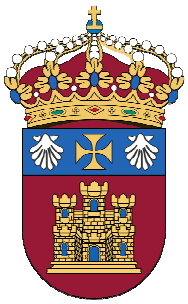
Análisis de la situación actual de EL CAMINO S.L. (Productos y Servicios en el Camino de Santiago)



Universidad de Burgos

Autor del proyecto: Jesús Hernando Burgos
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 del documento

1. INTRODUCCIÓN

El objeto del presente documento es analizar la situación actual de la empresa **EL CAMINO S.L.** (por expreso deseo de la empresa se ha cambiado el nombre, aunque todo lo que se trata en el documento son datos reales) en relación a:

- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos (en adelante LOPD),
- Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y de comercio electrónico (LSSI)
- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley 11/2007, de 22 de Junio, de acceso electrónico de los ciudadanos a los Servicios Públicos.
- Ley 5/1998, de 6 de Marzo, sobre la protección jurídica del las bases de datos.
- Y otras muchas vistas a lo largo del Magister.

Así como las posibles soluciones en caso de que la situación actual no cumpla la normativa vigente.

EL CAMINO S.L. es una empresa dedicada al Camino de Santiago y sus peregrinos. Ofrece información gratuita desde su web, de los distintos Caminos de peregrinación españoles a Santiago (23 reconocidos). Esto incluye información de las distintas etapas que forman cada uno de los caminos, con descripción detallada de los pueblos, aldeas y ciudades por los que discurren, así como de los distintos servicios disponibles en cada sitio (dónde dormir, dónde comer, cultura del lugar, tiendas, asistencia sanitaria, folklore…).

Como buena empresa necesita ingresos para subsistir, para ello dispone de varios sistemas de conseguir ingresos:

Tienda online en la que ofrece diversos productos demandados por los peregrinos. Entre estos productos destacan las guías en papel de los caminos más demandados, algunas de las cuales son escritas y editadas por ellos mismos.

Servicios al peregrino como el transporte de mochilas, transporte de bicis, alquiler de bicis y seguro de asistencia en viaje. Algunos de estos servicios se realizan completamente por la empresa o con la colaboración de terceras empresas.

Venta al por mayor de los mismos productos de la web, a minoristas y asociaciones a lo largo del Camino Francés.

Cobro de una cuota anual a los hoteles, restaurantes y tiendas que quieran mostrar todos sus servicios en la web.

Cobro de una cantidad variable (en función del tamaño y el tiempo) por poner un banner publicitario en la página principal de la web.

Para incrementar el número de visitas y promocionar los distintos servicios, envía un boletín quincenal a sus cerca de 10.000 suscriptores. Dispone así mismo de una página en Facebook donde informar directamente a los peregrinos y recibir de la misma forma sus inquietudes, para aplicarlas a la web.

2. ANÁLISIS DE LA LOPD EN LA EMPRESA

2.1.- INTRODUCCIÓN A LA LOPD

Antes de comenzar a analizar los principales aspectos de la Ley de Protección de Datos y cómo afecta esto a la empresa que estamos analizando, conviene hacer una introducción para entender conceptos tan importantes como: qué es la protección de datos, qué es un dato de carácter personal, a quién afecta o qué protege…

El artículo 18.4 de la Constitución Española dice lo siguiente:

"*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*".

En base a esto podemos decir que la protección de datos es "*el amparo debido a los ciudadanos contra la posible 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*".

Cabe destacar que el Tribunal Constitucional en la Sentencia 292/2000, de 30 de noviembre, dictamina que el derecho a la protección de datos es un derecho fundamental, autónomo e independiente al derecho a la intimidad.

En esta sentencia se resalta (primer párrafo del Fundamento Jurídico 6) que el derecho fundamental a la protección de datos "*garantiza a los individuos un poder de disposición sobre esos datos, que nada vale si el afectado desconoce qué datos son los que poseen terceros, quienes los poseen y con qué fin*".

La Agencia Española de Protección de Datos es el organismo encargado por la LOPD de velar por el cumplimiento de la legislación sobre protección de datos y garantizar a los individuos el cumplimiento de sus derechos a este respecto.

Una vez que sabemos qué es la Ley de Protección de Datos, debemos aclarar qué es un dato de carácter personal. El artículo 3 de la LOPD en su letra a) lo define como:

"*cualquier información concerniente a personas físicas identificadas o identificables*".

Esta definición se amplía en el apartado 1.f del artículo 5 del R.D. 1720/2007 para poder recoger todas las posibilidades en cuestión de medios, condiciones y procedimientos, quedando la definición como:

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

Otras definiciones a tener en cuenta que aparecen en el artículo 3 de la LOPD son:

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

Dentro de esta definición entran tanto los ficheros manuales (típicos archivadores en los cuales la información esta separa en carpetas), como los ficheros automatizados (puede ser la misma información de los ficheros físicos pero en soporte electrónico, bien sean bajo una base de datos u otro método de organización).

En el siguiente punto se mostrarán los ficheros que tiene la empresa y los tipos de datos que almacenan.

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

El tratamiento de los datos es una de las 3 fases del tratamiento (valga la redundancia).

Responsable del fichero o tratamiento: *"la persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que decida sobre la finalidad, contenido y uso del tratamiento".*
De la ley deducimos que el responsable es el que decide en la empresa qué fines tendrán los ficheros y qué tratamiento tendrán.

Afectado o interesado: *"la personal física titular de los datos que sean objeto de tratamiento a que se refiere el apartado c) del presente artículo 3".*
Quedan excluidas las personas jurídicas, ya que se hace mención exclusivamente a las personas físicas. Hay que tener en cuenta, que en ocasiones se guardan datos de carácter personal del representante de la empresa, por lo que esos datos estarían afectados.

Disociación de los datos: *"todo tratamiento de datos personales de modo que la información que se obtenga no pueda asociarse a personas identificadas o identificables".*
Es un procedimiento por el cual, se pueden mostrar los resultados de un tratamiento, siempre que no haya datos de carácter personal que permitan asociarlo a la persona afectada. Este es un procedimiento típico de las estadísticas.

Encargado del tratamiento: *"la persona física o jurídica, autoridad pública, servicio o cualquier otro organismo que, solo o conjuntamente con otros, trate datos de carácter personal por cuenta del responsable del tratamiento".*
La figura de encargado del tratamiento surgió de la necesidad de contratar empresas que realizan un servicio de tratamiento de datos para terceros. El responsable del fichero decide los fines, contenidos y uso, pero no tiene por qué hacer el tratamiento.

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

El consentimiento salvo que la ley disponga de lo contrario, es necesario para el tratamiento de los datos.

Cesión o comunicación de los datos: *"toda revelación de datos realizada a una persona distinta del interesado".*
Cualquier acceso a los datos por una persona no autorizada, y a la que no se le haya dado un consentimiento explícito (salvo excepciones), es una cesión de datos. No será cesión cuando los datos se ceden para la prestación de un servicio.

En las siguientes páginas de este documento se realizará el estudio de la Protección de Datos en la empresa El Camino S.L. mencionada en la introducción del documento.
El tratamiento de los datos se divide en tres fases:
Recogida de datos:
Tratamiento de los datos:
Uso y/o cesión de los datos:

La estructura del estudio se hará siguiendo lo aprendido durante el magíster. Primero se analizará si se tienen en cuenta los principios de la protección de datos por parte de las personas que intervienen en el tratamiento.
Se continuarán con los derechos que asisten a los interesados y que derivan de los principios y por último los procedimientos que garantizan el ejercicio efectivo de los derechos.

Tanto los principios como los derechos deben ser tenidos en cuenta en las tres fases del tratamiento.
El no cumplimiento por parte de **EL CAMINO S.L.** de los principios, o la negativa al ejercicio de los derechos de los interesados en cualquier fase de las existentes para el tratamiento de la información, o un acceso o comunicación indebidas a los datos personales, pueden acarrear una sanción a **EL CAMINO S.L.** que dependiendo de la criticidad de lo acaecido así será lo económico de la sanción.

2.2.- FICHEROS REGISTRADOS

La empresa objeto de estudio El Camino S.L. es una empresa privada y como tal, tiene dados de alta en la Agencia Española de Protección de Datos 2 ficheros de titularidad privada:
Fichero de Clientes y Proveedores y Fichero de Gestión de personal.
Si acudimos a la página web de la Agencia podemos ver las características de estos ficheros:

Nombre del fichero: *CLIENTES Y PROVEEDORES*
Dirección: *C/ XXXXXX Nº X, Bajo.*
Código Postal - Población: *0900X-Burgos*.
Provincia - País: *Burgos-ESPAÑA*.
Finalidad: *Fichero con datos de carácter personal de los clientes y proveedores para la gestión integral de los mismos*.
Tipificación de la finalidad: *Gestión de clientes, contable, fiscal y administrativa; Publicidad y prospección comercial; Comercio electrónico;*

Tipos de datos, estructura y organización del fichero:
Otros datos especialmente protegidos:
Datos de carácter identificativo: *D.N.I./N.I.F.; Dirección; Firma/Huella; Teléfono; Nombre y Apellidos;*
Otros tipos de datos: *Datos de características personales; Datos de información comercial; Datos de transacciones;*
Sistema de tratamiento: *Mixto*.

Origen y procedencia de los datos:
Origen: *El propio interesado o su representante legal;*
Colectivos: *Clientes y usuarios; Proveedores; Personas de contacto; Asociados o miembros; representante legal; solicitantes; beneficiarios*.

Cesión o comunicación de datos:

Destinatarios: *Organizaciones o personas directamente relacionadas con el responsable; Administración tributaria; Otros órganos de la administración pública; Bancos, cajas de ahorro y cajas rurales; administración pública con competencia en la materia; Entidades aseguradoras; Asociaciones y Organizaciones sin ánimo de lucro*.

Transferencia internacional:
Destinatarios en países con nivel de protección adecuado: *No hay.*
Destinatarios en países sin nivel de protección adecuado: *No hay.*
Otros destinatarios de Transferencias Internacionales: *No hay.*
Transferencias internacionales con autorización del Director de la AEPD: *No hay.*

Nombre del fichero: ***GESTION DE PERSONAL***
Dirección: *C/ XXXXXX Nº X, BAJO*
Código Postal - Población: *0900X-BURGOS*
Provincia - País: *BURGOS-ESPAÑA*
Finalidad: Fichero con datos de carácter personal de los trabajadores para la gestión laboral y la realización de las nóminas.
Tipificación de la finalidad: *Prevención de riesgos laborales; Recursos humanos; Gestión de nominas.*

Tipos de datos, estructura y organización del fichero:
Otros datos especialmente protegidos:
Datos de carácter identificativo: *D.N.I./N.I.F.; Nombre y Apellidos; Teléfono; Imagen/Voz; Firma/Huella; Dirección; Num.S.S./Mutualidad;*
Otros tipos de datos: *Datos de características personales; Datos de circunstancias sociales; Datos académicos y profesionales; Datos de detalles de empleo; Otros tipos de datos; Datos de transacciones; Datos económicos financieros y de seguros*.
Sistema de tratamiento: *Mixto*.

Origen y procedencia de los datos:

Origen: *El propio interesado o su representante legal;*
Colectivos: *Empleados*.

Cesión o comunicación de datos:
Destinatarios: *Organismos de la Seguridad Social; Administración tributaria; Bancos, cajas de ahorro y cajas rurales; Entidades aseguradoras;*

Transferencia internacional:
Destinatarios en países con nivel de protección adecuado: *No hay.*
Destinatarios en países sin nivel de protección adecuado: *No hay.*
Otros destinatarios de Transferencias Internacionales: *No hay.*
Transferencias internacionales con autorización del Director de la AEPD: *No hay.*

Resultado del análisis de los ficheros de la empresa
La comunicación de datos se realiza siempre mediante prestación de servicios, amparados por el artículo 12 de la LOPD. De este modo por cada uno de estas empresas que prestan servicio debe existir un contrato de prestación de servicios. En el documento de seguridad del punto 2.6 se ha añadido un documento tipo de prestación de servicios.

El fichero de empleados originalmente almacenaba también datos de solicitantes de empleo. Tras el análisis se ha sugerido eliminar esto del fichero, ya que la empresa ha mantenido el mismo personal desde su inicio y no se prevé que vaya a aumentar en el futuro. De esto modo también disminuimos el nivel de seguridad del fichero de Medio a Básico. Esto permite relajar las medidas de seguridad en los accesos a los ficheros, la figura de responsable de seguridad pasa a ser optativa y se ahorran la auditoría bienal.

En el documento de seguridad que se encuentra en el punto 2.6 del análisis de la protección de datos podemos consultar los siguientes puntos relativos a estos ficheros:

- El responsable de los ficheros.
- La/s persona/s que tienen acceso y el tipo de acceso.
- El nivel de seguridad de los ficheros
- Las medidas de seguridad adoptadas, de acuerdo al nivel.

2.3.- PRINCIPIOS DE LA PROTECCIÓN DE DATOS

EL CAMINO S.L. como responsable del fichero y en este caso, también del tratamiento debe seguir unas reglas o principios que aseguren que los datos que va a recoger de sus usuarios son correctos, que les ha informado convenientemente, que el tratamiento se realiza sobre los fines para los que han sido recogidos y consentidos por el usuario y que su uso se ajusta a lo autorizado.

Con estas medidas lo que se pretende es proteger el tratamiento de la información y por tanto al titular de los datos, y no a la información en sí, ya que una información que no es tratada se convierte en un mero dato, y un dato por sí solo no nos indica nada y por tanto no es necesario protegerlo.

Los escenarios en los que la empresa **EL CAMINO S.L.** recoge datos para sus ficheros son los siguientes:

Caso 1	Petición de información, sobre cómo conseguir la credencial del peregrino.
Caso 2	Suscripción para el envío de un boletín quincenal acerca del Camino de Santiago.
Caso 3	Petición de cuenta de usuario para el uso de los foros.
Caso 4	Inscripción de las asociaciones del Camino de Santiago en un buscador.
Caso 5	Compra de algún artículo en la tienda online.
Caso 6	Contrato para anunciar un albergue, restaurante, hotel, tienda… situada en algún punto del Camino de Santiago.
Caso 7	Servicio de transporte de bicicletas al Camino y/o de regreso al hogar.
Caso 8	Solicitud de un seguro de asistencia en viaje.
Caso 9	Contratación de un nuevo empleado por la empresa.
Caso 10	Contratación de servicios o materias primas con un nuevo proveedor.

A continuación para el análisis de los principios, se seguirá el orden que marca la ley. Algunos autores marcan como primer principio la información al usuario, ya que no se debe recoger información si el usuario no ha sido convenientemente informado.

2.3.1 Calidad de los datos (art.4)

En el principio de Calidad de los datos se trata de regular, que los datos que se recogen para su tratamiento, son adecuados, pertinentes y no excesivos para el fin/es que se tienen previstos y que estos se actualizan o cancelan si no coinciden con la realidad.

El diseño de un buen formulario de recogida de datos es fundamental, ya que de ello deriva el resto del tratamiento. Un formulario con un exceso de datos puede llevar a un consentimiento más severo por parte del usuario, lo que a su vez puede aumentar el nivel de seguridad de los ficheros y las medidas de seguridad necesarias para mantenerlos.

La LOPD lo define de la siguiente manera:

" 1. Los datos de carácter personal sólo se podrán recoger para su tratamiento, así como someterlos a dicho tratamiento, cuando sean adecuados, pertinentes y no excesivos en relación con el ámbito y las finalidades determinadas, explícitas y legítimas para las que se haya obtenido.

2. Los datos de carácter personal objeto de tratamiento no podrán usarse para finalidades incompatibles con aquellas para las que los datos hubieran sido recogidos. No se considerará incompatible el tratamiento posterior de éstos con fines históricos, estadísticos o científicos.

3. Los datos de carácter personal serán exactos y puestos al día de forma que respondan con veracidad a la situación actual del afectado.

4. Si los datos de carácter personal registrados resultaran ser inexactos, en todo o en parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificados o completados, sin perjuicio de las facultades que a los afectados reconoce el artículo 16.

5. Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes para la finalidad para la cual hubieran sido recabados o registrados.
No se conservarán en forma que permita la identificación del interesado durante un periodo superior al necesario para los fines en base a los cuales hubieran sido recabados o registrados.
Reglamentariamente se determinará el procedimiento por el que, por excepción, atendidos los valores históricos, estadísticos o científicos de acuerdo con la legislación específica, se decida el mantenimiento íntegro de determinados datos.
6. Los datos de carácter personal serán almacenados de forma que permitan el ejercicio del derecho de acceso, salvo que sean legalmente cancelados.
7. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos".

A continuación se resume en la siguiente tabla los datos recogidos en cada uno de los casos mencionados y los fines para los que se recogen:

Nº de Caso	**Datos solicitados**	**Fin/es**
Caso 1º	Nombre, Apellidos y Correo electrónico	Ofrecer información.
Caso 2º	Correo electrónico	Ofrecer información y boletín electrónico.
Caso 3º	Nick, contraseña y correo electrónico	Control de accesos.
Caso 4º	Nombre de la asociación, del presidente/secretario o persona de contacto. Tfnos y/o emails de contacto y dirección web.	Ofrecer información y ofertas comerciales.
Caso 5º	Nombre, apellidos, dni, tfno, dirección, provincia/estado, localidad, cp, pais, email.	Gestionar el pedido y ofertas comerciales.
Caso 6º	Datos personales del dueño/gerente del local que se va a anunciar así como de los servicios que proporciona.	Ofrecer información.
Caso 7º	Nombre, apellidos, dni, tfno, dirección, provincia/estado, localidad, cp, pais,	Gestionar el pedido y ofertas comerciales.

	email, fecha de inicio y fecha de fin, nº de bicicletas, lugar de inicio y lugar de regreso.	
Caso 8º	Nombre, apellidos, fecha de nacimiento dni, tfno, dirección, provincia/estado, localidad, cp, pais, email, fecha de inicio y fecha de fin.	Gestionar el pedido y ofertas comerciales.
Caso 9º	Datos personales y de contacto, datos para la realización de las nóminas.	Realizar nóminas y pagos.
Caso 10º	Datos del proveedor (empresa o comercial). Tfnos y/o emails de contacto y dirección web. Productos o servicios que ofrece y sus precios.	Gestionar los pedidos

Resultado del análisis del artículo 4º

Los datos recogidos son apropiados y no excesivos para cada caso particular y se actualizan cuando el usuario así lo solicita.

Los datos son suministrados por el propio interesado y se usan para los fines propios de cada caso.

Una vez completados los fines para los que fueron recogidos, y las posibles responsabilidades con las administraciones públicas, los datos se borran de los ficheros.

Para una mayor claridad a la hora de analizar los casos anteriores vamos a agruparlos según su tipología del siguiente modo:

Casos del 1º al 4º: Son personas que visitan la web o el local de la empresa en busca de información. A partir de ahora los llamaremos **Visitantes** (el tratamiento es el mismo que los clientes, pero en general los datos que almacenamos de ellos son mínimos).

Casos del 5º al 8º: Son personas generalmente físicas, con los que se establece una relación contractual, bien mediante la compra de

artículos/servicios o anunciando sus locales comerciales a cambio de una cuota. A partir de ahora los llamaremos **Clientes**.

Caso 9º: Son las personas que trabajan actualmente en la empresa. Tienen una relación contractual, han sido instruidas en la LOPD, han firmado la cláusula de secreto profesional y han recibido su copia del documento de seguridad. A partir de ahora los llamaremos **Empleados**.

Caso 10º: Son los datos personales de los proveedores actuales de la empresa, ya sea de artículos como de servicios. Los datos de proveedores antiguos se guardan un tiempo prudencial, por si hay que volver a negociar con ellos. Habitualmente se tienen datos personales para un mejor contacto, por lo que se deben tener en cuenta a la hora del análisis. A partir de ahora los llamaremos **Proveedores**.

2.3.2 Derecho de información (art.5)

El siguiente artículo trata sobre el derecho de información que tiene el interesado según la Ley. Es tanto un principio como un derecho, ya que el responsable del fichero debe informar en el momento previo a la recogida de datos y el usuario tiene derecho a esa información.
El artículo se desarrolla como sigue:

"1. Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso e inequívoco:
De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos y de los destinatarios de la información.
Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Cuando el responsable del tratamiento no esté establecido en el territorio de la Unión Europea y utilice en el tratamiento de datos medios situados en territorio español, deberá designar, salvo que tales medios se utilicen con fines de trámite, un representante en España, sin perjuicio de las acciones que pudieran emprenderse contra el propio responsable del tratamiento.

2. Cuando se utilicen cuestionarios u otros impresos para la recogida, figurarán en los mismos, en forma claramente legible, las advertencias a las que se refieren el apartado anterior.

3. No será necesaria la información a que se refieren las letras b), c) y d) del apartado 1 si el contenido de ella se deduce claramente de la naturaleza de los datos personales que se solicitan o de las circunstancias en que se recaban.

4. Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento de registro de los datos, salvo que ya hubiera sido informado con anterioridad, del contenido del tratamiento, de la procedencia de los datos, así como de lo previsto en las letras a), d) y e) del apartado 1 del presente artículo.

5. No será de aplicación de lo dispuesto en el apartado anterior, cuando expresamente una ley lo prevea, cuando el tratamiento tenga fines históricos, estadísticos o científicos, o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados, a criterio de la Agencia de Protección de Datos o del organismo autonómico equivalente, en consideración al número de interesados, a la antigüedad de los datos y a las posibles medidas compensatorias.

Asimismo, tampoco regirá lo dispuesto en el apartado anterior cuando los datos procedan de fuentes accesibles al público y se destinen a la actividad de publicidad o prospección comercial, en cuyo caso, en cada comunicación que se dirija al interesado se le informará del origen de los datos y de la identidad del responsable del tratamiento así como de los derechos que le asisten".

Una vez conocido lo que dice la Ley sobre el derecho de información, se va a analizar sobre los mismos casos, si **EL CAMINO S.L.** cumple con la Ley y en caso contrario, qué tendría que cambiar para hacerlo.

Resultado del análisis del artículo 5º

Todos los casos excepto el 1º y el 3º informan correctamente de todos los aspectos que marca el artículo 5º. Los datos son proporcionados siempre por el interesado. Esto es claramente verificable cuando acuden personalmente al local de la empresa.

En el caso de que los datos se proporcionen desde la web se envía un correo electrónico como confirmación del hecho.

Los campos obligatorios están convenientemente señalizados. No se especifica la consecuencia de no aceptación, ya que se considera obvio que es el no uso del servicio que se pretende usar.

Ej. Si el gerente de un local anexo al Camino no quiere que se traten sus datos, la consecuencia lógica es que no podrá mostrar los servicios que ofrece, en el listado de locales del tramo del Camino correspondiente.

Volviendo a los casos 1º y 3º la empresa consideraba que como no se realiza tratamiento con estos datos, no es necesaria la información.

En la definición de tratamiento de datos se incluye el almacenamiento de los mismos, por lo que se podría deducir que sería necesario. También hemos visto que la información que no se trata es un dato y los datos no necesitan protección, además en esos casos en particular, es poco probable que se puedan asociar estos datos a personas concretas, por lo que difícilmente se podrían catalogar como datos de carácter personal.

Aún y con todo, sería recomendable que se añadiera la cláusula de información para evitar problemas futuros.

2.3.3 Consentimiento del afectado (art.6)

El siguiente paso tras la información al interesado es que éste, de su consentimiento para el tratamiento de sus datos. El artículo 6 de la Ley lo expresa del siguiente modo:

"1. El tratamiento de los datos de carácter personal requerirá el consentimiento inequívoco del afectado, salvo que la ley disponga otra cosa.

2. No será preciso el consentimiento cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias; cuando se refieran a las partes de un contrato o precontrato de una relación negociad, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento; cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado en los términos del artículo 7, apartado 6, de la presente Ley, o cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado.
3. El consentimiento a que se refiere el artículo podrá ser revocado cuando exista causa justificada para ello y no se le atribuyan efectos retroactivos.
4. En los casos en los que no sea necesario el consentimiento del afectado para el tratamiento de los datos de carácter personal, y siempre que una ley no disponga lo contrario, éste podrá oponerse a su tratamiento cuando existan motivos fundados y legítimos relativos a una concreta situación personal. En tal supuesto, el responsable del fichero excluirá del tratamiento los datos relativos al afectado".

La ley define distintos tipos de consentimientos en función del tipo de dato que se está pidiendo. Los tipos de consentimientos son los siguientes:

- El consentimiento "tácito" es aquel en el cual dicho consentimiento no se deriva de actos del interesado sino precisamente "de su falta de actuación", es decir, de su silencio.
- El consentimiento "expreso" es aquel que exige que se declare de forma clara e inequívoca por parte del interesado que acepta o consiente el tratamiento o la cesión de los que se le informa, mediante la expresión de su voluntad, que podrá ser por escrito, verbalmente, mediante comunicación telemática o por cualquier otro medio.

La ley exigirá el consentimiento expreso del afectado para el tratamiento de datos de carácter personal, cuando éstos hagan referencia al origen racial, salud y la vida sexual, salvo que una ley disponga lo contrario, así lo indica en su apartado 3 el artículo 7 de la LOPD al establecer que:

"Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente"

La ley exigirá el consentimiento expreso y por escrito del afectado para el tratamiento de datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Indicándolo así en el apartado 2 del artículo 3 de la LOPD al establecer que:

"Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado"

Fuera de estos casos, el consentimiento debe reunir simplemente la característica de ser inequívoco, permitiéndose de esta forma el consentimiento tácito.

Excepciones a la necesidad de consentimiento del afectado:

- Cuando así lo disponga una ley.
- Cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones Públicas en el ámbito de sus competencias.
- Cuando se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento.
- Cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado, porque resulte necesario para la prevención o para el diagnostico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que

dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta a una obligación equivalente de secreto.

- Cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por **ELCAMINO S.L.**

Resultado del análisis del artículo 6º

Proveedores:

Si bien el artículo 6.2 LOPD, exceptúa del cumplimiento del deber de información en la recogida de datos a las partes firmantes de contratos o precontratos en relaciones de negocio, cuando la empresa recoge más datos que los estrictamente necesarios para la firma de los contratos con sus proveedores (por ejemplo: datos de persona de contacto), es necesario obtener el consentimiento del afectado para el tratamiento de sus datos de carácter personal en estos casos.

Clientes:

Teniendo en cuenta lo especificado respecto de los proveedores, decir que la situación respecto de los clientes es similar. El consentimiento del afectado para el tratamiento de sus datos personales es necesario en estos casos y se realiza correctamente. Al no haber ni datos especialmente protegidos, ni datos relativos a la salud, es suficiente con el consentimiento tácito.

Empleados:

En el caso de los empleados, el art. 6. 2 de la LOPD exceptúa la obligación de obtener el consentimiento de los afectados por el tratamiento “cuando los datos de carácter personal se refieran a las partes de unan relación laboral”.
No obstante, esta excepción de obtención del consentimiento del afectado para el tratamiento de sus datos de carácter personal, no supone una excepción al

deber de información antes mencionado, por lo que habrá que informar del mismo modo a los empleados.

Visitantes:
En el momento de la recogida de los datos, se le informa de los fines, por lo que al aceptar da su consentimiento tácito al tratamiento con los fines señalados.

En general, falta demostrar la evidencia clara de que se han aceptado los fines. En el caso de los proveedores y los empleados no hay tal problema, ya que los trámites se realizan en papel, por lo que queda la evidencia de la firma contractual.
En el caso de clientes y visitantes es más complejo. El simple hecho de continuar con el proceso de compra no demuestra judicialmente que se han leído y aceptado los términos relativos a los fines y cesión de los datos. Se recomendaría modificar los formularios de este tipo, para que no se pueda avanzar hasta haber aceptado los términos. Aunque no quede una evidencia real, sí que se podría demostrar que técnicamente no es posible continuar sin haber aceptado que se han leído y aceptado los términos.

Se recomienda separar los fines del tratamiento para que el usuario pueda dar consentimiento a cada uno por separado. La empresa considera necesario aceptar todos los fines o ninguno.

Otro punto importante es demostrar que quien da el consentimiento es el titular. Otra vez volvemos a la debilidad de la web.

2.3.4 Datos especialmente protegidos (art.7)

La LOPD confiere una especial protección a lo que llama datos especialmente protegidos (ideología, afiliación sindical, religión, creencias, origen racial, salud y vida sexual).

El artículo 7 detalla los tipos de consentimiento necesario, en función de los datos recogidos, así como si se pueden crear ficheros exclusivos con datos de salud, afiliación sindical o creencias.

"1. De acuerdo con lo establecido en el apartado 2 del artículo 16 de la Constitución, nadie puede ser obligado a declarar sobre su ideología, religión o creencias.
Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.
2. Sólo con el consentimiento expreso y por escrito del afectado podrán ser objeto de tratamiento los datos de carácter personal que revelen la ideología, la afiliación sindical, religión y creencias. Se exceptúan los ficheros mantenidos por los partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas y asociaciones, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, en cuanto a los datos relativos a sus asociados o miembros, sin perjuicio de que la cesión de dichos datos precisará siempre el previo consentimiento del afectado.
3. Los datos de carácter personal que hagan referencia al origen racial, a la salud y a la vida sexual sólo podrán ser recabados, tratados y cedidos cuando, por razones de interés general, así lo disponga una ley o el afectado consienta expresamente.
4. Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.
5. Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.
6. No obstante lo dispuesto en los apartados anteriores, podrán ser objeto de tratamiento los datos de carácter personal a que se refieren los apartados 2 y 3 de este artículo, cuando dicho tratamiento resulte necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de los servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.
También podrá ser objeto de tratamiento los datos a los que se refiere el párrafo anterior cuando el tratamiento sea necesario para salvaguardar el interés vital del

afectado o de otra persona, en el supuesto de que el afectado esté físicamente o jurídicamente incapacitado para dar su consentimiento".

