su identidad.
3. Para poder establecer una comunicación de confianza, el navegador realiza la verificación del certificado y, si es correcto, envía un mensaje al servidor.
4. El servidor retorna la confirmación firmada digitalmente y se da inicio a la sesión con cifrado TLS.
5. Validación del proceso: el navegador y el servidor intercambian datos de forma segura por medio de una comunicación cifrada.

Para acceder a un sitio web, es recomendable utilizar el protocolo HTTPS, a menudo representado con un candado en la barra del navegador. Si el protocolo TLS cumple su función, podremos acceder sin problemas al sitio; en caso contrario o si existe algún error, entonces aparecerá un mensaje de advertencia.

El protocolo TLS es la forma más segura de navegar y ofrece una garantía de confianza en el sitio web por varias razones:

- Permite establecer una conexión segura gracias al cifrado de datos confidencial en las transacciones online.
- El certificado TLS supone una credencial única que indica quién es el propietario único del certificado.
- Permite que dos aplicaciones distintas intercambien códigos sin necesidad de que cada una conozca los códigos de la otra. Además, no se trata de un

protocolo limitado, ya que permite ir incorporando nuevos algoritmos criptográficos.

- Cuenta con una garantía de certificación de identidad del propietario del certificado antes de emitirlo.

El protocolo se divide en dos niveles:

- **Protocolo de registro (Record Protocol)*:*** Se trata del protocolo de más bajo nivel, y proporciona una conexión fiable y privada por medio de algoritmos de cifrado simétrico. Para cada conexión se crea una clave basada en el protocolo de mutuo acuerdo.
- **Protocolo de mutuo acuerdo (Handshake Protocol):** Permite que tanto el servidor como el cliente puedan autentificarse y acordar un algoritmo para la encriptación antes del intercambio de datos. Se trata de una conexión segura debido a que la identidad se verifica utilizando una clave pública. La negociación es segura y fiable, y no se puede modificar sin ser detectada.

6.1.2 Aplicaciones

La principal aplicación del protocolo TLS es crear versiones seguras de programas que utilizan protocolos de baja fiabilidad. Existen versiones seguras para diferentes servidores y protocolos como pueden ser el HTTP, SMTP, POP3, NNTP, LDAP, ETC... Puede ofrecer seguridad a cualquier protocolo que use conexiones de confianza como el TCP.

Entre las aplicaciones del protocolo TLS, existen algunas muy extendidas como la Biblioteca Openssl, (con Licencia Pública General, GNU) que dispone de versiones tanto SSL como TLS y muchos algoritmos criptográficos (www.openssl.org).

6.1.3 Ventajas

A modo de resumen, podemos decir que el protocolo TLS supone un avance en lo que a garantías de seguridad se refiere, algo fundamental para el eCommerce. Su gran valía es lograr la encriptación en la comunicación que mantienen el servidor y el cliente

como consecuencia del uso de algoritmos cifrados. Supone también una mejora respecto al protocolo anterior (SSL) que poseía un sistema de cifrado más débil.

No obstante, no podemos olvidar la cita con la que iniciábamos el capítulo y hay que ser conscientes de que la seguridad absoluta en la red no existe. Pese a todo, este sistema ha contribuido a que los niveles de confidencialidad a la hora de llevar a cabo transacciones e intercambios de datos privados posean un grado de fiabilidad cada vez más elevado, implicando ello que el cliente sienta confianza hacia la empresa y el eCommerce y no tenga miedo a realizar sus compras de manera online.

6.2 PROTOCOLO DE TRANSACCIONES ELECTRÓNICAS SEGURAS (SET)

EL Protocolo SET es un sistema de comunicaciones diseñado para llevar a cabo de forma segura las transacciones comerciales con tarjeta de crédito a través de Internet. Se trata de un protocolo elaborado por Visa y Mastercard, en el que también participaron otras grandes empresas como American Express, Microsoft, IBM, Netscape o Verisign, para proporcionar mayor seguridad al eCommerce.

