



102

El Comercio Electrónico en el sector asegurador

Estudio realizado por: Mireia Rubio Cantisano
Tutor: May Plana Bernal

**Tesis del Máster en Dirección de Entidades
Aseguradoras y Financieras**
Curso 2009/2010

Cuadernos de Dirección Aseguradora es una colección de estudios que comprende las tesis realizadas por los alumnos del Máster en Dirección de Entidades Aseguradoras y Financieras de la Universidad de Barcelona desde su primera edición en el año 2003. La colección de estudios está dirigida y editada por el Dr. José Luis Pérez Torres, profesor titular de la Universidad de Barcelona, y la Dra. Mercedes Ayuso Gutiérrez, catedrática de la misma Universidad.

Esta tesis es propiedad del autor. No está permitida la reproducción total o parcial de este documento sin mencionar su fuente. El contenido de este documento es de exclusiva responsabilidad del autor, quien declara que no ha incurrido en plagio y que la totalidad de referencias a otros autores han sido expresadas en el texto.

Presentación

Agradezco la presente tesis a las personas que han hecho posible que pueda realizar este Master, en especial a May Plana, Rosa Ortín y Dolores de Rueda. Asimismo, me gustaría dar las gracias a mis padres por su apoyo incondicional y a aquellas personas que han estado a mi lado todo este año.

Bucaneros, ha sido todo un placer!

Resumen

El comercio electrónico surge con la aparición de las nuevas tecnologías de la información y la comunicación. Internet es el escenario donde se desarrollan las operaciones comerciales, siendo las más importantes las que hacen referencia al proceso de venta al cliente final a través de Internet, es decir, el Business to Consumer (B2C). Modelo de negocio que también se desarrolla por las entidades aseguradoras, si bien con las dificultades que las características del sector acarrearán.

En ésta tesis, en una primera parte he querido plasmar la realidad actual en la que se encuentran las empresas dentro del comercio electrónico y más concretamente las entidades aseguradoras, analizado todo ello desde la perspectiva de los modelos de negocio que se adoptan.

La segunda parte de ésta tesis se centra en los principales problemas que surgen a la hora de la comercialización de los seguros por este canal directo, buscando soluciones técnicas y jurídicas a los riesgos que son propios de la comercialización a distancia.

Resum

El comerç electrònic sorgeix amb l'aparició de les noves tecnologies de la informació i la comunicació. Internet és l'escenari on es desenvolupen les operacions comercials, essent les més importants les que fan referència al procés de venda al client final a través d'Internet, és a dir, el Business to Consumer (B2C). Model de negoci que també es desenvolupa per les entitats asseguradores, encara que amb les dificultats que les característiques del sector impliquen.

En aquesta tesi, a la primera part he volgut plasmar la realitat actual en la que es troben les empreses dins el comerç electrònic i més concretament les entitats asseguradores, analitzant tot això des de la perspectiva dels models de negoci que s'adopten.

La segona part d'aquesta tesi es centra en els principals problemes que sorgeixen en el moment de la comercialització de les assegurances per aquest canal directe, buscant solucions tècniques i jurídiques als riscos que són propis de la comercialització a distància.

Summary

E-commerce emerges by the arising of the new information and communication technologies. Internet is the scenario where the financial operations develop. The most important operations are the ones that use Internet for selling to the end customer, Business to Consumer (B2C). This business model is also used by the insurance companies, although the difficulties this sector features leads to.

At the first part of this thesis, I would like to capture the companies present reality about e-commerce, specifically on insurance companies respect, by analyzing this matter from the business model perspective.

The second part of this thesis is focused on the main problems that arise when insurances are sold through this direct channel, and the proposal of legal and technical solutions to the risks this kind of marketing branch brings.

Índice

1. Presentación del problema	9
2. El e-Business	
2.1 Concepto y clases.....	11
2.2 Factores que han contribuido al nacimiento del e-Business.....	13
2.3 Beneficios del e- Business.....	15
3. El Comercio Electrónico B2C (Business to Consumer)	19
3.1 Introducción.....	19
3.2 Modelos de negocio	23
3.3 El Comercio Electrónico en España	25
3.4 Situación de las empresas españolas en la Web.....	34
4. El Comercio Electrónico B2C en el sector asegurador	37
4.1 Modelos de negocio de las entidades aseguradoras.....	37
4.2 Las entidades aseguradoras y el B2C.....	42
5. Presupuestos principales del B2C: un reto técnico y jurídico	47
5.1 Protección de los datos personales en la prestación de servicios electrónicos en el sector asegurador.....	47
5.1.1 La LOPD: Objeto, ámbito de aplicación y principios rectores.....	47
5.1.2 Obligaciones en materia de protección de datos de carácter personal... ..	55
5.2 Sistemas de pago <i>on line</i>	62
5.2.1 Formas de pago.....	62
5.2.2 Mecanismos de seguridad en los medios de pago electrónicos.....	68
5.2.3 Tendencias en el uso de los medios de pago.....	69
5.3 La seguridad en transacciones comerciales a través de la Red: riesgos y soluciones técnicas.....	70
5.3.1 El Principio de Seguridad.....	70
5.3.2. Los riesgos en las transacciones comerciales: soluciones técnicas y jurídicas.....	78
6. Contratación online de seguros	85
6.1 Ámbito normativo.....	85
6.2 El contrato electrónico: conceptos generales y presupuestos.....	86
6.3 Solicitud y propuesta <i>on line</i> del seguro.....	90
6.4 Momento y lugar de perfeccionamiento del contrato de seguro electrónico... ..	93
6.5 La prueba del contrato electrónico.....	95
6.6 El derecho de desistimiento del tomador en el contrato <i>on line</i>	97
6.7 El marco jurídico y sus aplicaciones prácticas.....	98
7. Conclusiones	103
8. Bibliografía	105

El Comercio Electrónico en el sector asegurador

1. Introducción

A través de la presente Tesis se pretende examinar el papel desempeñado por las entidades aseguradoras en el marco del comercio electrónico denominado B2C, entendido éste como proceso de venta de bienes y servicios al cliente final a través de medios electrónicos. Modalidad del Negocio electrónico (*e- Business*) que comprende las operaciones comerciales desarrolladas fundamentalmente a través de Internet.

En concreto, este estudio, tras realizar un análisis de la situación del comercio electrónico en España de las empresas y más concretamente, de las entidades aseguradoras, aborda la problemática de los presupuestos que deben concurrir en las operaciones comerciales: protección de los datos de carácter personal, medios de pago electrónicos y los riesgos técnicos y jurídicos.

En el último capítulo de este trabajo se estudia la contratación electrónica desde una perspectiva jurídica, teniendo en cuenta la diversidad legislativa existente en la materia, así como los problemas que la aplicación práctica de las Leyes acarrearán para las entidades aseguradoras.

2. El e-Business

La economía mundial está en plena transformación, se está pasando de una sociedad industrial a una Sociedad de la información regida por nuevas reglas. Una sociedad en la cual, las tecnologías que facilitan la creación, distribución, acceso, tratamiento y manipulación de la información juegan un papel importante en las actividades sociales, culturales y económicas.

Como consecuencia de la proliferación de cantidad de información, surgen nuevas oportunidades a explorar, transformando la información digital en valor económico y social, con lo que se crean nuevas industrias o se modifican otras.

Desde el punto de vista de la económica global, la Sociedad de la Información o también denominada sociedad del conocimiento, confiere a las Tecnologías de la Información y del Conocimiento (TIC) el poder de convertirse en los nuevos motores de desarrollo y progreso. Tecnologías que se caracterizan por agrupar los elementos y las técnicas utilizadas en el tratamiento y la transmisión de la información, principalmente de informática, Internet y telecomunicaciones.

En este proceso de transformación, el rápido desarrollo de Internet en apenas 5 años, como medio que facilita el acceso e intercambio de información y datos, ha desempeñado un papel muy importante. Lo cierto es que el uso de Internet se ha incorporado a nuestra vida diaria sin darnos cuenta (e-mail, ocio, conocimiento) y nos estamos acostumbrando al uso de nuevas tecnologías a una velocidad insospechada, aunque determinadas aplicaciones, como el comercio B2C (empresa cliente final) no están teniendo el éxito esperado inicialmente.

2.1 Concepto y clases

El Negocio Electrónico o *e-Business*, se refiere al conjunto de actividades y prácticas de gestión empresarial, que resultan de la incorporación a los negocios, de las tecnologías de la información y la comunicación (TIC) y particularmente de Internet, así como a la nueva configuración descentralizada de las organizaciones y su adaptación a las características de la nueva economía, denominada Economía Digital.

El e-Business consiste en utilizar los medios electrónicos para la creación de valor, reorganizando la empresa para que tenga la capacidad de intercambiar bienes, servicios, dinero y conocimiento digitalmente.

Es decir, las actividades que ponen en contacto clientes, proveedores y socios como el marketing y ventas, la producción y logística, gestión y finanzas tienen lugar en el e-Business, a través de redes informáticas que permiten a su vez una descentralización en línea del negocio.

El e-Business es un concepto general que comprende todos los demás relacionados con los medios electrónicos:

➤ **Comercio Electrónico (e-Commerce)**

Es una parte del e-Business, que se refiere al conjunto de actividades alrededor de la comercialización de un producto o servicio en Internet. Este tipo de comercio permite llevar los procesos de promoción, compra, venta y marketing de productos y servicios utilizando Internet. Incluye:

- Comercio Electrónico B2B (Business to Business): es la automatización a través de la Web de los procesos de compra y venta entre empresas.
- Comercio Electrónico B2C (Business to Consumer): es la automatización del proceso de venta al cliente final, a través de Internet. Es decir, es la venta directa que una empresa hace a los consumidores finales, utilizando medios electrónicos. Objeto de estudio en la presente tesis.
- Comercio Electrónico C2C (Consumer to Consumer): Son las subastas en Internet. Consiste en que una persona ofrece un producto y otras pujan por él. El que ofrece el precio más alto se lo lleva.
- Comercio Electrónico C2B (Consumer to Business): Son las subastas inversas en Internet, en las que el cliente fija el precio de compra y la empresa lo acepta o no. Similar al regateo que se realiza en mercadillos.

➤ **E- Business Interpresarial.**

Permite crear valor con otros agentes externos a la empresa. Incluye:

- SCM (Supply Chain Management). Gestión de la cadena de suministros. Permite intercambiar todo tipo de información entre empresas que colaboran para crear valor al cliente final. Permite coordinar los intercambios de información dentro de lo que hemos denominado sistema de valor.
- PRM (Partner Relationship Management). Gestión de las relaciones con los asociados. Este tipo de software se utiliza para intercambiar información con las empresas asociadas.
- Extranet: Redes privadas entre empresas en las que se intercambia información.

➤ **E- Business con el Gobierno.**

Parte del negocio electrónico que permite a la empresa relacionarse eficientemente con las administraciones públicas. Incluye, entre otros:

- B2G (Business to Government). La empresa vende productos o servicios a la administración pública usando Internet.
- G2B (Government to Business). La administración proporciona información a la empresa a través de Internet.

➤ **E-Business Intraempresarial.**

Permite crear valor dentro de la propia empresa. Incluye multitud de tecnologías, entre otras destacan:

- Aplicaciones de Gestión del Conocimiento.
- ERP (Enterprise Resource Planning). Gestión de recursos empresariales. Este tipo de software permite gestionar el interior de la organización, automatizando los procesos internos. En los últimos años ha evolucionado hasta poder ejecutarse a través de la intranet.
- Intranet. Red basada en tecnología Web, técnicamente idéntica a Internet, pero a la que sólo pueden acceder los empleados de una organización. En la misma la empresa ofrece todo tipo de servicios a sus empleados a través de la Intranet (gestión de vacaciones, acceso a datos laborales, gestión de viajes...)
- CRM (Customer Relationship Management o Gestión de las relaciones con los clientes). El e- CRM es la Gestión de las relaciones con los clientes en tiempo real, a través de Internet. Consiste en aplicar el modelo CRM a la Web.

2.2 Factores que han contribuido al nacimiento del e-Business

El Negocio Electrónico o e-Business surge como consecuencia de la aparición de una serie de factores que confluyen al mismo tiempo y contribuyen al desarrollo de los negocios de las empresas. Dichos factores son:

1. Globalización y liberalización del acceso a mercados

Tradicionalmente, el acceso a los mercados transfronterizos ha resultado sumamente difícil debido a las barreras legales, de comunicación y a la insuficiencia o inexistencia de infraestructuras viarias.

En los últimos tiempos esta situación ha cambiado dado que el acceso a dichos mercados, ha resultado posible en parte por la eliminación de las barreras legales, con la creación en la Unión Europea de un mercado interior que crea un espacio sin fronteras interiores, en el que la libre circulación de mercancías y servicios y la

libertad de establecimiento están garantizadas. Lo que a su vez, ha favorecido el acceso a mercados y recursos de todo el mundo.

Con la liberalización del comercio, se produce una mejora de las infraestructuras viarias de transporte y por lo tanto un reducción de los costes y, una mejora de las redes globales de telecomunicaciones.

2. Desarrollo de las nuevas Tecnologías

El otro gran factor que ha contribuido al desarrollo del e-Business ha sido la concurrencia de tecnologías en dos niveles claramente diferenciados. El primero, exterior a la empresa, producido por el creciente desarrollo de las tecnologías de la información y las telecomunicaciones, como medio esencial para eliminar las barreras que separan a la Sociedad. El ejemplo más evidente ha sido la red de redes, Internet.

El segundo nivel, posibilitado por el primero, se ha desarrollado dentro de las propias organizaciones empresariales, y ha consistido en integrar los sistemas de información que gestionaban internamente los procesos internos de negocio con los sistemas que relacionan a la empresa con su entorno exterior, especialmente clientes y proveedores.

En un principio las empresas desarrollaron sus sistemas de información internos con el objeto de soportar sus procesos y mejorar su eficiencia, no obstante dichos sistemas limitaban sus ámbitos de aplicación a un área o departamento de la empresa como administración, producción o ventas. De forma progresiva, esos sistemas aislados comenzaron a compartir información entre ellos para posteriormente integrarse en sistemas más amplios dentro de la empresa. El ejemplo más claro de esta tendencia hacia la integración han sido los ERP's (Enterprise Resource Planning).

Con posterioridad al desarrollo de los sistemas internos, muchas empresas descubrieron que los sistemas de información les permitían mejorar su coordinación con proveedores y clientes. Momento en el que aparece un sector de la industria (del automóvil) los sistemas EDI (Electronic Data Interchange) que constituyen la primera manifestación del comercio electrónico. Sin embargo, y pese a su potencialidad, el desarrollo de estos sistemas quedó limitado a sectores muy concretos debido a sus altos costes y a su complejidad.

Es en los años 90, con el desarrollo de Internet, cuando se dispone por primera vez de un canal de comunicación caracterizado por: su bajo coste, enorme funcionalidad (tanto para clientes corporativos como para individuales) y suficiente flexibilidad para permitir la personalización de la información que se intercambia con cada uno de los clientes. Canal de acceso (Internet) que da lugar al nacimiento del comercio electrónico en sus dos aplicaciones fundamentales: Business to Business (B2B) y Business to consumer (B2C).

Por lo tanto, desde un punto de vista tecnológico, el e-Business es simplemente la integración en el entorno empresarial de los sistemas internos, previamente integrados, que permiten a las empresas dar respuesta a demandas crecientemente personalizadas que le llegan mediante sus sistemas de información externos.

Personalización del consumo

Con la globalización de los mercados, los hábitos de consumo han cambiado. Antes, el cliente sólo podía disponer de productos o servicios tangibles y elaborados de forma masiva. Ahora, este cliente demanda que los productos o servicios que adquiere se encuentren adaptados a sus necesidades, gustos o preferencias. Por lo tanto, busca un producto personalizado, pero además necesita mantener los precios propios de la producción en serie, o sea, precios competitivos.

Esta característica es más propia de la artesanía tradicional, con carácter muy local pero totalmente personalizada. El polo opuesto se encuentra en la producción industrial en serie: recursos globales sin ningún tipo de personalización.

2.3 Beneficios del e- Business

En los últimos años Internet se ha convertido en una ventaja competitiva para aquellas empresas que han dado el salto hacia los negocios *on line*. Los beneficios que este medio ofrece, sólo se limitan a la imaginación y el empeño de los líderes de las empresas.

Algunos de los principales beneficios que las empresas en Internet están alcanzado, son los siguientes:

➤ Mayor captación de clientes

Internet es una herramienta de comunicación global que puede ser utilizada por las empresas para llegar potencialmente a millones de clientes. Este canal habilita a las empresas para brindar atención a sus clientes actuales así como a clientes nuevos. El alcance de cualquier sitio Web depende de la estrategia digital que la empresa haya adoptado. Entre los principales factores de un sitio Web que influyen directamente para captar una mayor cantidad de visitantes se encuentran:

- Percepción de valor por parte de los visitantes
- Buen posicionamiento en buscadores
- Presencia en directorios (en categorías de acuerdo con el ramo de la empresa)
- Versiones en varios idiomas

- Mercadotecnia en línea
- Presencia de la empresa en el mercado

No hay que olvidar que un sitio Web compite con otros miles de Sitios por la atención de los visitantes de la Red, por ello es esencial ofrecer un valor diferenciador del resto para captar la atención de manera significativa.

➤ **Mejora en la atención de los clientes**

Las empresas a través de su página o de un sitio Web, tienen la oportunidad de ofrecer a sus clientes nuevos servicios on line y un sitio Web o una página Web puede incorporar una gran cantidad de herramientas encaminadas a mejorar la atención de los clientes. Algunas de éstas son las siguientes:

- Correo electrónico
- Preguntas Frecuentes
- Herramientas para cotización
- Soporte *on line* (live chat)
- Bases de conocimiento
- Guías prácticas para contratar
- Explicación de la gama de productos

➤ **Mejor comunicación interna**

Una de las características más importante de Internet es la versatilidad con la que cuentan las empresas para establecer comunicaciones internamente o con otros agentes económicos que intervengan o formen parte de su organización empresarial (ej. en el caso de los seguros con sus mediadores o con los corredores).

Característica que puede ser aprovechada por las empresas para implementar soluciones que permitan establecer y organizar de manera más eficiente la comunicación entre colaboradores y directivos. Para este propósito, muchas de las empresas importantes crean intranets (conjunto de aplicaciones que son utilizados de manera interna) con una gran cantidad de servicios para los colaboradores y mediante los cuales, los directivos pueden comunicar y recibir información.

➤ **Reducción de costes**

Otras de las ventajas que ofrece el e-Business es la posibilidad de implantar un Sitio Web para ahorrar costes, dado que esta herramienta permite a la empresa integrar algunos de sus procesos internos de su organización (atención al cliente, venta, publicidad) y le da la posibilidad de llegar a un mercado mucho más amplio.

De esta forma, las empresas pueden realizar publicidad más barata (como por ejemplo catálogos de productos digitalizados que el cliente se pueda descargar), tienen un horario de atención de 24 horas al día y el contacto con el cliente y la venta de productos pueden ser realizados mediante el sitio Web de manera más eficiente.

➤ **Incremento en sus ventas**

La empresa que opta por vender sus productos por Internet, como canal directo y alternativo a los canales tradicionales de ventas, no sólo obtiene grandes beneficios para ella sino también para sus clientes, debido al bajo costo de las transacciones, la comodidad y la rapidez del proceso de contratación on line. De ahí que se diga que el comercio electrónico es una de las herramientas que puede generar un mayor y más rápido retorno de inversión a las empresas.

➤ **Mejora en la imagen corporativa**

Para cualquier empresa, contar con un sitio Web funcional significa una mejora en la percepción por parte de los clientes para la organización. Los consumidores valoran las empresas que procuran utilizar nuevas estrategias y herramientas para brindar un mejor servicio.

➤ **Mayor conocimiento del mercado**

Una función muy importante de los sitios Web es la posibilidad de investigar el mercado del sector en el que actúa, con el fin de tener bases para la mejora continua de su contenido así como de los servicios que ofrece, así como de poder configurar un perfil de los consumidores que se convierten en sus clientes finales. Son numerosas las herramientas que se utilizan para llevar a cabo esta tarea y entre otras podemos señalar las encuestas, grupos de discusión, los formularios, formas de registro de usuario, estadísticas del servidor...

3. El Comercio Electrónico B2C

3.1. Introducción

No cabe duda que, el desarrollo de las nuevas tecnologías de la comunicación y de la información (TIC) ha sido un factor determinante en los cambios que ha experimentado nuestra sociedad en los últimos tiempos. Ello es debido a las opciones ilimitadas que ofrecen estas nuevas tecnologías, como Internet o la Red de redes, inimaginables hace unas décadas.

Internet pone al alcance de la sociedad la posibilidad de comunicarnos con cualquier parte del mundo, de obtener información o escuchar música con el sólo uso de un ordenador y un solo clic. La Red es el escenario donde se realizan las operaciones.

Pero del amplio abanico de operaciones que nos permiten realizar las tecnologías de la información, las más frecuentes y más importantes son aquellas que permiten contratar al consumidor particular, bienes y servicios desde su ordenador. Con lo que nos estamos refiriendo a lo que comúnmente se denomina comercio electrónico B2C (Business to consumer) y que se refiere al proceso de venta de bienes y servicios al cliente final a través de Internet, o lo que es lo mismo, a la estrategia que desarrollan las empresas comerciales para llegar directamente al cliente o usuario final.

Estamos pues, ante un nuevo tráfico jurídico y económico que se caracteriza por el canal que utiliza para su desarrollo: las nuevas tecnologías de la Información y comunicación. Con lo que estamos hablando de tecnologías como las redes cerradas (como el conocido *Electronic Data Exchange*, EDI), el correo electrónico o Internet. De todos los canales electrónicos que existen en el comercio electrónico, nos vamos a centrar en Internet y correo electrónico, por resultar las vías más utilizadas para la contratación con consumidores y usuarios.

Desde un punto de vista económico, el B2C por el medio que emplea para la exteriorización de la voluntad negocial, es una nueva modalidad de contratación que tiene las ventajas propias de la contratación a distancia, pero a su vez, sus inconvenientes. Por un lado, la empresa no tiene límites territoriales por lo que acelera el proceso de contratación (no necesita esperar a la apertura de establecimientos físicos), aumentado sus beneficios operacionales y disminuyendo sus costes de producción.

Por otro lado, los consumidores obtienen una serie de ventajas tales como: mayor rapidez y comodidad a la hora de comprar bienes o contratar servicios (no se han de desplazar con lo que ahorran tiempo), mayor abanico de productos y ofertas actualizados (posibilidad de comparar el mismo producto con el de varios proveedores), integración en la Web de los centros de atención al cliente, y

finalmente que, en principio, los precios son más asequibles (pues los empresarios tenderán a repercutir los menores costes que soportan en sus precios, que de este modo serán inferiores, siempre que haya una situación de efectiva competencia).

En contrapartida, el comercio electrónico presenta los inconvenientes propios de la contratación a distancia. Tradicionalmente se ha mantenido que el mayor peligro al que se enfrenta el consumidor final, es el incumplimiento, total o parcial, por el empresario de su obligación de entrega del bien o de la prestación del servicio. Es decir, que el cliente reciba un producto o servicio defectuoso o no exactamente coincidente con el que el contrató o creyó contratar. Pero en la actualidad, además del riesgo anterior, podemos hablar de otros riesgos igual de importantes para el consumidor: la desinformación o la información incompleta y la dificultad del cliente para adaptarse al nuevo proceso de venta (que depende en gran medida de los países).

En efecto, la contratación a distancia presenta como inconvenientes: la soledad del cliente cuando compra, pues para adoptar su decisión sólo ha dispuesto de los datos que del producto le ha facilitado la entidad en su website o en el Sitio Web, sin que por regla general, se le facilite asesoramiento profesional y/o personalizado; y que por desconocimiento del medio empleado o dificultad para adaptarse al mismo, el cliente en ocasiones adopte sus decisiones irreflexivamente. Riesgos que en el contexto de la contratación a distancia sitúan al consumidor o cliente en una posición especialmente vulnerable.

En el caso de la contratación electrónica, a los inconvenientes enumerados se suma la desconfianza o inseguridad que esta nueva modalidad de contratación suscita en una parte de la sociedad, y que ha sido el factor principal por el que el comercio electrónico no se ha desarrollado según lo esperado. Esta inseguridad provocada por el comercio electrónico es debido a dos tipos de riesgos: riesgos jurídicos y los puramente técnicos.

Como riesgos jurídicos podemos citar:

- La incertidumbre acerca de la validez y eficacia de las transacciones electrónicas,
- La determinación del lugar y el perfeccionamiento de los contratos celebrados por vía electrónica,
- La prueba de los contratos electrónicos,

Como riesgos técnicos, se enumeran:

- El riesgo de que el autor de un determinado mensaje o declaración de voluntad sea suplantado, o el de que el mensaje sea alterado,
- El riesgo de que el emisor o el receptor del mensaje nieguen, respectivamente, haberlo emitido o haberlo recibido,
- El de que el contenido del mensaje llegue a ser conocido por una persona no autorizada

Para intentar remediar en todo lo posible los riesgos referidos, se ha intentado incrementar respectivamente:

- La seguridad jurídica contractual (dirigida a obtener en la contratación electrónica, la válida prestación del consentimiento y la producción de los efectos) a través de la Ley de la Sociedad de la Información y Comunicaciones y el Comercio Electrónico, entre otras leyes.
- La seguridad técnica (para evitar problemas de autenticidad, integridad, confidencialidad y no repudio en la transmisión de la información por la Red) a través de la figura de la firma electrónica, inicialmente regulada por el Real Decreto-Ley 1/1999, y, más tarde, por la Ley de Firma Electrónica de 2003 (en adelante, LFE), que ha derogado la ley anterior.

Conjunto de factores que, por su importancia en el comercio electrónico serán objeto de estudio en los capítulos siguientes dedicados respectivamente, a la seguridad en las transacciones comerciales (riesgos técnicos) y a la contratación on-line (riesgos jurídicos).

Principios generales

A continuación vamos a enumerar los principios que rigen la actividad del comercio electrónico en su modalidad Business to Consumer, que tienen como objetivo principal que el grado de seguridad jurídica del comercio electrónico sea similar o superior al comercio escrito.

1) Principio de equivalencia funcional

Este principio determina que los contratos electrónicos son válidos y eficaces “cuando concurren el consentimiento y los demás requisitos necesarios para su validez”. Por lo tanto, con este principio se equipara en validez y eficacia a los documentos electrónicos con los documentos con forma escrita, siempre que cumplan los requisitos establecidos legamente para que produzcan efectos.

Excepciones al principio:

- a) No se equiparan al documento o contrato solemne, público o notarial salvo disposición legal en contrario.
- b) Por ley puede regularse casos en los que no sea posible la equiparación, está habilitada la exclusión del sometimiento determinados documentos y firmas (inmobiliarias, sucesiones, familia,...).
- c) El soporte electrónico de una declaración viciada no produce el saneamiento de la misma, al igual que el papel escrito.

2) Principio de inalteración del derecho preexistente de obligaciones y contratos privados

En virtud de este principio se establece que la contratación electrónica es un nuevo soporte y vía de transmisión de voluntades contractuales o negociales, y no una parte del derecho regulador de las mismas, por lo que no se altera el derecho aplicable a dichas relaciones con independencia del soporte mediante el cual son contraídas.

3) Principio de neutralidad tecnológica

En relación con el principio de equivalencia funcional y con la finalidad de que la ley favorezca el desarrollo del mercado tecnológico, este principio señala que las normas jurídicas que regulen o modifiquen las instituciones jurídicas tradicionales, para dar cabida a sus homólogas electrónicas o telemáticas, deben ser neutrales desde un punto de vista tecnológico.

Por lo tanto, con la consagración de este principio y la normativa del comercio electrónico se pretende que, el régimen jurídico que regula el mismo no sólo abarque la tecnología existente en el momento en que se formula, sino también las tecnologías futuras, sin necesidad de tener que modificarla en un horizonte cronológico razonable.