Resultado del análisis del artículo 7º

No se recogen datos relativos al origen racial, vida sexual, ideología, afiliación sindical, religión o creencias de los interesados, por lo que no es aplicable. Los datos relativos a la salud recogidos para la mutua los trata la mutua. Estos datos se llevan en persona a la empresa.

2.3.5 Datos relativos a la salud (art.8)

El artículo 8 detalla quiénes pueden tratar los datos relativos a la salud:

"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."

La definición de los datos de carácter personal relacionados con la salud, lo podemos encontrar en el apartado 1.g, del artículo 5, del RD 1720/2007 que lo define como sigue:

"Las informaciones concernientes a la salud pasada, presente y futura, física o mental de un individuo. En particular, se consideran datos relacionados con la salud de las personas los referidos a su porcentaje de discapacidad y a su información genética"

Resultado del análisis del artículo 8º

No es aplicable en nuestro caso, ya que no se almacenan datos de este tipo. Las bajas de los empleados son inmediatamente enviadas (por uno de los empleados) a la gestoría y a la mutua de la empresa.

2.3.6 Seguridad de los datos (art.9)

La seguridad de los datos es parte fundamental tanto durante el tratamiento de los datos, como mientras los datos sigan almacenados en los ficheros de la empresa. Se debe garantizar que nadie que no tenga derecho a ello pueda acceder, modificar o borrar los datos para poder garantizar su integridad y confidencialidad. El artículo 9 de la ley lo detalla del siguiente modo:

"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 estén 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."

En el apartado 2.7 se encuentra el documento de seguridad donde se especifican con claridad las medidas de seguridad a aplicar en el caso concreto de la empresa que estamos analizando.

2.3.7 Deber de secreto (art.10)

El deber de secreto es fundamental en las 3 fases del tratamiento de los datos y concierne no sólo al titular del fichero y/o al responsable del tratamiento de los datos, si no, a cualquier persona de la empresa que intervenga en cualquier momento del tratamiento o tenga acceso a los datos. El artículo 10 de la Ley lo redacta del siguiente modo:

"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".

Resultado del análisis del artículo 10

Para garantizar el deber de secreto, todos los empleados de **EL CAMINO S.L.** han firmado o deben firmar una cláusula de confidencialidad que podemos encontrar en el documento de seguridad del apartado 2.6 del presente documento.

2.3.8 Comunicación de los datos (art.11)

Como dice el profesor Davara en el Factbook Comercio electrónico:
"la cesión o comunicación de datos se muestra como un punto conflictivo en la ley, ya que se posibilita el cruce de los datos (con toda la intensidad que permite la informática), además de que facilita la utilización de los datos para un uso que no es el mismo para el que se habían recabado".

El artículo 11 de la ley lo define del siguiente modo:
"1. Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.
2. El consentimiento exigido en el apartado anterior no será preciso:
Cuando la cesión está autorizada en una ley.
Cuando se trate de datos recogidos de fuentes accesibles al público.
Cuando el tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.
Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el

ejercicio de las funciones que tiene atribuidas. Tampoco será preciso el consentimiento cuando la comunicación tenga como destinatario a instituciones autonómicas con funciones análogas al Defensor del Pueblo o al Tribunal de Cuentas.
Cuando la cesión se produzca entre Administraciones públicas y tenga por objeto el tratamiento posterior de los datos con fines históricos, estadísticos o científicos.
Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia que requiera acceder a un fichero o para realizar los estudios epidemiológicos en los términos establecidos en la legislación sobre sanidad estatal o autonómica.
3. Será nulo el consentimiento para la comunicación de los datos de carácter personal a un tercero, cuando la información que se facilite al interesado no le permita conocer la finalidad a que destinarán los datos cuya comunicación se autoriza o el tipo de actividad de aquel a quien se pretenden comunicar.
4. El consentimiento para la comunicación de los datos de carácter personal tiene también un carácter de revocable.
5. Aquel a quien se comuniquen los datos de carácter personal se obliga, por el solo hecho de la comunicación, a la observancia de las disposiciones de la presente Ley.
6. Si la comunicación se efectúa previo procedimiento de disociación, no será aplicable lo establecido en los apartados anteriores."

Resultado del análisis del artículo 10

En el caso de **EL CAMINO S.L.** se pide el consentimiento para la cesión de los datos a las empresas asociadas a **EL CAMINO S.L.** aunque nunca se ha producido tal cesión. Los fines de dichas empresas son los mismos que los de **EL CAMINO S.L.** por lo que no son incompatibles.

2.3.9 Acceso a los datos por cuenta de terceros (art.12)

Un tipo más común de acceso a los datos por terceros ocurre cuando la empresa necesita recurrir a los servicios de un tercero y para ello necesita que esta empresa acceda a los datos.

Esto está previsto por la ley en su artículo 12 que dice lo siguiente:

"1. No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.
2. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito o en alguna otra forma que permita acreditar su celebración y contenido, estableciéndose expresamente que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.
En el contrato se estipularán, asimismo, las medidas de seguridad a que se refiere el artículo 9 de esta Ley que el encargado del tratamiento está obligado a implementar.
3. Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.
4. En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente."

Como podemos ver en el punto primero dice que la ley no lo considera comunicación de datos si el acceso es necesario para la prestación de un servicio. Continúa en el punto 2 diciendo que es necesario que exista un contrato en el que se establecen las condiciones de acceso a esos datos.

En el caso de **EL CAMINO S.L.** algunos de los servicios nombrados en la introducción son realizados por terceros. En el documento de seguridad de la empresa (punto 2.6 de este documento), en su anexo 9 están los contratos de prestación de servicios actuales (sólo se ha incluido uno genérico para no alargar en exceso este documento).

Los servicios realizados por terceros son:

- Transporte de bicis al camino y de vuelta a casa.
- Transporte de mochilas/equipaje.
- Seguro de asistencia en viaje.
- Realización de nóminas (empleados).
- Prevención de riesgos laborales (empleados).

2.4.- DERECHOS DE LOS AFECTADOS

Estos derechos de la protección de datos se encuentran contemplados en el Título III de la LOPD.

Los derechos nacen de la necesidad de que el afectado pueda conocer los tratamientos que se están realizando sobre sus datos y que pueda exigir el cumplimiento de los principios que rigen la protección de datos.

Los derechos siempre deben ser ejercidos por el propio titular de los datos (son personalísimos), o por un representante elegido por él a tal fin.

De la misma forma, podrá ejercitar dicho derecho un representante legal cuando el afectado esté en situación de incapacidad o minoría de edad.

EL CAMINO S.L. debe asegurarse que la persona que ejerce los derechos es el titular de los datos y negarse a su prestación en caso contrario. Si todo es correcto debe permitir y facilitar el ejercicio de los derechos.

Estos derechos se consideran independientes, por lo cual no es necesario el requisito previo de uno para el ejercicio de otro.

2.4.1.- Procedimiento de ejercicio de los derechos

El titular de los datos o un representante puede dirigirse mediante una comunicación a EL CAMINO S.L. para ejercer sus derechos. El artículo 25.1 del RD 1720/2007 define la información necesaria como la siguiente:

- Nombre y apellidos del interesado o en su caso persona que lo represente, acompañado de una fotocopia de un documento válido que lo identifique (DNI, pasaporte, firma electrónica, etc..).
- Petición en que se concreta la solicitud.
- Dirección a efectos de notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición que formula en caso que fueran necesarios.

Una vez que se ha recibido la petición y comprobado que cumple los requisitos anteriores, se debe responder al interesado aunque no existan datos en los ficheros sobre esa persona.
Si la solicitud no reúne los requisitos, se le debe responder indicando que debe realizar la petición con los términos oportunos.

EL CAMINO S.L. como responsable del tratamiento, deberá garantizar que todo el personal que tiene acceso a datos de carácter personal en la empresa pueda informar del procedimiento a seguir por el afectado para el ejercicio de sus derechos.

2.4.2.- Impugnación de valores (art.13)

Este derecho permite al interesado impugnar aquellas decisiones que tengan efectos jurídicos y cuya base sea únicamente un tratamiento de datos de carácter personal.
El artículo 13 lo detalla de este modo:

"1. Los ciudadanos tienen derecho a no verse sometidos a una decisión con efectos jurídicos, sobre ellos o que les afecte de manera significativa, que se base únicamente en un tratamiento de datos destinados a evaluar determinados aspectos de su personalidad.
2. El afectado podrá impugnar los actos administrativos o decisiones privadas que impliquen una valoración de su comportamiento, cuyo único fundamento sea un tratamiento de datos de carácter personal que ofrezca una definición de sus características o personalidad.
3. En este caso, el afectado tendrá derecho a obtener información del responsable del fichero sobre los criterios de valoración y el programa utilizados en el tratamiento que sirvió para adoptar la decisión en que consistió el acto.
4. La valoración sobre el comportamiento de los ciudadanos, basada en un tratamiento de datos, únicamente podrá tener valor probatorio a petición del afectado."

Resultado del análisis en la empresa

Este derecho no es de aplicación en la empresa que se está analizando, ya que no se toman decisiones que puedan tener efectos jurídicos en base a datos de carácter personal.

2.4.3.- Derecho de consulta al RG.P.D. (art.14)

Este derecho permite a cualquier persona recabar información con el fin de conocer la existencia de tratamientos de datos de carácter personal, la finalidad de los mismos y la identidad del responsable del fichero.
En el artículo 14 se redacta del siguiente modo:

"Cualquier persona podrá conocer, recabando a tal fin la información oportuna del Registro General de Protección de Datos, la existencia de tratamientos de datos de carácter personal, sus finalidades y la identidad del responsable del tratamiento. El Registro General será de consulta pública y gratuita."

2.4.4.- Derecho de acceso (art.15)

El usuario puede dirigirse al responsable del fichero para conocer qué datos personales suyos figuran en el fichero, cuál es su origen y las comunicaciones que se hubieran realizado o se vayan a realizar en el futuro. El artículo 15 lo detalla así:

"*1. El interesado tendrá derecho 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. 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.
3. El derecho de acceso a que se refiere este artículo sólo podrá ser ejercitado a intervalos no inferiores a doce meses, salvo que el interesado acredite un interés legítimo al efecto, en cuyo caso podrán ejercitarlo antes."

EL CAMINO S.L. deberá de resolver la solicitud en el plazo máximo de un mes desde la recepción de la solicitud y de forma gratuita. En caso que no disponga en sus ficheros datos de carácter personal del afectado, deberá igualmente de responderle en el mismo plazo.
Podrá negarse a resolver la solicitud si ya hubiese recibido una solicitud de la misma persona en un plazo inferior a 12 meses.

Resultado del análisis en la empresa
Hasta ahora no se ha dado el caso de que un usuario quiera conocer qué datos suyos figuran en los ficheros de **EL CAMINO S.L.** Se dispone de los mecanismos apropiados para informarle llegado el caso.
En todo caso, se deberá de informar al afectado de su derecho a la tutela de la Agencia Española de Protección de Datos o, en su caso de las autoridades de control de las Comunidades Autónomas, según lo dispuesto en el artículo 18 de la LOPD.

2.4.5.- Derecho de rectificación y cancelación

El afectado o interesado puede cancelar sus datos cuando no esté de acuerdo con el tratamiento que se les esté dando o cuando hayan dejado de ser necesarios para la finalidad para la que fueron registrados. La rectificación conlleva la modificación de unos datos erróneos o incompletos. La Ley lo desarrolla del siguiente modo:

"1. El responsable del tratamiento tendrá la obligación de hacer efectivo el derecho de rectificación o cancelación del interesado en el plazo de diez días.
2. Serán rectificados o cancelados, en su caso, los datos de carácter personal cuyo tratamiento no se ajuste a lo dispuesto en la presente Ley y, en particular, cuando tales datos resulten inexactos o incompletos.
3. La cancelación dará lugar al bloqueo de los datos, conservándose únicamente a disposición de las Administraciones públicas, Jueces y Tribunales, para la atención de las posibles responsabilidades nacidas del tratamiento, durante el plazo de prescripción de éstas. Cumplido el citado plazo deberá procederse a la supresión.

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

En la solicitud de cancelación, el afectado deberá incluir en la petición, los datos referidos, aportando la documentación que lo justifique.

Se dispondrá de un periodo máximo de diez días, a partir de la recepción de la solicitud, para responder al afectado de las medidas tomadas. En caso de que no se disponga en los ficheros, datos de carácter personal del afectado, deberá igualmente de responderle en el mismo plazo. Transcurridos los diez días, si **EL CAMINO S.L.** no responde a la solicitud, ésta podrá entenderse como desestimada.

EL CAMINO S.L. puede negarse al derecho del afectado de rectificar o cancelar sus datos de carácter personal en los siguientes casos:

- Cuando los datos deban de ser conservados durante los plazos previstos en las disposiciones aplicables, o en las relaciones contractuales entre el afectado y la empresa que justificaron el tratamiento de los datos.
- Cuando una Ley o una norma de derecho comunitario de aplicación directa lo prevea, o cuando éstas impidan a la empresa revelar a los afectados el tratamiento de datos a los que se refiera el acceso.

De igual modo que en el artículo anterior, deberá comunicarse al afectado de la posibilidad de pedir la tutela de derechos a la AEPD.

Resultado del análisis en la empresa

Los usuarios, especialmente los locales que pagan cuota por mostrar sus servicios, piden habitualmente la rectificación de sus datos cuando estos cambian, o han sido introducidos erróneamente.

El responsable del fichero actualiza los datos en los plazos debidos e informa al interesado de este hecho.

2.4.6.- Derecho de oposición (art 6.4)

El afectado o interesado puede oponerse al tratamiento de sus datos si existen motivos fundados y legítimos de que no se están tratando adecuadamente.

El artículo queda como sigue en la LOPD:

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

EL CAMINO S.L. deberá excluir del tratamiento los datos relativos al afectado que ejercite su derecho de oposición o denegar motivadamente la solicitud del afectado en el plazo de 10 días desde el momento de la solicitud.

Del mismo modo que en los anteriores derechos, deberá informar al afectado de la posibilidad de pedir la tutela de derechos a la AEPD si no está de acuerdo con el resultado obtenido.

Resultado del análisis en la empresa

No se ha dado el caso del ejercicio de este derecho en ningún caso

2.4.7.- Derecho a indemnización (art.19)

Este derecho permite que aquellos usuarios que hayan sido perjudicados por el incumplimiento de las obligaciones del responsable o encargado del tratamiento del fichero puedan ser indemnizados.

"1. Los interesados que, como consecuencia del incumplimiento de lo dispuesto en la presente Ley por el responsable o el encargado del tratamiento, sufran daño o lesión en sus bienes o derechos tendrán derecho a ser indemnizados.
2. Cuando se trate de ficheros de titularidad pública, la responsabilidad se exigirá de acuerdo con la legislación reguladora del régimen de responsabilidad de las Administraciones públicas.
3. En el caso de los ficheros de titularidad privada, la acción se ejercitará ante los órganos de la jurisdicción ordinaria."

2.5.- PROCEDIMIENTOS DE LA LOPD

Los procedimientos son los medios a través de los cuales se garantiza el cumplimiento de la LOPD por parte del responsable del fichero o del encargado del tratamiento. La ley contempla 2: La tutela de derechos y el procedimiento sancionador que se detallan a continuación.

2.5.1.- Tutela de los derechos (art.18)

La tutela de derechos pretende garantizar que el usuario afectado de una actuación incorrecta por parte del responsable del fichero o del responsable del tratamiento ante el ejercicio de sus derechos.

El artículo 18 lo define del siguiente modo:

"1. Las actuaciones contrarias a lo dispuesto en la presente Ley pueden ser objeto de reclamación por los interesados ante la Agencia Española de Protección de Datos, en la forma que reglamentariamente se determine.

2. El interesado al que se deniegue, total o parcialmente, el ejercicio de los derechos de oposición, acceso, rectificación o cancelación, podrá ponerlo en conocimiento de la Agencia Española de Protección de Datos o, en su caso, del organismo competente de cada Comunidad Autónoma, que deberá asegurarse de la procedencia o improcedencia de la denegación.

3. El plazo máximo en que debe dictarse la resolución expresa de tutela de derechos será de seis meses.

4. Contra las resoluciones de la Agencia Española de Protección de Datos procederá recurso contencioso-administrativo."

2.5.2.- Procedimiento sancionador (art.48)

Su objetivo es sancionar las acciones contrarias a la Ley por parte de los responsables y encargados del tratamiento.

"1. Por vía reglamentaria se establecerá el procedimiento a seguir para la determinación de las infracciones y la imposición de las sanciones a que hace referencia el presente Título.

2. Las resoluciones de la Agencia Española de Protección de Datos u órgano correspondiente de la Comunidad Autónoma agotan la vía administrativa.

3. Los procedimientos sancionadores tramitados por la Agencia Española de Protección de Datos, en ejercicio de las potestades que a la misma atribuyan esta u otras Leyes, salvo los referidos a infracciones de la Ley 32/2003, de 3 de noviembre, General de Telecomunicaciones, tendrán una duración máxima de seis meses."

2.6.- DOCUMENTO DE SEGURIDAD

En el presente Documento de Seguridad se recogen las medidas de seguridad necesarias para cumplir con las exigencias propias del **NIVEL DE SEGURIDAD BÁSICO** aplicable a los ficheros de **EL CAMINO, S.L.**

Para la determinación del antedicho nivel de seguridad han sido tenidas en cuenta las pautas fijadas en los artículos 79 a 81 del Real Decreto 1720/2007, por el que se aprueba el Reglamento de desarrollo de la L.O. 15/1999 de 13 de Diciembre de Protección de Datos de Carácter Personal, en atención a la naturaleza de los datos de carácter personal contenidos en los ficheros de la Empresa.

Las medidas de seguridad correspondientes al **NIVEL BÁSICO** serán adoptadas e implantadas por **EL CAMINO, S.L.,** tal y como le compete en su condición de Responsable del Fichero salvo las que expresamente hayan sido delegadas en el presente documento al encargado del tratamiento si así se cita.

Es necesario destacar la mención expresa en el art. 88.7 del Real Decreto 1720/2007, acerca de la obligatoriedad de mantener el documento de seguridad actualizado en todo momento, lo que supone realizar revisiones de forma periódica para contemplar posibles cambios relevantes que se pudieran producir.

Así mismo, tratándose de medidas de seguridad de **NIVEL BÁSICO,** en el art. 88.4 del Real Decreto 1720/2007, en su apartado b), se menciona la exigencia de realizar controles periódicos para verificar el cumplimiento de lo dispuesto en el presente documento.

2.6.1.- Ámbito de aplicación del documento

En el presente apartado del Documento de Seguridad se describe conforme establece el artículo 88 del R.D. 1720/2007, el ámbito en el que resultan de aplicación las medidas de seguridad aquí recogidas.

La delimitación del ámbito de aplicación se hace conforme a tres criterios básicos:

A) Atendiendo al lugar en el que se van a implantar todas y cada una de las medidas descritas en el Documento de Seguridad, se va a determinar lo que es el **ÁMBITO FUNCIONAL.**

B) Atendiendo a las personas que deberán cumplir lo dispuesto en el presente Documento, se determina cuál es el **ÁMBITO PERSONAL.**

C) En atención a los recursos de la Empresa sobre los que se van a aplicar e implantar efectivamente las medidas de seguridad previstas, queda fijado el **ÁMBITO MATERIAL.**

Ámbito Funcional

Este Documento de Seguridad es de aplicación única y exclusivamente a **EL CAMINO, S.L.,** con domicilio social en C/ XXXXX nº X, Bajo; 0900X Burgos (Burgos).

Las medidas de seguridad recogidas en el presente Documento de Seguridad podrán ser extendidas a cualesquiera otras instalaciones que **EL CAMINO, S.L.** pudiera crear y en las que se llevasen a cabo cualquier tipo de tratamiento de datos de carácter personal así como en aquellas otras personas jurídicas que presten servicios al responsable del fichero o bien sean encargados del tratamiento de este tal y como establece el Artículo 82 del RD 1720/2007.

Ámbito Personal

Se encuentran obligadas al cumplimiento de las prescripciones legales conforme a las cuales se redacta el presente Documento de Seguridad, las siguientes personas:

Quienes presten servicios, ya sea de forma directa o indirecta en **EL CAMINO, S.L.,** para, cualquiera que sea la naturaleza de la relación jurídica que le una con la misma.

Toda persona que por la labor que desempeñe, tenga o pueda tener acceso a las instalaciones o departamentos donde están ubicados los sistemas de información a través de los cuales se tratan datos de carácter personal.

La Empresa se hace responsable de la labor de formar e informar a las personas que, por su condición de usuarios, se encuentren bajo el ámbito de aplicación del presente Documento de Seguridad, sobre el adecuado cumplimiento de lo establecido en el mismo.

El Responsable del Fichero, ha establecido una relación de usuarios en la que se hacen constar los datos de los usuarios, los cuales debido a sus funciones desarrolladas en la Empresa, tienen acceso a los datos de carácter personal contenidos en los ficheros tratados por la misma.

Dicha relación será actualizada a fin de que responda con veracidad a la situación existente en cada momento en la Empresa, con respecto a la identificación de los usuarios.

Ámbito Material

En el tratamiento automatizado de los datos de carácter personal, es preciso garantizar la seguridad, mediante el control de los accesos a los ficheros, a través de cualquier vía que lo permita.

La normativa contenida en el presente Documento se aplica a todos los recursos de los sistemas de información por medio de los cuales se puede acceder a los ficheros que contienen datos de carácter personal, así como todo dispositivo que efectúe cualquier proceso de tratamiento o almacenamiento de datos de carácter personal.

Se entiende por "recurso" cualquier parte componente del sistema de información.

Dichos recursos están reflejados en el apartado 4.1. del presente documento.

2.6.2.- Funciones y obligaciones

2.6.2.1 Funciones y obligaciones del Responsable del Fichero

EL CAMINO, S.L., ostenta la condición de Responsable del Fichero, por cuanto detenta íntegramente la facultad de decisión sobre la finalidad, contenido y uso en el tratamiento de los ficheros que contienen datos de carácter personal.
Se detallan a continuación las obligaciones atribuidas legalmente a Persona Jurídica, por su condición de Responsable del Fichero:

1°.- Realizar por sí mismo, por representante o por medio de persona autorizada al efecto, cualesquiera de las gestiones de notificación ante la Agencia Española de Protección de Datos.
2°.- Redactar, establecer y comprobar la aplicación y el cumplimiento del presente Documento de Seguridad así como completar los Documentos de Seguridad de aquellas otras personas jurídicas sobre las que realice tratamiento de datos como encargado del tratamiento siempre que los realice en sus propios locales.
3°.- Velar por el cumplimiento de todos los derechos y obligaciones establecidos en la Ley Orgánica 15/1999, de 13 de Diciembre, de Protección de Datos de Carácter Personal, así como en el R.D. 1720/2007; en particular permitir a los afectados (titulares de los datos de carácter personal), el ejercicio de los derechos de acceso, rectificación, cancelación y oposición a los mismos.
4°.- Nombrar uno o varios Responsables de Seguridad, que se encarguen de coordinar y controlar las medidas de seguridad definidas en el presente Documento de Seguridad, estableciendo los criterios de actuación a seguir.

2.6.2.2 Funciones y obligaciones del Personal o Usuarios

Se considera ***usuario,*** a los efectos de la legislación aplicable en materia de protección de datos de carácter personal, *el sujeto autorizado para acceder a datos de carácter personal* o *recursos que contienen datos de carácter personal.*

Lo anteriormente expuesto supone que, aquella persona que por prestar sus servicios para **EL CAMINO, S.L.** tenga autorizado el acceso a los sistemas de información con datos de carácter personal facilitado por los afectados, quedará sujeto al control de su actividad por parte del Responsable o Responsables de Seguridad, quienes han sido nombrados para ocupar el cargo y ejercer las facultades correspondientes a los Responsables de Seguridad. Así mismo, quedan inmediatamente obligadas a cumplir las prescripciones establecidas en el presente Documento conforme a la normativa reguladora de Protección de Datos de Carácter Personal, en cuanto a:

2.6.2.4.1. Confidencialidad de la información.
2.6.2.4.2. Números de identificación y claves de acceso.
2.6.2.4.3. Uso del correo electrónico.
2.6.2.4.4. Acceso a Internet.
2.6.2.4.5. Uso de programas de ordenador.
2.6.2.4.6. Incidencias.
2.6.2.4.7. Otras medidas de seguridad interna.
2.6.2.4.8. Incumplimiento de las Obligaciones.

2.6.2.2.1 Confidencialidad de la información

Los usuarios tienen expresamente prohibido, mientras dure la relación de prestación de servicios para la Empresa para la que desempeñan sus funciones laborales, así como una vez se haya extinguido la misma, comunicar procedimientos, información, datos financieros o comerciales (en especial los datos de los clientes), así como, trabajos encomendados por su empleador

incluidos en las bases de datos y, en general, cualquier dato referido a los negocios o finanzas de **EL CAMINO, S.L.** y que hayan conocido tanto por razón de su trabajo en la Empresa, como por cualquier otra causa.

Por este motivo, todos y cada uno de los empleados de **EL CAMINO, S.L.** habrán de firmar un recibo del Documento de Seguridad, una vez les haya sido facilitado y hayan tenido ocasión de leerlo, informándose así de todas las obligaciones a las que quedan sujetos como consecuencia del tratamiento de datos de carácter personal que realizan en el cumplimiento de sus funciones.

Finalmente, todas las circulares, documentos, disquetes, etc., que contengan datos de carácter personal relacionadas con las actividades de la Empresa, son propiedad de la misma; estando obligado todo trabajador, a devolverlos cuando así le sea solicitado por **EL CAMINO, S.L.** y, en cualquier caso, con motivo de la extinción del contrato de trabajo.

Lo expuesto anteriormente supone que:

1 Queda absolutamente prohibida la utilización, divulgación o cesión de los datos de los afectados para finalidades diferentes a aquellas para las que hubieren sido facilitados.

2 Todo usuario autorizado para llevar a cabo el tratamiento de datos de carácter personal, queda obligado legalmente al secreto profesional respecto de los mismos, incluso una vez extinguida la relación laboral o de colaboración que le une con la Empresa.

3 Queda absolutamente prohibido, revelar, permitir o facilitar el acceso a la información contenida en los ficheros de la Empresa, sean automatizados o no, a terceras personas ajenas a la misma sin autorización del titular de dichos datos, así como a otros trabajadores de la Empresa que, por sus funciones, no tengan autorizado el acceso a los datos de carácter personal.

4 Recopilar información acerca de otras personas, incluidas las direcciones de correo electrónico, sin su consentimiento.

5 Transmitir cualquier material que pueda infringir los derechos de propiedad intelectual u otros derechos, incluida la marca registrada o los derechos publicitarios.

En caso de plantearse dudas sobre el acceso a los datos de carácter personal de terceras personas, debe consultarse al Responsable de Seguridad del fichero pertinente o, en su caso, al Responsable del Fichero.

2.6.2.2.2 Números de identificación y claves de acceso

Los números de identificación y las claves de acceso son proporcionados por el Responsable del Fichero a cada uno de los usuarios de forma individualizada y tendrán carácter personal e intransferible, debido a lo cual, queda absolutamente prohibido comunicar a persona distinta del propio interesado, la clave de usuario y la contraseña (salvo autorización expresa del Responsable del Fichero o, en su caso, del Responsable de Seguridad).
Si el usuario tiene conocimiento de que otra persona conoce su clave y/o contraseña de identificación y acceso, deberá ponerlo inmediatamente en conocimiento del Responsable de Seguridad o, en su caso, del Responsable del Fichero, con el fin de que le sea asignada una nueva clave de usuario y contraseña de acceso y se proceda a cancelar la anterior. En caso de incumplimiento de esta obligación, el usuario será el único responsable de los actos realizados por la persona que utilice de forma no autorizada su identificador.

Lo expuesto anteriormente supone que está totalmente prohibido:

1 Intentar descifrar las claves, sistemas o algoritmos de cifrado usando métodos de desencriptación u otros.

2 Obstaculizar voluntariamente el acceso de otros usuarios a la red mediante el consumo masivo de los recursos informáticos de la Empresa, así como realizar acciones que dañen, interrumpan o generen errores en dichos sistemas informáticos.

3 Intentar utilizar el sistema para acceder a áreas que el usuario tenga restringidas de los sistemas informáticos de la Empresa o de terceros.

4 Intentar aumentar el nivel de privilegios de un usuario del sistema.

5 Intentar acceder sin la debida autorización, al servidor, a otras cuentas o a sistemas de equipos o redes conectadas a Internet, a través del uso no lícito de la contraseña (o cualquier otro modo).

2.6.2.2.3 Normas de uso de correo electrónico

Se considerará correo electrónico a los efectos del presente Documento de Seguridad, tanto el interno (entre los terminales de la Intranet), como el externo (dirigido o proveniente de otras redes públicas o privadas, especialmente Internet).