6.2.1 Funcionamiento

Para poder utilizar este sistema, en primer lugar es necesario que la empresa tenga un certificado digital certificado. En segundo lugar, el usuario debe disponer de otro certificado, esta vez emitido por la empresa de su tarjeta bancaria, que incorpora la firma digital de la empresa (Visa, Mastercard, etc.) y la fecha de expiración.

El desarrollo del protocolo SET consta de los siguientes pasos:

- La empresa y el cliente llevan a cabo el proceso de identificación y verificación mediante certificados digitales.
- El comprador y su entidad bancaria cierran la transacción. En este proceso, el comerciante no tiene acceso a los datos de la tarjeta del usuario, lo que garantiza la confidencialidad de la información personal y bancaria.
- Finaliza el proceso y la información se transfiere de forma encriptada.

Se trata de un protocolo muy interesante por su sistema de autentificación, ya que permite evitar actividades ilegales, usos fraudulentos de tarjetas o falsificaciones web. Los certificados digitales suponen que empresas y usuarios puedan autentificarse mutuamente para mayor seguridad.

A la hora de realizar la transacción SET, el proceso sigue las siguientes etapas:

- Antes de que el pedido haya concluido, el usuario recibe la firma digital de la tienda online y comprueba su validez.
- El usuario envía a la empresa los datos del pedido, la fecha, el precio del artículo o servicio, la orden de pago encriptada de tal forma que el banco sea el único que tenga acceso a dicha información, y la relación entre ese pedido y su orden de pago que los vincula de manera definitiva.
- La empresa recibe el pedido y autentifica su validez con la firma digital y envía al banco su orden de pago.
- Finalmente, el banco autoriza la orden y retorna una confirmación para la empresa y otra para el usuario.

6.2.2 Seguridad

El protocolo SET proporciona numerosas ventajas en cuanto a seguridad se refiere. En primer lugar, y como ya hemos comentado, lo más interesante es que el comerciante nunca tiene acceso a los datos de la tarjeta de crédito, ya que el usuario se identifica con un certificado digital que emite su propia entidad bancaria.

También otorga una importante garantía de que los datos no puedan ser manipulados durante la transacción, debido a que se encuentran encriptados y protegidos por la firma digital.

Finalmente, hay que destacar la seguridad que ofrece por su capacidad para autentificar, tanto al cliente como verdadero poseedor de una tarjeta bancaria, como a la empresa como entidad autorizada para realizar el ingreso de esa tarjeta.

6.2.3 Inconvenientes

Actualmente, el protocolo SET es uno de los medios de pago más frecuentes en el eCommerce ya que supone un avance respecto a protocolos más antiguos como el SSL. No obstante, todavía existen Proveedores de Servicios de Internet (ISP) que no están adaptados para trabajar con este sistema.

Esto obliga a las empresas a tener que combinar el protocolo SSL con el protocolo SET, lo que supone una mayor complejidad de la estructura. Además, en el sistema SET, las transacciones se realizan con mayor lentitud y suponen un coste adicional para la empresa, ya que deben abonar el certificado digital.

6.3 SISTEMAS DE CODIFICACIÓN

La informática del siglo XXI, en su empeño por la búsqueda de un tráfico de información privado y confidencial, ha desarrollado sistemas criptográficos basados en códigos matemáticos que transforman la información para que sólo puedan tener acceso a ella las personas autorizadas.

Para que un sistema criptográfico sea realmente seguro deber cumplir algunas características:

- Privacidad: Los códigos utilizados deben conceder acceso únicamente al personal autorizado.
- Autentificación: Deben verificarse las identidades de ambas partes dentro de la comunicación.
- Integridad: Se debe garantizar el contenido completo del mensaje.
- Vinculación: Es posible relacionar directamente una información a una determinada persona o sistema. Esa acción implica que esa persona entiende y acepta esta vinculación.

Los datos encriptados que viajan a través de la red están codificados en un sistema binario a través de operaciones matemáticas que los hacen indescifrables. Para poder tener acceso a esa información es necesario hacer uso de las claves que tiene el personal autorizado y aplicar el mismo algoritmo que descifre el mensaje. Estos datos

incluyen una fecha digital que puede servir como garantía jurídica en caso de que fuera necesario.