4) Principio de buena fe

Principio consagrado en materia civil y comercial desde 1885 (año de promulgación del Código de Comercio), y que se extienden en el tiempo hasta nuestros días.

La buena fe constituye un principio básico en aras a interpretar y ejecutar contratos de compra-venta internacional, y es uno de los fundamentos del régimen jurídico aplicable al intercambio internacional y nacional de bienes y servicios, siendo a este efecto irrelevante que se haya llevado a cabo por medios escritos, verbales o electrónicos.

5) Principio de libertad contractual o de autonomía de la voluntad

Consiste en la posibilidad de que las partes contractuales celebren convenciones de cualquier tipo, aún no reglamentadas expresamente por la ley. No obstante lo dispuesto, la no exclusión de libertad de pacto en la contratación electrónica, surgen diversas excepciones cuyo fundamento se encuentra en el orden público de los Estados, pudiendo resumirse en:

- i) En materia de confidencialidad de los datos electrónicamente intercambiados con fines negociales. En España habrá que estarse a la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal.
- ii) Régimen de responsabilidad contraída por las partes relacionadas electrónicamente y su disponibilidad contractual, ya que no siempre es

posible ni en cualquier relación, por ejemplo entre empresarios y consumidores (B2C: Business To Consumer).

- iii) Régimen de libertad empresarial de establecimiento como Prestador de Servicios de Certificación de firmas electrónicas y el reconocimiento nacional de firmas certificadas en el extranjero, lo que supone un gran freno en el comercio electrónico internacional.

6) Principio de regulación mínima

Establece la conveniencia de evitar que el comercio se regule en exceso, de forma que ponga en peligro la aparición de los nuevos negocios en Internet e impidiendo que se desarrolle la Sociedad de la Información.

3.2 Modelos de negocio

Según el modelo de negocio que desarrollen las empresas podemos clasificar el B2C en las siguientes categorías:

➤ **Intermediarios *on-line***

Los **intermediarios *on-line*** son aquellos que facilitan a las entidades las transacciones entre compradores y vendedores y que, como contraprestación económica reciben un porcentaje del valor de la transacción.

- **Infomediarios:** Son intermediarios que operan en la Red con el objetivo de alinear la oferta y la demanda, por lo que su valor radica en la reducción de costes temporales (menor tiempo de búsqueda) y económicos (costes de la transacción).

Ejemplos: Travelocity.com, Expedia.com...

- **Brokers o Servicios financieros:** Estos portales tienen como objetivo proporcionar una plataforma para la compra y venta de acciones por Internet, para ahorrar tiempo a sus usuarios. Si bien en EEUU estas webs se caracterizan por tener un gran éxito y estar especializadas por productos (hipotecas, operaciones bursátiles...), en España las mismas proporcionan todos los servicios en un mismo sitio.
- **Subastas:** Portales en los que la empresa proveedora de servicios se limita a establecer las reglas de funcionamiento y a cobrar sus comisiones. Son los usuarios los que proporcionan los bienes que se vende, fijan los precios mínimos de los mismos y realizan los envíos.

El ejemplo más claro de este tipo de negocio sin duda alguna viene representado por eBay dado su gran rentabilidad.

En España a lo largo de 2008 la oferta en Internet se ha diversificado cobrando mayor importancia los sitios de subastas que pasan del 16% de compras en 2007 al 25% en 2008,

- **Clasificados:** estas webs obtienen sus ingresos de las cuotas que pagan los usuarios por la inclusión del anuncio en el portal.

Ejemplos: segundamano.com, clasifica.com..

- **Centros Comerciales Virtuales:** Son webs que incluyen tiendas con numerosas ofertas y sus ingresos vienen de las altas, las cuotas mensuales o del cobro de comisiones por las transacciones. El principal problema que presenta este tipo de negocio es la dificultad a la hora de segmentar a los clientes.

➤ Modelos basados en la publicidad

- **Portal Horizontal:** Este tipo de negocio ofrece por un lado, gran cantidad de contenido sobre multitud de temas (política, deporte, noticias, callejeros...) y por otro, numerosos servicios como foros, buscadores, correo electrónico.

Ejemplos: Yahoo!, Terra, Jaztel...

- **Portal Vertical o Vortal.** Son portales temáticos, por lo que su propuesta de valor son los contenidos especializados, el comercio electrónico, los servicios y la comunidad. Esta webs permiten la segmentación de la audiencia por temas o servicios específicos y su objetivo es fidelizar a las personas que estén interesados en un contenido concreto. Por sus características, podemos afirmar que se trata de modelos que a pesar de atraer menor número de usuarios que los portales horizontales, tienen mayor posibilidad de suscribir una venta por visita.

Ejemplos: Amazon, marketingdirecto.com...

- **Comunidad Virtual:** Son webs que reúnen a grupo de personas que tienen intereses comunes, que tienen como finalidad interactuar unos con otros sobre la base de áreas similares de interés.

- Estas empresas ganan dinero por medio de la acumulación de leales usuarios y la orientación con la publicidad.

Ejemplos: pobladores.com, Tripod.com

- **Servicios gratuitos:** Portales que te ofrece numerosos servicios gratuitos (chats, información, callejeros...). Su negocio procede de la publicidad.

Ejemplo: tuportal.com.

➤ Modelos basados en venta

- **Venta on line (e-shop):** Son las empresas que se dedican al B2C puro, por lo que le dan mucha importancia a la atención personalizada. Son las denominadas “.com”.
Presentan como punto débil que sólo tienen un canal de distribución (la Red), por lo que la comunicación con el cliente resulta a veces difícil.

- **Ventas por catálogo:** Negocios de gran expansión en EEUU, que en España durante años han sido calificadas de marginales, si bien en los últimos tiempos están sufriendo grandes cambios, posiblemente por cambio de público objetivo y de los bienes ofertados (gente dispuesta a acceder a moda de marca a precios inferiores)

Un ejemplo clásico de este tipo de webs es Venca.es. En la actualidad, se han creado páginas como Privalia.com (especializada en ropa, complementos y menajes de decoración de primeras marcas, vendidas a precios inferiores a los de la venta *on line*).

- **Vendedores de bist:** comercializan productos y servicios digitales (MP3, fotos, estudios...). Su propuesta de valor está en que la red les facilita la reducción de costes de producción, logística y de tiempo.
- **Vendedores on y off (Clicks&Tricks):** Son empresas que complementan su cana tradicional de venta (venta presencial) con un nuevo canal (Internet), mediante la creación de tiendas virtuales.
Ejemplos: elcorteinglés.com, viajesiberia.com...
- **E-Learning:** Empresas que se dedican a la formación a distancia a través de Internet.
Ejemplos: UOC, IE.

3.3 El Comercio Electrónico en España

Centrado el tema en el negocio electrónico entre empresas y consumidores (B2C), a continuación vamos a analizar la situación en la que se encuentra esta nueva modalidad de negocio en España.

A finales del siglo pasado fuimos testigos del “boom” del comercio electrónico y a su posterior caída al inicio del nuevo por no llegar a las expectativas esperadas.

Lo cierto es que la Red es el futuro y su evolución es irreversible, pero la implementación de estas tecnologías en una empresa, depende

fundamentalmente del sector en el que compite la misma, sin olvidar que la adopción de las tecnologías no implica obtener ventajas competitivas.

¿Que se vende en Internet?

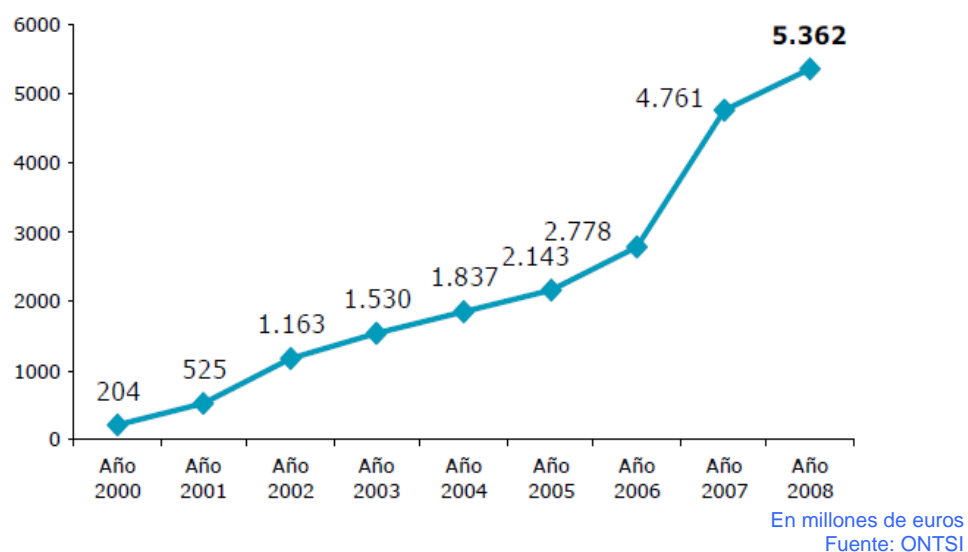
Aunque en un principio se pensó que todo se podía vender por Internet, al final los productos que más éxito tienen son los intangibles (música, películas, billetes de avión...) por lo fácil que es digitalizarlos. En cambio, los productos tangibles como ropa, coches o cosméticos, son más difíciles de vender por la Red por la necesidad que tiene el cliente final de comprobar físicamente que se adaptan a sus necesidades particulares.

Aunque en los últimos tiempos y quizás motivado por la crisis económica, el consumismo y el deseo de las personas de obtener productos de marcas conocidas a precios inferiores, se están creando negocios webs que venden bienes tangibles (ropa, perfumes...), estandarizados y de primeras marcas conocidas (Nike, Levis, DNK) a precios muy competitivos. Ejemplo: Privalia.com

De acuerdo con los últimos datos procedentes del "Estudio sobre Comercio Electrónico B2C 2009" publicado por ONTSI, el comercio electrónico en España crece de forma moderada hasta el año 2006 (pero sostenida) y a partir de ese año se produce un incremento (motivado por la proliferación de las empresas ".com.") hasta finales del 2007 momento en que se produce una desaceleración del consumo.

Según dicho estudio, la cifra del B2C en España durante el 2008, llega a los 5.362 millones de euros, lo que supone un incremento del 12,6% respecto al año 2007 (que registró 4.761 millones de euros).

Volumen de negocio del comercio electrónico B2C



Este crecimiento es debido principalmente:

- Al incremento del número de internautas, que pasa del 53,5% al 58,3% en población de más de 15 años.
- Al aumento del número de compradores *on line* que pasa del 39,8% al 40,3%, hasta alcanzar los 8,9 millones de compradores
- A que el gasto medio por comprador es de 604€.

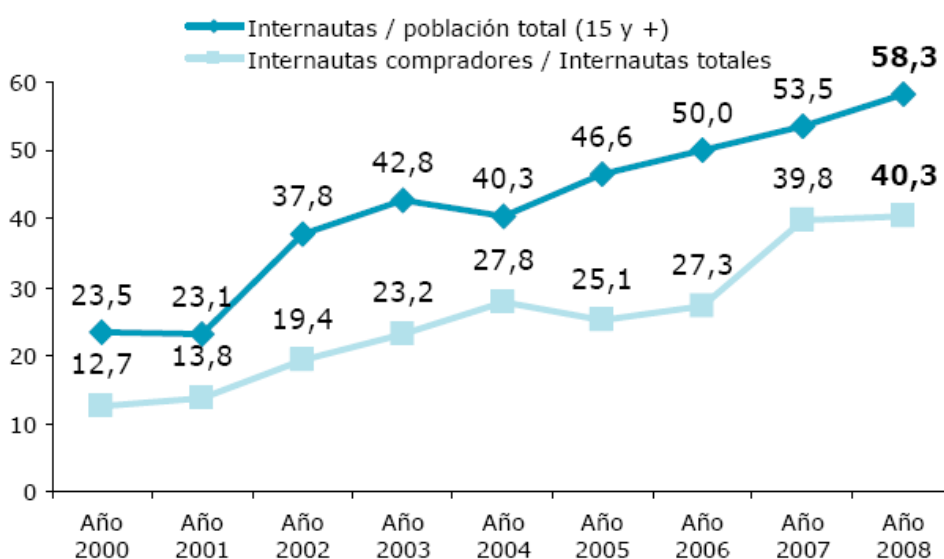
¿Qué perfil tienen las personas que compran en Internet?

El perfil de los compradores on-line responde a las siguientes características sociodemográficas:

- Hombres
- De 25 a 49 años
- Residentes en hábitats urbanos (más de 50.000 habitantes)
- Con estudios universitarios
- De nivel socioeconómico alto y medio alto
- Trabajadores en activo a tiempo completo

El volumen de compradores *on line* se ha visto aumentado en un 11% pasando de casi 8 millones a 8,9 millones de individuos. A pesar de este aumento en el número absoluto de compradores, los compradores a través de Internet han pasado de un 39,8% en 2007 al actual 40,3% —del total de internautas—. Por lo tanto, el motor del aumento en el número de compradores se basa principalmente en la ampliación de la población internauta.

Evolución en el número de internautas e internautas compradores



Fuente: ONTSI

¿Quién utiliza más Internet?

Según el informe, los usuarios de Internet que compraron a través de la Red en 2008, son los que más la utilizan.

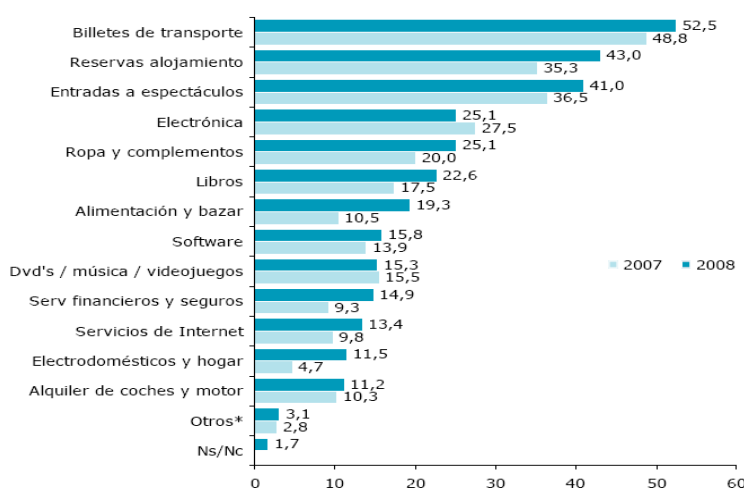
En concreto, el 77% de los compradores declaran que han transcurrido al menos 3 años desde que se conectaron por primera vez, frente al 59% de los no compradores. Y de los compradores on-line, un 86% ha accedido a Internet la última semana, disponiendo de Banda Ancha el 79% de los mismos. De lo que se desprende, que incide positivamente tanto la experiencia como la velocidad de la conexión.

Asimismo, destaca la entrada de nuevos usuarios a la Red, alejados de la tecnología: mayores de 65 años, individuos no activos y jubilados, individuos con estudios primarios o Bachiller elemental y de nivel socioeconómico bajo.

¿Qué compran los españoles en Internet?

Según el informe elaborado por ONTSI, los billetes de transporte (52,5%), las reservas de alojamiento (43%) y las entradas a espectáculos (41%) continúan siendo los productos estrella del comercio electrónico. Ahora bien, los productos que han experimentado un crecimiento más importante con respecto al año pasado son las categorías de alimentación y bazar (con 9 puntos porcentuales más, alcanza el 19,3%), reservas de alojamiento (con 8 puntos más alcanza el 43%) y electrodomésticos y hogar (con 7 puntos más alcanza el 11,5%). Los servicios financieros, entre los que se encuentran las operaciones de seguros y planes de pensiones también ven incrementados su cuota de mercado de manera significativa en 5 puntos porcentuales.

Productos comprados por Internet

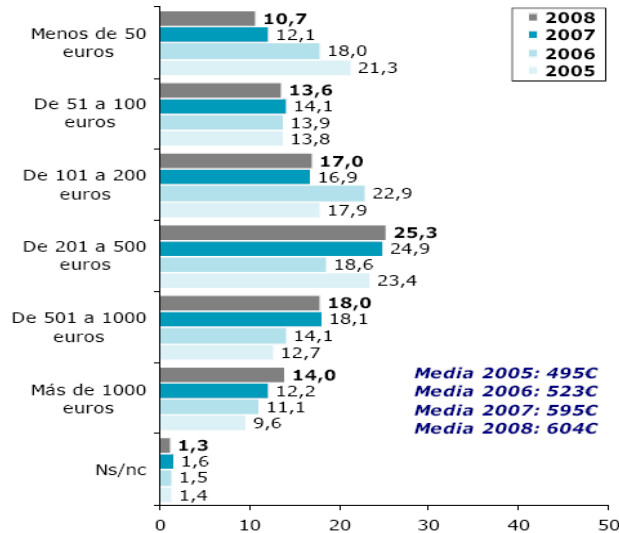


* Incluye juegos de azar/ concursos y redes sociales de pago

Base: Total internautas compradores

¿Cuanto dinero se gastan en Internet los españoles?

Gasto medio en las compras por Internet en el último año



Base: Total internautas compradores

Cada comprador *on line* ha gastado en el 2008 una media de 604€. Este importe medio de compra, se ha incrementado respecto del año anterior en 1,5%, que se situaba en 595€. Por otro lado, hay un 0,9% de los compradores que han realizado gastos que rondan de media los 34.000€ anuales, justificados por inversiones en productos financieros, y que no han sido contemplados en la media global (604€).

Perfil socioeconómico del volumen de compras por Internet

GASTO MEDIO (€)

TOTAL	603,8
--------------	--------------

SEXO

Hombre	573,0
Mujer	649,3

EDAD

De 15 a 24	376,5
De 25 a 34	496,7
De 35 a 49	689,7
De 50 a 64	843,1
65 y más	354,9

HÁBITAT

Menos 10 mil	607,1
10 a 20 mil	669,0
20 a 50 mil	471,8
50 a 100 mil	463,7
+100 mil y cap.	652,1

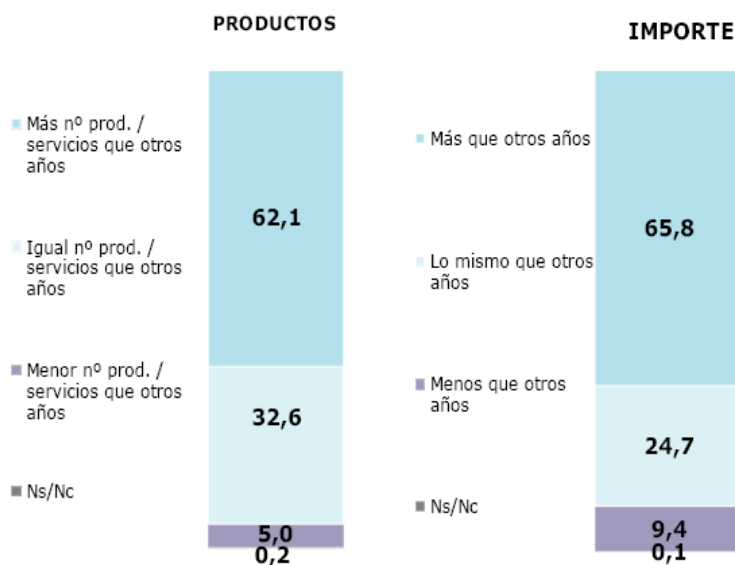
Si se analiza el gasto medio, observamos que existe una diferencia importante entre hombres y mujeres; las mujeres han gastado 75€ más de media en el año 2008.

La variable edad es también discriminante. Los más jóvenes (menores de 25 años) y más mayores (65 o más años) tienen un gasto medio considerablemente inferior, con una media de 377€ y 355€ respectivamente. En cambio, los individuos de 35 a 64 años gastan más que la media. Concretamente, los individuos de 35 a 49 años gastan de media 690€, mientras que los de 50 a 64 años gastan hasta 843€.

En cuanto al tamaño de hábitat, se observa que en las ciudades de tamaño medio (20.000 a 100.000 habitantes) se concentra un gasto medio inferior al resto y a la media nacional.

Por su parte, las personas con estudios universitarios superiores (906€) y los individuos con nivel socioeconómico alto o medio alto (765€), también realizan un consumo medio considerablemente superior al resto de los grupos analizados.

Percepción de cuantía de compras por Internet en 2008 vs. años anteriores



Base: Compradores que además compraron en algún año anterior a 2008

Del análisis por tipo de producto y servicio, respecto al número medio de veces que ha sido adquirido *on line* y al gasto medio anual en el 2008 por comprador (en compradores de dicho producto), se desprende que:

- Los aumentos más destacables del número medio de compras se producen en los servicios financieros y seguros (pasan de 3 a 3,8 veces) y en la categoría de electrodomésticos y hogar (de 4 a 4,5 veces). El promedio de compras de billetes de transporte también crece, aunque de forma más moderada, pasando de 3,2 a 3,4 veces.
- Respecto a los servicios financieros y seguros (fondos de inversión, acciones, seguros médicos, seguros de coche, etc.), cabe destacar, al igual que en otros años, que es el servicio con mayor gasto medio (5.272€), y que este año además, es el tercer servicio más importante en términos de número medio de compra (3,8) y la única categoría de producto o servicio donde los dos indicadores han subido con respecto al año pasado.
- El gasto medio en entradas a espectáculos asciende a 119€, lo que se traduce en un 27% más que el año anterior, segundo incremento en importancia por detrás de los servicios financieros.
- Los juegos de azar y concursos mantienen la primera posición en el número medio de compra, aunque disminuyendo de 8,7 a 7,4 veces. Sin embargo, el gasto medio anual crece un 24% alcanzando los 225€.
- Alimentación y bazar es la quinta categoría más importante en cuanto a número medio de compras (3,6) y gasto medio (237€) realizado en 2008. Con respecto a 2007, no obstante, estos dos indicadores han bajado.

¿Qué medios de pago se utilizan en las compras por Internet?

La mitad de los compradores *on line* (50,2%) prefieren pagar sus compras a través de tarjeta (crédito y débito), pero la preferencia por la tarjeta de crédito se ha reducido notablemente del 39,6% en 2007 al 33,1% en 2008, descenso que viene acompañado del aumento de la preferencia por tarjeta de débito, del 14,4% en el año 2007 al 17,1% en 2008.

Formas de pago por Internet



Base: Total internautas compradores

Conjuntamente consideradas ambas tarjetas, la predilección por las mismas no es tan manifiesta como en años anteriores, puesto que el pago contra reembolso ha aumentado hasta el 29,1% en los últimos años.

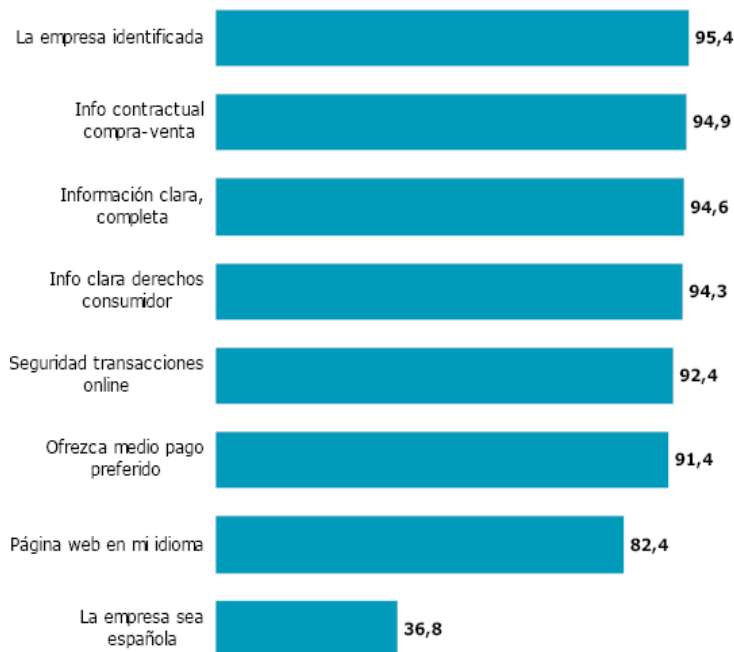
También la tendencia del sistema PayPal es ascendente, con un 10,7% de preferencia en 2008, se duplica con respecto a 2007 (4,5%). Por el contrario las transferencias bancarias son año a año menos atractivas. Ahora sólo el 6,7% lo considera una forma de pago preferida.

¿Qué valoran los internautas a la hora de comprar por Internet?

Respecto a los aspectos más esenciales o más relevantes a la hora de realizar compras *on line*, casi la totalidad de los compradores están de acuerdo en que es esencial que la empresa esté bien identificada y, por supuesto, que ofrezca la posibilidad de contactar con la misma.

También es prioritario que sea clara, completa y entendible la información relativa a temas contractuales de compra-venta, así como también es fundamental que exista información precisa sobre el bien a comprar, sus precios, los gastos que van incluidos o no en la compra, etc. Tampoco obvian disponer de toda la información necesaria para conocer los derechos del consumidor (posibilidad de cancelar la compra, etc.).

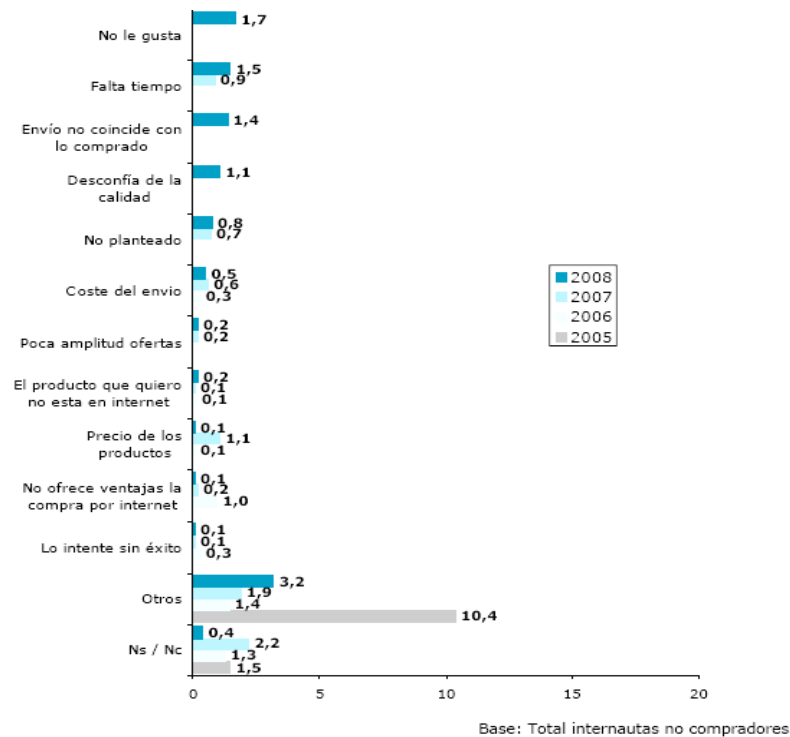
Importancia a la hora de comprar por Internet



Base: Total internautas compradores

En un segundo nivel, los compradores de 2008 consideran fundamental conocer todos los mecanismos que está aplicando la empresa para preservar la seguridad de las transacciones *on line*. De igual forma, es importante que la empresa ofrezca alternativas de medio de pago para que se adecuen al preferido por el comprador.

Razones por las que no se compra por Internet



Por lo general, es la preferencia por las tiendas físicas (34,2%) lo que motiva que los internautas no compraran *on line* durante el año 2008, aunque ha disminuido algo esta causa con respecto a 2007 (38,3%).

Al contrario de lo que ocurrió en el 2007, la desconfianza que suscita Internet en relación a los datos personales o bancarios, es el segundo motivo más citado por los no compradores, desconfianza que también es más patente entre los internautas compradores. En concreto, en 2008 esta actitud ha sido más evidente por:

- La creencia de que la Red es un medio inseguro (28,4% vs. 25,7% de 2007). Tendencia al alza que se viene registrando en esta creencia desde 2005.
- Por mayor desconfianza de los usuarios a la hora de facilitar sus datos personales: 20,3% frente a 14,0%. En cambio, mejora la confianza en los medios de pago, aunque todavía sea una barrera para la compra: esta

desconfianza alcanza al 16,3% de los no compradores en 2008 y alcanzaba al 22% en el año anterior.

