

ADECUACIÓN A LAS TIC DE UNA EMPRESA DE TRANSPORTES



Universidad de Burgos

Autor del proyecto: Javier Sáez Moneo

Tutor del proyecto: Prof. Miguel Ángel Davara Rodríguez

Directores del Magíster:

Dr. Emilio S. Corchado Rodríguez

Dr. Álvaro Herrero Cosío

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

UNIVERSIDAD DE BURGOS

II Edición. Burgos, Julio 2010.

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

AGRADECIMIENTOS

En primer lugar quisiera agradecer a Emilio Corchado la oportunidad que me ha brindado para realizar este Magister, y por todo lo que he aprendido en su desarrollo. Gracias por todos los esfuerzos que has hecho siempre para que los estudiantes de la Universidad de Burgos tengamos las mejores oportunidades de formación.

Gracias a mi familia. A los que están y me apoyan, y a los que ya no están y recuerdo todos los días.

Gracias a los profesores del Magister Miguel Ángel Davara, Elena Davara y Emilio Montoya, por todos los conocimientos que han compartido con los alumnos. Por transmitirlos desde la experiencia, pero con la ilusión del primer día.

Gracias a los profesores de la parte técnica, porque ha sido un placer volver a ver a quienes me formaron como ingeniero, y recordar los tiempos de estudiante.

Y gracias también a todos los compañeros del Magister. A muchos ya os considero amigos. Sin el apoyo mutuo de todos, no estaríamos hoy aquí.

Gracias a todos vosotros, el Magister ha llegado a buen puerto.

Javier Sáez Moneo

(Mi firma no electrónica)

ÍNDICE GENERAL

CASO DE ESTUDIO

Caso de Estudio	página 4
-----------------------	----------

PROTECCIÓN DE DATOS

Introducción LOPD	página 14
Definiciones.....	página 19
Fases de tratamiento	página 23
Principios.....	página 26
Derechos	página 42
Procedimientos	página 52
Medidas de Seguridad	página 57
Obligaciones y Responsabilidades del Titular del Fichero	página 64
Ficheros de Publicidad y Prospección Comercial	página 80
Ficheros de Solvencia Patrimonial	página 84

TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Comercio Electrónico	página 94
Firma Electrónica	página 111
Protección Jurídica del Software	página 123
Protección Jurídica de las BBDD	página 129
Nombres de Dominio	página 133
Contratación Informática.....	página 143
Administración y Fiscalidad Electrónicas	página 155
Web 2.0.....	página 163

BIBLIOGRAFÍA

Bibliografía.....	página 172
-------------------	------------

ADECUACIÓN A LAS TIC DE UNA EMPRESA DE TRANSPORTES



CASO DE ESTUDIO

Autor del proyecto: Javier Sáez Moneo

Tutor del proyecto: Prof. Miguel Ángel Davara Rodríguez

Directores del Magíster:
Dr. Emilio S. Corchado Rodríguez
Dr. Álvaro Herrero Cosío

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

UNIVERSIDAD DE BURGOS

II Edición. Burgos, Julio 2010.

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

CONTENIDO

Contenido	4
1. Presentación de la empresa	5
2. Necesidades de la Empresa	6
Tratamiento de Datos de Carácter Personal.....	6
Desarrollo Software de la Empresa.....	6
Presencia en Internet	7
Trato con la Administración Pública	7
Empresa 2.0	7

1. PRESENTACIÓN DE LA EMPRESA

La empresa a la que se asesorará en el presente proyecto es Transportes S.A. Se trata de una empresa de transportes terrestres de ámbito nacional, recién fundada, que requiere que sus procedimientos de tratamiento informatizado de datos sean adecuados a las tecnologías de la información y la comunicación.

De este modo, cuando la empresa comience a operar en su ámbito empresarial, deberá cumplir con las leyes vigentes que regulen su cometido, así como con las referidas al tratamiento de datos de carácter personal y al comercio electrónico.

Asimismo, se deberá adecuar su actividad dentro del ámbito de la sociedad de la información en la que vivimos: la empresa requerirá presencia en Internet para la oferta y contratación de sus servicios, trabajará con la administración electrónica, requerirá desarrollos de software que necesitarán protección y tratará de ser una empresa 2.0.

2. NECESIDADES DE LA EMPRESA

La empresa que se presenta en éste Caso de Estudio ha sido elegida debido a que la naturaleza de su actividad permite abordar todos los aspectos que se han desarrollado teóricamente durante el curso. De éste modo, se tiene una empresa que:

- Manejará datos de carácter personal de los clientes, y de trabajadores.
- Realizará operaciones de comercio y contratación electrónica, ya que permitirá solicitar servicios por Internet.
- Tendrá publicidad en Internet.
- Necesitará desarrollos de software y de bases de datos para el desempeño de su actividad.
- Necesitará un nombre de dominio para su página en Internet.
- Permitirá comercio electrónico seguro en su página.
- Tratará con la Administración Pública.
- Será una Empresa 2.0

TRATAMIENTO DE DATOS DE CARÁCTER PERSONAL

- Datos de los clientes. Los clientes realizan los encargos de transporte de mercancías, de modo que sus datos tendrán que ser manejados por la empresa para poder cumplir con su cometido. También serán manejados para fines publicitarios.
- Datos de trabajadores. El manejo de los datos de los trabajadores es necesario en la relación laboral que mantienen con la empresa, para cumplir obviamente con las obligaciones que se tienen mutuamente. También se tratarán datos de posicionamiento, debido al control que se tendrá sobre la flota de vehículos.

DESARROLLO SOFTWARE DE LA EMPRESA

La empresa necesitará desarrollar programas informáticos que ayuden el desempeño de sus funciones. De éste modo manejará programas para:

- Gestión de los envíos.
- Gestión de las nóminas.
- Control de la flota de vehículos.

La base de datos de la empresa mantendrá la información del desempeño de la actividad empresarial. Se almacenarán datos de los envíos, de los trabajadores y de la flota de vehículos.

PRESENCIA EN INTERNET

La empresa tendrá una importante presencia en Internet, ya que permitirá contratar sus servicios por éste medio, además de publicitar los mismos. Esto conlleva a la creación de un sitio web en Internet que ofrezca dichos servicios, y a la creación del dominio asociado, a los sistemas de firmado digital y la seguridad en la red.

TRATO CON LA ADMINISTRACIÓN PÚBLICA

La empresa regulará su relación con la administración pública utilizando la administración electrónica, con el objetivo de abaratar los costes de explotación. Del mismo modo resolverá su fiscalidad por vía electrónica.

EMPRESA 2.0

Adecuándose al ámbito de las TIC, otro de los objetivos de la empresa es hacer que su presencia en Internet sea participativa, logrando una sinergia con los clientes, que resulte beneficiosa para ambos.

ADECUACIÓN A LAS TIC DE UNA EMPRESA DE TRANSPORTES



PROTECCIÓN DE DATOS PERSONALES

Autor del proyecto: Javier Sáez Moneo

Tutor del proyecto: Prof. Miguel Ángel Davara Rodríguez

Directores del Magíster:
Dr. Emilio S. Corchado Rodríguez
Dr. Álvaro Herrero Cosío

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

UNIVERSIDAD DE BURGOS

II Edición. Burgos, Julio 2010.

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

CONTENIDO

Contenido	9
Ilustraciones.....	12
Tablas	13
Formularios.....	13
1. Introducción	14
Ley Orgánica de Protección de Datos.....	14
¿Qué es la LOPD?.....	14
Panorama Legislativo Básico.....	14
Objetivo de LOPD:.....	15
Recogida y empleo de datos personales.....	15
Medidas Necesarias para el cumplimiento.....	16
Estructura del Estudio	16
2. Definiciones	19
Caso de Estudio	20
3. Fases del tratamiento.....	23
Caso de Estudio	23
4. Principios.....	26
Principios de la Protección de Datos	29
Caso de Estudio	34
Contratos.....	38

Prestación de Servicios.....	38
Laboral	40
5. Derechos.....	42
Derechos del Titular de los Datos.....	42
Ejercicio de los Derechos	43
Tutela de Derechos	44
Caso de Estudio	44
Solicitud de ejercicio de derecho	44
Ejercicio del derecho de acceso	45
Ejercicio de los derechos de Rectificación y Cancelación.....	45
Ejercicio del derecho de oposición.....	46
Formularios e instrucciones de ejercicio de derechos.....	46
6. Procedimientos.....	52
Procedimiento de tutela	52
Procedimiento sancionador.....	52
Caso de Estudio	54
Procedimiento de Tutela.....	54
Procedimiento Sancionador.....	55
7. Medidas de Seguridad.....	57
Presentación	57
Niveles de Seguridad	57
Obligaciones	59

Sanciones	59
Documento de Seguridad	60
Caso de Estudio	61
Contenido del documento de seguridad de nivel básico	61
Contenido del documento de seguridad de nivel medio	61
Contenido del documento de seguridad de nivel alto	62
8. Obligaciones y responsabilidades del titular del fichero:.....	64
El Registro General.....	64
Inscripción de Ficheros en el Registro.....	64
Manejo de ficheros de titularidad privada	65
Caso de Estudio	65
Configuración del Documento Nota	67
Inscripción del fichero de clientes.....	68
Inscripción del fichero de trabajadores	72
Inscripción del Fichero de Fines Publicitarios	76
9. Ficheros de Publicidad y Prospección Comercial.....	80
Caso de Estudio	80
Captación de Nuevos Clientes.....	81
Publicidad para Clientes.....	83
10. Ficheros de Solvencia Patrimonial	84
Caso de Estudio	87

ILUSTRACIONES

Ilustración 1-1: Estructura del Estudio	16
Ilustración 1-2: Esquema de la consultoría.....	18
Ilustración 7-1: Cuadro Resumen de Medidas de Seguridad	58
Ilustración 8-1: Configuración de Creación del Fichero NOTA	67
Ilustración 8-2: Documento NOTA para el Fichero de Clientes.....	68
Ilustración 8-3: Documento NOTA para el Fichero de Clientes, página 2	69
Ilustración 8-4: Documento NOTA para el Fichero de Clientes, página 3	70
Ilustración 8-5: Documento NOTA para el Fichero de Clientes, página 4	71
Ilustración 8-6: Documento NOTA para el Fichero de Trabajadores, página 1.....	72
Ilustración 8-7: Documento NOTA para el Fichero de Trabajadores, página 2.....	73
Ilustración 8-8: Documento NOTA para el Fichero de Trabajadores, página 3.....	74
Ilustración 8-9: Documento NOTA para el Fichero de Trabajadores, página 4.....	75
Ilustración 8-10: Documento NOTA para el Fichero de Fines Publicitarios, página 1.	76
Ilustración 8-11: Documento NOTA para el Fichero de Fines Publicitarios, página 2..	77
Ilustración 8-12: Documento NOTA para el Fichero de Fines Publicitarios, página 3..	78
Ilustración 8-13: Documento NOTA para el Fichero de Fines Publicitarios, página 4..	79
Ilustración 9-1: Ejemplo publicitario 1.....	82
Ilustración 9-2: Ejemplo publicitario 2.....	83

TABLAS

Tabla 1-1: Resumen de Principios, Derechos y Procedimientos.....	17
Tabla 2-1: Definiciones según la LOPD	20
Tabla 2-2: Definiciones en el contexto de los clientes	20
Tabla 2-3: Definiciones en el contexto de los trabajadores.....	21
Tabla 2-4: Definiciones en el contexto de fines publicitarios	22

FORMULARIOS

Formulario 4-1: Formulario de prestación de servicios, página 1	38
Formulario 4-2: Formulario de prestación de servicios, página 2.....	39
Formulario 4-3: Contrato laboral del trabajador, página 1	40
Formulario 4-4: Contrato laboral del trabajador, página 2.....	41
Formulario 5-1: Formulario de ejercicio del derecho de acceso	47
Formulario 5-2: Formulario de ejercicio del derecho de cancelación.....	48
Formulario 5-3: Formulario de ejercicio del derecho de rectificación.....	49
Formulario 5-4: Formulario de ejercicio del derecho de oposición	50
Formulario 5-5: Instrucciones de ejercicio de los derechos	51

1. INTRODUCCIÓN

LEY ORGÁNICA DE PROTECCIÓN DE DATOS

¿QUÉ ES LA LOPD?

La Ley Orgánica 15/1999 de 13 de diciembre de Protección de Datos de Carácter Personal, (en adelante LOPD), es una Ley Orgánica española que tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor, intimidad y privacidad personal y familiar. Esta ley viene a derogar a la antigua LORTAD y está compuesta de un marco legislativo bastante amplio.

Artículo 1 de la LOPD. Objeto.

La presente Ley Orgánica tiene por objeto garantizar y proteger, en lo que concierne al tratamiento de los datos personales, las libertades públicas y los derechos fundamentales de las personas físicas, y especialmente de su honor e intimidad personal y familiar.

PANORAMA LEGISLATIVO BÁSICO.

Dentro del ámbito de la protección de datos de carácter personal, se enmarcan las siguientes leyes:

- Ley orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal.
- Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal..
- Directiva 95/46/CE relativa a la protección de las personas físicas en el tratamiento de Datos Personales y a la libre circulación de los datos.
- Instrucciones de la Agencia Española de Protección de Datos sobre diversas materias (Ej. Instrucción 1/2006 video vigilancia).
- Recomendaciones de la Agencia Española de Protección de Datos.

- Legislación autonómica.

OBJETIVO DE LOPD:

Tiene por objeto proteger y garantizar las libertades y los derechos fundamentales de las personas físicas, su honor e intimidad personal y familiar.

- No se podrán tratar informáticamente datos personales ni cederse a terceros sin el consentimiento del interesado.
- No se podrá guardar datos que no sean verdaderos.
- No se podrán usar datos personales para un fin distinto del que se haya autorizado.
- No se podrán conservar durante un periodo superior al necesario para la finalidad para la que se recogieron.

RECOGIDA Y EMPLEO DE DATOS PERSONALES

Los datos personales solo podrán recogerse y emplearse en las siguientes circunstancias:

- El interesado ha dado su consentimiento.
- El tratamiento es necesario para el mantenimiento o cumplimiento de un contrato de relación de negocios, laboral o administrativo.
- El tratamiento es necesario para proteger el interés vital del interesado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.
- El tratamiento es necesario para cumplir las necesidades de las Administraciones Públicas en el ámbito de sus competencias.
- Cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo del responsable del fichero.
- Cuando una ley habilite el tratamiento sin requerir el consentimiento inequívoco de su titular.

MEDIDAS NECESARIAS PARA EL CUMPLIMIENTO.

Técnicas:

- El Reglamento de Medidas de Seguridad obliga a que las empresas y Profesionales protejan sus sistemas de información, como los equipos informáticos, con procedimientos de identificación, registros de accesos e incidencias o protocolos de recuperación de la información, entre otros.

Organizativas:

- Entre otras medidas, se exige definir y documentar las funciones y obligaciones del personal que accede a los datos y la creación de las figuras del Responsable del Fichero y del Responsable de Seguridad, con sus correspondientes funciones y obligaciones.

Jurídicas:

- Tales como los procedimientos para atender los derechos de los afectados, cesión a terceros de los datos o la calidad de los datos recogidos.

ESTRUCTURA DEL ESTUDIO

El estudio de la protección de datos que se va a realizar se desarrollará en base a la estructura enunciada por el Profesor Davara, como un triángulo en cuyos vértices se sitúan los principios de la protección de datos, los derechos que emanan de dichos principios y los procedimientos que aseguran que dichos derechos podrán ejercerse.

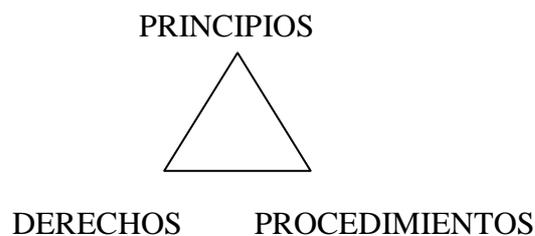


Ilustración 1-1: Estructura del Estudio

Los principios quedan marcados por la LOPD, y deberán ser cumplidos por el responsable del fichero, o del tratamiento; los derechos representan el vehículo mediante el cual se da ejercicio efectivo a los principios; y los procedimientos se encargan de tutelar al interesado cuando no puede o no se le permite satisfacer los principios de la ley.

De éste modo tenemos que recoger en el estudio una revisión sobre los siguientes principios, derechos y procedimientos en las distintas etapas del tratamiento de datos, para asegurar el correcto cumplimiento de las leyes:

principios	Derechos	procedimientos
Calidad de los datos (art.4 LOPD)	Derecho de impugnación (art.13 LOPD)	Tutela de derechos
Información de la recogida (art.5 LOPD)	Derecho de consulta (art.14 LOPD)	Procedimiento sancionador
Consentimiento (art.6 LOPD)	Derecho de acceso (art.15 LOPD)	
Datos especialmente protegidos (art.7 LOPD)	Derecho de rectificación y cancelación (art.16 LOPD)	
Datos relativos a la salud (art.8 LOPD)	Derecho de oposición(art.6.4 LOPD)	
Seguridad de los datos (art.9 LOPD)	Derecho a indemnización (art.19 LOPD)	
Deber de secreto (art.10 LOPD)		
Comunicación o cesión de datos (art.11 LOPD)		
Acceso por terceros (art.12 LOPD)		

Tabla 1-1: Resumen de Principios, Derechos y Procedimientos

La finalidad de éste proceso de asesoría es adecuar el tratamiento de datos que la empresa Transportes S.A. realiza durante el desempeño de sus funciones laborales. De éste modo, cuando acabe el estudio, se obtendrá un documento de guía, más las instrucciones de actualización de ficheros para la AEPD.

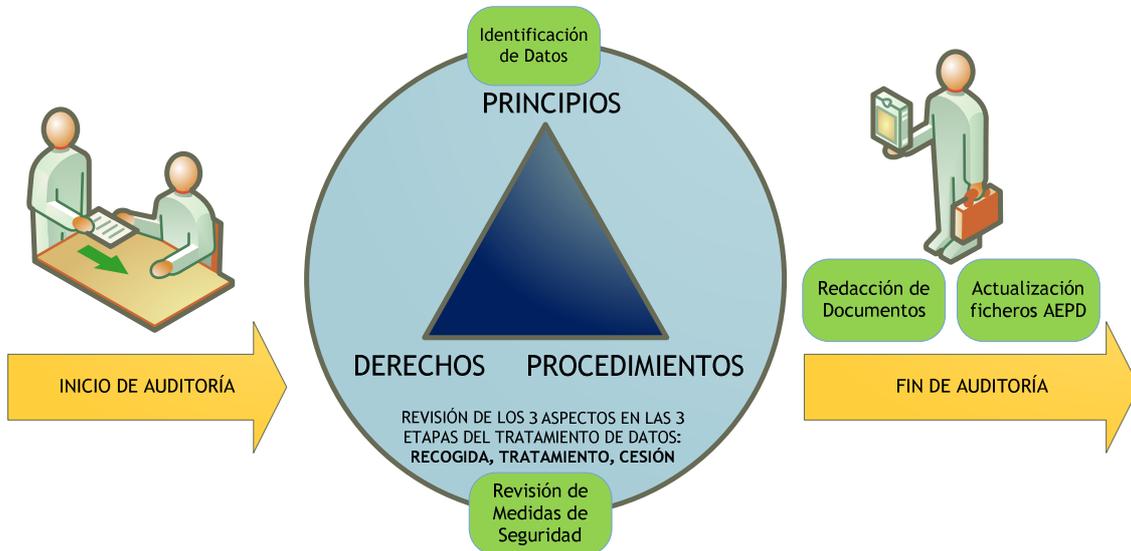


Ilustración 1-2: Esquema de la consultoría

2. DEFINICIONES

Los artículos 3 de la LOPD y 5 del RD 1720/2007 están dedicados a la definición de los diversos conceptos relacionados con el tratamiento de datos. Dichas definiciones sirven para aclarar conceptos que puedan resultar problemáticos en la aplicación de la norma.

En este apartado, se realizará una asociación entre las definiciones presentadas en la ley, y la situación real que se está tratando. De éste modo, se obtendrá una primera aproximación al contexto del problema que se presenta en el caso de estudio

Tal como están presentadas en la ley, las definiciones son:

Definición	
Datos de Carácter Personal	Cualquier información concerniente a personas físicas identificadas o identificables. Se incluyen: <ul style="list-style-type: none"> • Datos de contactos de empresa: se consideran protegidos porque normalmente contienen datos de personas físicas. • Datos de correo electrónico: El dato está protegido si en la configuración de la dirección se ha utilizado el nombre y apellidos del usuario, no en el caso en que el usuario no sea identificable. • Datos de imagen y sonido: siempre que identifiquen o puedan identificar a una persona física entran en el ámbito de protección especial de la LOPD.
Fichero	Todo conjunto organizado de datos de carácter personal, cualquiera que fuere la forma o modalidad de su creación, almacenamiento, organización y acceso.
Tratamiento de datos	Cualquier utilización que se haga del “dato”, desde su recogida hasta su cancelación o bloqueo.
Responsable de fichero o tratamiento	Cualquier persona física o jurídica que decida sobre la finalidad, contenido y uso del mismo.
Afectado	Cualquier persona física cuyos datos son tratados.
Procedimiento de disociación	Cualquier tratamiento que separe el dato de su titular, de forma que no sea identificado o identificable.
Encargado del tratamiento	Cualquier persona física o jurídica que trate los datos por cuenta del responsable del fichero.
Consentimiento del interesado	Cualquier manifestación, libre, inequívoca, específica e informada prestada por el titular de los datos.
Cesión o comunicación de datos	Toda comunicación de datos a persona distinta del interesado.
Fuentes accesibles al público	Aquellas a las que puede acceder cualquier persona, en particular, el censo promocional, los repertorios telefónicos, listas de personas pertenecientes a grupos profesionales, los diarios, boletines oficiales y medios de comunicación. Internet no tiene la consideración de medio de comunicación.
Bloqueo de Datos	Identificación y reserva de datos con el fin de impedir su tratamiento.

Identificación del Afectado	Cualquier elemento que permita determinar directa o indirectamente la identidad física, fisiológica, económica, cultural o social de la persona física afectada.
------------------------------------	--

Tabla 2-1: Definiciones según la LOPD

CASO DE ESTUDIO

Ahora, dichas definiciones se trasladarán al contexto real que se está estudiando, para los datos personales que se tratarán. Las definiciones aplicadas a los clientes son:

Definición	En Contexto del cliente
Datos de Carácter Personal	Nombre, Apellidos, Dirección, DNI, Teléfono.
Fichero	Fichero de la base de datos donde se guarden los datos de clientes. Nombre genérico “clientes.db”.
Tratamiento de datos	Los datos de clientes se utilizan para conocer el remite y destino de los envíos, y tramitar los pagos. Los datos se podrán introducir y eliminar de la base de datos.
Responsable de fichero o tratamiento	En este caso es el jefe de la sección de logística.
Afectado	Los clientes de la empresa.
Procedimiento de disociación	Se utilizarán procedimientos de cálculos estadísticos sobre envíos habituales, pero de forma anónima. También se dará una clave y usuario para acceder al sistema online, pero se asegurará el anonimato de dichos datos.
Encargado del tratamiento	En este caso, es el jefe de la sección informática
Consentimiento del interesado	El cliente manifestará su consentimiento, al firmar el contrato de prestación de servicios. Dicho contrato deberá contener una cláusula que indique su conformidad para el tratamiento de sus datos.
Cesión o comunicación de datos	Los datos de los clientes podrán pasar a formar parte de ficheros de solvencia patrimonial, si procede. Dicha condición deberá ser conocida y aceptada por el cliente.
Fuentes accesibles al público	No se utilizarán, ya que el cliente cede sus datos para el cumplimiento de una relación contractual.
Bloqueo de Datos	Si procede, se podrá bloquear el registro de la base de datos con los datos personales del cliente afectado.
Identificación del Afectado	DNI

Tabla 2-2: Definiciones en el contexto de los clientes

En el caso de los trabajadores son:

Definición	En Contexto del trabajador
Datos de Carácter Personal	Nombre, Apellidos, Dirección, DNI, Teléfono, N° SS, Nómina, Situación GPS, Salud, Afiliación Sindical.
Fichero	Fichero de la base de datos donde se guarden los datos de trabajadores. Nombre genérico "trabajadores.db"
Tratamiento de datos	Los datos de clientes se utilizan para conocer quienes tramitan los envíos, y tramitar los pagos de las nóminas. Los datos se podrán introducir y eliminar de la base de datos, y se podrán cruzar con los datos de envíos.
Responsable de fichero o tratamiento	En este caso es el jefe de la sección de recursos humanos.
Afectado	Los trabajadores de la empresa.
Procedimiento de disociación	No existirá disociación en éste caso.
Encargado del tratamiento	En este caso, es el jefe de la sección informática
Consentimiento del interesado	El trabajador manifestará su consentimiento, al firmar el contrato de trabajo. Dicho contrato deberá contener una clausula que indique su conformidad para el tratamiento de sus datos.
Cesión o comunicación de datos	No habrá revelación de datos de trabajadores a terceros.
Fuentes accesibles al público	No se utilizarán, ya que el cliente cede sus datos para el cumplimiento de una relación laboral.
Bloqueo de Datos	Si procede, se podrá bloquear el registro de la base de datos con los datos personales del trabajador afectado.
Identificación del Afectado	DNI

Tabla 2-3: Definiciones en el contexto de los trabadores

Finalmente, para fines publicitarios, se manejarán los siguientes datos:

Definición	En Contexto de fines publicitarios
Datos de Carácter Personal	Nombre, Apellidos, Dirección, Teléfono.
Fichero	Fichero de la base de datos donde se guarden los datos de clientes. Nombre genérico "publicidad.db".
Tratamiento de datos	Los datos de destinos publicitarios, que pueden provenir del fichero de clientes, o de fuentes públicas. Los datos se podrán introducir y eliminar de la base de datos.
Responsable de fichero o tratamiento	En este caso es el jefe de la sección de publicidad.
Afectado	Los clientes de la empresa, y otros clientes potenciales.
Procedimiento de disociación	No es necesario.
Encargado del tratamiento	En este caso, es el jefe de la sección informática
Consentimiento del interesado	El cliente podrá manifestar su consentimiento a la recepción de publicidad, al firmar el contrato de prestación de servicios.
Cesión o comunicación de datos	Existirá acceso a los datos por un tercero que se encargue de las campañas publicitarias de la empresa.
Fuentes accesibles al público	Se utilizarán fuentes accesibles al público en campañas de captación de clientes.
Bloqueo de Datos	Si procede, se podrá bloquear el registro de la base de datos con los datos personales del cliente afectado.
Identificación del Afectado	DNI

Tabla 2-4: Definiciones en el contexto de fines publicitarios

3. FASES DEL TRATAMIENTO

El tratamiento de datos, en base al cumplimiento de las leyes, se estructura en tres fases, en las que se deberá velar por el cumplimiento de los principios, derechos y procedimientos anteriormente mencionados:

- 1- El momento de recabar los datos, sea directamente del interesado, o de un tercero, siendo muy importante la licitud, lealtad y el consentimiento.
- 2- El momento de tratar los datos, que pueden ser utilizados para crear perfiles que el propio propietario desconozca.
- 3- El momento de la utilización, y posible cesión de los mismos, en la que también se tendrá que tener en cuenta el conocimiento y consentimiento del titular.

Es muy importante, al estudiar las fases por las que pasa el tratamiento de los datos, atender el cumplimiento de los principios ajustados a cada fase. Mientras que los derechos y procedimientos se pueden ejercer en cualquier momento del tratamiento de los datos, los principios pueden ir más ajustados a una u otra etapa y por ello, merecerán una mayor atención.

CASO DE ESTUDIO

Tratamiento de datos de clientes

Las fases del tratamiento de los datos del cliente, serán a grandes rasgos los siguientes:

Recabar los datos: El cliente se pone en contacto con la empresa para contratar un envío. La cesión de datos será voluntaria, con el fin de satisfacer una relación contractual. En el contrato se hará constar claramente en cláusulas los principios que rigen el uso de sus datos personales, y los derechos que podrá ejercer. Muy importante es que en estas cláusulas, se informe al cliente que sus datos serán tratados, se le pida el consentimiento para ello, y se pidan sólo datos bien ajustados al contexto.

Tratamiento de los datos. Los datos se utilizarán con la finalidad de que el envío llegue a destino. Una vez que el envío se haya completado, los datos del cliente se eliminarán al no ser necesarios por más tiempo. Habrá un procedimiento de disociación que permitirá utilizar los datos recogidos para crear estadísticas y optimizar las rutas de los

transportes, pero de forma totalmente anónima. Se comunicará al cliente dicho procedimiento de disociación, por si no quisiese que sus datos se utilicen en el mismo, y también se indicará qué datos se utilizarán.

Cesión a terceros. Podrá existir acceso por terceros a datos personales de los clientes, si estos dan su aprobación, para finalidades comerciales y de publicidad. Se solicitará consentimiento expreso al cliente para poder realizar la cesión. También podrán cederse los datos de los clientes a ficheros de solvencia, en caso de impago. Dicha condición también se deberá recoger como clausula en el contrato de prestación de servicios.

Tratamiento de datos de trabajadores

Recabar los datos: El trabajador es contratado para el desempeño de una tarea. El acuerdo de cesión de datos se cierra a través del contrato laboral, en el que también se deberán hacer constar los principios del tratamiento de sus datos. Del mismo modo que en el caso anterior, se informará del tratamiento de los datos y se recogerán sólo datos bien ajustados al contexto. El consentimiento del trabajador se asegura a través de la firma del contrato.

Tratamiento de los datos. Los datos del trabajador se utilizarán para poder satisfacer la relación laboral entre el mismo y la empresa. Un dato importante que se comunicará en el contrato del trabajador, es el tratamiento de su posición por GPS durante las horas de trabajo. Los vehículos de la empresa utilizarán un localizador para poder hacer seguimiento de los envíos, pero sin embargo, al ser la posición del vehículo la misma que la de su conductor, será necesario informar de su uso. El trabajador que conduzca el vehículo deberá aprobar que la empresa conozca su localización, y que la maneje entre los datos de los vehículos.

Cesión a terceros. No se contempla la cesión de datos, ni el acceso por terceros.

Tratamiento de datos con fines publicitarios

Recabar los datos: El origen de los datos manejados para publicidad puede ser clientes que hayan solicitado la recepción de publicidad, o de posibles clientes, obtenidos de fuentes accesibles al público.

Tratamiento de los datos: Los datos serán manejados por una empresa dedicada a la realización de campañas publicitarias. En el caso de clientes, recibirán publicidad de fidelización, adecuada a los servicios que suelen utilizar. En el caso de no clientes, la publicidad se orientará a su captación.

Acceso por terceros: De la gestión del fichero se encargará la propia empresa, ocupándose de las bajas y altas del mismo, aunque el uso de la información del mismo, recaerá en la empresa de publicidad.

4. PRINCIPIOS

Los principios representan las bases que la LOPD, como ley, deberá asegurar en el tratamiento de datos, para la salvaguarda de los derechos de los afectados.

Los principios sobre los que se sustenta la LOPD son los siguientes:

Calidad de los datos (artículo 4 LOPD):

Los datos deben adecuarse a la finalidad para los que fueron conseguidos, ser exactos, no mantenerse más allá de su uso normal y ser recogidos de forma lícita. La exactitud de los datos no se extiende a los cambios que no pudieron ser conocidos por el responsable del fichero, por ejemplo cambio de dirección, pero si deberán ser corregidos una vez notificado por el titular.

Derecho de información (artículo 5 LOPD):

Cuando se recaben datos de un interesado, este deberá saber de la existencia del fichero, de su finalidad y de los destinatarios, de la obligatoriedad o no de facilitarlos, así como de su derecho de acceso, rectificación, cancelación y oposición. Por último deberá conocer la identidad y dirección del responsable del tratamiento o de su representante.

Cuando los datos sean recabados de terceros, el responsable tendrá tres meses para informar al interesado. Si proceden de fuentes públicas, se deberá entonces informar del origen de los mismos y del responsable del fichero.

Consentimiento inequívoco del afectado (artículo 6 LOPD):

Las exclusiones vienen tasadas en el art 6.2, indicando que no será necesario, cuando se recojan los datos para funciones propias de las administraciones públicas, cuando se refieran a las partes de un contrato o precontrato, de una relación laboral o administrativa y sean necesarias para su mantenimiento y cumplimiento. Esto no impide que el consentimiento sea revocado por su titular.

Datos especialmente protegidos (artículo 7 LOPD):

Es preciso el consentimiento expreso y por escrito para recabar los datos relativos ideología, afiliación política y sindical, religión, salud, vida sexual y origen racial, salvo que se trate de un partido político, sindicato, asociación o fundación, o en el caso de la salud sea para prestar asistencia sanitaria.

Datos relativos a la salud (artículo 8 LOPD):

Siendo un caso específico de datos especialmente protegidos, este artículo autoriza a los profesionales de la medicina al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan.

Seguridad de los datos (artículo 9 LOPD):

El responsable del fichero y en su caso el encargado del tratamiento adoptarán las medidas físicas y tecnológicas apropiadas (o reglamentariamente establecidas) para garantizar la seguridad de los mismos en función de su importancia y sensibilidad.

Obligación de secreto (artículo 10 LOPD):

El responsable del fichero y cualquier persona que tenga acceso a su tratamiento tienen una obligación de secreto profesional con respecto a los datos.

Comunicación de los datos a terceros (artículo 11 LOPD):

Solo podrán cederse datos en cumplimiento de los fines directamente relacionados con las funciones legítimas del cedente y del cesionario, con el previo consentimiento informado del interesado. Las principales excepciones son cuando se trate de cesión de datos públicos o ligados a una relación contractual, entre administraciones públicas y afines.