El sistema informático, la red interna y los terminales utilizados por los usuarios, son titularidad de **EL CAMINO, S.L.**

El correo electrónico tan sólo podrá ser utilizado, para llevar a cabo las tareas que sean encomendadas directamente a cada persona, sin que pueda en ningún caso, ser utilizado para fines particulares salvo autorización del Responsable del Fichero.

Se declara expresamente la inseguridad del correo electrónico a través de Internet, al poder los mensajes ser objeto de falsificaciones y suplantaciones de personalidad. Esta afirmación deberá ser tenida en cuenta por cada usuario siempre que haga uso de él por lo que, al menos deberá cumplir con las siguientes medidas:

1 Deberán reunir los mismos requisitos establecidos en el presente Documento de Seguridad todos los ficheros que se introduzcan en la red interna o en los terminales de los usuarios a través de correo electrónico.
2 Nunca se deberán abrir archivos adjuntos que provengan de un origen desconocido, ya que podrían contener virus o código que desestabilice el sistema.

3 Siempre se ha de cerrar la sesión de cada programa de correo una vez se haya terminado de utilizar el mismo. De esta forma, se puede impedir que intrusos no deseados tengan acceso a la cuenta de cada usuario.
4 No se ha de responder a mensajes no solicitados u otro tipo de correo ofensivo o de acoso. Respondiendo se confirma que se tiene una dirección de correo electrónico activa a la que se puede enviar constantemente correo electrónico no solicitado.

Lo anteriormente expuesto supone que queda totalmente prohibido:

1 Enviar mensajes de correo electrónico de forma masiva *(spam)* o con fines comerciales o publicitarios, sin el conocimiento ni del Responsable del Fichero, ni de los destinatarios de los mismos.
2 Interceptar correo electrónico de otros usuarios para intentar leerlo, borrarlo, copiarlo o modificarlo. Esta actividad puede constituir delito de interceptación de las telecomunicaciones, tipificado en el artículo 197 del Código Penal.
3 Queda terminantemente prohibido utilizar los equipos informáticos y las redes internas o externas de la Empresa, para uso particular de los trabajadores y de las demás personas que colaboren con ella. En especial, queda prohibido recibir y enviar correo electrónico con mensajes o información particular o introducir contenidos obscenos, inmorales u ofensivos, de acoso, difamatorios, abusivos, amenazadores, hirientes, vulgares y, en general, carentes de utilidad para los objetivos de la Empresa.
4 Enviar o reenviar mensajes en cadena en la red corporativa de **EL CAMINO, S.L.** o redes externas, sin la debida autorización del Responsable de Seguridad.

2.6.2.2.4 Normas de acceso a Internet

El sistema informático, la Intranet y los terminales utilizados por los usuarios son titularidad de **EL CAMINO, S.L.** Esta exclusiva titularidad permite a la Empresa, comprobar de forma aleatoria y sin previo aviso, cualquier sesión de

acceso a Internet iniciada en la misma por cualquier usuario, cumpliendo en tales situaciones, las exigencias legales que legitiman dicha actividad.
El acceso a páginas Web, grupos de noticias, listas de distribución y otras fuentes de información del personal de la Empresa, queda restringido a las materias estricta y directamente relacionadas con las funciones que desempeña cada trabajador dentro de la misma.
En las visitas a los diferentes servidores Web deben suministrarse únicamente los datos de carácter personal necesarios para hacer uso del servicio.
Con el objeto de evitar intromisiones indebidas, deben utilizarse los programas de navegación más actualizados y activar aquellas opciones que informen de la existencia de mecanismos ajenos que tienen como objetivo la obtención ilícita y no consentida de datos. No obstante, para evitar incompatibilidades en el sistema será necesario consultar con el Responsable de Seguridad de forma previa a la actualización o instalación de cualquier tipo de Software o aplicación no autorizada.

Lo anteriormente expuesto supone que queda totalmente prohibido:

1 Introducir, descargar de Internet, reproducir, utilizar o distribuir programas informáticos, sin autorización expresa por parte del Responsable de Seguridad correspondiente, así como respecto de cualquier otro tipo de obra o material, cuyos derechos de propiedad intelectual o industrial pertenezcan a terceros, cuando no se disponga de autorización del Responsable de Seguridad.
2 Utilizar los recursos telemáticos de (incluida las redes Internet e Intranet) para actividades que no se hallen directamente relacionadas con el puesto de trabajo asignado a cada usuario.

2.6.2.2.5 Normas sobre el uso de los programas de ordenador

A los efectos del presente Documento de Seguridad, se entiende por programa de ordenador *toda secuencia original de instrucciones* o *indicaciones destinadas a ser utilizadas (directa* o *indirectamente) en un sistema informático*

para realizar una función o *tarea,* o *para obtener un resultado determinado (cualquiera que fuera su formato), incluidas las sucesivas versiones del programa, la documentación preparatoria y técnica, así como los manuales de uso.*

Únicamente podrán utilizarse aquellos programas de ordenador que hayan sido creados el Responsable del Fichero a través de cualquiera de sus empleados, para uso propio, o bien aquellos programas de ordenador de los que se haya obtenido la correspondiente licencia de uso por quien legalmente es titular de los derechos de explotación.

Queda estrictamente prohibido el uso de programas informáticos sin la correspondiente licencia, así como el uso, reproducción, cesión, transformación o comunicación pública de cualquier tipo de obra o invención susceptible de protección por la normativa aplicable en materia de propiedad intelectual o industrial. En caso de duda, deberá consultar con el Responsable de Seguridad correspondiente.

2.6.2.2.6 Otras medidas de seguridad

Además de las medidas de política de seguridad interna expuestas anteriormente, también estará absolutamente prohibido:

1 Destruir, alterar, inutilizar o de cualquier otra forma dañar los datos, programas o documentos electrónicos de **EL CAMINO, S.L.** o de las bases de datos de terceros. Dichos actos pueden constituir un delito de daños, tipificado en el artículo 264.2 del Código Penal.

2 Introducir voluntariamente programas, virus, caballos troyanos, gusanos, bombas de relojería, robots de cancelación de noticias, macros, *applets,* controles *ActiveX* o cualquier otro dispositivo lógico o secuencia de caracteres que causen, o sean susceptibles de causar, cualquier tipo de alteración en los sistemas informáticos de la entidad o de terceros. El usuario tendrá la obligación de utilizar los programas antivirus establecidos en la Empresa e implantados por el Responsable de Seguridad y estar al tanto de sus

actualizaciones periódicas, para prevenir la entrada en el sistema informático de cualquier virus destinado a borrar o alterar los datos alojados en los sistemas informáticos implantados en la Empresa.

3 Instalar copias ilegales de cualquier programa sin la correspondiente licencia preceptiva o sin la autorización del titular de los derechos de autor del mismo.

4 Desinstalar, eliminar o inutilizar cualquier programa que esté instalado legalmente en los sistemas informáticos de la Empresa, sin la correspondiente autorización del Responsable de Seguridad.

2.6.2.2.7 Incumplimiento de las obligaciones

El incumplimiento de las obligaciones anteriormente descritas dará lugar a la imposición de las correspondientes sanciones disciplinarias por parte de la mercantil en la que el trabajador haya cometido la infracción. Las sanciones serán las previstas por el Convenio Colectivo vigente en cada momento aplicable al Responsable del Fichero, y el texto refundido del Estatuto de los Trabajadores, en lo referente a la ordenación jurídica de faltas y sanciones.

La graduación de las sanciones previstas en el Convenio Colectivo, variarán en función a la naturaleza de la infracción cometida, así como de los daños y perjuicios ocasionados tanto a la propia Empresa, como a los titulares de los datos de carácter personal.

EL CAMINO, S.L. podrá reservarse contra el trabajador o prestador de servicios las acciones civiles y/o penales que de acuerdo con la legislación vigente procedan, sin perjuicio de la sanción que pudiera imponerse en el seno de la relación laboral.

En relación con la última advertencia, el Código Penal incluye varios tipos penales de aplicación a la materia analizada en sus artículos 278 y 279.

2.6.3.- Descripción de los sistemas de información que los tratan y estructura de los ficheros

En el presente apartado se describen los ficheros ya inscritos en el Registro General de Protección de Datos.

Los ficheros, en cuanto contienen datos de carácter personal, se declaran a la Agencia Española de Protección de Datos con objeto de que dicho organismo tenga conocimiento de qué datos y con qué finalidad se tratan y se encuentran los archivos de la Empresa.

De esta forma se garantiza el cumplimiento de una de las premisas básicas de la legislación sobre Protección de Datos de Carácter Personal, como es la existencia de un organismo independiente que controla y verifica la correcta utilización de los ficheros que contienen datos de carácter personal.

2.6.3.1 Sistema de Información que los trata

Los ficheros que contienen datos de carácter personal están implantados en los Equipos informáticos y ficheros en formato papel de uso por los trabajadores de la empresa.

Los sistemas de información que tratan Datos de Carácter Personal se concentran en los siguientes recursos:

⊗ Servidor Central (si lo hubiese)

☒ Sistema Operativo: WINDOWS XP

☐ Dispone de SAI (Sistema Alimentación Ininterrumpida)

☐ Copia de Seguridad

☐ Nombre Aplicación Copia de Seguridad:

☐ Soporte Copias de Seguridad:

☐ Cinta ☐ Disco Duro Ext. ☐ Memoria externa ☐ CD ☐ DVD

☐ A Distancia

Si a Distancia indique el nombre del proveedor:

☐ Lugar de Almacenamiento de Copias de Seguridad:

☐ Mismo lugar que el servidor

☐ Lugar distinto.

Indicar dirección o proveedor de servicio:

☐ Tiempo (periodicidad):

☐ Diaria ☐ Semanal (todos los niveles) ☐ Mensual

☐ Cifrado de Datos (nivel alto)

☐ Nombre Aplicación Cifrado de Datos en Discos Internos

☐ El cifrado de datos se realiza por la aplicación de gestión de datos (ej. Contraseñas)

☐ Soporte Copias de Seguridad:

☐ Cinta ☐ Disco Duro Ext. ☐ Memoria externa ☐ CD ☐ DVD

☐ A Distancia

Si a Distancia indique el nombre del proveedor:

⊗ PCS (ordenadores de sobremesa)

☒ Sistema Operativo instalado en la mayoría de PCS: WINDOWS XP

☒ Conectados en Red a Servidor Central para acceso a aplicaciones

☐ Copia de seguridad realizada desde el Servidor Central

☒ Copia de seguridad realizada desde el propio PC

☒ Tiempo (periodicidad):

☐ Diaria ☒ Semanal (todos los niveles) ☐ Mensual

☐ Aplicación para Copia de Seguridad (Sólo si no es volcado directo):

☒ Volcado directo de archivos a soporte

☒ Soporte Utilizado:

☐ Disco Duro Externo ☒ Memoria externa ☐ CD ☐ DVD ☐ A Distancia

Si a Distancia indique el nombre del proveedor:

○ Equipos portátiles

☐ Sistema Operativo instalado en la mayoría de portátiles:

☐ Conectados en Red a Servidor Central para acceso a aplicaciones

☐ Copia de seguridad realizada desde el Servidor Central

☐ Copia de seguridad realizada desde el propio portátil

☐ Tiempo (periodicidad):

☐ Diaria ☐ Semanal (todos los niveles) ☐ Mensual

☐ Aplicación para Copia de Seguridad (Sólo si no es volcado directo):

☐ Volcado directo de archivos a soporte

☐ Soporte Utilizado:

☐ Disco Duro Externo ☐ Memoria externa ☐ CD ☐ DVD ☐ A Distancia

Si a Distancia indique el nombre del proveedor:

2.6.3.2 Estructura de los Ficheros

Dando cumplimiento a la normativa vigente en materia de Protección de Datos de Carácter Personal, se ha procedido a la inscripción de los ficheros que contienen datos de carácter personal ante la Agencia Española de Protección de Datos, conforme se detalla a continuación y se adjuntan al presente Documento de Seguridad las Resoluciones de inscripción del Director de la Agencia Española de Protección de Datos en el **Anexo X.**

-> NOMBRE DEL FICHERO: CLIENTES Y PROVEEDORES

• **Descripción.-** Fichero con datos de carácter personal de los clientes y proveedores para la gestión integral de los mismos.

• **Finalidad y usos previstos.-** Gestión contable, fiscal y administrativa; Publicidad y prospección comercial; Comercio Electrónico.

• **Carácter voluntario u obligatorio.-** Obligatorio.

• **Origen y procedencia de los datos.-** El propio interesado o su representante legal.

• **Datos de carácter personal incluidos en el fichero.-** Datos de carácter identificativo: DNI/NIF, nombre y apellidos, dirección y teléfono, firma/huella; Datos de características personales; Datos de información comercial; Datos de transacciones de bienes y servicios.

• **Código de inscripción nº.-**

-> NOMBRE DEL FICHERO: GESTIÓN DE PERSONAL

• **Descripción.-** Fichero con datos de carácter personal de los trabajadores para la gestión laboral y la realización de las nóminas.

• **Finalidad y usos previstos.-** Recursos Humanos; Gestión de Nóminas; Prevención de Riesgos Laborales.

• **Carácter voluntario u obligatorio.-** Obligatorio.

• **Origen y procedencia de los datos.-** El propio interesado o su representante legal.

• **Datos de carácter personal incluidos en el fichero.-** Datos de carácter identificativo: DNI/NIF, Nº SS/Mutualidad, nombre y apellidos, tarjeta sanitaria,

dirección y teléfono, firma/huella, imagen/voz; Datos de características personales;
Datos de circunstancias sociales; Datos académicos y profesionales; Datos de detalles de empleo; Datos de transacciones de bienes y servicios;
• Código de inscripción nº.-

2.6.3.3 Encargados del Tratamiento y Prestaciones de Servicio

Las siguientes sociedades actúan como prestadores de servicios para **EL CAMINO, S.L..** Tal y como se requiere en el Artículo 82, puede consultarse en el Anexo IX los contratos de prestación de servicios donde se incluyen las medidas a adoptar por dichos prestadores.
La siguiente plantilla será la usada para anotar los prestadores de servicios, junto al servicio prestado y los ficheros a los que accede:

Empresa
Nombre o razón social: CIF: Domicilio: Servicio Prestado: Ficheros a los que accede: Fecha del contrato de prestación de servicio:

Igualmente **EL CAMINO, S.L.** puede actuar como prestador de servicios para diversas sociedades. A continuación, en caso de que **EL CAMINO, S.L.** preste algún servicio a una tercera empresa u organismo, se establece una lista con la denominación de las mismas, el servicio que se presta, la fecha del contrato de prestación de servicios o bien el lugar donde los contratos pueden ser consultados, así como si se ha delegado o no la actualización del Documento de Seguridad a **EL CAMINO, S.L.** (en caso de que la totalidad del tratamiento de datos se realice desde sus instalaciones y el Responsable del Fichero así lo

delegue). Igualmente **EL CAMINO, S.L.** se compromete a adaptar las medidas de seguridad establecidas en cada uno de los contratos suscritos.
Los contratos se encuentran ubicados en el despacho del Responsable de Seguridad.

2.6.4.- Medidas para mantener la seguridad de nivel básico de los ficheros de carácter personal.

Se detallan y describen en el presente apartado, las medidas de **NIVEL BÁSICO** encaminadas a garantizar los fines del Documento de Seguridad y, de esta forma, el cumplimiento de la legislación en materia de Protección de Datos de Carácter Personal.

2.6.4.1 Identificación y autenticación

Un objetivo prioritario para la normativa aplicable en materia de protección de datos es evitar cualquier tipo de uso indebido o no autorizado en los ficheros que contienen datos de carácter personal. Por ello, se deben implantar una serie de procedimientos de identificación y autenticación que permitan obtener y verificar puntualmente la identidad del usuario de forma inequívoca.

• En primer lugar, la *configuración del Servidor Central, si lo hubiera,* o *terminales* de la Empresa, se realizará de forma que sea necesario introducir una contraseña o clave para poder arrancarlo.

• Por otra parte, se configurará el *sistema operativo,* de tal modo que cuando éste vaya a ser cargado, sea necesario introducir un nuevo clave.

• Las contraseñas tienen una composición de mínimo 6 caracteres, tanto para el nombre de usuario como para la clave de acceso o contraseña propiamente dicha.

Para dar efectividad al proceso de identificación y autenticación, el Responsable de Seguridad debe, con carácter previo a la asignación de nombres de usuarios y claves de acceso, definir las pantallas, módulos y

procesos a los que tiene acceso autorizado cada uno de los usuarios que prestan servicios para la Empresa.

El Servidor Central, si lo hubiera, o los terminales tienen limitado el acceso a través del menú inicial, en el que tan sólo se permitirá el acceso, en función del usuario de que se trate, a aquellas partes de los sectores de la aplicación a la que si se le hubiera autorizado el acceso.

• Todas las *aplicaciones estándar bajo sistema operativo,* se configurarán de tal modo que, al ejecutarse alguna de ellas, se debe introducir una clave si dicha aplicación conlleva la gestión de datos de carácter persona, hojas de cálculo que contengan datos de carácter personal; bases que contengan datos personales; documentos de texto que contengan datos personales.

Se exceptuará esta obligación en caso de existencia de aplicativos de gestión de identidades o Single Sign On.

• En lo que respecta a las *aplicaciones a medida,* deberá introducirse igualmente un clave que tendrá un contador de intentos.

El Responsable del Fichero o en su defecto el Responsable de Seguridad tendrá la labor de cambiar la clave o contraseña de cada uno de los usuarios con una periodicidad de mínimo 1 año.

No obstante lo anterior y por causas sobrevenidas, dicho periodo podrá ser inferior o superior al establecido anteriormente, conforme al razonable criterio del Responsable de Seguridad, previa autorización del Responsable de Fichero.

El Responsable del Fichero, puede autorizar el almacenamiento, asignación y distribución de claves a una persona distinta del Responsable de Seguridad cuando así lo aconsejen las circunstancias y así se refleje en el apartado de Delegación de Autorizaciones del presente Documento de Seguridad.

2.6.4.2 Control de acceso

Independientemente del soporte en el que se contenga y el formato en el que se encuentre, toda la información albergada en los sistemas de información de EL CAMINO, S.L. es de su propiedad y tiene carácter confidencial.

• La autorización de los usuarios para acceder a datos, sistemas y recursos dependerá de las funciones que desarrollen en cada momento.
Los usuarios solo tendrán acceso a aquellos datos estrictamente necesarios para el desarrollo de las funciones que la Empresa les haya encomendado dentro de su organigrama y que están reflejados en el presente Documento de Seguridad en el Anexo I o bien en las opciones de configuración del programa de gestión de Identidades.
• Tiene la consideración de *información especialmente reservada y confidencial,* la que se relaciona a continuación, sin que tenga dicha enumeración carácter limitativo:
a) Datos, instrucciones o informes emitidos por **EL CAMINO S.L.**
b) Bases de datos de terceros, planes de marketing, informes, datos de facturación y contabilidad.
c) Cualquier otro material que forme parte de la estrategia industrial o comercial de la Empresa.
Los sistemas citados, a través del cual se tratan datos de carácter personal, se encuentran ubicados en un especia físico cual sólo accesible para aquellas personas autorizadas por el Responsable del Fichero.
• El acceso físico a las instalaciones en la que se encuentran los Sistemas de Información queda absolutamente restringido a las personas autorizadas por el Responsable del Fichero, de tal modo que, el personal no autorizado o incluso personas ajenas al Responsable del Fichero, no puedan tener acceso a él, evitando de este modo su manipulación, alteración o utilización indebida.

El Responsable de Seguridad podrá conceder, alterar o anular el acceso autorizado sobre datos y recursos, conforme a los criterios establecidos expresamente por **EL CAMINO, S.L.**

Tanto las dependencias donde se encuentran los Sistemas de Información, como los habitáculos donde se guarden las copias de seguridad, deben tener una temperatura y humedad adecuadas.

Siguiendo con lo expuesto anteriormente cabe afirmar que el Responsable de Seguridad adoptará las medidas necesarias para evitar que el personal no autorizado o personas ajenas a la Empresa tengan acceso a la instalación en el que se encuentran ubicados los Sistemas de
Información.

El Responsable de Seguridad comprobará, los siguientes extremos:

Que la lista de usuarios autorizados que se contiene en el Anexo 1 o bien en la herramienta de gestión de identidades se corresponde con la lista de los usuarios realmente autorizados en la aplicación de acceso a los Ficheros, sin que exista ningún nombre de usuario o contraseña vigentes tras la baja del usuario al que pertenecían.

La existencia de copias de respaldo que permitan la recuperación de datos según lo estipulado en este Documento.

Los usuarios autorizados comunicarán al Responsable de Seguridad cualquier cambio del que tengan conocimiento que se produzca respecto a los extremos consignados en este Documento y sus Anexos.

2.6.4.3 Gestión de Soportes

Se entiende por ***soporte*** cualquier objeto físico susceptible de ser tratado en un Servidor Central y sobre el cual se pueden grabar o recuperar datos.

2.6.4.3.1 Tratamiento de los soportes

Todos los soportes a los que tengan acceso tanto los usuarios, como el Responsable de Seguridad y/o el Responsable del Fichero, deben ser tratados de modo que:

- Se respete en todo momento las normas contenidas en el presente Documento.
- Se permita identificar el tipo de información que contienen.
- Puedan ser inventariados y almacenados en un lugar con acceso restringido, a fin de facilitar la búsqueda y control de los soportes.

A los efectos de identificar la información y facilitar su inventariado, será necesario adherir a los soportes una etiqueta identificativa en la que consten los datos que contiene cada uno de ellos y su número correlativo de referencia.
En cualquier caso, el Responsable de Seguridad podrá determinar la inclusión de datos adicionales a fin de obtener un mayor control en la gestión de soportes.

2.6.4.3.2 Control de entrada y salida de soportes

El Responsable del Fichero será la única persona que puede autorizar la salida de soportes que contengan datos de carácter personal, fuera de los locales en los que estén ubicados.

Existe un registro de entrada y salida de soportes cuya coordinación, custodia y control es competencia del Responsable del Fichero, quien podrá delegar dicha función en el Responsable de Seguridad.

En dicho Registro consta:

- La autorización expresa del Responsable del Fichero, para poder efectuar la salida o entrada.
- El tipo y cantidad de soportes que entran o salen.
- La referencia genérica del tipo de datos contenido.
- La fecha y hora de salida o entrada.
- La forma de envío o recepción e identificación detallada de los datos del receptor, o en su caso emisor.

Se adjunta como **Anexo II** del presente Documento la hoja Registro de entrada de soportes y como **Anexo III,** la hoja Registro de salida de soportes.

2.6.4.3.3 Procedimiento de desecho de soportes

Cuando un soporte que ha contenido o contiene datos de carácter personal sea desechado, previamente deberá ser borrada toda la información que contiene mediante un sistema que no permita su posterior aprovechamiento.

• *En entornos WINDOWS, LINUX y MSDOS,* se podrá actuar bajo cualquiera de las dos opciones:
1. Borrado lógico de la información de los soportes, de tal forma que no se permita el recuperado de la información.
2. Destrucción completa del soporte.

2.6.4.3.4 Procedimiento de reutilizado de soportes

Cuando un soporte que ha contenido o contiene datos de carácter personal sea reutilizado, previamente debe ser borrada toda la información que contiene mediante un sistema que no permita su aprovechamiento posterior.

• *En entornas WINDOWS, LINUX y MSDOS* se procederá al borrado lógico de la información de los soportes, de tal forma que no se permita el recuperado de la información.

2.6.4.3.5 Distribución de soportes

Por distribución de soportes se ha de entender toda salida o entrada de soportes que contengan datos de carácter personal, ya sea para la custodia de las copias de respaldo, ya sea para cualquier otra finalidad en la que esté claramente justificada esta distribución, y teniendo siempre presente la obligación de anotar en el control de entrada y salida de soportes **(Anexos II y III)** dicha distribución.

2.6.4.4 Pruebas con Datos Reales

Con el fin de que la seguridad de los datos de carácter personal se encuentre garantizada, se realizarán pruebas con carácter previo a la implantación o modificación de los sistemas de información que traten ficheros con datos de carácter personal.

Las pruebas anteriores a la implantación de las medidas de seguridad no se realizarán en ningún caso con datos reales.

Únicamente cuando se garantice el nivel de seguridad correspondiente al fichero tratado, podrán utilizarse datos reales en la realización de las mismas.

El Responsable de Seguridad está obligado a comprobar el cumplimiento de la presente medida de seguridad.

2.6.4.5 Plan de Contingencias

Para el supuesto en el que se produzca una pérdida total y absoluta de datos o que los sistemas sean destruidos total o parcialmente por cualquier contingencia imposible de prever, se deberá proceder de la siguiente forma:

1. Organizar y estructurar el sistema informático en otro centro o dependencia que posea la Empresa; o bien acudir al alquiler de oficinas donde instalar la unidad del Servidor Central o sistemas de tratamiento.
2. Existe una copia de Seguridad de todos los ficheros y archivos, con la cual la Empresa, podrá poner en marcha su actividad y desarrollar la misma sin mayor problema.

2.6.4.6 Procedimiento de realización de copias de respaldo y recuperación de datos

La posibilidad de que en una incidencia puedan perderse los datos de carácter personal que constan en los archivos informáticos de **EL CAMINO, S.L.** obliga a que en el presente Documento se prevea la necesidad de conservar copias de seguridad de todos los archivos, programas, etc. Con motivo de evitar pérdidas irreparables, se prevé a continuación, un procedimiento de realización de copias de respaldo o seguridad y recuperación de los archivos que contengan datos de carácter personal. Este procedimiento deberá ser comunicado de forma clara y legible al personal a quien haya sido encomendada dicha función de forma expresa.
El Responsable de Seguridad tendrá la obligación de informar al personal autorizado sobre los siguientes aspectos:

a) Obligatoriedad de la realización de las copias de seguridad y la conservación de las mismas conforme a lo establecido en el presente Documento.
b) Obligatoriedad de confidencialidad en el modo o sistema de realización de las mencionadas copias salvo a las personas autorizadas.
c) Prohibición de entregar las copias de seguridad a persona distinta de aquellas que han sido designadas como Responsables de Seguridad, o al Responsable del Fichero, o en su caso, a persona que hubiera sido autorizada por estos.
d) Prohibición de manipular, alterar o deteriorar los soportes (cintas, disquetes, etc.) en los que se realizan las copias de seguridad.

Las características de las copias de seguridad por recurso están contempladas en el punto 4.1. del presente Documento de Seguridad.
Es necesario realizar pruebas cada 6 meses que verifiquen la disponibilidad efectiva de los datos contenidos en los dispositivos de copias de seguridad.
Antes de proceder al almacenamiento de la copia de seguridad se verificará que ésta se ha realizado correctamente y sin ninguna incidencia. A los soportes

donde se contienen las copias de seguridad se les aplicarán las normas relativas a gestión de soportes contenidas en los **Anexos II y III.**

Todo programa, aplicación o base de datos utilizado para el tratamiento de datos personales deberá proveer la función de realización de copias de seguridad, o bien, permitir la realización de copias de seguridad de tal forma que se garantice la recuperación de datos en los términos expuestos en las normas precedentes.

Todo procedimiento de recuperación de datos deberá ser realizado por personal con los necesarios conocimientos técnicos. En el caso de que dicho procedimiento sea realizado por personal externo, el Responsable de Seguridad verificará que durante su ejecución se mantenga la más estricta confidencialidad sobre los datos de carácter personal obrantes en los ficheros.

2.6.4.7 Medidas de Seguridad en soporte papel

En relación a la información de los ficheros que se encuentra en soporte manual en formato papel, la Sociedad tiene implementadas las siguientes medidas de seguridad

- Únicamente las personas autorizadas disponen de acceso a la información en soporte papel. Estas personas se corresponden con la relación de usuarios recogida en el **Anexo I** de este Documento, dependiendo de los ficheros de la empresa a los que tengan acceso autorizado.
- Deben adoptar las mismas medidas de seguridad que los ficheros en soporte informatizado/automatizado relativas a:
    - Funciones y obligaciones del personal
    - El control de acceso físico
    - Gestión de soportes (documentación en papel en este caso)
- La documentación se debe almacenar en armarios, u otro tipo de mobiliario, con sistemas de cierre, de forma que se obstaculice su apertura. En caso de que esto no sea posible, deben adoptarse las

medidas necesarias para impedir el acceso a la documentación en papel por personas no autorizadas.

- Mientras la documentación con datos de carácter personal no se encuentre archivada en los dispositivos de almacenamiento establecido en el punto anterior, por estar en proceso de revisión o tramitación, ya sea previo o posterior a su archivo, la persona que se encuentre al cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por persona no autorizada.

2.6.5.- Anexos

2.6.6.1 Anexo I: Relación de usuarios.

2.6.6.2 Anexo II: Hoja-Registro de entrada de soportes.

2.6.6.3 Anexo III: Hoja-Registro de salida de soportes.

2.6.6.4 Anexo IV: Recibo Del Documento por los empleados o usuarios.

2.6.6.5 Anexo V: Cláusula de consentimiento informado en la recogida de datos de carácter personal.

2.6.6.6 Anexo VI: Cláusula de cesión de datos.

2.6.6.7 Anexo VII: Contrato de acceso a datos por cuenta de Terceros.

2.6.6.8 Anexo VIII: Cláusula de confidencialidad de los empleados.

2.6.6.9 Anexo IX: Resoluciones de Inscripción de los Ficheros en el registro de la Agencia española de Protección de Datos.