Por otra parte, la falta de interés y la ausencia de percepción de necesidad, está suponiendo una barrera menos frecuente, menos del 10% la mencionan.

El desconocimiento y la falta de información han tenido más repercusión que en el año anterior. Y de forma más residual la desconfianza en aspectos logísticos como recepción y devolución de la compra, en cierto modo también se considera una barrera de segundo *orden*.

3.4 Situación de las empresas españolas en la Web

El comercio electrónico en España se encuentra por detrás de la media de la Unión Europea (de los 15 como de la UE-27) en la venta *on line*, con un 8% de penetración y en las compras a proveedores se encuentra con valores ligeramente por encima de la media europea (16%).

En relación a la tipología de los clientes que utilizan Internet como medio para el comercio electrónico, a los que las empresas venden sus productos, destaca en primer lugar la venta a particulares, con el 45% de empresas, seguido por la venta a empresas privadas, con el 38% y a empresas públicas con el 17%.

Un informe de ONTSI relativo a las “Tecnologías de la Información y las Comunicaciones en la empresa española”, indica que en el 2008 sólo el 47,6% de las empresas españolas posee una página Web corporativa, cifra similar a la del año anterior (47,1%). Éstas páginas, son mayoritariamente, de las denominada de presencia o de comunicación, es decir, en ellas solo aparece el nombre de la empresa y contenido informativo.

Ahora bien, el porcentaje de empresas que disponen de página Web corporativa se concentra principalmente en las que tienen 250 o más empleados (86,2%) y en las de 50 a 249 trabajadores (79,1%). En cambio, las empresas que menores cifras alcanzan en la posesión de Web corporativa son las de 1 ó 2 y las de 3 a 5 empleados (42,5% y 45,5% respectivamente). Pero la evolución más positiva entre las empresas con página Web la experimentan las de 6 a 9 empleados, con un incremento de 6,5 puntos porcentuales respecto al pasado año (44,9% en 2008, 51,4% en 2009).

En una visión más amplia de la situación, puede indicarse que existe una relación directa por la que a mayor tamaño de la empresa mayor es el número de las mismas que poseen página Web corporativa.

En Europa (según un estudio de la Fundación Telefónica), la incorporación de Web corporativa en el ámbito empresarial se encuentra en una situación adelantada respecto a la situación de España, que va por detrás de la media UE-

27 situada en el 63% y UE-15 del 66%. Los países nórdicos son los que encabezan la lista de penetración, con valores en torno al 80-85%.

Sin embargo, la tasa de crecimiento para el caso de España ha sido muy positiva en el último año. Según datos de AETIC se ha producido un incremento de 6,6 puntos porcentuales entre 2007 y 2008. En este caso nuevamente hay que hablar de un nivel de dependencia importante de la penetración respecto al tamaño de la empresa.

A nivel sectorial, el sector de la “informática e I+D” se sitúa a la cabeza en la posesión de Web corporativa, con un 75,7%, seguido de “servicios empresariales” (55,9%) y “transporte y comunicaciones” (55%). En cambio, los sectores “servicios financieros y seguros” (41,2%) y “construcción” (41,4%) son los que menores porcentajes registran. Sin embargo, ambas poseen algunos de los porcentajes más elevados en la intención de implantar Web de empresa a corto o medio plazo (el 18,8% y el 15,9% respectivamente).

Desde una perspectiva territorial, las comunidades autónomas que mayores cifras de posesión de Web corporativa poseen son Madrid (53,3%), Cataluña (51,1%) y País Vasco (50,3%). En el lado opuesto se encuentran Galicia (44,7%) y la Región de Murcia (45%).

Por otro lado, en el informe se señala que, aproximadamente el 18,4% de las empresas españolas ha contratado publicidad en Internet en el último año. En términos interanuales esto supone un incremento de 5 puntos porcentuales. Además este crecimiento se percibe en todos los tamaños de empresa y sectores. La publicidad se inserta principalmente en portales específicos de su actividad y en portales de uso general, contando ambos tipos con una cuota muy parecida y constituyendo entre ambos las dos terceras partes del total.

Señala el documento que los motivos que frenan el avance del comercio electrónico entre las empresas españolas destaca la inseguridad, con el 62,4% de empresas, seguido de que los productos no son adecuados para el comercio electrónico, con el 38,2%.

Actualmente, el 63% del tejido empresarial indica que su página Web es segura. Esta cifra significa continuar con la tendencia de ascenso en la conciencia de la necesidad de que las páginas sean seguras. En concreto, puede apreciarse una subida de 4,2 puntos porcentuales con respecto al 2008 (58,8%). En cuanto al desconocimiento acerca de si la página Web es segura o no, al igual que en el estudio precedente, cabe considerar que el porcentaje es similar al registrado el año anterior (18,1%).

Asimismo el número de empresas que afirman que su Web no es segura ha descendido este año en 4 puntos porcentuales (el 22,9% en 2008 frente al 18,9% actual).

4. El Comercio Electrónico B2C en el sector asegurador

4.1. Modelos de negocio

Internet es la herramienta tecnológica de comunicación que permite a las empresas dirigir sus negocios de forma distinta. En este sentido, este canal de comunicación ofrece a las empresas grandes oportunidades para acercarse más sus clientes y poder ofrecerles: información transparente, diversidad de productos, precios competitivos, seguridad, velocidad y confidencialidad

Por ello, las entidades aseguradoras en España están desarrollando diversas alternativas de negocio en Internet, en función de los productos que ofrecen y de las características de su red comercial. Modelos de negocio que suponen, la reorientación de los productos, la reorganización de los procesos internos de las entidades y la adaptación a las TIC de los sistemas de transferencia de información.

Según el “X Informe de Capgemini sobre el Sector Asegurador” de Capgemini tradicionalmente se distinguen cuatro modelos de negocio en el sector asegurador:

- **Entidades multirramo** (o también denominadas compañías tradicionales).
Con esta denominación se engloba a las entidades que operan fundamentalmente *off line* y utilizan Internet como medio de comunicación a través de su página Web.

No obstante, en los últimos tiempos se está observando una evolución hacia los servicios *on line* destinados a los mediadores y peritos.

- **Entidades de operadores-banca seguros**
Este modelo de negocio comprende a las entidades bancarias que junto a los servicios bancarios, ofrecen servicios *on line* relativos a los seguros, operando casi exclusivamente a través de la red.
- **Aseguradoras *on line* o de directo**
Se refieren a aquellas entidades que actúan exclusivamente a través de Internet, comercializando sus productos y servicios. Sus páginas webs tienen como objetivos: una publicidad muy directa y sencilla y, que sean el soporte de sus ventas en líneas.
- **Los mediadores on-line** (brokers on-line o agentes).
Son mediadores virtuales creados para funcionar en línea. Tienen las mismas características que cualquier aseguradora *on line* pero adaptadas al negocio de la mediación.

No obstante, si analizamos las aseguradoras españolas, en función del papel que Internet desempeña en relación a sus productos y sus canales de distribución, podemos diferenciar los siguientes modelos de negocio (según fuentes de ICEA):

➤ Internet como medio de comunicación

Son modelos que utilizan Internet como medio de comunicación, de ofrecer información a través de la Red. Son cada vez menos, las entidades que no han pasado al nivel siguiente. Todas las aseguradoras cuentan con página Web, que utilizan mayoritariamente como canal de información.

Características

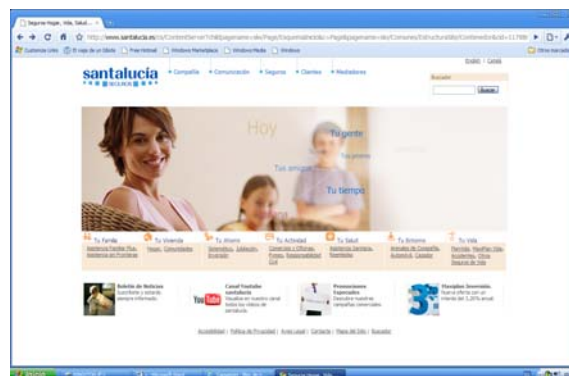
- Es el nivel inicial de un negocio en Internet.
- La website funciona como ventana de la empresa: se da información sobre la entidad, los productos, la red comercial...
- Es el primer paso para continuar con otras actividades en Internet.

Implicaciones

- 1) Operativas: este modelo no tiene implicaciones operativas directas, sólo la generación y actualización de contenidos para la website, que debe ser complementarios y coherentes con la comunicación *off line*.
- 2) De canal: No genera conflictos con otros canales y puede resultar beneficioso la utilización de la website para facilitar información relativa a los intermediarios.
- 3) Inversión: Esta primera fase no requiere una gran inversión que estará en función del diseño, las funciones o la complejidad técnica de la página Web.

Aplicaciones

Las aplicaciones se centran en facilitar información a los interesados y supone aumentar la transparencia informativa de la empresa.



Ejemplos: Santa Lucía, Axa

➤ Internet como herramienta de marketing

Son aquellas modalidades de negocio que adoptan las entidades que utilizan la Red como herramienta de marketing, sin olvidar su función de comunicación.

Características

- Modelo que concibe Internet como una ampliación de su negocio, aprovechando la Web para dar servicio a sus clientes, tanto a tomadores/asegurados, como a mediadores.
- La Web de la entidad aporta directamente valor al cliente (ventajas por ser cliente y utilizar la Red) a través de la información, servicios, herramientas y soporte.
- Es útil para la captación y fidelización de los clientes.

Implicaciones

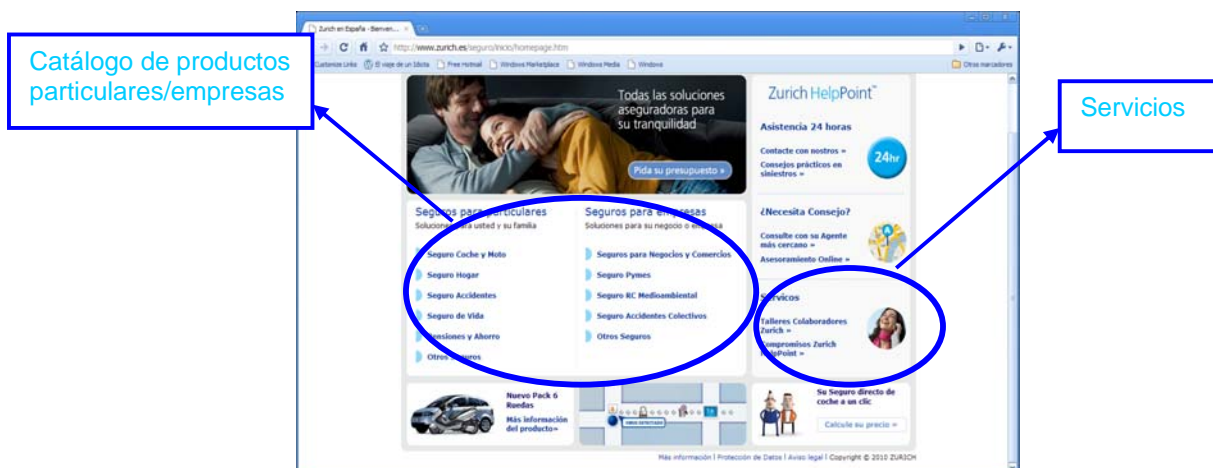
- 1) Operativas: Aumentan y se han de coordinar. Se debe crear un nuevo departamento que gestione todo lo relacionado con la Web y se integre en el resto de departamentos de la organización.
- 2) Canal: Es considerado un cliente más, por lo tanto los servicios de la Web también se dirigen al mismo. De esta forma, los mediadores obtienen un beneficio directo al establecer una relación directa con la entidad y un beneficio indirecto con el marketing que hace la aseguradora.
- 3) Inversión: Tiene un efecto positivo en la cuenta de resultados. Produce un aumento de los ingresos (por incremento de las ventas *off line* y la fidelización) y una disminución de costes por el uso de la Red en determinados servicios (tramitación de siniestros, atención al cliente...).

Aplicaciones

Las aplicaciones se multiplican y se integran en todas las áreas de la empresa. Entre otras, son aplicaciones:

- Difundir y reforzar la imagen de empresa
- La comunicación con clientes y la red de ventas
- Fidelización de clientes
- Marketing al cliente final y al canal
- Posibilidad de integrar procesos como las contrataciones y la tramitación de siniestros.

Ejemplos: Zurich, Ocaso, Mapfre...



➤ Internet como canal de ventas

Se trata de un modelo que apuesta por Internet como una parte imprescindible del negocio.

Características

- El negocio de la Red se integra en los departamentos de la empresa y con los procesos internos.
- Se produce una segmentación de los clientes para atender con mayor eficacia sus necesidades y requerimientos.
- Favorece la captación de nuevos clientes.

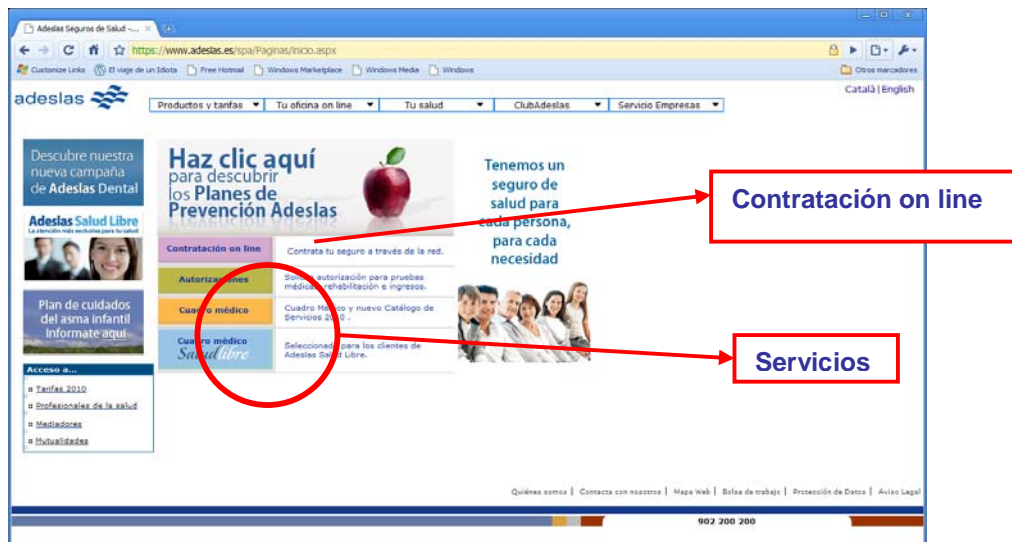
Implicaciones

- 1) Operativas: Requiere la coordinación interna entre departamentos y externa con el canal, así como una buena comunicación y marketing.
- 2) Canal: A través de la Web recibe información de la empresa y de los clientes.
- 3) Inversión: El canal directo debe contribuir con otros canales a la venta de seguros, sin que se produzca canibalismo entre los distintos canales de la entidad.

Aplicaciones

Las aplicaciones van desde las vistas anteriormente hasta el establecimiento definitivo de un canal de venta directa.

Ejemplos: Sanitas, Adeslas, Groupama...



➤ Brokers on line

Resulta de la aplicación a Internet del modelo comercial de los brokers tradicionales de seguros.

Características

- Se surte de diferentes proveedores para ofrecerle al cliente distintas alternativas que se adapten a sus necesidades.
- La Red permite que sea el cliente el que realice la comparación y decida entre las opciones ofrecidas.

Implicaciones

- 1) Operativas: Se centra en operativas relativas a Internet y en el aprovechamiento de las tecnologías.
- 2) Canal: El broker, es un intermediario por lo que mantiene una estrecha relación con los clientes y los proveedores.
- 3) Inversión: Se produce una inversión importante, dado que la tecnología es la vía de comunicación con el cliente y los proveedores.

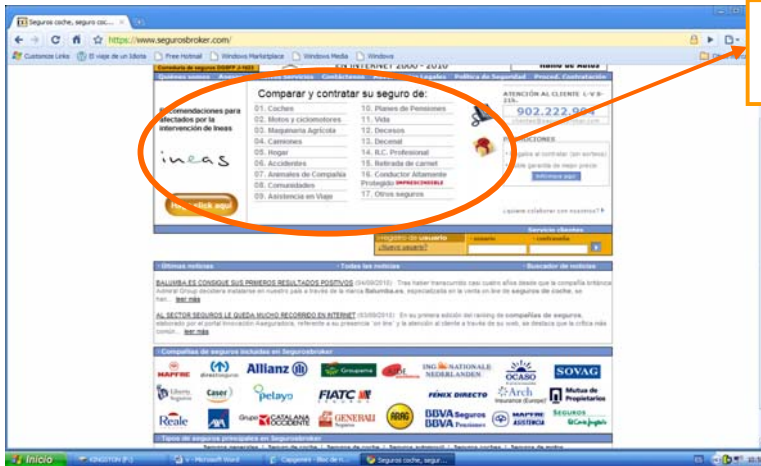
Aplicaciones

Las aplicaciones son muy diversas y siempre dirigidas a conocer y satisfacer las necesidades de los clientes, podemos señalar a título de ejemplo las siguientes inversiones:

- Segmentar a los clientes
- Ofrecer productos ajustados a las necesidades del cliente

- Selección de productos de los distintos proveedores

Ejemplos: SegurosBrokers, Lapoliza...



Comparativa de productos y contratación on line

4.2 Las entidades aseguradoras y el B2C

Cuando hablamos de comercio electrónico (y por extensión de Internet) no podemos olvidar que estamos refiriéndonos a un medio que hace 10 años prácticamente no existía y que en los últimos 5 años se ha desarrollado de forma espectacular: hoy día hay más de 1.300 millones de personas conectadas a Internet en todo el mundo, existen 190 millones de servidores Web y más de 12.000 millones de páginas. Estamos ante una realidad social y económica de la que necesariamente se ha de formar parte.

Por ello, no hay negocio que por pequeño o sofisticado, especializado que sea cuya presencia en Internet no suponga una ventaja. En España hay más de 9 millones de internautas compradores, que crecen exponencialmente a medida que la población nativa va alcanzando madurez.

En España, el mercado de seguros on-line en comparación con otros sectores es todavía escaso. Las entidades aseguradoras están presentes en la Red, si bien por la complejidad del negocio tienen un menor nivel de desarrollo que otras entidades del sector financiero (como bancos o agencias de valores). A pesar de ello, la situación está empezando a cambiar dado que las principales aseguradoras, empiezan a tener presencia en la Red de redes.

Así, destacan entidades como Mapfre que crea la "Oficina Internet Particulares" y que permite a los clientes realizar distintos servicios (consultar, gestionar..) en relación a sus seguros o producto. Por su parte Aegon, resulta un claro ejemplo de empresa que pasa de utilizar Internet como herramienta de marketing a canal de venta directa, cambiando su estrategia.

De hecho según un estudio de Capgemini, existe un notable crecimiento de las funcionalidades online de las aseguradoras. Así, la contratación online ha pasado del 37,5% al 75% en los últimos diez años. No obstante, Internet es un canal complementario para el 40% de las entidades mientras que para el 32% es una red que compite con otros canales de la aseguradora.

Internet se concibe mayoritariamente como un canal de comunicación con clientes, tanto actuales como potenciales, que contribuye a mantener o incrementar la relación con aquellos usuarios que ya son clientes de la compañía. Casi el 60% de las entidades define como objetivo de Internet el acceder a nuevos segmentos de clientes. Sólo un 40% considera que Internet es un medio para mejorar el posicionamiento de ramos o productos estratégicos. Algunas aseguradoras identifican otros objetivos como la innovación y el incremento de la eficiencia así como mejorar la notoriedad de marca de las entidades.

Asimismo, se señala en el referido informe que actualmente el sector asegurador se halla inmerso en una doble transición:

- 1) La transformación del actual modelo de negocio basado en la prestación parcial de servicios online, en un modelo en el que el canal Web ofrezca circuitos de actuación completamente online.

Transformación que las entidades aseguradoras realizan en cumplimiento de la obligación contenida en la Ley 56/2007 de Impulso de la Sociedad de la Información (artículo 2), de poner a disposición de sus clientes de un medio de interlocución telemática (mediante el uso de certificados reconocidos de firma electrónica) que permita la contratación electrónica y la realización de otras operaciones a través de Internet, sin perjuicio de la utilización de otros medios de comunicación a distancia.

En dicho precepto se hace referencia a operaciones como la contratación *on line*, la modificación y finalización o rescisión de los correspondientes contratos, así como cualquier acto o negocio jurídico con los tomadores del seguro, sin perjuicio de lo establecido en la normativa sectorial y, sin que ello afecte a productos que por su complejidad no puedan ser comercializados por Internet.

En cumplimiento de dicha ley, las aseguradoras están realizando un importante esfuerzo para implementar el canal on line, que es una prioridad para el 70% de las mismas.

Para que esto sea una realidad es necesaria la adopción generalizada, tanto por parte de las entidades como de los usuarios, del DNI electrónico y de la firma digital. De las 47 entidades que participan en la encuesta un 40% de las entidades ya han incorporado el DNI electrónico, y de entre ellas, cinco de las 28 compañías multirramo han incorporado el acceso con DNI electrónico o

firma digital (casi un 18%). El resto de aseguradoras, un 50% prevé incorporarlo en los próximos dos años.

Esta evolución resulta beneficiada por dos tendencias generales del mercado: el incremento en el número de usuarios de Internet y de visitas a los websites de las aseguradoras, y el incremento de los usuarios que tienen un certificado digital de firma electrónica (casi un 30%, un 5% más que en 2008).

- 2) Por otro, se pretende pasar de un modelo transaccional a uno colaborativo mediante el uso de las tecnologías Web 2.0 (wikis, marshups, foros...). La incorporación de estas tecnologías todavía es reducida pero efectiva en el sector, destacando Santa lucía y Mutua Madrileña en segundo lugar.

Los servicios online para clientes que un 62,5% de las webs del sector ofrecían en el año 2000, en la actualidad alcanzan el 80%, en el caso de tarificación y, casi el 70% para la declaración de siniestros online. *“La totalidad de las compañías participantes en la encuesta manifiesta contar con servicios a colaboradores y mediadores a través de Internet”*. Estos servicios se prestan a través de los websites públicos (70%) o mediante websites específicos para colaboradores y mediadores (30%).

Respecto a la captación por Internet, el informe refleja que, si bien para la mayoría de entidades el canal genera todavía menos de un 5% de su negocio, un 23% ha cerrado el año con más de un 10% de sus pólizas de nueva producción captadas por Internet. Asimismo, se indica que *“el análisis comparativo de los últimos 4 años revela que la captación a través de Internet va ganando terreno. Cada año son menos las compañías que obtienen menos del 1% de su negocio por Internet, al contrario de lo que ocurre con las que captan entre un 3% y un 5% o más de un 10%, que son cada vez más”*.

Por otro lado, el Informe de 2009 de “Seguros y Fondos de Pensiones” elaborados por la Dirección General de Seguros y Fondos de Pensiones, extrae en relación al canal “Portal de Internet” las siguientes conclusiones:

“La utilización de Internet para la promoción y también para la contratación en línea continúa su implantación. No obstante, los resultados obtenidos no están en consonancia con las expectativas de volumen de negocio previstas, ya que únicamente el 0,41 por ciento del total de primas de cartera han sido conseguidas por este medio, y en cuanto a la nueva producción, este canal tiene una cuota del 0,31 por ciento, lo que indica que no acaba de implantarse como medio alternativo a la contratación tradicional.”

DISTRIBUCIÓN PORCENTUAL DE LAS PÓLIZAS DEL NEGOCIO VIDA Y NO VIDA POR CANALES

PÓLIZAS	VIDA		NO VIDA	
	VOLUMEN CARTERA	NUEVA PRODUCCIÓN	VOLUMEN CARTERA	NUEVA PRODUCCIÓN
Agentes exclusivos	15,54	11,82	43,10	34,99
Agentes vinculados	0,49	0,58	2,00	5,60
OBS-exclusivos	21,49	19,59	3,57	4,98
OBS-vinculados	47,17	57,27	9,92	13,33
Corredores	3,59	2,11	19,59	25,09
Oficinas de la Entidad	9,21	7,27	16,67	8,72
Portal de Internet	0,09	0,29	0,68	1,42
Otros Canales	2,43	1,06	4,47	5,88

DISTRIBUCIÓN DE LA CARTERA y NUEVA PRODUCCIÓN
POR PRIMAS Y CANALES*

	VIDA				NO VIDA			
	CARTERA	%	NUEVA PRODUCCIÓN	%	CARTERA	%	NUEVA PRODUCCIÓN	%
Agentes exclusivos	3.880	13,90	2.076	10,97	11.357	35,70	1.855	31,63
Agentes vinculados	98	0,35	48	0,25	558	1,75	80	1,36
OBS-exclusivos	6.883	24,66	4.785	25,28	824	2,59	206	3,51
OBS-vinculados	11.222	40,21	8.733	46,13	1.993	6,26	662	11,29
Corredores	1.763	6,32	862	4,55	9.062	28,49	2.146	36,59
Oficinas de la Entidad	3.307	11,85	2.104	11,12	6.164	19,38	573	9,76
Portal de Internet	5	0,02	4	0,02	238	0,75	72	1,23
Otros Canales	748	2,68	317	1,68	1.615	5,08	271	4,63
TOTAL	27.906	100,00	18.929	100,00	31.811	100,00	5.866	100,00
AGENTES DE SEGUROS+ CORREDORES	5.741	20,57	2.985	15,77	20.977	65,94	4.081	69,57
OBS (exclusivos + vinculados)	18.105	64,88	13.518	71,41	2.817	8,85	868	14,80

(*) Datos en millones de euros

5. Presupuestos principales del B2C: un reto técnico y jurídico

Cuando una entidad aseguradora quiere vender sus productos o servicios a través de la Red, tres son las cuestiones que principalmente se plantea:

1. Protección de los datos de carácter personal de los consumidores o usuarios.
2. Formas de pago.
3. La seguridad en las transacciones comerciales: riesgos y soluciones técnicas y jurídicas.

5.1 Protección de los datos personales en la prestación de servicios electrónicos en el sector asegurador

En una sociedad donde la forma tradicional de realizar operaciones comerciales está siendo reemplazada por métodos electrónicos, resulta de suma importancia contar no sólo con la tecnología, sino con un marco legal que dote de mayor seguridad la transmisión de datos realizados por cualquier canal, en especial si se realiza por Internet.

Es precisamente el desarrollo y aplicación de las nuevas tecnologías, lo que ha contribuido al aumento del número de tratamientos de los datos personales de los usuarios que interactúan con las entidades a través de red. Por lo que nos encontramos ante la necesidad de equilibrar la balanza entre la implementación en las empresas de las nuevas tecnologías de la información y el derecho de los consumidores a la libre disposición de sus datos personales, contexto en el se que consagra el derecho fundamental a la protección de los datos de carácter personal.

Este derecho a la protección de los datos personales, es un derecho fundamental que deriva directamente de la Constitución Española (en adelante CE), en virtud del cual se atribuye a los ciudadanos un poder de disposición sobre los mismos.

En efecto, la CE consagra en su artículo 10 el derecho de la dignidad de la persona como fundamento del orden político y la paz social. Posteriormente, el artículo 18 del mismo cuerpo legal, tras *“garantizar el derecho al honor, a la intimidad personal y familiar y a la propia imagen”*, dispone que *“la ley limitará el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos”*. De ambos preceptos se deriva el derecho fundamental a la protección de datos de carácter personal regulado en la Ley Orgánica de Protección de datos de carácter personal 15/1999 (en adelante LOPD).

Los datos de carácter personal a la vista de la regulación vigente se pueden definir como “*cualquier información numérica, alfabética, gráfica, fotográfica, acústica o de cualquier otro tipo concerniente a personas físicas identificadas o identificables*”. Es decir, datos tales como el nombre y apellidos, el nº del Documento Nacional de Identidad, la fecha de nacimiento, la dirección de correo electrónico... son datos que identifican a una persona directa o indirectamente.