La cesión entre empresas de un mismo grupo, se consideran cesión a terceros y por tanto sujetas a las normas de la LOPD.

Cesión de datos para la prestación de un servicio (artículo 12 LOPD):

No se considera cesión de datos, cuando mediante contrato, el responsable del tratamiento de datos los cede a un encargado para la realización de un servicio. En el contrato se deberá especificar, la finalidad del servicio, prohibición de cederlo a terceros, obligación de cumplir con las instrucciones del responsable, las medidas de seguridad a adoptar y la obligación de devolver o destruir los datos y soportes.

A continuación se realizará un estudio del cumplimiento de los principios de la protección de datos, en el contexto que se está tratando. En todos los casos, primero se expondrá la base teórica que se extiende de la propia LOPD, para después aplicarla. Una vez estudiados todos los principios que se deben respetar, se presentarán los contratos correspondientes que permitan su recogida.

PRINCIPIOS DE LA PROTECCIÓN DE DATOS

Principio de Consentimiento

El artículo 6 de la LOPD, indica la necesidad de recabar el consentimiento inequívoco del titular de los datos, para poder tratar los mismos, salvo que una ley disponga lo contrario.

De éste modo, sólo el titular de los datos tiene potestad para decidir cuándo, dónde y cómo se tratarán sus datos, y si estos se podrán dar a conocer a terceros.

Las excepciones para el principio de consentimiento son:

- La existencia de una Ley que disponga la contrario
- Si los datos son recogidos para el ejercicio de las funciones propias de las administraciones públicas, en el ámbito de sus competencias.
- Cuando exista una relación contractual negocial ó laboral entre dos partes, y los datos sean necesarios para el mantenimiento ó cumplimiento.
- Cuando el tratamiento de los datos esté destinado a proteger un interés vital del interesado.
- Cuando los datos figuren en fuentes accesibles al público, y sean tratados para un interés legítimo, siempre que no se vulneren libertades y derechos fundamentales.

En la empresa Transportes S.A., los datos que necesitan consentimiento provendrán de dos grupos de personas: clientes y trabajadores. En ambos casos, existe una relación contractual entre la empresa y la otra parte interesada.

En el caso de los trabajadores se trata una relación laboral, en la que el trabajador se compromete a realizar una determinada tarea para la empresa. Sus datos serán recogidos en el momento de completar el contrato, y en el mismo se le deberá informar de que dichos datos, se utilizarán en la empresa para tratamientos que determinen su rendimiento, o calculen su salario, por ejemplo. Cada vez que la empresa considere realizar un tratamiento de datos de los trabajadores, no será necesario solicitar su consentimiento.

Para los clientes la situación es similar, simplemente que en este caso, la empresa es la parte contratada para el desempeño de la labor. Cuando se firme el contrato de prestación de servicios, se recogerá en una cláusula, la condición de que los datos del cliente se podrán tratar sin su consentimiento, siempre y cuando sea un tratamiento necesario para el desempeño del contrato, como puede ser el cálculo de rutas de viaje, por ejemplo.

En el caso de los datos recabados de fuentes accesibles al público, no será necesaria la obtención del consentimiento del titular. De este modo, se podrán realizar campañas publicitarias sin consentimiento previo del receptor.

Principio de calidad de los datos

El principio de calidad de los datos se recoge en el artículo 4 de la LOPD. Este principio expone la necesidad de que los datos tratados deberán ser pertinentes, adecuados y no excesivos en relación con la finalidad para la que fueron recabados, debiendo mantenerse exactos, y puestos al día, no pudiendo permanecer en el fichero más tiempo del estrictamente necesario.

Los trabajadores facilitarán sus datos personales al firmar el contrato de trabajo. Dichos datos se limitarán a datos de ámbito público sobre el trabajador, que permitan identificarlo, ejercer sus derechos, y recibir sus honorarios. Los datos del trabajador permanecerán en el fichero, mientras el mismo sea operario de la empresa.

En el caso de los clientes, los datos de contacto y localización, se recogen en el momento de encargar un envío. El cliente podrá aceptar, si lo desea, que sus datos permanezcan en el fichero de publicidad, para poder recibir envíos publicitarios. Los datos de los destinatarios, deberán permanecer simplemente desde que comienza el envío, hasta que se complete, luego pasarán a estar bloqueados.

Los datos de los no clientes que figuran en el fichero de fines publicitarios permanecerán hasta que los titulares de los mismos ejerzan su derecho de cancelación.

Principio de información en la recogida de los datos

El artículo 5 de la LOPD recoge el principio de información en la recogida de datos. Según éste artículo, cuando se recaben datos al afectado, éste debe ser informado con carácter previo, y de manera expresa, precisa e inequívoca de estos puntos:

- Existe un fichero al que se van a incorporar sus datos.
- La finalidad con la que se incorporan.
- Los destinatarios de la información que se recoge.
- Las consecuencias de negarse a proporcionar los datos.
- La posibilidad de acceder, rectificar, cancelar, y oponerse a los datos.
- Los datos de identidad y localización del responsable del fichero.

Tanto en el caso de los empleados, como en el caso de los clientes, sus datos se recogen únicamente para satisfacer algún tipo de relación contractual. De este modo, en el contrato que reciba cada uno, se deberá hacer constar todos estos aspectos en una cláusula, que el firmante deberá leer y aceptar previamente.

Datos especialmente protegidos

Los datos especialmente protegidos son regulados en el artículo 7 de la LOPD. Se pueden considerar datos especialmente protegidos a la ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual. Son todos datos muy sensibles, que necesitan un consentimiento expreso y por escrito para poder ser tratados, aparte de requerir medidas de seguridad especialmente rigurosas.

Los datos relativos a la salud de una persona podrán ser utilizados siempre que exista un motivo médico.

En el caso de estudio que nos ocupa, los datos especialmente protegidos que se tratarán serán referentes a la salud y la afiliación sindical de los trabajadores.

Seguridad de los datos

Según se trata en el artículo 9, el responsable del fichero, y el encargado del tratamiento deberán poner en marcha todas las medidas de seguridad, técnicas y organizativas que

sean necesarias para garantizar la seguridad, confidencialidad e integridad de los datos personales objeto del tratamiento.

Los clientes requieren un nivel de seguridad básico, ya que se manejan datos personales simples, estrictamente necesarios para el desempeño de una labor.

Los datos que la empresa mantiene para fines publicitarios también son datos personales simples, por lo que el nivel de seguridad será el básico.

En el caso de los trabajadores, el nivel de seguridad requerido es alto, debido a que se manejan datos especialmente protegidos.

Deber de secreto

El responsable del fichero debe asegurar el secreto de los datos personales que está tratando. Dicho secreto se consigue implementando las adecuadas medidas de seguridad que se han comentado anteriormente.

Independientemente del fichero que se esté tratando, se establecerá un nivel de secreto adecuado. Los datos personales son sólo propiedad del titular, de modo que se usarán los procedimientos de disociación pertinentes para que sea imposible asociar a cada titular los resultados de su tratamiento de datos personales.

Cesión

La cesión de datos de carácter personal sólo se podrá realizar para cumplir fines relacionados con el cumplimiento de la misión con la que fueron cedidos, salvo que una ley disponga lo contrario.

Al tratarse de una relación contractual, con un pago económico de por medio, existen riesgos para la solvencia de la empresa. Dicho de un modo más simple, existe el riesgo de que el cliente no pague. Es por ello, que como parte del contrato, se permitirá que los datos de encargos impagados, puedan ser incorporados a ficheros de solvencia patrimonial.

En resumen, existirá una cesión de datos personales a un tercero, como parte de la relación contractual. Los datos que se han cedido al tercero, podrán ser cancelados ó devueltos una vez que el cliente haya satisfecho la deuda. Los términos de ésta cesión, se explicarán con más detalle en el punto 7 del presente capítulo.

Acceso por terceros

En éste caso, la gestión del fichero de datos personales sigue siendo responsabilidad de la empresa, aunque su uso sea desarrollado por otra.

Existirá un acceso a datos por terceros para finalidades publicitarias y comerciales. Sólo se cederán los datos indispensables para ejercer esta finalidad, y sólo en caso de que el cliente lo autorice.

CASO DE ESTUDIO

En relación a los puntos anteriormente comentados, se puede construir una lista de requisitos para asegurar que los principios se salvaguardarán en el procesado de datos:

Calidad de los datos (art.4)

Los datos recogidos deberán ser pertinentes, adecuados al contexto y no excesivos, no pudiendo permanecer en el fichero más tiempo del estipulado.

Los datos personales que se tratarán son:

Para los clientes: Nombre, Apellidos, Dirección, DNI, Teléfono.

Para los trabajadores: Nombre, Apellidos, Dirección, DNI, Teléfono, N°SS, Nomina, posición gps, salud, afiliación sindical.

Para fines publicitarios: Nombre, Apellidos, Dirección, Teléfono.

Información de la recogida (art.5)

Se recojan directamente del interesado, o a través de un tercero, el titular de los datos deberá ser informado de recogida de sus datos.

En éste caso, la empresa deberá informar al titular de los datos cuando estos vayan a ser recogidos para su tratamiento. El formulario de recogida deberá contener una clausula contractual solicitando permiso para tratar los datos.

En el caso de los trabajadores, además se solicitará el tratamiento de su localización durante las horas de trabajo. Este dato no es necesario para el desarrollo de la actividad contractual, pero debido a que los vehículos de la empresa utilizan un localizador, el dato coincide con el del vehículo, con lo cual se estará utilizando por extensión, de modo que se necesitará permiso para su tratamiento.

Consentimiento (art.6)

Establece los criterios de consentimiento, y revocación del mismo, del tratamiento de los datos del titular.

Del mismo modo que en el principio anterior, el titular de los datos deberá consentir el tratamiento de sus datos, y tendrá la opción de retirar dicho consentimiento en cualquier momento de la relación. Este hecho también deberá ser plasmado en el formulario de recogida de la información. El consentimiento al tratamiento se otorgará a través de la firma del contrato.

Datos especialmente protegidos (art.7)

Se establece la manera de tratar datos que puedan resultar especialmente comprometedores para el titular, como ideología, creencias, afiliaciones, religión, salud, vida sexual y origen racial.

En el caso de los trabajadores, se manejarán datos sensibles como salud y afiliación sindical. Esto obliga a un especial cuidado en el tratamiento de estos datos del trabajador, debiéndose utilizar las medidas de seguridad pertinentes.

Datos relativos a la salud (art.8)

Autoriza a los profesionales de la medicina al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan.

Tampoco procede en éste caso, ya que el servicio a prestar es de transportes, no médico.

Seguridad de los datos (art.9)

Se establecen niveles para las medidas de seguridad para asegurar la confidencialidad e integridad de la información.

En el caso de los trabajadores se tratan datos personales que se pueden considerar íntimos, como pueden ser el poder adquisitivo, la salud y la afiliación sindical. Se imponen, en tal caso unas medidas de seguridad de nivel alto.

Para el caso de los clientes, al tratarse simplemente datos personales, el nivel es básico.

Deber de secreto (art.10)

Se expone la necesidad de que las personas que intervienen en el proceso de tratamiento de datos, deberán cumplir severas normas de conducta que aseguren el secreto y eviten el mal uso de los datos.

En una clausula en el formulario, se indicará el cumplimiento del deber de secreto. Es especialmente importante asegurar el deber de secreto, ya que se están manejando datos que el titular puede considerar íntimos.

Para asegurar dicho secreto, se ponen en marcha los procesos de disociación de datos.

Por ejemplo, los clientes cuanto quieran acceder o crear una cuenta para hacer uso de la contratación de servicios por Internet tendrán un nombre de usuario y contraseña. Dicho nombre y contraseña no se almacenarán en la base de datos junto a los datos personales, sino que se creará otra tabla, y se vincularán ambas mediante un campo que no identifique al cliente a los ojos de un usuario, pero sí a los del sistema.

En el fichero de trabajadores se puede establecer un mecanismo similar para que los usuarios que monitoricen la posición gps de los camiones y los envíos no tengan un acceso directo a información del trabajador.

Comunicación o cesión de datos (art.11)

Expone las bases de la cesión de datos. Dicha cesión deberá ser con el consentimiento del titular (pudiendo ser revocado), y sólo se podrá llevar a cabo cuando se cumpla la finalidad con la que los datos fueron recogidos originalmente.

En éste caso, se deberá aclarar que los datos del cliente se cederán a un gestor de ficheros de solvencia patrimonial, como parte de la relación contractual, en el caso de que la deuda contraída por la prestación de servicios no sea satisfecha.

Acceso por terceros (art.12)

Regula la cesión de datos a terceros, las responsabilidades y la duración del contrato con el tercero.

También se solicitará al cliente permiso para que sus datos puedan ser usados por una empresa que se encargue de campañas publicitarias. Sólo se realizará el uso de estos datos si el cliente lo solicita expresamente.

CONTRATOS

PRESTACIÓN DE SERVICIOS

CONTRATO DE PRESTACIÓN DE SERVICIOS DE TRANSPORTE

DATOS DEL REMITENTE			
Nombre y apellidos			
Domicilio			
Localidad			
Provincia		Código Postal	
e-mail		Teléfono	
DATOS DEL DESTINATARIO			
Nombre y apellidos			
Domicilio			
Localidad			
Provincia		Código Postal	
e-mail		Teléfono	

DESCRIPCIÓN DEL ENVÍO	
Número de Bultos	
Embalaje	
Peso	
Descripción	

En..... a..... de..... de 20...	
Firma	

CONTRATO DE PRESTACIÓN DE SERVICIOS DE TRANSPORTE

Deseo recibir comunicaciones comerciales en nombre de Transportes S.A.

En cumplimiento de lo dispuesto en la Ley Orgánica 13/1999 de Protección de Datos de Carácter Personal, Transportes S.A., le informa que sus datos personales obtenidos mediante la cumplimentación de este formulario, van a ser incorporados para su tratamiento en un fichero automatizado. Asimismo, se le informa que la recogida y tratamiento de dichos datos tienen como finalidad permitir al cliente el envío de una mercancía. Dicha autorización de tratamiento podrá ser revocada por el titular de los datos cuando así lo requiera.

Si lo desea, el titular puede ejercitar los derechos de acceso, rectificación, cancelación y oposición, previstos por la Ley, dirigiendo un escrito a la sede central de Transportes S.A..

Transportes S.A. ha adoptado los niveles de seguridad de protección de los Datos Personales legalmente requeridos, y ha instalado todos los medios y medidas técnicas a su alcance para evitar la pérdida, mal uso, alteración, acceso no autorizado y robo de los datos. De éste modo, Transportes S.A. se hace responsable del mantenimiento del secreto de los datos aquí recogidos.

Transportes S.A. está suscrita al sistema de ficheros de solvencia patrimonial mantenido por ASNEF. En caso de que no se satisfaga la deuda económica contraída por el cliente tras la realización del envío, sus datos personales pasarán a formar parte del fichero de morosos. Los datos serán retirados del fichero, una vez que se satisfaga la deuda.

Transportes S.A. será la única empresa responsable del tratamiento de los datos para la prestación del servicio contratado, y en ningún momento dichos datos serán cedidos a terceros.

Rellenando este impreso, usted autoriza a que en caso de impago del importe fijado por la prestación del servicio, será penalizado enviando sus datos personales, así como los de la infracción al fichero de solvencia patrimonial mantenido por ASNEF.

LABORAL



MINISTERIO
DE TRABAJO
Y ASUNTOS SOCIALES



INEM
INSTITUTO DE EMPLEO
SERVICIO PÚBLICO
DE EMPLEO ESTATAL

CONTRATO DE TRABAJO POR TIEMPO INDEFINIDO

CÓDIGO DE CONTRATO

DATOS DE LA EMPRESA CIF/NIF/NIE: <input style="width: 150px;" type="text"/>		<input type="checkbox"/> TIEMPO COMPLETO	<input style="width: 20px;" type="text"/> 1 <input style="width: 20px;" type="text"/> 0 <input style="width: 20px;" type="text"/> 0
		<input type="checkbox"/> TIEMPO PARCIAL	<input style="width: 20px;" type="text"/> 2 <input style="width: 20px;" type="text"/> 0 <input style="width: 20px;" type="text"/> 0
D.DÑA.		NIF/NIE	EN CONCEPTO (1)
NOMBRE O RAZÓN SOCIAL DE LA EMPRESA		DOMICILIO SOCIAL	
PAIS	MUNICIPIO	C. POSTAL	

DATOS DE LA CUENTA DE COTIZACIÓN

REGIMEN	COD. PROV.	NUMERO	DIG. CONTR.	ACTIVIDAD ECONOMICA
<input style="width: 20px;" type="text"/>	<input style="width: 20px;" type="text"/>	<input style="width: 40px;" type="text"/>	<input style="width: 20px;" type="text"/>	<input style="width: 20px;" type="text"/>

DATOS DEL CENTRO DE TRABAJO

PAIS	MUNICIPIO
<input style="width: 20px;" type="text"/>	<input style="width: 40px;" type="text"/>

DATOS DEL TRABAJADOR

D.DÑA.		NIF/NIE (2)	FECHA DE NACIMIENTO
Nº AFILIACIÓN S.S.	NIVEL FORMATIVO	NACIONALIDAD	
MUNICIPIO DEL DOMICILIO	PAIS DOMICILIO		
<input style="width: 40px;" type="text"/>	<input style="width: 20px;" type="text"/>	<input style="width: 20px;" type="text"/>	<input style="width: 20px;" type="text"/>

Con la asistencia legal, en su caso, de D./Dña.
 con NIF./NIE., en calidad de (3)

DECLARAN

Que reúnen los requisitos exigidos para la celebración del presente contrato y, en su consecuencia, acuerdan formalizarlo con arreglo a las siguientes:

CLÁUSULAS

PRIMERA: El trabajador prestará sus servicios como (4), incluido en el grupo profesional / categoría / nivel profesional de, de acuerdo con el sistema de clasificación profesional vigente en la empresa, en el centro de trabajo ubicado en (calle, nº y localidad)

SEGUNDA: La jornada de trabajo será:

A tiempo completo: la jornada de trabajo será de horas semanales, prestadas de a, con los descansos que establece la ley.

A tiempo parcial: la jornada de trabajo ordinaria será de horas al día, a la semana, al mes, al año, siendo esta jornada inferior a (marque con una X lo que corresponda):

La de un trabajador a tiempo completo comparable.

La jornada a tiempo completo prevista en el Convenio Colectivo de aplicación.

La jornada máxima legal.

Que es de horas (5)

Mod. PE-170 A (VIII)
<http://www.inem.es>

Formulario 4-3: Contrato laboral del trabajador, página 1

La distribución del tiempo de trabajo será de

Señálese, en el caso de jornada a tiempo parcial, si el contrato corresponde o no, a la realización de trabajos fijos discontinuos y periódicos que se repiten en fechas ciertas dentro del volumen normal de actividad de la empresa.

SI NO

TERCERA: En el caso de jornada a tiempo parcial señálese si existe o no pacto sobre la realización de horas complementarias (6):

SI NO

CUARTA: La duración del presente contrato será INDEFINIDA, iniciándose la relación laboral en fecha y se establece un período de prueba de (7)

QUINTA: El presente contrato se formaliza bajo la modalidad de contrato de relevo: SI NO
En caso afirmativo cumplimentar el anexo «Contrato de relevo».

SEXTA: El trabajador percibirá una retribución total de euros brutos (8) que se distribuirán en los siguientes conceptos salariales (9)

SEPTIMA: La duración de las vacaciones anuales será de (10)

OCTAVA: En lo no previsto en este contrato se estará a la legislación vigente que resulte de aplicación y, particularmente, a lo dispuesto en el Texto Refundido del Estatuto de los Trabajadores, y en especial el art.12, según la redacción dada por el R.D. 15/98, modificado por el artículo primero de la Ley 12/2001, de 9 de Julio (BOE de 10 de Julio) y en el Convenio Colectivo de

NOVENA: El contenido del presente contrato se comunicará al Servicio Público de Empleo de , en el plazo de los 10 días siguientes a su concertación (11).

CLÁUSULAS ADICIONALES

DÉCIMA: El Trabajador acepta que la empresa trate los datos de carácter personal que figuran en éste contrato, para poder satisfacer la relación contractual entre ambas partes.

UNDÉCIMA: Si el puesto de trabajo es conductor de alguno de los vehículos de la empresa, el trabajador acepta el tratamiento de sus datos de salud, por motivos de seguridad en el trabajo.

Y para que conste, se extiende este contrato por triplicado ejemplar en el lugar y fecha a continuación indicados, firmando las partes interesadas.

En a de de 20

El trabajador	El representante de la Empresa	El representante legal del menor, si procede
---------------	-----------------------------------	---

Mod. PE-170R (VII)

- (1) Director, Gerente, etc.
- (2) En el caso de contratación a través de contingente a una persona extranjera no comunitaria y no residente en España, deberá cumplimentarse el anexo Mod. PE- 217
- (3) Padre, madre, tutor o persona o institución que le tenga a su cargo.
- (4) Indicar profesión.
- (5) Indique el número de horas que corresponde a la jornada a tiempo completo, solo en caso de solicitar subvenciones establecidas en la O.M. 15-07-99 (BOE de 31 de Julio).
- (6) Señálese lo que procede, y en caso afirmativo, adjunte el anexo si hay horas complementarias.
- (7) Habrá de respetarse, en todo caso, lo dispuesto en el art. 14.1 del Texto Refundido de la Ley del Estatuto de los Trabajadores, aprobado por Real Decreto Legislativo 1/1995, de 24 de Marzo (BOE de 29 de marzo).
- (8) Diarios, semanales o mensuales.
- (9) Salario base, complementos salariales, pluses.
- (10) Mínimo: 30 días naturales.
- (11) PROTECCIÓN DE DATOS.- Los datos consignados en el presente modelo tendrán la protección derivada de Ley Orgánica 15/1999, de 13 de diciembre (BOE de 14 de diciembre).

5. DERECHOS

En el título tercero de la LOPD, se reconocen los derechos del titular de los datos. Mediante este conjunto de derechos, la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal garantiza a las personas el poder de control sobre sus datos personales. Estos derechos constituyen el haz de facultades que emanan del derecho fundamental a la protección de datos y «sirven a la capital función que desempeña este derecho fundamental: garantizar a la persona un poder de control sobre sus datos personales, lo que sólo es posible y efectivo imponiendo a terceros los mencionados deberes de hacer».

DERECHOS DEL TITULAR DE LOS DATOS

Derecho de Impugnación de valoraciones – Artículo 13:

Otorga al afectado la capacidad de impugnar decisiones únicamente basadas en datos obtenidos en base a un tratamiento de datos de carácter personal.

El derecho de impugnación de valoraciones ofrece la posibilidad de limitar el uso de técnicas que faciliten una información ó perfil del interesado que vayan más allá de los datos por él facilitado.

Derecho de Consulta al Registro General de Protección de Datos – Artículo 14:

Cualquier persona puede solicitar al RGPD conocer la existencia de tratamientos de datos, finalidad, e identidad del responsable del fichero que existen sobre sus datos personales. Estos registros son de consulta pública y gratuita, sin que existan limitaciones sobre las consultas que el usuario puede realizar.

Derecho de Acceso – Artículo 15:

Representa el derecho del afectado a conocer los datos de carácter personal que figuran en un fichero de datos de carácter personal. El responsable del fichero es el encargado de satisfacer éste derecho, y deberá informar de qué datos contiene el fichero, cual es su origen, y las comunicaciones realizadas de los mismos.

Derecho de rectificación – Artículo 16:

Permite que el titular de los datos pueda corregir los datos que figuren en un fichero si los mismos son inexactos ó incompletos.

Derecho de cancelación – Artículo 16:

El titular de los datos puede solicitar que los mismos sean cancelados cuando hayan dejado de servir para la finalidad con la que fueron recogidos.

Derecho de oposición – Artículo 6.4:

El titular de los datos puede oponerse al tratamiento de sus datos personales cuando existan motivos fundados y legítimos. Este derecho se podrá ejercer si no ha sido necesario el consentimiento del titular para realizar el tratamiento, y si una ley no indica lo contrario. La exclusión de los datos del fichero será realizada por el responsable del fichero mismo.

Derecho a indemnización – Artículo 19:

Si se produce algún daño ó lesión sobre los bienes o derechos del titular de los datos por parte del personal que realiza el tratamiento de datos, él titular podrá solicitar su indemnización, mediante vía jurídica.

EJERCICIO DE LOS DERECHOS

El ejercicio de los derechos del titular de los datos, se describe en la LOPD, básicamente en torno a dos ideas: Los derechos en protección de datos son personalísimos, por lo que sólo el titular de los datos puede ejercerlos, y los derechos en protección de datos son independientes, por lo que no será necesario ejercer uno previamente al ejercicio de otro.

El titular del fichero deberá cumplir los principios que la LOPD expone, para permitir y facilitar el ejercicio de los derechos que la ley reconoce al titular de los datos.

La solicitud de ejercicio de un derecho se llevará a cabo mediante una comunicación que permita identificar a la persona que ejercita el derecho como titular de los datos, contenga sus datos identificativos, concrete el derecho que se ejerce, y acredite la petición que formula.

Todos los derechos tienen tipificado en la LOPD el tiempo permitido para su cumplimiento por parte del responsable del fichero, así como las situaciones especiales en las que el ejercicio se podría denegar.

TUTELA DE DERECHOS

Cuando al titular de los datos se le deniegue el ejercicio de los derechos de acceso, rectificación, cancelación u oposición de los mismos, podrá comunicárselo a la AEPD (o al organismo competente correspondiente a su comunidad autónoma), para que participe en el proceso y pueda asegurar el cumplimiento de la LOPD.

Una vez que la AEPD reciba la reclamación, se informará al responsable del fichero, para que en un plazo de quince días, formule las alegaciones correspondientes. Una vez transcurrido ese plazo, la AEPD resolverá sobre el caso.

CASO DE ESTUDIO

Los derechos de cuyo ejercicio debe hacerse responsable la empresa son los derechos de acceso, rectificación, cancelación y oposición. Puesto que es una obligación a cumplir, la empresa se deberá preocupar de que el trámite sea fácil y rápido para ambas partes, lo cual se traducirá la mayor parte de las veces en un trámite satisfactorio.

SOLICITUD DE EJERCICIO DE DERECHO

La empresa pondrá a disposición de cualquier cliente un impreso estandarizado (ilustraciones 5-1 a 5-5) para registrar (la empresa) y describir (el cliente) el ejercicio del derecho. La empresa debe atender la petición por cualquier medio que le llegue, ya sea en persona, por teléfono, por email, fax, etc. En cualquier caso, se contestará al cliente, proporcionando el formulario. Así, si el cliente se persona en la sede de la empresa, se le entregará el formulario impreso; si llama por teléfono, se le envía por correo ordinario; si se comunica por fax, se contesta por fax; si es por email, se contesta

por email. No se deberá escatimar en esfuerzos para que el cliente pueda ejercer sus derechos, habida cuenta de las sanciones que el incumplimiento puede representar. El responsable del fichero está obligado a atender el ejercicio de los derechos siempre que se solicite.

EJERCICIO DEL DERECHO DE ACCESO

El cliente elegirá la manera en la que recibirá la información sobre sus datos personales por un medio que elija:

- Visualización en pantalla.
- Escrito.
- Telecopia ó fax.
- Correo electrónico

Una vez que la solicitud de acceso (ilustración 5-1) llegue a manos del responsable, y la verifique, este responderá al titular de los datos, en un plazo de cómo máximo un mes tras la recepción, para satisfacer su petición. La contestación se atenderá, haya o no datos de la persona que la solicite en el fichero.

Como respuesta, sea por el medio que sea, se presentará un informe que de forma legible e inteligible pueda interpretar el titular. Se presentarán todos los datos que la empresa mantenga en el fichero sobre el titular, sean los datos que el usuario cedió, o aquellos que se obtienen derivados del tratamiento de sus datos, así como la información de origen y finalidad de los mismos.

El derecho de acceso se podrá denegar si ya se ha ejercitado en los últimos 12 meses desde el anterior ejercicio, o si una Ley así lo prevé.

EJERCICIO DE LOS DERECHOS DE RECTIFICACIÓN Y CANCELACIÓN

El resultado de ejercitar este derecho es que los datos del titular se verán corregidos ó eliminados en el fichero que la empresa mantiene.

La rectificación procede cuando el encargado comprueba que la empresa mantiene datos inexactos ó incompletos, inadecuados o excesivos. Para ejecutarla, hay que comprobar que junto a la solicitud de rectificación (ilustración 5-3), se recibe alguna documentación que acredite el error en los datos.

El derecho de rectificación se debe hacer efectivo en un plazo de diez días (naturales para ficheros de titularidad privada, hábiles para titularidad pública), tras recibir la solicitud, y comprobar su validez.

Se podrá denegar el ejercicio del derecho de cancelación cuando todavía se estén usando los datos para satisfacer una relación contractual, o se deban conservar durante un periodo, debido a alguna disposición. La rectificación se podrá denegar si no se puede acreditar el error que se afirma tienen los datos. Ambos derechos se podrán denegar además, si una Ley así lo prevé.

EJERCICIO DEL DERECHO DE OPOSICIÓN

El derecho de oposición (ilustración 5-4) se ejercita mediante un escrito al responsable del tratamiento, que resolverá en un plazo de diez días.

Aunque el responsable del tratamiento no disponga de datos, del solicitante, se lo deberá informar igualmente. Si se acepta el ejercicio del derecho, el responsable excluirá del tratamiento los datos correspondientes al solicitante.

Como en otros casos, el ejercicio de éste derecho se podrá denegar si existe una Ley que así lo disponga.