2.6.5.1 ANEXO I: Relación de usuarios

A continuación se detalla la relación de usuarios que tienen acceso a cada una de las Bases de datos de la Empresa.

Nombre y Apellidos	Fecha de alta en el sistema	Ficheros con permiso de acceso	Nivel de acceso (Acceso/Modificacion)

2.6.5.2 ANEXO II: Hoja-Registro de entrada de soportes

Fecha y hora de entrada del soporte	
Número y tipo de soportes	
Información que contienen	
Destinatario	
Forma de envío	
	Firma del responsable del fichero:

2.6.5.3 ANEXO III: Hoja-Registro de salida de soportes

Fecha y hora de salida del soporte	
Número y tipo de soportes	
Información que contienen	
Destinatario	
Forma de envío	
	Firma del responsable del fichero:

2.6.5.4 ANEXO IV: Recibo del Documento de Seguridad por los empleados o usuarios

El presente modelo de recibo del Documento de Seguridad debe ser firmado por cada trabajador/usuario de la empresa que acceda a los datos de carácter personal, como prueba de la recepción por el mismo del presente Documento de Seguridad.

RECIBO DEL DOCUMENTO DE SEGURIDAD		
Como usuario autorizado para acceder a ficheros que contienen datos personales, cuyo Responsable es **EL CAMINO, S.L.,** manifiesto que tengo pleno conocimiento del documento de seguridad y de las obligaciones que me conciernen en mi condición de usuario de los ficheros		
USUARIO (Nombre y apellidos)	DNI	FECHA Y FIRMA

2.6.5.5 ANEXO V: Cláusula de consentimiento informado en la recogida de datos de carácter personal.

La siguiente cláusula deberá ser incluida en todos los nuevos contratos que firmen con sus clientes y proveedores y, en su defecto, en los documentos que intercambien con ellos. Por ejemplo, si se trata de las facturas, deberán incluirlo a pie de página en las mismas:

En cumplimiento del artículo 5 de la Ley Orgánica *15/1999,* de 13 de diciembre, de Protección de Datos de Carácter Personal, por el que se regula el derecho de información en la recogida de datos, le informamos de que sus datos personales serán incorporados a un Fichero de Datos de Carácter Personal, titularidad de **EL CAMINO, S.L.** como Responsable del Fichero, con la finalidad de mantener nuestras relaciones contractuales, comerciales y profesionales que nos unen a Ud., así como para el envío de comunicaciones postales, telemáticas, o por otros medios, con ocasión de acontecimientos puntuales, o en ciertos periodos del año, que puedan ser de interés para el afectado.
Asimismo, **EL CAMINO, S.L.** garantiza al titular de los datos el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los datos que le conciernen, debiendo, para ello, dirigirse mediante comunicación escrita a la siguiente dirección: *C/* XXXXXX nº X, Bajo; 0900X Burgos (Burgos). En cualquier caso, el titular de los datos resulta informado y consiente en la conservación de dichos datos bajo las debidas condiciones de seguridad y secreto profesional, por el período que resulte necesario para la finalidad para la que son recabados.

2.6.5.6 ANEXO VI: Cláusula de cesión de datos.

Al igual que en el caso anterior, la siguiente cláusula deberá ser incluida en todos los nuevos contratos que firmen con sus clientes y proveedores y, en su defecto, en los documentos que intercambien con ellos. Por ejemplo, si se trata de las facturas, deberán incluirlo a pie de página en las mismas:

En cumplimiento del artículo 11 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, por al que se regula la cesión o comunicación de datos de carácter personal por parte del Responsable del Fichero a terceros, le informamos de que sus datos personales serán comunicados a los Organismos y Administraciones públicas que corresponda, y a las entidades bancarias con las que trabajamos.

No obstante lo anterior, **EL CAMINO, S.L.** garantiza al titular de los datos el ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los datos que le conciernen, debiendo, para ello, dirigirse mediante comunicación escrita a: C/ XXXXXX nº X, Bajo; 0900X Burgos (Burgos).

En cualquier caso, el titular de los datos resulta informado y consiente en la comunicación de dichos datos bajo las debidas condiciones de seguridad y secreto profesional, por el período que resulte necesario para la finalidad para la que son recabados, tratados y cedidos.

2.6.5.7 ANEXO VII: Contrato de acceso a datos por cuenta de terceros.

Burgos, a _____ de _____ de 2.0__

REUNIDOS

De una parte,

D/ Dña ……, mayor de edad, con N.LF. …….., en nombre y representación de **EL CAMINO, S.L.,** con CIF. Nº **B-09.XXX.XXX** y con domicilio en *CI* XXXXXXXXX nº X, Bajo; 0900X Burgos (Burgos), en adelante EL RESPONSABLE DEL FICHERO.

De otra parte,

……. mayor de edad, con N.I.F. ....., en su propio nombre y representación, y con domicilio en ……, en adelante EL ENCARGADO DEL TRATAMIENTO.

Las partes se reconocen la capacidad legal para el presente acto y de forma voluntaria y espontánea

EXPONEN

I.- Que el RESPONSABLE DEL FICHERO es el titular de determinados Ficheros que contienen datos de carácter personal, inscritos en el Registro General de la Agencia Española de Protección de Datos.

II.- Que el RESPONSABLE DEL FICHERO descrito en el antecedente expositivo primero, está interesado en que el ENCARGADO DEL TRATAMIENTO le preste el servicio de Asesoría Laboral al RESPONSABLE DEL FICHERO a través de los cuales trata los datos de carácter personal que posee en sus Ficheros, con las instrucciones, fines y medidas de seguridad estipuladas en el presente contrato y con base a lo expuesto ambas partes proceden a formalizar el presente contrato de acceso a datos conforme a las siguientes

ESTIPULACIONES

PRIMERA. OBJETO DEL CONTRATO.

El objeto del presente contrato consiste en el acceso a datos, descritos en el expositivo segundo, por parte del ENCARGADO DEL TRATAMIENTO, en la forma y bajo las condiciones que a continuación se expondrán.

SEGUNDA. PROPIEDAD DE LOS DATOS.

EL ENCARGADO DEL TRATAMIENTO reconoce expresamente que los datos contenidos en dicho fichero son de exclusiva propiedad del RESPONSABLE DEL FICHERO, por lo tanto, no podrá aplicarlos o utilizarlos con fines distintos a los previstos en este contrato. De la misma manera se irán añadiendo a estos Ficheros los registros que se generen con posterioridad a la firma de este contrato y que también serán objeto del mismo.

EL ENCARGADO DEL TRATAMIENTO devolverá a la finalización del contrato, cuantos soportes contengan datos de carácter personal, procediendo al borrado de aquellos que se encuentren en su poder, ya sea manual o automatizado, de forma que se garantice plenamente la devolución al RESPONSABLE DEL FICHERO de todos los datos, salvo cuando una Ley en vigor obligue al ENCARGADO DE TRATAMIENTO a conservar dichos datos durante un período de tiempo determinado, en cuyo caso se procederá al bloqueo de los mismos durante el período de tiempo que imponga dicha legislación.

TERCERA. PROTECCIÓN DE DATOS DE CARÁCTER PERSONAL

Conforme al artículo 12 de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal EL ENCARGADO DEL TRATAMIENTO únicamente tendrá acceso a aquellos datos que el RESPONSABLE DEL FICHERO le proporcione y procederá a su tratamiento de acuerdo con las instrucciones señaladas por EL RESPONSABLE DEL FICHERO Y de acuerdo al régimen de responsabilidad señalado en el presente contrato, no constituyendo dicho acceso en ningún caso, cesión o comunicación de los datos, ni siquiera a efectos de su conservación; sino que se trata únicamente de una simple entrega de los mismos.

CUARTA. MEDIDAS DE SEGURIDAD.

El RESPONSABLE DEL FICHERO informa al ENCARGADO DE TRATAMIENTO de su adaptación a la Ley Orgánica de Protección de Datos (15/1999) y al Reglamento de desarrollo de la LOPD (1720/2007).
A este fin solicita el mantenimiento del deber de secreto (artículo 10 LOPD) por parte del ENCARGADO DE TRATAMIENTO respecto a los datos de carácter personal transmitidos a esta misma entidad jurídica con el fin de realizar el servicio de Asesoría Laboral al RESPONSABLE DEL FICHERO, informa de la prohibición del ENCARGADO DE TRATAMIENTO de vender o ceder dichos

datos a terceros, de la obligación de la devolución, del borrado o bloqueo, en su caso, de los datos por parte de la Empresa una vez finalizada la relación contractual o cuando dejen de ser necesarios para la finalidad con que se recopilaron, así como de la obligación por parte de la Empresa que presta el servicio de someterse a auditorías (pudiendo ser interna o externa) de seguridad.

Finalmente, el RESPONSABLE DEL FICHERO cumple con una serie de medidas de seguridad contenidas en su Documento de seguridad y acordes a los distintos niveles de Seguridad de los Ficheros de Datos de Carácter Personal de los que es titular, que el ENCARGADO DE TRATAMIENTO está obligado a implementar respecto de los Ficheros, cuyo acceso por parte del ENCARGADO DE TRATAMIENTO es objeto del presente contrato.

QUINTA. CONFIDENCIALIDAD.

EL ENCARGADO DEL TRATAMIENTO se obliga a no divulgar la información contenida en los Ficheros, a los que únicamente tendrán acceso los trabajadores de dicha Empresa, comprometiéndose a guardar dicha obligación.
La confidencialidad no se aplicará a la información que sea o se convierta en públicamente disponible, sin que las partes hayan contravenido sus compromisos de confidencialidad anteriores.
Dichas obligaciones subsistirán aún con posterioridad a la finalización de la prestación objeto del presente contrato, sin límite temporal alguno.

SEXTA. RESPONSABILIDADES.

EL ENCARGADO DEL TRATAMIENTO asume la obligación de realizar un tratamiento adecuado de los Ficheros, y conforme a las instrucciones y directrices del RESPONSABLE DEL FICHERO.

En virtud del presente contrato EL ENCARGADO DEL TRATAMIENTO no se responsabilizará de los daños y perjuicios derivados de actuaciones u omisiones imputables al RESPONSABLE DEL FICHERO. Así mismo, si el ENCARGADO DEL TRATAMIENTO destina los datos a otra finalidad, los comunica o los utiliza incumpliendo las estipulaciones del contrato, será considerado RESPONSABLE DEL FICHERO, respondiendo de las infracciones que hubiera incurrido personalmente.

SÉPTIMA. RESOLUCIÓN.

En caso de que se resuelva este contrato por EL ENCARGADO DEL TRATAMIENTO, esté vendrá obligado a devolver la totalidad de la información contenida en los Ficheros sin quedarse copia alguna, salvo la exigida por la legislación vigente durante el tiempo determinado en dicha legislación, en cuyo caso se procederá al bloqueo de los mismos durante el período de tiempo que imponga dicha legislación.

OCTAVA. JURISDICCIÓN.

Con expresa renuncia al fuero que pudiera corresponderles, ambas partes se someten a la jurisdicción y competencia de los Juzgados y Tribunales del lugar y para que así conste y en prueba de conformidad, firman el presente contrato por duplicado y a un solo efecto en el lugar y fecha a su comienzo indicados.

EL RESPONSABLE DEL FICHERO	EL ENCARGADO DEL TRATAMIENTO
D. …..……..	D.……
N.I.F. núm.	N.I.F. núm

2.6.5.8 ANEXO VIII: Cláusula de confidencialidad de los empleados

La Empresa **EL CAMINO, S.L.** pone en conocimiento de sus empleados, adjuntos, colaboradores y, en general, cualquier persona que tenga acceso a los datos de carácter personal contenidos en los ficheros propiedad de
EL CAMINO, S.L. que, conforme a la Ley Orgánica de Protección de Datos de Carácter Personal, Ley Orgánica 15/1999, de 13 de diciembre, 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 aún después de finalizar sus relaciones con el titular del fichero automatizado o, en su caso, con el responsable del mismo.
La infracción de este deber puede dar lugar a las siguientes sanciones:

a) De índole administrativa:

La LOPD configura la vulneración del deber de secreto respecto a los datos de carácter personadle la siguiente forma:

- Como **infracción muy grave,** sancionada con multa de 50 a 100 millones de pesetas (aprox. entre 301.000 y 601.000 Euros), la vulneración del deber de secreto respecto de los datos relativos a la salud.
- Como **infracción grave,** sancionada con multa de 10 a 50 millones de pesetas (aprox. entre 60.010 y 301.000 Euros) la vulneración del deber de guardar secreto sobre los datos de carácter personal suficientes en su conjunto para obtener una evaluación de las personalidad del individuo.
- y como **infracción leve,** sancionada con multa de 100.000 a 10 millones de pesetas (aprox. entre 601 y 60.010 Euros), el incumplimiento del deber de secreto salvo que constituya infracción grave.

b) De índole penal:

Responsabilidad penal tipificada en el Título X del Libro II del vigente Código Penal, donde se castiga:

- Con prisión de 1 a 4 años y multa de 12 a 24 meses a quien, sin estar autorizado, acceda, se apodere, altere o utilice, en perjuicio de tercero datos de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, o de cualquier otra clase.
- Con pena a prisión de 2 a 5 años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos.
- Con pena de prisión de 1 a 3 años y multa de 12 a 24 meses, a quien con conocimiento de su origen ilícito pero sin haber participado en su descubrimiento, los difunda o revele.
- Si los hechos son cometidos por la persona encargada o responsable del fichero la pena de prisión será de 3 a 5 años, y si se difunden, revelan o ceden se impondrá la pena en su mitad superior.

Constituyen circunstancias agravantes, que supondrán la aplicación de las penas señaladas en su mitad superior, que los datos se refieran a la salud, a un menor o incapaz o que los hechos se cometan con carácter lucrativo.
Si además esta última circunstancia va referida a datos de la salud, la pena será de 4 a 6 años de prisión.
Por todo lo anteriormente expuesto el que suscribe declara expresa y formalmente conocer:

- La obligación de guardar secreto que le incumbe con relación a los datos personales a los que está autorizado a acceder en virtud de su responsabilidad profesional, laboral o de cualquier otra naturaleza que ostenta, o con relación a los datos de esa naturaleza a los que accediese por cualquier otra circunstancia.

- Las consecuencias sancionadoras de orden administrativo y penal que puede acarrear su incumplimiento, así como las eventuales indemnizaciones por responsabilidad de daños y perjuicios que la infracción puede llevar aparejadas.
- Y a estos efectos, declara expresa y formalmente su compromiso de cumplir con este deber de guardar secreto, aceptando y asumiendo, en otro caso, su responsabilidad personal frente al titular de los datos personales para resarcirle personalmente de los daños y perjuicios que se le pudieren irrogar al titular como consecuencia de su incumplimiento culpable, aceptando asimismo las consecuencias sancionadoras de orden laboral o profesional que se arbitren al efecto por los procedimientos legalmente procedentes.

EL CAMINO S.L.			
Nombre y Apellidos	Puesto de trabajo	DNI	Fecha y Firma

2.6.5.9 ANEXO IX: Resoluciones de Inscripción de los Ficheros en el Registro General de la Agencia Española de Protección de Datos

2.7.- PUBLICIDAD Y COMUNICACIONES COMERCIALES

El artículo 30 dice lo siguiente acerca del tratamiento con fines publicitarios y las comunicaciones comerciales:

"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."

Resultado del análisis en la empresa
EL CAMINO S.L. a través de un boletín electrónico quincenal ofrece información sobre las distintas rutas del Camino de Santiago, aprovechando para promocionar los artículos de la tienda que puedan ser más interesantes en función de la época del año y otras circunstancias.
Este boletín sólo se envía a las personas que voluntariamente se inscriben en él, pudiendo cancelar la suscripción cuando quieran, bien por petición mediante correo electrónico, o bien desde el enlace disponible en el propio boletín.
Ocasionalmente se realizan comunicaciones a antiguos clientes, la ley nos lo permite debido a que son artículos o servicios similares a los comprados en otras ocasiones y a que está dentro de los fines que han consentido en la relación contractual anterior.

2.8.- CONCLUSIONES TRAS EL ANÁLISIS

Tras analizar los puntos más importantes de la LOPD que afectan a la empresa, las conclusiones son las siguientes:

Entre los empleados de la empresa hay conciencia sobre la importancia de la protección de datos. Los nuevos desarrollos que se han hecho en la web, posteriores a la adaptación de la empresa a la LOPD, se han hecho siguiendo los principios marcados por ésta (información, calidad de los datos, consentimiento…).

Se echa en falta una mejor puesta al día del documento de seguridad. Faltan varios de los contratos de prestación de servicios, pese a que éstos se están realizando desde hace algún tiempo.

Habría que actualizar el sistema de administración de la web, ya que el que tiene permiso de acceso/modificación lo tiene para todos los datos. La antigüedad del sistema hace que no existan perfiles ni trazabilidad, por lo que en caso de mal uso de los datos, resultaría altamente improbable encontrar al culpable.

La fortaleza de las contraseñas en la administración de la web y en los equipos es bastante cuestionable y no se actualizan.

3. COMERCIO ELECTRÓNICO: ANÁLISIS DE LA LCE EN LA EMPRESA

3.1 INTRODUCCIÓN

La ley que tenemos que seguir como referencia es la Ley 34/2002 de 11 de Julio o Ley de Servicios de la Sociedad de la Información y Comercio Electrónico.

Antes de empezar a analizar cómo afecta en el caso que nos ocupa, vamos a intentar aclarar qué es un Servicio de la Sociedad de la Información y de ese modo saber si **EL CAMINO S.L.** es un prestador de ese tipo de servicios y se le debe aplicar esta ley.

La Ley en su apartado de definiciones dice que un servicio de la sociedad de la información es:

"Todo servicio prestado normalmente a título oneroso, a distancia, por vía electrónica y a petición individual del destinatario.

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

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

1. *La contratación de bienes o servicios por vía electrónica.*
2. *La organización y gestión de subastas por medios electrónicos o de mercados y centros comerciales virtuales.*
3. *La gestión de compras en la red por grupos de personas.*
4. *El envío de comunicaciones comerciales.*
5. *El suministro de información por vía telemática.*
6. *El vídeo bajo demanda, como servicio en el que el usuario puede seleccionar a través de la red, tanto el programa deseado como el momento de su suministro y recepción, y , en general, la distribución de contenidos previa petición individual.*

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

1. *Los servicios prestados por medio de telefonía vocal, fax o télex.*
2. *El intercambio de información por medio de correo electrónico u otro medio de comunicación electrónica equivalente para fines ajenos a la actividad económica de quienes lo utilizan.*
3. *Los servicios de radiodifusión televisiva (incluidos los servicios de cuasi vídeo a la carta), contemplados en el artículo 3.a) de la Ley 25/1994, de 12 de julio, por la que se incorpora al ordenamiento jurídico español la Directiva 89/552/CEE, del Consejo, de 3 de octubre, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva, o cualquier otra que la sustituya.*
4. *Los servicios de radiodifusión sonora, y*
5. *El teletexto televisivo y otros servicios equivalentes como las guías electrónicas de programas ofrecidas a través de las plataformas televisivas."*

El primer párrafo define claramente las características de una página web, ya que es un servicio que se ofrece a distancia, por vía electrónica (Internet), a petición individual del usuario (el usuario decide si entra o no) y a título oneroso (generar ingresos).

Existen varios tipos de servicios:

Servicios de intermediación: Son los realizados por los buscadores de Internet, los servicios de hosting y los servicios de acceso a internet (ej. adsl).

Servicios de información: Son las llamadas páginas web, que pueden ser estáticas (si sólo muestran una pantalla con información), o dinámicas (si permiten la navegación de las distintas páginas).

A su vez las dinámicas se pueden dividir en:

Conversacionales: Conversación entre usuario y empresa, pero sin llegar a la contratación desde la web. No hay comercio electrónico

Contractuales: Tras la conversación, se llega a una contratación. Aquí sí hay comercio electrónico.

Tras aclarar qué es un servicio de la sociedad de la información y los tipos de servicios, podemos decir sin miedo a equivocarnos que **EL CAMINO S.L.** es un prestador de servicios de información dinámico y contractual, ya que desde la propia web se puede realizar la compra de bienes y la contratación de servicios.

Como prestadores de servicios de la información, la ley impone una serie de obligaciones que se analizarán en el apartado 3.2, así como unas responsabilidades (apartado 3.3).

La web de **EL CAMINO S.L.** dispone de una tienda en la que se realiza la contratación de bienes y servicios. Se analizará en el apartado 3.4, si la empresa tiene correctamente especificadas las condiciones generales de contratación.

En el punto 3.5 se tratarán las comunicaciones comerciales que realiza la empresa con sus clientes.
Por último en el apartado 3.6 se mostrarán las conclusiones tras el análisis de la Ley en la empresa.

3.2 OBLIGACIONES DE LOS PRESTADORES DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN

La sección I del Capítulo II de la Ley de Comercio Electrónico define las obligaciones de los prestadores de servicios de la sociedad de la información. Para no alargar demasiado el documento sólo se tendrán en cuenta los que afectan a **EL CAMINO S.L.** (artículos 9 y 10).

*"**Artículo 9.** Constancia registral del nombre de dominio."*
(Suprimido en LEY 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información).

*"**Artículo 10.** Información general.*
1. Sin perjuicio de los requisitos que en materia de información se establecen en la normativa vigente, el prestador de servicios de la sociedad de la información estará obligado a disponer de los medios que permitan, tanto a los destinatarios del servicio como a los órganos competentes, acceder por medios electrónicos, de forma permanente, fácil, directa y gratuita, a la siguiente información:

a. *Su nombre o denominación social; su residencia o domicilio o, en su defecto, la dirección de uno de sus establecimientos permanentes en España; su dirección de correo electrónico y cualquier otro dato que permita establecer con él una comunicación directa y efectiva.*
b. *Los datos de su inscripción en el Registro Mercantil en el que, en su caso, se encuentren inscritos o de aquel otro registro público en el que lo estuvieran para la adquisición de personalidad jurídica o a los solos efectos de publicidad.*
c. *En el caso de que su actividad estuviese sujeta a un régimen de autorización administrativa previa, los datos relativos a dicha autorización y los identificativos del órgano competente encargado de su supervisión.*
d. *Si ejerce una profesión regulada deberá indicar:*
    1. *Los datos del Colegio profesional al que, en su caso, pertenezca y número de colegiado.*
    2. *El título académico oficial o profesional con el que cuente.*
    3. *El Estado de la Unión Europea o del Espacio Económico Europeo en el que se expidió dicho título y, en su caso, la correspondiente homologación o reconocimiento.*

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

e. *El número de identificación fiscal que le corresponda.*
f. *Cuando el servicio de la sociedad de la información haga referencia a precios, se facilitará información clara y exacta sobre el precio del producto o servicio, indicando si incluye o no los impuestos aplicables y, en su caso, sobre los gastos de envío o en su caso aquello que dispongan las normas de las Comunidades Autónomas con competencias en la materia.*
g. *Los códigos de conducta a los que, en su caso, esté adherido y la manera de consultarlos electrónicamente.*

2. La obligación de facilitar esta información se dará por cumplida si el prestador la incluye en su página o sitio de Internet en las condiciones señaladas en el apartado 1.
3. Cuando se haya atribuido un rango de numeración telefónica a servicios de tarificación adicional en el que se permita el acceso a servicios de la sociedad de la información y se requiera su utilización por parte del prestador de servicios, esta utilización y la descarga de programas informáticos que efectúen funciones de marcación, deberán realizarse con el consentimiento previo, informado y expreso del usuario.
A tal efecto, el prestador del servicio deberá proporcionar al menos la siguiente información:

a. *Las características del servicio que se va a proporcionar.*
b. *Las funciones que efectuarán los programas informáticos que se descarguen, incluyendo el número telefónico que se marcará.*
c. *El procedimiento para dar fin a la conexión de tarificación adicional, incluyendo una explicación del momento concreto en que se producirá dicho fin, y*
d. *El procedimiento necesario para restablecer el número de conexión previo a la conexión de tarificación adicional.*

La información anterior deberá estar disponible de manera claramente visible e identificable.
Lo dispuesto en este apartado se entiende sin perjuicio de lo establecido en la normativa de telecomunicaciones, en especial, en relación con los requisitos aplicables para el acceso por parte de los usuarios a los rangos de numeración telefónica, en su caso, atribuidos a los servicios de tarificación adicional."

3.3 RESPONSABILIDAD DE LOS PRESTADORES DE SERVICIOS DE LA SOCIEDAD DE LA INFORMACIÓN

La sección segunda del capítulo II de esta Ley hace referencia a las responsabilidades que tienen los proveedores de servicios. En el caso que se está analizando, el artículo 13.1 y el 17 son los que deben servirnos de referencia.

*"**Artículo 13.1**. Los prestadores de servicios de la sociedad de la información estén sujetos a la responsabilidad civil, penal y administrativa establecida con carácter general en el ordenamiento jurídico, sin perjuicio de lo dispuesto en esta Ley.*

***Artículo 17.** Responsabilidad de los prestadores de servicios que faciliten enlaces a contenidos o instrumentos de búsqueda.*
1. Los prestadores de servicios de la sociedad de la información que faciliten enlaces a otros contenidos o incluyan en los suyos directorios o instrumentos de búsqueda de contenidos no serán responsables por la información a la que dirijan a los destinatarios de sus servicios, siempre que:

a. *No tengan conocimiento efectivo de que la actividad o la información a la que remiten o recomiendan es ilícita o de que lesiona bienes o derechos de un tercero susceptibles de indemnización, o*
b. *Si lo tienen, actúen con diligencia para suprimir o inutilizar el enlace correspondiente.*

Se entenderá que el prestador de servicios tiene el conocimiento efectivo a que se refiere el párrafo a cuando un órgano competente haya declarado la ilicitud de los datos, ordenado su retirada o que se imposibilite el acceso a los mismos, o se hubiera declarado la existencia de la lesión, y el prestador conociera la correspondiente resolución, sin perjuicio de los procedimientos de detección y retirada de contenidos que los prestadores apliquen en virtud de acuerdos voluntarios y de otros medios de conocimiento efectivo que pudieran establecerse.
2. La exención de responsabilidad establecida en el apartado 1 no operará en el supuesto de que el proveedor de contenidos al que se enlace o cuya localización se facilite actúe bajo la dirección, autoridad o control del prestador que facilite la localización de esos contenidos."

3.4 CONDICIONES GENERALES DE CONTRATACIÓN

La protección al consumidor es un punto esencial en cualquier tipo de comercio. Esto es si cabe aún más importante, cuando hablamos del comercio electrónico, en el que se contratan bienes y servicios, casi con una confianza ciega en el cumplimiento de lo contratado.

Esto que suena tan exagerado ha sido y en algunos casos sigue siendo una de las grandes barreras para el avance del comercio electrónico. El usuario que accede por primera vez a Internet y ve la cantidad de ofertas de productos, una de las primeras preguntas que se hace es "¿y cómo se yo, que van a enviarme lo que he pedido, y que no van a usar mis datos para hacerme más cargos en la tarjeta?"

En este apartado se analizarán las Condiciones Generales de Contratación, que se definen como:

"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".

Las presentes Condiciones Generales, están sujetas a lo dispuesto a la Ley 7/1988, de 13 de abril, sobre Condiciones Generales de Contratación, a la Ley 26/1984, de 19 de julio, General para la Defensa de Consumidores y Usuarios, al Real Decreto 1906/1999, de 17 de diciembre de 1999, por el que se regula la Contratación Telefónica o Electrónica con condiciones generales, la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, la Ley 7/1996, de 15 de enero de Ordenación del Comercio Minorista, y a la Ley 34/2002 de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico.

Para una mejor comprensión se va a tratar de resumir la normativa.

Información previa a la contratación:

- Lugar de celebración del contrato: Al ser una relación Empresa – Consumidor, el lugar de celebración es el hogar del consumidor.

- Informar de si el producto incluye o no impuestos, gastos de envío.
- Garantía y plazo de devolución: La ley marca un plazo de al menos 7 días para devolver el dinero sin explicaciones, salvo productos a medida, perecederos o aquellos cuyo precio varíe con el tiempo.
- En caso de devolución quién paga los gastos que origina.
- Los trámites para la celebración del contrato (la lengua/s en que se podrá realizar, si va a archivar el documento electrónico en que se formalice el contrato y si va a estar accesible).
- Los medios técnicos de que dispone para corregir errores en la introducción de datos.

Obligaciones posteriores a la contratación:

- Se debe enviar al consumidor un acuse de recibo de la petición de contratación y la aceptación del contrato por medios electrónicos u otros (carta, fax…).
- Cumplir el derecho de resolución: El consumidor dispone de un plazo de siete días hábiles, que se contarán según el calendario oficial de su lugar de residencia habitual, para resolver el contrato sin que ello suponga incurrir en penalización no gasto alguno, incluidos los correspondientes a la devolución del bien.

3.5 LAS COMUNICACIONES COMERCIALES VÍA ELECTRÓNICA

Como se ha visto en la introducción del presente documento, **EL CAMINO S.L.** realiza el envío de un boletín informativo quincenal a sus suscriptores. Además, de cuando en cuando realiza campañas promocionales entre sus clientes (las personas que han hecho algún pedido en la tienda) y ofertas de banners promocionados (las compras en le tienda que provengan de una web con banner, se lleva un porcentaje) a webs relacionadas con el Camino de Santiago.