Por consiguiente, son aquellos datos que circulan por la Red cuando el usuario/cliente accede a la Web de una entidad aseguradora y realiza cualquier operación comercial, y que deben protegerse de cualquier agresión o uso indebido y/o fraudulento, sin olvidarnos del derecho del usuario a disponer libremente de sus datos.

Jurídicamente esta protección se articula a través del principio de participación del usuario que comprende, a su vez, una serie de derechos y principios como son: el derecho a conocer la finalidad de la recogida o tratamiento de sus datos, a ser informado de forma clara, precisa e inequívoca de la existencia del fichero automatizado de datos de carácter personal, a que se solicite su consentimiento para disponer de sus datos....

En definitiva, lo que se pretende instrumentar es la protección jurídica de los datos de carácter personal a través de la LOPD, que recoge los principios, derechos y medidas que se han de adoptar como garantía y que vamos a ver a continuación.

5.1.1 La LOPD: Objeto, ámbito de aplicación y principios rectores

En desarrollo del derecho fundamental a la protección de los datos personales, fue aprobada la Ley Orgánica 5/1992, de 29 de octubre, de regulación del tratamiento automatizado de datos de carácter personal (LORTAD). Ley que ha sido derogada por la actual Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, en virtud de la transposición a nuestro derecho de la Directiva 95/46/CE del Parlamento Europeo en materia de protección de datos personales. Ley desarrollada posteriormente por el Reglamento de desarrollo de la LOPD, aprobado por el Real Decreto 1720/2007, de 21 de diciembre.

➤ Objeto

El objeto de la LOPD extiende su protección, en lo concerniente al tratamiento de los datos personales, a todas las libertades públicas y derechos fundamentales de las personas físicas, y especialmente, al honor e intimidad personal y familiar.

Ley que presenta dos niveles de protección:

- **Jurídico**, relativo al tratamiento de los datos, a las cesiones y a la información que debe facilitarse al titular de dichos datos.

En la práctica contractual del sector asegurador, se traduce en la firma por parte del tomador/asegurado de las cláusulas de protección de datos que incorporan los contratos o formularios de salud, autorizando el tratamiento y cesión de datos.

- **Informático o técnico**, integrado por el conjunto de medidas de seguridad que deben implementarse en los ficheros automatizados y los no automatizados.
Lo que implica que, en las entidades aseguradoras se deba establecer un sistema de seguridad compuesto por un conjunto de procedimientos técnicos y normas de comportamiento de las personas que intervienen en los sistemas informáticos.

➤ **Ámbito de aplicación de la ley**

La LOPD distingue entre:

1. **Ámbito objetivo:** se establece genéricamente que esta Ley será aplicable *“a los datos de carácter personal registrados en soporte físico, que los haga susceptibles de tratamiento, y a toda modalidad de uso posterior de estos datos por los sectores público y privado”* (art. 2.1).

Asimismo, se establece que la Ley será de aplicación con carácter supletorio, en lo no previsto por la legislación especial, a los siguientes ficheros (art. 2.3):

- Los regulados por la legislación de régimen electoral.
- Los que sirvan a fines exclusivamente estadísticos.
- Los que contengan los informes personales de calificación a que se refiere la legislación del régimen del personal de las Fuerzas Armadas.
- Los derivados del Registro Civil y del Registro Central de penados y rebeldes.
- Los procedentes de imágenes y sonidos obtenidos mediante la utilización de videocámaras por las Fuerzas y Cuerpos de Seguridad.

2. **Ámbito territorial**

La ley resultará de aplicación (art. 2.1 in fine):

- Cuando el tratamiento sea efectuado en territorio español en el marco de las actividades de un establecimiento del responsable del tratamiento.
- Cuando el responsable del tratamiento no establecido en territorio español le sea de aplicación la legislación española en aplicación de norma de Derecho Internacional Público.

- Cuando el responsable del tratamiento no esté establecido en territorio de la Unión Europea y utilice en el tratamiento medios situados en territorio español, salvo que los mismos se utilicen únicamente con fines de tránsito. En este caso, se deberá designar representante en España.

3. Ficheros o tratamientos excluidos (art. 2.2)

El régimen de protección de los datos de carácter personal establecido en Ley Orgánica no será de aplicación a:

- a. Los ficheros mantenidos por personas físicas en el ejercicio de actividades exclusivamente personales o domésticas.
- b. Los ficheros sometidos a la normativa sobre protección de materias clasificadas.
- c. Los ficheros establecidos para la investigación del terrorismo y de formas graves de delincuencia organizada. No obstante, en estos supuestos el responsable del fichero comunicará previamente la existencia del mismo, sus características generales y su finalidad a la Agencia Española de Protección de Datos.

➤ Principios rectores de la protección de datos

Los principios que rigen la protección de los datos de carácter personal se encuentra contenidos principalmente en la LOPD y en el Reglamento que la desarrolla.

Dichos principios se centran principalmente: en la obtención de los datos, la información a facilitar a su titular cuando se solicitan los mismos, la prestación del consentimiento a la recogida y tratamiento, así como qué dato deben recabarse en función del servicio requerido, estableciendo niveles de protección distintos en función de su naturaleza.

Los principios que inspiran las políticas de garantía y protección de datos personales son:

1. Calidad de los datos (art. 4 LOPD).

Principio que establece que los datos de carácter personal sólo podrán ser recogidos y tratados, cuando sean adecuados, pertinentes y no excesivos para el cumplimiento de las finalidades (determinadas, explícitas y legítimas) del fichero. Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

En este sentido, los datos deben tratarse para la finalidad para la que se han recogidos, si bien no se considerará incompatible el tratamiento posterior de estos datos con fines históricos, estadísticos y científicos.

Los datos personales deben ser exactos y mantenerse al día para que respondan con veracidad a la situación actual del afectado.

Ahora bien, si los datos de carácter personal sometidos a tratamiento resultaran ser inexactos, en todo o parte, o incompletos, serán cancelados y sustituidos de oficio por los correspondientes datos rectificadas o completados, en el plazo de diez días desde que se tuviese conocimiento de la inexactitud.

Los datos de carácter personal serán cancelados cuando hayan dejado de ser necesarios o pertinentes, y no se conservarán de forma que permitan la identificación del interesado durante un periodo superior al necesario para la finalidad en base a los cuales fueron recabados.

2. Derecho de información

El responsable del fichero en el momento de la recogida de los datos, está obligado a establecer los mecanismos que informen a los interesados de lo siguiente:

- La existencia de un fichero al que se incorporarán los datos solicitados, de la finalidad para la que se recogen y de los destinatarios de la información.
- El carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
- Las consecuencias de la obtención de los datos o de su negativa a suministrarlos.
- La posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición.
- La identidad y dirección del responsable del tratamiento o, en su caso, de su representante.

Esta información debe ser realizada, de forma expresa, inequívoca y precisa. Por lo tanto no es admisible una información genérica que no indique la finalidad y quién está recabando los datos. Este deber de información deberá realizarse por un medio que permita acreditar su cumplimiento, debiendo conservarse durante todo el tiempo que se traten los datos del interesado.

En caso que los datos de carácter personal no hayan sido recabados directamente del interesado, éste deberá ser informado de forma expresa, precisa e inequívoca, por el responsable del fichero o su representante, dentro de los tres meses siguientes al momento del registro de los datos, salvo que hubiera sido informado con anterioridad.

No obstante, no deberá cumplirse con el requisito de informar con posterioridad al interesado, en los casos siguientes:

- Cuando una ley lo prevea.
- Cuando el tratamiento tenga fines históricos, estadísticos o científicos.
- Cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados en consideración al número de interesados o a la antigüedad de los datos.

3. Consentimiento del afectado (Art. 6 LOPD)

El consentimiento es la manifestación de voluntad, libre, inequívoca, específica e informada, en virtud de la cual el interesado consiente el tratamiento de los datos personales que ha facilitado.

Para poder utilizar los datos personales de un persona, la ley exige que se recabe el consentimiento consciente e informado de su titular. Lo que implica que el consentimiento del afectado deberá ser precedido por el cumplimiento del principio de información.

Sin embargo, la prestación de dicho consentimiento presenta las siguientes excepciones:

- Cuando una ley disponga otra cosa
- Cuando los datos de carácter personal se recojan para el ejercicio de las funciones propias de las Administraciones públicas en el ámbito de sus competencias.
- Cuando los datos se refieran a las partes de un contrato o precontrato de una relación comercial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento.
- Cuando el tratamiento de los datos tenga por finalidad proteger un interés vital del interesado y éste se encuentre física o jurídicamente incapacitado para dar su consentimiento.
- Cuando los datos figuren en fuentes accesibles al público y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero.

Excepción que no exime de la obligación de informar ni permite el tratamiento de cualquier dato, sino únicamente de aquellos que sean adecuados, pertinentes y no excesivos (principio de calidad)

No obstante haberse prestado el consentimiento por el afectado, éste podrá revocar el mismo a través de un medio sencillo, gratuito y que no implique ingreso alguno para el responsable del fichero o tratamiento. En cuyo caso, el responsable cesará en el tratamiento de los datos en el plazo máximo de diez días a contar desde la recepción de la revocación del consentimiento, sin perjuicio de su obligación de bloquear los datos conforme a la Ley.

Por último, en caso de menores de edad sólo se podrá tratar los datos de los mayores de catorce años con su consentimiento, salvo que la ley exija la asistencia de los titulares de la patria potestad o tutela. En los casos de menores de catorce años se requerirá el consentimiento de los padres o tutores.

4. Datos especialmente protegidos

La LOPD considera que los datos relativos a la ideología, afiliación sindical, religión y creencias, el origen racial, la salud y la vida sexual son datos especialmente protegidos, lo que implica que se establezcan algunas especialidades en el nivel de protección y en la forma de obtención del consentimiento del interesado, así como en las medidas de seguridad aplicables.

En cuanto a su tratamiento, la Ley establece lo siguiente:

- Nadie puede ser obligado a declarar sobre su ideología, religión o creencias
- Se prohíbe la creación de ficheros creados con la finalidad exclusiva de almacenar datos especialmente protegidos, salvo que tengan por finalidad el tratamiento de datos de salud en los términos previstos en la normativa vigente.
- Se exige el consentimiento expreso y por escrito del afectado de los datos relativos a la ideología, afiliación sindical, religión y creencias. Si los datos se refieren al origen racial, la salud o la vida sexual se exige el consentimiento expreso del interesado.

5. Datos relativos a la salud.

Como se ha indicado con anterioridad los datos relativos a la salud son considerados de especial protección, lo que supone que debe garantizarse la confidencialidad de los mismos mediante unas medidas de seguridad adecuadas (que serán las de nivel alto).

Este principio implica que, sin perjuicio de lo que dispone la Ley respecto de la cesión, las instituciones y centros sanitarios públicos y privados y los profesionales médicos, podrán tratar los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

6. Seguridad de los datos

La ley establece la obligación de adoptar una serie de medidas de índole técnica y organizativa que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado.

Medidas que habrán de adoptarse o implementarse por el profesional que almacene los datos (responsable del fichero/responsable del tratamiento). Entre estas medidas destaca: la elaboración de un documento de seguridad detallando los datos almacenados, las medidas de seguridad adoptadas y las personas que tienen acceso a los datos.

7. Deber de secreto

La LOPD establece un deber de secreto profesional y de custodia para los que intervengan en cualquier fase del tratamiento de los datos de carácter personal, obligaciones que subsistirán aún después de finalizar el tratamiento de los datos.

8. Comunicación de datos

Principio que se refiere al cumplimiento de las obligaciones que deben cumplirse en caso de cesión de datos personales, a persona que no es ni el interesado ni las autorizadas a acceder al fichero que contenga los datos.

Las obligaciones para la realización de la cesión de datos son:

- Informar al interesado de la identidad del cesionario y de la finalidad de la cesión.
- Que el interesado preste su consentimiento previo. Consentimiento que tiene carácter revocable.
- Que la cesión se realice para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario.

El consentimiento exigido en el apartado anterior no será preciso, entre otros, cuando:

- 1) La cesión está autorizada en una ley.
- 2) se trate de datos recogidos de fuentes accesibles al público.
- 3) El tratamiento responda a la libre y legítima aceptación de una relación jurídica cuyo desarrollo, cumplimiento y control implique necesariamente la conexión de dicho tratamiento con ficheros de terceros. En este caso la comunicación sólo será legítima en cuanto se limite a la finalidad que la justifique.

9. Acceso a los datos por cuenta de terceros

El acceso a los datos por cuenta de terceros no se considerará cesión o comunicación de datos, dado que el acceso a los datos por parte del encargado del tratamiento es necesario para la prestación de un servicio al responsable del fichero.

Asimismo, el contratante responsable del tratamiento y la empresa contratada (encargado del tratamiento) son responsables de la implantación de las medidas de seguridad, así como del cumplimiento del resto de obligaciones que se contienen en el contrato por el que se regula el acceso a los datos. La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que deberá constar por escrito, estableciéndose expresamente:

- El contenido del tratamiento que se va realizar.
- Que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento.
- Que no aplicarán o utilizarán los datos con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.
- La definición de las medidas de seguridad que el encargado se compromete a adoptar.
- En caso de subcontratación estará autorizada por el responsable del tratamiento.

Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.

5.1.2 Obligaciones en materia de protección de datos de carácter personal

Analizados los principios rectores que inspiran la protección de los derechos de carácter personal de las persona físicas, vamos a examinar las principales obligaciones que, en comercio electrónico tienen que cumplir las entidades aseguradoras en materia de protección de datos de carácter personal.

➤ **Notificación a la Agencia Española de Protección de Datos de los ficheros**

Cuando en la página Web de una entidad aseguradora se soliciten o se recogen datos personales, ya sea de clientes, usuarios, potenciales clientes, etc., para su tratamiento, dicha entidad está obligada a notificar con carácter previo, a la Agencia Española de Protección de Datos (en adelante, AEPD), todos los ficheros que contengan estos datos personales. Debiéndose realizar una notificación distinta por cada uno de los ficheros que se deban inscribir.

Para ello, la entidad aseguradora deberá proceder a rellenar un formulario de notificación del fichero que podrá remitir a la Agencia por correo postal o por Internet con o sin firma electrónica. Una vez el fichero esté inscrito, la AEPD envía por correo postal a la entidad, la resolución con el código de inscripción otorgado a cada fichero. No obstante, si transcurrido un mes no se ha recibido ninguna noticia, se presume que el fichero se ha inscrito correctamente (silencio administrativo positivo). Se trata de un trámite de carácter gratuito,

para el que la AEPD ha habilitado en su página Web (www.agpd.es) un Sistema de Notificaciones Telemáticas de la AEPD denominado “Programa NOTA”. A título de ejemplo, podemos señalar como ficheros de datos de carácter personal que normalmente se tratan en una entidad aseguradora con página Web de comercio electrónico: Tomadores/asegurados, Potenciales clientes, Suscriptores y Usuarios.

➤ **Formulario de recogida de datos: Obligación de Información**

Cuando en la página Web se utiliza un formulario o documento en el que se solicitan datos personales de los clientes: bien para poder informar sobre los productos o servicios que presta la entidad (presupuesto, simulación o características de un seguro) o bien para la suscripción de un contrato; es obligatorio incluir un aviso legal en materia de protección de datos, cuyo contenido debe informar de lo siguiente:

1. De la existencia de un fichero o tratamiento de datos;
2. De la finalidad de su recogida y de los destinatarios de la información;
3. Del carácter obligatorio o facultativo de la respuesta a las preguntas que se plantean;
4. De las consecuencias de la obtención de los datos o de la negativa a suministrarlos;
5. De la posibilidad de ejercitar los derechos de acceso, rectificación, cancelación y oposición al tratamiento de los datos;
6. De la identidad y dirección del responsable del tratamiento de los datos.

Para cumplir con esta obligación, puede optarse por incluir una cláusula de protección de los datos de carácter personal indicando los extremos anteriores (Artículo 5 de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal), o bien insertar un enlace permanentemente visible en la Web a la de privacidad. En cualquier caso, la información a facilitar será siempre la misma.

Modelo de aviso legal

En virtud de lo dispuesto en la Ley 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal, le informamos que mediante la cumplimentación del presente formulario sus datos personales quedarán incorporados y serán tratados en los ficheros titularidad de (nombre de la Compañía), con el fin de (indicar la finalidad de la recogida de datos), así como para mantenerle informado, incluso por medios electrónicos, sobre cuestiones relativas a la actividad de la Compañía y sus servicios.

Usted puede ejercer, en cualquier momento, los derechos de acceso, rectificación, cancelación y oposición de sus datos de carácter personal mediante correo electrónico dirigido a (indicar e-mail) o bien mediante un escrito dirigido a (indicar dirección y postal), acompañando siempre una fotocopia de su D.N.I.

Modelo de Política de privacidad de entidad aseguradora

En cumplimiento de lo establecido en la normativa de protección de datos española y, en particular, en el artículo 5 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal (LOPD), [nombre de la entidad] le informa que los datos de carácter personal que nos proporcione a través del envío de correos electrónicos, así como los datos a los (nombre de la entidad) que tenga acceso como consecuencia de su navegación, consulta, solicitudes o simulaciones realizadas a través del sitio Web de [nombre de la entidad] (en adelante, "el Sitio Web"), serán recogidos en un fichero cuyo responsable es [nombre del Responsable del fichero].

Usted podrá ejercer sus derechos de acceso, rectificación, cancelación y oposición al tratamiento de dichos datos en [dirección y CIF de la entidad aseguradora], en los términos establecidos en la LOPD. Para su mayor comodidad, puede remitirnos la petición y documentación correspondiente a través de [otros medios de envío facilitados por la entidad].

La no cumplimentación o cumplimentación parcial de los datos de carácter personal que se le requieran podría suponer que [nombre de la entidad] no pueda atender su solicitud de información o de contratación. Asimismo, le rogamos que nos comunique cualquier modificación de sus datos personales, a fin de que la información contenida en nuestros ficheros esté en todo momento actualizada y no contenga errores. Para su mayor comodidad, puede hacerlo a través de [medio de envío de la solicitud].

Las finalidades de la recogida de sus datos son las de remitirle la información comercial de carácter general relativa a los productos y servicios [nombre de la entidad/es que recogen los datos] que en cada momento estén disponibles en el Sitio Web (en adelante, "los Productos y Servicios") y en el supuesto de que usted contrate alguno de dichos Productos o Servicios, gestionar los servicios contratados y mantener la relación contractual.

Si Usted no desea recibir dichas comunicaciones comerciales, publicitarias o promocionales, cualquiera que sea el canal utilizado al efecto, puede comunicar gratuitamente su decisión a través de los medios anteriormente indicados para ejercer sus derechos. Su aceptación para que se remita información comercial tiene siempre carácter revocable, sin efectos retroactivos.

De conformidad con lo dispuesto en el artículo 11 de la LOPD, Usted autoriza a [nombre entidades a las que se autorizan para la cesión de los datos personales] para que pueda [finalidad de la cesión].

Asimismo, por la presente se tiene por informado de lo dispuesto en el artículo 27 de la LOPD, relativo a la primera comunicación de datos a [nombre de entidades]. Dicho consentimiento es revocable en cualquier momento, sin efectos retroactivos.

Con carácter general, el responsable del fichero que contenga los datos personales tiene la obligación de poder acreditar que ha obtenido el consentimiento informado de las personas afectadas.

Por último, debemos señalar que todas las páginas Web en las que se recaben datos de carácter personal de personas físicas, deben incluir la información referida en lugar visible, de forma que el usuario pueda obtenerla con facilidad y de forma directa y permanente.

La Agencia ha manifestado en las recomendaciones que realizó en el año 2000 al sector del comercio electrónico, que se puede optar por incorporar en todas esas páginas un texto o un botón adecuadamente etiquetado que, al ser seleccionado mediante un "click", permita obtener la citada información. No obstante, considera más adecuada una opción según la cual, la lectura de dicha información se presente como ineludible (y no optativa) dentro del flujo

de acciones que deba ejecutar el usuario para expresar la aceptación definitiva de la transmisión de sus datos a la entidad que los está recabando.

También es recomendable tener constancia de la fecha en que el usuario facilita sus datos a través de la Web. Información que se debe conservar durante todo el tiempo que se vayan a tratar los datos, puesto que constituyen una prueba de la obtención del consentimiento informado del usuario para su tratamiento.

➤ **Comunicaciones comerciales**

La ley como norma general (LSSICE), prohíbe el envío de comunicaciones comerciales (sean publicitarias o promocionales) por correo electrónico u otro medio de comunicación electrónica equivalente, si previamente el destinatario de las mismas, no las ha solicitado o, en su caso, no las ha autorizado expresamente.

No obstante, si la entidad remitente (empresa aseguradora) mantiene con el destinatario una relación contractual previa como cliente, se permite el envío de dichas comunicaciones comerciales, siempre que la entidad hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente

En cualquier caso, tanto en el momento de recoger los datos del destinatario, como en el contenido de cada comunicación comercial, la entidad remitente debe informar al cliente sobre:

- Las cuestiones de protección de datos antes referenciadas (principio de información y de calidad).
- La posibilidad de revocar su consentimiento, poniendo para ello a su disposición un medio sencillo y gratuito (ejemplo, el envío de un correo electrónico a una dirección determinada o mediante un formulario en la página Web).

Asimismo, cuando se manda por la entidad una comunicación electrónica publicitaria o de carácter comercial, es imprescindible que el destinatario pueda identificarla como tal. Por ello, es obligatorio incluir al comienzo del mensaje la palabra *publicidad* o la abreviatura *publi*. Además, la empresa que realiza la promoción debe identificarse claramente.

Si el contenido del mensaje versa sobre ofertas o concursos promocionales, como descuentos, premios y regalos, deberán incluirse de forma clara las condiciones de acceso o participación, o bien indicar donde éstas pueden consultarse.

Al igual que hemos señalado en el apartado anterior (consentimiento cláusula LOPD), lo normal es que la obligación de solicitarse el consentimiento se cumpla: incluyendo en la cláusula de protección de los datos de carácter personal del contrato, un apartado en el que se solicite el consentimiento para comunicaciones comerciales con fines publicitarios o promocionales; o bien, insertando un enlace permanentemente visible en la Web a nuestra política de privacidad en donde se recoja la cláusula de comunicaciones comerciales.

Modelo de cláusula relativa a las comunicaciones comerciales

Como quiera que [entidad aseguradora] tienen intención de remitir a los usuarios comunicaciones comerciales por medios electrónicos, en cumplimiento de lo dispuesto en el artículo 21 de la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico (LSSI), mediante la aceptación de esta Política de Privacidad y Comunicaciones Comerciales el usuario autoriza expresamente a [entidad aseguradora] a remitirle comunicaciones comerciales, promocionales o publicitarias por correo electrónico o cualquier otro medio de comunicación electrónica equivalente.

Si Usted no desea recibir dichas comunicaciones comerciales, publicitarias o promocionales, cualquiera que sea el canal utilizado al efecto, puede comunicar gratuitamente su decisión a través de [indicar los canales de comunicación].

Su aceptación para que se remita información comercial tiene siempre carácter revocable, sin efectos retroactivos, conforme a lo dispuesto en el artículo 22.2 de la LSSI.

➤ **Información sobre las cookies**

Cuando en la página Web se utilizan cookies u otros dispositivos de almacenamiento y recuperación de datos, que se instalen en el ordenador del usuario, para guardar información necesaria para la navegación del usuario por nuestra Web, existe la obligación de informar de manera clara y completa sobre su utilización y finalidad, así como de ofrecer la posibilidad de rechazar el tratamiento de los datos mediante un procedimiento sencillo y gratuito.

Se puede cumplir con esta obligación: informando de ello en el aviso legal o en las condiciones de contratación de la página Web e informando sobre cómo pueden rechazar la instalación de estos archivos a través de los programas de navegación que el usuario utilice.

Ejemplo cláusula de cookies ubicada en aviso legal de la página Web

La página de entrada al Sitio Web dispone de una *cookie* que permite a nuestro sistema recordar el idioma escogido por el usuario en su primera sesión. De esta manera se evita la selección del idioma en las visitas sucesivas al Sitio Web. Esta *cookie* no es invasiva ni nociva y la única función que realiza es la de informar al sistema del idioma anteriormente escogido por el usuario. Si el usuario lo desea, puede denegar toda *cookie* desde la opción de menú correspondiente de su propio navegador. Para cambiar el idioma de la *cookie* tan sólo debe eliminarla y volver a escoger el idioma deseado al entrar en el Sitio Web.

➤ **Otras obligaciones relacionadas con la protección de datos personales**

. Derechos de los interesados

La LOPD reconoce a los interesados o afectados una serie de derechos con la finalidad de que todo tipo de tratamiento de datos se realice efectivamente mediante el consentimiento informado de los mismos. Derechos que se traducen en obligaciones para las entidades aseguradoras y que los interesados pueden ejercer a través de la Web de la entidad.

- 1) **Ejercicio del derecho de acceso:** En virtud del mismo, se faculta al interesado para obtener toda la información de sus datos sometidos a tratamiento, su origen, las cesiones realizadas o que prevean realizar.

En este caso, el interesado puede ejercitar su derecho a través de la Web y, tanto si utiliza este canal como cualquier otro (presencialmente, por correo postal o certificado, teléfono...), el procedimiento será el siguiente:

- Se identificará al interesado o a su representante legal, con documentación acreditativa.
- Formalización por el afectado del impreso de Solicitud de Acceso a Datos.
- El responsable de Seguridad de la entidad, recabará los datos del interesado y los remitirá al interesado en el plazo máximo de un mes a contar de la solicitud, por cualquiera de los siguientes medios:
 - . Consulta en pantalla del ordenador o portátil.
 - . Escrito, fotocopia o copia remitida por correo, certificado o no.

El responsable de Seguridad contabilizará cada una de las peticiones, dado que puede denegar la misma en caso de ejercerse el derecho de acceso en un plazo inferior a 12 meses y no se acredite interés legítimo o sea presentada por persona diferente al afectado.

- 2) **Ejercicio del derecho de rectificación y cancelación:** El interesado podrá rectificar o cancelar aquellos datos personales que considere inexactos, incompletos, inadecuados o excesivos o, simplemente, que desee no mantener en el fichero en el que se encuentren por resultar innecesarios o no pertinentes.

Procedimiento del derecho de rectificación:

- Se identificará al interesado o a su representante legal, con documentación acreditativa.
- Formalización por el afectado del impreso de Solicitud de Rectificación de Datos.

- Se rectificarán los datos por el responsable del tratamiento si se puede en el momento o en un plazo máximo de 10 días y se notificará al interesado.
- En caso de que no se puede rectificar en el momento o se haya realizado la solicitud por canal distinto al presencial, se enviará la confirmación de rectificación por correo postal.
- Si los datos han sido cedidos, se debe comunicar la rectificación para que los cesionarios la efectúen en un plazo de diez días.

Procedimiento del derecho de cancelación.

- Se identificará al interesado o a su representante legal, con documentación acreditativa.
- Formalización por el afectado del impreso de Solicitud de Cancelación de Datos.
- Se procederá a bloquear los datos si se puede en el momento o en un plazo máximo de 10 días y se notificará al interesado.
- En caso de que no se pueda realizar la cancelación en ese momento o se haya realizado la solicitud por canal distinto al presencial, se enviará la confirmación de cancelación por correo postal.
- Si los datos han sido cedidos, se debe comunicar la cancelación para que los cesionarios la efectúen en un plazo de diez días.

3) Ejercicio del Derecho de oposición: A través de este ejercicio, el afectado puede oponerse, previa petición y sin gastos, al tratamiento de sus datos o que se cese en el mismo en los siguientes supuestos:

- o Cuando no sea necesario su consentimiento para el tratamiento.
- o Cuando se trate de ficheros que tengan por finalidad la realización de actividades publicitarias y/o prospección comercial.
- o Cuando el tratamiento tenga por finalidad la adopción de una decisión referida al afectado y basada únicamente en el tratamiento automatizado de sus datos de carácter personal.