6.4 CIFRADO SIMÉTRICO Y ASIMÉTRICO

La **criptografía simétrica** (o de clave privada) es un sistema que consiste en el uso de una misma clave secreta para cifrar y descifrar la información, compartida y acordada por el emisor y el receptor de la comunicación. La clave está creada a partir de algoritmos que aportan confidencialidad al mensaje.

Teniendo en cuenta que el algoritmo debe estar en clave, en caso de que un supuesto atacante conociera el algoritmo, no le serviría de nada ya que necesitaría la clave. El problema se plantea a la hora de hacer llegar esa clave a nuevos clientes de forma segura, ya que en ese proceso sí podría ser interceptada. Se necesitaría además crear una clave secreta para cada uno de los usuarios que compraran por Internet. Así que podemos ver que a pesar de la seguridad que proporciona, el uso del sistema simétrico no está muy extendido en caso de querer acceder a un buen número de clientes.

La **criptografía asimétrica** (o de clave pública) consiste en el uso de dos claves, una pública conocida por las dos partes de la comunicación y otra privada accesible únicamente para el propietario.

El proceso sería el siguiente:

- El emisor crea un mensaje y lo cifra con la clave pública del receptor.
- El mensaje cifrado se envía a través de la red.
- El receptor descifra el mensaje mediante su clave privada y tiene acceso a la información original.

Este sistema se ha convertido en el más habitual en Internet ya que garantiza la autenticidad de los miembros y la integridad del mensaje. Además, es el ideal para el

campo del eCommerce ya que soluciona los problemas de intercambio de claves de los sistemas simétricos. En este aspecto, no es necesario que los participantes se pongan de acuerdo en qué clave utilizar, simplemente lo que se requiere es que el remitente obtenga una copia de la clave pública del destinatario.

Uno de los inconvenientes de la clave asimétrica es que requiere más recursos para funcionar y se desarrolla con más lentitud, por lo que existen también criptografías híbridas que combinan la rapidez del algoritmo simétrico con la seguridad del intercambio de claves que proporciona el sistema asimétrico.

6.5 FIRMA Y CERTIFICADOS DIGITALES

La **firma digital o electrónica** es la encargada de identificar al firmante como creador del mensaje y da validez al contenido del mensaje. Para ello, utiliza un sistema de codificación asimétrico en el que el emisor utiliza su clave privada para codificar el mensaje y queda vinculado al mensaje.

Para decodificarlo, el receptor utilizar la clave pública del autor y consigue verificar su autenticidad, comprobando que el emisor es quien dice ser y confirmando que la información no ha sido alterada. Se trata de una buena medida para evitar falsificaciones y manipulaciones de información. Además, estas firmas digitales tienen validez a efectos jurídicos y están sujetas a consideraciones legales.

Los **certificados digitales o electrónicos** son ficheros creados por entidades de servicios de certificación en los que se asocian los siguientes datos:

- Autoridad que firma el certificado.
- Datos personales del emisor.
- Periodo de validez.
- Número de certificado.
- Clave pública del propietario.
- Firma electrónica de la autoridad que firma el certificado.

Las entidades de servicios de certificación son las encargadas de validar la información presentada por los solicitantes y crear los certificados. Además, estas entidades deben

presentar garantías económicas y se les exige un seguro de responsabilidad civil. Estos certificados suponen una herramienta importante en lo que a creación de confianza se refiere ya que garantiza la autoría del mensaje de una forma fidedigna.

6.6 MEDIDAS DE SEGURIDAD Y AMENAZAS EN EL ECOMMERCE

Hasta ahora, hemos hablado de protocolos de seguridad para evitar infracciones en la red que puedan perjudicar la privacidad de las transacciones vía Internet. Pero existen otras amenazas que pueden afectar al buen funcionamiento tanto de las empresas online como a particulares.

Los temidos virus informáticos son programas capaces de alterar el desarrollo de nuestra computadora y destruir o modificar los datos almacenados. Para ello es necesario tener precaución con los archivos que descargamos o incorporamos mediante discos duros y estar prevenido mediante el uso de un buen antivirus.