Hasta hace poco, estas comunicaciones se hacían como se dice popularmente "a las bravas", dando como resultado frecuentes problemas de "spam".

La Ley regula este tipo de comunicaciones en los artículos 20-22 que se citan a continuación.

*"**Artículo 20.** Información exigida sobre las comunicaciones comerciales, ofertas promocionales y concursos.*

1. Las comunicaciones comerciales realizadas por vía electrónica deberán ser claramente identificables como tales y la persona física o jurídica en nombre de la cual se realizan también deberá ser claramente identificable.

En el caso en el que 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*.*

2. En los supuestos de ofertas promocionales, como las que incluyan descuentos, premios y regalos, y de concursos o juegos promocionales, previa la correspondiente autorización, se deberá asegurar, además del cumplimiento de los requisitos establecidos en el apartado anterior y en las normas de ordenación del comercio, 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.

3. Lo dispuesto en los apartados anteriores se entiende sin perjuicio de lo que dispongan las normativas dictadas por las Comunidades Autónomas con competencias exclusivas sobre consumo, comercio electrónico o publicidad.

***Artículo 21.** Prohibición de comunicaciones comerciales realizadas a través de correo electrónico o medios de comunicación electrónica equivalentes.*

1. Queda prohibido el envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas.
2. Lo dispuesto en el apartado anterior no será de aplicación cuando exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente.
En todo caso, el prestador deberá ofrecer al destinatario la posibilidad de oponerse al tratamiento de sus datos con fines promocionales mediante un procedimiento sencillo y gratuito, tanto en el momento de recogida de los datos como en cada una de las comunicaciones comerciales que le dirija.

***Artículo 22.** Derechos de los destinatarios de servicios.*
1. El destinatario podrá revocar en cualquier momento el consentimiento prestado a la recepción de comunicaciones comerciales con la simple notificación de su voluntad al remitente.
A tal efecto, los prestadores de servicios deberán habilitar procedimientos sencillos y gratuitos para que los destinatarios de servicios puedan revocar el consentimiento que hubieran prestado.
Asimismo, deberán facilitar información accesible por medios electrónicos sobre dichos procedimientos.
2. Cuando los prestadores de servicios empleen dispositivos de almacenamiento y recuperación de datos en equipos terminales, informarán a los destinatarios de manera clara y completa sobre su utilización y finalidad, ofreciéndoles la posibilidad de rechazar el tratamiento de los datos mediante un procedimiento sencillo y gratuito.
Lo anterior no impedirá el posible almacenamiento o acceso a datos con el fin de efectuar o facilitar técnicamente la transmisión de una comunicación por una red de comunicaciones electrónicas o, en la medida que resulte estrictamente necesario, para la prestación de un servicio de la sociedad de la información expresamente solicitado por el destinatario."

3.6 OTRAS FORMAS DE COMERCIO ELECTRÓNICO

EL CAMINO S.L. no se financia exclusivamente de la venta de productos y servicios en la página web de la empresa. Hoy en día para que una empresa sobreviva en Internet con la gran competencia que hay, tiene que diversificar sus estrategias de venta.
Una de las claves ha sido siempre la gran cantidad de información actualizada que ha ofrecido la web, no sólo de los distintas ciudades, pueblos y aldeas por las que pasa el Camino de Santiago en sus distintas rutas, sino sobre todo por la información que se ofrece del entorno.

En la empresa se ha hecho un gran esfuerzo para incluir en cada tramo del camino, información sobre los monumentos, folklore, ayuntamientos, hospitales y establecimientos imprescindibles para los peregrinos, como albergues municipales, hoteles, hostales, restaurantes, farmacias y comercios en general.

Este esfuerzo inicial ha supuesto que con el crecimiento en importancia de la página, muchos de esos establecimientos han visto una gran oportunidad de anunciarse. De este modo, se pudo establecer una cuota anual, para aquellos establecimientos que quisieran mostrar información adicional (servicios disponibles, página web…), aparte de unos datos básicos de contacto (nombre del establecimiento y dirección).
Si pensamos en los más de 1000 localidades por las que pasa el Camino de Santiago, podemos hacernos una pequeña idea de que la cantidad de establecimientos objetivo es muy alta y que es un nicho importante a tener en cuenta.

Otro punto interesante de ingresos secundarios proviene de la publicidad. La web dispone de una banda que aparece en distintas partes de la web, en la que se alojan banners **publicitarios a otras webs**, preferentemente servicios paralelos al Camino de Santiago a los que no llega **EL CAMINO S.L**. El precio de estos banner

varían en función del tiempo que vayan a estar presentes en la web, su localización (todas las páginas, página principal, páginas secundarias…) y de su tamaño.
Otro tipo de publicidad que se está usando en la web, es la proporcionada por **empresas especializadas en publicidad**.
En estos momentos se está trabajando con 2 empresas totalmente distintas entre sí: Coguan adshare y Google Adsense.
El funcionamiento de Coguan es el siguiente:

Se da de alta la web como soporte de anuncios y se rellenan los datos de sus formularios (nombre de la web, nº medio de visitas diarias, nº de usuarios únicos mensuales…). Un vez que la empresa ha confirmado el alta, se deben establecer los tipos y tamaños de anuncios que se quieren usar y el tipo de pago que se va a recibir por ellos. Existen 2 tipos pago por CPM (pago por impresión) y CPC (pago por Click).

El pago por CPM supone el pago de una cantidad a establecer (negociable con el anunciante) por cada 1000 impresiones del anuncio, es decir, por cada 1000 usuarios distintos que han visto la página en la que está el anuncio.
El pago por click supone el pago de una cantidad (negociable, aunque generalmente de 0.20€/click) por cada click que realice un usuario en el anuncio.

Coguan adshare tiene una base de datos de anunciantes y cuando un anunciante decide abrir una campaña, Coguan se lo comunica a la/s empresa/s que puedan estar interesadas. La empresa que acepte la oferta en cuanto a modo de pago y cantidad, debe copiar el script proporcionado, en la zona de la web donde quiera que aparezca el anuncio (todos los anuncios son de tipo gráfico).
Recientemente han incorporado un servicio de publicidad generalista para aprovechar los espacios publicitarios, cuando no se tienen ofertas de anunciantes especializados. Este servicio funciona sólo en el formato de CPC.

Google Adsense funciona de forma similar, sólo que es exclusivamente pago por click. La cantidad a pagar depende del anuncio en el que se haga click. El tipo de

publicidad es no especializada, pero permite filtrar determinados temas y evitar anuncios los anuncios de un nº de webs.

Los espacios de publicidad se pueden configurar de diversos modos:

Elegir entre anuncio de texto, gráfico o mixto.

Configurar los colores de los anuncios de texto (borde, link, descripción, fondo, forma de las esquinas…) para que se adapten a la tipografía y colores de tu web.

Un ejemplo de configuración sería:

Pantalla de configuración del aspecto de los anuncios en Adsense.

También permite obtener informes del rendimiento de cada uno de los anuncios:

Pantalla de informe de rendimiento de un anuncio en Adsense.

La diferencia fundamental es que Coguan adshare es más específico, por lo que se puede llegar a ganar mucho dinero siempre que haya campañas que se adapten a tus necesidades.

Google Adsense por el contrario tiene muchos más formatos de anuncios, desde muy pequeños (120X90 pixeles) hasta los más grandes (728X90 o 160X600 pixeles), por lo que pueden colocarse de forma estratégica en la página de forma que sean más eficaces y no molesten al que visita la página.

3.7 CONCLUSIONES TRAS EL ANÁLISIS

Resultado del análisis de las obligaciones

La web de **EL CAMINO S.L.** presenta todos los datos que pide el artículo 10 en una sección denominada "¿quienes somos?" accesible desde cualquier punto de la misma.

Resultado del análisis de las responsabilidades

EL CAMINO S.L. dispone de un buscador en el que se encuentran gran cantidad de asociaciones (de todo el mundo) y webs relacionadas con el Camino de Santiago. Antes de dar de alta en el directorio estas webs, se verifica el contenido de las mismas, con el fin de asegurarse de que no contienen contenidos que puedan ser ofensivos.

Posteriormente a esto, no se vuelven a verificar. Si se diera el caso de que una de estas webs cambiara su contenido, se borraría del directorio en el momento en que así se notificara (normalmente por los propios usuarios).

Resultado del análisis de las Condiciones Generales de Contratación

Las condiciones generales de contratación no cumplen al 100% con la norma. Se encuentran en una sección de "ayuda",en la tienda de la web, junto con otras respuestas a dudas acerca de la seguridad en los pagos electrónicos.

No se encuentran disponibles para su descarga (salvo que el propio consumidor guarde el contenido de la página).

Sería recomendable una nueva redacción de las mismas, especificando las posibles diferencias en los distintos tipos de servicios.

Resultado del análisis de las comunicaciones comerciales

En la actualidad se han mejorado las comunicaciones comerciales gracias a lo aprendido durante el magíster:

Las suscripciones al boletín electrónico las realiza el propio usuario. Anteriormente se incluían todos los correos electrónicos que llegaban a la empresa, sin

consentimiento previo, lo cual atenta gravemente con los principios de información y consentimiento de la LOPD.

En el propio boletín y en la web, se incluye un sencillo formulario para darse de baja en cualquier momento.

Se atienden al momento las peticiones de baja del boletín.

Se incluye la palabra publicidad al inicio de cada una de estas comunicaciones.

En el caso de las comunicaciones de ofertas comerciales a clientes, la ley lo permite al haber una relación contractual previa, en la que han dado su consentimiento.

4. LA FIRMA ELECTRÓNICA EN LA EMPRESA

4.1.- INTRODUCCIÓN

Hasta hace pocos años, la validez de los contratos se basaba en la firma de los contratantes. Una firma no es otra cosa que una representación gráfica que identifica a una persona y ratifica el contenido del documento firmado.
Esto presupone que vista una firma podemos saber qué persona ha firmado y que un documento firmado no ha podido modificarse tras la firma.

Estas afirmaciones son demasiado generalistas y han dado lugar a grandes luchas judiciales, por la validez o no de un determinado contrato. Son necesarios grandes expertos para demostrar que una firma no ha sido falsificada y lo mismo podemos decir de un documento.
Si extrapolamos el problema al nivel electrónico, el problema se multiplica ya que no podemos asegurar la no manipulación (intencionada o accidental), de una transmisión electrónica que puede pasar por cientos de ordenadores o routers, antes de llegar a su destino.

Afortunadamente la tecnología ha avanzado lo suficiente y ahora disponemos de la firma electrónica. Su definición según el artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica es:

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

De la definición anterior se deduce que la firma electrónica identifica al firmante, pero no garantiza que el documento firmado no haya sido manipulado.
También se llama Firma Electrónica Simétrica, ya que se basa en una única clave privada que sirve para encriptar y desencriptar el documento. Sólo es válida para entornos de confianza, ya que en el momento en que se conozca, cualquiera puede firmar por ti.

A estos efectos surge la firma electrónica avanzada que se define como:

"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 que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control."

Con este tipo de firma avanzamos un paso más, sabemos que el mensaje no ha sido manipulado y

El siguiente nivel de firma es la firma electrónica reconocida:

"firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma"

La Ley define claramente en el artículo 11 qué es un certificado reconocido y su contenido:

"1. Son certificados reconocidos los certificados electrónicos expedidos por un prestador de servicios de certificación que cumpla los requisitos establecidos en esta Ley en cuanto a la comprobación de la identidad y demás circunstancias de los solicitantes y a la fiabilidad y las garantías de los servicios de certificación que presten.

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

- *a. La indicación de que se expiden como tales.*
- *b. El código identificativo único del certificado.*
- *c. La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.*
- *d. La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.*
- *e. La identificación del firmante, en el supuesto de personas físicas, por su nombre y apellidos y su número de documento nacional de identidad o a través de un seudónimo que conste como tal de manera inequívoca y, en el supuesto de personas jurídicas, por su denominación o razón social y su código de identificación fiscal.*
- *f. Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.*
- *g. El comienzo y el fin del período de validez del certificado.*

h. Los límites de uso del certificado, si se establecen.
i. Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

3. Los certificados reconocidos podrán asimismo contener cualquier otra circunstancia o atributo específico del firmante en caso de que sea significativo en función del fin propio del certificado y siempre que aquél lo solicite.

4. Si los certificados reconocidos admiten una relación de representación incluirán una indicación del documento público que acredite de forma fehaciente las facultades del firmante para actuar en nombre de la persona o entidad a la que represente y, en caso de ser obligatoria la inscripción, de los datos registrales, de conformidad con el apartado 2 del artículo 13."

Existen dispositivos hardware que realizan esta labor de firma de forma automática, son los dispositivos seguros de creación de firma.El artículo 24 de la Ley en sus puntos 2 y 3 definen el concepto de dispositivo seguro de creación de firma del siguiente modo:

"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."

Básicamente un dispositivo de creación de firma debe realizar los pasos de creación de firma correctamente, asegurándose de que el sistema usado para ello impide que la firma pueda repetirse en algún momento, que la firma no puede

derivarse de los datos usados para su creación, que el dispositivo no modifica el documento al crear la firma, y que un tercero no puede acceder a los datos de creación de firma.

Tanto los dispositivos seguros de creación de firma, como los prestadores de servicios de certificación pueden ser certificados (aunque no es necesario). Los artículos 26 y 27 de la Ley lo definen con claridad.

En el caso de los prestadores de servicios de certificación, la ley dice:

"1. La 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."

El punto 4 ratifica que siendo voluntario no pierde su validez judicial.

En el caso de los dispositivos seguros de creación de firma la ley dice lo siguiente:

1. La 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.

2. La certificación podrá ser solicitada por los fabricantes o importadores de dispositivos de creación de firma y se llevará a cabo por las entidades de certificación reconocidas por una entidad de acreditación designada de acuerdo con lo dispuesto en la Ley 21/1992, de 16 de julio, de Industria y en sus disposiciones de desarrollo.

4. Los certificados de conformidad de los dispositivos seguros de creación de firma serán modificados o, en su caso, revocados cuando se dejen de cumplir las condiciones establecidas para su obtención.

Los organismos de certificación asegurarán la difusión de las decisiones de revocación de certificados de dispositivos de creación de firma.

Las funciones de la firma electrónica son las siguientes:

- Identificar inequívocamente al titular de la firma.

- Autenticar / autentificar el contenido del documento.
- Garantizar la integridad del documento.
- No repudio: Lograr la seguridad jurídica en la conservación del documento, de forma que ninguna de las partes pueda negar haber recibido o enviado el mensaje.

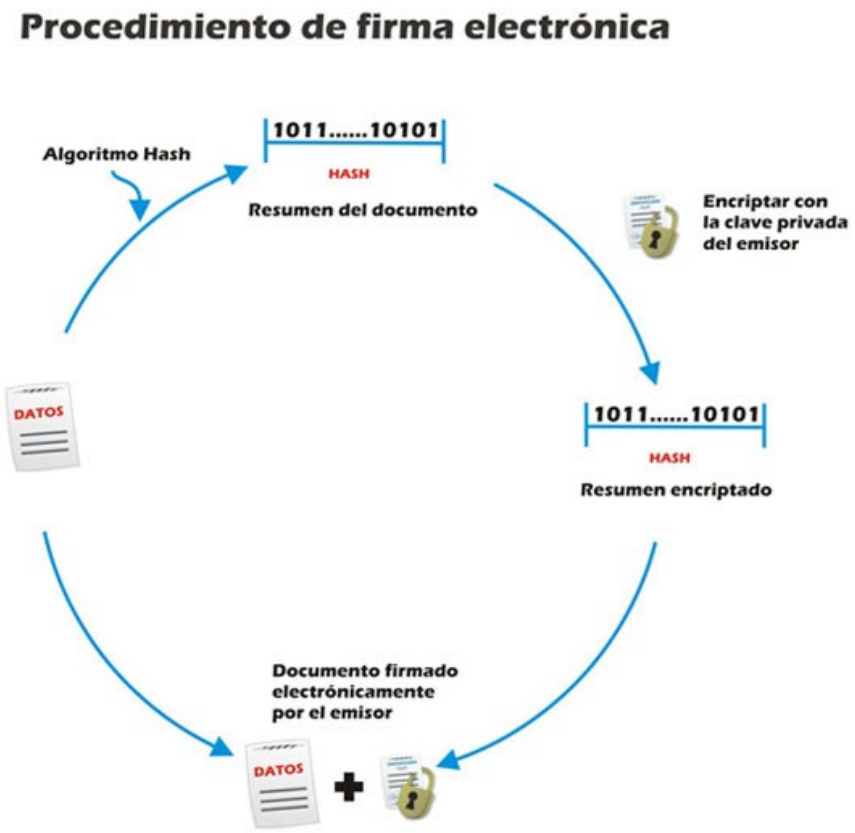
Proceso de firma electrónica de un documento

Se basa en la utilización de una infraestructura de claves asimétrica compuesto por una clave privada que sólo conoce el firmante y una clave pública que la desencripta y se envía con el mensaje.

El proceso de creación de la firma electrónica es el siguiente:

Un emisor escribe un mensaje y dispone de todos los medios necesarios para firmarlo electrónicamente. El proceso de firma recoge el mensaje y mediante una función de hash, obtiene un resumen o digest del tamaño asignado.

Este resumen se encripta con la clave privada del emisor (que sólo el conoce) y se envía el mensaje al destinatario junto con el resumen encriptado.



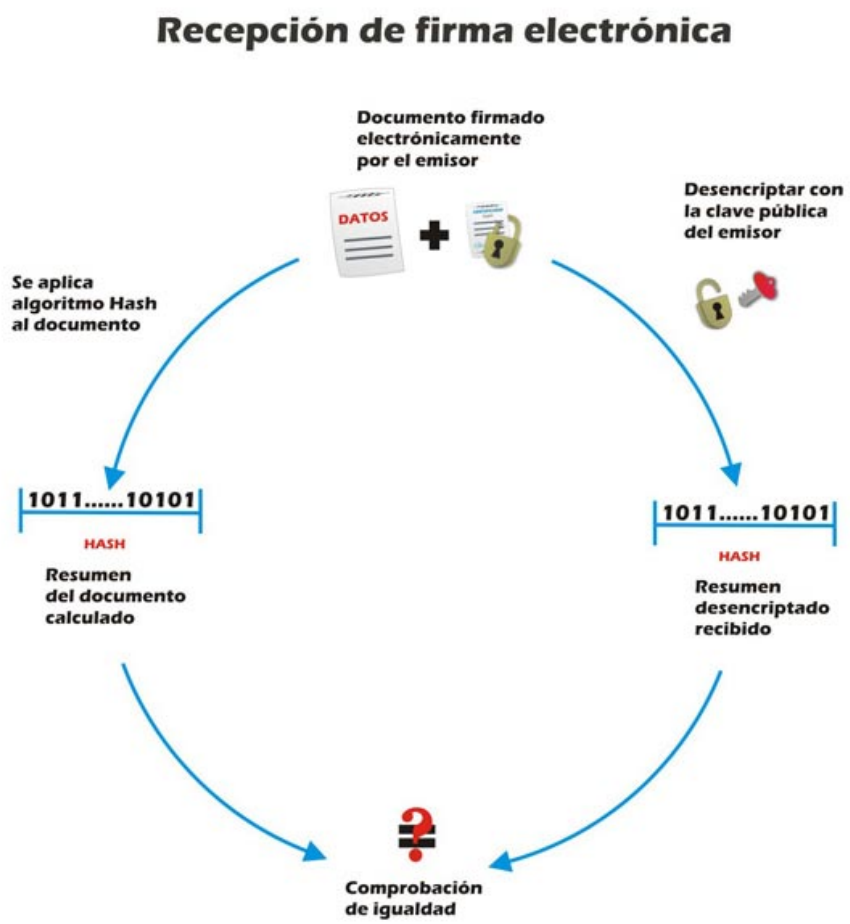
Representación gráfica del proceso de firma.

En destino para asegurarse de que no ha habido manipulación intencionada o no del conjunto se realizan las siguientes operaciones:

Se aplica la función de hash sobre el mensaje para obtener el resumen.

Se desencripta con la clave pública el resumen encriptado (enviado junto al mensaje) con la clave privada del emisor.

Se comparan ambos resúmenes. Si son iguales, el mensaje y la firma no se han manipulado (integridad del conjunto mensaje y firma).



Representación gráfica de la recepción de la firma.

El que se haya podido desencriptar el resumen recibido con la clave pública **identifica al emisor del mensaje**, ya que el único modo de desencriptar la clave privada es tener la clave pública asociada.

La validez jurídica de la firma electrónica sólo es válida para la firma electrónica reconocida, equiparable a la manuscrita como dice el artículo 3 apartado 4 de la Ley de Firma Electrónica:

"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".

En los siguientes puntos se tratarán los siguientes temas relacionados con la firma electrónica:

- Los prestadores de servicios de certificación y sus obligaciones y responsabilidades.
- El uso actual de la firma electrónica en **EL CAMINO S.L.**
- Posibles usos de la firma electrónica en **EL CAMINO S.L.**

4.2.- LOS PRESTADORES DE SERVICIOS DE CERTIFICACIÓN (OBLIGACIONES Y RESPONSABILIDADES)

En la introducción ha quedado claro que para que haya validez jurídica con la firma electrónica, es preciso que se usen certificados reconocidos generados mediante un dispositivo seguro de creación de firma. El artículo 11 define qué es un certificado reconocido y su contenido.

El **Prestador de Servicios de Certificación o Autoridad de Certificación** es el encargado de emitir y revocar certificados.
Almacena la relación entre la clave pública y la privada de cada certificado. De este modo permite identificar al propietario de la clave pública que da a conocer a todos aquellos que quieran ponerse en contacto con él.
La clave privada, correspondiente a **la clave pública**, sólo será conocida por el propietario del certificado. Aquí radica la seguridad del sistema.

Para que una autoridad de certificación pueda ser reconocida como tal debe cumplir con una serie de obligaciones para su emisión, así como revocar el certificado cuando el propietario lo solicite o cuando se sospeche de un uso indebido por terceros no autorizados.
Deben estar acreditadas por Entidades de Certificación y cumplir con las obligaciones que marcan los artículos 17-19 y 21 de la presente Ley:

*"**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.

***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.*

***Artículo 19.** Declaración de prácticas de certificación.*

1. Todos los prestadores de servicios de certificación formularán una declaración de prácticas de certificación en la que detallarán, en el marco de esta Ley y de sus disposiciones de desarrollo, las obligaciones que se comprometen a cumplir en relación con la gestión de los datos de creación y verificación de firma y de los certificados electrónicos, las condiciones aplicables a la solicitud, expedición, uso, suspensión y extinción de la vigencia de los certificados las medidas de seguridad técnicas y organizativas, los perfiles y los mecanismos de información sobre la vigencia de los certificados y, en su caso la existencia de procedimientos de coordinación con los Registros públicos correspondientes que permitan el intercambio de información de manera inmediata sobre la vigencia de los poderes indicados en los certificados y que deban figurar preceptivamente inscritos en dichos registros.

2. La declaración de prácticas de certificación de cada prestador estará disponible al público de manera fácilmente accesible, al menos por vía electrónica y de forma gratuita.

3. La declaración de prácticas de certificación tendrá la consideración de documento de seguridad a los efectos previstos en la legislación en materia de protección de datos de

carácter personal y deberá contener todos los requisitos exigidos para dicho documento en la mencionada legislación.

***Artículo 21.** Cese de la actividad de un prestador de servicios de certificación.*
1. El prestador de servicios de certificación que vaya a cesar en su actividad deberá comunicarlo a los firmantes que utilicen los certificados electrónicos que haya expedido así como a los solicitantes de certificados expedidos a favor de personas jurídicas; y podrá transferir, con su consentimiento expreso, la gestión de los que sigan siendo válidos en la fecha en que el cese se produzca a otro prestador de servicios de certificación que los asuma o, en caso contrario, extinguir su vigencia. La citada comunicación se llevará a cabo con una antelación mínima de dos meses al cese efectivo de la actividad e informará, en su caso, sobre las características del prestador al que se propone la transferencia de la gestión de los certificados.
2. El prestador de servicios de certificación que expida certificados electrónicos al público deberá comunicar al Ministerio de Ciencia y Tecnología, con la antelación indicada en el anterior apartado, el cese de su actividad y el destino que vaya a dar a los certificados, especificando, en su caso, si va a transferir la gestión y a quién o si extinguirá su vigencia. Igualmente, comunicará cualquier otra circunstancia relevante que pueda impedir la continuación de su actividad. En especial, deberá comunicar, en cuanto tenga conocimiento de ello, la apertura de cualquier proceso concursal que se siga contra él.
3. Los prestadores de servicios de certificación remitirán al Ministerio de Ciencia y Tecnología con carácter previo al cese definitivo de su actividad la información relativa a los certificados electrónicos cuya vigencia haya sido extinguida para que éste se haga cargo de su custodia a efectos de lo previsto en el artículo 20.1.f. Este ministerio mantendrá accesible al público un servicio de consulta específico donde figure una indicación sobre los citados certificados durante un período que considere suficiente en función de las consultas efectuadas al mismo."

Los prestadores de servicios certificación reconocidos deben cumplir obligaciones especiales, ya que tienen validez judicial. Además de los artículos anteriores deben cumplir con el artículo 12 y el 20 que dicen lo siguiente:

*"**Artículo 12.** Obligaciones previas a la expedición de certificados reconocidos.*
Antes de la expedición de un certificado reconocido, los prestadores de servicios de certificación deberán cumplir las siguientes obligaciones:

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

Artículo 20. *Obligaciones de los prestadores de servicios de certificación que expidan certificados reconocidos.*

1. Además de las obligaciones establecidas en este capítulo, los prestadores de servicios de certificación que expidan certificados reconocidos deberán cumplir las siguientes obligaciones:

a. *Demostrar la fiabilidad necesaria para prestar servicios de certificación.*
b. *Garantizar que pueda determinarse con precisión la fecha y la hora en las que se expidió un certificado o se extinguió o suspendió su vigencia.*
c. *Emplear personal con la cualificación, conocimientos y experiencia necesarios para la prestación de los servicios de certificación ofrecidos y los procedimientos de seguridad y de gestión adecuados en el ámbito de la firma electrónica.*
d. *Utilizar sistemas y productos fiables que estén protegidos contra toda alteración y que garanticen la seguridad técnica y, en su caso, criptográfica de los procesos de certificación a los que sirven de soporte.*
e. *Tomar medidas contra la falsificación de certificados y, en el caso de que el prestador de servicios de certificación genere datos de creación de firma, garantizar su confidencialidad durante el proceso de generación y su entrega por un procedimiento seguro al firmante.*
f. *Conservar registrada por cualquier medio seguro toda la información y documentación relativa a un certificado reconocido y las declaraciones de prácticas de certificación vigentes en cada momento, al menos durante 15 años contados desde el momento de su expedición, de manera que puedan verificarse las firmas efectuadas con el mismo.*
g. *Utilizar sistemas fiables para almacenar certificados reconocidos que permitan comprobar su autenticidad e impedir que personas no autorizadas alteren los datos, restrinjan su accesibilidad en los supuestos o a las personas que el firmante haya*

indicado y permitan detectar cualquier cambio que afecte a estas condiciones de seguridad.

2. Los prestadores de servicios de certificación que expidan certificados reconocidos deberán constituir un seguro de responsabilidad civil por importe de al menos 3.000.000 de euros para afrontar el riesgo de la responsabilidad por los daños y perjuicios que pueda ocasionar el uso de los certificados que expidan.

La citada garantía podrá ser sustituida total o parcialmente por una garantía mediante aval bancario o seguro de caución, de manera que la suma de las cantidades aseguradas sea al menos de 3.000.000 de euros.

Las cuantías y los medios de aseguramiento y garantía establecidos en los dos párrafos anteriores podrán ser modificados mediante real decreto."

Responsabilidades de los prestadores de servicios de certificación

Las responsabilidades de los prestadores de servicios de certificación vienen derivadas de resarcir los daños derivados del incumplimiento de sus obligaciones con la Ley. El artículo 22 lo detalla del siguiente modo:

*"**Artículo 22.** Responsabilidad de los prestadores de servicios de certificación.*

1. Los prestadores de servicios de certificación responderán por los daños y perjuicios que causen a cualquier persona en el ejercicio de su actividad cuando incumplan las obligaciones que les impone esta Ley.

La responsabilidad del prestador de servicios de certificación regulada en esta Ley será exigible conforme a las normas generales sobre la culpa contractual o extracontractual, según proceda, si bien corresponderá al prestador de servicios de certificación demostrar que actuó con la diligencia profesional que le es exigible.

2. Si el prestador de servicios de certificación no cumpliera las obligaciones señaladas en los párrafos b al d del artículo 12 al garantizar un certificado electrónico expedido por un prestador de servicios de certificación establecido en un Estado no perteneciente al Espacio Económico Europeo, será responsable por los daños y perjuicios causados por el uso de dicho certificado.

3. De manera particular, el prestador de servicios de certificación responderá de los perjuicios que se causen al firmante o a terceros de buena fe por la falta o el retraso en la inclusión en el servicio de consulta sobre la vigencia de los certificados de la extinción o suspensión de la vigencia del certificado electrónico.