Procedimiento del derecho de oposición.

- Se identificará al interesado o a su representante legal, con documentación acreditativa.
- Formalización por el afectado del impreso de Solicitud de Oposición de Datos.
- Se procederá a excluir el tratamiento de los datos si se puede en el momento o en un plazo máximo de 10 días y se notificará al interesado.
- En caso de que no se pueda realizar la exclusión en ese momento o se haya realizado la solicitud por canal distinto al presencial, se enviará la confirmación de exclusión por correo postal.

. Contrato de tratamiento de datos

Cuando la página Web en la que se recogen datos personales esté alojada en los servidores de otra empresa, un informático que no es de nuestra empresa haga el mantenimiento de la página Web u otra empresa vaya a prestarle un servicio de tratamiento de datos accediendo para ello, a la información que su base de datos, será necesario firmar un contrato de tratamiento de datos.

Se trata de un contrato que está regulado en el artículo 12 de la LOPD y en los artículos 20, 21 y 22 del 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.

. Medidas de seguridad

La creación y mantenimiento de un fichero de datos personales exige la aplicación de unas determinadas medidas de seguridad, tanto técnicas como organizativas, que podrán variar en función de la mayor o menor sensibilidad de los datos que lo integran. Medidas que serán objeto de desarrollo en el apartado relativo al principio de seguridad.

5. 2 Sistemas de pago on-line

En los últimos años, con el desarrollo de las tecnologías de la información y en concreto del comercio electrónico B2C, se ha experimentado una clara tendencia en el crecimiento del número de operaciones electrónicas realizadas a través de la Red.

Lo que requiere que, por parte de las empresas que venden sus productos por Internet, se ofrezcan medios de pago que resulten seguros, flexibles y cómodos para los clientes o usuarios (cuantas más opciones y facilidades tenga el comprador más posibilidades de cerrar ventas por la Red), además de rentables para las propias empresas.

5.2.1 Formas de pago

En la actualidad los medios de pago más utilizados y que conocemos los podemos agrupar: en:

Métodos *off line*

Son métodos en los que el pago no se efectúa en el momento de realizar la compra; se realiza a posteriori o de forma diferida.

Estos métodos se suelen considerar como medios más seguros que los métodos *on line* dado que no se transmiten por Internet los datos bancarios del cliente, lo que disminuye el riesgo de uso fraudulento o ilícito de los datos obtenidos indebidamente por un tercero.

Entre estas formas de pago destacamos:

- **Transferencia bancaria**

Método de pago por el cual el comercio notifica al usuario una cuenta bancaria donde el cliente debe realizar una transferencia para que se gestione su pedido.

Ventajas e Inconvenientes

- Sistema seguro ya que la operación se realiza por la entidad bancaria y tras una orden del comprador. La transacción queda grabada en el banco del usuario y en el banco del comercio *on line*.
- No implica ningún coste al comercio, y al comprador en algunos casos un coste muy bajo.
- El comprador, realiza el pago previamente a la recepción del artículo. La orden de pago se puede realizar por el comprador físicamente (visitando su banco), o de forma online para poder realizar la transferencia. No es un sistema automático, y requiere de una comprobación periódica por parte del comercio antes de procesar un pedido. Es un sistema efectivo pero lento, ya que normalmente el dinero tarda dos días hábiles en llegar a su destino.
- Es el comprador el que paga la comisión correspondiente asociada a la transacción.

- **Domiciliación bancaria.**

En esta forma de pago, el cliente facilita al comercio un número de cuenta bancaria para que éste le gire un cobro con una periodicidad determinada. Esta forma de pago, toma sentido sobre todo cuando hablamos de un entorno B2B (comercio entre empresas), o bien para la venta de servicios de suscripción periódica, como son los seguros con prima periódica.

Ventajas e Inconvenientes:

- Sistema seguro. El comprador se despreocupa de realizar el pago cada vez que adquiere un producto. El comercio, cobra el precio del producto antes de la entrega o en el momento de perfección del contrato.
- No es un sistema automático, y requiere de una comprobación periódica por parte del comercio antes de procesar un pedido o de continuar prestando el servicio.

- Se pierde el control de los pagos realizados dado que no requiere de una intervención por parte del comprador.
- Favorece los casos de impagos de recibos.

- **Contra reembolso**

Este método lo podemos considerar como el método de pago más seguro, ya que el pago se realiza cuando el producto adquirido llega al usuario.

Ventajas e Inconvenientes

- Para el comprador es una ventaja, el pago se efectúa una vez recibido el producto adquirido.
- Para el comercio tiene como inconvenientes que, cuando el usuario realiza la compra del producto deseado no deja ninguna señal económica de que vaya a querer el pedido realmente. Asimismo, supone un coste que la empresa de reparto se haga cargo del cobro del envío, suele ser un porcentaje de la transacción realizada.
- Métodos que no se utiliza en la venta de servicios o productos intangibles, dado que no se produce la entrega física del producto.
- No hay una automatización, por lo que requiere una mayor dedicación en la gestión y seguimiento por parte del comercio.

Métodos *on line*

Son aquellos métodos en los que el pago se realiza en el momento en que se realiza de la compra, mediante conexión directa a través de una pasarela de pago o similar.

Los métodos *on line*, son más rápidos pero requieren de elementos complementarios que eleven el nivel de seguridad en la transacción.

Dentro de los métodos *on line* encontramos:

- **Tarjeta de crédito (TPV virtual)**

Es el sistema de pago electrónico más común y aceptado hoy en día para las transacciones de consumo dado el uso generalizado de las tarjetas de crédito.

En este procedimiento de pago intervienen cuatro elementos personales: comprador, vendedor, banco del vendedor (Banco Merchant) y banco emisor, y se hace a través de un *TPV virtual* (Terminal Punto de Venta).

El comprador se conecta a la website del comercio o empresa (vendedor) y por medio de un *TPV virtual* realiza el pago al banco del vendedor con la autorización del banco emisor. La autenticidad se verifica por el número de tarjeta, la fecha de caducidad y el importe. El *TPV* comunica el resultado de la operación.

De esta forma, los datos sólo circulan por red bancaria y encriptados, garantizando la confidencialidad del proceso. Además, los datos del comprador no son visibles para el vendedor, sólo el resultado de la operación y lo necesario para realizar la entrega.

Existen dos tipos de *TPVs*: el tradicional a través del cual se puede usar cualquier tarjeta de crédito y los *TPVs 3D Secure*, en los que el pago se realiza mediante conexión telemática directa con una pasarela de pago de una entidad bancaria. En ambos casos el vendedor, o su caso la entidad bancaria, solicitan los datos de la tarjeta de crédito para poder finalizar la compra. El coste económico de esta forma de pago depende del acuerdo al que se llegue con la entidad bancaria.

Ventajas e inconvenientes

- Sistema cómodo y fácil de usar por resultar familiar a la mayoría de los usuarios que acostumbran a utilizarla en sus transacciones habituales. Al ser un sistema automático es muy rápido y eficaz; basta con aportar unos pocos datos para que se pueda hacer un cargo a una tarjeta de crédito: identificación del usuario (nombre, DNI...), y número y fecha de caducidad de la tarjeta.
- La transacción es respaldada por la entidad emisora de la tarjeta de crédito.
- El comprador no paga ninguna comisión por la transacción realizada. El comercio, recibe el dinero de forma inmediata.
- El comercio asume los costes en forma de comisiones y mantenimiento del *TPV*. Requiere de una intervención técnica con la pasarela de pagos de la entidad bancaria.
- Los riesgos de utilización de la tarjeta de crédito son compartidos entre la empresa, el cliente e incluso la empresa gestora (Visa, American Express...). Ahora bien, el riesgo de fraude lo soporta el comercio si la pasarela de pago que se usa es convencional y no está securizada (3D Secure).

Entre los inconvenientes de la utilización de este medio de pago están:

- Que es un sistema de pago que requiere y exige de un Certificado de Seguridad por parte del comercio (vendedor) para garantizar la comunicación de una forma segura. Al realizar la introducción de datos bancarios, es posible el fraude por terceras personas al no disponerse de la firma del comprobante de la tarjeta de crédito como así sucede en las ventas presenciales.
- No resulta operativo para la realización de transacciones de baja cuantía.
- No se puede utilizar para pagos entre particulares.

- **Tarjeta virtual**

Se trata de una tarjeta de uso exclusivo en Internet. Se caracterizan por ser de prepago, el usuario paga cierta cantidad a la entidad emisora de la tarjeta, que le da crédito por esa cantidad para utilizar en los sitios de Internet que lo permitan y, además por ser recargable.

La tarjeta virtual funciona del siguiente modo:

- Se cargan por medio de transferencia.
- En el momento de la compra los datos circulan por red bancaria.
- Se confirman por medio del número de tarjeta, caducidad y PIN.
- La entidad emisora adeuda la cantidad al establecimiento.
- En caso de pérdida se mantiene el saldo de la tarjeta.

Ventajas e inconvenientes

- Medio que simplifica el procedimiento de pago en Internet y elimina la desconfianza de los usuarios al introducir los datos de su tarjeta de crédito en la Red
- Estas tarjetas son muy sencillas y seguras, su extravío no suponen la pérdida del dinero.
- Se pueden utilizar para transacciones y están al alcance de todo tipo de público objetivo. Sin embargo, tienen la limitación de que su uso está restringido a los websites que la admitan, y tampoco se puede utilizar para el pago entre particulares.

- **Tarjetas inteligentes**

Son tarjetas físicas que incorporan un chip con la información del usuario. Se caracterizan por ser de prepago, la carga queda almacenada en el chip y es la cantidad de dinero que el poseedor dispone. Algunas de las empresas gestoras las poseen, y son conocidas como monederos electrónicos o como tarjetas monedero.

Una tarjeta inteligente funciona del siguiente modo: El dinero de la recarga se almacena en el chip de la tarjeta que es el que autoriza la transacción. A continuación el establecimiento da también su autorización.

Ventajas e inconvenientes

- Evitan el posible fraude, ya que son tarjetas de prepago, así que el establecimiento sabe que dispone del dinero.
- Resulta muy operativa para la realización de pequeñas transacciones y a ellas tienen acceso todo el público.
- Posibilidad de poder almacenar gran cantidad de datos sobre el usuario.

- En caso de extravío de la tarjeta el usuario pierde la cantidad de dinero almacenado.
- Presenta un inconveniente físico, la necesidad de la existencia de un lector de chip, lo cual es posible en los establecimientos físicos pero no en los virtuales. Obligaría al usuario a tener en su ordenador un lector de chip.
- No se puede utilizar para pagos entre particulares.

- **El teléfono móvil**

A través de los móviles, los compradores pueden abonar sus compras en aquellos negocios cuyas infraestructuras lo permitan.

Este sistema resulta sencillo para las personas que utilizan habitualmente el móvil: primero el usuario se da de alta en el sistema, con un número de cuenta, el número de móvil y un PIN. Cuando realiza una compra, el sistema llama al móvil del comprador y se acredita para que el usuario autorice la transacción con el PIN. Por último, El sistema realiza una domiciliación a la cuenta del usuario por el importe de la transacción.

Ventajas e inconvenientes

- Sistema que elimina dos de los principales problemas de las tarjetas:
 - Los micropagos: las tarjetas no son útiles para pequeñas transacciones debido a las comisiones, este sistema sí.
 - El público objetivo: muchas empresas del mundo on line tienen como público jóvenes de entre 15 y 25 años, muchos de los cuales no tienen tarjetas de crédito pero sí tienen teléfono móvil.
- No todas las empresas están preparadas tecnológicamente para utilizar esta forma de pago.

- **El e- Cheque**

Sistema de pago alternativo para todo tipo de transacciones a través de Internet. Es un documento electrónico que incluye el contenido legal mínimo de todo cheque y la firma digital del librador. Es necesario que el vendedor tenga una cuenta bancaria donde poder hacer efectivo el cheque.

Ventajas e inconvenientes

- Es un método rápido y fácil de cobro para los vendedores, y al mismo tiempo mantiene la confidencialidad del comprador.
- Es muy seguro.

- Es muy versátil, se puede utilizar en cualquier tipo de transacción y puede ser portador de mucha información.

- **PayPal**

Es uno de los sistemas de pago online relativamente más reciente dentro del marco del comercio electrónico. Este método de pago, propiedad de la empresa norteamericana Ebay, consiste en la recepción y envío de dinero en Internet de forma rápida y segura entre comprador y vendedor.

Con este sistema, el usuario debe registrarse gratis en su Web (Web www.paypal.es), creando un cuenta que le facilita el envío de dinero desde varias fuentes (tarjeta de crédito o débito o cuenta bancaria) al destinatario que se desee (tiendas en Internet o personas) y obtener servicios como suscripción a pagos periódicos, realizar el pago desde una cuenta bancaria, o incluso que el dinero se deposite en la propia cuenta de PayPal.

Ventajas e Inconvenientes

- Sistema rápido al ser online o mediante soporte móvil El comprador puede pagar con tarjeta de crédito, tarjeta de débito o por cuenta bancaria.
- Sistema seguro, ya que no se envía en ningún momento al comercio la información financiera o de tarjeta de crédito.
- Sistema global, es aceptado en cualquier transacción nacional e internacional. Para el comercio, al igual que si se tratase de una entidad bancaria, hay un coste de comisionado.

5.2.2 Mecanismos de seguridad en los medios de pago electrónicos

Los mecanismos o requisitos de seguridad pueden variar ligeramente de un sistema de pago a otro, puesto que dichos mecanismos estarán en función tanto de las características propias del sistema como por la confianza y seguridad que ofrezca el entorno donde va a realizar el pago.

En cualquier caso, no obstante ocuparnos más tarde de la seguridad en la Red, podemos decir que en general, los requisitos de seguridad de un sistema de pago electrónico son los siguientes:

➤ Autenticación de los datos

En todo método de pago, tanto el comprador como el vendedor deben identificarse para comprobar que no existe fraude. En un sistema de pago a través de *TPV*, existe una entidad certificadora que durante la operación de pago garantiza la

autenticidad de la transacción, validando la información de tarjeta de crédito y al titular de la misma.

La autenticación de otros datos que puedan afectar a la legalidad de la compra realizada, se garantiza gracias a protocolos criptográficos de autenticación.

➤ **Disponibilidad y fiabilidad**

Una característica fundamental de los medios electrónicos de pago es la alta disponibilidad y fiabilidad de las operaciones, ya que en el momento de la transacción no puede existir una pérdida del servicio.

No obstante, podría producirse algún fallo en el sistema, y una peculiaridad de las transacciones es que o se realizan correctamente o no se realizan. De esta forma, la fiabilidad del sistema es total. Por tanto, un sistema fiable y disponible no sólo depende de que sus transacciones lo sean, sino de que toda la arquitectura y elementos del sistema cumplan los mismos requisitos.

➤ **Integridad**

Otro aspecto importante en todo sistema de pago electrónico es la integridad de los datos intercambiados entre las partes de la operación comercial. Es decir, no puede haber forma de manipular la información o alterarla mientras se realiza una transacción electrónica. Para ello existen mecanismos de seguridad como son códigos de autenticación o la firma digital.

➤ **Confidencialidad**

Los datos que se envían en una operación electrónica no pueden ser visibles para terceros, de ahí que se empleen técnicas de encriptado y cifrado de la información por partes que intervienen en la transacción.

En este sentido, la entidad emplea un Certificado de Seguridad emitido por una entidad colaboradora certificadora, que permite el cifrado, encriptado y envío de la información de forma segura, empleando un canal de comunicación seguro (SSL). De tal forma que únicamente las partes de la transacción, empresa y destinatario (entidad bancaria, autenticadota...) son concedores de la información de forma clara tras un proceso inverso de desencriptado.

5.2.3 Tendencias en el uso de los medios de pago

Según el último estudio publicado por ONTSI en el año 2008, el 50,2% de los compradores prefiere pagar sus compras online a través de la tarjeta de crédito.

Las siguientes formas de pago mas utilizadas por la población española, son; el contra reembolso con un 29,1%; el sistema PayPal con un 10,7%y las

transferencias bancarias con un 6,7%. Las tres formas de pago han aumentado significativamente en su utilización respecto al año 2007.

La conclusión que extraemos es que los métodos tradicionales u *off line* están entre los tres primeros métodos más utilizados por la población, por los que los últimos métodos de pago online como PayPal tienen aún un largo recorrido para su aceptación en la sociedad de la información.

En sector asegurador, los medios de pago que generalmente se utilizan en la contratación electrónica están en función de la modalidad de pago del seguro escogido por el tomador. Así, en aquellas modalidades de seguro en que el pago es a prima única, generalmente se utiliza el pago con tarjeta de crédito o débito o la domiciliación bancaria, pudiéndose utilizar cualquier otra forma de pago *on line*.

La especialidad la encontramos en aquellos seguros que tienen con forma de pago fraccionado o seguros fraccionarios, en los que la única modalidad de pago que se permite por las entidades que venden *on line*, es la domiciliación bancaria. Sistema de pago, que puede plantear problemas de la confidencialidad de los datos bancarios del tomador.

5.3 La seguridad en transacciones comerciales a través de la Red: riesgos y soluciones técnicas

5.3.1 El Principio de Seguridad

Como ya hemos indicado, la normativa de protección de datos despliega una amplia protección en dos niveles, el jurídico y el informático. Así, junto a los requisitos exigidos en relación a la recogida y cesión de datos, se establecen una serie de medidas de seguridad que se exigen para la custodia de los datos por parte del responsable del fichero.

De esta forma, la LOPD (art. 9) y con posterioridad el Reglamento que lo desarrolla, regulan un aspecto esencial para la tutela del derecho fundamental a la protección de datos, el principio de seguridad, que repercute sobre múltiples aspectos organizativos, de gestión y de inversión en todas las organizaciones que traten datos personales. En dicho precepto se establece:

“Artículo 9. Seguridad de los datos.

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

2. No se registrarán datos de carácter personal en ficheros que no reúnan las condiciones que se determinen por vía reglamentaria con respecto a su integridad y seguridad y a las de los centros de tratamiento, locales, equipos, sistemas y programas (...).”

La normativa regula esta materia de modo que contempla las múltiples formas de organización material y personal de la seguridad que se da en la práctica en los ficheros automatizados (y no automatizados), ofreciendo a los responsables un marco claro de actuación.

De esta forma, se establecen las medidas mínimas 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. En consecuencia, todos los responsables de los tratamientos o de los ficheros y los encargados del tratamiento deberán implantar las medidas de seguridad, con independencia de cual sea su sistema de tratamiento.

Según la ley, las medidas de índole técnica y organizativas que se adopten deben garantizar la seguridad de los datos y evitar 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.

Por su parte, el Reglamento establece tres niveles de medidas de seguridad en función de la importancia de los datos tratados y de la conveniencia de asegurar su confidencialidad e integridad.

Estos niveles se caracterizan por: configurarse como mínimos legales exigibles (por lo que podrán incrementarse las medidas de seguridad de acuerdo a otros criterios) y, ser acumulativos (en el tratamiento de ficheros de nivel medio, deberán implantarse todas las medidas de seguridad descritas para el nivel básico y las del medio y así sucesivamente).

1) Niveles de seguridad y aplicación

➤ Nivel básico

- Ámbito de aplicación

Estas medidas deberán aplicarse a todos los ficheros de datos de carácter personal.

- Medidas aplicables:

- Por el responsable del fichero deberá redactarse un documento de seguridad de carácter privado y de obligado cumplimiento para todo el

personal con acceso a los ficheros de datos de carácter personal y a los sistemas de información, en el que debe recoger las políticas, reglas, medidas y procedimientos de seguridad establecidos por el dicho responsable.

- Adopción por el responsable del fichero de las medidas necesarias para que el personal conozca las normas de seguridad.
- Creación de un registro de incidencias.
- Establecimiento de una redacción actualizada de personas autorizadas para acceder a los datos o recursos que tengan acceso al sistema de información, debiendo establecer procedimientos de identificación y autenticación de los usuarios que tengan acceso a los datos.
- Establecimiento de un mecanismo de control de soportes, de forma que estos soportes que contengan datos de carácter personal deben ser controlados por el responsable de seguridad.

➤ **Nivel medio**

- Ámbito de aplicación

Además de las medidas de nivel básico, las medidas de nivel medio deberán aplicarse en los siguientes ficheros o tratamientos de datos de carácter personal:

- Los relativos a la comisión de infracciones administrativas o penales.
- Los relativos a prestación de servicios de información sobre solvencia patrimonial y crédito.
- Aquellos de los que sean responsables las entidades financieras para finalidades relacionadas con la prestación de servicios financieros.
- Aquellos que contengan un conjunto de datos de carácter personal que ofrezcan una definición de las características o de la personalidad de los ciudadanos y que permitan evaluar determinados aspectos de la personalidad o del comportamiento de los mismos.

- Medidas aplicables:

- Identificación en el documento de seguridad del responsable de seguridad, de los controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el propio documento y de las medidas que sea necesario adoptar cuando un soporte vaya a ser desechado o reutilizado.

- Realización a los sistemas de información e instalaciones de tratamiento de datos de una auditoría interna o externa que verifique el cumplimiento del propio reglamento y de los procedimientos e instrucciones vigentes en materia de seguridad de datos, al menos, cada dos años.
- Establecimiento de un mecanismo que permita la identificación de forma inequívoca y personalizada de todo usuario que intente acceder al sistema y la verificación de que está autorizado⁵¹.
- Prohibición de las pruebas con datos reales, salvo que se asegure el nivel de seguridad correspondiente al tipo de fichero tratado.

➤ **Nivel alto**

● Ámbito de aplicación

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

- Los que se refieran a datos de ideología, afiliación sindical, religión, creencias, origen racial, salud o vida sexual.
- Los que contengan o se refieran a datos recabados para fines policiales sin consentimiento de las personas afectadas.
- Aquellos que contengan datos derivados de actos de violencia de género.

● Medidas aplicables:

- La distribución de los soportes que contengan datos de carácter personal cifrando dichos datos o utilizando cualquier mecanismo que garantice que la información no será exigible ni manipulada durante su transporte.
- Instalación de un registro de accesos, lo que implica que de cada acceso deberá guardarse, como mínimo, la identificación del usuario que accede a los datos de nivel alto, la fecha y hora en que se realiza el acceso, el fichero accedido, el tipo de acceso y si el acceso ha sido autorizado o denegado.
- Conservación de una copia de respaldo de los datos en un lugar diferente de aquel en que se encuentren los equipos informáticos que los tratan.

- Transmisión de datos de carácter personal de nivel alto a través de redes de telecomunicaciones, cifrando dichos datos o utilizando cualquier otro mecanismo que garantice que la información no sea inteligible ni manipulada por terceros.

Supuestos especiales

Cuando los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas sean responsables de los ficheros, en relación a los datos de tráfico y a los datos de localización, se aplicará, además de las medidas de seguridad de nivel básico y medio, la medida de seguridad de nivel alto correspondiente al registro de accesos.

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

1. Los datos se utilicen con la única finalidad de realizar una transferencia dineraria a las entidades de las que los afectados sean asociados o miembros.
2. Se trate de ficheros o tratamientos no automatizados en los que de forma incidental o accesorio se contengan aquellos datos sin guardar relación con su finalidad.

El encargado del tratamiento

Cuando el responsable del fichero o tratamiento facilite el acceso a los datos, a los soportes que los contengan o a los recursos del sistema de información que los trate, a un encargado de tratamiento que preste sus servicios en los locales del primero, deberá hacerse constar esta circunstancia en el documento de seguridad de dicho responsable, comprometiéndose el personal del encargado al cumplimiento de las medidas de seguridad previstas en el citado documento.

En caso de que el servicio fuera prestado por el encargado del tratamiento en sus propios locales, ajenos a los del responsable del fichero, deberá elaborar un documento de seguridad o completar el que ya hubiera elaborado, en su caso, identificando el fichero o tratamiento y el responsable del mismo e incorporando las medidas de seguridad a implantar en relación con dicho tratamiento.

Acceso a datos a través de redes de comunicación

Si el acceso a los datos se realiza a través de redes de comunicaciones, sean o no públicas, deberá garantizarse un nivel de seguridad equivalente al

correspondiente a los accesos en modo local, conforme a los criterios ya señalados, es decir, niveles básico, medio y alto de seguridad.

Régimen del responsable del fichero o encargado de tratamiento que trabaje fuera de los locales

Si los datos personales se almacenan en dispositivos portátiles o se tratan fuera de los locales del responsable de fichero o tratamiento, o del encargado del tratamiento, será preciso que exista una autorización previa del responsable del fichero o tratamiento y en todo caso, deberá garantizarse el nivel de seguridad correspondiente al tipo de fichero tratado.

Esta autorización tendrá que constar en el documento de seguridad y podrá establecerse para un usuario o para un perfil de usuarios y determinando un periodo de validez para las mismas.

Ficheros temporales o copias de trabajo de documento

Los ficheros temporales o copias de documentos que se hubiesen creado exclusivamente para la realización de trabajos temporales o auxiliares deberán cumplir el nivel de seguridad que les corresponda conforme a los criterios ya citados, es decir, niveles básico, medio y alto de seguridad.

Todo fichero temporal o copia de trabajo así creado será borrado o destruido una vez que haya dejado de ser necesario para los fines que motivaron su creación.

2) Tratamiento automatizado de datos

➤ Medidas de seguridad de nivel básico

- **Funciones y obligaciones del personal**

En el documento de seguridad se deben definir y recoger de forma precisa las funciones y obligaciones de cada uno de los usuarios con acceso a los datos de carácter personal y a los sistemas de información.

También se definirán las funciones de control o autorizaciones delegadas por el responsable del fichero o tratamiento.

El responsable del fichero o tratamiento adoptará las medidas necesarias para que todo el personal conozca y comprenda las normas de seguridad que afectan al desarrollo de sus funciones, así como las consecuencias en caso de incumplimiento.

- **Identificación y autenticación**

Se exige la identificación inequívoca y personalizada para todos los usuarios con acceso a datos de carácter personal. El responsable del

fichero o tratamiento deberá adoptar las medidas que garanticen la correcta identificación. Si el mecanismo de autenticación se basa en contraseñas, existirá un procedimiento de asignación, distribución y almacenamiento que garantice su confidencialidad e integridad.

La periodicidad de cambio de contraseña se establecerá en el documento de seguridad y en ningún caso será superior a un año. Mientras estén vigentes, las contraseñas se almacenarán de forma ininteligible.

➤ **Medidas de seguridad de nivel medio**

- **Responsable de seguridad**

Se deben designar uno o varios responsables de seguridad encargados de coordinar y controlar las medidas definidas en el mismo. Esta designación puede ser única para todos los ficheros o tratamientos de datos de carácter personal o diferenciado según los sistemas de tratamiento utilizados, circunstancia que deberá hacerse constar claramente en el citado documento.

- **Identificación y autenticación**

El responsable del fichero o tratamiento establecerá un mecanismo que limite la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

- **Control de acceso físico**

Sólo tendrá acceso a los lugares donde se hallen instalados los equipos físicos que den soporte a los sistemas de información, el personal autorizado en el documento de seguridad.

- **Registro de incidencias**

En el registro de incidencias deberán consignarse igualmente los procedimientos realizados de recuperación de los datos, indicando la persona que ejecutó el proceso, los datos restaurados y, en su caso, qué datos ha sido necesario grabar manualmente en el proceso de recuperación.

Para la ejecución de los procedimientos de recuperación de los datos siempre será necesaria la autorización del responsable del fichero.

➤ **Medidas de seguridad de nivel alto**

- **Gestión y distribución de soportes**

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

Deberá evitarse el tratamiento de datos de carácter personal en dispositivos portátiles que no permitan su cifrado. Pero en caso de que sea estrictamente necesario, se hará constar motivadamente en el documento de seguridad y se adoptarán medidas que tengan en cuenta los riesgos de realizar tratamientos en entornos desprotegidos.