FORMULARIOS E INSTRUCCIONES DE EJERCICIO DE DERECHOS

A continuación, se van a presentar los formularios estandarizados que se proporcionarán al titular de los datos para permitir el ejercicio de sus derechos. Estos formularios deberán aparecer en la página web de la empresa de manera accesible, y si el cliente así lo desea, se le deberán proporcionar impresos por otros medios. Del mismo modo, se deberán tratar, se reciban por el medio que se reciban

FORMULARIO DE EJERCICIO DEL DERECHO DE ACCESO

DATOS DE LA UNIDAD DE ATENCIÓN DE EJERCICIO DE DERECHOS			
Nombre	Oficina Central de Transportes S.A.		
Dirección	Calle Mayor s/n	C.P.	09001
Localidad	Burgos	Provincia	Burgos
DATOS DEL SOLICITANTE			
Nombre y apellidos			
Domicilio			
Localidad			
Provincia		Código Postal	
e-mail		Teléfono	
DATOS DEL REPRESENTANTE LEGAL			
Nombre y apellidos			
Domicilio			
Localidad			
Provincia		Código Postal	
e-mail		Teléfono	

SOLICITUD DEL DERECHO DE ACCESO	
Nombre del Fichero	
<p>El solicitante, mayor de edad, con DNI....., del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de acceso, de conformidad con los artículos 15 de la Ley Orgánica 15/1999, y los artículos 27 a 30 del Real Decreto 1720/2007.</p> <p>SOLICITA :</p> <p>1.- Que se le facilite gratuitamente el acceso a su fichero/s en el plazo legalmente establecido desde la recepción de esta solicitud.</p> <p>2.- Que si la solicitud del derecho de acceso fuese estimada, se le remita la información a través del siguiente medio y dirección:</p> <p>.....</p> <p>.....</p> <p>.....</p> <p>3.- Que esta información comprenda de modo legible los datos de base que sobre su persona están incluidos en el fichero/s, y los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los datos, los cesionarios y la especificación de los concretos usos y finalidades para los que se almacenaron.</p> <p>En..... a..... de..... de 20...</p> <p>Firma</p>	

Formulario 5-1: Formulario de ejercicio del derecho de acceso

FORMULARIO DE EJERCICIO DEL DERECHO DE CANCELACIÓN

DATOS DE LA UNIDAD DE ATENCIÓN DE EJERCICIO DE DERECHOS			
Nombre	Oficina Central de Transportes S.A.		
Dirección	Calle Mayor s/n	C.P.	09001
Localidad	Burgos	Provincia	Burgos
DATOS DEL SOLICITANTE			
Nombre y apellidos			
Domicilio			
Localidad			
Provincia		Código Postal	
e-mail		Teléfono	
DATOS DEL REPRESENTANTE LEGAL			
Nombre y apellidos			
Domicilio			
Localidad			
Provincia		Código Postal	
e-mail		Teléfono	

SOLICITUD DEL DERECHO DE CANCELACIÓN	
Nombre del Fichero	
<p>El solicitante, mayor de edad, con DNI....., del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de acceso, de conformidad con los artículos 16 de la Ley Orgánica 15/1999, y los artículos 31 a 33 del Real Decreto 1720/2007.</p> <p>SOLICITA :</p> <ol style="list-style-type: none"> 1. Que se proceda a la efectiva cancelación de cualesquiera datos relativos a su persona que se encuentren en el fichero indicado, en los términos previstos en la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal y se comunique de forma escrita a la dirección arriba indicada. 2. Que, en el caso de que el responsable del fichero considere que dicha cancelación no procede, lo comunique igualmente, de forma motivada. <p>En..... a..... de..... de 20...</p> <p>Firma</p>	

ANEXO: RELACION DE DATOS A CANCELAR		
En caso de que no se requiera cancelar todo el fichero, haga constar sólo los datos a cancelar		
#	Dato a Cancelar	Documento Acreditativo
1		
2		
3		
4		

Formulario 5-2: Formulario de ejercicio del derecho de cancelación

FORMULARIO DE EJERCICIO DEL DERECHO DE RECTIFICACIÓN

DATOS DE LA UNIDAD DE ATENCIÓN DE EJERCICIO DE DERECHOS			
Nombre	Oficina Central de Transportes S.A.		
Dirección	Calle Mayor s/n	C.P.	09001
Localidad	Burgos	Provincia	Burgos
DATOS DEL SOLICITANTE			
Nombre y apellidos			
Domicilio			
Localidad			
Provincia		Código Postal	
e-mail		Teléfono	
DATOS DEL REPRESENTANTE LEGAL			
Nombre y apellidos			
Domicilio			
Localidad			
Provincia		Código Postal	
e-mail		Teléfono	

SOLICITUD DEL DERECHO DE RECTIFICACIÓN	
Nombre del Fichero	
<p>El solicitante, mayor de edad, con DNI....., , del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de rectificación, de conformidad con el artículo 16 de la Ley Orgánica 15/1999, y los artículos 31 a 33 del Real Decreto 1720/2007.</p> <p>SOLICITA :</p> <ol style="list-style-type: none"> 1. Que se proceda gratuitamente, a la efectiva corrección de los datos inexactos relativos a su persona que se encuentren en el fichero indicado. 2. Los datos que hay que rectificar se enumeran en la hoja anexa, haciendo referencia a los documentos que se acompañan a esta solicitud y que acreditan, en caso de ser necesario, la veracidad de los nuevos datos. 3. Que se comunique de forma escrita a la dirección arriba indicada, la rectificación de los datos una vez realizada. 4. Que, en el caso de que el responsable del fichero considere que la rectificación o la cancelación no procede, se comunique igualmente, de forma motivada. <p>En..... a..... de..... de 20...</p> <p>Firma</p>	

ANEXO: RELACION DE DATOS A RECTIFICAR		
#	Dato a Rectificar	Documento Acreditativo
1		
2		
3		
4		

Formulario 5-3: Formulario de ejercicio del derecho de rectificación

FORMULARIO DE EJERCICIO DEL DERECHO DE OPOSICIÓN

DATOS DE LA UNIDAD DE ATENCIÓN DE EJERCICIO DE DERECHOS			
Nombre	Oficina Central de Transportes S.A.		
Dirección	Calle Mayor s/n	C.P.	09001
Localidad	Burgos	Provincia	Burgos
DATOS DEL SOLICITANTE			
Nombre y apellidos			
Domicilio			
Localidad			
Provincia		Código Postal	
e-mail		Teléfono	
DATOS DEL REPRESENTANTE LEGAL			
Nombre y apellidos			
Domicilio			
Localidad			
Provincia		Código Postal	
e-mail		Teléfono	

SOLICITUD DEL DERECHO DE OPOSICIÓN	
Nombre del Fichero	
<p>El solicitante, mayor de edad, con DNI....., del que acompaña fotocopia, por medio del presente escrito manifiesta su deseo de ejercer su derecho de oposición, de conformidad con el artículo 17 de la Ley Orgánica 15/1999, y los artículos 34 a 36 del Real Decreto 1720/2007</p> <p>SOLICITA :</p> <ol style="list-style-type: none"> 1. Que se ejecute la baja en el tratamiento_ que de sus datos de carácter personal se está actualmente efectuando no existiendo ley a tal efecto que disponga lo contrario. 2. Que el ejercicio del presente derecho se fundamenta por parte del solicitante y, de acuerdo a la normativa actualmente vigente en materia de protección de datos, en el motivo fundado y legítimo que a continuación expone: 	
	
<p>En..... a..... de..... de 20...</p> <p>Firma</p>	

Formulario 5-4: Formulario de ejercicio del derecho de oposición

INSTRUCCIONES EJERCICIO DE DERECHOS LOPD

Los pasos a seguir para el ejercicio de derechos LOPD son:

1. Descargar en su ordenador el formulario de solicitud facilitado por Aena para ejercer sus derechos ARCO, imprimirlo y cumplimentarlo, o bien, si no se desea utilizar el formulario, mediante solicitud indicando:
 - a. Nombre y apellidos del interesado.
 - b. Contenido o petición de la propia solicitud.
 - c. Dirección a efectos de notificaciones, lugar y fecha del solicitante.
2. Firmar la solicitud.
3. Aportar la siguiente documentación junto a la solicitud:
 - a. Fotocopia (por ambas caras) del DNI, o pasaporte, carnet de conducir o cualquier otro medio válido en derecho que acredite la identidad del interesado. En los casos en los que se admita la representación legal, deberá acreditarse la misma mediante la documentación necesaria.
 - b. Documento acreditativo ante petición de rectificación o cancelación que se formula, en su caso.
4. Entregar presencialmente o enviar por correo la documentación requerida junto con la solicitud cumplimentada, a la siguiente dirección:

Oficina Central de Transportes S.A.

Calle Mayor s/n, 09001, Burgos

Asimismo, podrá presentarla en cualquier Centro de Trabajo de Transportes S.A., los cuales, lo comunicarán de inmediato a la central de la empresa.

La empresa comunicará y atenderá a la mayor brevedad posible y en los plazos legalmente previstos su solicitud, atendiendo al tipo de ejercicio de derechos remitido.

6. PROCEDIMIENTOS

La LOPD establece dos procedimientos relacionados con la salvaguarda de los derechos del titular de los datos:

- Procedimiento de tutela de derechos: Su finalidad es garantizar el ejercicio de los derechos que la Ley reconoce a los ciudadanos, independientemente del resultado de los mismos.
- Procedimiento sancionador: Está dirigido a sancionar las conductas contrarias a la LOPD por parte de los responsables del tratamiento de datos de carácter personal.

PROCEDIMIENTO DE TUTELA

Cualquier persona que estime que no se le ha facilitado o atendido correctamente el ejercicio de su derecho de acceso, rectificación, cancelación u oposición, puede interponer la oportuna reclamación ante la Agencia Española de Protección de Datos para que inicie un procedimiento de tutela de sus derechos.

Para ello, resulta necesario que haya transcurrido el plazo de un mes, si se trata de ejercitar el derecho de acceso, o de 10 días naturales si se trata del ejercicio de los derechos de rectificación, cancelación u oposición, desde la solicitud, sin que de forma expresa se le haya contestado.

El procedimiento se encargará de determinar si se ha producido una infracción o no, indicando en caso de existir el tipo de infracción y las sanciones asociadas a la misma.

PROCEDIMIENTO SANCIONADOR

El procedimiento sancionador se encarga de determinar si existe algún tipo de infracción contra el tratamiento de datos de carácter personal, y en su caso de imponer las sanciones.

Los responsables de los ficheros y los encargados de los tratamientos estarán sujetos al régimen sancionador establecido en la Ley Orgánica 15/1999, de 13 de diciembre.

Con anterioridad a la iniciación del procedimiento sancionador, se podrán realizar actuaciones previas con objeto de determinar si concurren circunstancias que justifiquen tal iniciación. En especial, estas actuaciones se orientarán a determinar, con la mayor precisión posible, los hechos que pudieran justificar la incoación del procedimiento, identificar la persona u órgano que pudiera resultar responsable y fijar las circunstancias relevantes que pudieran concurrir en el caso.

Cuando el Director de la Agencia Española de Protección de Datos aprecia la existencia de indicios susceptibles de motivar la imputación de una infracción, dictará acuerdo de inicio de procedimiento sancionador o de infracción de las Administraciones públicas.

Dicho acuerdo de inicio del procedimiento sancionador deberá contener:

- Identificación de la persona o personas presuntamente responsables.
- Descripción sucinta de los hechos imputados, su posible calificación y las sanciones que pudieran corresponder, sin perjuicio de lo que resulte de la instrucción.
- Indicación de que el órgano competente para resolver el procedimiento es el Director de la Agencia Española de Protección de Datos.
- Indicación al presunto responsable de que puede reconocer voluntariamente su responsabilidad, en cuyo caso se dictará directamente resolución.
- Designación de instructor y, en su caso, secretario, con expresa indicación del régimen de recusación de los mismos.
- Indicación expresa del derecho del responsable a formular alegaciones, a la audiencia en el procedimiento y a proponer las pruebas que estime procedentes.
- Medidas de carácter provisional que pudieran acordarse, en su caso, conforme a lo establecido en la sección primera del presente capítulo.

El plazo máximo para dictar resolución será el que determinen las normas aplicables a cada procedimiento sancionador, y se computará desde la fecha en que se dicte el acuerdo de inicio hasta que se produzca la notificación de la resolución sancionadora, o se acredite debidamente el intento de notificación. El vencimiento del citado plazo máximo, sin que se haya dictado y notificado resolución expresa, producirá la caducidad del procedimiento y el archivo de las actuaciones. Las resoluciones de la Agencia

Española de Protección de Datos u órgano correspondiente de la Comunidad Autónoma agotan la vía administrativa.

CASO DE ESTUDIO

En el ejercicio de procedimientos de tutela, o sancionadores, la empresa no participaría como parte iniciadora del proceso, sino como la parte ante la cual se interpone una reclamación. Es por ello que ante la recepción de una reclamación en forma de procedimiento de tutela o sanción, la empresa deberá tener bien prepara la actuación.

La LOPD reconoce al interesado la facultad de solicitar la tutela de la Agencia cuando considere que sus derechos de acceso, rectificación, cancelación u oposición no han sido atendidos correctamente. En estos casos, la AEPD actúa casi como un centro de arbitraje y estima o desestima la petición del interesado.

Incluso, se puede estimar la petición del interesado por motivos formales, aunque no haya lugar a hacer efectivo el derecho nuevamente (por ejemplo, porque se respondió fuera de plazo o durante el propio procedimiento). Nunca un procedimiento de tutela se resuelva con la imposición de una multa al responsable del fichero.

PROCEDIMIENTO DE TUTELA

El comienzo del procedimiento es iniciativa del afectado. Éste deberá expresar con claridad el contenido de su reclamación y de los derechos que se consideran vulnerados.

Una vez que se reciba la reclamación en la AEPD, se remitirá la misma al responsable del fichero, para que en un plazo de quince días, formule las alegaciones que estime pertinentes. Puesto que el responsable del fichero deberá presentar sus alegaciones contra dicha reclamación, es muy importante que se registre y justifique el motivo de la negación del ejercicio. El responsable deberá desarrollar las condiciones de negación de ejercicio de derechos. Por ejemplo:

- Negación del derecho de acceso
 - Ya se realizó el ejercicio en los últimos 12 meses
 - Previsto por ley
 - Ejercicio por un no titular o no autorizado de los datos

- Negación del derecho de rectificación
 - Los datos todavía están en uso para una relación contractual
 - Imposible acreditar error por el que se reclama
 - Previsto por ley
- Negación del derecho de cancelación
 - Datos todavía en uso para una relación contractual
 - Previsto por ley
- Negación del derecho de oposición
 - No existen datos en tratamiento
 - Previsto por ley

Como prueba la empresa aportará los formularios de ejercicio de derecho que se hayan utilizado, y se deberán cotejar ante notario con aquellos que aporte el titular de la reclamación. También se aportará la correspondiente documentación que argumente el motivo de la negación del ejercicio del derecho.

Una vez que se hayan preparado las alegaciones o haya transcurrido el plazo de quince días, la AEPD, utilizando los informes, pruebas y otros actos de instrucción pertinentes, incluida la audiencia del afectado y nuevamente del responsable del fichero, resolverá sobre la reclamación formulada.

Es importante recordar, que aunque el fallo de la AEPD sea contra la empresa, en éste punto, no se podría todavía imponer una sanción a la misma.

PROCEDIMIENTO SANCIONADOR

Si la AEPD detecta una infracción muy grave sobre la LOPD, consistente en la utilización o cesión ilícita de los datos de carácter personal en la que se impida o se atente contra el ejercicio de los derechos de los ciudadanos y las libertades que la Constitución y las leyes garantizan, el Director de la AEPD podrá, en cualquier momento del procedimiento, requerir a los responsables de ficheros o tratamientos de datos de carácter personal, tanto de titularidad pública como privada, el cese en el tratamiento de los datos.

El requerimiento deberá ser atendido en el plazo no prorrogable de tres días, durante el cual el responsable del fichero podrá formular las alegaciones que considere oportunas para demostrar su inocencia. En éste caso, al igual que en el anterior, se deberá tener bien definida la actuación de la empresa. Se utilizarán como prueba de defensa los procedimientos de disociación que la empresa, y los documentos que se relacionen con la cesión de datos que realice la empresa, para así justificar que ni se han utilizado indebidamente, ni se han cedido a terceros no autorizados.

Si el requerimiento fuera desatendido, el Director de la Agencia Española de Protección de Datos podrá, mediante resolución motivada, acordar la inmovilización de tales ficheros o tratamientos, a los solos efectos de restaurar los derechos de las personas afectadas.

7. MEDIDAS DE SEGURIDAD

PRESENTACIÓN

El artículo 9 de la LOPD, establece que "el responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural".

El Reglamento de desarrollo de la LOPD en su Título VIII, desarrolla las medidas de seguridad en el tratamiento de datos de carácter personal y tiene por objeto establecer las medidas de índole técnica y organizativa necesarias para garantizar la seguridad que deben reunir los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos de carácter personal.

Entre estas medidas, se encuentra la elaboración e implantación de la normativa de seguridad mediante un documento de obligado cumplimiento para el personal con acceso a los datos de carácter personal.

Con el objeto de facilitar a los responsables de ficheros y a los encargados de tratamientos de datos personales la adopción de las disposiciones del Reglamento, la AEPD pone a su disposición este documento, en el que se recopila un cuadro resumen de las medidas de seguridad recogidas en el citado Título VIII, un modelo de "Documento de Seguridad", que sirve de guía y facilita el desarrollo y cumplimiento de la normativa sobre protección de datos, y por último, una relación de comprobaciones con el objeto de facilitar la realización de la auditoría de seguridad.

NIVELES DE SEGURIDAD

La ley identifica tres niveles de medidas de seguridad, BÁSICO, MEDIO y ALTO, los cuales tendrán que adoptarse dependiendo del tipo de datos que contengan (datos de

salud, ideología, religión, creencias, infracciones administrativas, de tendencia sexual, etc.).



CUADRO RESUMEN MEDIDAS DE SEGURIDAD

Reglamento de medidas de seguridad de los ficheros que contengan datos de carácter personal (RD 994/1999)

Nivel básico: Ficheros que contengan datos de carácter personal.

Nivel medio: Ficheros que contengan datos relativos a la comisión de infracciones administrativas o penales, Hacienda Pública, servicios financieros y los que se rijan por el artículo 29 de la LOPD (prestación de servicios de solvencia y crédito).

Nivel alto: Ficheros que contengan datos de ideología, religión, creencias, origen racial, salud o vida sexual así como los recabados para fines policiales sin consentimiento de las personas afectadas.

	NIVEL BÁSICO	NIVEL MEDIO	NIVEL ALTO
DOCUMENTO DE SEGURIDAD	<ul style="list-style-type: none"> - Ambito de aplicación. - Medidas, normas, procedimientos reglas y estándares de seguridad. - Funciones y obligaciones del personal. - Estructura y descripción de ficheros y sistemas de información. - Procedimiento de notificación, gestión y respuesta ante incidencias. - Proced. realización copias de respaldo y recuperación de datos. 	<ul style="list-style-type: none"> - Identificación del responsable de seguridad. - Control periódico del cumplimiento del documento. - Medidas a adoptar en caso de reutilización o desecho de soportes. 	
PERO TUAL	<ul style="list-style-type: none"> - Funciones y obligaciones claramente definidas y documentadas. - Difusión entre el personal, de las normas que les afecten y de las consecuencias por incumplimiento. 		
INCIDEN CIAS	<ul style="list-style-type: none"> - Registrar tipo de incidencia, momento en que se ha producido, persona a la que se comunica y efectos derivados. 	<ul style="list-style-type: none"> - Registrar realización de procedimientos de recuperación de los datos, persona que lo ejecuta, datos restaurados y grabados manualmente. - Autorización por escrito del responsable del fichero para su recuperación. 	
IDENTIFICACIÓN Y AUTENTICACIÓN	<ul style="list-style-type: none"> - Relación actualizada de usuarios y accesos autorizados. - Procedimientos de identificación y autenticación. - Criterios de accesos. - Procedimientos de asignación y gestión de contraseñas y periodicidad con que se cambian. - Almacenamiento ininteligible de contraseñas activas. 	<ul style="list-style-type: none"> - Se establecerá el mecanismos que permita la identificación de forma inequívoca y personalizada de todo usuario y la verificación de que está autorizado. - Limite de intentos reiterados de acceso no autorizado. 	
CONTROL DE ACCESO	<ul style="list-style-type: none"> - Cada usuario accederá únicamente a los datos y recursos necesarios para el desarrollo de sus funciones. - Mecanismos que eviten el acceso a datos o recursos con derechos distintos de los autorizados. - Concesión de permisos de acceso sólo por personal autorizado. 	<ul style="list-style-type: none"> - Control de acceso físico a los locales donde se encuentren ubicados los sistemas de información. 	
GESTIÓN DE SOPORTES	<ul style="list-style-type: none"> - Identificar el tipo de información que contienen. - Inventario. - Almacenamiento con acceso restringido. - Salida de soportes autorizada por el responsable del fichero. 	<ul style="list-style-type: none"> - Registro de entrada y salida de soportes. - Medidas para impedir la recuperación posterior de información de un soporte que vaya a ser desechado o reutilizado. - Medidas que impidan la recuperación indebida de la información almacenada en un soporte que vaya a salir como consecuencia de operaciones de mantenimiento. 	<ul style="list-style-type: none"> - Cifrado de datos en la distribución de soportes.
COPIAS DE RESPALDO	<ul style="list-style-type: none"> - Verificar la definición y aplicación de los procedimientos de copias y recuperación. - Garantizar la reconstrucción de los datos en el estado en que se encontraban en el momento de producirse la pérdida o destrucción. - Copia de respaldo, al menos semanal. 		<ul style="list-style-type: none"> - Copia de respaldo y procedimientos de recuperación en lugar diferente del que se encuentren los equipos.
RESPON SABLE		<ul style="list-style-type: none"> - Uno o varios nombrados por el responsable del fichero. - Encargado de coordinar y controlar las medidas del documento. - No supone delegación de responsabilidad del responsable del fichero. 	
PRUE BAS		<ul style="list-style-type: none"> - Solo se realizarán si se asegura el nivel de seguridad correspondiente al tipo de fichero tratado. 	
AUDITORIA		<ul style="list-style-type: none"> - Al menos cada dos años, interna o externa. - Adecuación de las medidas y controles. - Deficiencias y propuestas correctoras. - Análisis del responsable de seguridad y conclusiones al responsable del fichero. - Adopción de las medidas correctoras adecuadas. 	
REGISTRO DE ACCESOS			<ul style="list-style-type: none"> - Registrar usuario, hora, fichero, tipo acceso y registro accedido. - Control del responsable de seguridad. Informe mensual. - Conservación 2 años.
TELE COMU NICACIONES			<ul style="list-style-type: none"> - Transmisión de datos cifrada.

- Los niveles son acumulativos y tienen la condición de mínimos exigibles.
- Los accesos a través de redes de telecomunicaciones deben garantizar un nivel de seguridad equivalente al de los accesos en modo local.
- La ejecución de trabajos fuera de los locales de la ubicación del fichero debe ser expresamente autorizada por el responsable del fichero y garantizar el nivel de seguridad.
- Los ficheros temporales deberán cumplir el nivel de seguridad correspondiente y serán borrados una vez que hayan dejado de ser necesarios.
- Los ficheros de nivel básico que contengan datos que permitan obtener una evaluación de la personalidad del individuo deberán garantizar, además de las medidas de nivel básico, las de nivel medio relativas a auditoría, identificación y autenticación, control de acceso físico y gestión de soportes.

Ilustración 7-1: Cuadro Resumen de Medidas de Seguridad

OBLIGACIONES

La LOPD impone una serie de obligaciones legales para aquellas personas físicas o jurídicas que dispongan de ficheros con datos de carácter personal.

El R.D. 1720/2007 establece la obligación de las empresas/Instituciones a poner en marcha las medidas detalladas en la mencionada ley y que afectan a sistemas informáticos, archivos de papel, personal, procedimientos operativos, medidas de seguridad, etc.

Las obligaciones legales son:

- Inscripción de los ficheros en el Registro General de la Protección de Datos.
- Redacción del documento de seguridad.
- Redacción de cláusulas de protección de datos.
- Auditoría.
- Otras medidas de seguridad de tipo técnico y organizativo necesarias para poder garantizar la seguridad de los datos objeto del tratamiento.
- Redacción de los contratos, formularios y cláusulas necesarias para la recogida de datos, los tratamientos efectuados por terceros y las cesiones o comunicaciones de datos.

SANCIONES

Se establecen una serie de sanciones, por el incumplimiento de la ley, a los responsables de los ficheros que contengan datos de carácter personal. Estas se clasifican como leves, graves y muy graves, dependiendo de la infracción cometida.

LEVES - Multa de 601,01 € a 60.101,21 € (100.000 a 10.000.000 de pesetas.)

GRAVES - Multa de 60.101,21 € a 300.506,05 € (10.000.000 a 50.000.000 pesetas)

MUY GRAVES - Multa de 300.506,05 € a 601.012,10 € (50.000.000 a 100.000.000 de pesetas)

DOCUMENTO DE SEGURIDAD

El documento de seguridad es una de las partes fundamentales de la protección de datos. Se trata de un documento mediante el cual se elabora y adoptan las medidas técnicas y organizativas necesarias para garantizar la seguridad de los datos de carácter personal, su adopción es de obligado cumplimiento para el responsable del fichero, o en su caso, del encargado del tratamiento.

El Real Decreto 1720/2007, en el que se desarrolla la LOPD, establece el reglamento de medidas de seguridad de los ficheros automatizados que contengan datos de carácter personal, indicando que es obligatoria su adopción siempre que se traten datos personales, cualquiera que sea el nivel de seguridad al que correspondan.

Se considera una infracción grave “Mantener los ficheros, locales, programas o equipos que contengan datos de carácter personal sin las debidas condiciones de seguridad que por vía reglamentaria se determinen”.

Toda persona con acceso a datos personales, o que intervenga en alguna fase del tratamiento de los mismos, debe ceñirse a lo establecido en el documento de seguridad, en el cual se establecerán claramente las funciones y obligaciones del personal.

Sin embargo, es responsabilidad del responsable del fichero adoptar las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

CASO DE ESTUDIO

Esta empresa mantiene tres ficheros que serán objeto de aplicación de medidas de seguridad al contener datos de carácter personal. En el caso de los clientes y de los datos publicitarios, se tratan datos personales sencillos, por lo que el nivel de seguridad a aplicar será de nivel básico. Sin embargo, en el caso de los trabajadores, se mantienen datos sensibles, como son la salud, la afiliación sindical y la solvencia, de modo que se aplicarán medidas de seguridad de nivel alto.

CONTENIDO DEL DOCUMENTO DE SEGURIDAD DE NIVEL BÁSICO

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

- Ámbito de aplicación del documento con especificación detallada de los recursos protegidos.
- Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en este Reglamento.
- Funciones y obligaciones del personal.
- Estructura de los ficheros con datos de carácter personal y descripción de los sistemas de información que los tratan.
- Procedimiento de notificación, gestión y respuesta ante las incidencias.
- Los procedimientos de realización de copias de respaldo y de recuperación de los datos.

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

El contenido del documento deberá adecuarse, en todo momento, a las disposiciones vigentes en materia de seguridad de los datos de carácter personal.

CONTENIDO DEL DOCUMENTO DE SEGURIDAD DE NIVEL MEDIO

El documento de seguridad deberá contener, además de lo dispuesto en las medidas de seguridad de nivel bajo:

- La identificación del responsable o responsables de seguridad: El responsable del fichero designará uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el documento de seguridad. En ningún caso esta designación supone una delegación de la responsabilidad que corresponde al responsable del fichero de acuerdo con este Reglamento.
- Los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento. Los sistemas de información e instalaciones de tratamiento de datos se someterán a una auditoría interna o externa, que verifique el cumplimiento del presente Reglamento, de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.
- Las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado. Deberá establecerse un sistema de registro de entrada y salida de soportes informáticos. Cuando un soporte vaya a ser desechado o reutilizado, se adoptarán las medidas necesarias para impedir cualquier recuperación posterior de la información almacenada en él, previamente a que se proceda a su baja en el inventario.

CONTENIDO DEL DOCUMENTO DE SEGURIDAD DE NIVEL ALTO

Además de las medidas de nivel básico y medio, se adoptarán las siguientes:

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

Registro de accesos. De cada acceso se guardarán, como mínimo, la identificación del usuario, la fecha y hora en que se realizó, el fichero accedido, el tipo de acceso y si ha sido autorizado o denegado.

- En el caso de que el acceso haya sido autorizado, será preciso guardar la información que permita identificar el registro accedido.
- Los mecanismos que permiten el registro de los datos detallados en los párrafos anteriores estarán bajo el control directo del responsable de seguridad

competente sin que se deba permitir, en ningún caso, la desactivación de los mismos.

- El período mínimo de conservación de los datos registrados será de dos años.
- El responsable de seguridad competente se encargará de revisar periódicamente la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes.

Copias de respaldo y recuperación.

- Deberá conservarse una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente de aquél en que se encuentren los equipos informáticos que los tratan cumpliendo en todo caso, las medidas de seguridad exigidas en este Reglamento.

8. OBLIGACIONES Y RESPONSABILIDADES DEL TITULAR DEL FICHERO:

El responsable del fichero es la persona que decide sobre la finalidad, contenido y uso del tratamiento. Básicamente, es quien toma las decisiones sobre el fichero, pero a su vez es el encargado de cumplir con una serie de obligaciones referentes al manejo del mismo:

- Se encargará de inscribir el fichero en el Registro General de Protección de Datos que mantiene la Agencia Española de Protección de Datos.
- Definirá la titularidad y responsabilidad del fichero.
- Actuará ante las sanciones, y dará cuenta de la corrección del fichero.
- Asegurará el cumplimiento de los principios básicos que enuncia la LOPD.
- Asegurará la existencia de los oportunos procedimientos de ejercicio de derechos de los titulares de los datos.
- Solicitará autorizaciones para la transferencia de datos a otros países.

EL REGISTRO GENERAL

El Registro General de Protección de Datos (RGPD) es un órgano perteneciente a la Agencia Española de Protección de Datos (AEPD), encargado de permitir el acceso público a los ficheros de datos de carácter personal, para así facilitar el ejercicio de los derechos del titular de los datos. Asimismo, el RGPD tiene entre sus funciones instruir los expedientes de modificación y cancelación de los asientos, instruir los expedientes de transferencias internacionales, rectificar los posibles errores de los asientos, certificar los asientos y publicar anualmente la relación de ficheros inscritos.

INSCRIPCIÓN DE FICHEROS EN EL REGISTRO

La creación de cualquier fichero de datos personales, obliga al responsable del mismo a su inscripción en el RGPD, ya sea persona física ó jurídica, de naturaleza pública ó privada, ó pertenecientes a un órgano administrativo.

Además, a parte de los ficheros de datos personales, se deberán inscribir en el registro las autorizaciones de transferencia internacional de datos, y los códigos de conducta.

MANEJO DE FICHEROS DE TITULARIDAD PRIVADA

Los ficheros de datos personales se podrán crear cuando resulten necesarios para realizar una actividad legítima para el titular y se respeten las garantías que la LOPD establece para la protección de las personas.

Su inscripción se realizará mediante formulario facilitado por la AEPD. Si se trata de un fichero público, será necesario que aparezca la notificación de su creación en el BOE, mientras que si es privado se crea directamente.

La notificación de los ficheros de titularidad privada deberá ser anterior a su creación, y contendrá la información solicitada por los formularios oficiales correspondientes. Las modificaciones y cancelaciones se deberán notificar en el plazo de un mes desde la modificación, usando también los formularios oficiales correspondientes.

En caso de discrepancia con las resoluciones del Director de la AEPD sobre modificación o cancelación de la inscripción de un fichero de titularidad privada procederá el recurso contencioso administrativo.

CASO DE ESTUDIO

En el caso de estudio, nuestro responsable del fichero es el Sr. Responsable, una persona, nombrada específicamente por la dirección de la empresa para encargarse de dichas tareas.

Primero se encargará de revisar los ficheros para asegurar que su estructura cumple con los principios que enuncia la LOPD. Los ficheros se deberán revisar hasta que la estructura de los mismos sea correcta.

Una vez revisados los ficheros, el primer cometido que el Sr. Responsable tendrá que ejecutar será la inscripción de los ficheros de la empresa en el RGPD de la AEPD. Será necesaria la inscripción de los dos ficheros creados, el de clientes, y el de trabajadores. La inscripción se realiza mediante el impreso NOTA (Notificaciones Telemáticas a la AEPD), que se puede conseguir en la página web de la AEPD. En el propio impreso, aparte de inscribir el propio fichero, se definirá los datos identificativos y descriptivos del mismo. La legitimidad de los ficheros está asegurada, al tratarse de ficheros para la ejecución de una actividad comercial.

Ahora que los ficheros ya se encuentran inscritos en el RGPD, y cualquier ciudadano puede consultar si sus datos están siendo tratados en los ficheros, hay que poner en marcha los mecanismos que permitan el ejercicio de los derechos. Los derechos de los que deberá dar cuenta el Sr. Responsable son los de acceso, rectificación, cancelación y oposición. Éste es el momento de poner en práctica los mecanismos para el ejercicio de derechos que se enunciaron en el apartado de derechos del presente volumen.

De manera similar a como se han creado los ficheros, será también el responsable quien deberá notificar las modificaciones y cancelaciones que los ficheros de clientes y trabajadores puedan sufrir, teniendo siempre como plazo máximo un mes.

Ante cualquier sanción, es el Sr. Responsable quien deberá hacerse cargo de su gestión. Al tratarse de ficheros de naturaleza privada, las sanciones serán en forma de multa, y el responsable del tratamiento es quien deberá recurrir a la vía jurídica como se estime oportuno para recurrir la sanción.

En el caso que nos atañe, no existirá una transferencia internacional de datos, ya que, aunque la empresa pueda realizar envíos a escala mundial, los datos del envío en sí mismo no se trasladarán.

A continuación, se presentan los impresos NOTA, rellenos con los datos de inscripción de los ficheros de clientes, trabajadores y fines publicitarios.

CONFIGURACIÓN DEL DOCUMENTO NOTA



Fichero de titularidad privada
CONTENIDO DE LA NOTIFICACIÓN



Tipo de solicitud de inscripción.

Indique qué operación va a realizar sobre el fichero. En caso de modificaciones y supresiones se deberá indicar el Código de Inscripción que se asignó al fichero en el momento de su alta en el RGD así como el CIF/NIF con el que fue inscrito. En caso de modificación se solicitan los apartados que se desea modificar y el Nombre o Razón Social del responsable.

Alta Modificación Supresión

Modelo de declaración

Si la notificación se refiere a un tratamiento de datos sobre miembros de comunidades de propietarios, clientes propios, libro de recetario, (clientes de farmacias), nóminas-recursos humanos (empleados) o pacientes, y la finalidad es la gestión propia de estos colectivos, puede marcar el cuadro TIPO y seleccionar el modelo que corresponda (se rellenan determinados apartados con valores apropiados) o bien seleccionar NORMAL para partir de un formulario totalmente vacío.

Normal Tipo

Tipos

Comunidad de Propietarios Nóminas - Recursos Humanos Videovigilancia
 Clientes y/o proveedores Pacientes
 Libro Recetario Gestión Escolar

Presentación de la documentación

¿Cuál es el sistema que empleará para presentar la declaración?

Formulario en papel
 Internet
 Internet firmado con certificado digital

Ilustración 8-1: Configuración de Creación del Fichero NOTA

INSCRIPCIÓN DEL FICHERO DE CLIENTES



**Fichero de titularidad privada
CONTENIDO DE LA NOTIFICACIÓN**



No válida para presentación

1 Responsable del fichero Validar Borrar ?

Denominación social del responsable del fichero		Actividad	
DEPARTAMENTO LOGISTICA		TRANSPORTE	
CIF/NIF	Domicilio Social		
12345678Z	CALLE MAYOR S/N		
Localidad	Código Postal	Provincia	País
BURGOS	09001	BURGOS	ESPAÑA
Teléfono	Fax	Correo electrónico	
947123456	947123456	logistica@transportes.com	

2 Derechos de oposición, acceso, rectificación y cancelación Validar Borrar ?

Nombre de la oficina o dependencia			
OFICINA CENTRAL DE TRANSPORTES S.A.			
CIF/NIF	Dirección postal / Apdo. de Correos		
23456789D	CALLE MAYOR S/N		
Localidad	Código Postal	Provincia	País
BURGOS	09001	BURGOS	ESPAÑA
Teléfono	Fax	Correo electrónico	
947234567	947234567	derechos@transportes.com	

4 Encargado del tratamiento Validar Borrar ?

Denominación social del encargado del tratamiento			
DEPARTAMENTO DE INFORMÁTICA			
CIF/NIF	Dirección postal		
34567890V	CALLE MAYOR S/N		
Localidad	Código Postal	Provincia	País
BURGOS	09001	BURGOS	ESPAÑA
Teléfono	Fax	Correo electrónico	
947345678	947345678	informatica@transportes.com	

5 Identificación y finalidad del fichero Validar Borrar ?

Denominación	
Nombre del fichero o tratamiento	
CLIENTES Y/O PROVEEDORES	
Descripción detallada de finalidad y usos previstos	
GESTION DE CLIENTES Y/O PROVEEDORES	
Tipificación correspondiente a la finalidad y usos previstos	
Finalidades	
COMERCIO ELECTRONICO	GESTION DE CLIENTES CONTABLE, FISCAL Y ADMINISTRATIVA PUBLICIDAD Y PROSPECCION COMERCIAL OTRO TIPO DE FINALIDAD

Ilustración 8-2: Documento NOTA para el Fichero de Clientes


**AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS**



**Fichero de titularidad privada
CONTENIDO DE LA NOTIFICACIÓN**


NOTA
TIFICACIONES
ELEMATICAS A
LA AEPD

No válida para presentación

6 Origen y procedencia de los datos Validar ?

Origen

<input checked="" type="checkbox"/> El propio interesado o su representante legal	<input type="checkbox"/> Otras personas físicas	<input type="checkbox"/> Fuentes accesibles al público
<input type="checkbox"/> Registros públicos	<input type="checkbox"/> Entidad privada	<input type="checkbox"/> Administraciones Públicas

Colectivos o categorías de interesados

PROPIETARIOS O ARRENDATARIOS
PERSONAS DE CONTACTO

CLIENTES Y USUARIOS
PROVEEDORES

Otros colectivos

Ilustración 8-3: Documento NOTA para el Fichero de Clientes, página 2



Fichero de titularidad privada CONTENIDO DE LA NOTIFICACIÓN



No válida para presentación

7 Tipos de datos, estructura y organización del fichero Validar | Borrar | ?

Datos especialmente protegidos :
Los tratamientos de datos de carácter personal que revelen o hagan referencia a ideología, afiliación sindical, religión o creencias, deberán ampararse en alguno de los supuestos que la Ley establece al efecto para poder tratarlos.
El tratamiento de estos datos sólo puede realizarse si se ha recabado el consentimiento expreso y por escrito del afectado. Para más información consulte la ayuda del formulario.