4. Los prestadores de servicios de certificación asumirán toda la responsabilidad frente a terceros por la actuación de las personas en las que deleguen la ejecución de alguna o algunas de las funciones necesarias para la prestación de servicios de certificación.
5. La regulación contenida en esta Ley sobre la responsabilidad del prestador de servicios de certificación se entiende sin perjuicio de lo establecido en la legislación sobre cláusulas abusivas en contratos celebrados con consumidores."

Otros elementos imprescindibles en un sistema de certificación electrónica son:
Las Autoridades de Registro son las encargadas de identificar de manera inequívoca a los usuarios para que, posteriormente, éstos puedan obtener los certificados.

Los certificados tienen una validez en el tiempo, para garantizar la validez de un certificado existen la Autoridad de Validación.

4.3.- USO DE LA FIRMA ELECTRÓNICA EN LA EMPRESA

EL CAMINO S.L. es una empresa con casi 10 años de presencia en Internet. Usa la firma electrónica en sus comunicaciones con las entidades de pago con tarjeta.
El proceso es el siguiente:
Cuando un cliente realiza una compra en la tienda virtual de la empresa, puede elegir entre el pago por transferencia, pago por tarjeta de crédito y pago por paypal.

Cuando elige el pago por tarjeta de crédito se conecta a una pasarela de pagos segura (https), en la que el cliente puede suministrar sus datos de pago (Nº de tarjeta, fecha de caducidad y CVV).
A estos datos junto con el precio a pagar, el código de comercio y otros datos relativos al pago se les aplica el proceso de firma electrónica (con la clave privada del comercio, que ha sido suministrada por la pasarela de pago) visto anteriormente.
La pasarela de pagos comprueba que la transmisión no ha sufrido cambios, e identifica al comercio. A continuación se realiza una doble verificación:

- Se verifica la validez de la tarjeta.
- Se verifica que la persona que está realizando el pago es el titular de la tarjeta.

La primera verificación consiste en asegurarse que la tarjeta está activa (no se ha anulado por robo, no ha caducado y el nº de seguridad CVV coincide con la numeración de la tarjeta).

La segunda verificación se está realizando en los últimos años para evitar las compras con tarjetas robadas, y evitar el repudio de la compra por un cliente.
Cada entidad bancaria realiza comprobaciones distintas. La mayoría consisten en un redireccionamiento a la web de la entidad financiera, en la que se solicita:

- Una clave genérica para cualquier pago.
- Una clave variable (la resultante de unas coordenadas en una cuadrícula) para cada pago.

- Una clave enviada al teléfono móvil del titular.
- Una mezcla de ambas soluciones.

Cada una de estas soluciones tiene sus puntos fuertes y débiles. La principal pega de cara al cliente es la pesadez del proceso. El cliente está acostumbrado a introducir los datos de la tarjeta y finalizar el pago. El proceso de conectarse a su banco, introducir sus claves y confirmar el pago mediante una o varias claves, suele resultarle molesto y en ocasiones abandonan la compra.
Las entidades bancarias están empezando a introducir el uso del dni electrónico. Esto debería facilitar el proceso de confirmación del titular.

Las ventajas del uso de una plataforma de pagos externa a la web de la empresa son evidentes:

- No se almacenan datos sensibles como nº de tarjeta de crédito/débito, que sólo dan problemas de cara a la seguridad de los clientes.
- La seguridad de la transmisión queda en manos de la plataforma.
- La verificación de los datos los realiza la plataforma. Con esta doble verificación asumen el riesgo de fraude.

4.4.- POSIBLES USOS FUTUROS EN LA WEB

Uno de los posibles usos de la firma electrónica en la empresa tiene que ver con la administración electrónica. Este año las administraciones públicas deben proporcionar al ciudadano la posibilidad de realizar la mayor parte de sus gestiones (pago de impuestos municipales, recursos administrativos…) a través de la administración electrónica.

El requisito principal para realizar estos trámites es disponer de una firma electrónica reconocida (con sellado de tiempo). Este hecho da validez jurídica a los trámites realizados con la administración, ya que junto con la firma va incluido el momento exacto en el que se hizo el trámite para que no haya dudas acerca de los plazos.

EL CAMINO S.L. como empresa puede sacarse un certificado como persona jurídica que le permita realizar los citados trámites por Internet, además de usarlo para la firma de contratos electrónicos con otras empresas. El artículo 7 de la LFE lo dispone del siguiente modo:

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

"2. La custodia de los datos de creación de firma asociados a cada certificado electrónico de persona jurídica será responsabilidad de la persona física solicitante, cuya identificación se incluirá en el certificado electrónico."

"3. Los datos de creación de firma sólo podrán ser utilizados cuando se admita en las relaciones que mantenga la persona jurídica con las Administraciones públicas o en la contratación de bienes o servicios que sean propios o concernientes a su giro o tráfico ordinario. Asimismo, la persona jurídica podrá imponer límites adicionales, por razón de la cuantía o de la materia, para el uso de dichos datos que, en todo caso, deberán figurar en el certificado electrónico."

"4. Se entenderán hechos por la persona jurídica los actos o contratos en los que su firma se hubiera empleado dentro de los límites previstos en el apartado anterior.
Si la firma se utiliza transgrediendo los límites mencionados, la persona jurídica quedará vinculada frente a terceros sólo si los asume como propios o se hubiesen celebrado en su interés. En caso contrario, los efectos de dichos actos recaerán sobre la persona física

responsable de la custodia de los datos de creación de firma, quien podrá repetir, en su caso, contra quien los hubiera utilizado."

En estos momentos la web no dispone de servicios personalizados para los usuarios. Todos los usuarios que acceden a la web ven las mismas cosas, a excepción de clientes como hoteles, ayuntamientos y asociaciones que disponen de una zona personal donde modificar sus datos, servicios y demás información que ofrecen al peregrino.

Como hemos comentado en anteriores ocasiones, la web lleva en activo casi 10 años y no ha tenido grandes cambios desde entonces. Desde hace algún tiempo se está pensando en servicios personalizados para el peregrino, se quiere acercar la web, a la llamada web 2.0 en la que los usuarios puedan colaborar y beneficiarse unos y otros de la colaboración general.

El usuario en general está cansado de acceder a una web e introducir un usuario y contraseña para acceder a sus servicios personalizados, por lo que el uso del dni electrónico como sistema seguro de acceso sería algo a tener en cuenta. Esto permitiría realizar compras sin rellenar los pesados formularios con los datos personales.
Los artículos 15 y 16 de la Ley de Firma Electrónica definen qué es el dni electrónico y sus requisitos y características:

*"**Artículo 15.** Documento nacional de identidad electrónico.*
1. El documento nacional de identidad electrónico es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos.
2. Todas la personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia del documento nacional de identidad electrónico para acreditar la identidad y los demás datos personales del titular que consten en el mismo, y para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica en él incluidos.

Artículo 16. *Requisitos y características del documento nacional de identidad electrónico.*

1. Los órganos competentes del Ministerio del Interior para la expedición del documento nacional de identidad electrónico cumplirán las obligaciones que la presente Ley impone a los prestadores de servicios de certificación que expidan certificados reconocidos con excepción de la relativa a la constitución de la garantía a la que se refiere el apartado 2 del artículo 20.

2. La Administración General del Estado empleará, en la medida de lo posible, sistemas que garanticen la compatibilidad de los instrumentos de firma electrónica incluidos en el documento nacional de identidad electrónico con los distintos dispositivos y productos de firma electrónica generalmente aceptados."

5. ADMINISTRACIÓN ELECTRÓNICA

5.1.- INTRODUCCIÓN

Según nos indica el profesor Davara en el manual sobre este tema, el artículo 45 de la Ley de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común (LRJPAC), en su epígrafe "Incorporación de medios técnicos" indica que:

"las Administraciones Públicas impulsarán el empleo y aplicación de las técnicas y medios electrónicos, informáticos y telemáticos, para el desarrollo de su actividad y el ejercicio de sus competencias, con las limitaciones que a la utilización de estos medios establecen la Constitución y las Leyes y que, los documentos emitidos , cualesquiera que sea su soporte, por medios electrónicos informáticos o telemáticos por las AAPP, o lo que éstas emitan como copias de originales almacenados por estos mismos medios, gozarán de la validez y eficacia de documento original siempre que quede garantizada su autenticidad, integridad y conservación y, en su caso, la recepción por el interesado, así como el cumplimiento de la garantías y requisitos exigidos por ésta u otras Leyes".

Esto que en un principio era un ejercicio de buena voluntad, por parte de las administraciones, con la llegada de la Ley 11/2007, de 22 de Junio, de acceso electrónico de los ciudadanos a los Servicios Públicos se convirtió en algo de obligado cumplimiento.
Las Administraciones Públicas han tenido como plazo hasta el 1 de Enero de este año 2010, para adecuar sus procedimientos para que el ciudadano pueda llevarlos a cabo de forma telemática, sin ningún menoscabo en el servicio.
En definitiva, lo que en un primer momento era un *podrán*, pasó a un *deberán* y en la actualidad a un *deben*.

El ciudadano podrá exigir su derecho a comunicarse con las Administraciones por medios electrónicos y la contrapartida de ese derecho es la obligación de éstas de dotarse de los medios y sistemas electrónicos para que ese derecho pueda ejercerse.

El artículo 3 de la Ley declara los fines de la misma, que son los siguientes:

1. *Facilitar el ejercicio de derechos y el cumplimiento de deberes por medios electrónicos.*
2. *Facilitar el acceso por medios electrónicos de los ciudadanos a la información y al procedimiento administrativo, con especial atención a la eliminación de las barreras que limiten dicho acceso.*
3. *Crear las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos.*
4. *Promover la proximidad con el ciudadano y la transparencia administrativa, así como la mejora continuada en la consecución del interés general.*
5. *Contribuir a la mejora del funcionamiento interno de las Administraciones Públicas, incrementando la eficacia y la eficiencia de las mismas mediante el uso de las tecnologías de la información, con las debidas garantías legales en la realización de sus funciones.*
6. *Simplificar los procedimientos administrativos y proporcionar oportunidades de participación y mayor transparencia, con las debidas garantías legales.*
7. *Contribuir al desarrollo de la sociedad de la información en el ámbito de las Administraciones Públicas y en la sociedad en general.*

El Título Preliminar de la Ley reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos indicando que las AAPP utilizarán la Tecnologías de la Información asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen.

5.2.- DERECHOS DE LOS CIUDADANOS

En el Título I de la Ley se establecen los derechos de los ciudadanos en sus relaciones con las Administraciones Públicas por medios electrónicos.

La Ley para garantizar el ejercicio de los derechos, establece la obligación para la administración de habilitar canales para la prestación de dichos servicios electrónicos.

También establece la obligación de cada Administración de facilitar a las otras Administraciones los datos de los interesados que se requieran para la tramitación de un procedimiento. Atendiendo a la LOPD el afectado debe haber dado su consentimiento, pudiendo ser emitido y recabado por medios electrónicos.

De este modo se evita al ciudadano tener que reenviar sus datos cada vez que tenga una relación con al Administración y no aportar documentos que ya haya aportado anteriormente.

Esto exige a la Administración una buena gestión del consentimiento y de las posibles revocaciones del mismo,.

Para la defensa de los derechos del ciudadano se incorpora la figura del "Defensor del usuario de la Administración electrónica".

El artículo 6 de la Ley describe los derechos de los ciudadanos como sigue:

"1. Se reconoce a los ciudadanos el derecho a relacionarse con las Administraciones Públicas utilizando medios electrónicos para el ejercicio de los derechos previstos en el artículo 35 de la Ley 30/1992, de 26 de noviembre, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, así como para obtener informaciones, realizar consultas y alegaciones, formular solicitudes, manifestar consentimiento, entablar pretensiones, efectuar pagos, realizar transacciones y oponerse a las resoluciones y actos administrativos.

2. Además, los ciudadanos tienen en relación con la utilización de los medios electrónicos en la actividad administrativa, y en los términos previstos en la presente Ley, los siguientes derechos:

- *a. A elegir, entre aquellos que en cada momento se encuentren disponibles, el canal a través del cual relacionarse por medios electrónicos con las Administraciones Públicas.*

b. *A no aportar los datos y documentos que obren en poder de las Administraciones Públicas, las cuales utilizarán medios electrónicos para recabar dicha información siempre que, en el caso de datos de carácter personal, se cuente con el consentimiento de los interesados en los términos establecidos por la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal, o una norma con rango de Ley así lo determine, salvo que existan restricciones conforme a la normativa de aplicación a los datos y documentos recabados. El citado consentimiento podrá emitirse y recabarse por medios electrónicos.*
c. *A la igualdad en el acceso electrónico a los servicios de las Administraciones Públicas.*
d. *A conocer por medios electrónicos el estado de tramitación de los procedimientos en los que sean interesados, salvo en los supuestos en que la normativa de aplicación establezca restricciones al acceso a la información sobre aquéllos.*
e. *A obtener copias electrónicas de los documentos electrónicos que formen parte de procedimientos en los que tengan la condición de interesado.*
f. *A la conservación en formato electrónico por las Administraciones Públicas de los documentos electrónicos que formen parte de un expediente.*
g. *A obtener los medios de identificación electrónica necesarios, pudiendo las personas físicas utilizar en todo caso los sistemas de firma electrónica del Documento Nacional de Identidad para cualquier trámite electrónico con cualquier Administración Pública.*
h. *A la utilización de otros sistemas de firma electrónica admitidos en el ámbito de las Administraciones Públicas.*
i. *A la garantía de la seguridad y confidencialidad de los datos que figuren en los ficheros, sistemas y aplicaciones de las Administraciones Públicas.*
j. *A la calidad de los servicios públicos prestados por medios electrónicos.*
k. *A elegir las aplicaciones o sistemas para relacionarse con las Administraciones Públicas siempre y cuando utilicen estándares abiertos o, en su caso, aquellos otros que sean de uso generalizado por los ciudadanos.*

3. En particular, en los procedimientos relativos al acceso a una actividad de servicios y su ejercicio, los ciudadanos tienen derecho a la realización de la tramitación a través de una ventanilla única, por vía electrónica y a distancia, y a la obtención de la siguiente información a través de medios electrónicos, que deberá ser clara e inequívoca:

a. *Los requisitos aplicables a los prestadores establecidos en territorio español, en especial los relativos a los procedimientos y trámites necesarios para acceder a las actividades de servicio y para su ejercicio.*

b. *Los datos de las autoridades competentes en las materias relacionadas con las actividades de servicios, así como los datos de las asociaciones y organizaciones distintas de las autoridades competentes a las que los prestadores o destinatarios puedan dirigirse para obtener asistencia o ayuda.*
c. *Los medios y condiciones de acceso a los registros y bases de datos públicos relativos a prestadores de actividades de servicios.*
d. *Las vías de reclamación y recurso en caso de litigio entre las autoridades competentes y el prestador o el destinatario, o entre un prestador y un destinatario, o entre prestadores."*

5.3.- RÉGIMEN JURÍDICO

La regulación del régimen jurídico de la administración electrónica se encuentra en el Título II de la Ley y tiene 4 capítulos acerca de la regulación de:

- La sede electrónica.
- La identificación inequívoca y autenticación de los ciudadanos y administraciones.
- Los registros, las comunicaciones y las notificaciones electrónicas.
- Los documentos y archivos electrónicos.

5.3.1.- La sede electrónica

El profesor Davara en el manual correspondiente a la Administración electrónica, define la sede electrónica como:

"una dirección electrónica que cada administración deberá poner a disposición de los ciudadanos a través de redes electrónicas y cuya gestión y administración corresponde a una Administración Pública funcionando con plena responsabilidad respecto de la integridad, veracidad y actualización de la información y los servicios a los que puede accederse a través de la misma".

La Administración oportuna es la responsable de la integridad, veracidad y actualización de la información y los servicios a los que pueda accederse a través de ella.

La integridad conlleva que la información sea veraz y completa. Esto exige la actualización, como corresponde con el principio de calidad de los datos y el derecho de rectificación presentes en la LOPD (lo mismo ocurre con la información obtenida tras el tratamiento de los datos).

En la sede electrónica se podrán publicar:

- Los Diarios o Boletines Oficiales, con los mismos efectos que en su formato en papel. La publicación del BOE en la sede electrónica tendrá carácter oficial y auténtico, derivándose de dicha publicación los efectos previstos en el título preliminar del Código Civil y en las restantes normas aplicables.

- Los actos y comunicaciones, que por disposición legal o reglamentaria deban publicarse en tablón de anuncios o edictos.

5.3.2.- Identificación y autenticación

En el Capítulo Segundo del Título II de la Ley se encuentran los métodos de identificación y autenticación centradas en la firma electrónica.
La identificación y autenticación es en ambos sentidos. La administración debe conocer con qué ciudadano está tratando, y el ciudadano debe tener garantía y seguridad jurídica de que accede a una sede electrónica.

El artículo 13 en su apartado 2 identifica las formas de identificación y autenticación para el ciudadano potenciando el uso del DNi-e:
"Los ciudadanos podrán utilizar los siguientes sistemas de firma electrónica para relacionarse con las Administraciones Públicas, de acuerdo con lo que cada Administración determine:

a. *En todo caso, los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, para personas físicas.*
b. *Sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico reconocido, admitidos por las Administraciones Públicas.*
c. *Otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen."*

En el apartado 3 del mismo artículo se encuentran las formas de identificación electrónica y autenticación de documentos para la administración pública:
"Las Administraciones Públicas podrán utilizar los siguientes sistemas para su identificación electrónica y para la autenticación de los documentos electrónicos que produzcan:

a. *Sistemas de firma electrónica basados en la utilización de certificados de dispositivo seguro o medio equivalente que permita identificar la sede electrónica y el establecimiento con ella de comunicaciones seguras.*
b. *Sistemas de firma electrónica para la actuación administrativa automatizada.*

c. *Firma electrónica del personal al servicio de las Administraciones Públicas.*
d. *Intercambio electrónico de datos en entornos cerrados de comunicación, conforme a lo específicamente acordado entre las partes."*

No obstante, las Administraciones Públicas podrán determinar, de forma justificada, los supuestos y condiciones de utilización por los ciudadanos de otros sistemas de firma electrónica, como claves concertadas en un registro previo, aportación de información conocida por ambas partes u otros sistemas no criptográficos.

Los certificados electrónicos reconocidos serán admitidos por las AAPP como válidos para relacionarse con las mismas, siempre y cuando el prestador de servicios de certificación ponga a su disposición la información que sea precisa en condiciones que resulten tecnológicamente viables y sin que suponga coste alguno para aquellas.

5.3.3.- Los registros, las comunicaciones y las notificaciones electrónicas

En el Capítulo Tercero del Título II de la Ley, se encuentra la regulación sobre los registros electrónicos, las comunicaciones y las notificaciones electrónicas.
En el caso de los registros electrónicos se trata su creación y funcionamiento, indicando qué tipos de documentos podrán admitir así como el cómputo de plazos.

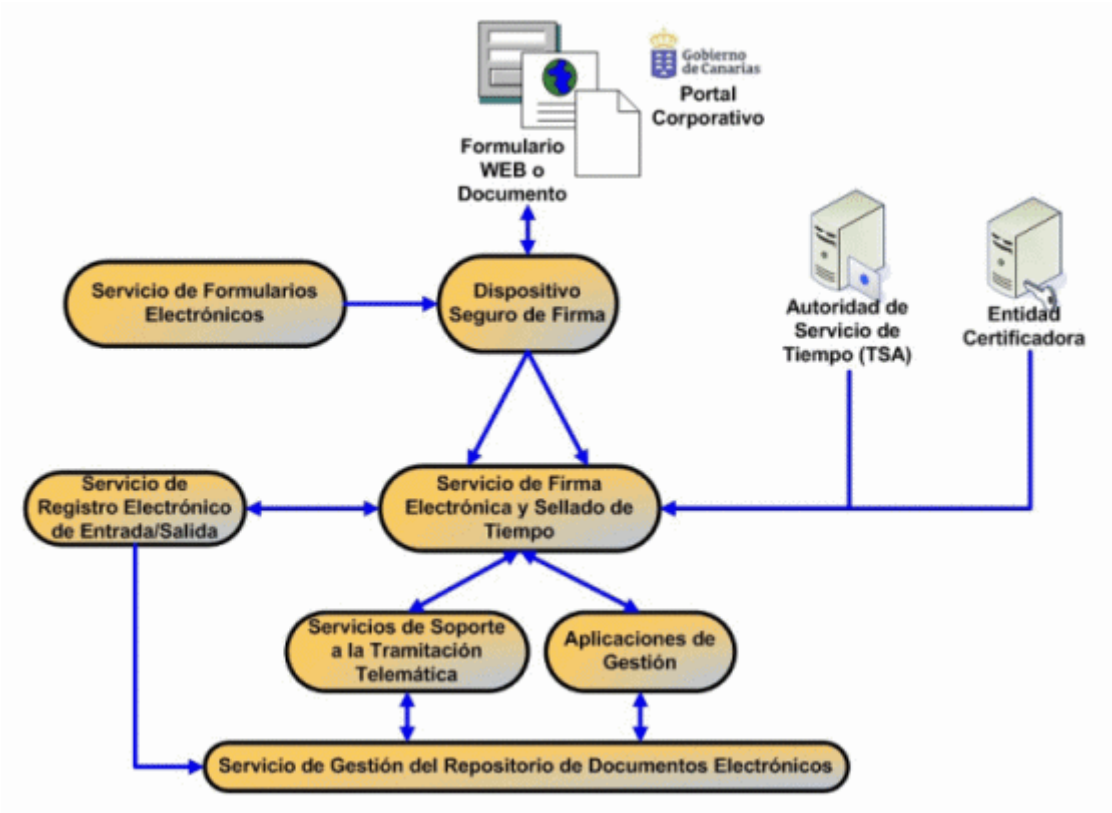
El ciudadano puede elegir la forma de comunicarse con la administración, sea de forma electrónica o no, y sin que esto le vincule pudiendo cambiar cuando quiera.

"Las comunicaciones electrónicas serán válidas siempre que exista constancia de la transmisión y recepción, de sus fechas, del contenido íntegro de las comunicaciones y se identifique inequívocamente al remitente y al destinatario" [art. 27.3].

"La realización en la práctica de las notificaciones por medios electrónicos exigirá que el ciudadano haya señalado dicho medio como preferente o haya consentido su utilización" [art. 28.1].

"El sistema de notificación debe permitir acreditar la fecha y hora en la que se produzca la puesta a disposición del interesado al acto objeto de notificación, así como la de acceso a su contenido, momento a partir del cual al notificación se entenderá practicada a todos los efectos legales"[art. 28.2].

La acreditación de la fecha y hora se lleva a cabo con la intervención de una autoridad de sellado de tiempo. Éste se junta con la firma electrónica y permite acreditar el momento en que se realizó el trámite.



Ejemplo de sellado de tiempo con la firma electrónica en la AAPP de Canarias

5.3.4.- Los documentos y los archivos electrónicos

En este cuarto capítulo se regulan las condiciones de validez de un documento electrónico y el proceso de las copias electrónicas, tanto las realizadas a partir de documentos emitidos en papel, como las copias en soporte electrónico y las condiciones para realizar en soporte papel copia de originales emitidos en formato electrónico y viceversa.

También se trata la posibilidad de almacenar por medios electrónicos los documentos utilizados en las actuaciones administrativas. Define el expediente

electrónico como el conjunto de documentos electrónicos correspondientes a un procedimiento administrativo, cualquiera que sea el tipo de información que contenga.

El artículo 30.1 indica que:

"Las copias realizadas por medios electrónicos de documentos electrónicos emitidos por el propio interesado o por las Administraciones Públicas, manteniéndose o no el formato original, tendrán inmediatamente la consideración de copias auténticas con la eficacia prevista en el artículo 46 de la Ley 30/1992, de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común, siempre que el documento electrónico original se encuentre en poder de la Administración, y que la información de firma electrónica y, en su caso, de sellado de tiempo permitan comprobar la coincidencia con dicho documento".

El punto 2 del mismo artículo dice que:

"Las Administraciones Públicas podrán obtener imágenes electrónicas de los documentos privados aportados por los ciudadanos, con su misma validez y eficacia, a través de procesos de digitalización que garanticen su autenticidad, integridad y la conservación del documento imagen, de lo que se dejará constancia. Esta obtención podrá hacerse de forma automatizada, mediante el correspondiente sello electrónico."

Los medios o soportes en que se almacenen documentos deberán contar con medidas de seguridad que garanticen la integridad, autenticidad, confidencialidad, calidad, protección y conservación de los documentos almacenados, asegurando la identificación de los usuarios y el control de accesos, así como el cumplimiento de las garantías previstas en la legislación de protección de datos.

5.4.- CONDICIONES DE CONFIANZA: TRAZABILIDAD

En la introducción a este tema se han nombrado los fines de la presente Ley. El tercero de los fines es crear las condiciones de confianza en el uso de los medios electrónicos, estableciendo las medidas necesarias para la preservación de la integridad de los derechos fundamentales, y en especial los relacionados con la intimidad y la protección de datos de carácter personal, por medio de la garantía de la seguridad de los sistemas, los datos, las comunicaciones y los servicios electrónicos.

Los procedimientos para establecer una política de seguridad efectiva, con una correcta definición y gestión de los servicios y procesos de seguridad, en el flujo de la información son el elemento necesario en su propio diseño.

Suponemos que las administraciones habrán seguido unas directrices comunes en el uso de las TIC, para posibilitar la interoperabilidad del sistema y el acceso común a bases de datos y ciudadanos.
Esto habrá facilitado la integración de sistemas y procedimientos con el aprovechamiento y optimización de resultados y dar de este modo una imagen de unidad que de confianza al usuario.

El apartado V de la Exposición de Motivos de la Ley dice que el principal reto que tiene la implantación de las TIC en la sociedad en general y en la Administración en particular es la generación de confianza suficiente que elimine o minimice los riesgos asociados a su utilización. Entendiendo la confianza como algo que posee las cualidades recomendables para el fin que se destina. Esta confianza viene de la mano de la seguridad física, lógica y jurídica de la utilización de las TIC.

La trazabilidad es el seguimiento de actos, comunicaciones y expedientes. Esto genera diversos beneficios en los mecanismos en la administración electrónica:

- Accesibilidad y conveniencia.
- Rapidez.

- Bajo coste.
- Reducción de la carga de trabajo.

Otra definición de trazabilidad o rastreabilidad es la "aptitud para rastrear la historia, la aplicación o la localización de una entidad mediante indicaciones registradas".
Conocer los pasos que ha seguido un expediente permite conocer si ha sido bien tratado, los tiempos de tratamiento… esto genera confianza en el ciudadano y sobre todo una mayor validez jurídica.

5.5.- USOS EN LA EMPRESA

Como ya se ha comentado en el tema de la firma electrónica, la empresa como tal carece de firma electrónica, por lo que su relación con la administración es de forma personal, acudiendo el representante a realizar los trámites que necesite en cada momento.

Sería interesante acudir a la Fábrica Nacional de Moneda y Timbre para adquirir un certificado de persona jurídica. De esta forma se mejoraría la seguridad en las comunicaciones de la empresa y se podían hacer los trámites oportunos con la Administración de forma electrónica.
Esto ahorraría bastante tiempo al personal de la empresa, ya que no siempre se consigue realizar los trámites en una sola vez, por lo que hay que volver a llevar un papel u otro. De forma electrónica se consigue hacer esto sin tener que moverse de la oficina.

6. DOMINIOS REGISTRADOS EN LA EMPRESA

6.1.- INTRODUCCIÓN

Como dice el profesor Davara en el Factbook Comercio Electrónico, "los nombres de dominio han pasado de ser un elemento casi desconocido dentro delámbito 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 el número de ordenadores era tan pequeño, que para comunicarse entre ellos era asequible conocer la IP del ordenador en la red.
Con la ampliación del número se hizo necesario idear una forma más amigable de identificar los ordenadores. En ese momento nacieron los nombres de dominio y los DNS (sistemas de nombre de dominio), sistema que identifica la ip de un ordenador a través de su nombre de dominio.

Poco a poco los nombres de dominio se empezaron a convertir en identificadores comerciales, aparecieron los primeros conflictos relacionados con estos nombres.

Los nombres de dominio se clasifican en dos grupos: nombres de dominio de primer nivel y nombres de dominio de segundo nivel.
Los nombres de dominio de primer nivel conocidos por las siglas TLD (Top Level Domain), son los que se sitúan al final de la dirección, después del último punto. Hay 2 tipos principales de nombres de dominio de primer nivel: genéricos y de país. La entidad responsable de los genéricos es el ICANN y el CCTLD para el caso de los códigos de pais. En España el responsable es RED.es.

Los nombres genéricos se crearon para hacer referencia al tipo de actividad que se desarrolla en ese dominio. Dentro de este tipo hay unos de libre acceso y otros de acceso restringido (hacen referencia a un tipo de ejercicio específico y para poder solicitarlo hay que demostrar su pertenencia).

Genéricos – Libres: **.com** (comercio), **.net** (empresas que sólo operan en la red), **.org** (organizaciones).

Genéricos – Restringidos: **.gov** y .**gob** (para Gobierno y Entidades Públicas), **.mil** (para el Departamento de Defensa de los Estados Unidos), **.int** (para Entidades Internacionales, organizaciones como la ONU), **.edu** (servicios de educación).