Los **antivirus** son programas destinados a detectar y combatir estas amenazas informáticas. Deben estar siempre alerta para ser capaces de actuar antes de que el virus se ejecute y estar actualizados permanentemente, ya que a diario aparecen nuevos programas malintencionados. Además, es aconsejable que puedan realizar revisiones de una forma rápida y no interferir en las actividades que desarrolla la computadora. Otra medida de protección interesante es el **Firewall**, que actúa como cortafuegos, filtrando la información en función de las instrucciones con las que se haya configurado. Se trata de una herramienta para realizar una criba de información potencialmente dañina, aunque su labor es simplemente de filtrado y no de detección específica de virus.

Amenazas en el eCommerce

A pesar del incremento en las medidas de protección al usuario, todavía existen algunas amenazas que pueden exponer y poner en peligro nuestro equipo y nuestros datos personales y bancarios. A continuación veremos algunas de estas amenazas y conoceremos la forma más segura para poder evitarlas.

- **Pishing.** Se trata de un abuso informático que consiste en la suplantación de identidad, ya sea personal o empresarial, para que el usuario reciba una comunicación electrónica que simule ser oficial y facilite los datos personales, bancarios o contraseñas que solicite el estafador.

  Se trata de un delito a nivel global, y una de sus formas más corrientes es la de hacerse pasar por una entidad bancaria para solicitar números de tarjeta de crédito, contraseñas de acceso, códigos PIN, y credenciales necesarios para llevar a cabo operaciones financieras.
- **Malware.** Es otra técnica dañina basada en un software hostil y malicioso que se integra en el equipo del usuario sin su consentimiento. La conciencia social acerca de la seguridad y las estafas en Internet han hecho que los usuarios sean más cautelosos con los posibles engaños ocasionados por el pishing, y por ello se ha incrementado la tendencia de este nuevo sistema fraudulento, ya que se puede instalar en la computadora sin conocimiento de la víctima.

  El malware puede incluir virus, troyanos, gusanos, spyware, adware, etc. y su finalidad es similar a la del pishing, tratando de conseguir contraseñas, datos o dirigir al usuario a webs falsas.
- **Scam.** Proviene del término inglés "estafa" y consiste en la acción delictiva que implica al comercio electrónico. Habitualmente se sirve del uso de perfiles fraudulentos para comercializar productos inexistentes y engañar al usuario gracias a la reputación del vendedor original. No obstante, también pueden considerarse scam los correos que prometen premios o donaciones inexistentes previo pago de una suma de dinero.
- **Otras prácticas.** Desgraciadamente hay muchos tipos de estafas por medio de la red. El **carding** y **skimming** se basan en la copia de las bandas magnéticas de las tarjetas para su uso indebido y el acceso a datos personales y bancarios. El **crimeware** consiste en el robo de contraseñas por medio de capturas de vídeo o registro de pulsaciones del teclado. El **clickjacking** afecta a los navegadores y permite al atacante obligar a hacer clic en cualquier vínculo que desee sin que el usuario sea consciente de ello, y pudiendo dirigir la navegación hacia páginas infectadas. El **malversting** suma de los conceptos de malware y advertising

(publicidad) implica el establecimiento de trampas en webs de confianza a partir de un código malicioso en medio de la publicidad.

Para prevenir este tipo de amenazas se recomienda:

- Instalar uno o varios antivirus que detecten software y códigos maliciosos que puedan sustraer información de nuestra computadora.
- Evitar acceder a enlaces sospechosos, correos en otros idiomas, premios desconocidos o webs de dudosa reputación.
- Verificar el dominio y el protocolo HTTPS para evitar ingresar información en sitios falsos.
- Utilizar contraseñas seguras y alfanuméricas para evitar accesos peligrosos.
- Evitar formularios sospechosos que puedan solicitar más información de la necesaria.
- En caso de duda, ponerse en contacto con el proveedor para validar cualquier información susceptible de estafa.