Datos especialmente protegidos

Ideología Afiliación sindical Religión Creencias

Otros Datos especialmente protegidos :
Los tratamientos de datos de carácter personal que revelen o hagan referencia al origen racial, la salud o la vida sexual deberán ampararse en alguno de los supuestos que la Ley establece al efecto para poder tratarlos.
Para el tratamiento de estos datos será obligatorio recabar el consentimiento expreso del afectado o que, por razones de interés general, así lo disponga una Ley.

Otros Datos especialmente protegidos

Origen racial o Étnico Salud Vida sexual

Datos de carácter identificativo

<input checked="" type="checkbox"/> NIF / DNI	<input type="checkbox"/> Nº SS / Mutualidad	<input checked="" type="checkbox"/> Nombre y apellidos	<input type="checkbox"/> Tarjeta Sanitaria
<input checked="" type="checkbox"/> Dirección	<input checked="" type="checkbox"/> Teléfono	<input type="checkbox"/> Firma / Huella	
<input type="checkbox"/> Imagen / voz	<input type="checkbox"/> Marcas físicas	<input type="checkbox"/> Firma electrónica	

Otros datos de carácter identificativo

Otros datos tipificados

ACADEMICOS Y PROFESIONALES
DETALLES DEL EMPLEO

>

<

CARACTERISTICAS PERSONALES
CIRCUNSTANCIAS SOCIALES
INFORMACION COMERCIAL
ECONOMICOS, FINANCIEROS Y DE SEGUROS
TRANSACCIONES DE BIENES Y SERVICIOS

Otros tipos de datos

Sistema de tratamiento

Automatizado Manual Mixto

8 Medidas de seguridad Validar | Borrar | ?

Nivel básico Nivel Medio Nivel Alto

Ilustración 8-4: Documento NOTA para el Fichero de Clientes, página 3


**AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS**



**Fichero de titularidad privada
CONTENIDO DE LA NOTIFICACIÓN**


**NOTIFICACIONES
ELEMATICAS A
LA AEPD**

No válida para presentación

9 Cesión o comunicación de datos Validar Borrar ?

Este apartado únicamente ha de cumplimentarse en el caso de que se prevea realizar cesiones o comunicaciones de datos. No se considerará cesión de datos la prestación de un servicio al responsable del fichero por parte del encargado del tratamiento. La comunicación de los datos ha de ampararse en alguno de los supuestos legales establecidos en la LOPD. Para mayor información consulte la ayuda de este formulario.

Categorías de destinatarios de cesiones

<p>OTROS ORGANOS DE LA ADMINISTRACION PUBLICA FUERZAS Y CUERPOS DE SEGURIDAD OTRAS ENTIDADES FINANCIERAS</p>	<p>></p> <p><</p>	<p>ORGANIZACIONES O PERSONAS DIRECTAMENTE RELACIONADAS ADMINISTRACION TRIBUTARIA BANCOS, CAJAS DE AHORRO Y CAJAS RURALES ENTIDADES DEDICADAS AL CUMPLIMIENTO/INCUMPLIMIENTO EMPRESAS DEDICADAS A PUBLICIDAD O MK DIRECTO</p>
--	-------------------------	--

Otros destinatarios de cesiones

Ilustración 8-5: Documento NOTA para el Fichero de Clientes, página 4

INSCRIPCIÓN DEL FICHERO DE TRABAJADORES



Fichero de titularidad privada CONTENIDO DE LA NOTIFICACIÓN



No válida para presentación

1 Responsable del fichero Validar | Borrar | ?

Denominación social del responsable del fichero Actividad
DEPARTAMENTO DE RECURSOS HUMANOS TRANSPORTE

CIF/NIF Domicilio Social
12345678Z CALLE MAYOR S/N

Localidad Código Postal Provincia País
BURGOS 09001 BURGOS ESPAÑA

Teléfono 947123456 Fax 947123456 Correo electrónico rrhh@transportes.com

2 Derechos de oposición, acceso, rectificación y cancelación Validar | Borrar | ?

Nombre de la oficina o dependencia
OFICINA CETNRL DE TRANSPORTES S.A.

CIF/NIF Dirección postal / Apdo. de Correos
23456789D CALLE MAYOR S/N

Localidad Código Postal Provincia País
BURGOS 09001 BURGOS ESPAÑA

Teléfono 947234567 Fax 947234567 Correo electrónico derechos@transportes.com

4 Encargado del tratamiento Validar | Borrar | ?

Denominación social del encargado del tratamiento
DEPARTAMENTO DE INFORMATICA

CIF/NIF Dirección postal
34567890V CALLE MAYOR S/N

Localidad Código Postal Provincia País
BURGOS 09001 BURGOS ESPAÑA

Teléfono 947345678 Fax 947345678 Correo electrónico informatica@transportes.com

5 Identificación y finalidad del fichero Validar | Borrar | ?

Denominación
Nombre del fichero o tratamiento
NOMINAS, PERSONAL Y RECURSOS HUMANOS

Descripción detallada de finalidad y usos previstos
GESTION DE NOMINAS Y RECURSOS HUMANOS

Tipificación correspondiente a la finalidad y usos previstos

Finalidades

PREVENCION DE RIESGOS LABORALES
OTRO TIPO DE FINALIDAD

>

<

RECURSOS HUMANOS
GESTION DE NOMINAS

Ilustración 8-6: Documento NOTA para el Fichero de Trabajadores, página 1


**AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS**



**Fichero de titularidad privada
CONTENIDO DE LA NOTIFICACIÓN**


NOTA
TIFICACIONES
ELEMATICAS A
LA AEPD

No válida para presentación

6 Origen y procedencia de los datos Validar Borrar ?

Origen

<input checked="" type="checkbox"/> El propio interesado o su representante legal	<input type="checkbox"/> Otras personas físicas	<input type="checkbox"/> Fuentes accesibles al público
<input type="checkbox"/> Registros públicos	<input type="checkbox"/> Entidad privada	<input type="checkbox"/> Administraciones Públicas

Colectivos o categorías de interesados

EMPLEADOS

Otros colectivos

Ilustración 8-7: Documento NOTA para el Fichero de Trabajadores, página 2



Fichero de titularidad privada CONTENIDO DE LA NOTIFICACIÓN



No válida para presentación

7 Tipos de datos, estructura y organización del fichero Validar | Borrar | ?

Datos especialmente protegidos :
Los tratamientos de datos de carácter personal que revelen o hagan referencia a ideología, afiliación sindical, religión o creencias, deberán ampararse en alguno de los supuestos que la Ley establece al efecto para poder tratarlos.
El tratamiento de estos datos sólo puede realizarse si se ha recabado el consentimiento expreso y por escrito del afectado. Para más información consulte la ayuda del formulario.

Datos especialmente protegidos
 Ideología Afiliación sindical Religión Creencias

Otros Datos especialmente protegidos :
Los tratamientos de datos de carácter personal que revelen o hagan referencia al origen racial, la salud o la vida sexual deberán ampararse en alguno de los supuestos que la Ley establece al efecto para poder tratarlos.
Para el tratamiento de estos datos será obligatorio recabar el consentimiento expreso del afectado o que, por razones de interés general, así lo disponga una Ley.

Otros Datos especialmente protegidos
 Origen racial o Étnico Salud Vida sexual

Datos de carácter identificativo
 NIF / DNI Nº SS / Mutualidad Nombre y apellidos Tarjeta Sanitaria
 Dirección Teléfono Firma / Huella
 Imagen / voz Marcas físicas Firma electrónica

Otros datos de carácter identificativo
POSICION GPS

Otros datos tipificados

>

<

CARACTERISTICAS PERSONALES
ACADEMICOS Y PROFESIONALES
DETALLES DEL EMPLEO
ECONOMICOS, FINANCIEROS Y DE SEGUROS
TRANSACCIONES DE BIENES Y SERVICIOS

Otros tipos de datos

Sistema de tratamiento
 Automatizado Manual Mixto

8 Medidas de seguridad Validar | Borrar | ?

Nivel básico Nivel Medio Nivel Alto

Ilustración 8-8: Documento NOTA para el Fichero de Trabajadores, página 3


**AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS**


**Fichero de titularidad privada
CONTENIDO DE LA NOTIFICACIÓN**


NOTA
TIFICACIONES
ELEMATICAS A
LA AEPD

No válida para presentación

9 Cesión o comunicación de datos Validar Borrar ?

Este apartado únicamente ha de cumplimentarse en el caso de que se prevea realizar cesiones o comunicaciones de datos. No se considerará cesión de datos la prestación de un servicio al responsable del fichero por parte del encargado del tratamiento. La comunicación de los datos ha de ampararse en alguno de los supuestos legales establecidos en la LOPD. Para mayor información consulte la ayuda de este formulario.

Categorías de destinatarios de cesiones

<p>ORGANIZACIONES O PERSONAS DIRECTAMENTE RELACIONADAS COLEGIOS PROFESIONALES OTROS ORGANOS DE LA ADMINISTRACION PUBLICA OTRAS ENTIDADES FINANCIERAS ENTIDADES SANITARIAS</p>	<p>></p> <p><</p>	<p>ORGANISMOS DE LA SEGURIDAD SOCIAL ADMINISTRACION TRIBUTARIA BANCOS, CAJAS DE AHORRO Y CAJAS RURALES ENTIDADES ASEGURADORAS</p>
---	-------------------------	---

Otros destinatarios de cesiones

Ilustración 8-9: Documento NOTA para el Fichero de Trabajadores, página 4

INSCRIPCIÓN DEL FICHERO DE FINES PUBLICITARIOS



**Fichero de titularidad privada
CONTENIDO DE LA NOTIFICACIÓN**



No válida para presentación

1 Responsable del fichero Validar Borrar ?

Denominación social del responsable del fichero		Actividad	
DEPARTAMENTO DE PUBLICIDAD		TRANSPORTE	
CIF/NIF	Domicilio Social		
12345678Z	CALLE MAYOR S/N		
Localidad	Código Postal	Provincia	País
BURGOS	09001	BURGOS	ESPAÑA
Teléfono	Fax	Correo electrónico	
947123456	947123456	publicidad@transportes.com	

2 Derechos de oposición, acceso, rectificación y cancelación Validar Borrar ?

Nombre de la oficina o dependencia			
OFICINA CENTRAL DE TRANSPORTES S.A.			
CIF/NIF	Dirección postal / Apdo. de Correos		
23456789D	CALLE MAYOR S/N		
Localidad	Código Postal	Provincia	País
BURGOS	09001	BURGOS	ESPAÑA
Teléfono	Fax	Correo electrónico	
947234567	947234567	derechos@transportes.com	

4 Encargado del tratamiento Validar Borrar ?

Denominación social del encargado del tratamiento			
DEPARTAMENTO DE INFORMATICA			
CIF/NIF	Dirección postal		
34567890V	CALLE MAYOR S/N		
Localidad	Código Postal	Provincia	País
BURGOS	09001	BURGOS	ESPAÑA
Teléfono	Fax	Correo electrónico	
947345678	947345678	informatica@transportes.com	

5 Identificación y finalidad del fichero Validar Borrar ?

Denominación	
Nombre del fichero o tratamiento	
FINES PUBLICITARIOS	
Descripción detallada de finalidad y usos previstos	
GESTION DE DESTINATARIOS DE CAMPAÑAS PUBLICITARIAS	
Tipificación correspondiente a la finalidad y usos previstos	
Finalidades	
COMERCIO ELECTRONICO OTRO TIPO DE FINALIDAD GESTION DE CLIENTES CONTABLE, FISCAL Y ADMINISTRATIVA	PUBLICIDAD Y PROSPECCION COMERCIAL

Ilustración 8-10: Documento NOTA para el Fichero de Fines Publicitarios, página 1


**AGENCIA
ESPAÑOLA DE
PROTECCIÓN
DE DATOS**



**Fichero de titularidad privada
CONTENIDO DE LA NOTIFICACIÓN**


**NOTIFICACIONES
ELECTRONICAS A
LA AEPD**

No válida para presentación

6 Origen y procedencia de los datos Validar Borrarr ?

Origen

<input checked="" type="checkbox"/> El propio interesado o su representante legal	<input type="checkbox"/> Otras personas físicas	<input type="checkbox"/> Fuentes accesibles al público
<input type="checkbox"/> Registros públicos	<input type="checkbox"/> Entidad privada	<input checked="" type="checkbox"/> Administraciones Públicas

Colectivos o categorías de interesados

PROPIETARIOS O ARRENDATARIOS
PERSONAS DE CONTACTO
PROVEEDORES

>

<

CLIENTES Y USUARIOS

Otros colectivos

CLIENTES POTENCIALES

Ilustración 8-11: Documento NOTA para el Fichero de Fines Publicitarios, página 2



**Fichero de titularidad privada
CONTENIDO DE LA NOTIFICACIÓN**



No válida para presentación

7 Tipos de datos, estructura y organización del fichero Validar Borrar ?

Datos especialmente protegidos :
Los tratamientos de datos de carácter personal que revelen o hagan referencia a ideología, afiliación sindical, religión o creencias, deberán ampararse en alguno de los supuestos que la Ley establece al efecto para poder tratarlos.
El tratamiento de estos datos sólo puede realizarse si se ha recabado el consentimiento expreso y por escrito del afectado. Para más información consulte la ayuda del formulario.

Datos especialmente protegidos

<input type="checkbox"/> Ideología	<input type="checkbox"/> Afiliación sindical	<input type="checkbox"/> Religión	<input type="checkbox"/> Creencias
------------------------------------	--	-----------------------------------	------------------------------------

Otros Datos especialmente protegidos :
Los tratamientos de datos de carácter personal que revelen o hagan referencia al origen racial, la salud o la vida sexual deberán ampararse en alguno de los supuestos que la Ley establece al efecto para poder tratarlos.
Para el tratamiento de estos datos será obligatorio recabar el consentimiento expreso del afectado o que, por razones de interés general, así lo disponga una Ley.

Otros Datos especialmente protegidos

<input type="checkbox"/> Origen racial o Étnico	<input type="checkbox"/> Salud	<input type="checkbox"/> Vida sexual
---	--------------------------------	--------------------------------------

Datos de carácter identificativo

<input type="checkbox"/> NIF / DNI	<input type="checkbox"/> Nº SS / Mutualidad	<input checked="" type="checkbox"/> Nombre y apellidos	<input type="checkbox"/> Tarjeta Sanitaria
<input checked="" type="checkbox"/> Dirección	<input checked="" type="checkbox"/> Teléfono	<input type="checkbox"/> Firma / Huella	
<input type="checkbox"/> Imagen / voz	<input type="checkbox"/> Marcas físicas	<input type="checkbox"/> Firma electrónica	

Otros datos de carácter identificativo

Otros datos tipificados

ACADEMICOS Y PROFESIONALES DETALLES DEL EMPLEO CARACTERISTICAS PERSONALES CIRCUNSTANCIAS SOCIALES INFORMACION COMERCIAL ECONOMICOS, FINANCIEROS Y DE SEGUROS TRANSACCIONES DE BIENES Y SERVICIOS	>	
	<	

Otros tipos de datos

Sistema de tratamiento

<input checked="" type="checkbox"/> Automatizado	<input type="checkbox"/> Manual	<input type="checkbox"/> Mixto
--	---------------------------------	--------------------------------

8 Medidas de seguridad Validar Borrar ?

<input checked="" type="checkbox"/> Nivel básico	<input type="checkbox"/> Nivel Medio	<input type="checkbox"/> Nivel Alto
--	--------------------------------------	-------------------------------------

Ilustración 8-12: Documento NOTA para el Fichero de Fines Publicitarios, página 3

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS

NOTA NOTIFICACIONES ELECTRONICAS A LA AEPD

Fichero de titularidad privada
CONTENIDO DE LA NOTIFICACIÓN

No válida para presentación

9 Cesión o comunicación de datos Validar Borrar ?

Este apartado únicamente ha de cumplimentarse en el caso de que se prevea realizar cesiones o comunicaciones de datos. No se considerará cesión de datos la prestación de un servicio al responsable del fichero por parte del encargado del tratamiento. La comunicación de los datos ha de ampararse en alguno de los supuestos legales establecidos en la LOPD. Para mayor información consulte la ayuda de este formulario.

Categorías de destinatarios de cesiones

OTROS ORGANOS DE LA ADMINISTRACION PUBLICA
FUERZAS Y CUERPOS DE SEGURIDAD
ENTIDADES DEDICADAS AL CUMPLIMIENTO/INCUMPLIM
OTRAS ENTIDADES FINANCIERAS
ORGANIZACIONES O PERSONAS DIRECTAMENTE RELAC
ADMINISTRACION TRIBUTARIA
BANCOS, CAJAS DE AHORRO Y CAJAS RURALES

EMPRESAS DEDICADAS A PUBLICIDAD O MK DIRECTO

Otros destinatarios de cesiones

Ilustración 8-13: Documento NOTA para el Fichero de Fines Publicitarios, página 4

9. FICHEROS DE PUBLICIDAD Y PROSPECCIÓN COMERCIAL

El tratamiento de datos de carácter personal con fines de publicidad y prospección comercial supone una excepción a la regla general de necesidad de consentimiento, y queda recogido bajo el artículo 30 de la LOPD, en 4 puntos:

- Los ficheros de publicidad y prospección comercial pueden contener datos procedentes de fuentes accesibles al público o del titular de los mismos, ya sea directamente, o con su consentimiento. Dicho tratamiento puede ser realizado, si la actividad que realiza el responsable del fichero, requiere de publicidad.
- Cuando se envía publicidad a una persona, se le debe indicar el origen de sus datos, la identidad del responsable del fichero y los derechos que tiene el titular de los datos.
- El titular de datos personales contenidos en un fichero de publicidad que ejercite el derecho de acceso, tiene un especial derecho a conocer cuál es el origen de que sus datos figuren en el fichero.
- El titular de datos personales puede oponerse a que sus datos figuren en un fichero de publicidad y prospección comercial sin necesidad de causa justificada.

Aunque el tratamiento de datos personales para fines publicitarios represente una excepción al principio de consentimiento, es importante asegurar que el destinatario desee recibir publicidad, por lo que será necesario consultar, antes de comenzar ninguna campaña las listas Robinson. Las listas Robinson son listas de personas que no desean recibir publicidad no solicitada y son válidas para el Correo, E-Mail, SMS, Teléfono y Fax. En aquellos países en que existen, el empresariado se ha comprometido a respetar ese deseo.

CASO DE ESTUDIO

El sistema publicitario de la empresa incluye el envío de publicidad a los clientes, presentando productos similares a los que ya tienen contratados, y también incluye el mantenimiento de un fichero de destinatarios de publicidad, construido a partir de los datos de clientes que quieren recibir comunicaciones comerciales, y de clientes potenciales, obtenidos de fuentes accesibles al público.

El interés de la empresa en la publicidad es importante, al comenzar su andadura comercial. Es importante captar y fidelizar clientes, por lo que a continuación se establecerán pautas para realizar campañas de publicidad adecuadas a los principios que la LOPD expone.

CAPTACIÓN DE NUEVOS CLIENTES

La información para publicidad destinada a nuevos clientes puede ser obtenida de fuentes públicas. Puesto que aquí utilizaremos la parte de datos obtenida de fuentes accesibles al público, resulta muy importante consultar las listas Robinson antes de mandar. Aunque no sea necesario asegurar el consentimiento del receptor, es muy importante asegurar que quiera recibir algún tipo de publicidad.

Un ejemplo de campaña publicitaria de este tipo, ajustada a la LOPD, podría consistir en realizar una campaña de mailing, desarrollada a nivel nacional, que ponga en contacto al mayor número de posibles clientes con la empresa.

Los destinatarios serían hombres y mujeres, con un perfil medio-alto y edades comprendidas entre los 25 y los 55 años. De esta forma, la compañía amplía el número de registros de personas interesadas y logra establecer un nuevo canal de comunicación con perfiles afines a los servicios que ofrece.

TRANSPORTES S.A.

Comunicación Comercial

Estimado Sr. Pérez:

Nos ponemos en contacto con usted para hacerle llegar nuestras nuevas tarifas para el próximo mes.

Categoría X: X €
Categoría Y: Y €
Categoría Z: Z €

También aprovechamos para recordarle que tiene a su disposición las siguientes promociones:

Promoción X: X €
Promoción Y: Y €
Promoción Z: Z €

Los datos presentes en ésta publicidad han sido obtenidos del fichero de destinos publicitarios de Transportes S.A.

El titular de ésta carta podrá ejercer sus derechos de acceso, cancelación, rectificación y oposición sobre estos datos personales, poniéndose en contacto con Transportes S.A, en cualquier momento.

Ilustración 9-1: Ejemplo publicitario 1

Otras medidas existentes, pueden ser el marketing online para captar nuevos clientes, estrategias virales o email marketing, entre otros. Ahora bien, el éxito de estas campañas se centrará, principalmente, en contar con una base de datos bien segmentada y formada por registros bien identificados.

PUBLICIDAD PARA CLIENTES

Según la LOPD, se puede mandar publicidad personalizada de servicios similares a los prestados, a aquellos clientes que lo soliciten. Es por esto que se puede añadir una cláusula en el contrato de prestación de servicios, verificando que el cliente desea o no, recibir información de servicios similares a los que usa habitualmente.

En éste caso, también se respetarán claramente los derechos del titular de los datos que está recibiendo la publicidad, y en cada envío, se le informará de cuál es el origen de sus datos, y de los derechos que pueda ejercer.

Como ejemplo serviría, que puesto que la empresa dispone de teléfonos de los clientes, puede realizar una campaña “casi” instantánea, al poder enviar mensajes de texto a los terminales de los clientes mientras se les esté realizando un servicio de envío. En este ejemplo, tal y como marca la ley, se deberá añadir un identificativo, indicando que se trata de publicidad.

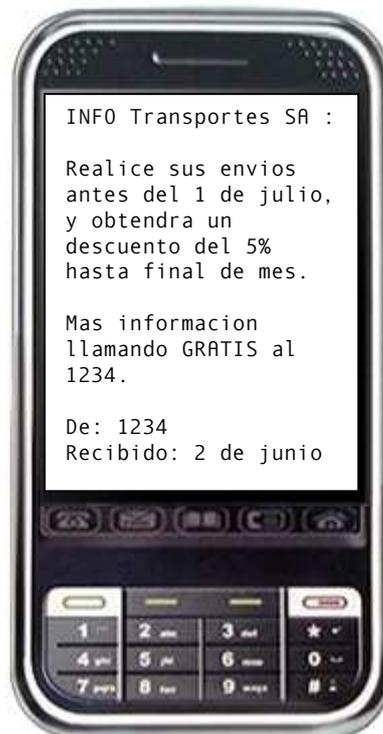


Ilustración 9-2: Ejemplo publicitario 2

10. FICHEROS DE SOLVENCIA PATRIMONIAL

Para la creación de cualquier fichero compuesto por datos de carácter personal, la LOPD establece una serie de obligaciones al responsable del tratamiento del fichero.

En primer lugar, el fichero deberá ser notificado previamente a su creación ante la Agencia Española de Protección de Datos. Los datos que conforman dicho fichero, deberán ser adecuados, pertinentes, no excesivos, exactos y puestos al día y deberán tratarse con la finalidad para lo cual hayan sido recabados.

Asimismo, el Responsable del fichero, deberá informar a las personas de las cuales recabará los datos, acerca de la finalidad del tratamiento de los datos, de los derechos de acceso, rectificación, cancelación y oposición, de la identidad y dirección del Responsable del fichero, etc.

Del mismo modo, en caso de proceder a ceder o comunicar dichos datos a un tercero, como norma general, el Responsable del fichero deberá solicitar el consentimiento para realizar dicha cesión.

Mientras el fichero de morosos se mantenga en un ámbito interno al de la propia empresa no entraría en el objeto de aplicación del artículo 29 de la Ley Orgánica de Protección de Datos relativo a la Prestación de Servicios de Información sobre Solvencia Patrimonial y Crédito.

En cambio la LOPD, sí regula a través del ya nombrado artículo 29, la prestación de servicios de información sobre solvencia patrimonial y crédito.

En cuanto a los ficheros de morosos más conocidos, podemos señalar a modo de ejemplo, el fichero ASNEF (Asociación Nacional de Entidades de Financiación), el cual se creó para la gestión de los impagados de las financieras y cuenta actualmente con los datos de las entidades de crédito, las entidades gestoras de tarjetas de crédito y las operadoras de telefonía.

Asimismo podemos hablar acerca del RAI (Registro de Aceptos Impagados) dependiente del centro de Cooperación Interbancaria, creado por una serie de bancos

con la finalidad de controlar la identidad de los que devolvían las letras de cambio y los pagarés.

En los supuestos anteriores subrayar que la información de los deudores, es proporcionada a dichos ficheros de morosos por parte de sus miembros, asociados o clientes. De esta forma, los miembros de estas entidades realizan consultas a los ficheros de morosos titularidad de éstas, con la finalidad de informarse acerca de la morosidad de una determinada persona, pero también como acreedores, tienen acceso a datos de las personas con las que mantengan una deuda cierta.

Los registros de almacenamiento de datos relativos al cumplimiento o incumplimiento de obligaciones dinerarias, pueden obtener sus datos tanto de fuentes accesibles al público, o directamente de informaciones facilitadas por el interesado o con su consentimiento, o también de un acreedor, o de quien actúe por su cuenta o interés. A esta clase de ficheros le es aplicable en su totalidad el artículo 29 de la LOPD, relativo a la Prestación de servicios de información sobre solvencia patrimonial y crédito.

Para que el acreedor pueda ceder los datos al registro de morosidad, son requisitos imprescindibles:

- La existencia previa de una deuda vencida y exigible, que haya resultado impagada.
- El requerimiento previo de pago a quien corresponda el cumplimiento de la obligación.
- Que el acreedor o quien actúe por su cuenta e interés, se asegure de que concurren todos los requisitos exigidos en los apartados anteriores en el momento de notificar los datos adversos al responsable del registro de morosos.
- Si el dato cedido por el acreedor resultase inexacto o no está actualizado, deberá el acreedor comunicar al responsable del registro en el mínimo tiempo posible la modificación del dato, sin perjuicio del derecho de rectificación y cancelación.
- El responsable del fichero común deberá proceder a la cancelación cautelar del dato, cuando el deudor aporte un principio de prueba documental suficiente, que desvirtúe alguno de los requisitos necesarios.

La característica más sobresaliente de este tipo de ficheros es que no se exige el consentimiento del afectado para realizar el tratamiento de sus datos. Por tanto, no encontramos ante una excepción del artículo 6.1 LOPD.

Estos ficheros de morosos, únicamente podrán ser tratados por una empresa que se dedique a los servicios anteriormente comentados y por lo tanto, según el artículo 29.1 LOPD sólo será legítimo tratar estos datos personales, siempre y cuando la finalidad sea informar acerca de la solvencia patrimonial, capacidad económica, etc. Por lo tanto, un destinatario de los servicios de información sobre solvencia patrimonial podrá consultar libremente la información de uno de estos ficheros, siempre y cuando necesite analizar la solvencia de una persona en relación con sus funciones legítimas, artículo 11.1 LOPD. En base a lo anterior se puede afirmar que la aportación de datos a los ficheros de morosos, aun siendo una cesión de datos, no necesita cumplir con lo establecido por el artículo 11 LOPD, ya que la legitimación proviene directamente del artículo 29 LOPD.

Es más, según el artículo 29.4 LOPD sólo se podrán registrar y ceder datos de carácter personal que sean determinantes para enjuiciar la solvencia patrimonial. En este mismo precepto también se establece un máximo de tiempo por el cual se pueden mantener dichos datos, siendo el mismo de seis años siempre y cuando respondan los datos a la situación actual de aquellos, característica que también recoge el artículo 4.3 relativo a la calidad de los datos.

La obligación de comunicar la inclusión corresponde al responsable del fichero de morosos, y debe realizarse en el plazo máximo de 30 días a contar desde dicha inclusión, informando al afectado de su derecho a recabar información sobre los datos recogidos en el fichero.

Asimismo, existen una serie de limitaciones al tratamiento de los datos de morosidad:

- No pueden facilitarse datos sin relevancia económica.
- El dato registrado (un impago por ejemplo) no puede tener más de seis años de antigüedad, contados desde la fecha de inclusión del dato en el Registro.

- No puede incluirse ningún impago o cumplimiento irregular, sino desde el cuarto mes, contado a partir del vencimiento de la obligación incumplida o del plazo en concreto de la misma si fuera de cumplimiento periódico.

Por lo tanto, a partir de la entrada en vigor de la LOPD, se prohibió la práctica habitual de este tipo de prestadores de servicios, los cuales cuando una deuda era satisfecha mantenían el “saldo 0” del deudor, datos considerado adverso, ya que cualquier asociado que consultase la situación de esa persona podía observar que anteriormente había sido deudor. En definitiva, el deudor que cumplió con su deuda, y conforme a lo establecido en la LOPD, el Responsable del fichero común, deberá excluir automáticamente de dicha lista dichos datos. No cabrá, por tanto, ni que la entidad acreedora notifique tales datos, ni que el responsable del fichero común (prestadora de servicios de información de solvencia patrimonial) los registre, trate y haga accesible a terceros.

CASO DE ESTUDIO

De las dos opciones posibles, sobre el trato de información de morosos, la más completa es la que proporciona la suscripción a una empresa de tratamiento de datos de solvencia como Asnef. Si la empresa crea un fichero de morosos propio, tendrá control total sobre el mismo, pero sólo conocerá las deudas que se han contraído contra la propia empresa. Sin embargo, si se convierte en cliente de Asnef, la cantidad de información que se obtiene en cada consulta será mayor, al obtenerse los datos aportados por los demás clientes.

Como ya se ha comentado anteriormente, es muy importante mostrar en el contrato de prestación de servicios que la empresa es cliente de Asnef. Aunque no es necesario el consentimiento del cliente para ceder sus datos en caso de impago, sí que hay que respetar el principio de información.

ADECUACIÓN A LAS TIC DE UNA EMPRESA DE TRANSPORTES



TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN

Autor del proyecto: Javier Sáez Moneo

Tutor del proyecto: Prof. Miguel Ángel Davara Rodríguez

Directores del Magíster:
Dr. Emilio S. Corchado Rodríguez
Dr. Álvaro Herrero Cosío

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

UNIVERSIDAD DE BURGOS

II Edición. Burgos, Julio 2010.