Recientemente han aparecido un nuevo conjunto, para una mejor clasificación y evitar la actual saturación:

- **.aero**: Reservado para la industria aeronáutica.
- **.asia:** Reservado para los paises asiáticos.
- **.biz**: Genérico libre equivalente al .com para fines comerciales.
- **.cat**: Reservado para la comunidad catalana.
- **.coop**: Restringido para las cooperativas, hecho que habrá que demostrar al adquirirlo.
- **.info**: Genérico libre sin ningún requisito específico.
- **.jobs**: Reservado para la comunidad de gestión de recursos humanos.
- **.mobi**: Reservado para la comunidad de consumidores y proveedores de servicios de telefonía móvil.
- **.museum**: Restringido para los museos que quieran tener presencia en Internet.
- **.name**: Genérico libre, con el único requisito de que sean personas físicas. Serán de doble punto para nombre y apellido.
- **.pro**: Reservado para profesionales de determinadas categorías, que se dividirán en subcategorías. Se deberá demostrar el ejercicio de la profesión para la que se reserve.
- **.tel**: Reservado para particulares y empresas que quieran almacenar y gestionar su agenda de contactos.
- **.travel**: Reservado para la comunidad cuya actividad principal sea la industria de los viajes turísticos.

Los nombres de país hacen referencia al país y están formados por 2 caracteres (**.es**, **.co**, **.au**, **.en**).

Los nombres de dominio de segundo nivel, conocidos por las siglas SLD (Second Level Domain) hacen referencia a la marca o nombre comercial.
Estos son los que las empresas y otras entidades quieren registrar bajo distintos nombres de primer nivel distintos.
Pueden surgir conflictos por el derecho a usar cierto nombre, ya que puede infringir derechos de propiedad intelectual, industrial, o derechos de la competencia.

En España existe un tercer nivel (entre el primero y el segundo) para indicar la actividad dentro de del país. Hay que demostrar la pertenencia al tipo de actividad y que esta se realiza en el país. Los aprobados son:

- **.com.es**: Personas físicas o jurídicas y las entidades sin personalidad que tengan intereses o mantengan vínculos con España.
- **.nom.es**: Personas físicas que tengan intereses o mantengan vínculos con España.
- **.org.es**: Entidades, instituciones o colectivos con o sin personalidad jurídica y sin ánimo de lucro que tengan intereses o mantengan vínculos con España.
- **.gob.es**: Administraciones Públicas españolas y las entidades de Derecho público de ella dependientes, así como cualquiera de sus dependencias.
- **.edu.es**: Entidades, instituciones o colectivos con o sin personalidad jurídica, que gocen de reconocimiento oficial y realicen funciones o actividades relacionadas con la enseñanza o la investigación en España.

Las entidades que verifican qué dominios están ocupados y si se cumplen las condiciones para seleccionar uno u otro son los agentes registradores auditables.

6.2.- REGISTRO DE UN NOMBRE DE DOMINIO

A la hora de registrar un dominio en Internet, se debe tener claro que lo que registramos es un nombre de dominio de segundo nivel, bajo un dominio de primer nivel. También hay que tener en cuenta qué tipo de dominio de primer nivel vamos

a reservar (genérico o territorial) y si cumplimos las posibles condiciones en el caso de los genéricos reservados.

Una vez que se tiene seguro el dominio que se quiere registrar, se debe acudir al ICANN para localizar los registradores acreditados. En la siguiente dirección están disponible los distintos tipos de dominios de primer nivel, junto con las entidades autorizadas para registrar dominios de Internet, el país al que pertenecen, los dominios con los que trabajan y un enlace a su web.
http://www.icann.org/en/registrars/accredited-list.html

El siguiente paso es seleccionar la entidad registradora que mejor se adapte a nuestras necesidades. Se rellena el impreso de solicitud de nombre de registro y se pagan las tasas del registro.
Las propias entidades nos informarán en el momento del registro, si éste está ocupado o no, para el dominio de primer nivel seleccionado y si existen otros de primer nivel libres (podemos reservar los que queramos siempre que cumplamos los requisitos).

Una vez hecho esto, sólo debemos esperar la confirmación de registro por parte de la entidad registradora.
Una vez que se ha confirmado el registro, nuestros datos estarán disponibles en una base de datos de libre acceso en Internet, por dos motivos principalmente:

- Que cualquiera que quiera registrar un dominio sepa cuáles están ocupados o no.
- Que en caso de conflicto acerca del nombre de dominio, la persona que quiera hacer una reclamación ante los órganos adecuados sepa contra quién tiene que hacerlo.

Registro de un dominio .es

La disposición adicional sexta (Sistema de asignación de nombres de dominio bajo el ".es") de la Ley 34/2002 de Comercio Electrónico regula los principios de asignación de dominios de primer nivel de país para España (".es").

El último Plan Nacional de Nombres de Dominio aprobado el 18 de marzo de 2003 simplificó las reglas que permiten obtener un nombre de dominio a:
"cualquier persona física o jurídica y a las entidades sin personalidad que tengan intereses o mantengan vínculos con España".
Ante dos solicitudes que cumplan los requisitos, se mantiene la norma *"el primero que llega se lo queda"*.
Redujo las limitaciones y prohibiciones exigidas para la formación de nombres de dominio de segundo nivel.
Permite la transmisión del nombre de dominio con el requisito del consentimiento de su titular y la notificación a la Autoridad de asignación. Con esto se pretende evitar los registros abusivos y especulativos de los nombres de dominio.

El plan según cuenta el profesor Davara en el Manual de Derecho Informático consta de cuatro capítulos:
"El primero dedicado a disposiciones generales, objeto del Plan, la autoridad de asignación de nombres de código de país <<.es>> (Red.es), a la posibilidad de asignar nombres de dominio de segundo y tercer nivel y a los agentes registradores acreditados.

El segundo establece las reglas de asignación de los nombres de dominio de segundo nivel, su legitimación para la asignación y las limitaciones específicas, listas de nombres prohibidos y listas de nombres reservados.

El tercero hace referencia a las reglas de asignación de los nombres de dominio de tercer nivel, tipos de nombres asignables, criterio general de asignación y la legitimación para la asignación de estos nombres.

El cuarto recoge las disposiciones comunes para nombres de dominio de segundo y tercer nivel y las normas comunes para la asignación de nombres de dominio, su transmisión, derechos y obligaciones derivados de la asignación y mantenimiento de los nombres de dominio y la responsabilidad por su utilización."

Derechos y deberes de los titulares de un dominio .es

Los derechos de los titulares de un dominio .es son los siguientes:

- Utilizar el nombre de dominio a efectos de direccionamiento, siempre que respete las normas comunes de asignación y el mantenimiento de las condiciones exigidas para su concesión.
- Derecho a la continuidad en el uso y calidad del servicio que presta la autoridad de asignación, siempre que se mantenga al día de los pagos.

Los deberes de los titulares son los siguientes:

- Facilitar sus datos identificativos, siendo responsables de su veracidad y exactitud.
- Respetar las reglas y condiciones técnicas que establezca la autoridad de asignación para el adecuado funcionamiento del sistema.
- Informar inmediatamente a la autoridad de asignación de todas las modificaciones que se produzcan en los datos asociados al registro del nombre de dominio.
- Obligación de someterse al sistema de resolución extrajudicial de conflictos previsto en el Plan Nacional.

6.3.- PASOS A DAR EN CASO DE CONFLICTO

Los conflictos entre la propiedad intelectual y los nombres de dominio se basan en que las marcas tienen generalmente un ámbito territorial en su creación, mientras que los nombres de dominio no. Un dominio de Internet es accesible desde cualquier parte del mundo.

Esto posibilita la mala fe, en la creación de un nombre de dominio, permitiendo que una persona se apropie de un nombre de dominio que recuerde al nombre de una marca, o incluso con el mismo nombre y distinto nombre o extensión del primer nivel.

Para resolver estos casos de conflicto entre nombres de dominio y marcas, la ICANN dispone de proveedores de servicios para resolución de controversias.
Uno de los más conocidos es la OMPI/WIPO (Organización Mundial de la Propiedad Intelectual) que dispone de un centro de arbitraje y mediación.

En el caso que estamos estudiando podríamos decir que existe un posible conflicto con los dominios **.org** y **.net**, ya que cuando acudimos a estos, se redireccionan a otro dominio con un nombre totalmente distinto: http://www.elcaminoasantiago.com/ Esta web tiene cierta información acerca del Camino de Santiago aunque la empresa que está detrás de la misma es un bar de Madrid llamado CafeCoke.

Se podría considerar que es un caso de **explotación de reputación ajena,** un registro de un nombre de dominio que coincide con una marca con alta reputación, con el fin de beneficiarse de este hecho (en visitas, publicidad, ventas…).

Por el momento no se ha pensado en tomar medidas legales, ya que no se le considera una competencia lo suficientemente importante (tras una breve visita a la web, la impresión general es de un sitio bastante cutre, mal diseñado, difícil de manejar…) como para considerar un posible gasto en arbitraje. Los pasos a seguir en caso de conflicto son los siguientes:

Visitar la página whois.org para verificar el propietario del dominio conflictivo, su idioma (hay que redactar la demanda en el lenguaje del demandado) y dónde lo registró.

Debe acudir al agente registrador oportuno para que bloquee la página conflictiva.
Acudir a la OMPI y seleccionar el número de árbitros que quiere para este conflicto (y pagar la cuantía oportuna).

Redactar una demanda por triplicado (el propietario, el agente registrador y el OMPI) en la que se solicite la devolución del dominio. **Para ello debe demostrar claramente** (aportando todas las pruebas que se consideren oportunas) **los siguientes tres puntos**:

- El demandado no tiene derecho o interés legítimo para reservar ese nombre de dominio.
- Existe mala fe en la selección del dominio, o en los contenidos que aparecen en el mismo (burla, enriquecimiento personal…). *****
- Carácter idéntico o similar, hasta el punto de causar confusión, entre el nombre de dominio objeto de la disputa y la marca de la cual el demandante es titular.

* La Política de Resolución de Controversias de Nombres de Dominio Genéricos (UDRP), ha establecido una serie de factores que podrían ayudar a EL CAMINO a demostrar el uso de la mala fe (uno de los tres aspectos a demostrar) por parte del demandado, como pueden ser:

1. *circunstancias que indiquen que usted ha registrado o que ha obtenido el nombre de dominio fundamentalmente con el objeto de vender, alquilar o para transferir el registro del nombre de dominio al demandante que es el propietario de la marca o marca de servicio o a un competidor de éste, por una valiosa cantidad superior a sus gastos documentados relacionados directamente con el nombre de dominio; o*
2. *circunstancias que indiquen que usted ha registrado el nombre de dominio con el fin de impedir que el propietario de la marca o marca de servicio desprestigie la marca con un nombre de dominio semejante, siempre y cuando esté ligado a un modelo de tal conducta; o*

3. *circunstancias que indiquen que usted ha registrado el nombre de dominio fundamentalmente con el propósito de crear problemas en el negocio de un competidor; o*
4. *circunstancias que indiquen que al usar el nombre de dominio, usted intencionadamente intenta atraer, para beneficio comercial, usuarios de Internet a su sitio web o a cualquiera otra localización on line, favoreciendo una posibilidad de confusión con la marca del demandante en cuanto a origen, patrocinio, filiación o promoción de su sitio web o de un producto o de un servicio en su sitio web.*

El punto 4 parece el indicado a usar en caso de querer resolver el conflicto. Parece claro que en principio la web de un bar de Madrid, poco tiene que ver con el dominio usurpado, ya que ni la temática del local tiene que ver con el Camino de Santiago, ni su nombre comercial hace referencia al mismo.

En la demanda también se debe dejar claro si se quiere recuperar el dominio, o que deje de usarlo en los términos actuales.

Se debe presentar la demanda ante el centro de mediación y arbitraje (incluida la portada de transmisión). Se debe enviar el original y 4 copias por mensajería. Deberemos entregar una copia al demandado, otra al registrador del dominio.

El siguiente paso será seleccionar cuántos árbitros se quiere que intervengan en la demanda (1 o 3) y pagar la tasa correspondiente.

A partir de aquí el centro de arbitraje deberá verificar que se cumplen los requisitos formales en la demanda, la presentarán al demandado que deberá responder en 20 días.

El centro de arbitraje nombrará al árbitro/s. Una vez nombrado el árbitro/s se notificará a las partes y la fecha límite de resolución (salvo circunstancias excepcionales).

El árbitro/s puede dirigirse a cualquiera de las partes y solicitar la documentación que considere oportuna.

Una vez que el árbitro/s ha tomado una decisión esta es irrevocable, salvo que una de las partes considere que ha habido defecto de forma y lo demande por vía judicial.

7. PROPIEDAD INTELECTUAL

7.1.- INTRODUCCIÓN

Las empresas trabajan con dos tipos de productos, los bienes materiales y los bienes inmateriales.
Una definición muy simple de bien material es aquel que se puede tocar. Hace muchos años que las empresas comprendieron que los productos que inventaban, fabricaban y vendían podían ser copiados, por lo que se crearon leyes que permitieran proteger, tanto el diseño, como los procesos de fabricación de estos bienes. De esta idea surgió la Propiedad Industrial.

Con el tiempo las empresas se dieron cuenta que no sólo sus bienes materiales eran importantes, si no, que la información y otros bienes no materiales eran tan importantes o más y no estaban protegidos.

Los bienes inmateriales se pueden usar por muchas personas a la vez, no se deterioran con el uso, pudiendo incluso mejorar.
Copiar un bien material tiene un coste y un esfuerzo, mientras que los inmateriales son tan reducidos que pueden llegar a ser despreciables.

Con esta nueva perspectiva se crearon los instrumentos necesarios para proteger y evitar cualquier problema con los activos inmateriales. Destacan entre estos:

- Los nombres de dominio: Se han incorporado recientemente como objeto de proporción, ya que como se vió en el tema anterior se asocian directamente al nombre o marca de la empresa y se identifica con él.
- Las creaciones del intelecto: Las creaciones cada vez tienen un mayor valor en la empresa por las posibilidades que abren.

La aparición de las nuevas tecnologías hizo necesaria una modificación de esta legislación para permitir la protección de nuevos bienes.

El Real Decreto Legislativo 1/1996 de 12 de abril, en su artículo 10 dice lo siguiente acerca de la propiedad intelectual:

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

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

El objeto de protección es sobre el bien y la persona que gozará de protección será el autor, que suele ser una persona física, aunque la ley también prevé que sea una persona jurídica.

Los derechos que atribuye la Ley son de dos tipos: derechos personales y derechos patrimoniales.

- Los derechos personales: Son irrenunciables e inalienables. No tienen valor económico y no caducan.
- Los derechos patrimoniales: Permiten obtener retribución por la explotación de su obra. Son derechos transmisibles por el autor. Puede ser en exclusiva o no.

Las obras pueden ser de varios tipos:

Independientes: Son las realizadas íntegramente por una sola persona aunque se publique en conjunto con otras. Esta persona tiene por tanto los derechos personales y patrimoniales de la misma.

En colaboración: El artículo 7 dice lo siguiente acerca de la autoría y sus derechos:

"1. Los derechos sobre una obra que sea resultado unitario de la colaboración de varios autores corresponden a todos ellos.

2. Para divulgar y modificar la obra se requiere el consentimiento de todos los coautores. En defecto de acuerdo, el Juez resolverá.

Una vez divulgada la obra, ningún coautor puede rehusar injustificadamente su consentimiento para su explotación en la forma en que se divulgó.

3. A reserva de lo pactado entre los coautores de la obra en colaboración, éstos podrán explotar separadamente sus aportaciones, salvo que causen perjuicio a la explotación común.

4. Los derechos de propiedad intelectual sobre una obra en colaboración corresponden a todos los autores en la proporción que ellos determinen. En lo no previsto en esta Ley, se aplicarán a estas obras las reglas establecidas en el Código Civil para la comunidad de bienes."

Colectivas: El artículo 8 dice lo siguiente sobre la autoría y derechos en este tipo de obras:

"Se considerará 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.

Salvo pacto en contrario, los derechos sobre la obra colectiva corresponderán a la persona que la edite y divulgue bajo su nombre."

Compuestas: Se considerará 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.

Se presume autor, salvo que se pruebe lo contrario, a quien aparezca como tal en la obra. La firma de la obra, salvo prueba en contra, da la autoría de la misma al firmante y gozará de la protección de la ley.

A nivel europeo, la regulación de los derechos de autor en la Sociedad de la Información ha sido regulada por la Directiva 20001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo.
Su objeto es armonizar las legislaciones de los Estados miembros en relación con la protección jurídica de los derechos de autor con especial consideración a la sociedad de la información, sin modificar las normas existentes, como la protección jurídica de los programas de ordenador o de las bases de datos.

Las medidas tecnológicas son definidas en la Directiva como "*toda técnica, dispositivo o componente que, en si funcionamiento normal, esté destinado a impedir o restringir actos referidos a obras o prestaciones protegidas que no cuenten con la autorización del titular de los derechos de autor o de los derechos afines a los derechos de autor establecidos por ley o el derecho sui generis previsto en el Capítulo III de la Dorectiva 96/9/CE*"

7.2.- PROTECCIÓN JURÍDICA DEL SOFTWARE

El software es un producto obtenido a través de una actividad creativa, con una gran carga de intelecto. El software por sí sólo no hace nada, necesita una máquina que permita su funcionamiento y esta máquina se encuentra bajo protección de los derechos de protección de la propiedad industrial (patentes).

En cambio en el caso del software no existe uniformidad respecto a la protección que debe recibir. Estados Unidos y Japón protegen el software mediante derechos de propiedad industrial y en la Unión Europea se protege mediante derechos de propiedad intelectual.

Como trata el profesor Davara en el Manual de Derecho Informático:
"El software ha sido excluido del ámbito de protección por el camino de las patentes. Nuestra Ley de Patentes (art. 4.2) excluye la protección de los programas de ordenador por medio de las patentes. Sin embargo, se acepta la patentabilidad de un proceso completo en el que una parte del mismo sea desarrollada por un programa de ordenador.

Debido a la gran facilidad de copia, sin apenas coste y de ser utilizados por diferentes personas en múltiples copias, se ha hecho evidente la necesidad de una forma de protección jurídica, debido a la importancia económica y el desarrollo que tienen en la actualidad"

Ventajas de la protección del software mediante derechos de autor.

- **Plazo de protección**: El plazo de protección de los derechos de autor es de 70 años después de la muerte del autor, mucho más amplio que en las patentes (20 años). La ventaja es evidente, en cambio otras corrientes dicen que el plazo de patente es más que suficiente debido a la obsolescencia de este tipo de productos.

- **Copias no autorizadas**: La copia es uno de los mayores problemas debido a su facilidad, pudiendo en algunos casos tener mejor calidad la copia que el original. Esta facilidad posibilita su comercialización bajo otro nombre y por personas que no tengan derechos sobre el.

  Los derechos de autor parece que protegen mejor este hecho que las patentes.

- **Nacimiento de la protección de forma automática**: La protección mediante derechos de autor nace en el momento en que una persona crea una obra, por lo que evita trámites que se desconocen y permite centrarse en la creación.

  La protección mediante patentes precisa de su inscripción registral para surtir efecto. A la hora de registrarlo será necesario que se comprueben una serie de requisitos.

- **Pocas obligaciones para el titular**: El titular de los derechos de autor no necesita cumplir ningún requisito adicional a la propia creación de la obra, mientras que para la patentabilidad de un objeto hay que tener en cuenta el estado de la técnica, que sea algo completamente original, que sea susceptible de entrar a formar parte de la industria…

7.3.- PROTECCIÓN JURÍDICA DE LA BASE DE DATOS

Las bases de datos son de una forma genérica depósitos de información que puede ser útil para distintos usuarios y que pueda ser recuperable por distintas aplicaciones.

Estos depósitos guardan la información de manera estructurada, añadiéndole el valor de una recuperación y tratamiento (automatizado o no), que permita una mayor utilidad.

El contenido de la base de datos será un conjunto de documentos o datos, y la propia base de datos, le otorga una estructura lógica que le da un valor añadido.

Los documentos no tienen por qué ser propiedad de la misma persona que la base de datos. Son objetos distintos con protección distinta.

En función del tipo de acceso las bases de datos pueden ser:

- **Autónomas**: De acceso local, desde el lugar en que nos encontremos utilizando el ordenador, normalmente la base de datos se encontrará en el mismo equipo, en el propio disco duro (si son de consulta y/o modificación), en un cd o dvd (si son sólo de consulta).
- **On-line**: A las que se accede de forma remota, y que se encontrarán en un servidor común.

La ley considera base de datos:

"las 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"

De esta forma se confiere protección a las bases de datos on-line y off-line.

Las bases de datos son obras de creatividad intelectual en cuanto a la estructura que contiene información.

Se realiza un importante esfuerzo creativo para crear una estructura que permita almacenar información y recuperarla de acuerdo a una consulta planteada. Este esfuerzo se ve protegido contra posibles ataques.

Al igual que ocurre con el software, la copia o el acceso a las bases de datos, se puede hacer a un coste muy inferior al de su creación y desarrollo. El objeto de protección no es sólo la recopilación de información, sino todo el procedimiento de creación de una base de datos.

La protección de la estructura de la base de datos se entiende como "forma de expresión de la selección o disposición de sus contenidos, no siendo extensiva a éstos".

Tal y como explica el profesor Davara en el Factbook Comercio electrónico, las bases de datos llevan una doble protección en nuestro ámbito jurídico. Por un lado una previsión específica en la Ley 5/1998, de 6 de marzo y por otro el RDLeg 1/1996 sobre protección intelectual.
Por un lado tienen la protección de los derechos de autor, y por el otro el derecho "sui generis", resultando ambos derechos complementarios.

El derecho de autor requiere del requisito de originalidad, como el resto de obras amparadas por la propiedad intelectual, en la selección o disposición de sus contenidos, y sin prejuicio de la protección que recaiga sobre estos.
El contenido por tanto recibe una protección específica en función de la materia e independiente al de la base de datos.

La protección conferida por el derecho de autor tampoco se extiende a los elementos que resulten necesarios para el funcionamiento o la consulta de algunas bases de datos como tesauro y los sistemas de indexación. Estos elementos en cambio sí que están protegidos por el derecho "sui generis".

El derecho "sui generis" por tanto, es una figura jurídica para proteger una base de datos con respecto a:
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.

Esta protección también recaerá sobre las modificaciones sustanciales que se produzcan posteriormente que cumplan con los requisitos de protección.
El titular del derecho "sui generis" es el fabricante. Este derecho 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 al término del proceso.

7.4.- EN QUÉ AFECTA LA LPI A EL CAMINO S.L.

La web de la empresa surge mediante un contrato informático con una empresa socia. En este contrato el gerente de EL CAMINO S.L. solicita la creación de una página web con unas características concretas.
Una página web dinámica y contractual como es el caso consta de 2 partes bien diferenciadas:
Un software que manipula la lógica de la página web y permite la presentación de los datos (almacenados en una base de datos) por pantalla, en función una estructura proporcionada por el diseñador.
Un base de datos donde se almacena información estructurada en forma de tablas, con una serie de campos. Estos datos se pueden modificar por medio del software y son los que se van a presentar por pantalla.

Como se ha visto en la introducción esto es un caso bastante claro de obra colectiva. El gerente tiene la iniciativa de la creación y la coordina para que se ajuste a sus necesidades. Diferentes personas colaboran en su creación, pero sólo tiene derechos sobre la obra el gerente, tanto en el caso de derechos personales como patrimoniales.

8. CONTRATACIÓN INFORMÁTICA

8.1.- INTRODUCCIÓN

La contratación informática no es otra cosa que la contratación de bienes o servicios informáticos, es decir, el contrato por el que por una parte se obliga a entregar un bien informático o prestar un servicio informático y la otra parte a pagar por ello.

Es importante diferenciarlo del concepto contratación electrónica, en la que se contrata cualquier tipo de bien o servicio, por medios electrónicos. El soporte de contratación es electrónico, los bienes o servicios de cualquier clase.
En un contrato informático, la contratación puede ser electrónica o no, pero los bienes o servicios deben estar relacionados con la informática (compraventa de equipos, mantenimiento de redes, desarrollo de software…).

¿Qué es un bien informático o un servicio informático?
El profesor Davara lo define en el Factbook Comercio electrónico del siguiente modo:
“Por bienes informáticos debemos entender 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.”

“Los servicios informáticos son todos aquellos que sirven de apoyo y complemento a la actividad informática en una relación de afinidad con ella”.

Características de los contratos informáticos

Los contratos informáticos no tienen legislación propia, lo que hace que para su composición haya que elegir contratos similares, y adaptarlos a las necesidades del momento, esto hace que tengan unas características propias:

Son contratos atípicos: Como no tienen regulación propia, se basan en la autonomía de la voluntad de las partes.

Su objeto suele estar compuesto por un conjunto de prestaciones, esto puede suponer un conjunto de normas de aplicación. Como ejemplo, una venta de un equipo informático además de la entrega del equipo a cambio de un precio, puede incluir la instalación del equipo, la prueba…

Los contratantes no suelen estar en la misma posición de conocimiento (especialmente entre persona jurídica y persona física). Esto puede provocar inseguridad jurídica por el desconocimiento de la totalidad de las prestaciones, o si la solución es la más adecuada a sus necesidades. En algunos casos puede conllevar la intervención de abogados y expertos informáticos para la redacción precisa del contrato.

La importancia de la protección al consumidor en los contratos informáticos. Se aplica la Ley 26/1984, de 19 de Julio, General para Defensa de los Consumidores y Usuarios.

Son contratos complejos que pueden incluir prestaciones de distintos tipos de contratos. Se pueden considerar contratos híbridos entre varios debido a la amplitud de su objeto.

Son contratos que pueden llevar mucho tiempo en su redacción por largas negociaciones entre las partes (ej. Desarrollo de aplicaciones a medida, contratos de outsourcing entre empresas…)

8.2.- TIPOS DE CONTRATOS

Los contratos informáticos se clasifican generalmente según 2 criterios:

El objeto: Debido a que hay distintos tipos de objetos y cada uno tiene unas características propias conviene hacer un estudio por separado de cada uno de estos.

- Contratos de hardware: El concepto del contrato hace referencia a todo aquello que físicamente forme parte del equipo y aquellos elementos auxiliares necesarios para el funcionamiento del sistema a implementar.
- Contratos de software: Hay que diferenciar el tipo de software sobre el que se basa el contrato (de base o sistema, de utilidad o de usuario). El software de usuario responderá a las características específicas del que contrata, mientras que el de utilidad o el de base tienen unas características más generales o concretas.
- Contratos de instalación llave en mano: Incluyen tanto el hardware, el software y determinados servicios de mantenimiento y formación del usuario.
- Contratos de servicios auxiliares: El concepto del contrato lo forman servicios complementarios como mantenimiento de equipos o programas, la formación de las personas que van a usar los equipos y programas…

El negocio jurídico: Otra forma de clasificación se puede realizar basándose en el negocio jurídico en el que se realiza.

- De compraventa: En el que un suministrador o vendedor se obliga a entregar una cosa determinada y el comprador a pagar un precio cierto.
- De arrendamiento financiero o leasing: En el que una entidad o intermediario financiero adquiere un bien del suministrador, y lo pondrá en posesión del usuario, que lo tendrá en régimen de arrendamiento financiero, hasta que pase a su propiedad.
- De alquiler: En el que el suministrador de un bien informático da al usuario el goce o uso del mismo durante un tiempo determinado y por un precio cierto.

El suministrador tendrá la obligación de efectuar todas aquellas reparaciones necesarias para que se conserve en estado de servir para el uso a que ha sido destinada (Código Civil, art.1554).

- De mantenimiento: Puede ser tanto de equipos como de programas o integral. Se puede incluir un servicio de formación, asesoramiento o consulta.
- De prestación de servicios: En el que se pueden incluir análisis, especificaciones, horas máquina, tiempo compartido, programas, etc.

Outsourcing informático: Se puede definir como 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, con la finalidad de optimizar los resultados de la misma, a la vez que permite a la entidad el acceso a nuevas tecnologías y la utilización de recursos especializados de los que no dispone.
El outsourcing puede llegar a la transferencia de personas de la plantilla de una a otra entidad.

Facilities Management: Consiste en la gestión de las instalaciones, recursos y elementos que componen un centro de informática de una entidad. Atenderá a la gestión de los elementos que componen el sistema de información, como la gestión de las redes (internas y externas), mantenimiento preventivo, operativo y de solución de problemas.

8.3.- CONTENIDO RECOMENDADO DE UN CONTRATO

A la hora de redactar un contrato informático hay una serie de puntos que conviene tratar y dejar claro. A continuación se van a nombrar los más importantes y en el siguiente punto se verá un contrato real donde se analizará si están bien tratados y si alguno es mejorable.