6.7 ASPECTOS LEGALES EN EL ECOMMERCE

Suele decirse que en el juego de los negocios los ganadores no son los mejores sino los que dominan el juego. Para ello es necesario conocer las reglas o las estructuras legales y consideraciones jurídicas que amparan la forma de llevar a cabo un comercio electrónico. Y es que el auge de las nuevas tecnologías y del eCommerce ha obligado a las autoridades a mostrarse firmes para evitar amenazas de un negocio en constante cambio y ser consecuentes con las leyes establecidas en cada país. Por ello es necesario conocer los aspectos jurídicos que rodean al eCommerce y permanecer dentro de un marco legal que evite sorpresas desagradables para una compañía y sus clientes.

6.7.1 LOPD

La Ley Orgánica de Protección de Datos de Carácter Personal (LOPD) es la encargada de velar por el derecho a la intimidad y privacidad de los usuarios a la hora de realizar trámites mediante nuevas tecnologías. Se trata de una ley que se adapta al movimiento actual de Internet en constante cambio y que sustituye a la LORTAD (Ley Orgánica de Regulación del Tratamiento Automatizado de Datos).

Cualquier empresa que utilice bases de datos que contengan información personal de sus usuarios es responsable de esos datos y debe seguir las principales obligaciones de la LOPD para garantizar la privacidad y el cumplimiento de la ley y el artículo 18.4 de la Constitución Española: "*La Ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos*".

Entre las principales obligaciones que deben seguirse para un correcto uso de la LOPD encontramos las siguientes:

- Todos los datos deben darse de alta en la Agencia Española de Protección de Datos. Esta notificación no tiene ningún coste y puede hacerse mediante el Programa NOTA desde la página www.agpd.es
- Debe elaborarse un Documento de Seguridad y se debe mantener actualizado.
- Es necesario contar con la legitimidad de los usuarios a la hora de obtener los datos incluyendo un aviso legal bien visible en materia de protección de datos.
- Deben establecerse unas medidas de seguridad, técnicas y organizativas a la hora de crear un fichero de datos personales.

Es muy importante cumplir estos requisitos para evitar sanciones, ya que actividades como la cesión de información sin consentimiento del afectado se considera una infracción muy grave que puede alcanzar los 600.000 €.

En función de la tipología de datos personales que puedan almacenarse en un fichero, pueden distinguirse tres niveles diferentes de seguridad:

- El nivel básico es el que hace referencia a los datos personales básicos, como el nombre, dirección, teléfono, correo electrónico, etc.
- El segundo nivel de seguridad es el que contiene datos económicos o fiscales del usuario.
- El nivel de máxima seguridad es el que hace referencia a datos médicos, creencias religiosas o ideología personal.

Agencia de protección de datos

Para garantizar el cumplimiento de la LOPD, existe la Agencia de Protección de Datos, que controla el uso de esta ley a la hora de establecer derechos, acceso a determinada información o cancelaciones y modificaciones de datos. A través de la LOPD se gestionan las reclamaciones de afectados por incumplimientos de privacidad y se promueve el buen uso y concienciación de los datos vía Internet, así como el derecho a la intimidad.

6.7.2 Propiedad intelectual

EL TRLPI o Texto Refundido de la Ley de Propiedad Intelectual es el encargado de velar por los derechos de la propiedad intelectual. Esta ley implica cómo gestionar los contenidos propios para un sitio web así como los contenidos de terceros. De todos modos no hay que olvidar que a nivel de contenido, las ideas no se pueden registrar o proteger, tan solo podemos hacerlo con la forma en la que estas ideas se plasman y toman forma.

Entre los elementos que se pueden proteger según la ley de Propiedad intelectual encontramos los siguientes:

- El texto y contenido de la página.
- El diseño y grafismo del sitio.
- El código fuente de la web.

También será necesario obtener una licencia por escrito en caso de que la web incluya obras o fragmentos de terceros.

6.7.3 Ley de servicios de la sociedad de la información

La ley LSSI (o LSSICE) hace referencia a la Ley de Servicios de la Sociedad de la Información y el Comercio Electrónico, y agrupa todas las normas que regulan la contratación por vía electrónica. La LSSI afecta tanto al comercio electrónico como a las contrataciones en línea, información, publicidad y servicios de intermediación.