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

CONTENIDO

Contenido	88
Ilustraciones.....	93
1. Comercio Electrónico.....	94
Introducción	94
Normativa Vigente.....	94
Servicios de Información	95
Clasificación de los Servicios de Información.....	96
Obligaciones del Prestador de Servicios.....	97
Mera presencia	97
Contratación electrónica.....	98
Publicidad.....	98
Tipos de Comercio Electrónico	99
Comercio electrónico en función del medio	99
Comercio electrónico en función de los participantes	100
Seguridad en el Comercio Electrónico	100
Caso de Estudio	101
Necesidades de la Empresa en el Comercio Electrónico	101
Naturaleza de la Página Empresarial.....	102
Sistema de Seguridad para Comercio Electrónico	102
Obligaciones por prestación de servicios	104

Prototipos para Pagina Web	105
2. Firma Electrónica	111
Firma Electrónica.....	111
Normativa Vigente.....	113
Clases de Firma Electrónica	113
Validez Probatoria	114
Certificación.....	115
Proceso de Certificación.....	115
Participantes en el proceso de certificación	116
Ejemplo	116
Caso De Estudio.....	118
Obtener la Firma Digital	118
Obtener Certificado Digital.....	119
3. Protección Jurídica del Software.....	123
Introducción	123
Normativa Vigente.....	123
Protección	123
Derechos del Autor	125
derecho moral.....	125
Derechos de Explotación.....	125
Otros Derechos.....	126
Caso de Estudio	126

Necesidades Software de la empresa	126
Posibilidades de Protección del Software	127
Contrato de Protección en Escrow	127
Pasos para proteger el Software empresarial.....	128
4. Protección Jurídica de las Bases de Datos	129
Introducción	129
Normativa Vigente.....	129
Ambitos de Protección.....	130
Derecho Sui Generis	130
Caso de Estudio	131
Necesidades de Base de Datos de la Empresa.....	131
Contrato de Protección en Escrow y Derecho Sui Generis.....	131
Pasos para proteger la base de datos empresarial.....	131
5. Nombres de Dominio	133
Introducción	133
Tipos de nombre de dominio	133
Nombres de dominio de primer nivel.....	133
Nombres de dominio de segundo nivel.....	134
Nombres de dominio de tercer nivel	135
Entidades Gestoras de Nombres de Dominio	135
Cómo Registrar un Dominio.....	137
Conflictos de Nombres de Dominio	138

Caso Práctico	139
Obtener el Nombre de Dominio Empresarial.....	139
Resolución de Conflictos con el Nombre de Dominio.....	141
6. Contratación Informática.....	143
Introducción	143
Contenido del Contrato	143
Fases del Contrato.....	144
Tipos de Contrato Informático.....	144
Clasificación en base al objeto	144
Clasificación en base al negocio jurídico.....	145
Tipos Generales.....	146
Caso de Estudio	146
Necesidades de la Empresa	146
Contrato Informático – Hardware	146
Contrato Informático – Software.....	150
7. Administración y Fiscalidad Electrónica	155
Administración Electrónica	155
Marco legal en España.....	155
Fiscalidad Electrónica.....	156
Caso de Estudio	158
8. WEB 2.0.....	163
Introducción	163

Tecnologías	164
Empresa 2.0	165
Caso de Estudio	167
Pasos de adaptación a la empresa 2.0.....	167
Puesta en práctica	168

ILUSTRACIONES

Ilustración 1-1: Página principal de la Web	106
Ilustración 1-2: Detalle de Certificado en el Navegador	106
Ilustración 1-3: Información previa a la contratación	109
Ilustración 1-4: Información posterior a la contratación	110
Ilustración 2-1: Proceso de Firma Digital	113
Ilustración 2-2: Certificado en un Navegador	117
Ilustración 2-3: Detalles de un Certificado.....	117
Ilustración 2-4: Ejemplo de Certificado Digital de FNMT – Propiedades Generales.....	121
Ilustración 2-5: Ejemplo de Certificado Digital de FNMT – Propiedades del Certificado.	122
Ilustración 2-6: Ejemplo de Certificado Digital de FNMT – Autoridad de Certificación ..	122
Ilustración 7-1: Página web de la seguridad social	160
Ilustración 7-2: Página web del Ministerio de Hacienda.....	161
Ilustración 7-3: : Página web del Ministerio de Transporte	162

1. COMERCIO ELECTRÓNICO

INTRODUCCIÓN

El término “comercio electrónico” se refiere a la compra y venta de productos o de servicios a través de medios electrónicos, tales como Internet y otras redes informáticas. Este término ha evolucionado en el tiempo: originalmente se aplicaba a la realización de transacciones mediante medios electrónicos tales como el intercambio electrónico de datos, sin embargo a mediados de los años 90, debido a la llegada de Internet y la Web al público, comenzó a referirse principalmente a la venta de bienes y servicios a través de Internet, usando como forma de pago medios electrónicos, tales como las tarjetas de crédito.

En España, el Comercio Electrónico queda regulado por la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI).

“Es objeto de la presente Ley la regulación del régimen jurídico de los servicios de la sociedad de la información y de la contratación por vía electrónica, en lo referente a las obligaciones de los prestadores de servicios incluidos los que actúen como intermediarios en la transmisión de contenidos por las redes de telecomunicaciones, las comunicaciones comerciales por vía electrónica, la información previa y posterior a la celebración de contratos electrónicos, las condiciones relativas a su validez y eficacia y el régimen sancionador aplicable a los prestadores de servicios de la sociedad de la información.”

NORMATIVA VIGENTE

En España el comercio electrónico se rige por la Ley de Servicios de la Sociedad de la Información y del Comercio Electrónico (LSSI), también conocida como la ley 34/2002.

Esta ley afecta a todas aquellas personas o empresas que actúan desde España ya sean europeas o españolas, y a los que lo hagan en la Unión Europea o fuera de ella y cuyos destinatarios están en España.

Otras leyes que afectan tanto a nivel europeo como nacional son:

- Directiva 2000/31/CE del Parlamento Europeo y consejo del 8 de junio del 2000 sobre comercio electrónico.
- Ley 59/2003, de 19 de diciembre, de firma electrónica.

SERVICIOS DE INFORMACIÓN

El concepto de Servicio de Información es presentado por la propia LSSI:

"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:

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

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

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

- 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.
- Los servicios de radiodifusión televisiva (incluidos los servicios de cuasivídeo a la carta), contemplados en el artículo 3.a) de la Ley 25/1994, de 12 de julio, por la que se incorpora al ordenamiento jurídico español la Directiva 89/552/CEE, del Consejo, de 3 de Octubre, sobre la coordinación de determinadas disposiciones legales, reglamentarias y administrativas de los Estados miembros relativas al ejercicio de actividades de radiodifusión televisiva, o cualquier otra que la sustituya.
- Los servicios de radiodifusión sonora, y
- El teletexto televisivo y otros servicios equivalentes como las guías electrónicas de programas ofrecidas a través de las plataformas televisivas.

CLASIFICACIÓN DE LOS SERVICIOS DE INFORMACIÓN

La presencia en Internet de un prestador de servicios, puede clasificarse según la dirección de la comunicación que establece con el posible usuario de sus servicios. Si es unidireccional, partiendo del prestador, se trata de una presencia estática, mientras que si existe una posibilidad de diálogo, la presencia se considera dinámica:

Presencia Estática en Internet:

El prestador mantiene en Internet información sobre los servicios que ofrece, datos de contacto, productos, etc, pero de una forma que no implica interrelación con el cliente. De éste modo, el cliente puede obtener información del prestador, pero no podrá ponerse en contacto con él utilizando el mismo mecanismo.

Presencia Dinámica en Internet:

En éste caso, los prestadores mantienen una interrelación de diálogo con su posible cliente.

Presencia Dinámica Conversacional: El prestador ofrece una posibilidad de diálogo con el cliente, pero no la posibilidad de contratación a través del mismo medio.

Presencia Dinámica Contractual: El prestador ofrece la posibilidad de dialogar con el cliente, pudiendo concluir dicho diálogo con la contratación de un determinado servicio.

OBLIGACIONES DEL PRESTADOR DE SERVICIOS

MERA PRESENCIA

Éstas son las obligaciones generales de los prestadores de servicios:

- Inscribirse en un Registro Público, figurando el nombre de la empresa, un dominio ó dirección de internet, y cualquier cambio sobre los mismos.
- La empresa deberá informar permanente, fácil, directa y gratuitamente de :
 - Nombre, o denominación social.
 - Domicilio o dirección.
 - Dirección de correo electrónico.
 - Datos que permitan una comunicación directa y efectiva.
 - Datos de inscripción en el registro público.
 - Datos de autorización administrativa, si existe.
 - Si se ejerce una profesión regulada:
 - Datos del colegio profesional, y número de colegiado.
 - Título académico y lugar de expedición.
 - Normas profesionales aplicables.
 - Número de identificación fiscal.
 - Precio del producto, detallando si incluye impuestos, o gastos de envío.
 - Códigos de conducta a los que se adhiera.
 - Si se ejercen servicios de tarificación adicional:
 - Características del servicio a proporcionar.
 - Funciones de los programas informáticos que se descarguen.
 - Procedimiento para dar fin a la conexión de tarificación adicional
 - Procedimiento para restablecer el número de conexión previo a la tarificación adicional.

CONTRATACIÓN ELECTRÓNICA

Estas son las obligaciones de aquellos prestadores que realizan contratación por Internet. Son acumulativas a las anteriores obligaciones.

- Información previa a la contratación:
 - Qué trámites deben seguirse para celebrar el contrato.
 - Indicar si el prestador de servicios va a archivar el documento electrónico en que se formalice el contrato y si éste va a ser accesible.
 - Los medios técnicos que pone a su disposición para identificar y corregir errores en la introducción de los datos.
 - Lengua o lenguas en las que podrá formalizarse el contrato.
 - Condiciones generales del contrato.
- Información posterior a la contratación:
 - Un acuse de recibo que confirme la recepción de la aceptación del contrato, en las 24 horas posteriores.

PUBLICIDAD

Si una página ejerce servicios de publicidad a través de Internet, deberá cumplir las siguientes obligaciones expuestas en la Ley:

- Información exigida:
 - Comunicaciones comerciales por vía electrónica:
 - Serán claramente identificables.
 - Indicando quién es el emisor.
 - Incluyendo la palabra identificativa “publicidad” al comienzo del mensaje.
 - Promociones y concursos:
 - Se cumplirán las normas sobre ordenación del comercio.
 - Se indicarán las condiciones de acceso o participación clara e inequívocamente.
- Prohibiciones:
 - Queda prohibido realizar comunicaciones comerciales a través del correo electrónico o medios de comunicación electrónicos equivalentes.

- Excepciones a la prohibición:
 - Las comunicaciones comerciales han sido previamente solicitadas.
 - Las comunicaciones comerciales han sido expresamente autorizadas.
 - Existe una relación contractual previa.
- Respetar derechos de los destinatarios:
 - Revocación del consentimiento prestado.
 - Conocer electrónicamente los procedimientos de revocación.

TIPOS DE COMERCIO ELECTRÓNICO

Se pueden dar dos clasificaciones para el comercio electrónico, según si se clasifica atendiendo al medio utilizado, o si se clasifica atendiendo a los participantes

COMERCIO ELECTRÓNICO EN FUNCIÓN DEL MEDIO

Por Comercio electrónico indirecto se entiende todo aquel comercio en donde sólo la oferta y la solicitud de compra se va a realizar por medios de equipos electrónicos (online) y, sin embargo, la entrega del producto y/o el pago se va a realizar en el "mundo físico" (offline). En concreto es lo que equivale a la modalidad de contratación recogida en la Ley de Comercio Minorista, la llamada venta a distancia, donde la transmisión de oferta y aceptación se realiza por cualquier medio de comunicación a distancia, cualesquiera que sea su naturaleza y a través de un sistema de comunicación organizado por el vendedor. El típico ejemplo es una página web donde existe una serie de productos y servicios con un precio determinado, y el consumidor escoge el que mejor se adecua a sus necesidades, pero en el que la entrega y/o pago de ese producto se realiza fuera de la página web, en un lugar físico (offline).

Por Comercio electrónico directo se entiende todo aquel comercio en donde el proceso de compra y venta (oferta y aceptación del producto) se realiza por medio de equipos electrónicos (Internet, teléfonos móviles, PDA's, etc.), por ejemplo, la compra de un libro por Internet en el que el consumidor visualiza la oferta insertada en una página web y acepta la misma, pagando el precio ofertado y descargándose el libro en su propio equipo electrónico, es decir, toda la operativa de compra-venta se realiza desde la

página web del vendedor y desde el equipo electrónico del comprador. Dentro de este tipo de comercio electrónico se asimilarían las ventas a distancia recogidas en la Ley del Comercio Minorista, aunque no serán aplicables ciertos derechos que, por el contrario sí afectan al comercio electrónico indirecto. Esto sucede puesto que, la mayoría de servicios que se ofrecen en este comercio tienen excepciones de aplicación a la citada Ley.

COMERCIO ELECTRÓNICO EN FUNCIÓN DE LOS PARTICIPANTES

- B2B (Business to Business): se realiza entre dos o más empresas.
- B2C (Business to Consumer): operaciones comerciales llevadas a cabo por una empresa y dirigidas al consumidor final.
- B2A (Business to Administration): negocio de una empresa para la Administración Pública.
- B2E (Business to Employee): relación comercial de una empresa y los empleados de la misma.
- C2C (Consumer to Consumer): operación comercial llevada a cabo entre dos consumidores.
- P2P (Peer to Peer): negocio que no tiene clientes fijos. Se trata de la comunicación directa entre dos clientes a través de e-mail o internet. Se utiliza para el intercambio de información y/o archivos.

Todas estas relaciones son bidireccionales.

SEGURIDAD EN EL COMERCIO ELECTRÓNICO

Teniendo en cuenta que el comercio electrónico implica la transmisión de datos personales entre dos partes (que, posiblemente, se desconozcan), y que además, esos datos pueden afectar a la seguridad económica del receptor de los servicios, es necesario poner en funcionamiento sistemas de seguridad que permitan realizar transacciones seguras.

La encriptación es la codificación de la información, mediante la cual no se podrá acceder a los datos codificados sin la clave correspondiente. El usuario cuenta con un código privado personal y otro público para los destinatarios.

La tecnología de certificación digital se utiliza conjuntamente con la encriptación. Las más conocidas son el SSL y el SET.

SSL (Secure Sockets Layer) es un método de encriptación basado en el cifrado de datos en el origen de la comunicación, antes de enviar el mensaje, para asegurar autenticación y privacidad de la información entre extremos. Habitualmente, sólo el servidor es autenticado mientras que el cliente se mantiene sin autenticar.

SET (Secure Electronic Transaction) es un conjunto de especificaciones de seguridad desarrollado por Visa y Mastrecard, que asegura la confidencialidad e integridad de la información transmitida, asegurando que ni el emisor ni el receptor pueden negar su participación en la transacción.

Uno de los métodos más utilizados para la compra en internet es la firma electrónica, que es un conjunto de datos que identifica a sus usuarios. Utiliza tanto la encriptación como la tecnología de certificación digital.

CASO DE ESTUDIO

NECESIDADES DE LA EMPRESA EN EL COMERCIO ELECTRÓNICO

La empresa tiene la necesidad de permitir a los clientes contratar sus servicios a través de Internet, ya que la contratación in situ en las sucursales de la empresa limitaría demasiado su penetración en el mercado.

De este modo, la empresa ofrecerá servicios a la sociedad de la información a través de Internet, al realizarlos

- Mediante medios electrónicos ó informáticos
- A petición individual del cliente
- A distancia
- De manera onerosa

De este modo, la empresa va a necesitar una página empresarial que permita presentar a la empresa socialmente, permita el cierre de contratos con el cliente a través de medios telemáticos, y publicite su actividad en el mercado.

NATURALEZA DE LA PÁGINA EMPRESARIAL

Las necesidades de la empresa para su página son 3:

- Vender
- Informar
- Publicitar

La página de la empresa proveerá de servicios de información, estáticos y dinámicos. Mediante páginas estáticas, se presentará al usuario la empresa y los servicios que esta realiza. También se utilizarán páginas estáticas para presentar al usuario la información que la ley exige. La parte dinámica permitirá que el usuario, si lo desea, pueda contratar los servicios de la empresa que se mostraban en la parte estática.

SISTEMA DE SEGURIDAD PARA COMERCIO ELECTRÓNICO

Básicamente, la empresa necesitará emitir un Certificado Digital de Firma Electrónica para que los clientes tengan confianza en las relaciones de comercio electrónico que deseen mantener.

A parte de obtener dicho certificado, del que se hablará más adelante, es necesario establecer un sistema de seguridad. Como se ha comentado, actualmente se manejan SSL y SET principalmente. Analicemos a continuación las fortalezas y debilidades de ambos:

SET

- Protocolo de Seguridad.
- Es un protocolo multiparte. Permite que en la transacción participen varios implicados, asegurando la confidencialidad e integridad entre todos.
- Autentica al servidor al que se conecta el usuario para realizar la transacción.
- Autentica la identidad del comprador.
- Autentica a otros terceros que participen en la transacción, como bancos.
- Hace uso de firmas electrónicas. Importante factor para el no repudio y la integridad.

- Garantiza el no repudio, ya que todos los participantes hacen uso de la firma.
- Proporciona confidencialidad mediante la encriptación.
- Integridad garantizada a través de la firma electrónica. La firma electrónica se genera usando el mensaje y la clave privada. A través de la clave pública, se obtiene el mensaje, que deberá coincidir con el original.
- Inadecuado para transacciones de poco valor. Es un protocolo muy robusto, y por ello, muy pesado. Si es necesario usarlo mucho, se requerirán muchos recursos en el sistema.

SSL

- Protocolo de Seguridad.
- No es un protocolo multiparte, ya que sólo se autentica al servidor, no al resto de implicados.
- Autentica el servidor.
- No autentica al comprador.
- No autentica al banco del comprador.
- No usa firmas electrónicas. Sólo autentica al servidor, de modo que no se requiere firma para la autenticación.
- No garantiza el no repudio, al autenticarse sólo a una de las partes implicadas.
- Garantiza confidencialidad entre emisor y receptor mediante encriptación.
- No garantiza integridad. Al no usarse la firma electrónica, no hay ningún sistema de comprobación de la integridad.
- Apropiado para operaciones de poco valor. Es más rápido, pero menos seguro. Esto lo hace adecuado para operaciones habituales, de menor importancia.

Las principales diferencias entre SSL y SET son el concepto de protocolo multiparte, y uso de la firma electrónica, como manera de asegurar integridad, autenticidad y recepción.

La adecuación de un protocolo u otro es determinada por la situación en la que se requiere su uso. SSL es un protocolo sencillo y ligero, que es adecuado para asegurar una confidencialidad básica entre dos extremos, en las situaciones más habituales. SET es un protocolo más avanzado, y más pesado que certifica una mayor seguridad en la

transacción, lo que lo convierte en un protocolo más adecuado para operaciones más importantes y menos habituales.

Las necesidades de la empresa se adecuan más al uso de SSL, ya que las operaciones que los clientes soliciten, serán muchas de poco valor. Los clientes son la parte que necesita tener confianza en la empresa, ya que es esta la que recibirá un pago por la realización de un determinado servicio. Desde la parte de la empresa, esta puede confiar en la palabra del cliente: un envío no se llevará a cabo hasta que no se haya transferido el valor del mismo, o en caso de un envío contra reembolso, en caso de impago, el envío no se entrega.

OBLIGACIONES POR PRESTACIÓN DE SERVICIOS

La presencia en Internet de la página empresarial lo convierte en prestadora de servicios de información. Al permitir realizar contratación electrónica, la empresa dispone además de una presencia dinámica contractual. Y además, la empresa va a ejercer servicios de publicidad a través de Internet.

En éste caso, la empresa se inscribirá en el Registro Mercantil como “Transportes S.A.”, su dirección en Internet será “www.transportes.com”, y su dominio “transportes.com”.

En base a los puntos enunciados por la Ley, se recomienda que la web de la empresa contenga una página estática dedicada a mostrar todos los datos pertinentes expuestos en la lista, que sea enlazada desde cualquier otro punto de la web, pudiéndose utilizar un nombre como “datos de la empresa” ó “acerca de la empresa” para el documento. Se deberán mostrar todos los datos estáticos que definen a la empresa, como la razón social, domicilio, formas de contacto, códigos de conducta adheridos, etc. Otra opción es la creación de un pie de página que contenga todos estos datos, y que se muestre en todas las páginas de la web.

En el caso de los precios de los servicios, se puede optar por presentar los gastos de envío e impuestos como parte de una cuenta, debido a que el comprador puede que contrate varios. Dicha cuenta, se presentará con el importe total de las compras al usuario, antes de que acepte la compra, desglosando cada uno de los términos que la componen.

Para mostrar la información previa a la contratación, se recomienda crear páginas estáticas, similares a la creada para mostrar los datos de la empresa, en las que se muestren las condiciones generales de la contratación, y que sean enlazados desde cualquier punto de la web, para que el cliente pueda consultarlas en cualquier momento de su visita.

Para la información posterior a la contratación, se puede optar por presentar al comprador un documento con el resumen del pedido, a modo de factura. Esto asegura que la empresa ha recibido el pedido correctamente, y además, el comprador podrá mantener una copia del contrato para poder realizar posibles reclamaciones.

Para mostrar la información exigida en el ámbito publicitario, también se recomienda la creación de documentos estáticos donde se recoja la información comercial. Se pueden crear páginas donde mostrar ofertas, promociones, concursos, etc., según la empresa considere, siempre que se muestren claramente las condiciones de los mismos.

Las comunicaciones comerciales sólo se enviarán a clientes que las hayan aceptado previamente, o a personas dispuestas a su recepción. Se deberán identificar muy claramente como publicidad. Y se informará en el mensaje de cómo contactar con la empresa para poder revocar su envío.

En cuanto a los derechos de revocación, se deberá informar electrónicamente al usuario de su posible ejercicio, por ejemplo, mediante el sistema de documento estático dentro de la web de la empresa donde se explique el procedimiento, y se pondrá a su alcance un medio accesible, como email, o teléfono para que pueda ejercerlos.

PROTOTIPOS PARA PAGINA WEB

A continuación se presentan varios prototipos de página web en los que se tratará de plasmar los requisitos mínimos que la ley exige en el ámbito del comercio electrónico.

La página principal de la empresa da acceso a todas las secciones. Puede dar acceso a usuarios registrados, o a usuarios que sólo quieren consultar tarifas. En la zona inferior de la página, se mostrarán los datos de la empresa.

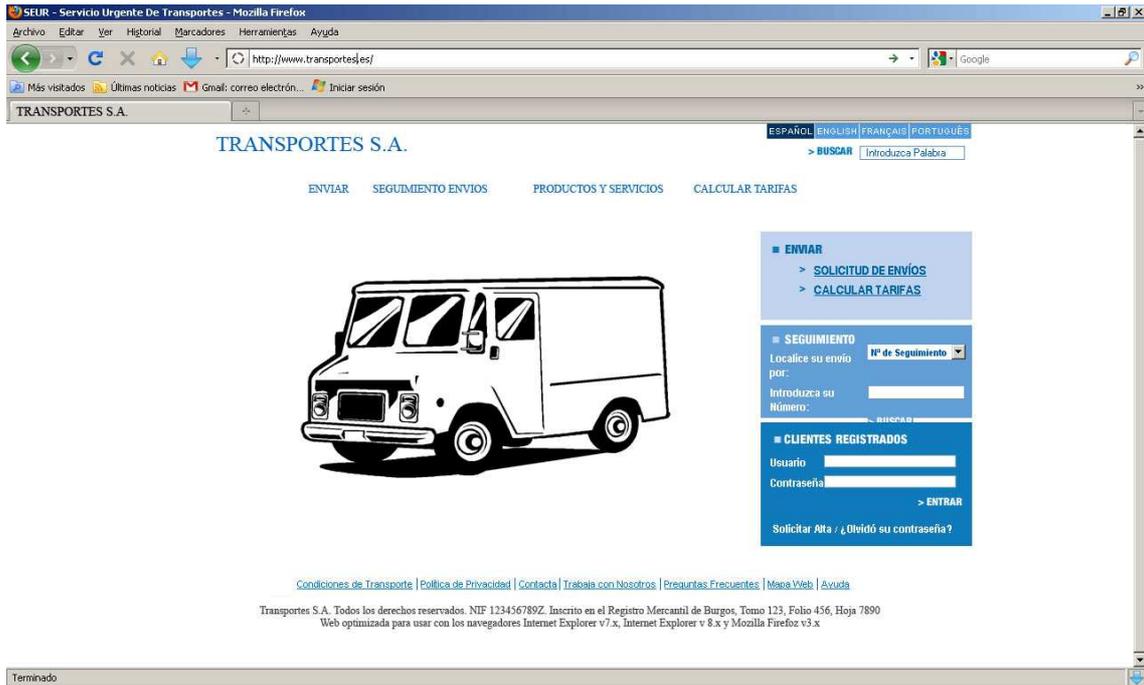


Ilustración 1-1: Página principal de la Web

La seguridad en la contratación se consigue a través del uso de usuarios registrados, y de firma electrónica. Para que un usuario pueda contratar un servicio, deberá registrarse primero en la página web. Durante todo el proceso de registro y contratación, el navegador deberá hacer uso del sistema de autenticación que la página web proveerá, mediante certificado electrónico:



Ilustración 1-2: Detalle de Certificado en el Navegador

La información previa a la contratación, se mostrará en una página estática, a la que se accede desde la opción de condiciones de transporte:



TRANSPORTES S.A.

Condiciones de Transporte

Las presentes condiciones serán de aplicación para los envíos contratados en defecto de pactos o condiciones específicas derivadas de la singularidad de cada producto o servicio. Consultar página de tarifas vigentes relativas a cada servicio o producto.

Los datos contractuales sobre designación de mercancía, denominación, domicilio y población del destinatario y remitente, son facilitados por éste y bajo su responsabilidad, no siendo comprobados por la Agencia, salvo grave riesgo inminente u orden de la autoridad.

La prestación de los servicios se efectuará de lunes a viernes, salvo sábados mañana para aquellos envíos en los que se contraten los servicios complementarios Entrega en Sábado y/o Recogida en Sábado. En el cómputo temporal se excluyen los días festivos en la localidad de destino, y el sábado correspondiente a Semana Santa.

GARANTÍA DE ENTREGA: En caso de incumplimiento del plazo de entrega contractualmente pactado según el servicio contratado, la indemnización a abonar consistirá en la devolución de los portes satisfechos por el cliente. No se considerará incumplimiento de plazo de entrega el causado por ausencia del destinatario, cambio del domicilio, consignatario o dirección desconocidos, impago de portes, suplidos o reembolsos, cierre por vacaciones, entregas fuera de plazo en segundo intento de entrega, causas de fuerza mayor o caso fortuito u otras no imputables a la Agencia. Quedan excluidas de esta garantía las mercancías enviadas "a recogerán" en el domicilio o almacenes de la Agencia TRANSPORTES S.A. de destino. Asimismo, se exime de responsabilidad en los casos de incumplimiento de plazo de entrega en envíos a Canarias, Baleares, Ceuta y Melilla por causas ajenas a la Agencia TRANSPORTES S.A. (retrasos de compañías aéreas, marítimas, transportistas, carga y/o descarga, etc.).

Se hace constar la posibilidad de suscribir en el presente seguro suplementario que cubra, con declaración de valor real, los daños que las mercancías puedan sufrir hasta el valor declarado de las mismas. El coste de este seguro a repercutir en factura será del 1,25% del valor declarado (mínimo 2,71€). En este caso no se aplicará el recargo dispuesto en el apartado anterior. De no contratarse este seguro, serán de aplicación EN TODO CASO, los límites de responsabilidad contractual antes reseñados. Lo anterior no se verá alterado por la necesaria presentación de documentos en que, para realizar el tránsito de la mercancía, venga referido su valor o contenido, el cual será considerado como declaración extracontractual y a los solos efectos de gestión ante terceros.

El remitente declara conocer y aceptar las condiciones y plazos de entrega del servicio contratado, fijación, repercusión, y cuantía del precio del transporte contratado, y demás gastos, según ejemplar de tarifas vigentes de la compañía, conocidas, facilitadas y a disposición del mismo. Para las recogidas y entregas fuera de la capital de provincia se cobrarán las cantidades que según cada servicio, se indican en el libro de tarifas.

La Agencia de Transporte se reserva en todo momento la facultad de aceptar un paquete y consecuentemente prestar un servicio por insuficiencia de embalaje para el transporte, parecerle anómalo, o por otras causas extrañas del encargo. En caso de rechazo por insuficiencia de embalaje e insistencia por parte del remitente en el envío, la Agencia de Transportes no responderá de daños o averías que pudiesen producirse en las mercancías, bastando a tal efecto la firma del cliente en el espacio correspondiente del albarán. Queda excluido el transporte de paquetes y objetos cuyo contenido sea contrario a la Ley o cuyo transporte esté sometido a requisitos o disposiciones especiales (armas, fondos o efectos, materiales tóxicos, inflamables o peligrosos, explosivos, etc.), siendo de responsabilidad única y exclusiva del remitente, el cual exonera expresamente a la Agencia de cualquier responsabilidad al respecto. Asimismo, queda excluido el transporte de mercancías cuya longitud supere la medida de tres metros.

La entrega de la mercancía se realizará en el domicilio designado por el remitente, salvo por reiterada ausencia del destinatario o que por su peso, volumen o características funcionales del inmueble no permitan a una persona normal la citada realización, en cuyo caso, previo aviso se efectuará a puerta de calle o en la central TRANSPORTES S.A. de destino. En caso de ausencia del destinatario se dejará aviso del intento de entrega, así como de la forma de acordar la misma. (Se cobrará el importe del Servicio Complementario Gestión por aquellos servicios que excedan de la mera recogida y entrega de la mercancía o que conlleven un trámite inusual). La no entrega de la mercancía transportada por ausencia o rehúse del destinatario, deficiencia de sus datos o impago de las cantidades derivadas del porte realizado, será responsabilidad de remitente, quien vendrá obligado a soportar, a su cargo, todos los gastos de dicha incidencia, incluidos, en su caso, los gastos de depósito, el precio, la prima de reembolso y demás gastos del porte de la mercancía producidos en su retorno a origen o posteriores entregas, y la repercusión del seguro correspondiente.

Será requisito necesario para proceder a la entrega de la mercancía la firma del albarán de entrega por el destinatario. En caso de negativa del destinatario a firmar el albarán la Agencia quedará eximida de toda responsabilidad.

Los PLAZOS para efectuar la RECLAMACIÓN POR DAÑOS en la mercancía serán de VEINTICUATRO HORAS desde la entrega si los daños no son apreciables exteriormente, o EN EL MISMO ACTO DE LA ENTREGA, y precisamente en el documento contractual, si se pueden apreciar exteriormente. Lo anterior, salvo envíos con origen o destino en Portugal, en que el plazo será de ocho días desde la entrega. LAS ACCIONES derivadas del contrato de transporte PRESCRIBEN AL AÑO.

Transportes S.A. se reserva el derecho a revisar las tarifas del presente documento, en base a las variaciones en el precio de los proveedores de transporte (compañías aéreas, marítimas, transportistas, etc.). Además, se repercutirá mensualmente un cargo por combustible en base a los precios medios mensuales (impuestos incluidos) del combustible diesel para los envíos marítimos o terrestres con origen o destino España y Portugal, y en base a los precios medios mensuales del barril de petróleo Brent, para los envíos aéreos con origen y destino Canarias, Baleares y Melilla. Se podrán consultar las posibles variaciones mensuales de los

cargos por combustible en www.Transportes.com

El remitente designa al transportista como agente plenamente autorizado para gestionar el despacho de aduanas cuando éste sea necesario, así como para designar a un Agente de Aduanas para tal fin. El remitente está obligado a suministrar toda la documentación e información que sea necesaria para el cumplimiento de las formalidades aduaneras, paraduaneras y de seguridad con anterioridad a la aceptación del envío. El transportista no está obligada a examinar o comprobar si la referida documentación e información es exacta o suficiente. El remitente se compromete a indemnizar al transportista por cualquier sanción, gasto o coste en que pudiera incurrir ésta en el despacho aduanero por cualquier causa imputable a aquél.

[Condiciones de Transporte](#) | [Política de Privacidad](#) | [Contacta](#) | [Trabaja con Nosotros](#) | [Preguntas Frecuentes](#) | [Mapa Web](#) | [Ayuda](#)

Transportes S.A. Todos los derechos reservados. NIF 123456789Z. Inscrito en el Registro Mercantil de Burgos, Tomo 123, Folio 456, Hoja 7890
Web optimizada para usar con los navegadores Internet Explorer v7.x, Internet Explorer v 8.x y Mozilla Firefox v3.x

Terminado

Ilustración 1-3: Información previa a la contratación

La información posterior a la contratación, se mostrará en una página después de la realización del envío, a modo de factura.

TRANSPORTES S.A.

Detalles del Envío

Fecha 10/10/10

Cliente: Sr.X

Modo de pago: Contrareembolso

Producto	Importe	Importe con IVA
Transporte Urgente Burgos-Caceres Código 12345A	15 €	17,4 €
Envío Certificado Burgos-Albacete Código 23456B	20 €	23,2 €
PARCIAL	35 €	40,6 €
DESCUENTO	3 €	3,48 €
TOTAL	32 €	37,12 €

[Condiciones de Transporte](#) | [Política de Privacidad](#) | [Contacta](#) | [Trabaja con Nosotros](#) | [Frecuentes Frecuentes](#) | [Mapa Web](#) | [Ayuda](#)

Transportes S.A. Todos los derechos reservados. NIF 123456789Z. Inscrito en el Registro Mercantil de Burgos, Tomo 123, Folio 456, Hoja 7890
Web optimizada para usar con los navegadores Internet Explorer v7.x, Internet Explorer v 8.x y Mozilla Firefox v3.x

Terminado

Ilustración 1-4: Información posterior a la contratación

2. FIRMA ELECTRÓNICA

FIRMA ELECTRÓNICA

La firma digital de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido y, seguidamente, aplicar el algoritmo de firma (en el que se emplea una clave privada) al resultado de la operación anterior, generando la firma electrónica o digital. El software de firma digital debe además efectuar varias validaciones, entre las cuales podemos mencionar:

- Vigencia del certificado digital del firmante,
- Revocación del certificado digital del firmante (puede ser por OCSP o CRL),
- Inclusión de sello de tiempo.

La función hash es un algoritmo matemático que permite calcular un valor resumen de los datos a ser firmados digitalmente. Funciona en una sola dirección, es decir, no es posible, a partir del valor resumen, calcular los datos originales. Cuando la entrada es un documento, el resultado de la función es un número que identifica inequívocamente al texto. Si se adjunta este número al texto, el destinatario puede aplicar de nuevo la función y comprobar su resultado con el que ha recibido. No obstante, este tipo de operaciones no están pensadas para que las lleve a cabo el usuario, sino que se utiliza software que automatiza tanto la función de calcular el valor hash como su verificación posterior.

Para que sea de utilidad, una función hash debe satisfacer dos importantes requisitos:

- debe ser difícil encontrar dos documentos cuyo valor para la función hash sea idéntico.
- dado uno de estos valores, debe ser imposible producir un documento con sentido que dé lugar a ese hash.

Existen funciones hash específicamente diseñadas para satisfacer estas dos importantes propiedades. SHA y MD5 son dos ejemplos de este tipo de algoritmos.