- **Copias de respaldo y distribución**

Deberá conservarse una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en lugar diferente a aquel en que se encuentren los equipos informáticos que los tratan. Este lugar deberá cumplir en todo caso las medidas de seguridad exigidas en el reglamento, o utilizando elementos que garanticen la integridad y recuperación de la información en forma que sea posible su recuperación.

- **Registro de acceso**

- De cada intento de 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 acceso estarán bajo el control directo del responsable de seguridad competente sin que deban permitir la desactivación ni la manipulación de los mismos.
- El período mínimo de conservación de los datos registrados será de dos años.
- El responsable de seguridad se encargará de revisar al menos una vez al mes la información de control registrada y elaborará un informe de las revisiones realizadas y los problemas detectados.
- No será necesario el registro de acceso en caso de que concurren las siguientes circunstancias:
- Que el responsable del fichero o tratamiento sea una persona física.
- Que el responsable del fichero o del tratamiento garantice que únicamente él tiene acceso y trata los datos personales.

- La concurrencia de las dos circunstancias a las que se refiere el apartado anterior deberá hacerse constar expresamente en el documento de seguridad.

- **Telecomunicaciones**

Cuando deban implementarse las medidas de nivel alto establecidas para aquellos datos de carácter personal que así lo requieren⁶³, la transmisión de los mismos a través de redes públicas o redes inalámbricas de comunicaciones electrónicas se realizará cifrando datos o bien utilizando cualquier otro mecanismo que garantice que la información no sea legible ni manipulada por terceros.

5.3.2. Los riesgos en las transacciones comerciales: soluciones técnicas y jurídicas

Como ya hemos puesto de manifiesto con anterioridad, las comunicaciones electrónicas suscitan desconfianza o inseguridad en los usuarios que temen que en la prestación de los servicios de la sociedad de la información sus derechos resulten lesionados.

Por lo tanto, la seguridad es uno de los principales problemas que se encuentran las entidades aseguradoras en el desarrollo del comercio electrónico. Por este motivo las empresas del sector presentes en la Red y organismos de todo el mundo, se esfuerzan en garantizar la seguridad en transacciones para prevenir conductas ilícitas (fraudes, robos, usurpación de identidades, uso no autorizados de datos...).

La ISO (Organización Internacional de Normalización o Internacional Standard Organisation), presenta una arquitectura de seguridad según la cual, para proteger las comunicaciones de los usuarios en las redes, es necesario dotar a las mismas de los siguientes cuatro principios:

- Principio de autenticidad: Que la persona o empresa que dice estar al otro lado de la red es quién dice ser.
- Principio de integridad: Que lo transmitido a través de la red no haya sido modificado.
- Principio de intimidad o confidencialidad: Que los datos transmitidos no hayan sido vistos durante el trasiego telemático por persona no autorizada.
- Principio de no repudio (no rechazo): Que lo transmitido no pueda ser repudiado o rechazado.

Se trata de principios que no se garantizan completamente en la actualidad. No hay seguridad en el pago con tarjetas, en la identificación de las partes de la comunicación, en la transmisión de los mensajes...

No cabe duda que, los riesgos principales que se derivan de las transacciones electrónicas se conectan con el uso de tecnologías invasivas de la intimidad de las personas, que persiguen en muchos casos obtener datos personales anulando, eludiendo o limitando el consentimiento de su titular.

Como ejemplos de tecnologías invasivas podemos citar:

- Programa conocido como Sniffers, que olfatean secuencias de dígitos que se parezcan a los de las tarjetas de crédito con el fin de conseguir los datos completos del titular de una tarjeta y realizar transacciones fraudulentas en la Red.
- Phising: técnica por la que los estafadores se hacen con los datos del usuario que les interesa a través de correos electrónicos en los que suplantan la identidad de un banco u organismo público. Para ello suelen solicitar las cuentas bancarias y las claves de acceso con el pretexto de actualizar las bases de datos o de hacer una devolución de la Agencia Tributaria.
- Pharming, técnica que infecta el ordenador del usuario con un virus troyano que redirige la página Web que se visita (por regla general de una entidad bancaria) a la fraudulenta creada por el estafador con el objetivo de recabar datos confidenciales.
- Las cookies: son ficheros de datos que determinados servidores envían a los ordenadores que se conectan a sus páginas Web, quedando almacenados en el disco duro.
Cuando esto se produce sin límites temporales, cada vez que un usuario visita estas páginas Web, la cookie almacenada es reenviada al servidor, proporcionándole información diversa, entre la que se incluyen importantes datos personales como: el número IP, datos sobre el software y hardware, el E-mail del usuario y hasta passwords...
Es por todo ello, que se considera las cookies en la práctica son un poderoso instrumento de obtención de información por parte de los servidores de Internet, que tienen un papel fundamental en el marketing por Internet.

➤ **Protocolos de seguridad**

Para intentar evitar todos estos peligros, las empresas han ideado un sistema que garantiza el secreto en la comunicación, mediante la implantación de

protocolos de comunicación seguros, es decir, sistemas de seguridad informática que permitan conexiones seguras. Entre otros podemos destacar:

- **El protocolo de seguridad SSL** (Secure Sockets Layer), utilizado para la encriptación de una comunicación segura entre el servidor de la empresa y clientes, asegura la confidencialidad e integridad de los datos (se pueden transmitir los datos de la tarjeta sin que nadie los pueda capturar), es fácil de implantar y tiene un coste bajo. La entidad financiera y el cliente autentifican a la empresa.

Estos servidores SSL se identifican porque en la esquina inferior derecha del navegador (en el caso del Explorer) aparece un candado cerrado y además la URL cambia de Http:// a Https:// (Hypertext Transport Protocol Secure).

Presenta los siguientes inconvenientes:

- a. La empresa conoce los datos de pago y el cliente no está autenticado, por lo que puede estar sufriendo un robo o no ser quien dice (incumplimiento del principio de no repudio).
- b. Puede producir desconfianza en el cliente, ya que la entidad vendedora posee su número de tarjeta y no se garantiza la integridad del documento de pago.
- c. El precio de la compra puede verse incrementado por la comisión que las entidades de crédito añaden para compensar el posible fraude con número de tarjetas robados,
- d. El consumidor que paga con tarjeta puede negar la compra del producto y el banco estará obligado a devolver el dinero si “no ha sido presentada directamente o identificada electrónicamente (art. 46 de la Ley 7/96 de Comercio Minorista).
- e. Existe el peligro de que por parte de un tercero se acceda, por motivos ilícitos, a la base de datos de número de las tarjetas de los clientes que estén en posesión de las empresas por lo pagos realizados.

Para evitar este peligro se han ideado los *TPV virtuales* que lanzan los servidores de los bancos para que el pago lo haga directamente el comprador con el banco y no tenga que pasar por el comercio el número de tarjeta, o bien el protocolo SET (Secure Electronic Transaction).

- **El Protocolo SET.** Garantiza íntegramente los principios antes mencionados y un total anonimato por parte de las tres partes intervinientes (cliente, empresa y pasarela de pagos con sus correspondientes certificados digitales), de forma que el banco no conoce la compra que realiza el consumidor y la empresa no conoce el número de tarjeta o de cuenta que tiene el comprador.

Sistema tiene como gran inconveniente, que resulta costosa su implantación (es necesario software específico).

➤ **Sistemas de encriptación**

Junto a las conexiones seguras del tipo del protocolo SSL, SET o a las redes seguras VPN, la articulación de las técnicas de seguridad ha llevado a la utilización de las técnicas de la criptografía y de la firma electrónica.

La Criptografía es una rama de las Matemáticas que, al aplicarse a mensajes digitales, proporciona las herramientas idóneas para solucionar los problemas de confidencialidad, integridad, autenticidad y no repudiación.

Existen fundamentalmente dos sistemas de encriptación:

- De clave simétrica o privada: se cifra el contenido del mensaje con una clave y se envía. El receptor necesita la misma clave para descifrar el mensaje.

El principal problema que plantea es que se ha de enviar la clave al receptor, y ésta puede ser interceptada en la transmisión.

- De clave asimétrica o pública: consiste en crear por medio de un algoritmo matemático dos claves emparejadas y diferentes, una de cifrado y otra de descifrado. No es necesario enviar ninguna clave por ningún canal ya que una de ellas es pública. Esta clave pública (la de cifrado) es conocida por todos los sujetos intervinientes en el sector mientras que la otra sólo la conoce el emisor del mensaje.

De esta forma, para cifrar un mensaje el emisor lo encripta con la clave pública del receptor. Para descifrarlo, el receptor debe aplicar su clave privada.

➤ **Firma digital**

- Concepto

La firma electrónica o digital es un conjunto de datos electrónicos que identifican a una persona determina. Se suelen unir al documento que se envía por medio telemático, como si de la firma manuscrita se tratara, de esta forma el receptor está seguro de quién ha sido el emisor, así como que el mensaje no ha sido alterado o modificado.

- Funcionamiento

La firma electrónica funciona con un método de encriptación de clave pública o asimétrica, es decir, cifrando los datos que la componen, de forma

que si no se tiene la clave, el documento se convierte en ilegible. Para ello es necesario contar con un par de claves: clave privada y clave pública que se corresponden de forma matemática.

Por ejemplo, si escribimos un mensaje y lo firmamos con la clave pública y lo enviamos a nuestro receptor al cual previamente le hemos dado nuestra clave pública, ésta clave pública es la que permite verificar la procedencia del mensaje y que verdaderamente lo hemos firmado nosotros.

Así, para firmar electrónicamente un mensaje, el emisor aplica su clave privada. Para comprobar la firma, el receptor utiliza la clave pública del emisor. Esto impide que el emisor que ha firmado digitalmente el mensaje pueda después negar su autoría. De esta forma, el autor queda vinculado al documento de la firma. Además la validez de dicha firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor. Al ser personal, acredita quién es el autor y que no ha existido ninguna modificación posterior.

- Clases de firma electrónica

La Ley 53/2003 de 19 de diciembre de Firma Electrónica, en adelante LFE, distingue entre:

- 1) **Firma electrónica:** es el conjunto de datos, en forma electrónica, consignados junto a otros o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o a los autores del documento que la recoge.
- 2) **Firma electrónica avanzada:** es la firma electrónica que permite identificar al firmante y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos a los que se refiere, lo que permite que sea detectable cualquier cambio ulterior de los datos firmados.
- 3) **Firma electrónica reconocida:** es la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación firma. Se equipara a la firma manuscrita.

Además de los algoritmos de encriptación asimétrica (que sirven para cifrar y descifrar mensaje), existen otros algoritmos de comprensión necesarios para conseguir que la firma digital tenga los mismos efectos que la manuscrita. Son los algoritmos de comprensión hash. Estos algoritmos aplican funciones de no retorno, que permiten que no sea necesario la tenencia de una clave, ya que aplica funciones matemáticas sencillas para cifrar. Pero los cálculos matemáticos a realizar para el descifrado son imposibles de encontrar. La comprensión crea un texto limitado y reducido de entre 128 y 160 bits que representa la integridad del documento (si se cambia un solo bit del documento

original el resultado obtenido al volver a aplicar la función hash sería totalmente diferente.

➤ **Certificados y autoridades de certificación**

Los certificados son documentos digitales el cual un tercero de confianza (autoridad de certificación) garantiza que una clave pública pertenece a determinado individuo o entidad. Los certificados intentan evitar que alguien utilice una clave falsa haciéndose pasar por otro. Por lo tanto un certificado digital o electrónico es un documento digital que permite la identificación del titular del certificado, intercambiar información con otras personas y entidades de manera segura, y firmar electrónicamente los datos que se envían de tal forma que se pueda comprobar su integridad y procedencia. 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.

Se trata pues de un documento que presenta entre otras ventajas las siguientes:

- Se consigue una mayor seguridad en la identificación, evitando de forma más eficiente la suplantación de la identidad de los usuarios.
- El procedimiento de solicitud de alta en la Oficina es mucho más cómodo, rápido y sencillo, ya que el contrato se firma electrónicamente en lugar de enviarlo firmado por correo postal, fax o escaneado.
- Se facilita el acceso habitual al servicio, ya que se evita tener que recordar la contraseña de usuario y teclear dos campos de acceso (Usuario y Contraseña).

La autoridad Certificación puede emitir distintos tipos de certificados:

- 1) Certificados de identificación: identifican y conectan un nombre a una clave pública.

- 2) Certificados de autorización: ofrecen otro tipo de información correspondiente al usuario, como por ejemplo la dirección comercial, antecedentes, catálogos de productos, etc..
- 3) Otros certificados colocan a la Autoridad Certificante en el rol de notario, pudiendo ser utilizados para dar fe de la validez de un determinado hecho o que un hecho efectivamente ha ocurrido.
- 4) Otros certificados permiten determinar día y hora en que el documento fue digitalmente firmado (fecha digital).

Los usuarios o firmantes son aquellas personas que detentan la clave privada que corresponde a la clave pública identificada en el certificado. Por lo tanto, la principal función del certificado es identificar el par de claves con el usuario o firmante, de forma tal que quien pretende verificar una firma digital con la clave pública que surge de un certificado tenga la seguridad que la correspondiente clave privada es detentada por el firmante. Los certificados se inscriben en un Registro (repository), considerado como una base de datos a la que el público puede acceder directamente *on line* para conocer la validez de un certificado. El interesado en operar dentro del esquema establecido por la ley deberá, una vez creado el par de claves, presentarse ante la autoridad certificante (o funcionario que ella determine) a efectos de registrar su clave pública, acreditando su identidad o cualquier otra circunstancia que le sea requerida para obtener el certificado que le permita firmar el documento de que se trate.

Ejemplo: para realizar una operación financiera con un banco, éste puede requerir al interesado un certificado que acredite, además de la constatación de su identidad, el análisis de sus antecedentes criminales o financieros. Esto quiere decir que la firma digital del interesado sólo será aceptada por la otra parte si cuenta con el certificado apropiado para la operación a realizar.

Actualmente en entre otro tipo de certificados digitales, destacan los siguientes:

- Documento Nacional de Identidad electrónico (DNIe)
- Certificado de usuario de la Fábrica Nacional de Moneda y Timbre (FNMT)

Una Autoridad de Certificación (CA) es esa tercera parte fiable que acredita la ligazón entre una determinada clave y su propietario real. Según la ley son aquellas personas físicas o jurídicas que expiden certificados, pudiendo prestar, además, otros servicios en relación con la firma electrónica.

Actuaría como una especie de notario electrónico que extiende un certificado de claves el cual está firmado con su propia clave, para así garantizar la autenticidad de dicha información. Para evitar que se falsifiquen los certificados, la clave pública de la CA debe ser fiable: una CA debe publicar su clave pública o proporcionar un certificado de una autoridad mayor que certifique la validez de su clave.

6. Contratación *online* de seguros

6.1 Ámbito normativo

- **Legislación española:** las normas reguladoras en el ámbito de los seguros de este tipo de contratación dentro del comercio electrónico son:

Con carácter general, [Ley 22/2007, de 11 de julio, sobre comercialización a distancia de servicios financieros destinados a consumidores](#) (en adelante, LCDSFDC). Mediante la misma se ha producido la incorporación a nuestro Derecho interno de la Directiva comunitaria de idéntico nombre. Directiva 2002/65/CE del Parlamento Europeo y del Consejo de 23 de septiembre de 2002, relativa a la comercialización a distancia de servicios financieros destinados a los consumidores, y por la que se modifican la Directiva 90/619/CEE del Consejo y las Directivas 97/7/CE y 98/27/CE (DOCE L 271, de 9 de octubre de 2002)).

Asimismo, también será de aplicación la normativa general sobre servicios de la sociedad de la información y comercio electrónico que se contiene en la [Ley 34/2002, de 11 de julio, de servicios de la sociedad de la información y comercio electrónico](#) (en adelante, LSSICE) y, en su caso, [en el capítulo II del Título III y disposición adicional primera de la Ley 7/1996, de 15 de enero, de ordenación del comercio minorista](#).

[La Ley de Contrato de Seguro \(LCS\)](#), con anterioridad a la promulgación de la LCDSFDC, también se ocupaba de la contratación a distancia, con enfoque evidentemente sectorial, la DA 1ª (soporte duradero), 2ª (contratación a distancia) y 3ª (contratación electrónica), junto con los arts. 6 bis y 83.a), habían sido introducidas en la LCS por la Ley 34/2003, de 4 de noviembre, de modificación y adaptación a la normativa comunitaria de la legislación de seguros privados (BOE de 5 de noviembre), con el propósito de incorporar parcialmente aquella Directiva. La LCDSFDC (D.Dª) ha derogado el art. 6 bis, los párrs. 2º y 3.º del ap. 1 del art. 83.a) y la disposición adicional segunda LCS, de modo que, en lo sustancial, a partir de su promulgación queda sometida a una sola disciplina la comercialización a distancia (electrónica, pero también telefónica) de prestaciones subsumibles en lo que esta Ley denomina servicios financieros, entre los que se incluyen las operaciones de seguros y planes de pensiones.

Por otra parte, en la medida en que la contratación electrónica representa un caso concreto dentro de la contratación a distancia, aquélla queda asimismo sometida, con ciertos matices, a la disciplina jurídica aplicable a ésta. El régimen jurídico aplicable a la contratación a distancia también ha experimentado recientemente importantes modificaciones. Éstas son debidas a

la promulgación del Real Decreto Legislativo 1/2007, de 16 de noviembre, por el que se aprueba el [Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios](#) y otras leyes complementarias (BOE de 30 de noviembre), promulgado por el Gobierno al amparo de la delegación normativa conferida por la disposición final quinta de la Ley 44/2006, de 29 de diciembre, de mejora de la protección de los consumidores y usuarios (BOE de 31 de diciembre), que habilitó al Gobierno para que, en el plazo 12 meses, procediera a refundir en un único texto la Ley 26/1984, de 19 de julio, General para la Defensa de los Consumidores y Usuarios y las normas de transposición de las directivas comunitarias dictadas en materia de protección de los consumidores y usuarios que incidiesen en los aspectos regulados en ella, regularizando, aclarando y armonizando los textos legales que hubiesen de ser refundidos.

- **Legislación europea:** se aplican a este modelo de contratación electrónica las disposiciones contenidas en los Convenios de Bruselas (1968), Roma (1980), Viena (1980) y Lugano (1988).
- **Legislación comunitaria:** varias son las directivas transpuestas a nuestro derecho que, regulan la contratación en comercio electrónico:
 - Directiva 97/7/CE, 20 de mayo 1997 sobre Comercio a distancia: Protección a consumidores en materia de contratos.
 - Directiva 98/27/CE, del Parlamento Europeo y del Consejo, de 19 de mayo, relativa a acciones de cesación en protección de los intereses de los consumidores.
 - Directiva 2000/31/CE del Parlamento Europeo y del Consejo, de 8 de junio, sobre Comercio Electrónico.
 - Directiva 2002/58/CE, del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales.

6.2 El contrato electrónico: conceptos generales y presupuestos

➤ Concepto y generalidades

Con la expresión comercio electrónico se designa, aunque no existe un concepto inequívoco del mismo, a aquellas operaciones comerciales llevadas a cabo por medios electrónicos o como el conjunto de comunicaciones electrónicas efectuadas con fines publicitarios o contractuales entre las empresas o entre éstas y los consumidores.

Dentro del comercio electrónico, existe una modalidad de operaciones comerciales, que constituyen en sentido estricto la llamada contratación electrónica, es decir, la celebración o conclusión de contratos a distancia usando para ello medios o instrumentos electrónicos.

Al contrato electrónico se refiere la LSSICE, cuando califica, entre otros, de servicio de la Sociedad de la Información (Anexo letra a), *“La contratación de bienes o servicios por vía electrónica”* y también cuando la define en los siguientes términos:

“Todo contrato en el que la oferta y la aceptación se transmiten por medio de equipos electrónicos de tratamiento y almacenamiento de datos, conectados a una red de telecomunicaciones”.

Por su parte, la Ley 22/2007, de 11 de julio, sobre comercialización a distancia de servicios financieros destinados a los consumidores en su artículo 4.3, declara que *“Se entiende que el contrato se celebra a distancia cuando para su negociación y celebración se utiliza exclusivamente una técnica de comunicación a distancia, sin presencia física y simultánea del proveedor y el consumidor, consistente en la utilización de medios telemáticos, electrónicos, telefónicos, fax u otros similares”.*

De lo que se desprende que lo definatorio de esta nueva forma de contratación es el medio (electrónico) a través del cual se emiten las declaraciones de voluntad de las partes del contrato. Por lo que, en esta nueva modalidad de contrato, lo realmente importante no es ni su contenido ni su soporte, sino el cauce digital empleado para la celebración y perfección del contrato. En consecuencia hemos de entender que, a sensu contrario, se excluye del ámbito de aplicación de la LSSI cualquier acto o negocio jurídico que haya sido elaborado o ejecutado por medios electrónicos, pero haya sido perfeccionado *off-line* (presencialmente).

Motivo por el que se afirma que con el comercio electrónico y más concretamente con el contrato electrónico, se está produciendo la desaparición paulatina de la palabra verbal y escrita, siendo sustituida o reemplazada por sus equivalentes electrónicos. Así lo refleja el TS cuando declara que estamos *“asistiendo, en cierto modo, en algunas facetas de la vida, incluso jurídica, al ocaso de la civilización del papel, de la firma manuscrita y del monopolio de la escritura sobre la realidad documental. El documento, como objeto corporal que refleja una realidad fáctica con trascendencia jurídica, no puede identificarse, ya, en exclusiva, con el papel, como soporte, ni con la escritura, como unidad de significación. El ordenador y los ficheros que en él se almacenan constituyen, hoy día, una nueva forma de entender la materialidad de los títulos valores y, en especial, de los documentos mercantiles”.*

➤ **Presupuestos del contrato electrónico**

A) Contrato de seguro a distancia

Aunque la LSSICE, en su definición de contrato electrónico (Anexo letra h) no exige que sea un contrato “a distancia”, de la definición de “Sociedad de la Información” contenida en dicho anexo se desprende que, los contratos electrónicos por su consideración de servicios de la Sociedad de Información

debe ser celebrado “a distancia, por vía electrónica y a petición individual del destinatario”.

En este sentido se manifiesta la Ley 22/2007 de Comercialización a distancia de Servicios Financieros, cuando habla del “régimen de los contratos a distancia” y a lo largo de su articulado (artículos 1, 2, 3. 4.3, etc.).

B) Sujetos del contrato: el proveedor (entidad aseguradora/mediador) y el consumidor (tomador)

La LCDSF en su artículo 5 dispone que “Las partes del contrato a distancia son el proveedor y el consumidor”.

Se considera como proveedor toda persona física o jurídica, privada o pública, que, en el marco de sus actividades comerciales o profesionales, presta un servicio financiero a distancia. A los efectos de esta Ley, se considera como proveedores a quienes intervengan por cuenta propia como intermediarios en cualquier fase de la comercialización.

A los efectos de esta Ley, se consideran como consumidores las personas físicas que, en los contratos a distancia, actúan con un propósito ajeno a su actividad empresarial o profesional”.

De lo que se desprende que, de conformidad con este artículo en relación con la normativa aseguradora (artículo 7 y 8 LCS) y normativa de mediación sólo pueden ser parte del contrato:

- 1) Entidad aseguradora**, como proveedora de servicios financieros (contratos de seguros). Que para actuar en el ámbito de la contratación electrónica debe cumplir con los requisitos previstos en los artículos 2, 3 y 7 de la LCDSF, sin perjuicio de los requisitos exigidos en la normativa aseguradora aplicable.

Mediadores, agentes y corredores que presten servicios financieros a distancia o intervengan por cuenta propia como intermediarios en cualquier fase de la comercialización.

A esta parte del contrato (vendedora) se refiere la LSSICE cuando define en su Anexo letra a) los “Prestador de servicios o prestador: persona física o jurídica que proporciona un servicio de la sociedad de la información”.

- 2) Tomador**, persona física que actúa con un propósito ajeno a su actividad empresarial o profesional, con lo que se excluyen de la normativa de la contratación a distancia de servicios financieros a las personas jurídicas, apartándose de las definiciones que del “destinatario del servicio o destinatario” y “consumidor” contiene el Anexo de la LSSICE, que incluye a las personas jurídicas .

Por su parte, la “Guía de Buenas Prácticas de comercialización en Internet” elaborada por UNESPA y que tiene como finalidad orientar a las entidades aseguradoras para las decisiones que adopten en materia de contratación electrónica, concreta el concepto al referirse al cliente y definirlo como *“aquella persona física con la que la entidad aseguradora tiene o podría tener relación como tomador de un seguro, esto es, como contratante por cuenta propia y sobre cuya persona o bienes recae el riesgo objeto del seguro”*.

C) Forma del contrato electrónico de seguro

Con carácter general, y de modo coherente con el ordenamiento jurídico en que se incardina, la LSSICE, proclama expresamente el principio espiritualista o de libertad de forma, cuando declara que la LSSICE *“Se favorece igualmente la celebración de contratos por vía electrónica, al afirmar la Ley, de acuerdo con el principio espiritualista que rige la perfección de los contratos en nuestro Derecho, la validez y eficacia del consentimiento prestado por vía electrónica, declarar que no es necesaria la admisión expresa de esta técnica para que el contrato surta efecto entre las partes, y asegurar la equivalencia entre los documentos en soporte papel y los documentos electrónicos a efectos del cumplimiento del requisito de forma escrita que figura en diversas leyes”* (Exposición de Motivos, párrafo 1.º del apartado IV).

Consecuentemente lo verdaderamente relevante para poder hablar de un contrato de seguro válido y eficaz no es la forma sino el aspecto consensual o espiritual, o lo que es lo mismo, desde que hay consentimiento válido y eficaz existe contrato, independientemente de la forma utilizada por las partes para manifestarlo, momento en que las mismas quedan obligadas al cumplimiento de lo pactado y a las consecuencias que, según su naturaleza, sean conformes a la buena fe, al uso o a la ley (arts. 1.254 y 1.278 C.c.).

En el mismo sentido, el artículo 23 de la referida ley preceptúa que:

“1. Los contratos celebrados por vía electrónica producirán todos los efectos previstos por el ordenamiento jurídico, cuando concurren el consentimiento y los demás requisitos necesarios para su validez.

Los contratos electrónicos se registrarán por lo dispuesto en este Título, por los Códigos Civil y de Comercio y por las restantes normas civiles o mercantiles sobre contratos, en especial, las normas de protección de los consumidores y usuarios y de ordenación de la actividad comercial.

2. Para que sea válida la celebración de contratos por vía electrónica no será necesario el previo acuerdo de las partes sobre la utilización de medios electrónicos”.

Así pues, para celebrar un contrato electrónico basta con que el cliente emita la declaración de voluntad a través del ordenador, aunque no haya habido contacto anteriormente con la entidad aseguradora. Y por su parte el apartado 3º añade que, la exigencia legal de que un contrato o cualquier documento relacionado con él se documente por escrito, se entenderá cumplida si el contrato o la información de que se trate constan en soporte electrónico.

En el mismo sentido, la D.A.1ª de la LCS, relativa al soporte duradero, establece que *“siempre que esta ley exija que el contrato de seguro o cualquier otra información relacionada con el mismo conste por escrito, este requisito se entenderá cumplido si el contrato o la información se contienen en papel u otro soporte duradero que permita guardar, recuperar fácilmente y reproducir sin cambios el contrato o la información”*. Soporte duradero que a su vez, la LCDSF, en su artículo 4.1 exige para dejar constancia de las ofertas y la celebración de los contratos y que define en los siguientes términos:

“(…)Por soporte duradero se entiende todo instrumento que permita al consumidor almacenar la información dirigida personalmente a él, de modo que pueda recuperarla fácilmente durante un período de tiempo adecuado para los fines para los que la información está destinada y que permita la reproducción sin cambios de la información almacenada”.