Esta ley se aplica sobre toda aquella actividad realizada por Internet y medios electrónicos que tengan carácter comercial y ánimo de lucro. Se incluyen también todos aquellos servicios que aun siendo gratuitos para el usuario, constituyen una actividad económica para su responsable que recibe ingresos directos o indirectos (por medio de publicidad o patrocinio).

Entre los perfiles que pueden prestar servicios de Internet sobre los que se aplica la LSSICE, se pueden diferenciar 3 categorías:

- **Empresas**: personas jurídicas con actividades lucrativas por medio de la red.
- **Particulares**: personas físicas con actividades lucrativas por medio de la red.
- **Proveedores de Servicios de Intermediación**: empresas que ofrecen conexión de Internet a clientes (ISP), servicios de almacenamiento de datos, servidores y buscadores.

6.7.4 Obligaciones para el cumplimiento de la LSSICE

Los responsables de la página web deben mostrar la siguiente información:

- Nombre o denominación y datos de contacto: domicilio y teléfono, fax o email.
- NIF.
- Número de inscripción en el Registro Mercantil (en caso de estar registrado).
- Información detallada sobre el coste de productos o servicios, incluyendo cualquier gasto adicional que pueda variar el coste.
- En caso de estar adheridos a un código de conducta, deben especificarlo.

- Si se trata de una actividad que requiera una autorización administrativa para poder ejercerse, deben especificar el título o certificado que les acredita como hábiles para realizar dicha actividad.

En caso de realizar contratos online, los prestadores de servicios deberán incluir la siguiente información:

- Trámites que deben seguirse para hacer efectivo el contrato.
- Medios técnicos disponibles para modificar y corregir los datos introducidos.
- Si el documento del contrato será archivado y si se podrá tener acceso a él.
- Idioma de formalización del contrato.
- Condiciones generales a las que está sujeto el contrato.

En caso de realizar publicidad en sus páginas web, las empresas o particulares deberán identificar de manera clara quién es el anunciante y dejar patente el carácter publicitario del anuncio.

En el caso de los Proveedores de Servicios de Intermediación, tendrán la obligación de colaborar con órganos públicos siempre que sea necesario. Además, deberán informar a sus usuarios de los medios aplicados para garantizar la seguridad de sus datos y los disponibles en el mercado como antivirus o programa anti-espías e informar de las responsabilidades a la hora de acceder a Internet con fines ilícitos.

Las infracciones por el incumplimiento de la ley LSSI se pueden catalogar en tres grupos: leves (hasta 30.000 euros), graves (entre 30.000 y 150.000) y muy graves (entre 150.000 y 600.000).

6.7.5 Derechos del usuario

Gracias a esta ley, el usuario de Internet dispone de determinados derechos y garantías a la hora de navegar y hacer uso de la Red para el comercio electrónico. Tiene derecho a recibir toda la información relativa a la empresa o particular que ofrece el servicio, como su nombre, domicilio, email, etc. así como el precio real de los artículos que pueden ofrecer.

En lo relativo a la publicidad, cuentan con la garantía de conocer la identidad del anunciante y no recibir mensajes promocionales no deseados o a dejar de recibirlos en caso de que hubieran sido aceptados.

A la hora de contratar un servicio, tienen derecho a conocer todo el procedimiento para llevarlo a cabo, incluyendo todos los costes adicionales y obteniendo un comprobante del pago del vendedor.

6.7.6 LAESCP

Con el fin de desarrollar una administración moderna y eficaz, se crea la Ley de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAESCP), que implica la posibilidad de que los ciudadanos se relacionen electrónicamente con las administraciones públicas. De esta manera se pretende impulsar el uso de la Administración por medio de sus servicios electrónicos a la hora de realizar registros, pagos, trámites o notificaciones.

Para poder aplicar esta ley, es importante la existencia de la firma electrónica, que dispone de la misma validez legal que una firma manuscrita tradicional, lo que facilita el camino hacia una administración moderna que ahorre desplazamientos innecesarios, almacenamientos de papeles y pérdidas de tiempo.