Algunos sistemas de cifrado de clave pública se pueden usar para firmar documentos. El firmante cifra el hash calculado de un documento con su clave privada y cualquiera que quiera comprobar la firma y ver el documento, no tiene más que usar la clave pública del firmante para descifrar el hash, y comprobar que es el que corresponde al documento.

Un algoritmo efectivo debe hacer uso de un sistema de clave pública para cifrar sólo la firma. En particular, el valor "hash" se cifra mediante el uso de la clave privada del firmante, de modo que cualquiera pueda comprobar la firma usando la clave pública correspondiente. El documento firmado se puede enviar usando cualquier otro algoritmo de cifrado, o incluso ninguno si es un documento público. Si el documento se modifica, la comprobación de la firma fallará, pero esto es precisamente lo que la verificación se supone que debe descubrir.

Firma básica. Incluye el resultado de operación de hash y clave privada, identificando los algoritmos utilizados y el certificado asociado a la clave privada del firmante. A su vez puede ser "attached" o "detached", "enveloped" y "enveloping"

Firma fechada. A la firma básica se añade un sello de tiempo calculado a partir del hash del documento firmado por una TSA (Time Stamping Authority)

Firma validada o firma completa. A la firma fechada se añade información sobre la validez del certificado procedente de una consulta de CRL o de OCSP realizada a la Autoridad de Certificación.

La firma completa libera al receptor de la firma del problema de ubicar al Prestador de Servicios de Certificación y determinar los procedimientos de validación disponibles.

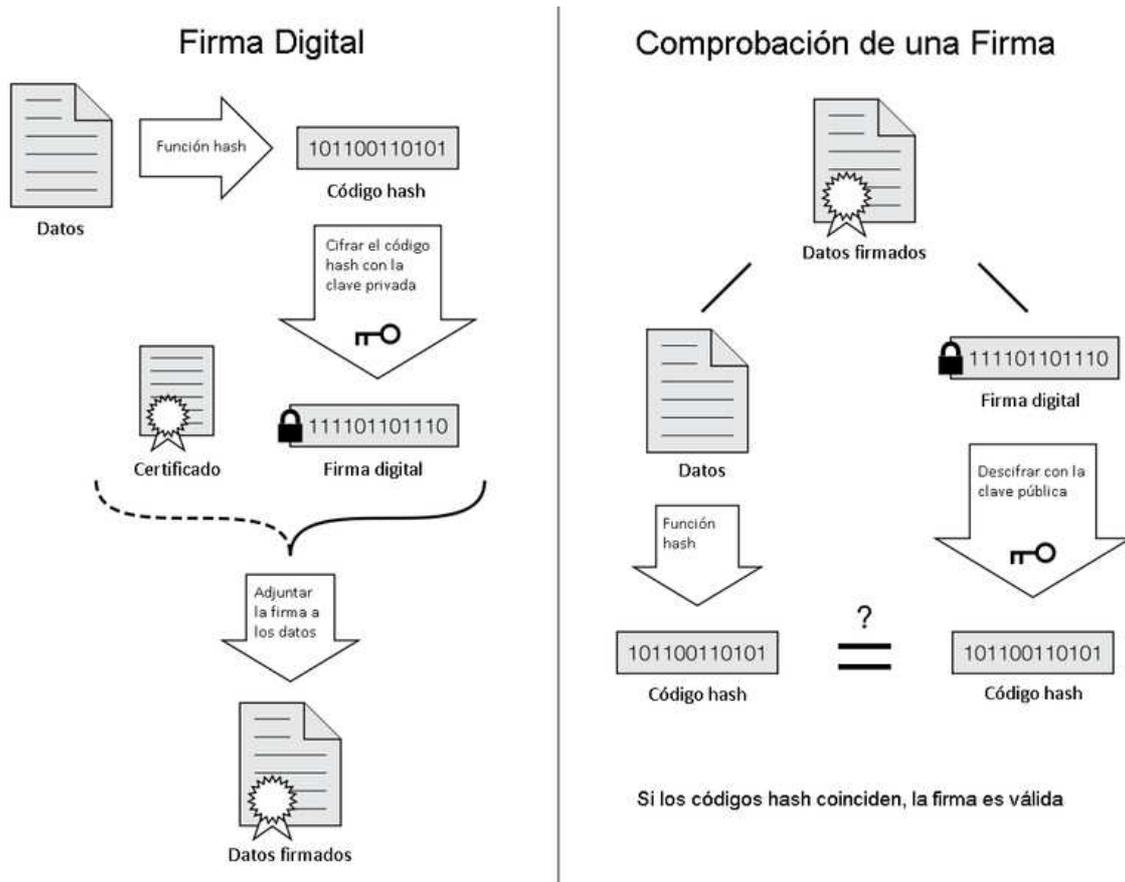


Ilustración 2-1: Proceso de Firma Digital

NORMATIVA VIGENTE

En España existe la Ley 59/2003, de Firma electrónica (LFE). Esta Ley regula la firma electrónica, su eficacia jurídica y la prestación de servicios de certificación.

En ese sentido la Directiva 1999/93/CE sienta un marco común para la firma electrónica que se concretó con la transposición de la Directiva a las diferentes legislaciones nacionales de los países miembros.

CLASES DE FIRMA ELECTRÓNICA

En el tercer artículo de la LFE, los tres primeros puntos establecen tres niveles de firma:

1. La **firma electrónica** es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

La principal finalidad de la firma electrónica sencilla es la identificación de las partes.

2. La **firma electrónica avanzada** es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

En éste nivel, al concepto de identificación de las partes, se añaden los siguientes conceptos

- autenticación del contenido: sólo el firmante posee los medios, bajo exclusivo control, para realizar la firma, asegurando que ha sido quien firmó el documento.
- integridad del contenido: la firma electrónica forma parte activa del proceso de comprobación de la corrección del mensaje enviado y recibido.
- no repudio: se describe como vinculada al firmante de manera única, es decir, del modo que asegura la identidad del firmante, asegura que éste no repudiará su autoría.

3. Se considera **firma electrónica reconocida** la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. 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 éste caso, los medios para asegurar la autenticación del firmante, no los pone él mismo, sino una entidad certificadora externa, que autentique de manera imparcial al firmante. Además, el cuarto punto da a la firma electrónica reconocida la misma validez que la firma manuscrita.

VALIDEZ PROBATORIA

La normativa de uso de la firma electrónica queda recogida en la Ley 59/2003, conocida como LFE, que sustituye a la anterior norma, el Real Decreto Ley 14/1999.

En ésta Ley, se define la firma electrónica como *“el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.”*

Además hay que definir las cinco funciones principales de la firma electrónica: identificación de las partes, autenticación del contenido, integridad del contenido, confidencialidad, no repudio.

La validez probatoria de la firma queda determinada por el tipo de firma escogida.

El primer tipo simplemente identifica a quien envía el mensaje, pero no asegura esa identidad.

El segundo tipo, comprende las funciones principales de la firma electrónica, como son la identificación, autenticidad del contenido, integridad del contenido, y el no repudio del mensaje. En éste caso sí que existe una validez probatoria al asegurar la identificación del firmante.

El tercer tipo, asegura todo lo que el segundo, añadiendo que la autenticación del firmante queda atestiguada por una entidad certificadora. En éste tipo existe validez probatoria, y además tiene el mismo valor que la firma escrita.

CERTIFICACIÓN

PROCESO DE CERTIFICACIÓN

Un certificado digital es un documento electrónico que vincula una clave pública a una organización ó particular. Los certificados son emitidos por un tercero de confianza, el Prestador de Servicios de Certificación (PSC). El PSC será el encargado de verificar que el remitente es quien dice ser, y que la clave que participa en el certificado, efectivamente le pertenece. Éste certificado participa posteriormente en un sistema de cifrado de clave asimétrica.

Un certificado emitido por una entidad de certificación autorizada, además de estar firmado digitalmente por ésta, debe contener por lo menos lo siguiente:

- Nombre, dirección y domicilio del suscriptor.
- Identificación del suscriptor nombrado en el certificado.
- El nombre, la dirección y el lugar donde realiza actividades la entidad de certificación.
- La clave pública del usuario.
- La metodología para verificar la firma digital del suscriptor impuesta en el mensaje de datos.
- El número de serie del certificado.
- Fecha de emisión y expiración del certificado.

PARTICIPANTES EN EL PROCESO DE CERTIFICACIÓN

Entidad prestadora de servicios de certificación (PSC): es una entidad de confianza, responsable de emitir y revocar los certificados utilizados en la firma electrónica, para la cual se emplea criptografía de clave pública. La confianza sobre dicha entidad deberá ser aceptada por ambas partes.

El remitente: Solicita al PSC la creación del certificado, a partir de su clave pública. Éste certificado le servirá para ser identificable, de manera segura, por parte del receptor del mensaje.

El destinatario: A través del certificado generado por el PSC, el destinatario obtiene la clave pública del remitente, con la certeza de que el remitente es quien dice ser. Así puede descifrar los mensajes que éste le manda, y responderle con otros mensajes cifrados con total seguridad.

EJEMPLO

A continuación se muestra la captura de la información sobre un certificado que muestra un navegador, donde se identificará a los participantes.

En el ejemplo, un usuario quiere acceder a su correo, utilizando el protocolo https (hiper text transmission protocole secure), que utiliza SSL como sistema de cifrado, y en el que una entidad PSC ha emitido el certificado:

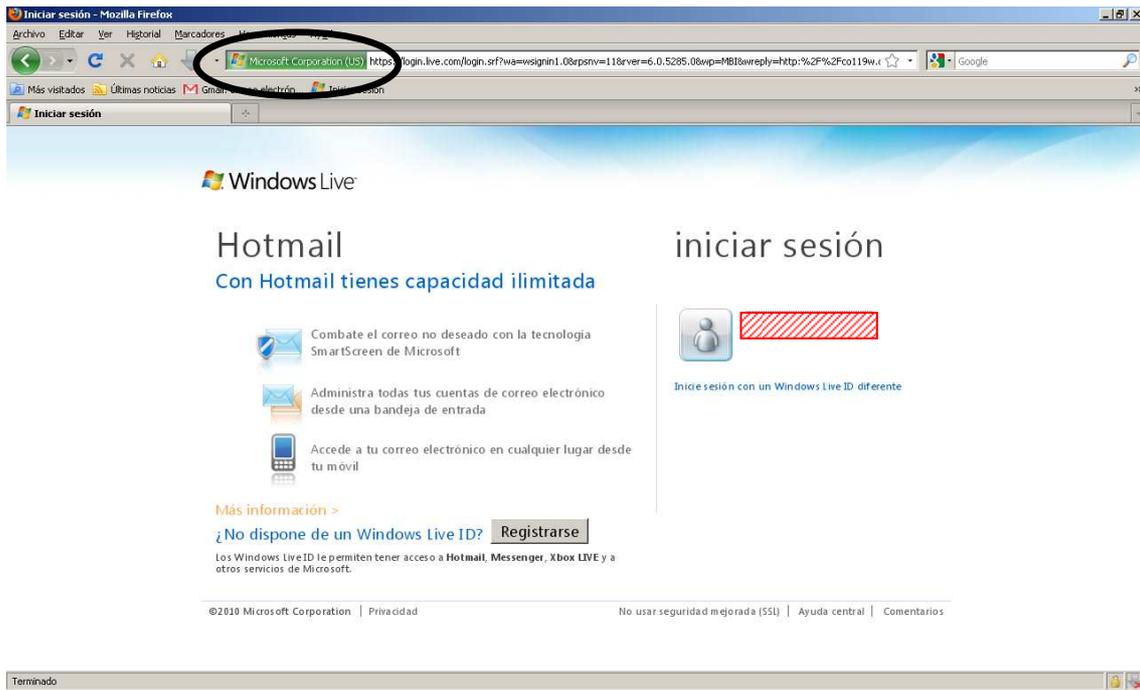


Ilustración 2-2: Certificado en un Navegador

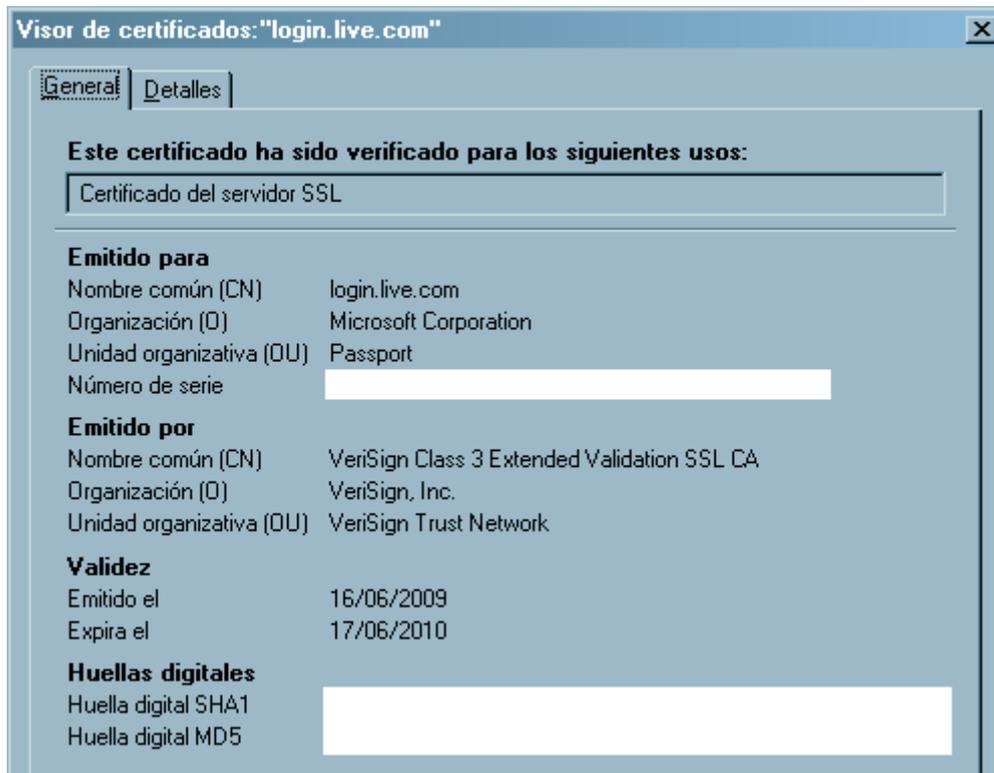


Ilustración 2-3: Detalles de un Certificado

Se identifica claramente a los participantes:

- El PSC es VeriSign Inc., emisor del certificado, y que tanto emisor como receptor del mensaje aceptan como tercero de confianza en la certificación.
- El remitente de la conexión segura es Microsoft Corporation, que ofrece los servicios de correo electrónico.
- El receptor es el navegador (en éste caso, Firefox), en manos de un usuario.

CASO DE ESTUDIO

Según se ha presentado, al necesitar una total confianza del usuario hacia la empresa, la firma electrónica que se necesita es de tipo reconocido. De este modo, la empresa necesita crear su firma digital, y posteriormente, certificarla.

En España, el tercero de confianza, encargado de emitir los Certificados Digitales es la Fábrica Nacional de Moneda y Timbre (FNMT). A través de la Plataforma Ceres, permite que los usuarios puedan conseguir su propio certificado digital acreditado.

OBTENER LA FIRMA DIGITAL

El proceso de firma es el siguiente:

1. El usuario prepara el mensaje a enviar.
2. El usuario utiliza una función hash segura para producir un resumen del mensaje.
3. El remitente encripta el resumen con su clave privada. La clave privada es aplicada al texto del resumen usando un algoritmo matemático. La firma digital consiste en la encriptación del resumen.
4. El remitente une su firma digital a los datos.
5. El remitente envía electrónicamente la firma digital y el mensaje original al destinatario. El mensaje puede estar encriptado, pero esto es independiente del proceso de firma.
6. El destinatario usa la clave pública del remitente para verificar la firma digital, es decir para desencriptar el resumen adosado al mensaje.

7. El destinatario realiza un resumen del mensaje utilizando la misma función resumen segura.
8. El destinatario compara los dos resúmenes. Si los dos son exactamente iguales el destinatario sabe que los datos no han sido alterados desde que fueron firmados.

Cuando el destinatario recibe el mensaje, lo descifra con su clave privada y pasa a comprobar la firma. Para ello, hace dos operaciones: por un lado averigua la clave pública del remitente y descifra con ella el resumen que calculó y cifró el remitente. Por otro lado, el destinatario calcula el resumen del mensaje recibido repitiendo el procedimiento que usó el remitente. Si los dos resúmenes (el del remitente descifrado y el calculado ahora por el destinatario) coinciden la firma se considera válida y el destinatario puede estar seguro de la integridad del mensaje: si el mensaje hubiera sido alterado a su paso por la red, el resumen calculado por el destinatario no coincidiría con el original calculado por el remitente.

Además, el hecho de que el resumen original se ha descifrado con la clave pública del remitente prueba que sólo él pudo cifrarlo con su clave privada. Así el destinatario está seguro de la procedencia del mensaje (autenticación del origen) y, llegado el caso, el remitente no podría negar haberlo enviado (no repudio) ya que sólo él conoce su clave secreta.

Los inconvenientes de este sistema son la lentitud de los algoritmos de clave asimétrica (típicamente varia veces más lentos que los de clave simétrica) y la necesidad de las autoridades de certificación ya mencionadas.

OBTENER CERTIFICADO DIGITAL

Cuando la empresa actúa como prestador de servicios, es necesario mantener un certificado digital para asegurar la comunicación con el cliente, y que este tenga confianza en la empresa. El Certificado que se obtenga deberá ser instalado en el servidor SSL de la empresa que contiene la página empresarial.

El proceso se divide en tres apartados que deben realizarse en el orden señalado en la página de Ceres de la Fábrica Nacional de Moneda y Timbre.

1 - Solicitud vía internet del Certificado.

Al final de este proceso se obtendrá un código que se deberá presentar para acreditar la identidad del solicitante.

2 - Acreditación de la identidad en una Oficina de Registro.

Una vez que se ha solicitado un certificado de persona jurídica (o de entidad sin personalidad jurídica) para el ámbito tributario, hay que dirigirse a las Oficinas de Registro de la Agencia Tributaria. El registro de usuario es presencial, para aumentar el nivel de seguridad del sistema.

3 - Descarga del Certificado de Usuario.

Una vez realizado el registro presencial y con la ayuda del código obtenido en el paso 1, se podrá descargar vía Internet el Certificado Digital.

Ahora que ya se dispone del Certificado Digital (un fichero *.pfx), se deberá instalar en el servidor al que los clientes se conectan utilizando HTTPS.

Visto desde un explorador, el Certificado Digital será similar al siguiente (en el ejemplo se ha utilizado el certificado de catastro, que también ha sido emitido por la FNMT):

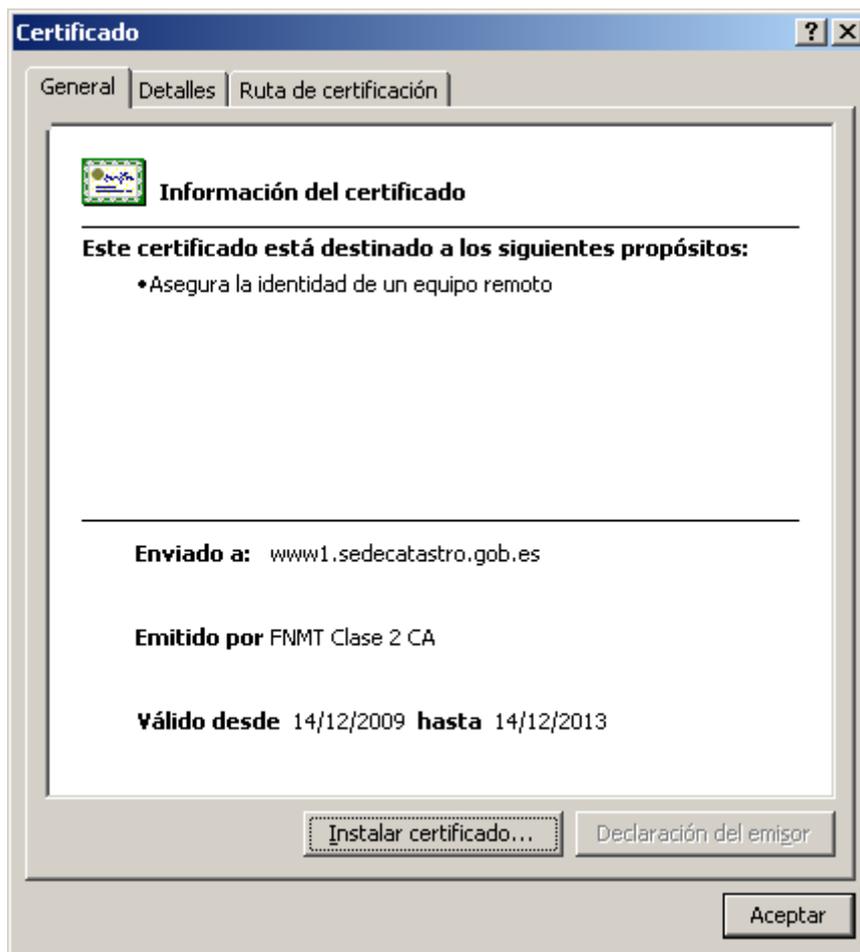


Ilustración 2-4: Ejemplo de Certificado Digital de FNMT – Propiedades Generales

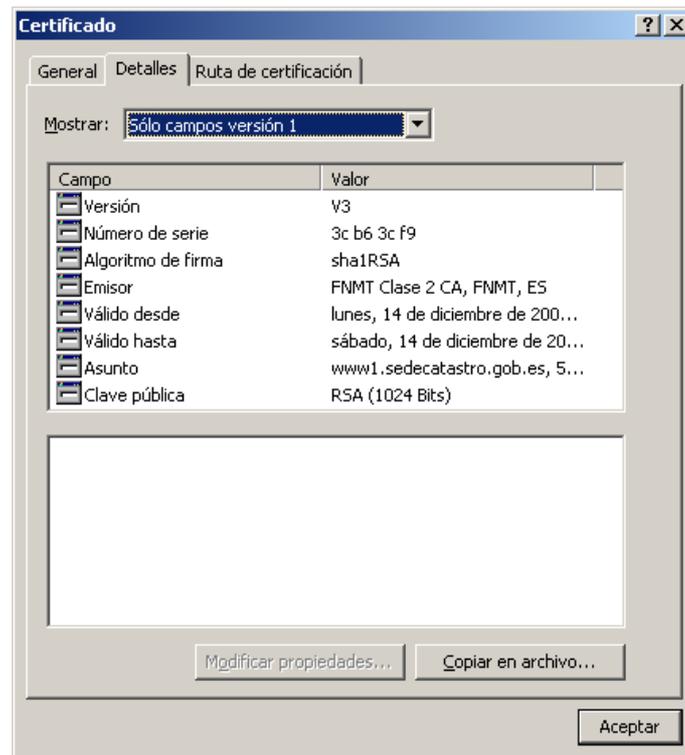


Ilustración 2-5: Ejemplo de Certificado Digital de FNMT – Propiedades del Certificado

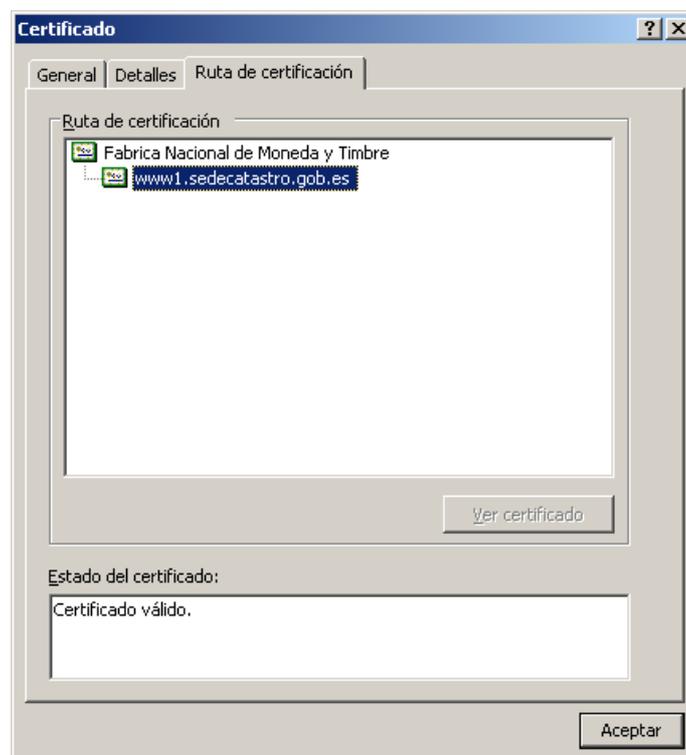


Ilustración 2-6: Ejemplo de Certificado Digital de FNMT – Autoridad de Certificación

3. PROTECCIÓN JURÍDICA DEL SOFTWARE

INTRODUCCIÓN

En España se conoce como derechos de la propiedad intelectual a lo que los ordenamientos jurídicos denominan derecho de autor. La vigente Ley de Propiedad Intelectual (LPI) data de 11 de noviembre de 1987. Tras algunas reformas y la aprobación de varias leyes especiales, en 1996 se llevó a cabo, mediante el Real Decreto Legislativo 1/1996, una refundición que ya ha sido objeto de modificaciones posteriores por la Ley 5/1998 y las Leyes 19 y 23/2006. Una característica fundamental de dicho Ordenamiento es que se configura al derecho de autor como único, pero integrado por varias facultades; así: de reproducción, comunicación, distribución, transformación... Una propiedad esencial del derecho de autor en España es que tiene por objeto un bien inmaterial: la obra.

NORMATIVA VIGENTE

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

Ley 19/2006, de 5 de junio, por la que se amplían los medios de tutela de los derechos de propiedad intelectual e industrial y se establecen normas procesales para facilitar la aplicación de diversos reglamentos comunitarios.

Ley 23/2006, de 7 de julio, por la que se modifica el texto refundido de la Ley de Propiedad Intelectual, aprobado por el Real Decreto Legislativo 1/1996, de 12 de abril.

La Directiva 2001/29/CE del Parlamento Europeo y el Consejo del 22 de mayo de 2001 sobre la armonización de ciertos aspectos del derecho de autor y derechos relacionados en la sociedad de la información de la Unión Europea.

PROTECCIÓN

El objeto de la protección de la LPI es el programa de ordenador, entendiéndose como toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas en un sistema

informático para realizar una función. Se incluye también su documentación preparatoria. La documentación técnica y los manuales de uso de un programa gozarán de la misma protección que los programas de ordenador. El programa de ordenador será protegido únicamente si fuese original, en el sentido de ser una creación intelectual propia de su autor.

Será considerado autor del programa de ordenador la persona o grupo de personas naturales que lo hayan creado, o la persona jurídica que sea contemplada como titular de los derechos de autor. Si el autor es una persona natural, la duración de los derechos de explotación de un programa de ordenador será de 70 años tras su fallecimiento. Cuando se trate de una persona jurídica la duración de los derechos se computará desde el día 1 de enero del año siguiente al de la divulgación del programa.

No se necesitará autorización del titular para la reproducción o transformación de un programa de ordenador incluido la corrección de errores, cuando dichos actos sean necesarios para la utilización del mismo por parte del usuario legítimo, con arreglo a su finalidad propuesta.

La realización de una copia de seguridad por parte de quien tiene derecho a utilizar el programa no podrá impedirse por contrato en cuanto resulte necesaria para dicha utilización. El usuario legítimo de la copia de un programa estará facultado para observar, estudiar o verificar su funcionamiento, sin autorización previa del titular, con el fin de determinar las ideas y principios implícitos en cualquier elemento del programa, siempre que lo haga durante cualquiera de las operaciones de carga, visualización, ejecución, transmisión o almacenamiento del programa que tiene derecho a hacer.

El autor, salvo pacto en contrario, no podrá oponerse a que el cesionario titular de derechos de explotación realice o autorice la realización de versiones sucesivas de su programa ni de programas derivados del mismo.

DERECHOS DEL AUTOR

La LPI asegura dos tipos de derechos para el autor: moral y patrimonial.

DERECHO MORAL.

Corresponden al autor los siguientes derechos irrenunciables e inalienables:

1. Decidir si su obra ha de ser divulgada y en qué forma.
2. Determinar si tal divulgación ha de hacerse con su nombre, bajo seudónimo o signo, o anónimamente.
3. Exigir el reconocimiento de su condición de autor de la obra.
4. Exigir el respeto a la integridad de la obra e impedir cualquier deformación, modificación, alteración o atentado contra ella que suponga perjuicio a sus legítimos intereses o menoscabo a su reputación.
5. Modificar la obra respetando los derechos adquiridos por terceros y las exigencias de protección de bienes de interés cultural.
6. Retirar la obra del comercio, por cambio de sus convicciones intelectuales o morales, previa indemnización de daños y perjuicios a los titulares de derechos de explotación.
7. Si, posteriormente, el autor decide reemprender la explotación de su obra deberá ofrecer preferentemente los correspondientes derechos al anterior titular de los mismos y en condiciones razonablemente similares a las originarias.
8. Acceder al ejemplar único o raro de la obra, cuando se halle en poder de otro, a fin de ejercitar el derecho de divulgación o cualquier otro que le corresponda. Este derecho no permitirá exigir el desplazamiento de la obra y el acceso a la misma se llevará a efecto en el lugar y forma que ocasionen menos incomodidades al poseedor, al que se indemnizará, en su caso, por los daños y perjuicios que se le causen.

DERECHOS DE EXPLOTACIÓN

1. Derecho de reproducción: Se entiende por reproducción la fijación directa o indirecta, provisional o permanente, por cualquier medio y en cualquier forma, de toda la obra o de parte de ella, que permita su comunicación o la obtención de copias.

2. Derecho de distribución: Se entiende por distribución la puesta a disposición del público del original o de las copias de la obra, en un soporte tangible, mediante su venta, alquiler, préstamo o de cualquier otra forma.
3. Derecho de comunicación pública: Se entenderá por comunicación pública todo acto por el cual una pluralidad de personas pueda tener acceso a la obra sin previa distribución de ejemplares a cada una de ellas.
4. Derecho de transformación: La transformación de una obra comprende su traducción, adaptación y cualquier otra modificación en su forma de la que se derive una obra diferente.

OTROS DERECHOS

1. Compensación equitativa por copia privada. La reproducción realizada exclusivamente para uso privado originará una compensación dirigida a indemnizar los derechos de propiedad intelectual que se dejaran de percibir por razón de la expresada reproducción. Este derecho será irrenunciable para los autores y los artistas, intérpretes o ejecutantes

CASO DE ESTUDIO

NECESIDADES SOFTWARE DE LA EMPRESA

La empresa va a necesitar que se desarrolle un software empresarial específico para que los trabajadores puedan usarlo para cumplir sus cometidos de la empresa. Aunque no entraremos en detalles de requisitos funcionales del mismo, a grandes rasgos, el software deberá poder controlar la parte del desempeño de las funciones de la empresa (la gestión y control de los envíos) y permitirá gestionar los recursos humanos de la misma.

En el capítulo de la contratación electrónica entraremos en los detalles del tipo de contrato que se utilizará para que se desarrolle dicho software, pero de momento consideremos que el mismo, será propiedad de la empresa.

Puesto que el software es propiedad de Transportes S.A., es la propia empresa quien se deberá encargar de dar la protección legal pertinente al mismo.

POSIBILIDADES DE PROTECCIÓN DEL SOFTWARE

En Europa, en materia de patente industrial se excluye la patente de los “programas de ordenador” pero sólo cuando sean reclamadas “como tales”. Por este motivo a la hora de tratar los aspectos de protección legal, habrá que referirse a la propiedad intelectual.

Los derechos de autor nacen desde el mismo momento de la creación de la obra, el problema nace cuándo se debe probar la autoría de la obra.

Existen diversos mecanismos para generar pruebas de autoría respecto a los programas de ordenador. Ninguno de estos mecanismos son constitutivos de derechos, sino que simplemente son una “prueba” y por lo tanto son “declarativos de derechos de autor”:

- **REGISTRO GENERAL DE LA PROPIEDAD INTELECTUAL:** las ventajas son que ya es telemático, por lo que puede hacerse desde internet, el problema es nuevamente los plazos de 6 meses de resolución así como que las categorías de registro pueden ser muy estrictas y obligar a realizar varios registros para un mismo programa (por ejemplo, registrar por un lado software y por otro la base de datos)
- **AUTOENVIO DE UN SOBRE LACRADO CON EL CONTENIDO DE LA CREACION INTELECTUAL.** El sobre lacrado mantiene una fecha de fin de desarrollo de la creación intelectual, y constituye una prueba del momento en el que el software ya estaba desarrollado y en manos de la empresa. Tiene el problema de que es fácilmente manipulable, y su autenticidad puede ser cuestionada.
- **DEPÓSITO NOTARIAL:** suele llevar costes más elevados y un mantenimiento, pero sin embargo es la mejor forma de asegurar la autoría de un desarrollo desde el primer momento. Si se establece un contrato con el notario, se le puede enviar desde la primera línea de código que se escriba.

CONTRATO DE PROTECCIÓN EN ESCROW

El contrato de Escrow, o de depósito de código fuente, consiste en depositar el código fuente de un programa ante un Notario o tercera parte confiable, condicionando su acceso en virtud de que se cumplan una serie de condiciones:

- Es un acto mediante el que el notario da fe pública de la fecha de entrega o depósito de una obra protegida por la propiedad intelectual recogida en cualquier formato.
- Cualquier obra protegida por derechos de propiedad industrial e intelectual.
- Permite reconstituir prueba documental de autoría de una obra única, perfectamente válida en procedimientos judiciales.

Esta forma de protección se caracteriza por la inmediatez, la confidencialidad, la seguridad jurídica y técnica tanto para el desarrollador como para sus clientes y potenciales inversores. Además, mediante este sistema, se podrá proteger cualquier creación intelectual reconocida en la legislación española.