De esta forma se establece el denominado principio de equivalencia entre los documentos con *“soporte papel”* y los documentos en *“soporte electrónico”*. Se consagra legalmente para aquellos casos en que una norma exija forma escrita en cuanto requisito de validez, y que despliega efectos en materia probatoria. En éste último sentido, la Ley de Firma Electrónica declara que *“se considera documento electrónico la información de cualquier naturaleza en forma electrónica, archivada en un soporte electrónico según un formato determinado y susceptible de identificación y tratamiento diferenciado”* (art. 3.5, ap. 1.º), y que *“el soporte en que se hallen los datos firmados electrónicamente será admisible como prueba documental en juicio”* (art. 3.8, primer inciso) carácter probatorio que recoge la LISSICE en su art. 24.3.

6.3 Solicitud y propuesta *on line* del seguro

En la contratación electrónica, la solicitud es el acto mediante el cual el consumidor, es decir, el potencial tomador se dirige a través de la Red a una entidad de seguros con el propósito de, eventualmente, contratar *on line* un seguro. Solicitud que se caracteriza por no resultar vinculante para quien la realiza, de manera que quien ha hecho una solicitud de seguro si por cualquier motivo decide no contratar el seguro, está perfectamente legitimado para no hacerlo.

Una vez solicitada la celebración del seguro, el asegurador hace una oferta *on line* al potencial tomador que contiene todos los elementos esenciales para su conclusión, con el fin de concluir un contrato de seguro una vez que éste acepte. Por lo tanto, la oferta es una declaración de voluntad unilateral en la que el oferente (asegurado) propone la celebración de un contrato al destinatario y, además, concreta los requisitos del mismo, de manera que, si el destinatario los acepta, se entiende perfeccionado el contrato.

La oferta o proposición del seguro debe ser completa, por lo que se exige que contenga las condiciones y elementos del contrato del seguro (objeto, interés, clase, duración, cuantía de las prestaciones y definición del riesgo), y las condiciones generales. Asimismo, ha de contener la firma del asegurador y dirigirse al peticionario.

La proposición del seguro que contiene la oferta del contrato de seguro, vincula a la entidad aseguradora por un plazo de 15 días o el plazo mayor a que se comprometa la entidad en la oferta realizada. Es decir, si se recibe una oferta o proposición de seguro por parte de una entidad o sus agentes, esa oferta no puede ser retirada ni sus condiciones modificadas durante un plazo de 15 días o el plazo mayor a que se haya comprometido la entidad.

Si se acepta dicha oferta por parte del destinatario a través de medios electrónicos y dentro de ese plazo, al concurrir *“la oferta y la aceptación sobre la cosa y la causa que ha de constituir el contrato”* (art.1262 CC y Anexo LSSICE letra h), el contrato se entiende perfeccionado y desde ese momento las partes quedan obligadas al cumplimiento de lo expresamente pactado y a las consecuencias que según su naturaleza, sean conforme a la buena fe y a la ley.

Por ultimo debemos señalar que, la Ley de Comercialización a distancia de Servicios Financieros establece que antes de la celebración del contrato de seguro a distancia, el asegurador deberá poner a disposición del consumidor, antes de que ninguna obligación nazca para este último, la siguiente información:

En cuanto a la entidad aseguradora:

- La identidad de la entidad aseguradora, su domicilio y su dirección a efectos de sus relaciones con los tomadores y asegurados.
- Si interviene algún representante legal de la entidad, se hará constar también su identidad.
- Si interviene un mediador de seguros, identificación del mismo.
- Identificación de los Registros Públicos en que está inscrita la entidad (Registro Mercantil y Registro administrativo de entidades aseguradoras) y número de registro.
- Autoridad encargada de la supervisión de la entidad.

Esta información, deberá suministrarse indicando expresamente su finalidad comercial y se comunicará de manera clara y comprensible por

cualquier medio que se adapte a la técnica de comunicación a distancia utilizada, respetando debidamente, en particular, los principios de buena fe en las transacciones comerciales y los principios que regulan la protección de las personas que carecen de capacidad de obrar y los derechos en materia de accesibilidad universal de las personas con discapacidad.

En cuanto al seguro:

- Descripción de las principales características del contrato de seguro.
- El precio total que debe satisfacer el tomador por el seguro, con inclusión de todas las comisiones, cargas y gastos, así como todos los impuestos pagados a través de la entidad aseguradora.
- Indicación del periodo para el que es válida la información suministrada.
- Modalidades de pago y ejecución.
- Si es el caso, indicación del coste suplementario que supone contratar a distancia.

En cuanto al contrato a distancia:

- Si existe o no derecho de desistimiento y, en su caso, el plazo y condiciones para su ejercicio.
- La duración contractual mínima.
- Información sobre la existencia o no de derechos, distintos del de desistimiento, que puedan tener las partes para resolver el contrato y las condiciones para su ejercicio.
- Estado en cuya legislación se basan las relaciones precontractuales, ley aplicable al contrato y jurisdicción a la que acudir en caso de conflicto.
- Lengua o lenguas en que se presenta la información previa al contrato y la lengua o lenguas en que puede formalizarse el mismo.

En cuanto a los medios de reclamación e indemnización:

- A qué sistemas de resolución extrajudicial de conflictos, de carácter público o privado, puede el consumidor tener acceso y cómo puede acceder a ellos.
- La existencia de fondos de garantía u otros mecanismos de indemnización, sean de carácter obligatorio o voluntario.
- Deberán cumplirse además, todos los requisitos de información previa al tomador que se exigen en todos los contratos de seguros, sean o no realizados a distancia.

Se trata de una información que el asegurador debe comunicar al consumidor junto con todas las condiciones contractuales, en soporte de papel u otro soporte duradero accesible al mismo, con suficiente antelación a la posible celebración del contrato a distancia o a la aceptación de una oferta y, en todo caso, antes de que el consumidor asuma las obligaciones mediante cualquier contrato a distancia u

oferta. Sin embargo, en caso de que el contrato no se hubiera celebrado a petición del tomador y utilizando una técnica de comunicación a distancia que no permita cumplir al asegurador con dichas obligaciones, éste deberá cumplirlas después de la perfección del seguro.

En el supuesto de incumplimiento de los requisitos relativos a la información previa que se deriven de los contratos, así como los relativos a la comunicación de dicha información previa, señala la ley (art. 9.4 LCDSF) que podrá dar lugar a la nulidad de los contratos, de acuerdo con lo previsto en la legislación española.

6.4 Momento y lugar de perfeccionamiento del contrato de seguro electrónico

En cuanto al momento en que han de reputarse perfeccionados los contratos electrónicos, resultan de aplicación las reglas generales aplicables en materia de contratación entre ausentes. Se encuentran éstas comprendidas en los arts. 1.262 CC y 54 C.Com., a los que la LSSICE ha dado nueva redacción, unificando su regulación y poniendo fin a una situación formal de disparidad de soluciones civil y mercantil

Con arreglo a los preceptos indicados en la D.A. 4ª, como regla general, se dispone que:

“El consentimiento se manifiesta por el concurso de la oferta y de la aceptación sobre la cosa y la causa que han de constituir el contrato.

Hallándose en lugares distintos el que hizo la oferta y el que la aceptó, hay consentimiento desde que el oferente conoce la aceptación o desde que, habiéndosela remitido el aceptante, no pueda ignorarla sin faltar a la buena fe. El contrato, en tal caso, se presume celebrado en el lugar en que se hizo la oferta.

En los contratos celebrados mediante dispositivos automáticos hay consentimiento desde que se manifiesta la aceptación.”

Solución que supone adoptar la llamada “teoría de la recepción”, en virtud de la cual el contrato debía reputarse perfeccionado no ya cuando el oferente tuviese efectivo conocimiento de la aceptación, sino cuando ésta pudiese ser razonablemente conocida por aquél. Con esta formulación legal se evita, en definitiva, que la perfección del contrato seguro quede al arbitrio de quien, pudiendo haber conocido la declaración negocial de aceptación de la oferta, no llega, sin embargo, a conocerla de modo efectivo por malicia o negligencia.

Por todo lo anterior, en el ámbito asegurador surge la cuestión de cuando se perfeccionan los seguros electrónicos en el caso de que el tomador emita su aceptación vía e-mail o vía los dispositivos establecidos al efecto en la página Web. Cuestión que debe ser resuelta conforme a lo establecido en el art. 28.2 de

la LSSICE, que entiende que se ha recibido la aceptación y su confirmación cuando las partes a las que se dirijan puedan tener constancia de ello. Por lo que se estará al momento de recepción del acuse de recibo de la aceptación: se presume que el asegurador tiene constancia desde el momento en que hay sido almacenado en el servidor en que esté dada de alta su cuenta de correo electrónico o en el dispositivo utilizado para la recepción de comunicaciones.

De esta forma, la perfección del contrato de seguro aceptado por correo electrónico tiene lugar con la recepción del mensaje por el asegurador (momento en el cual puede tener acceso al mismo), lo que desde el punto de vista técnico, se produce cuando los datos entran en el servidor del destinatario.

En el caso que se contrate el seguro a través de la página Web, éste se perfeccionará en el momento en que el tomador del seguro manifieste su aceptación utilizando el mecanismo dispuesto en la página por la aseguradora. Desde el punto de vista técnico, el tomador puede tener constancia de ésta en el momento en que el mensaje de datos es recibido por el dispositivo que la página emplea para la recepción de comunicaciones.

Esta regla general tiene una excepción, conforme a la cual *“en los contratos celebrados mediante dispositivos automáticos hay consentimiento desde que se manifiesta la aceptación”* (art. 54.2 C.Com. y art. 1.262.3 Cc), que se traduce en que el contrato se perfecciona cuando el aceptante emite su declaración negocial de aceptación *“teoría de la emisión o declaración”*. Lo que se discute es qué deba considerarse a estos efectos *contratos celebrados mediante dispositivos automáticos*. Y aunque no existe, parece razonable pensar que esta regla especial es aplicable a los contratos celebrados electrónicamente y en los que no llega a producirse un auténtico diálogo negocial entre las partes contratantes, dado que ese diálogo tiene lugar entre el cliente-aceptante y la máquina oferente a través de una página Web en la que se indican al aceptante (mediante iconos: cesta o carro de la compra, etc.) los sucesivos pasos que debe dar, o sea, los llamados contratos electrónicos celebrados mediante simple pulsación de teclas.

Finalmente, en relación al lugar de celebración de los contratos electrónicos en los que intervenga como parte un consumidor señala la ley que se presumirán celebrados en el lugar en que éste tenga su residencia habitual (art. 29.1 LSSICE), en tanto que si ambos contratantes actúan empresarialmente (29.2) se presumirán celebrados en el lugar en que esté establecido el prestador de servicios, salvo que las partes acuerden otra cosa.

6.5 La prueba del contrato electrónico

En relación a la prueba del contrato de seguro, podemos distinguir dos ámbitos probatorios: la prueba de la aceptación del contrato de seguro y la prueba del contenido del procedimiento contractual.

➤ Prueba de la aceptación del contrato de seguro electrónicos

La LSSICE, en su artículo 28 relativo a la información posterior a la contratación, tipifica los medios de confirmar la recepción que se caracterizan por no garantizar la inalterabilidad del mensaje y sólo su recepción por el destinatario.

De esta forma, se otorga mayor protección a los consumidores a través de los siguientes medios:

- 1) Un acuse de recibo por correo electrónico u otro medio de comunicación electrónica equivalente**, que debe enviarse a la dirección que el aceptante haya señalado, en el plazo de las veinticuatro horas siguientes a la recepción de la aceptación.

Por lo tanto, la aseguradora enviará al tomador el mensaje electrónico que acredite la llegada y recepción de la aceptación del contrato. Acuse de recibo que puede incluir los requisitos técnicos del mensaje recibido, concretamente la sintaxis informática o la legibilidad del mensaje, garantizando con ello no sólo la recepción del mensaje por el tomador sino que también lo ha leído.

Se presumirá que su destinatario puede tener la referida constancia desde que aquel haya sido almacenado en el servidor en que esté dada de alta su cuenta de correo electrónico, o en el dispositivo utilizado para la recepción de comunicaciones.

- 2) La confirmación de la aceptación recibida**, por un medio equivalente al utilizado en el procedimiento de contratación y al finalizar éste, siempre que la confirmación pueda ser archivada por su destinatario.

De esta forma, el asegurador puede comprobar el contenido del mensaje de aceptación que envió, el origen, la fecha... pudiendo ampliar la confirmación de la recepción al contenido de la misma.

Se entenderá que el asegurador ha recibido la aceptación y su confirmación cuando el tomador pueda tener constancia de ello.

Por último, la ley señala que no será necesario confirmar la recepción de la aceptación de una oferta cuando:

- “Ambos contratantes así lo acuerden y ninguno de ellos tenga la consideración de consumidor, o”*, excepción no aplicable en el ámbito asegurador cuando el tomador sea una persona física, dado tiene condición de consumidor siempre.

- b. *“El contrato se haya celebrado exclusivamente mediante intercambio de correo electrónico u otro tipo de comunicación electrónica equivalente, cuando estos medios no sean empleados con el exclusivo propósito de eludir el cumplimiento de tal obligación”.*

➤ **La prueba del contenido del procedimiento contractual**

La LSSICE declara en materia de la prueba del contrato electrónico y partiendo de la libertad de forma que rige todo el ordenamiento jurídico, la aplicabilidad de las reglas generales, remitiendo en particular, a la llamada firma electrónica. Por este motivo era necesario que se elevase el soporte electrónico a la categoría de prueba documental, equivalente a la del soporte papel. Acometido que se ha llevado a cabo a través del artículo 24.2 de la LSSICE, así como de la DA 1ª de la LCS, y el artículo 3 de la Ley de la Firma Electrónica.

Ello significa en la práctica que, el soporte electrónico en el que conste un negocio jurídico concluido por vía telemática o informática será, a estos efectos, una prueba documental y no una mera prueba complementaria sujeta a las reglas de la sana crítica (arts. 299.1 y 2 y 384.3 LEC), por lo que diremos que lo que constituye la prueba documental no es el soporte electrónico en sí, sino puesto en relación con su contenido o información que suministra, por medio de la firma electrónica.

En función de que exista la firma electrónica o no, y en qué términos, nos podemos encontrar con las siguientes situaciones:

- 1) Documentos electrónicos no firmados electrónicamente: hasta la promulgación de la LSSICE, pese a existir soporte electrónico, la falta de firma electrónica impedía que estos documentos se pudiesen calificar de documento electrónico comprendido a los efectos del art. 3.5 LFE. No obstante lo anterior, su eficacia probatoria sería la resultante de los arts. 299.2 y 384 LEC, de los que se infiere que serán admisibles como medios de prueba y serán valorados por el juez conforme a las reglas de la sana crítica.

La LSSICE ha modificado la redacción del art. 3.5 LFE, ampliando el concepto legal de documento electrónico, pero sin alterar su eficacia probatoria en los términos que acabamos de indicar.

- 2) Documentos con firma electrónica simple. Éstos reciben, la consideración legal de documentos electrónicos a tenor del art. 3.5 LFE, pero su eficacia probatoria es la que resulta de los arts. 299.2 y 384 LEC, dado que para que puedan ser considerados como prueba documental los documentos electrónicos deben tener firma electrónica avanzada.
- 3) Documentos con firma electrónica avanzada. Éstos se equiparan a efectos probatorios, a los documentos en soporte papel con firma manuscrita, con la salvedad de que en caso de impugnación de la autenticidad de la firma

electrónica resulta de aplicación el art. 326.2 LEC (relativo a la fuerza probatoria de los documentos privados).

- 4) Documentos con firma electrónica reconocida, que se equiparan a todos los efectos a los documentos privados con firma manuscrita. Para el caso de impugnación de la autenticidad de la firma, se establece un procedimiento especial (art. 3.8 LFE), consistente en la comprobación de si concurren o no los requisitos o elementos constitutivos de una firma electrónica avanzada.
- 5) Documentos electrónicos bajo condiciones acordadas, en cuyo caso se estará a lo acordado entre los interesados (art. 3.10 LFE).

Por otro lado, el art. 25 de la LSSICE se refiere a la posibilidad de garantizar la prueba de los contratos electrónicos mediante el acuerdo entre los contratantes, en cuya virtud se encomienda a un tercero el archivo y custodia de las declaraciones negociales producidas por vía telemática. En tal caso, y siempre que este tercero acepte el encargo, quedará obligado a archivar en soporte informático las declaraciones negociales de los contratantes, durante el plazo acordado, que no podrá ser inferior a cinco años.

Una de las primeras empresas españolas en actuar en este sector ha sido “terceros de confianza, S.L.”, A la misma actividad, entre otras, se dedica la entidad pública CERES “Certificación Española”, que es una entidad pública de certificación que también ofrece este servicio.

6.6 El derecho de desistimiento del tomador

El derecho del desistimiento del destinatario o cliente en el caso de la contratación electrónica se haya recogido expresamente para contratos electrónicos de servicios financieros en la LCDSF (art. 10). Se trata de un derecho que obedece a la necesidad de tutelar la libertad de decisión del cliente final en la celebración del contrato *on line*, al permitirle reconsiderar con libertad su decisión aun después de haber celebrado el contrato

Desde el punto de vista de su naturaleza jurídica, nos hallamos realmente ante un derecho de desistimiento o de arrepentimiento del tomador de vincularse contractualmente con la entidad aseguradora sin indicación de los motivos por lo que lo hace y sin penalización alguna. Por lo tanto, no se trata de una resolución o resolución del contrato de seguro.

Como excepciones al derecho de desistimiento, la ley establece que no se aplicará a los siguientes contratos de seguros:

- (1) contratos de seguro en los que el tomador asume el riesgo de la inversión, así como los contratos en los que la rentabilidad garantizada esté en función de inversiones asignadas a los mismos,

- (2) los de viaje o equipaje de una duración inferior a un mes,
- (3) aquéllos cuyos efectos terminen antes del plazo al que se refiere el apartado 1,
- (4) los que den cumplimiento a una obligación de aseguramiento del tomador,
- (5) los planes de previsión asegurados.

Para ejercer dicha facultad, el tomador dispondrá de un plazo de 30 días naturales en el caso de contratos relacionados con los seguros de vida o de catorce días, para el resto de seguros, a contar desde la celebración del contrato. No obstante, si el tomador no hubiera recibido las condiciones contractuales y la información contractual previa exigida por la ley (art. 7.1 LCDSF), el cómputo del plazo sería desde el día que reciba la citada información.

El tomador para ejercer su derecho de desistimiento, lo ha de comunicar a la entidad aseguradora en los términos previstos por el contrato, antes de que finalice el plazo correspondiente, por un procedimiento que permita dejar constancia de la notificación por cualquier medio admitido en Derecho. Sin embargo, la ley considera que la notificación se ha hecho dentro de plazo si se hace en un soporte de papel o sobre otro soporte duradero, disponible y accesible al destinatario, y se envía antes de expirar el plazo.

Asimismo, en dicho precepto se prevé que cuando el consumidor ejerza el derecho de desistimiento, sólo estará obligado a pagar el servicio financiero realmente prestado, hasta el momento del desistimiento, y cuyo importe no podrá ser superior al importe proporcional de la cobertura (principal) total del contrato.

Por último, señalar que se trata de un derecho que también está recogido en el Texto Refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, cuyo artículo 62.3 establece que el consumidor podrá ejercer su derecho a poner fin al contrato en la misma forma en que lo celebró, sin ningún tipo de sanción o cargas onerosas o desproporcionadas (tales como las pérdidas de las cantidades pagadas por adelantado, el abono de las cantidades por servicios no prestados efectivamente, etc).

6.7 El marco jurídico y sus aplicaciones prácticas

Si analizamos desde un punto de vista jurídico la difícil cuestión de comercializar seguros a través de Internet, resulta evidente la gran complejidad de la materia y la dificultad de cumplir con las numerosas normas que son aplicables. Ello nos lleva a pensar que hay una creciente oposición entre la realidad (la irrupción de las nuevas tecnologías que cada vez hacen más fácil, segura y fiable la contratación electrónica de seguros) y la normativa (cada vez hay más leyes que regulan la materia, resultando algunas de las mismas en la práctica imposibles o muy difíciles de cumplir). A lo que debemos añadir la falta de jurisprudencia interpretativa de estas nuevas exigencias normativas.

La Ley 56/2007, de Medidas de Impulso de la Sociedad de la Información señala que, la distribución de productos por Internet requiere de determinadas garantías en cuanto a:

- Identificación del cliente.
- Autenticidad del contrato.

Por lo tanto, las entidades aseguradoras deben adoptar las medidas técnicas necesarias que permitan la contratación y demás trámites de forma segura.

De todos los métodos técnicos que resultan seguros, sólo la firma electrónica reconocida tiene el mismo valor probatorio que la firma manuscrita consignada en papel. El sistema de doble PIN u otros sistemas similares cuya utilización permite la Ley de Firma Electrónica de 2003, no tiene la misma seguridad ni, los datos consignados en forma electrónica, el mismo valor.

En relación con la contratación tradicional, la contratación electrónica de los seguros sin disposición de firma electrónica reconocida, introducen riesgos de repudio:

1. de contenido, fecha y hora de las comunicaciones y
2. de la capacidad del contratante o representante del contratante.

Por ello, en caso de repudio, la situación en la que nos encontraríamos sería la misma que en el caso de que no se disponga de una copia del contrato firmado en por un canal presencial.

Esta ausencia en la práctica de una solución técnica que proporcione seguridad jurídica, ocasiona a las entidades o mediadores que quieran comercializar sus productos a través de Internet los siguientes problemas:

- **Incumplimiento de la obligación de conservación del documento electrónico**

La normativa de contratación a distancia establece la obligación de conservación del documento electrónico a efectos de prescripción y de prueba de la celebración del contrato y de su contenido.

Obligación que en la realidad, únicamente se realiza con garantías por aquellas entidades que disponen de la infraestructura necesaria para la implantación de la firma electrónica reconocida en la contratación de sus productos.

Las entidades aseguradoras por regla general, no disponen de dispositivos de firma electrónica reconocida para la contratación on line, por lo que no tampoco pueden conservar el documento electrónico que contiene el contrato.

Se guardan los datos mediante *logs*, que son registros oficiales utilizados para registrar datos o información sobre quién, qué, cuándo, dónde y por qué. Este sistema sólo permite guardar las 'trazas' de las condiciones particulares durante un tiempo determinado (un máximo de 5 años), pero no permite la conservación de las pantallas ni de los documentos que visualiza el cliente durante el proceso de contratación.

No obstante, sería necesario grabar y conservar el itinerario electrónico, el contenido de todos los documentos y páginas accedidas, así como la constancia del PIN utilizado. Dicha información debiera conservarse como mínimo 6 años desde la fecha de cancelación de la póliza, debiéndose prorrogar en caso de reclamación.

En caso de juicio, estos *logs* pueden ser aportados como prueba, pero el hecho de que no permitan hacer referencia al contenido del contrato firmado debilita mucho su fuerza probatoria. Asimismo, resulta escaso el plazo de conservación del documento.

Para reforzar el valor probatorio, mientras no se disponga de firma electrónica reconocida, es recomendable la contratación de servicios ofrecidos por "terceros de confianza" que permitan archivar las declaraciones de voluntad que integran los contratos electrónicos y acreditar, con un nivel razonable de seguridad jurídica, el contenido, la fecha y hora de los registros grabados durante la contratación.

- **Falta de prueba del consentimiento expreso e informado de los clientes**

La falta de medios técnicos seguros, dificulta el cumplimiento de la normativa de protección de datos. En el sentido de probar que, por parte de la entidad aseguradora se ha obtenido el consentimiento inequívoco de sus clientes en la recogida, cesión o tratamiento de los datos personales, en la realización de operaciones como la contratación *on line*, comunicaciones, declaraciones de estado de salud...

En la práctica este consentimiento se articula mediante la aceptación de las cláusulas de protección de datos que las entidades tienen en su página Web. Por lo que la prueba de dicho consentimiento resulta de difícil acreditación ante los tribunales.

- **Aceptación de cláusulas limitativas**

Existe otra particularidad legal de difícil cumplimiento en la contratación electrónica, como es la necesidad de destacar y aceptar expresamente las cláusulas limitativas del contrato de seguro, tal y como previene el art. 3 de la Ley 50/80 del Contrato de Seguro.

Al igual que en los supuestos de contratación tradicional, aunque la jurisprudencia considera el pago de la prima como acto presunto que convalida la falta de consentimiento del contrato, esta convalidación no alcanzaría a la aceptación de las cláusulas limitativas del contrato. El régimen específico de aceptación de tales cláusulas requeriría del conocimiento y aceptación por parte del tomador o un representante legitimado para ello, mediante un medio seguro como es la firma electrónica reconocida.

Por lo que las entidades que no disponen de un dispositivo de firma electrónica reconocida, podrían atemperar el riesgo mediante:

- Reconducción de las cláusulas limitativas a las cláusulas delimitadoras, o
- Diseño de productos con amplias coberturas y pocas exclusiones, o
- Con coberturas muy concretas y específicas

En caso de repudio, la situación es la misma que en la contratación presencial sin firma específica de las cláusulas limitativas.

A las dificultades que entraña el no disponer de medios técnicos que garanticen la confidencial, autenticación y el no repudio de las operaciones comerciales, se suman el difícil cumplimiento por las aseguradoras de otras obligaciones como:

- **Poder revocar el consentimiento en el envío publicitario y/o comercial (LOPD)**

La remisión de publicidad por canales electrónicos requiere la previa aceptación expresa por parte del cliente.

Como en el canal presencial, debiera permitirse al cliente oponerse a la remisión de publicidad, por medios electrónicos o en papel. Por un medio sencillo y gratuito.

Obligación de acreditar el cumplimiento del deber de información del 5 LOPD a través de los medios adecuados al efecto, los cuales habrán de conservarse durante todo el tratamiento de los datos personales obtenidos.

- **Resolución por mismo canal de contratación y derecho de desistimiento**

Otro problema que nos encontramos en la contratación electrónica, es el tema de la resolución por mismo canal de contratación y derecho de desistimiento.

Por un parte, la normativa protectora de los consumidores y usuarios establece que el consumidor podrá ejercer su derecho a poner fin al contrato en la misma forma en que lo celebró, sin ningún tipo de sanción o cargas onerosas o desproporcionadas (tales como las pérdidas de las cantidades

pagadas por adelantado, el abono de las cantidades por servicios no prestados efectivamente, etc).

Por otro lado, en la ley de comercialización a distancia de servicios financieros destinados a consumidores se prevé que cuando el consumidor ejerza el derecho de desistimiento, sólo estará obligado a pagar el servicio financiero realmente prestado, hasta el momento del desistimiento, y cuyo importe no podrá ser superior al importe proporcional de la cobertura (principal) total del contrato. Derecho unilateral del cliente que podría considerarse absolutamente injustificado en la venta *on line* dado que el tomador puede tomarse el tiempo que crea oportuno para la conclusión de su contrato.

Todas las dificultades enumeradas pueden llevar a pensar que los seguros no deberían comercializarse a través de Internet, pero no parece sea razonable que la norma dictada para regular una actividad tenga como consecuencia hacer imposible esa actividad. Debemos entender, por tanto, que debe esperarse por parte de los supervisores o autoridades judiciales una interpretación razonable de la normativa que haga posible su cumplimiento, sin olvidar que *“las normas se interpretarán atendiendo a la realidad social del tiempo en que han de ser aplicadas”* (art. 3 del Cc), pero sin olvidarnos del principio fundamental de seguridad jurídica consagrado por la CE.