Redacción de objetivos o resultados: Es uno de los puntos más importantes, ya que muchos de los contratos se basan en el resultado. Qué se espera obtener con el contrato, o qué se ofrece con el contrato (depende de quién lo redacte). Muy importante en el caso del desarrollo de aplicaciones a medida ya que es conveniente que toda la funcionalidad esperada esté lo más clara posible.
Se pueden incluir los requisitos para la aceptación del producto.
Definiciones: Al hilo de lo anterior, es recomendable un anexo de definiciones de aquellos términos más técnicos, o que un usuario medio no pueda entender.
Asesoramiento a la hora de posibles incompatibilidades con los equipos actuales, posibilidades de los equipos. El suministrador debe asesorar al cliente de que lo que contrata/adquiere es compatible con lo que tiene actualmente. Esto es válido tanto para el desarrollo de software a medida, compra o arrendamiento de equipos…
Plazo de entrega: Válido tanto para el desarrollo de software como entrega de equipos. Puede estar incluido el tiempo de pruebas/depuración o definirse por separado.
Mantenimiento/actualizaciones/ampliaciones: Diferenciar entre los tipos de mantenimiento (preventivo, correctivo y predictivo). Se pueden definir un nº de ampliaciones incluidas, diferenciadas por tipos o no.
Garantía: Importante en el caso de compra/venta de equipos. A diferenciar el resultado en función del tiempo, y del error/avería. Puede ser el cambio del equipo/sistema sin cargo, la reparación a cargo de uno u otro…
La garantía deberá hacerse extensible a posibles reclamaciones de terceros, respecto a cualquier derecho de propiedad intelectual o industrial, de forma que el

suministrador asegure al usuario que estará libre de reclamación. Deberá incluir defensa jurídica para exonerar al usuario en caso de reclamación.

Respuesta ante incidencias: Tiempo de respuesta, horario de atención al cliente, nº de incidencias incluidas en el precio, quién se desplaza y si implica un coste, tipos de incidencias y su coste…

Formación: En el caso del desarrollo de software a medida, actualizaciones de software, compra de nuevos equipos, puede ser necesaria una formación del personal. Debe quedar claro si está incluida en el precio final, quién la da, en qué horario y dónde (en la empresa cliente, local externo…).

Precio y forma de pago: Precio total o por servicios o entregas. Si el pago se realiza a la entrega o fraccionado y en qué tiempos.

Pago en garantía: Se puede pagar una parte en la entrega y el resto pasado un tiempo que permita verificar que todo funciona como se especificó.

Repuestos: Se deberá fijar el tiempo mínimo durante el que el usuario tendrá repuestos para su equipo/sistema.

Seguro: En este tipo de contrato se deben especificar 2 tipos de seguros. Uno es el de pérdida, deterioro o cualquier daño asegurable y que afecte patrimonialmente a equipos y programas.

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.

Exclusividad: Muy importante en el caso de desarrollos a medida, ya que si no se pone permites al desarrollador volver a vender la aplicación a terceros.

Confidencialidad: Imprescindible cuando el suministrador tiene acceso a las oficinas, datos de la empresa (puede ser imprescindible un contrato de prestación de servicios, art.12 de la LOPD). También cuando se accede a datos que puedan comprometer la propiedad intelectual o industrial de la empresa.

Propiedad: Deben quedar claros los derechos de propiedad que, sobre el equipo o sobre los programas, queden al firmarse el contrato, o con el pago de la cantidad pactada.

Transferencia de personal: En ocasiones puede ser necesario que personal del suministrador pase un tiempo en la empresa del cliente para una mejor recolección de requisitos, o conocimiento del problema a solucionar.

Preparación del local/es: Se especificará, en su caso, a cargo de quién corre la preparación de los locales, indicando su localización, las necesidades de adaptación, plazos y posibles penalizaciones.

Prohibición de subarrendar: Si se trata de un contrato de arrendamiento de un bien informático se establecerá esta cláusula. El artículo 1550 del Código Civil indica que si no se ha pactado expresamente lo contrario, el subarrendado podrá subarrendar en todo o en parte la cosa arrendada.

8.4.- EJEMPLO DE CONTRATO

CONTRATO MANTENIMIENTO INFORMÁTICO

De una parte, la empresa "**Info-Soluciones**, **Sociedad limitada**" con CIF B-09XXXXXX, con domicilio en Burgos, avenida xxx xxx nº x, , oficina nº 0, c.p. 09XXX, representada por D……., con NIF…….

De otra, el cliente, D……., con NIF……y con domicilio en Burgos, calle ……. / o la empresa …….. ……con CIF nº ……y domicilio social en ……, representada por D……, con NIF……., en calidad de ……. ……

Las partes intervinientes, por medio del presente contrato, convienen el servicio de mantenimiento informático que ofrece la empresa **Info-Soluciones**, **S.L.**, y que encarga el cliente firmante, para su regulación por medio de las siguientes

ESTIPULACIONES:

Objeto del contrato:

El objeto de este contrato es el arrendamiento de servicios de mantenimiento informático, que llevará a cabo la empresa "**Info-Soluciones**, **S.L.**", a través de personal especializado, y en las condiciones que se especifican seguidamente.

TRABAJOS INCLUIDOS EN EL SERVICIO:

Auditoria e inventario de hardware y software

Como parte del contrato de mantenimiento **Info-Soluciones** realizará un inventario inicial del equipamiento informático de la empresa cliente cubierto por el presente contrato, siendo firmado por las partes.

Primera actuación

Una vez realizado el inventario se procederá a poner a punto los sistemas informáticos de la empresa cliente, estimando una duración máxima de una hora por equipo[1].

Resto de Actuaciones

Actuación Preventiva: **Info-Soluciones** enviará un técnico a las oficinas del cliente para las siguientes actuaciones:

-Comprobar el correcto funcionamiento de todos los sistemas.

-Poner a punto los sistemas para los cuales se ha firmado este contrato.

-Realizar las reparaciones necesarias desde su última visita (En caso de no poder realizar la operación "in situ", la máquina será trasladada al servicio técnico de **Info-Soluciones** para ser reparada, sin coste adicional para el cliente por su traslado)

-Cumplimentación de un informe con los resultados de la asistencia. El cliente conservará una copia de este informe para hacer un seguimiento de las asistencias realizadas por nuestro personal.

La visita para la actuación preventiva será bimensual salvo que se acuerde con la empresa cliente otra periodicidad, con un máximo de seis visitas anuales.

[1] Si el cómputo total de horas sobrepasa la estimación prevista se facturará según la tarifa vigente.

Actuación bajo demanda: **Info-Soluciones** enviará un técnico a las oficinas del cliente cuando éste –o el personal autorizado para ello- lo solicite, con un máximo de doce visitas anuales.

-Comprobar el correcto funcionamiento de todos los sistemas

-Poner a punto los sistemas para los cuales se ha firmado este contrato

-Realizar las reparaciones necesarias desde su última visita (En caso de no poder realizar la operación "in situ", la máquina será trasladada al servicio técnico de **Info-Soluciones** para ser reparada sin coste adicional para el cliente por su traslado)

-Cumplimentación de un informe con los resultados de la asistencia. El cliente conservará una copia de este informe para hacer un seguimiento de las asistencias realizadas por nuestro personal.

Tiempo de respuesta: Para las visitas a petición de la empresa cliente, **Info-Soluciones** se compromete a desplazarse a la oficina de la empresa cliente a realizar la actuación en menos de 8 horas, siempre dentro de nuestro horario laboral.

-Las asistencias calificadas como urgentes serán atendidas en un plazo máximo de 4 horas. Las incidencias notificadas el viernes o víspera de festivo se resolverán el siguiente día hábil sin incluir sábados.

-La jornada laboral será de lunes a jueves de 9:00 a 14:00 y de 16:00 a 20:30 y los viernes de 9:00 a 14:00.

-Cualquier reparación fuera del horario laboral se facturará por separado. Las asistencias urgentes serán solicitadas siempre por el cliente y se facturarán aparte según la tarifa vigente.

OTROS SERVICIOS INCLUIDOS

Consultoría de Hardware: **Info-Soluciones** proporciona a sus clientes un servicio de asesoramiento en la adquisición, mejora, ampliación o actualización de sus equipos y sistemas instalados.

Consultoría de Software: **Info-Soluciones** proporciona a sus clientes un servicio de asesoramiento en la adquisición, certificación y definición de nuevas aplicaciones, así como optimización de las existentes.

Material informático: **Info-Soluciones** proporciona a sus clientes un servicio de transporte de consumibles, componentes y equipos informáticos hasta su oficina, referido a aquellos que sean objeto de una asistencia programada o bajo demanda; en el caso de que fuera necesario se llevaría fuera de esas visitas, pero se cobraría la pertinente salida.

Mantenimiento red: **Info-Soluciones** proporciona a sus clientes un servicio manteniendo las redes del cliente, tanto locales como de campo amplio (propiedad del cliente), así como el asesoramiento y negociación con operadores de redes de banda ancha.

Mantenimiento y asistencia remota: **Info-Soluciones** proporciona a sus clientes un servicio asistencia remota en horario laboral, que será de lunes a jueves de 9:00 a 14:00 y de 16:00 a 20:30 y los viernes de 9:00 a 14:00, para los equipos que estén cubiertos por este contrato.

Hotline o Asistencia telefónica: **Info-Soluciones** proporciona a sus clientes un servicio de asistencia telefónica para todos los usuarios del sistema, en horario de lunes a viernes de 9:00 a 22:00 en días laborables, excepto festivos en Burgos.

Recepción de avisos de asistencia (vía e-mail, helpdesk, sms, otros que se pacten; 24horas/7dias.)

ÁMBITO DE TRABAJO Y AUTORIZACIONES.

-El ámbito de trabajo será, siempre que sea posible, en las instalaciones del cliente. Cuando la situación así lo exija **Info-Soluciones** trasladará el/los equipos susceptibles de reparación a sus instalaciones en Avenida xxx XXXX, X Oficina 0. 09XXX Burgos. La empresa cliente deberá autorizar dicho traslado…. "autoriza dicho traslado, salvo manifestación en

contra, en cuyo caso asumirá el mayor coste que suponga la reparación dentro de sus instalaciones".

- **Info-Soluciones** queda autorizado a realizar cualquier tipo de intervención, en el equipamiento informático de la empresa cliente, para el correcto desempeño de su trabajo, pudiendo el cliente exigir ser informado de los posibles riesgos ello pudiera suponer. La empresa cliente puede designar una persona para la supervisión de las intervenciones, si se considera oportuno.

PIEZAS A SUSTITUIR

Los elementos o piezas deterioradas o averiadas que sea necesario reemplazar, según el criterio profesional de nuestros técnicos, deberán ser abonados por el cliente. El cliente no tiene obligación de comprar las piezas en **Info-Soluciones**, pero la instalación de piezas compradas a otro proveedor serán instaladas por **Info-Soluciones** y esa instalación será cobrada al precio vigente en nuestras tarifas.

HERRAMIENTAS Y ÚTILES DE REPARACIÓN

Los técnicos que **Info-Soluciones** envíe a realizar las reparaciones que el cliente precise estarán provistos de las herramientas y útiles de reparación necesarios para realizar eficazmente y de manera profesional su trabajo.

PRIVACIDAD Y PROTECCIÓN DE DATOS

Info-Soluciones se compromete por el presente contrato a mantener la privacidad de los documentos y la información contenida en los equipos del cliente, no manteniendo, archivando ni copiando ningún tipo de datos personales que pudieran contener los equipos manejados.

CONDICIONES GENERALES

Control de los equipos y software: **Info-Soluciones** no se considerará obligado a reparar aquellos equipos, programas o sistemas informáticos destinados a funciones impropias de la naturaleza de los mismos (no relacionados con el objeto o actividad de la empresa cliente). De igual forma tampoco estará obligado a reparar aquellos equipos o sistemas informáticos averiados por uso indebido, uso negligente o que haya sido manipulado por personal ajeno a **Info-Soluciones**. Para ello la empresa cliente, permitirá el control de los números de serie de los equipos que incluye este contrato y se equiparan con precintos especiales a todos los equipos sujetos a este contrato de mantenimiento, quedando excluidos del mantenimiento todos aquellos equipos que no tengan en perfecto estado dichos precintos.

La modificación de los equipos que están cubiertos por este contrato repercutirá en la cuota mensual que el cliente pagará a **Info-Soluciones**. A tal fin el cliente informará de estas modificaciones, variándose si procede el inventario antes citado.

El ordenador que sufra una tercera avería, análoga a las anteriores sufridas, deberá ser sustituido de inmediato (o en su defecto reparado en lo que sea menester) para que el puesto de trabajo afectado pueda seguir siendo beneficiario de este contrato de mantenimiento.

El cliente debe facilitar al equipo técnico de **Info-Soluciones** todo el software original con la correspondiente licencia, tanto del sistema operativo como de todos los programas que se utilicen, y ello exclusivamente para llevar a cabo el objeto de este contrato. Así mismo el cliente debe facilitar todos los controladores (drivers) de los dispositivos que tiene instalados. **Info-Soluciones** no se hará responsable de los problemas ocasionados por el uso de software y demás componentes sin licencia, declinando toda la responsabilidad por su uso.

Duración del contrato: Este contrato tendrá una duración inicial de un año. Una vez finalizado el contrato se prorrogará automáticamente, actualizando las tarifas a las vigentes en ese momento, a no ser que alguna de las dos partes avise con 30 días de antelación. El contrato comenzará su vigencia con la firma de este documento.

La rescisión del contrato por cualquiera de las dos partes sin acuerdo mutuo supondrá el abono de 20% del montante total del contrato a la otra parte, en concepto de indemnización.

El proveedor del servicio se reserva el derecho de traspasar el contrato a otra empresa, manteniendo las mismas condiciones generales y económicas.

Precios: El importe de los servicios de este contrato se corresponderá con el presupuesto presentado a la empresa cliente, o en su defecto regirán las tarifas vigentes en el momento de su contratación, las cuales están disponibles en http://www. **Info-Soluciones**.es/tarifas.html. Este contrato únicamente cubre los equipos del cliente para los que ha sido realizado.

El pago se realizará mediante domiciliación bancaria, con un solo pago anual o de la manera que se acuerde entre las partes. **Info-Soluciones** queda facultada para suspender o rescindir unilateralmente los compromisos objeto de este contrato, en el caso de resultar impagado dicho servicio o cualquier otro contratado a **Info-Soluciones** por dicho cliente. En este supuesto, el Cliente asumirá toda responsabilidad por las contingencias que pudieran derivarse de la rescisión de este servicio.

Cualquier impuesto o gravamen que se derive del desarrollo de este Contrato, así como de los pagos -en contraprestación del servicio- serán satisfechos por el Cliente.

Obligatoriedad y fuero: El presente contrato se considerará aceptado con su firma por ambas partes. La firma será realizada por el representante de la empresa Cliente, con facultades suficientes para obligarse en el tráfico.

Info-Soluciones se reserva el derecho de modificar las condiciones del presente contrato avisando siempre con 30 días de antelación a sus clientes. Durante este periodo el cliente tendrá derecho a rescindir el contrato sin penalización alguna.

Para cuantas cuestiones pudieran suscitarse, tanto en la interpretación como en la ejecución de este Contrato, ambas partes contratantes, con renuncia expresa al fuero que pudiera competerles, se someten a la jurisdicción de los Juzgados y Tribunales de Burgos.

Por **Info-Soluciones** _____ Por el cliente: _____

En Burgos, a ___ de _____ de _____

En este contrato se pueden observar claramente los elementos del contrato:

Los sujetos (Proveedor y usuario), *el objeto* (bienes materiales e inmateriales) y *la causa* (por qué se celebra el contrato).

También podemos ver las partes de un contrato:

La parte expositiva

Explicación detallada del objeto de contrato, que se oferta y qué se necesita…

La parte de cláusulas o pactos

Instrucciones de uso, plazo de ejecución, formación, pacto exclusividad, precio y forma de pago, restricciones de uso…

La parte de Anexos

No es necesaria en este caso.

9. MARKETING ELECTRÓNICO

9.1.- INTRODUCCIÓN

La página web www.marketingelectronico.com, define el marketing electrónico del siguiente modo:

"es el estudio de tácticas y estrategias del uso de medios electrónicos (principalmente la *Web*) con el objetivo de captar y fidelizar clientes a través de la publicidad y la venta de productos y servicios.

En consecuencia, el ***Marketing Online*** añade una mayor relevancia y valor estratégico para las empresas a la hora de lograr captar y fidelizar clientes en Internet o cualquier otro medio electrónico mediante numerosas y exitosas tácticas y estrategias."

Las tácticas o estrategias que define como claves se irán tratando en los siguientes puntos.

9.2.- POSICIONAMIENTO WEB

El **SEO** o **Posicionamiento Web** consiste en aplicar diversas técnicas y estrategias orientadas a lograr optimizar el resultado (primeros lugares) dentro de la página de resultados naturales de los motores de búsqueda para determinadas frases clave de búsqueda.

La forma natural se consigue optimizando las páginas teniendo en cuenta los criterios que siguen los buscadores para ordenar sus resultados.

Estos criterios varían de uno a otro, e incluso como en el caso de Google, modifica sus criterios y ofrece informes de los mismos, para que los desarrolladores y expertos puedan aplicarlos.

Estos informes y la experiencia de los internautas han permitido descubrir algunos de estos secretos. La mejor posición no depende de la inversión, sino de la habilidad del desarrollador con los algoritmos que aplica en la web.

Google hasta hace bien poco basaba sus búsquedas en lo que llama PageRank, clasifica las páginas según la cantidad y calidad (examina los términos de cada página y le da una puntuación según la coincidencia de la temática con la que está posicionando) de los enlaces que recibe.
Presupone que si una página ofrece contenidos atractivos y variados, con una buena estructura y orden serán enlazadas por otras páginas.
También tienen en cuenta aspectos internos de la página como:

- Emplear adecuadamente ciertas etiquetas HTML (Title, description, keywords, alt, anchor text,…).
- Estructurar adecuadamente las páginas web y ayudar a los robots de búsqueda a indexar el sitio.
- Redactar el texto haciendo uso de las palabras clave (sin abusar, ya que puede penalizar un exceso de éstas).
- Comentarios en foros, blogs,…

Como se vio durante las clases de Web 2.0. han aparecido los buscadores de nueva generación con un componente más humano a la hora de posicionar los resultados de búsqueda.
Estos buscadores tratan de promover un modelo que ofrece a los usuarios resultados supervisados de calidad, eliminando los resultados que no son de interés para los internautas. Los resultados no dependen exclusivamente de un algoritmo, sino también de la puntuación que dan los propios usuarios a estos enlaces.

Link Building

La **popularidad web** es fundamental para lograr potenciar el **Posicionamiento Natural** en relación a otros sitios de igualdad de condiciones bajo una frase clave. Se basa en la cantidad y calidad de páginas que enlazan a la nuestra.
Algunos de los errores más comunes en esta técnica son:

- **Enlazar sitios prohibidos:** Los sitios comúnmente llamados prohibidos, son aquellos que infringen con los términos de uso de cualquier buscador, por ejemplo, sitios con mensajes de odio, racismo, discriminación, pornografía

infantil, etc. Las penalizaciones por vincularse con websites de éste tipo suelen ser bastante severas, e incluso podría ser llevado a la justicia.

- **Subestimar la temática web:** Muchos piensan que si una web recibe cientos de enlaces, tendrá un buen posicionamiento de manera casi instantánea; sin embargo, esto no es así. Además de una buena cantidad de enlaces, es imprescindible que dichos enlaces sean de calidad. Mientras más relacionada esté la temática del sitio que brinda el enlace, mayor será la calidad del link.

- **Vincularse a granjas de enlaces:** Google no suele ver con buenos ojos que existan sitios webs que se dediquen al almacenamiento de enlaces. Constituye otro de los casos más comunes de black hat que terminan en penalizaciones por parte de los motores de búsqueda.

9.3.- PUBLICIDAD EN INTERNET

La publicidad en Internet tiene como principal ventaja su menor coste y su alta capacidad de personalización. Es un medio ideal para comunicarse con grupos de personas con intereses muy específicos, bien sea mediante herramientas de mailing (con las precauciones vistas en los temas de LOPD y Comercio Electrónico respecto al envío de publicidad), o incluyendo publicidad en webs que tratan temas específicos que puedan interesarnos.

Según un estudio del 2007, la publicidad en Internet en España creció un 132% con respecto al año anterior y un estudio de Microsoft de este año, afirma que se espera que siga subiendo a nivel mundial un 5%, a pesar de o debido a la crisis y recortes provocados por la situación económica actual.

El índice de respuesta en la publicidad online es mucho más elevado que en la publicidad tradicional, no sólo por la capacidad de personalización, sino también por la comodidad. Al hacer clic en el link o banner de una empresa, el acceso es inmediato. El receptor de la publicidad emitida tiene la capacidad de seleccionar qué es lo que quiere ver y cuándo, lo que mejora su atención.
La respuesta a campañas de publicidad online puede ser medida y analizada más eficazmente, gracias a la observación del servidor web mediante herramientas como Google Analytics.

Siguiendo con el tema anterior, **SEO** o posicionamiento web, una técnica de publicidad en Internet es el **SEM** (Search Engine Marketing). Esta consiste en la compra de espacios publicitarios que aparezcan en los buscadores, cuando el usuario usa determinadas palabras clave. Son los llamados enlaces patrocinados, generalmente de texto y presentes en los buscadores más importantes (Google, Yahoo!-Overture, MSN Search,...). A continuación se incluye un extracto del artículo incluido en la web http://google.dirson.com/posicionamiento.net/sem/ .

Muchas empresas son incapaces de llegar a todos los potenciales clientes que desearían, solamente mediante el posicionamiento. Así que recurren a estos

'enlaces patrocinados', los cuales se facturan por cada 'click' que el usuario realiza sobre ellos.
Algunos puntos a tener en cuenta en el uso de esta técnica son:

En qué sistema publicitario anunciarse.
Actualmente, los tres sistemas más importantes son AdWords (de Google),Overture (de Yahoo!) y espotting. Cada uno de ellos dispone de diferentes buscadores en cuyos resultados se sitúan los anuncios.
Por ejemplo, AdWords se muestra en Google, pero también en Terra, Ozú, 'ya.com', AOL o 'ask.com'. Y los anuncios de Overture se pueden ver en Yahoo!, Altavista, 'MSN Search' o Hispavista.

Un experto SEM debe conocer los buscadores en los que su producto pueda tener más impacto, para asesorarle qué producto le conviene para su campaña publicitaria.

En qué sitios web anunciarse.
Estos tres sistemas publicitarios disponen de redes de afiliados (portales, sitios web de diferente temática) en los que se puede insertar publicidad contextual (en función del contenido del que trate cada página web).

Qué palabras comprar.
Un experto SEM debe decidir qué palabras hay que comprar en una determinada campaña publicitaria en buscadores, puesto que existen numerosos términos que quizá atraigan a visitantes que no son potenciales clientes.

Por ejemplo, si una empresa que vende planes de pensiones online compra la palabra *pensiones*, quizá accedan a su web usuarios que buscaban información sobre pensiones para alojarse en vacaciones.

Con qué presupuesto contar.
Las tarifas de los sistemas publicitarios de los buscadores se establecen por Pago Por Click (sólo pagamos cuando el usuario pincha en el anuncio). Además, la

cantidad a pagar y la posición del anuncio dentro de los resultados del buscador se determina a través de un sistema de pujas que requiere una cierta práctica.

El experto SEM debe estimar qué precio pagar, así como cuál es el presupuesto con el que contar para cada campaña en función de las necesidades.

Qué textos elegir.

Gran parte del éxito de una campaña publicitaria está en el texto de los anuncios. Además de llamar la atención de muchos más usuarios (lo que supondrá más clientes potenciales), en algunos casos -como el de AdWords de Google- también supondrá mejor posicionamiento dentro del grupo de los enlaces patrocinados. Y es que este sistema premia a los anuncios que tienen mejor porcentaje de clicks con mejores posiciones, y castiga a los que no consiguen llamar la atención del usuario incluso con la eliminación dentro de determinadas búsquedas.

El profesional SEM debe optimizar el texto de un anuncio que, en muchos casos, no superará los 100 caracteres de longitud.

Qué segmentación utilizar.

Algunos de los sistemas publicitarios en buscadores son capaces de segmentar los anuncios en función de la localización geográfica del usuario, o del idioma en el que realiza las búsquedas.

Puede ser interesante mostrar la publicidad solamente a los que realizan búsquedas desde la misma provincia en la que se encuentra el negocio, o situados dentro de un radio de 50 km, ...

9.4.- LAS REDES SOCIALES

Las redes sociales son una herramienta más, que permite a una empresa un contacto directo con sus clientes.
En el caso que estamos analizando, **EL CAMINO S.L.** dispone de una página en Facebook. Desde esta página los usuarios interactúan entre ellos buscando compañeros de viaje, resolviéndose dudas entre ellos, o solicitando información directamente a la empresa mediante mensajes personales.

La página es un modo más de mantener informados (nuevos productor o servicios en la tienda, nuevos servicios en la web…) a usuarios actuales, o usuarios que no conocen la empresa, ni la página web, pero que la han visto a un amigo y se han unido.

Los propios usuarios nos informan de novedades en el camino, albergues que no funcionan correctamente, o han dejado de existir, tramos mal señalizados… esto nos permite actualizar la página día a día y fidelizar los clientes.

10. BIBLIOGRAFÍA

10.1.- APUNTES

📖 [Davara, 2009]
Davara Rodríguez, Miguel Ángel. “Teoría General sobre Protección de Datos”.

📖 [Davara, 2009]
Davara Rodríguez, Miguel Ángel. “Los Principios de la Protección de Datos”.

📖 [Davara, 2009]
Davara Rodríguez, Miguel Ángel. “Medidas de Seguridad”.

📖 [Davara, 2009]
Davara Rodríguez, Miguel Ángel. “Obligaciones y Responsabilidades del Titular de los Ficheros”.

📖 [Davara, 2009]
Davara Rodríguez, Miguel Ángel. “Reglamento de la LOPD”.

📖 [Davara, 2009]
Davara Rodríguez, Miguel Ángel. “Ficheros con Fines de Publicidad y Prospección Comercial”.

📖 [Davara, 2009]
Davara Rodríguez, Miguel Ángel. “Actualización del Factbook de Comercio Electrónico”.

📖 [Davara, 2009]
Davara Rodríguez, Miguel Ángel. “Normativa Firma Electrónica: Ámbito Nacional”.

📖 [Davara, 2009]
Davara Rodríguez, Miguel Ángel. “Normativa Firma Electrónica: Ámbito Comunitario”.

📖 [Davara, 2009]
Davara Rodríguez, Miguel Ángel. “Normativa Firma Electrónica: Ámbito Nacional”.

📖 [Davara, 2009]
Davara Rodríguez, Miguel Ángel. “La Administración Electrónica”.

📖 [Davara, 2009]
Davara Rodríguez, Miguel Ángel. “Protección Jurídica del Software”.

📖 [Davara, 2009]
Davara Rodríguez, Miguel Ángel. “Normativa Aplicable a los Nombres de Dominio”.

📖 [Davara, 2009]
Davara Rodríguez, Miguel Ángel. “Contratación Informática”.

📖 [Laso, Iglesias, 2010]
Laso Ballesteros Isidro, Iglesias Meléndez Marta. “Web 2.0 y Empresa 2.0: Legislación”.

10.2.- LIBROS

📖 [Davara, 2008]
Davara Rodríguez, Miguel Ángel. "Análisis del Real Decreto 1720/2007: El reglamento de la LOPD". Editorial: DaFeMa.
ISBN: 978-84-612-4744-8. Depósito legal: M-29520-2008

📖 [Davara, 2008]
Davara Rodríguez, Miguel Ángel. "***Manual de Derecho Informático***" 10ª Edición. Editorial: ARANZADI.
ISBN: 978-84-8355-819-5. Depósito legal: NA 2912/2008

📖 [Davara, 2004]
Davara & Davara Asesores Jurídicos. "***FACTBOOK® COMERCIO ELECTRÓNICO***". 3ª Edición. Editorial: ARANZADI.
ISBN: 84-9767-905-9. Depósito legal: NA 3383/2004

10.3.- RECURSOS ELECTRÓNICOS

📖 "Procedimiento de Resolución Unificado de Conflictos". Sítio oficial de ICANN, organismo regulador de nombres de dominio de primer nivel genéricos.
<http://www.wipo.int/amc/es/docs/icannpolicy.pdf>

📖 "Conceptos acerca de la Firma Electrónica". Xolido es una empresa que vende herramientas de creación de firma electrónica. Tiene una sección donde explica con sencillez estos conceptos y con diagramas sencillos.
<http://www.xolido.com/lang/productosyservicios/firmaelectronicayselladodetiempo/verificadoresxolido/?idboletin=1923&idseccion=10777&idarticulo=65729>

📖 "Documentación y legislación de todos los temas del Magister". La página de Davara & Davara Asesoría Jurídica ha sido el referente en los distintos temas que se han visto a lo largo del Magister.
<http://davara.net/c/mac-tic/pagina_centro_proteccion.asp>

📖 "El Nuevo Modelo de Comercialización del Marketing Actual". Gunther Ketterer el 22-05-2010. Página dedicada al mundo de la empresa, con artículos acerca del comercio electrónico, marketing, tecnología, redes sociales…
<http://marketingdiario.com/marketing-online/marketing-actual>

📖 "Marketing Electrónico". Empresa de marketing online que ofrece servicios de marketing basados principalmente en posicionamiento web, link building y publicidad online todo ello gestionado mediante la analítica web para medir los resultados.
<http://www.marketingelectronico.com/>

📖 "SEM Search Engine Marketing". Página web con diversos artículos y consejos para tener una web de calidad y bien posicionada.
<http://google.dirson.com/posicionamiento.net/sem/>

📖 "Firma electrónica y sellado de tiempo" Página del gobierno de Canarias con información del funcionamiento de la firma electrónica y el sellado de tiempo en la administración pública Canaria.
<http://www.gobiernodecanarias.org/platino/firmaysellado.html>