Es importante remarcar que el contrato de Escrow no interfiere con el contrato de desarrollo del software por parte de un tercero. Se puede hacer constar o indicar en el contrato de desarrollo, pero ambos no tienen implicaciones entre sí

PASOS PARA PROTEGER EL SOFTWARE EMPRESARIAL

1. Realizar el análisis funcional de requisitos del sistema.
2. Contratar un desarrollo a medida (se verá con detalle en el capítulo de contratación informática), asegurando en el contrato que la autoría del desarrollo será para la empresa.
3. Realizar un contrato de protección en escrow sobre el software desarrollado.
4. Solicitar un registro de propiedad intelectual, que actúa como salvaguarda del acta notarial. Debido a que puede representar una esperar de meses, se recomienda registrar el software primero ante notario.

4. PROTECCIÓN JURÍDICA DE LAS BASES DE DATOS

INTRODUCCIÓN

La misión de las bases de datos es el almacenamiento y tratamiento de la información dentro de una empresa. El tratamiento de dicha información, si es lo suficientemente bueno, puede representar una ventaja competitiva frente a otras empresas del sector, lo cual a su vez puede hacerlo deseado por esas otras empresas para implementarlo.

La base de datos contiene los datos “en bruto” que propiamente almacena, y que la empresa utiliza para el desarrollo de su actividad, pero son la estructura y los métodos que implementa para el tratamiento y la extracción lo que la proporcionan un valor añadido.

De éste modo, es necesario separar la protección de los datos de la base respecto de la protección de la base en sí misma. Para los datos se aplicará la normativa de la LOPD, mientras que la base, entendida como un desarrollo cuya finalidad es tratar los datos, se aplicará una normativa diferente.

Las bases de datos se protegen como obras de creación intelectual, al ser necesario el desarrollo informático de los mecanismos de almacenamiento y de recuperación. Además, al igual que en el caso del desarrollo software, al desarrollo de bases de datos le acompaña una serie de documentos y un posible mantenimiento y explotación.

NORMATIVA VIGENTE

La normativa específica de la protección de bases de datos queda también recogida dentro del Real Decreto 1/1996 sobre propiedad intelectual.

La Ley 5/1998, de 6 de marzo, de incorporación al Derecho Español de la Directiva 96/9/CE, del Parlamento Europeo y del Consejo, de 11 de marzo de 1996, sobre la protección jurídica de las bases de datos. Mediante esta Ley, el estado español se incorpora a un marco de protección para las bases de datos a nivel europeo.

AMBITOS DE PROTECCIÓN

El desarrollo de bases de datos queda defendido por las dos normas antes expuestas. De éste modo, una base de datos es protegida desde dos ámbitos:

- Desde el ámbito de la propiedad intelectual, aplicable como desarrollo informático que la propia base de datos es. Tenemos en cuenta que la base de datos incorpora sus mecanismos informatizados de recuperación y almacenamiento de datos, junto con su documentación, y sus contratos.
- Desde el ámbito propio de la construcción de la base de datos, que protege la inversión que ha sido necesaria para dicha construcción

DERECHO SUI GENERIS

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

Mediante este derecho, el fabricante de una base de datos, puede prohibir la extracción y/o reutilización de la totalidad o de una parte sustancial del contenido de ésta, evaluada cualitativa o cuantitativamente, siempre que la obtención, la verificación o la presentación de dicho contenido representen una inversión sustancial desde el punto de vista cuantitativo o cualitativo. Este derecho podrá transferirse, cederse o darse en licencia contractual.

No obstante, no estarán autorizadas la extracción y/o reutilización repetidas o sistemáticas de partes no sustanciales del contenido de una base de datos que supongan actos contrarios a una explotación normal de dicha base o que causen un perjuicio injustificado a los intereses legítimos del fabricante de la base.

Este derecho se aplicará con independencia de la posibilidad de que dicha base de datos o su contenido esté protegida por el derecho de autor o por otros derechos, sin perjuicio de los derechos existentes sobre su contenido.

CASO DE ESTUDIO

NECESIDADES DE BASE DE DATOS DE LA EMPRESA

Las necesidades de la empresa en el ámbito de las bases de datos, son similares al campo del software. La empresa va a necesitar un desarrollo específico de base de datos en base a necesidades específicas del negocio que realiza. Su desarrollo se contratará a una empresa especializada, que igual que con el software cederá su autoría y propiedad a Transportes S.A.

Sin embargo, las bases de datos, como se ha visto, tienen el problema añadido de que no sólo hay que proteger su diseño y estructura (que se podría proteger mediante escrow), sino que también hay que proteger su contenido, y la inversión que representan.

CONTRATO DE PROTECCIÓN EN ESCROW Y DERECHO SUI GENERIS

Las bases de datos, como se ha comentado tienen una doble vertiente de protección: a parte del desarrollo informático que se defiende mediante la LPI, también se ha de proteger la inversión sustancial que ha representado construir la base de datos, mediante el derecho sui generis.

Así, por un lado, tendremos un contrato similar al que se utilizó en el desarrollo del apartado de software (o incluso el mismo, si la base de datos forma parte del conjunto global de desarrollo a medida), en el que mediante el depósito del código fuente y las documentaciones, un notario atestiguará su propiedad a la empresa.

Sin embargo, en este caso, también es necesario que de manera imparcial, la inversión de recursos sea valorada, para establecer el valor cuantitativo que representa la base de datos, y que será defendida mediante el derecho sui generis.

PASOS PARA PROTEGER LA BASE DE DATOS EMPRESARIAL

Las primeras etapas son las de un programa informático, ya que se desea proteger los mecanismos de utilización de la base de datos:

1. Realizar el análisis funcional de requisitos del sistema.

2. Contratar un desarrollo a medida, asegurando en el contrato que la autoría del desarrollo será para la empresa.
3. Realizar un contrato de protección en escrow sobre el software desarrollado.
4. Solicitar un registro de propiedad intelectual, que actúa como salvaguarda del acta notarial. Debido a que puede representar una esperar de meses, se recomienda registrar el software primero ante notario.

Se añade la protección sui generis:

5. Un perito informático deberá determinar el valor cuantitativo de la base de datos, en cuanto a estructura y valor del contenido. El acta que expida deberá ser llevada ante el notario, para asociarla al desarrollo construido.

Ahora, se añade la protección de los datos:

6. Registro en la AEPD de los ficheros de la BD que contienen datos personales.

5. NOMBRES DE DOMINIO

INTRODUCCIÓN

En Internet, para comunicar dos máquinas, se utilizan las direcciones IP, que identifican las máquinas en los extremos de una comunicación. Las direcciones IP están compuestas por cuatro números separados por puntos. Originalmente, dichos números se introducían manualmente para comunicar con una máquina remota, pero con el crecimiento del número de direcciones en Internet pueden resultar difíciles de recordar. Es en éste punto cuando nace el Servicio de Nombres de Dominio (DNS), que permite asociar las IP a nombres fácilmente comprensibles y memorizables.

TIPOS DE NOMBRE DE DOMINIO

Para organizar los nombres de dominio, se establece una jerarquía de niveles. El nombre de dominio se escribe “en una línea”, y los niveles dentro del mismo se separan por puntos, siendo el de mayor importancia el que se sitúa más a la derecha

NOMBRES DE DOMINIO DE PRIMER NIVEL

Conocidos como TLD (top level domain), existen dos grupos: genéricos y de país

Nombres de dominio de primer nivel genéricos

Son nombres fijos que clasifican la finalidad de la página. Pueden tener un uso libre si cualquiera puede solicitarlos, o restringido, si es necesario algún tipo de acreditación.

- .com, originalmente dedicado para compañías, su uso es libre actualmente.
- .edu, para organizaciones educativas superiores. Uso restringido.
- .biz, para fines comerciales. Uso libre.
- .coop, para cooperativas. Uso restringido.
- .aero, para la industria aeronáutica. Uso restringido.
- .gov y .gob, para Gobierno y Entidades Públicas. Uso restringido.
- .info, para Información. Uso libre.
- .int, para Entidades Internacionales, organizaciones como la ONU. Uso restringido.

- .mil, para el Departamento de Defensa de los Estados Unidos (Único país con dominio de primer nivel para el ejército). Uso restringido.
- .museum, para los Museos. Uso restringido.
- .name, para Nombres de personas. Se puede usar tanto en primer como segundo nivel.
- .net, para Infraestructura de red originalmente. En la actualidad tiene un mismo uso que .com. Uso libre.
- .org, para organizaciones, aunque tampoco de manera estricta. Uso libre.
- .pro, para profesionales con una titulación universitaria. Uso restringido.
- .tel, para servicios de comunicación por internet. Uso restringido.
- .travel, para páginas de la industria de viajes y turismo. Uso restringido.

Nombres de dominio de primer nivel de código de país

Se utilizan dos letras para determinar el país en el que se ubica la página:

- .es, para servicios de España
- .eu, la región de Europa
- .ru, para servicios de Rusia
- .fr, para servicios de Francia
- .uk, para Reino Unido
- Etc...

NOMBRES DE DOMINIO DE SEGUNDO NIVEL

También conocidos como SLD (Second Level Domain), son los que habitualmente se equiparan al nombre de marca o empresa.

Estos nombres de dominio los debe registrar el dueño, y son los que más conflicto pueden generar al estar directamente relacionados con temas de propiedad intelectual.

El nombre de dominio de segundo nivel llega a tener valor comercial, al ser identificativo de la empresa, y se guarda como propiedad intelectual. Las entidades gestoras de nombres de segundo nivel, encargadas de su registro y consulta son Iann, Esnic y WhoIs.

En caso de un conflicto de nombres, se da preferencia según el orden de llegada, a menos que se pueda demostrar mala fe en el registro, en cuyo caso habría un delito contra la propiedad intelectual.

NOMBRES DE DOMINIO DE TERCER NIVEL

La finalidad de este grupo es similar al segundo nivel, pero en este caso, se sitúan bajo dos dominios anteriores, creados con la finalidad de ubicar a los solicitantes en un espacio adecuado a su actividad y de que los usuarios puedan distinguirla de manera intuitiva. En España, existe 5 prefijos para nombres de dominio de tercer nivel

- .com.es
- .nom.es
- .org.es
- .gob.es
- .edu.es

El significado del segundo dominio es el mismo que se vio en el primer apartado del ejercicio.

ENTIDADES GESTORAS DE NOMBRES DE DOMINIO

El ICANN es la Corporación para la Asignación de Nombres de Dominio en Internet. Esta organización tiene como principales objetivos administrar los recursos presentes en Internet, y establecer los criterios generales que deben seguirse a la hora de asignar los nombres de dominio, esto es, es la organización encargada del registro de los nombres de dominio y trata de armonizarlos y coordinarse con los registros delegados de cada país.

Asimismo, esta entidad dicta qué política debe aplicar la OMPI (Organización Mundial de la Propiedad Intelectual) en la resolución de los conflictos entre nombres de dominio. El sistema que se emplea para la resolución de estos incidentes es el arbitraje internacional.

Por su parte, la entidad ES-NIC lleva a cabo la asignación, gestión y administración de los nombres de dominio de Primer Nivel en Internet en España, bajo el distintivo ".es"; se trata, por tanto, del registro delegado de la ICANN para la asignación de nombres de dominio de Primer Nivel en España.

La OMPI son las siglas de la Organización Mundial de la Propiedad Intelectual encargada de aplicar las directrices facilitadas por la ICANN para la resolución de las controversias que puedan suscitarse en relación a los nombres de dominio.

Generalmente, estas cuestiones se dirimen dentro de un procedimiento ágil y relativamente rápido, cuyo coste es inferior a la resolución judicial del conflicto, y que concluye bien con la anulación, bien con la transferencia del dominio.

Para solucionar estas cuestiones, la anterior no es la última instancia a la que acudir, siempre es posible igualmente plantear el problema ante la vía judicial.

CÓMO REGISTRAR UN DOMINIO

El procedimiento es el siguiente:

1. Compra del dominio.
 - 1.1. Elegir un dominio.
 - 1.2. Verificar la disponibilidad del nombre de dominio deseado en algún registrador (empresa autorizada para el registro de dominios)
 - 1.3. Ingresar los datos personales.
 - 1.4. Elegir la cantidad de tiempo que el dominio permanecerá registrado.
 - 1.5. Pagar el dominio, normalmente con tarjeta de crédito (o también por transferencia bancaria)
2. Una vez comprado, el ahora dueño del dominio (registrante) debe configurarlo como URL a la cual redireccionar, IP del servidor al que resolver mediante DNS, servidor DNS usado, etc.
3. El dueño del dominio debe esperar un tiempo para que el dominio sea reconocido en todos los servidores de Internet. Para los dominios .com y .net la demora es entre 4 y 8 horas, y para otros es generalmente entre 24 y 48 horas. En ese período:
 - 3.1. El registrador contacta con InterNIC y realiza el proceso de forma transparente para el registrante.
 - 3.2. Se avisa al registrante que el dominio fue registrado.
4. El nuevo dominio funciona, y resuelve a la IP apropiada en el servidor DNS usado, pero no en el resto de servidores DNS del mundo. Poco a poco se va propagando el cambio al resto de servidores (propagación DNS). Como cada uno tiene distintos tiempos de actualización y parámetros de caché distintos, pasan varias horas (es difícil predecir cuántas) hasta que todos los servidores DNS del mundo conocen cómo hacer la resolución del dominio.
5. La página ya es accesible mediante un nombre de dominio desde cualquier computadora.

CONFLICTOS DE NOMBRES DE DOMINIO

Los conflictos relativos a los nombres de dominio pueden sistematizarse de la siguiente manera:

a) Conflictos entre particulares, que pueden fundamentarse, bien en la discusión entre dos partes para la obtención de un mismo dominio, o bien en el registro de un dominio que corresponda con la marca o el nombre comercial de una u otra parte.

Estas cuestiones pueden resolverse en virtud de la legislación aplicable al derecho infringido: el derecho de propiedad intelectual, el derecho de la competencia y el derecho de las marcas. Sobre este punto, la nueva Ley de Marcas prevé expresamente la protección de las marcas en Internet, estableciendo en su articulado que el titular del derecho conferido por el registro de una marca pueda prohibir a un tercero que utilice la marca en redes de comunicación telemáticas y como nombre de dominio.

La solución de este caso pasa por ejercitar acciones judiciales contra el usurpador, impugnándose un dominio registrado, o la solicitud de registro, alegando la infracción de un precepto de la normativa mencionada.

Por otro lado, la ICANN ha elaborado un sistema de arbitraje on line que permite solucionar los pleitos en un tiempo medio de 45 días y por un coste de entre 1.000 y 3.000 €. Las quejas se pueden presentar ante el Centro de Arbitraje de la OMPI.

Para poder presentar una denuncia ante la OMPI en materia de usurpación de dominios, lo que puede hacerse a través de Internet, hay que acreditar que se es titular de la marca y que el nombre de dominio demandado es idéntico o similar al propio, además de que se ha obtenido de mala fe y que está siendo utilizado.

b) Los conflictos pueden presentar también una vertiente pública: la denegación del registro de un determinado nombre de dominio por parte de la institución registradora y la responsabilidad de las entidades que llevan a cabo los registros de los nombres de dominio. En este caso, la impugnación podría dirigirse contra el registrador en virtud de las normas de registro establecidas por las instituciones registradoras.

CASO PRÁCTICO

OBTENER EL NOMBRE DE DOMINIO EMPRESARIAL

Para elegir un buen nombre de dominio hay que tener en cuenta lo siguiente:

- En lo posible, que el nombre sea corto, lo que va a hacer que sea más fácil de memorizar.
- Que no se preste a confusiones ortográficas, ya que puede dar mala imagen de empresa.
- De ser posible que el nombre esté relacionado al nombre del negocio o actividad y si es una keyword (palabra clave que las personas utilizan en los buscadores para encontrar el tipo de producto o servicio que ofrece), o un mnemónico, mucho mejor. También es recomendable utilizar el nombre de su empresa o su marca, si estas son conocidas.
- Elegir de preferencia un dominio con extensión .com, es el más usado y casi todos los usuarios están acostumbrados a asociarlo por defecto a cualquier dominio.

En cuanto a las reglas sobre los caracteres permitidos para la composición de un nombre de dominio debe tener en cuenta lo siguiente:

- Son permitidos todos los caracteres del alfabeto inglés: de la A hasta la Z.
- Son permitidos los dígitos del 0 al 9.
- Es permitido el guión: (-) pero no puede ser ni el primero ni el último carácter del nombre.
- El uso de mayúsculas y minúsculas es indiferente.
- El número máximo de caracteres permitidos es 67 incluyendo su extensión (.com, .net, .org, .biz, .info, .name).
- En cuanto al uso de caracteres especiales, como los acentuados y la (ñ) que son utilizados en el idioma español, también ahora son permitidos por algunos registradores, sin embargo no han tenido buena acogida, primero porque las personas ya se acostumbraron a no utilizarlos y segundo porque para visualizar una dirección con un carácter especial, es necesario instalar un plugin (pequeño arreglo), al menos en el caso de los que utilizan Internet Explorer, que es la mayoría y que muy pocos están dispuestos a hacer..

En cuanto al tipo de dominio a elegir, hay 2 opciones:

- Dominios universales, genéricos de segundo nivel, del tipo (.com, .net, .org, .biz, .info, .name), es recomendable el uso de un .com por ser el estándar. El precio de un dominio (.com) es 15 euros, incluidos impuestos, por año.
- Dominios territoriales, geográficos o de tercer nivel, los del tipo (.com.es, .es, .net.es, etc). En éste caso, el precio es 30 euros, incluidos impuestos, por año.

Tenidas en cuenta estas 3 premisas, se intentará registrar el dominio **transportes.com**. Este nombre cumple las premisas de ser un nombre fácil de recordar, que referencia el nombre de la empresa y utiliza el .com, que es más fácil de asociar, y más barato.

Antes de registrar el Dominio se deben realizar varias comprobaciones:

- Comprobar que el Dominio no está registrado por otra persona o entidad. Esta comprobación se puede realizar en cualquier empresa que preste servicios de Registro de Dominios.
- En caso de que esté libre el dominio que se ha decidido registrar, hay que asegurar que el nombre elegido no pertenece a ninguna marca registrada ya que podría provocar una demanda judicial por apropiación de una marca registrada.

Una vez comprobadas las premisas anteriores, se procede al registro del dominio.

Para ello se elige la empresa donde realizar la compra del dominio. Preferentemente, se elegirá una empresa que pertenezca al país de la empresa titular del dominio, ya que, aunque cueste unos Euros (o dólares) más caros, garantiza que el servicio técnico hable en el idioma local y que los datos personales asociados estén legalmente protegidos por la legislación oportuna.

Así, considerando que el nombre de dominio **transportes.com** está disponible para su uso, y que no genera ningún conflicto, la empresa puede proceder a su registro.

RESOLUCIÓN DE CONFLICTOS CON EL NOMBRE DE DOMINIO

Imaginemos que ante el nombre de dominio anteriormente registrado, que en el momento del registro se consideró oportuno, adecuado y correcto, surge un conflicto con otra entidad o individuo que considera que dicho nombre le perjudica de algún modo, o por el contrario, que inicia acciones que perjudican a la empresa.

La parte demandante se encargará de formalizar la demanda, interponiendo una demanda ante el otro titular que ha registrado un nombre de dominio, que legítimamente puede usar la empresa.

Los pasos para interponer la demanda son:

- 1°. Comprobar el nombre de dominio en ICANN, que es la organización responsable de asignar las direcciones del protocolo IP, de los identificadores de protocolo, de las funciones de gestión del sistema de dominio y de la administración del sistema de servidores raíz.
- 2°. Determinar a quién se está demandando. Esto se puede comprobar a través de los servicios de WhoIs. En éste caso, es un dominio territorial, pero aparte del registrador, conoceríamos el país donde registró, en qué fecha, en qué servidor de nombres, etc.
Con ésta información, sabremos a qué dirección remitir la demanda, y en qué idioma redactarla.
- 3°. Redacción de la demanda, en el idioma del demandado, entregando 3 copias para: OMPI, que es el agente registrador, WIPO, que es el organismo de arbitraje, y el demandado. En la demanda se debe hacer constar el hecho denunciado y el motivo por el que el demandante considera que existe una mala fe por parte del demandado.
- 4°. Se presenta la demanda ante OMPI, se elige el número de árbitros, y se paga.
- 5°. OMPI se encargará de revisar la demanda, y si se acepta, de hacerla llegar al demandado.

Es importante remarcar, que la aportación de la carga de pruebas depende exclusivamente del demandante, actuando la organización como órgano de arbitrio únicamente.

Las costas del trámite recaen siempre en el demandante, salvo que el demandado solicite que se establezca una comisión de tres árbitros, en cuyo caso se encargará de pagar la diferencia.

Una vez que se interpone la demanda, queda esperar a la contestación del demandado. El demandado dispondrá de 20 días para contestar con sus alegaciones, intentado demostrar que no ha habido mala fe por su parte.

Si las partes en conflicto no han nombrado a estas alturas del proceso a un grupo de tres expertos para realizar el análisis, OMPI se encargará de nombrar un único árbitro en un plazo máximo de 5 días. Una vez que se disponga de árbitro, se fijará una fecha para anunciar la resolución sobre el litigio.

Contra la resolución administrativa se puede interponer una demanda por la jurisprudencia ordinaria, que paralizarían la ejecución de la resolución, con el fin de facilitar el desarrollo de la nueva demanda.

6. CONTRATACIÓN INFORMÁTICA

INTRODUCCIÓN

La contratación informática implica la contratación de bienes informáticos ó servicios informáticos. Se entiende por bien informático cualquier elemento que forme parte de un sistema informático, ya sea hardware, software ó datos. Servicio informático se entenderá como servicio que sirve de apoyo a la actividad informática del sistema.

Es importante no confundir la contratación informática con la electrónica, ya que esta última hace referencia al medio utilizado para realizar la contratación, en lugar de referenciar el objeto como hace la primera

CONTENIDO DEL CONTRATO

Las clausulas mínimas recomendables para un contrato informático son:

- Obligaciones de las partes, claras y concisas.
- El deber de asesoramiento e información.
- El cumplimiento del plazo.
- La formación del usuario.
- Prohibición de subarrendar.
- Sustitución del equipo.
- Definición de términos o conceptos oscuros.
- El mantenimiento preventivo.
- Cláusulas de garantía.
- Anexos
 - Especificaciones del sistema a contratar.
 - Especificaciones de los programas a desarrollar.
 - Pruebas de aceptación.
 - Resultados a obtener.

FASES DEL CONTRATO

El proceso de contratación informática, implica un tiempo dilatado, debido a la complejidad que puede representar el sistema que se está contratando. Esto da lugar a tres fases largas y bien diferenciadas: la fase precontractual (o de formación del objeto), la fase contractual, y la fase de desarrollo y ejecución.

TIPOS DE CONTRATO INFORMÁTICO

La clasificación de los tipos de contrato informático se realiza principalmente en base a dos grupos:

- La clasificación en base al **objeto del contrato**, separando las características especiales de los elementos sobre los que pueden versar los contratos.
- La clasificación en base al **negocio jurídico**, separando la finalidad del propósito con el que se realiza la contratación.

CLASIFICACIÓN EN BASE AL OBJETO

- Contrato de Hardware: Incluye todo aquello que forma parte física del equipo, ya sea de manera directa, o auxiliar.
- Contrato de Software: en este caso hay que diferenciar entre el software de utilidad y de sistema. La diferencia se sitúa en que la naturaleza del desarrollo será la que marque quién especifica las características del mismo. En el caso del software de utilidad, el usuario deberá especificar en el contrato las características y funcionalidades que el software desarrollado deberá cumplir, mientras que en el software del sistema, son el desarrollador y el fabricante los que crean las características del producto.
- Contrato de instalación llave en mano: Incluyen el hardware y el software y determinados servicios de mantenimiento y formación, que se deberán indicar.
- Contrato de servicios auxiliares: Contratación de servicios complementarios al hardware o software contratado, como el mantenimiento del producto y la formación de los usuarios

CLASIFICACIÓN EN BASE AL NEGOCIO JURÍDICO

- Contrato de venta: El vendedor se compromete a entregar una determinada cosa por un precio estipulado en el contrato, por acuerdo entre las partes.
- Contrato de arrendamiento financiero: En éste tipo de contrato participan tres partes: vendedor, comprador y una entidad financiera independiente. La entidad se encarga de ayudar en la financiación al comprador, pero a cambio conserva la propiedad del objeto que se vende hasta que se paga por completo.
- Contrato de alquiler: El arrendador permite al usuario el derecho al goce o uso de un equipo ó desarrollo informático durante un tiempo determinado, a un precio estipulado en el contrato. Durante ese periodo de tiempo, el arrendador se encargará del mantenimiento del objeto arrendado. De este modo, el arrendador se responsabiliza de los perjuicios que pueda provocar la parada de los servicios que el objeto alquilado ofrece al usuario.
- Contrato de opción a compra: Este tipo de contrato recoge la posibilidad de que el alquilador ejerza la posibilidad de comprar el objeto del alquiler. El comprador tendrá la posibilidad unilateral de ejercer el derecho a compra, con el precio que se habrá fijado en el contrato, dentro de un plazo que también se deberá fijar en el contrato.
- Contrato de mantenimiento: Puede ser un contrato para el mantenimiento tanto de hardware como de software, o también de mantenimiento integral, que incluiría formación y asesoría.
- Contrato de prestación de servicios: También clasificable como de arrendamiento de servicios, que incluirían análisis, diseño, desarrollos, etc...
- Contrato de arrendamiento de obra: Ofrece la realización, o la terminación de una obra determinada, independientemente de los medios empleados, o del trabajo en sí mismo.
- Contrato de préstamo: Se trata de un caso especial de contrato de arrendamiento, gratuito, también conocido como comodato.
- Contrato de depósito: Se trata de otro contrato gratuito, en el que una persona recibe una cosa, con el fin de guardarla y devolverla una vez acabe el plazo estipulado.

TIPOS GENERALES

- Compraventa informática: Compraventa tradicional, solo que de un bien informático.
- Arrendamiento financiero ó leasing: una de las partes adquiere un producto informático y cede su uso a la otra durante un tiempo a cambio de unas cuotas. Transcurrido el plazo, se devuelve el bien, o se compra completamente por un precio residual.
- Desarrollo informático a medida: Se contrata la construcción de un software empresarial a medida de las necesidades de la empresa. El software se crea adaptado al cliente.
- Contrato de Licencia de Uso: A partir de un software existente ya creado se autoriza a su uso a los clientes que adquieran una licencia por un precio. El software no se adapta al cliente, sino que el cliente se adapta al software.
- Escrow, o depósito de código fuente: Es un contrato de depósito cuyo objeto es un programa de ordenador. En concreto, se deposita el código fuente, el compilador, el manual de usuario y el código objeto.
- Outsourcing: Cesión de los sistemas de información de la empresa a un tercero.

CASO DE ESTUDIO

NECESIDADES DE LA EMPRESA

La empresa tiene necesidades de contratar tanto hardware como software, debido a que no es una empresa del sector, y necesita que otro socio se encargue de esta área. Por un lado necesitará desarrollar un software que permita gestionar la información empresarial, y por otro lado necesitará de equipos informáticos para manejar las aplicaciones en los puestos de trabajo.

Es muy importante indicar que los objetos de los contratos queden bien definidos mediante estudios de necesidades previos.

CONTRATO INFORMÁTICO – HARDWARE

La empresa no va a necesitar hardware puntero ni actualizaciones continuas del mismo. Simplemente requiere de una arquitectura cliente – servidor, con equipos sencillos en el

lado del cliente (pcs en las oficinas, pda's para repartidores), y un servidor de aplicaciones y recursos (aplicación de gestión, correo, base de datos).

Lo mejor en ésta situación es que otra empresa se encargue de la compra y mantenimiento del hardware, y de la satisfacción de las necesidades empresariales en éste aspecto. Es por ello, que se recomienda un doble contrato, primero de compraventa y después de mantenimiento.

CLAUSULAS TÍPICAS DE LOS CONTRATOS

El contrato de **compraventa**:

1. Objeto del contrato: descripción de qué se está adquiriendo.
2. Precio: importe final de la compra.
3. Lugar y fecha de entrega del bien. Momento y lugar de entrega, o las distintas etapas en que se recibirá.
4. Garantía: Plazo y cobertura de la misma.
5. Obligaciones de las partes: Compromisos que se establecen entre las partes para la celebración del contrato.
6. Resolución del contrato: Causas que podrán disolver el contrato entre las partes.
7. Resolución de conflictos: Manera extrajudicial de resolver conflictos derivados del contrato, como puede ser mediante arbitraje, mediación, conciliación, etc..
8. Reserva de dominio: Si el vendedor se reserva la propiedad del objeto vendido hasta satisfacer el precio del contrato.

Para el contrato de **mantenimiento**:

1. Periodo de Vigencia: duración del contrato de mantenimiento.
2. Servicios de Asistencia Técnica Contratados: se recogen los detalles del mantenimiento que se realizará.
 - a. Servicios On-Site: qué servicios se prestarán presencialmente.
 - b. Servicios Off-Site: qué servicios se prestarán a distancia.
 - c. Utilización de asistencias: modo de actuación para solicitar un mantenimiento.

3. Periodo de Servicio de Mantenimiento: horario y calendario en el que se podrá llamar al servicio técnico para indicar una incidencia.
4. Cargo, facturación y pago: modo en el que se realizará el pago por los servicios de asistencia.
5. Terminación: Causas que podrán disolver el contrato entre las partes.
6. Servicios Excluidos: una lista de los servicios no incluidos en el mantenimiento para evitar problemas de coberturas

CONTRATO DE COMPRA Y MANTENIMIENTO DE HARDWARE

DE UNA PARTE:

Transportes S.A.

Y DE OTRA:

Venta y Mantenimiento Informáticos S.A.

Los contratantes se reconocen recíprocamente, en el carácter en que intervienen, plena capacidad jurídica para contratar y en el caso de representar a terceros, cada uno de los intervinientes asegura que, el poder con el que actúa no ha sido revocado ni limitado, y que es bastante para obligar a sus representados en virtud de este CONTRATO DE VENTA Y MANTENIMIENTO DE HARDWARE y a tal objeto:

En el ámbito de la Venta se establecen las siguientes cláusulas:

1. Objeto del contrato: Adquisición e instalación de los equipos informáticos especificados en el Anexo I.
2. Precio: XXXX euros.
3. Lugar y fecha de entrega del bien. Montaje de equipos de usuario en los distintos puestos de la empresa entre los días 10 y 12 de julio de 2010. Montaje de los equipos servidores en el local especificado por la empresa entre los días 5 y 9 de julio de 2010.
4. Garantía: 2 años desde el momento del montaje para fallos de fabricación, excluyendo las averías producidas por usuarios.
5. Obligaciones de las partes:

6. Resolución del contrato:
7. Reserva de dominio: El vendedor conservará la propiedad de los bienes impagados.

En el ámbito del Mantenimiento se establecen las siguientes cláusulas:

1. Periodo de Vigencia: 5 años.
2. Servicios de Asistencia Técnica Contratados:
 - a. Servicios On-Site: Sustitución de piezas
 - b. Servicios Off-Site: Determinación remota de la naturaleza de la avería
 - c. Utilización de asistencias: mediante teléfono o email.
3. Periodo de Servicio de Mantenimiento: de 9 a 19 en días laborables. Quedan excluidos de los servicios normales las actuaciones fuera de dichos horarios, facturándose con tarifa especial.
4. Cargo, facturación y pago: a mes cumplido XXX euros fijos, más los extras que se hayan efectuado durante el mes.
5. Terminación: tras los 5 años contratados, pudiéndose prorrogar si las partes así lo desean
6. Servicios Excluidos: Se excluye del mantenimiento los aparatos informáticos que los usuarios hayan podido aportar a título personal.

ANEXOS

1. Anexo I: Lista de equipos informáticos adquiridos

Y en prueba de conformidad ambas partes firman el presente, por duplicado ejemplar y a un sólo efecto en la fecha y lugar indicado:

.....

Burgos a 25 de junio de 2010

CONTRATO INFORMÁTICO – SOFTWARE

La empresa requiere del desarrollo de una aplicación específica para el desempeño de sus labores empresariales. Puesto que la propia empresa se dedica a otro sector, lo más recomendable es contratar a otra empresa el desarrollo de la aplicación y la base de datos, ya que mantener un equipo de desarrollo sería demasiado caro y desproporcionado.

El contrato que mejor se adapta a las necesidades de la empresa es un contrato de desarrollo de software a medida. Mediante este tipo de contrato se acuerda la implementación de un software específico, a medida de las necesidades del cliente, conteniendo el producto resultante el código fuente, manuales, ayudas, documentación de diseño, los ejecutables, la documentación de estándares, y la propiedad sobre los derechos de autor.

Al ser un software desarrollado a medida, está destinado a integrarse perfectamente en el funcionamiento de la empresa, adaptándose a las reglas y políticas del negocio.

A continuación se presentará el contrato de desarrollo de software. Éste contrato queda complementado por los de protección de software y de bases de datos que se vieron en anteriores capítulos, y que protegen la propiedad del software desarrollado.

COMPOSICIÓN DEL SOFTWARE

La empresa recibirá 4 productos

1. Análisis funcional: Documento que define las funciones que desarrollará el programa.
2. Análisis orgánico: Documento que detalla los métodos, lenguajes y sistemas operativos que participarán en el software.
3. Código fuente: Código de desarrollo del programa.
4. Código objeto: Código ejecutable del programa, obtenido a partir de la compilación del código fuente.

CLÁUSULAS TÍPICAS DEL CONTRATO

Este es el conjunto mínimo de cláusulas que deberá recoger un contrato de desarrollo de software a medida:

1. Objeto del contrato: Se define el programa desarrollado, siguiendo las indicaciones del cliente.
2. Precio y forma de pago: Se determina el precio del proyecto, que podrá ser:
 - a. A tanto alzado: el precio es cerrado desde el inicio del proyecto, siendo un precio fijo por todo el proyecto, o en varios pagos que se realizarán con la consecución de determinados hitos en el desarrollo.
 - b. Por lo trabajado: precio por horas/hombre, es un precio no cerrado, que reflejará el esfuerzo invertido en el desarrollo del proyecto.
3. Entrega: Podrá ser única, parcial, o por hitos. Es más habitual realizar una entrega en etapas, porque es la que mayor seguridad jurídica otorga al cliente, al poder comprobar su funcionamiento, y poder emitir un certificado de conformidad. También se pueden fijar sanciones para el desarrollador en caso de que alguna de las entregas se retrase o falle.
4. Calidad: Para evitar el riesgo de que el programa desarrollado no funcione bien, o no se ajuste a las necesidades del cliente, existen diversas opciones para determinar la calidad del desarrollo que se pueden fijar en el propio contrato:
 - a. Baterías de pruebas previamente pactadas por ambas partes.
 - b. Periodo de prueba por parte del cliente, para comprobar funcionamiento y funcionalidades, durante el que pueda notificar al desarrollador los problemas y reservas detectados.
 - c. Periodo de prueba por parte del desarrollador, durante el cual se encargará de realizar las correcciones y modificaciones que el cliente estime.
 - d. Exención de responsabilidades por parte del desarrollador.
5. Garantía: Se fijarán un plazo de duración y los límites de la garantía, durante los cuales el desarrollador se compromete a reparar los errores que se detecten en el funcionamiento normal del programa.

6. Mantenimiento: Se fijará una duración pactada del mantenimiento del programa, lugar donde se presta el servicio, la forma de pago del mismo, tiempo de respuesta, responsables de mantenimiento, etc.
7. Propiedad del programa: Si no se establece nada, los derechos patrimoniales y morales corresponden al programador. Sin embargo, también puede pactarse copropiedad entre desarrollador y cliente, o propiedad para el cliente, a través de la cesión de los derechos patrimoniales (que incluye la cesión del código fuente). Otra opción es que la propiedad quede en manos del desarrollador, y que éste decida si cede o no el código fuente al cliente.
8. Pacto de confidencialidad: Recoge el acuerdo por el que el desarrollador se compromete a guardar la información obtenida en el desarrollo del proyecto de manera completamente confidencial. Tiene como finalidad asegurar la confidencialidad de la información que ha sido necesaria para construir el software. Puede negociarse una duración del pacto de confidencialidad durante, o tras el desarrollo del proyecto. También puede pactarse la devolución, o destrucción de documentos que el desarrollador haya requerido para completar el proyecto. Se puede plantear como una cláusula del contrato, o como un contrato a parte.
9. Pacto de exclusividad: Refleja el compromiso del desarrollador de no crear programas idénticos al del proyecto para otros clientes.
10. Resolución anticipada: Recogerá los motivos por los que puede acabar de manera anticipada el contrato, por incumplimiento de alguna de las obligaciones asumidas en el contrato.

CONTRATO SOFTWARE

DE UNA PARTE:

Transportes S.A.

Y DE OTRA:

Desarrollos Informáticos S.A.

Los contratantes se reconocen recíprocamente, en el carácter en que intervienen, plena capacidad jurídica para contratar y en el caso de representar a terceros, cada uno de los intervinientes asegura que, el poder con el que actúa no ha sido revocado ni limitado, y que es bastante para obligar a sus representados en virtud de este CONTRATO DE DESARROLLO DE UN SISTEMA DE SOFTWARE A MEDIDA y a tal objeto:

1. Objeto del contrato: Se desarrollará un software específico a las necesidades globales de la empresa, que permita la gestión de la actividad propia de la empresa y de los recursos humanos. Los requisitos específicos del software se recogen en el Anexo I del contrato.
2. Precio y forma de pago: El pago se realizará a tanto alzado. Se realizará un pago por cada módulo del sistema desarrollado.
3. Entrega: Mediante hitos marcados, quedando en manos de Transportes S.A. la aceptación del nuevo módulo desarrollado.
4. Calidad: Se fijan las siguientes condiciones de aceptación:
 - a. Baterías de pruebas. Descritas en el Anexo II del contrato.
 - b. Periodo de prueba por parte del cliente.
5. Garantía: Durante 5 años, prorrogables, queda fijado una garantía sobre todos los defectos de fábrica y cualquiera detectado en la etapa de despliegue y explotación, quedando exentos los problemas generados por usuarios.
6. Mantenimiento: 5 años de mantenimiento in situ, prorrogables.
7. Propiedad del programa: La propiedad será para el cliente, mediante la cesión de los derechos patrimoniales (que incluye la cesión del código fuente).
8. Pacto de confidencialidad: Al cederse la propiedad del desarrollo al cliente, el desarrollador se compromete a no divulgar ni reproducir el código fuente del programa.
9. Pacto de exclusividad: Análogamente a la cláusula anterior, el programa es un desarrollo exclusivo para la empresa.
10. Resolución anticipada: El incumplimiento de la garantía o el mantenimiento motivarán el fin anticipado del contrato, sacándose entonces a concurso el mantenimiento, sin que la empresa que abandona pueda presentarse al mismo.

ANEXOS

1. Requisitos del Software

2. Pruebas de aceptación del Software

Y en prueba de conformidad ambas partes firman el presente, por duplicado ejemplar y a un sólo efecto en la fecha y lugar indicado:

.....

.....

Burgos a 25 de junio de 2010

7. ADMINISTRACIÓN Y FISCALIDAD ELECTRÓNICA

ADMINISTRACIÓN ELECTRÓNICA

La expresión “administración electrónica” se refiere al uso de técnicas y medios electrónicos, informáticos y telemáticos en el desarrollo de las actividades y procedimientos que competen a la Administración. En la Ley 30/1992 de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común se impulsaba el empleo de estos medios, si bien la puesta en marcha de los mismos no se planteaba como una obligación para las distintas Administraciones, sino que era voluntaria.

El gran salto en el desarrollo de una administración electrónica avanzada tiene su origen en la publicación de la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP). Esta Ley reconoce el «derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos» y, junto a ello, establece la «obligación de las Administraciones Públicas de rediseñar sus procedimientos y dotarse de los medios técnicos necesarios para que el ejercicio del nuevo derecho sea plenamente efectivo».

Es a partir del 1 de enero de 2010, la fecha que se establece en la ley de acceso a partir de la cual, las Administraciones Públicas estarán obligadas a proporcionar el acceso electrónico de los ciudadanos a los servicios públicos.

MARCO LEGAL EN ESPAÑA

La Administración Electrónica tiene su mayor impulso en la primera década del siglo XXI.

Principalmente, hay que mencionar la Ley 11/2007, de acceso electrónico de los ciudadanos a los Servicios Públicos (LAECSP), a la que en muchas ocasiones se refiere como "Ley de Administración Electrónica", que consagra el concepto de Administración Electrónica en el marco jurídico español y la eleva a la categoría de derecho de los ciudadanos. Es decir, los ciudadanos tienen el derecho de acceder electrónicamente a los servicios de la Administración Pública y éstos ya no son

facultativos para ésta, sino que la capacidad para proporcionarlos se convierte en una obligación para la misma, que deberá hacerse realidad a partir del 31 de diciembre del 2009.

La LAECSP es una regulación pionera en la materia a nivel mundial. En el momento de su aprobación, sólo cinco países contaban con una norma similar: EE.UU., Francia, Finlandia, Italia y Austria.

FISCALIDAD ELECTRÓNICA

Los tributos que gravan el comercio electrónico son los mismos que se aplican en la actualidad al comercio tradicional: Impuesto sobre la Renta de las Personas Físicas (IRPF), Impuesto sobre la Renta de los No Residentes (IRNR), Impuesto sobre Sociedades (IS) e Impuesto sobre el Valor Añadido (IVA). Estos impuestos, los tres que recaen sobre la renta y el que grava el consumo, son los que afectan de forma más directa al comercio, pero también inciden en la contratación otros tributos como los Impuestos Especiales (IIEE), el Impuesto sobre Transmisiones Patrimoniales (ITP) y los Impuestos Aduaneros (IIAA). A continuación se analizará el carácter de estos impuestos:

Impuesto sobre la renta de las personas físicas

Obtención de renta por el contribuyente, que debe ser una persona física con residencia habitual en España. Cuando quien lleva a cabo sus actividades económicas a través de la red es una persona física con residencia en España, los rendimientos obtenidos serán objeto de gravamen en este impuesto. Por el hecho de que el comercio pueda ser considerado electrónico no escapa a la tributación de este impuesto.

Impuesto sobre la renta de no residentes

El Impuesto sobre la Renta de No Residentes grava las rentas obtenidas en territorio español por las personas físicas y entidades no residentes en el mismo

Impuesto sobre sociedades

El Impuesto sobre Sociedades grava las rentas obtenidas por las sociedades y demás entidades jurídicas. El hecho imponible está constituido precisamente por la obtención de esas rentas, siendo indiferente su fuente u origen.

Impuesto sobre el valor añadido

El Impuesto sobre el Valor Añadido es un impuesto indirecto (los tres anteriores son directos) que recae sobre el consumo y grava las entregas y prestaciones de servicios efectuadas por empresarios o profesionales (operaciones interiores), las adquisiciones intracomunitarias de bienes y las importaciones de bienes. Las entregas de bienes y prestaciones de servicios deben ser realizadas por empresarios o profesionales a título oneroso, con carácter habitual u ocasional, en el desarrollo de su actividad empresarial o profesional.

Impuestos especiales

Los Impuestos Especiales, recaen sobre consumos específicos: alcohol y bebidas alcohólicas, hidrocarburos, labores del tabaco y electricidad y determinados medios de transporte. Gravan su fabricación, importación y, en su caso, introducción en el ámbito territorial interno, y la matriculación.

Impuesto sobre transmisiones patrimoniales

En este caso el impuesto se exige por las transmisiones patrimoniales onerosas de bienes y derechos, independientemente de su naturaleza, que estuvieran situados, pudieran ejercitarse o hubieran de cumplirse en territorio español o en territorio extranjero, cuando, en este último supuesto, el obligado al pago del impuesto tenga su residencia en España.

Impuestos aduaneros

Por Impuestos Aduaneros debemos entender todos aquellos que tienen como objeto el tráfico internacional de mercancías. En la actualidad son tributos de regulación comunitaria. La figura más importante que se incluye en ellos es la de los derechos a la

importación, tributo que se exige por la entrada de mercancías en el territorio aduanero comunitario

CASO DE ESTUDIO

La administración electrónica se define como el conjunto de procedimientos y sistemas soporte que permiten el acceso telemático externo e interno a los servicios ofertados por una administración, tanto para la consulta de información como para la tramitación en línea.

En este sentido hay que contemplar las tres categorías principales de servicios que ofrece la Administración:

- A2A, Administration to Administration: Servicios de Administración a Administración (plataformas de intercambio de servicios, legislación...)
- A2C, Administration to Consumer: Servicios de la Administración a los ciudadanos (Ejemplo: pago de impuestos, busca de trabajo a través de oficinas de empleo virtuales, matriculación en la Universidad, petición de citas para los servicios de salud...)
- A2B, Administration to Business: Servicios de la Administración a las empresas (Ejemplo: pago de tasas, impuestos, información sobre subvenciones, tramitación para la creación de empresas, compras públicas...)

Es el tercer caso, el A2B el que enmarca nuestro caso de estudio.

A2B

La Administración electrónica hace posible una Administración más rápida y transparente dónde se reduce en gran medida el tiempo necesario para crear una empresa y también su coste, ya que se ofrecen recursos gratuitos on line.

Los principales servicios que la administración pública ofrece a las empresas de manera electrónica son los siguientes:

- Contribuciones a la Seguridad Social por empleados
- Impuestos de Sociedades: declaración, presentación...

- IVA: declaración, presentación, pago
- Registro de nuevas sociedades
- Envío de datos para estadísticas oficiales
- Declaraciones de aduanas
- Permisos ambientales (incluida presentación de informes)
- Compras y licitaciones públicas

IMPUESTOS

Los impuestos a los que queda sujeta la empresa, debido a su naturaleza de prestador de servicios de transporte:

- Impuesto sobre la Renta de Personas Físicas
- Impuesto sobre sociedades
- Impuesto sobre el valor añadido
- Impuestos especiales (los referentes a transporte)
- Impuestos aduaneros

El ejercicio de subsanación de estos impuestos por parte de la empresa puede realizarse de manera presencial, o como veremos a continuación, a través de los sistemas de administración electrónica que actualmente la Ley 11/2007 exige a las administraciones públicas.

EJEMPLOS PRÁCTICOS DE ADMINISTRACIÓN ELECTRÓNICA ESPAÑOLA

A continuación, se van a presentar diversos ejemplos en los que la empresa puede hacer uso de servicios de administración electrónica:

Seguridad Social

La página web de la seguridad social permitirá a la empresa realizar sus cotizaciones de manera electrónica, o solicitar sus certificados electrónicos.

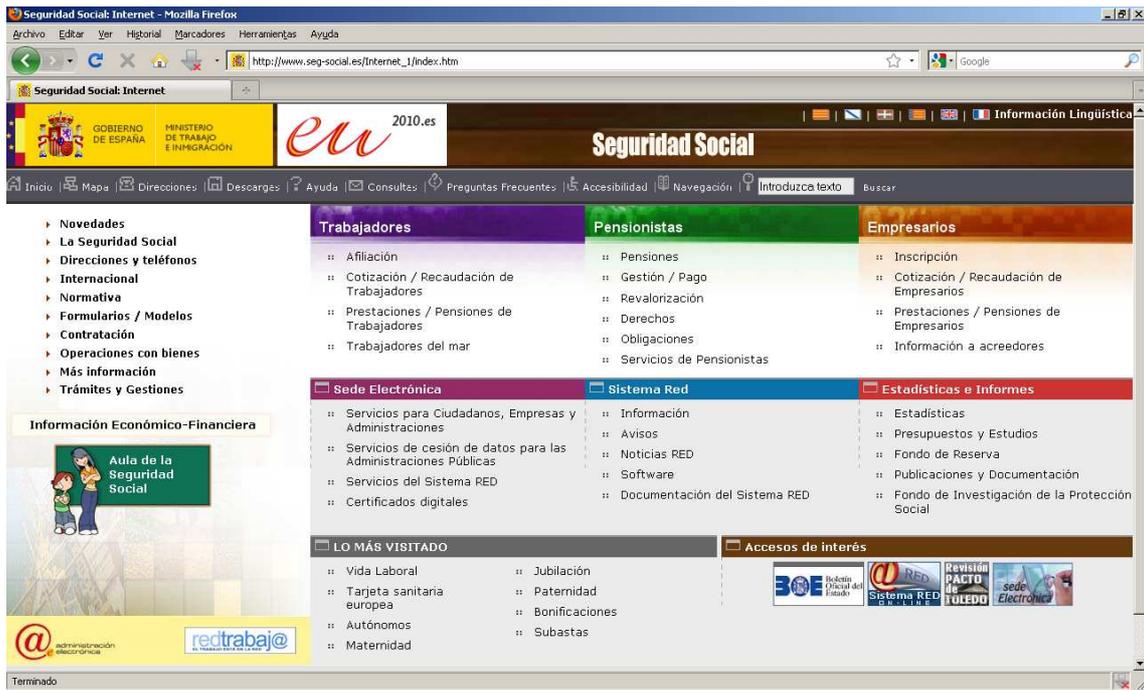


Ilustración 7-1: Página web de la seguridad social

Hacienda

Realización de declaraciones de renta, pago de impuestos, pago del IVA, etc. Directa relación con la fiscalidad electrónica, ya que permite realizar el pago de los impuestos relacionados con el comercio electrónico.



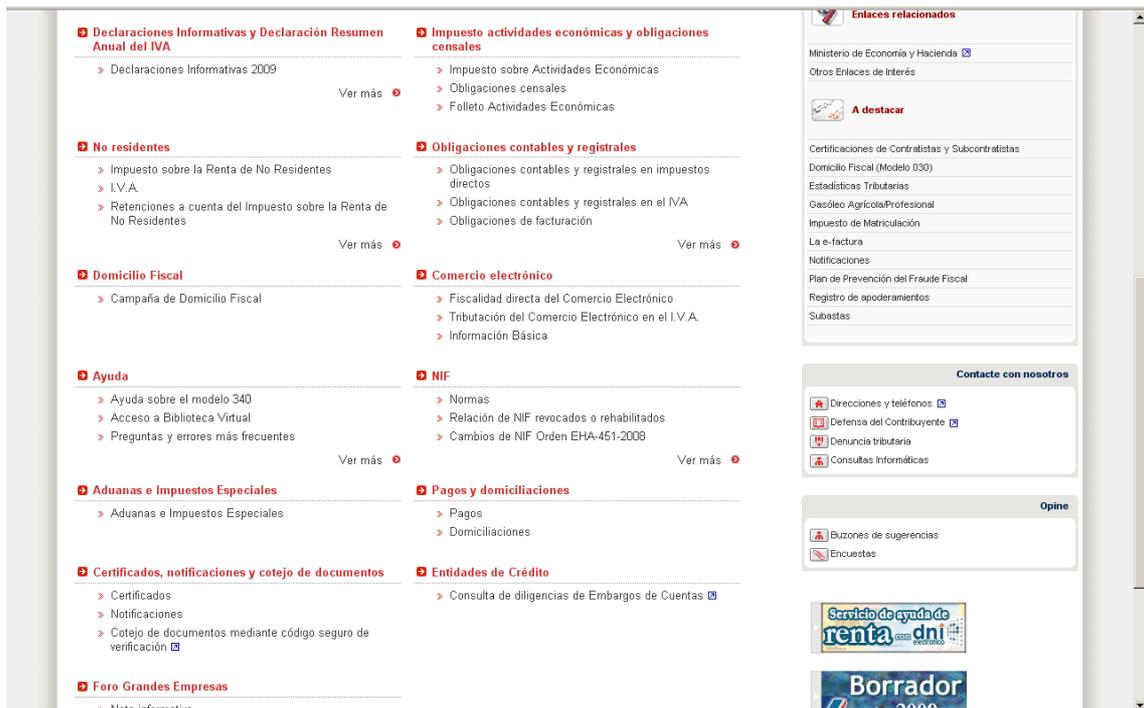


Ilustración 7-2: Página web del Ministerio de Hacienda

Ministerio de Transporte

Ministerio que regula las actividades de la empresa.

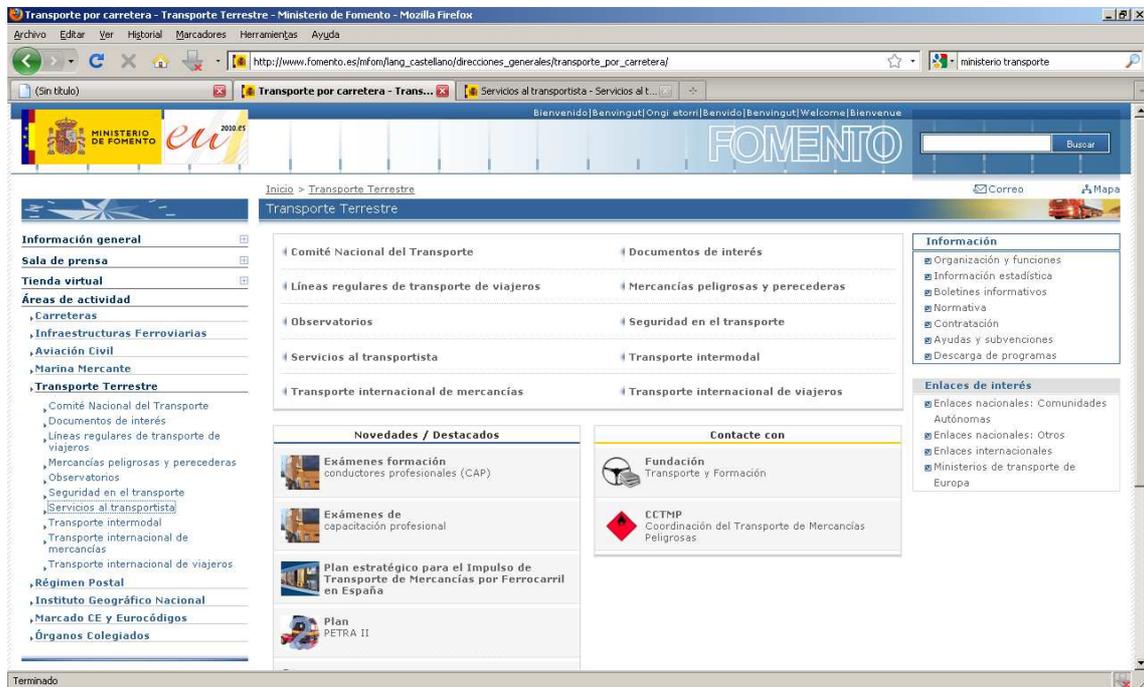


Ilustración 7-3: : Página web del Ministerio de Transporte

8. WEB 2.0

INTRODUCCIÓN

Web 2.0 es el término utilizado para describir la segunda generación de la World Wide Web, que está enfocada en la habilidad de la gente para colaborar y compartir información online.

Un primer paso en la evolución de la Web fue la transición del HTML estático de las páginas web, a webs más dinámicas, más organizadas y basadas en aplicaciones de servicio web a los usuarios. La auténtica evolución a la Web 2.0 se produce con la aparición de una comunicación abierta entre el usuario y la web, con énfasis en las web basadas en comunidades de usuarios.

Los blogs, wikis y otros servicios web son todos vistos como componentes del Web 2.0, asociándose en todos los casos a la gran expansión de la WWW y las tecnologías relacionadas.

El término fue acuñado por Dale Dougherty de O'Reilly Media en una tormenta de ideas con Craig Cline de MediaLive para desarrollar ideas para una conferencia. Dougherty sugirió que la web estaba en un renacimiento, con reglas que cambiaban y modelos de negocio que evolucionaban. Dougherty puso ejemplos en vez de definiciones, y reclutó a John Battelle para dar una perspectiva empresarial, y O'Reilly Media, Battelle, y MediaLive lanzó su primera conferencia sobre la Web 2.0 en octubre de 2004. La segunda conferencia se celebró en octubre de 2005.

En 2005, Tim O'Reilly definió el concepto de Web 2.0. El mapa meme mostrado (elaborado por Markus Angermeier) resume el meme de Web 2.0, con algunos ejemplos de servicios.

En su conferencia, O'Reilly, Battelle y Edouard resumieron los principios clave que creen que caracterizan a las aplicaciones web 2.0: la web como plataforma; datos como el "Intel Inside"; efectos de red conducidos por una "arquitectura de participación"; innovación y desarrolladores independientes; pequeños modelos de negocio capaces de

redifundir servicios y contenidos; el perpetuo beta; software por encima de un solo aparato.

En general, cuando mencionamos el término Web 2.0 nos referimos a una serie de aplicaciones y páginas de Internet que utilizan la inteligencia colectiva para proporcionar servicios interactivos en red dando al usuario el control de sus datos.

Así, podemos entender por Web 2.0, como propuso Xavier Ribes en 2007, "todas aquellas utilidades y servicios de Internet que se sustentan en una base de datos, la cual puede ser modificada por los usuarios del servicio, ya sea en su contenido (añadiendo, cambiando o borrando información o asociando datos a la información existente), bien en la forma de presentarlos o en contenido y forma simultáneamente".

TECNOLOGÍAS

Algunas de las principales tecnologías que forman parte de los mecanismos de la Web 2.0 son, por ejemplo:

1. Blogs: Bitácoras personales en las que un usuario, ó empresa ofrece información y opinión sobre aspectos de actualidad.
2. Mash-ups: aplicaciones que recogen información de distintas fuentes y se las presentan al usuario de manera unificada.
3. Efecto red: Nombre del efecto que dota de más valor a la información que más gente utiliza.
4. RSS: Sistema que permite al usuario recibir noticias desde un determinado origen, en tiempo casi real.
5. Clasificación: Etiquetado de un contenido digital por parte de los usuarios del mismo, creando un sistema de clasificación no jerárquico, sino grupal. Es un remanente de la idea de Web Semántica.
6. Wikis: Sitio web colaborativo que permite que los usuarios puedan aportar conocimientos sobre determinado tema, sin necesidad de programar.
7. AJAX y FLASH: Lenguajes de programación que permiten la creación de contenido web dinámico.
8. Peer-to-Peer: Protocolos que permiten la interacción distribuida de clientes sin necesidad de un servidor, sustituyendo a la arquitectura cliente-servidor.

EMPRESA 2.0

La empresa 2.0 es aquella que, por analogía con la web 2.0, toma la referencia de ésta en lo que se refiere al uso de herramientas de software social. La empresa 2.0 engloba el uso de los principios y prácticas de la denominada web social como plataforma de actuación dentro del campo empresarial.

Los empleados de la empresa hacen uso de las herramientas de Web 2.0 para crear contenido y formar comunidades sin requerir de un alto grado de conocimientos técnicos, pero en el ámbito de la organización. Las ideas en torno a las que se define la empresa 2.0, bajo el acrónimo SLATES son:

- Search (Búsqueda): las personas buscan y encuentran lo que necesitan para su actividad laboral navegando por los contenidos organizados de sus Intranets corporativas.
- Links: (Enlaces): la forma en que se busca información ya no es mediante secuencia de principio a fin, sino de un recurso a otro. El enlace es el orden de la empresa 2.0.
- Authoring (Generación): Cada cual es capaz de mostrar lo que sabe y de generar tráfico en torno a sus contenidos, siempre que sean útiles para los demás.
- Tag (Etiqueta): La experiencia de quien usa los sistemas de información de una empresa se ve enriquecida por la etiquetación. No son las máquinas sino los humanos quienes etiquetan el contenido. De esta forma la búsqueda se acerca al criterio de la persona, se humaniza.
- Extensions (Extensión): Este es un sistema de recomendación, que actúa como mejora de los motores de búsqueda. Si se da valor a los contenidos localizados, los contenidos valorados por muchas personas se etiquetarán como contenido útil, o más interesante para los posteriores buscadores.
- Signals (Señales): Se utilizan como forma de saber que algo relevante ha sucedido. Se pueden implementar sistemas de señalización que “detecten movimiento” dentro de un campo de interés.

Si la web 2.0 está dirigida para los usuarios, la Empresa 2.0 está dirigida a los empleados y clientes fomentándose el uso de herramientas de web social tanto a nivel

interno -en las diferentes unidades operativas de una empresa- como en su relación externa con el sector en el que se encuentre.

CASO DE ESTUDIO

PASOS DE ADAPTACIÓN A LA EMPRESA 2.0

Mediante una serie de sencillos pasos la empresa se puede adaptar al uso de las herramientas que la web 2.0 provee:

Escuchar:

Conviene monitorizar y analizar lo que los clientes comentan sobre la empresa en línea y luego utilizar esta información como un sistema de alerta temprana. Hasta la observación esporádica de las redes sociales es mejor que no hacer nada. De este modo se podrá saber qué piensa el cliente con respecto a lo que se ofrece.

Antes de mandar mensajes a los consumidores, hay que darles la oportunidad que se expresen, y escucharlos. Es importante también tener en cuenta que las cosas cambian en cuestión de horas en Internet, por lo que el monitoreo debe ser constante.

Experimentar:

No puede solo estar monitoreando, hay que involucrarse con los clientes a través de las herramientas existentes. Se puede comenzar por cosas sencillas como un perfil de la empresa en una red social que vaya atrayendo fans, para posteriormente promover nuevos productos, y enviar mensajes a los clientes potenciales por la misma red. Este método implica un bajo coste, ya que la mayor parte de las herramientas son gratuitas, y además genera reconocimiento de marca y percepción por su cliente. También se puede crear una cuenta en Google Analytics para saber cómo se accede a la página.

Aplicar:

Se toman los resultados de los experimentos y se aplican sobre las políticas de la empresa. Se puede comenzar por optimizar el sitio Web empresarial para que conecte fácilmente con las redes sociales y las comunidades.

Desarrollar:

Internet es un medio social que ofrece grandes posibilidades de marketing y publicidad. Dichas cualidades se pueden aprovechar para desarrollar programas de marketing integrados que utilicen la Web más que otro canal de publicidad. Esto puede representar un medio barato y sustitutivo a los medios masivos de publicidad.

Observar:

Es importante observar cómo los potenciales clientes acceden a la web de la empresa, y cómo la buscan. Google Analytics implementa medidores que analizan lo que está pasando en la web (visitas, páginas vistas, clics, usuarios nuevos, usuarios fidelizados, etc) Google AdWords, permite posicionar a la empresa dentro del buscador cuando el usuario hace uso de ciertas palabras. Que la empresa se encuentre entre los primeros resultados de una búsqueda aumenta las posibilidades de que el comprador entre en la página empresarial y contrate alguno de los servicios de la empresa.

PUESTA EN PRÁCTICA

A continuación, se presentarán ejemplos de utilización de las tecnologías de Web 2.0, aplicadas a las necesidades de nuestra empresa:

Wiki

Se puede utilizar el Wiki para escribir de forma colaborativa documentos empresariales entre varios empleados. Cada uno de los usuarios accede al documento web realiza las modificaciones pertinentes y el resto de usuarios puede comprobar qué, por quién y cuándo ha sido modificado el documento. Además permite clasificar mediante etiquetas toda la información que se vaya generando de forma que es un excelente repositorio.

Blog

Se puede establecer una comunicación fluida entre la empresa y sus empleados publicando noticias internas que les mantengan informados de todo lo que pase en la empresa. Los empleados podrán opinar sobre las entradas publicadas y así conocer su opinión de primera mano.

RSS

Asociada al ejemplo del blog, se puede utilizar la tecnología de RSS para comunicar en tiempo real cuándo se actualiza el blog, y enlazar con un solo clic el acceso a la noticia en sí misma.

Mash-up

Puesto que la naturaleza del trabajo de la empresa implica el uso de medios de transporte terrestre, muchas veces el cumplimiento de los envíos puede depender del estado de las vías de comunicación. Se podría construir una aplicación de mash-up, que recoja información climatológica, de obras públicas y de otros factores, que los unifique y presente a los usuarios repartidores, permitiéndoles determinar qué ruta escoger.

Contacto con el cliente

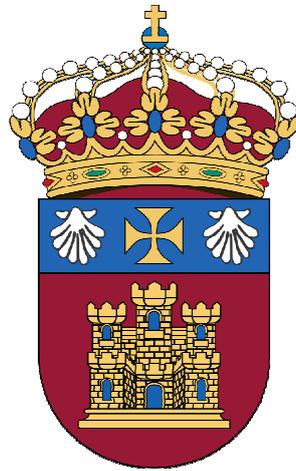
Herramientas como Facebook y Twitter permiten estar en contacto permanente con los consumidores, conocer lo que comentan, estar al día en lo que desean y quieren hacer, y aprovechar para mejorar la propuesta de valor de nuestros productos y servicios. Ahora la tarea es para que la empresa, que debe utilizar estos medios para estar en contacto con su cliente, para saber cuáles son sus gustos, en qué piensa, cuáles son sus intereses, en tiempo real, en forma inmediata.

Tener un canal en YouTube donde se pueden ir incluyendo videos de todos los eventos de la empresa alrededor de sus productos. Una página en Facebook donde invita a fans a unirse a ella para comentar sobre productos, tendencias, encuestarlos, y generar así productos más cercanos al querer del cliente.

Observación del cliente

Diversas herramientas de Google pueden permitir que la empresa analice cómo el cliente llega hasta la empresa. Google Analytics permite conocer estadísticas y marcadores de uso de la página web. Google Analytics tiene una interesante herramienta, el Optimizador de Web, que permite saber a medida que se cambian los contenidos de la página web, qué posiciones y movimientos obtienen mejores resultados. Google AdSense permite posicionar la empresa en los resultados de búsqueda.

ADECUACIÓN A LAS TIC DE UNA EMPRESA DE TRANSPORTES



BIBLIOGRAFÍA

Autor del proyecto: Javier Sáez Moneo

Tutor del proyecto: Prof. Miguel Ángel Davara Rodríguez

Directores del Magíster:
Dr. Emilio S. Corchado Rodríguez
Dr. Álvaro Herrero Cosío

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

UNIVERSIDAD DE BURGOS

II Edición. Burgos, Julio 2010.

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

BIBLIOGRAFÍA

Protección de Datos

“Factbook Comercio Electrónico”, Profesor Miguel Ángel Davara

“Formularios de ejercicio de derechos”, AENA

“Modelo de Documento de Seguridad”, AEPD

“Formularios NOTA”, AEPD

Tecnologías de la Información y la Comunicación

“Factbook Comercio Electrónico”, Profesor Miguel Ángel Davara

“Tecnologías de la Información: Aspectos Jurídicos”, Davara & Davara

“Saberes: Revista de Estudios Económicos, Jurídicos y Sociales – Volumen I, año 2003”, artículo sobre comercio electrónico, de Miguel Ángel Davara

“La protección jurídica de las bases de datos”, Comité Permanente de Derechos de Autor y Derechos Conexos, Octava sesión, Ginebra, 4 a 8 de noviembre de 2002

“Respuestas a las dudas iniciales sobre firma electrónica”, Dirección de Sistemas de Información Departamento CERES

“Nuevas formas de proteger el software”, Escrow Spain

“Empresas: 5 pasos para entrar a la Web 2.0”, artículo de Manuel Gross

“Pliego de condiciones de servicios de transporte”, Seur