7. Capítulo de conclusiones

Tras el análisis en la presente tesis de las implicaciones que para las entidades aseguradoras supone el desarrollo del comercio electrónico por las mismas, podemos realizar las siguientes reflexiones:

- Las entidades aseguradoras se hallan en un proceso de transformación como consecuencia del desarrollo del comercio electrónico y de las exigencias normativas. Pasan de un modelo en el que utilizan Internet como canal de comunicación y/o como herramienta de marketing, a la utilización de Internet como canal de venta.
- Este nuevo modelo de negocio, sin embargo, presenta una variada problemática legal y tecnológica que aun está lejos de solucionarse. En concreto, el medio de acreditar el consentimiento prestado por parte de los consumidores a través de este canal no es equiparable a la firma manuscrita en soporte papel, salvo cuando se lleva a cabo a través de la firma electrónica reconocida, de escasa implantación hasta ahora.
- La principal consecuencia de utilizar dispositivos de firma menos seguros (por ejemplo el método del doble pin) produce como consecuencia la falta de eficacia probatoria indubitada a la hora de que el cliente preste su consentimiento en materias de tal relevancia como el consentimiento para el tratamiento de sus datos de carácter personal (incluidos los de salud), la aceptación de las cláusulas limitativas y las exclusiones, la firma de los cuestionarios de salud, etc ..., que puede suponer un riesgo de repudio de dicho consentimiento con el consiguiente perjuicio para las entidades aseguradoras.
- La normativa actual en esta materia se caracteriza, por un lado por establecer mecanismos tecnológicamente muy avanzados a implementar por las empresas, y los ciudadanos, sin adaptarse a la realidad social que todavía no alcanza este grado de desarrollo tecnológico; y por otro, a imponer exigencias normativas y administrativas que son de difícil cumplimiento tanto para las entidades aseguradoras, como para los ciudadanos.
- Ante esta realidad, las entidades han de valorar la estrategia a seguir en la implantación de este modelo de venta directa de seguros. Pueden adoptar la decisión de convertirse en empresas de venta directa de todo tipo de seguros, con la inevitable consecuencia de asumir riesgos de negocio. Pueden también decidir adoptar una posición conservadora y comercializar únicamente aquellos seguros que no presentan prácticamente ningún riesgo en su venta, pero lo que no deberían en ningún caso decidir es no estar presente en Internet: "Quien no está en Internet no está en el mundo."

8. Bibliografía

Libros:

1. ICEA (2007) *Comercio electrónico: Venta de seguros por Internet*
2. AECEMfecemd (2007). *Libro blanco del comercio electrónico. Guía Práctica de Comercio Electrónico para PYMES*
3. *Derecho de la Contratación Electrónica – Rafael Illescas Ortiz – Editoria Civitas – 2001.*
4. (MIRANDA SERRANO, «La contratación a distancia [y electrónica]», cit., p. 337);

Artículos y Estudios:

1. Suñé Llinás, Emilio. IIº Congreso Mundial de Derecho Informático (2006). *La protección de datos personales en Internet*
2. Capgemini, revista Actualidad Aseguradora (2010). *El X Informe de Capgemini sobre el Sector Asegurador.*
3. Comisión del Mercado de las Telecomunicaciones (III Trimestre 2009). *Informe sobre el comercio electrónico en España a través de entidades de medios de pago.*
4. Capgemini, revista Actualidad Aseguradora (2010). *Cómo mejorar el negocio manteniendo la orientación al cliente.*
5. ONTSI (Septiembre de 2009). *Estudio sobre Comercio Electrónico B2C 2009.*
6. Red.es (2008). *Estudio de servicios para la empresa asociados a la implantación del DNI electrónico.*
7. Capgemini, revista Actualidad Aseguradora (2010). *Integración de canales y redes*

Webs: www.icea.es, www.capgemini.es, www.inese.es, www.ineas.es, www.wikipedia.com, www.notitiasjuridicas.com, www.rbi.es, www.boe.es, www.google.es, www.aimc.es

Mireia Rubio Cantisano

Licenciada en Derecho por la Universidad de Barcelona en el año 2002.

En mayo de 2008 se incorpora al grupo SegurCaixaHolding, en el Área Jurídica y Fiscal como abogada de la parte de seguros individuales.

COLECCIÓN “CUADERNOS DE DIRECCIÓN ASEGURADORA”

Máster en Dirección de Entidades Aseguradoras y Financieras
Facultad de Economía y Empresa. Universidad de Barcelona

PUBLICACIONES

- 1.- Francisco Abián Rodríguez: “Modelo Global de un Servicio de Prestaciones Vida y su interrelación con Suscripción” 2005/2006
- 2.- Erika Johanna Aguilar Olaya: “Gobierno Corporativo en las Mutualidades de Seguros” 2005/2006
- 3.- Alex Aguyé Casademunt: “La Entidad Multicanal. Elementos clave para la implantación de la Estrategia Multicanal en una entidad aseguradora” 2009/2010
- 4.- José María Alonso-Rodríguez Piedra: “Creación de una plataforma de servicios de siniestros orientada al cliente” 2007/2008
- 5.- Jorge Alvez Jiménez: “innovación y excelencia en retención de clientes” 2009/2010
- 6.- Anna Aragonés Palom: “El Cuadro de Mando Integral en el Entorno de los seguros Multirriesgo” 2008/2009
- 7.- Maribel Avila Ostos: “La tele-suscripción de Riesgos en los Seguros de Vida” 2009/2010
- 8.- Mercé Bascompte Riquelme: “El Seguro de Hogar en España. Análisis y tendencias” 2005/2006
- 9.- Aurelio Beltrán Cortés: “Bancaseguros. Canal Estratégico de crecimiento del sector asegurador” 2010/2011
- 10.- Manuel Blanco Alpuente: “Delimitación temporal de cobertura en el seguro de responsabilidad civil. Las cláusulas claims made” 2008/2009
- 11.- Eduard Blanxart Raventós: “El Gobierno Corporativo y el Seguro D & O” 2004/2005
- 12.- Rubén Bouso López: “El Sector Industrial en España y su respuesta aseguradora: el Multirriesgo Industrial. Protección de la empresa frente a las grandes pérdidas patrimoniales” 2006/2007
- 13.- Kevin van den Boom: “El Mercado Reasegurador (Cedentes, Brokers y Reaseguradores). Nuevas Tendencias y Retos Futuros” 2008/2009
- 14.- Laia Bruno Sazatornil: “L'ètica i la rentabilitat en les companyies asseguradores. Proposta de codi deontològic” 2004/2005
- 15.- María Dolores Caldés Llopis: “Centro Integral de Operaciones Vida” 2007/2008
- 16.- Adolfo Calvo Llorca: “Instrumentos legales para el recobro en el marco del seguro de crédito” 2010/2011
- 17.- Ferran Camprubí Baiges: “La gestión de las inversiones en las entidades aseguradoras. Selección de inversiones” 2010/2011
- 18.- Joan Antoni Carbonell Aregall: “La Gestió Internacional de Sinistres d'Automòbil amb Resultat de Danys Materials” 2003-2004
- 19.- Susana Carmona Llevadot: “Viabilidad de la creación de un sistema de Obra Social en una entidad aseguradora” 2007/2008
- 20.- Sergi Casas del Alcazar: “El PPlan de Contingencias en la Empresa de Seguros” 2010/2011
- 21.- Francisco Javier Cortés Martínez: “Análisis Global del Seguro de Decesos” 2003-2004
- 22.- María Carmen Ceña Nogué: “El Seguro de Comunidades y su Gestión” 2009/2010
- 23.- Jordi Cots Paltor: “Control Interno. El auto-control en los Centros de Siniestros de Automóviles” 2007/2008
- 24.- Montserrat Cunillé Salgado: “Los riesgos operacionales en las Entidades Aseguradoras” 2003-2004
- 25.- Ricard Doménech Pagés: “La realidad 2.0. La percepción del cliente, más importante que nunca” 2010/2011
- 26.- Luis Domínguez Martínez: “Formas alternativas para la Cobertura de Riesgos” 2003-2004
- 27.- Marta Escudero Cutal: “Solvencia II. Aplicación práctica en una entidad de Vida” 2007/2008
- 28.- Salvador Esteve Casablanca: “La Dirección de Reaseguro. Manual de Reaseguro” 2005/2006

- 29.- Alvaro de Falguera Gaminde: "Plan Estratégico de una Correduría de Seguros Náuticos" 2004/2005
- 30.- Isabel M^a Fernández García: "Nuevos aires para las Rentas Vitalicias" 2006/2007
- 31.- Eduard Fillet Catarina: "Contratación y Gestión de un Programa Internacional de Seguros" 2009/2010
- 32.- Pablo Follana Murcia: "Métodos de Valoración de una Compañía de Seguros. Modelos Financieros de Proyección y Valoración consistentes" 2004/2005
- 33.- Juan Fuentes Jassé: "El fraude en el seguro del Automóvil" 2007/2008
- 34.- Xavier Gabarró Navarro: ""El Seguro de Protección Jurídica. Una oportunidad de Negocio"" 2009/2010
- 35.- Josep María Galcerá Gombau: "La Responsabilidad Civil del Automóvil y el Daño Corporal. La gestión de siniestros. Adaptación a los cambios legislativos y propuestas de futuro" 2003-2004
- 36.- Luisa García Martínez: "El Carácter tuitivo de la LCS y los sistemas de Defensa del Asegurado. Perspectiva de un Operador de Banca Seguros" 2006/2007
- 37.- Fernando García Giralt: "Control de Gestión en las Entidades Aseguradoras" 2006/2007
- 38.- Jordi García-Muret Ubis: "Dirección de la Sucursal. D. A. F. O." 2006/2007
- 39.- David Giménez Rodríguez: "El seguro de Crédito: Evolución y sus Canales de Distribución" 2008/2009
- 40.- Juan Antonio González Arriete: "Línea de Descuento Asegurada" 2007/2008
- 41.- Miquel Gotés Grau: "Assegurances Agràries a BancaSeguros. Potencial i Sistema de Comercialització" 2010/2011
- 42.- Jesús Gracia León: "Los Centros de Siniestros de Seguros Generales. De Centros Operativos a Centros Resolutivos. De la optimización de recursos a la calidad de servicio" 2006/2007
- 43.- José Antonio Guerra Díez: "Creación de unas Tablas de Mortalidad Dinámicas" 2007/2008
- 44.- Santiago Guerrero Caballero: "La politización de las pensiones en España" 2010/2011
- 45.- Francisco J. Herencia Conde: "El Seguro de Dependencia. Estudio comparativo a nivel internacional y posibilidades de desarrollo en España" 2006/2007
- 46.- Francisco Javier Herrera Ruiz: "Selección de riesgos en el seguro de Salud" 2009/2010
- 47.- Alicia Hoya Hernández: "Impacto del cambio climático en el reaseguro" 2008/2009
- 48.- Jordi Jiménez Baena: "Creación de una Red de Agentes Exclusivos" 2007/2008
- 49.- Oriol Jorba Cartoixà: "La oportunidad aseguradora en el sector de las energías renovables" 2008/2009
- 50.- Anna Juncá Puig: "Una nueva metodología de fidelización en el sector asegurador" 2003/2004
- 51.- Ignacio Lacalle Goría: "El artículo 38 Ley Contrato de Seguro en la Gestión de Siniestros. El procedimiento de peritos" 2004/2005
- 52.- M^a Carmen Lara Ortíz: "Solvencia II. Riesgo de ALM en Vida" 2003/2004
- 53.- Haydée Noemí Lara Téllez: "El nuevo sistema de Pensiones en México" 2004/2005
- 54.- Marta Leiva Costa: "La reforma de pensiones públicas y el impacto que esta modificación supone en la previsión social" 2010/2011
- 55.- Victoria León Rodríguez: "Problemàtica del aseguramiento de los Jóvenes en la política comercial de las aseguradoras" 2010/2011
- 56.- Pilar Lindín Soriano: "Gestión eficiente de pólizas colectivas de vida" 2003/2004
- 57.- Víctor Lombardero Guarner: "La Dirección Económico Financiera en el Sector Asegurador" 2010/2011
- 58.- Maite López Aladros: "Análisis de los Comercios en España. Composición, Evolución y Oportunidades de negocio para el mercado asegurador" 2008/2009
- 59.- Josep March Arranz: "Los Riesgos Personales de Autónomos y Trabajadores por cuenta propia. Una visión de la oferta aseguradora" 2005/2006
- 60.- Miquel Maresch Camprubí: "Necesidades de organización en las estructuras de distribución por mediadores" 2010/2011

- 61.- José Luis Marín de Alcaraz: "El seguro de impago de alquiler de viviendas" 2007/2008
- 62.- Miguel Ángel Martínez Boix: "Creatividad, innovación y tecnología en la empresa de seguros" 2005/2006
- 63.- Susana Martínez Corveira: "Propuesta de Reforma del Baremo de Autos" 2009/2010
- 64.- Inmaculada Martínez Lozano: "La Tributación en el mundo del seguro" 2008/2009
- 65.- Dolors Melero Montero: "Distribución en bancaseguros: Actuación en productos de empresas y gerencia de riesgos" 2008/2009
- 66.- Josep Mena Font: "La Internalización de la Empresa Española" 2009/2010
- 67.- Angela Milla Molina: "La Gestión de la Previsión Social Complementaria en las Compañías de Seguros. Hacia un nuevo modelo de Gestión" 2004/2005
- 68.- Montserrat Montull Rossón: "Control de entidades aseguradoras" 2004/2005
- 69.- Eugenio Morales González: "Oferta de licuación de patrimonio inmobiliario en España" 2007/2008
- 70.- Lluís Morales Navarro: "Plan de Marketing. División de Bancaseguros" 2003/2004
- 71.- Sonia Moya Fernández: "Creación de un seguro de vida. El éxito de su diseño" 2006/2007
- 72.- Rocio Moya Morón: "Creación y desarrollo de nuevos Modelos de Facturación Electrónica en el Seguro de Salud y ampliación de los modelos existentes" 2008/2009
- 73.- María Eugenia Muguerra Goya: "Bancaseguros. La comercialización de Productos de Seguros No Vida a través de redes bancarias" 2005/2006
- 74.- Ana Isabel Mullor Cabo: "Impacto del Envejecimiento en el Seguro" 2003/2004
- 75.- Estefanía Nicolás Ramos: "Programas Multinacionales de Seguros" 2003/2004
- 76.- Santiago de la Nogal Mesa: "Control interno en las Entidades Aseguradoras" 2005/2006
- 77.- Antonio Nolasco Gutiérrez: "Venta Cruzada. Mediación de Seguros de Riesgo en la Entidad Financiera" 2006/2007
- 78.- Francesc Ocaña Herrera: "Bonus-Malus en seguros de asistencia sanitaria" 2006/2007
- 79.- Antonio Olmos Francino: "El Cuadro de Mando Integral: Perspectiva Presente y Futura" 2004/2005
- 80.- Luis Palacios García: "El Contrato de Prestación de Servicios Logísticos y la Gerencia de Riesgos en Operadores Logísticos" 2004/2005
- 81.- Jaume Paris Martínez: "Segmento Discapacitados. Una oportunidad de Negocio" 2009/2010
- 82.- Martín Pascual San Martín: "El incremento de la Longevidad y sus efectos colaterales" 2004/2005
- 83.- Montserrat Pascual Villacampa: "Proceso de Tarificación en el Seguro del Automóvil. Una perspectiva técnica" 2005/2006
- 84.- Marco Antonio Payo Aguirre: "La Gerencia de Riesgos. Las Compañías Cautivas como alternativa y tendencia en el Risk Management" 2006/2007
- 85.- Patricia Pérez Julián: "Impacto de las nuevas tecnologías en el sector asegurador" 2008/2009
- 86.- María Felicidad Pérez Soro: "La atención telefónica como transmisora de imagen" 2009/2010
- 87.- Marco José Piccirillo: "Ley de Ordenación de la Edificación y Seguro. Garantía Decenal de Daños" 2006/2007
- 88.- Irene Plana Güell: "Sistemas d'Informació Geogràfica en el Sector Assegurador" 2010/2011
- 89.- Sonia Plaza López: "La Ley 15/1999 de Protección de Datos de carácter personal" 2003/2004
- 90.- Pere Pons Pena: "Identificación de Oportunidades comerciales en la Provincia de Tarragona" 2007/2008
- 91.- María Luisa Postigo Díaz: "La Responsabilidad Civil Empresarial por accidentes del trabajo. La Prevención de Riesgos Laborales, una asignatura pendiente" 2006/2007
- 92.- Jordi Pozo Tamarit: "Gerencia de Riesgos de Terminales Marítimas" 2003/2004
- 93.- Francesc Pujol Niñerola: "La Gerencia de Riesgos en los grupos multisectoriales" 2003-2004

- 94.- M^a del Carmen Puyol Rodríguez: "Recursos Humanos. Breve mirada en el sector de Seguros" 2003/2004
- 95.- Antonio Miguel Reina Vidal: "Sistema de Control Interno, Compañía de Vida. Bancaseguros" 2006/2007
- 96.- Marta Rodríguez Carreiras: "Internet en el Sector Asegurador" 2003/2004
- 97.- Juan Carlos Rodríguez García: "Seguro de Asistencia Sanitaria. Análisis del proceso de tramitación de Actos Médicos" 2004/2005
- 98.- Mónica Rodríguez Nogueiras: "La Cobertura de Riesgos Catastróficos en el Mundo y soluciones alternativas en el sector asegurador" 2005/2006
- 99.- Susana Roquet Palma: "Fusiones y Adquisiciones. La integración y su impacto cultural" 2008/2009
- 100.- Santiago Rovira Obradors: "El Servei d'Assegurances. Identificació de les variables clau" 2007/2008
- 101.- Carlos Ruano Espí: "Microseguro. Una oportunidad para todos" 2008/2009
- 102.- Mireia Rubio Cantisano: "El Comercio Electrónico en el sector asegurador" 2009/2010
- 103.- María Elena Ruíz Rodríguez: "Análisis del sistema español de Pensiones. Evolución hacia un modelo europeo de Pensiones único y viabilidad del mismo" 2005/2006
- 104.- Eduardo Ruiz-Cuevas García: "Fases y etapas en el desarrollo de un nuevo producto. El Taller de Productos" 2006/2007
- 105.- Pablo Martín Sáenz de la Pascua: "Solvencia II y Modelos de Solvencia en Latinoamérica. Sistemas de Seguros de Chile, México y Perú" 2005/2006
- 106.- Carlos Sala Farré: "Distribución de seguros. Pasado, presente y tendencias de futuro" 2008/2009
- 107.- Ana Isabel Salguero Matarín: "Quién es quién en el mundo del Plan de Pensiones de Empleo en España" 2006/2007
- 108.- Jorge Sánchez García: "El Riesgo Operacional en los Procesos de Fusión y Adquisición de Entidades Aseguradoras" 2006/2007
- 109.- María Angels Serral Floreta: "El lucro cesante derivado de los daños personales en un accidente de circulación" 2010/2011
- 110.- David Serrano Solano: "Metodología para planificar acciones comerciales mediante el análisis de su impacto en los resultados de una compañía aseguradora de No Vida" 2003/2004
- 111.- Jaume Siberta Durán: "Calidad. Obtención de la Normativa ISO 9000 en un centro de Atención Telefónica" 2003/2004
- 112.- María Jesús Suárez González: "Los Poolings Multinacionales" 2005/2006
- 113.- Miguel Torres Juan: "Los siniestros IBNR y el Seguro de Responsabilidad Civil" 2004/2005
- 114.- Carlos Travé Babiano: "Provisiones Técnicas en Solvencia II. Valoración de las provisiones de siniestros" 2010/2011
- 115.- Rosa Viciano García: "Banca-Seguros. Evolución, regulación y nuevos retos" 2007/2008
- 116.- Ramón Vidal Escobosa: "El baremo de Daños Personales en el Seguro de Automóviles" 2009/2010
- 117.- Tomás Wong-Kit Ching: "Análisis del Reaseguro como mitigador del capital de riesgo" 2008/2009
- 118.- Yibo Xiong: "Estudio del mercado chino de Seguros: La actualidad y la tendencia" 2005/2006
- 119.- Beatriz Bernal Callizo: "Póliza de Servicios Asistenciales" 2003/2004
- 120.- Marta Bové Badell: "Estudio comparativo de evaluación del Riesgo de Incendio en la Industria Química" 2003/2004
- 121.- Ernest Castellón Texidó: "La edificación. Fases del proceso, riesgos y seguros" 2004/2005
- 122.- Sandra Clusella Giménez: "Gestió d'Actius i Passius. Inmunització Financera" 2004/2005
- 123.- Miquel Crespí Argemí: "El Seguro de Todo Riesgo Construcción" 2005/2006
- 124.- Yolanda Dengra Martínez: "Modelos para la oferta de seguros de Hogar en una Caja de Ahorros" 2007/2008
- 125.- Marta Fernández Ayala: "El futuro del Seguro. Bancaseguros" 2003/2004

- 126.- Antonio Galí Isus: "Inclusión de las Energías Renovables en el sistema Eléctrico Español" 2009/2010
- 127.- Gloria Gorbea Bretones: "El control interno en una entidad aseguradora" 2006/2007
- 128.- Marta Jiménez Rubio: "El procedimiento de tramitación de siniestros de daños materiales de automóvil: análisis, ventajas y desventajas" 2008/2009
- 129.- Lorena Alejandra Libson: "Protección de las víctimas de los accidentes de circulación. Comparación entre el sistema español y el argentino" 2003/2004
- 130.- Mario Manzano Gómez: "La responsabilidad civil por productos defectuosos. Solución aseguradora" 2005/2006
- 131.- Àlvar Martín Botí: "El Ahorro Previsión en España y Europa. Retos y Oportunidades de Futuro" 2006/2007
- 132.- Sergio Martínez Olivé: "Construcción de un modelo de previsión de resultados en una Entidad Aseguradora de Seguros No Vida" 2003/2004
- 133.- Pilar Miracle Vázquez: "Alternativas de implementación de un Departamento de Gestión Global del Riesgo. Aplicado a empresas industriales de mediana dimensión" 2003/2004
- 134.- María José Morales Muñoz: "La Gestión de los Servicios de Asistencia en los Multirriesgo de Hogar" 2007/2008
- 135.- Juan Luis Moreno Pedroso: "El Seguro de Caución. Situación actual y perspectivas" 2003/2004
- 136.- Rosario Isabel Pastrana Gutiérrez: "Creació d'una empresa de serveis socials d'atenció a la dependència de les persones grans enfocada a productes d'assegurances" 2007/2008
- 137.- Joan Prat Rifá: "La Previsió Social Complementaria a l'Empresa" 2003/2004
- 138.- Alberto Sanz Moreno: "Beneficios del Seguro de Protección de Pagos" 2004/2005
- 139.- Judith Safont González: "Efectes de la contaminació i del estils de vida sobre les assegurances de salut i vida" 2009/2010
- 140.- Carles Soldevila Mejías: "Models de gestió en companyies d'assegurances. Outsourcing / Insourcing" 2005/2006
- 141.- Olga Torrente Pascual: "IFRS-19 Retribuciones post-empleo" 2003/2004
- 142.- Annabel Roig Navarro: "La importancia de las mutualidades de previsión social como complementarias al sistema público" 2009/2010
- 143.- José Angel Ansón Tortosa: "Gerencia de Riesgos en la Empresa española" 2011/2012
- 144.- María Mercedes Bernués Burillo: "El permiso por puntos y su solución aseguradora" 2011/2012
- 145.- Sònia Beulas Boix: "Prevención del blanqueo de capitales en el seguro de vida" 2011/2012
- 146.- Ana Borràs Pons: "Teletrabajo y Recursos Humanos en el sector Asegurador" 2011/2012
- 147.- María Asunción Cabezas Bono: "La gestión del cliente en el sector de bancaseguros" 2011/2012
- 148.- María Carrasco Mora: "Matching Premium. New approach to calculate technical provisions Life insurance companies" 2011/2012
- 149.- Eduard Huguet Palouzie: "Las redes sociales en el Sector Asegurador. Plan social-media. El Community Manager" 2011/2012
- 150.- Laura Monedero Ramírez: "Tratamiento del Riesgo Operacional en los 3 pilares de Solvencia II" 2011/2012
- 151.- Salvador Obregón Gomá: "La Gestión de Intangibles en la Empresa de Seguros" 2011/2012
- 152.- Elisabet Ordóñez Somolinos: "El sistema de control Interno de la Información Financiera en las Entidades Cotizadas" 2011/2012
- 153.- Gemma Ortega Vidal: "La Mediación. Técnica de resolución de conflictos aplicada al Sector Asegurador" 2011/2012
- 154.- Miguel Ángel Pino García: "Seguro de Crédito: Implantación en una aseguradora multirramo" 2011/2012
- 155.- Genevieve Thibault: "The Customer Experience as a Source of Competitive Advantage" 2011/2012

- 156.- Francesc Vidal Bueno: "La Mediación como método alternativo de gestión de conflictos y su aplicación en el ámbito asegurador" 2011/2012
- 157.- Mireia Arenas López: "El Fraude en los Seguros de Asistencia. Asistencia en Carretera, Viaje y Multirriesgo" 2012/2013
- 158.- Lluís Fernández Rabat: "El proyecto de contratos de Seguro-IFRS4. Expectativas y realidades" 2012/2013
- 159.- Josep Ferrer Arilla: "El seguro de decesos. Presente y tendencias de futuro" 2012/2013
- 160.- Alicia García Rodríguez: "El Cuadro de Mando Integral en el Ramo de Defensa Jurídica" 2012/2013
- 161.- David Jarque Solsona: "Nuevos sistemas de suscripción en el negocio de vida. Aplicación en el canal bancaseguros" 2012/2013
- 162.- Kamal Mustafá Gondolbeu: "Estrategias de Expansión en el Sector Asegurador. Matriz de Madurez del Mercado de Seguros Mundial" 2012/2013
- 163.- Jordi Núñez García: "Redes Periciales. Eficacia de la Red y Calidad en el Servicio" 2012/2013
- 164.- Paula Núñez García: "Benchmarking de Autoevaluación del Control en un Centro de Siniestros Diversos" 2012/2013
- 165.- Cristina Riera Asensio: "Agregadores. Nuevo modelo de negocio en el Sector Asegurador" 2012/2013
- 166.- Joan Carles Simón Robles: "Responsabilidad Social Empresarial. Propuesta para el canal de agentes y agencias de una compañía de seguros generalista" 2012/2013
- 167.- Marc Vilardebó Miró: "La política de inversión de las compañías aseguradoras ¿Influirá Solvencia II en la toma de decisiones?" 2012/2013
- 168.- Josep María Bertrán Aranés: "Segmentación de la oferta aseguradora para el sector agrícola en la provincia de Lleida" 2013/2014
- 169.- María Buendía Pérez: "Estrategia: Formulación, implementación, valoración y control" 2013/2014
- 170.- Gabriella Fernández Andrade: "Oportunidades de mejora en el mercado de seguros de Panamá" 2013/2014
- 171.- Alejandro Galcerán Rosal: "El Plan Estratégico de la Mediación: cómo una Entidad Aseguradora puede ayudar a un Mediador a implementar el PEM" 2013/2014
- 172.- Raquel Gómez Fernández: "La Previsión Social Complementaria: una apuesta de futuro" 2013/2014
- 173.- Xoan Jovaní Guiral: "Combinaciones de negocios en entidades aseguradoras: una aproximación práctica" 2013/2014
- 174.- Àlex Lansac Font: "Visión 360 de cliente: desarrollo, gestión y fidelización" 2013/2014
- 175.- Albert Llambrich Moreno: "Distribución: Evolución y retos de futuro: la evolución tecnológica" 2013/2014
- 176.- Montserrat Pastor Ventura: "Gestión de la Red de Mediadores en una Entidad Aseguradora. Presente y futuro de los agentes exclusivos" 2013/2014
- 177.- Javier Portalés Pau: "El impacto de Solvencia II en el área de TI" 2013/2014
- 178.- Jesús Rey Pulido: "El Seguro de Impago de Alquileres: Nuevas Tendencias" 2013/2014
- 179.- Anna Solé Serra: "Del cliente satisfecho al cliente entusiasmado. La experiencia cliente en los seguros de vida" 2013/2014
- 180.- Eva Tejedor Escorihuela: "Implantación de un Programa Internacional de Seguro por una compañía española sin sucursales o filiales propias en el extranjero. Caso práctico: Seguro de Daños Materiales y RC" 2013/2014
- 181.- Vanesa Cid Pijuan: "Los seguros de empresa. La diferenciación de la mediación tradicional" 2014/2015.
- 182.- Daniel Ciprés Tiscar: "¿Por qué no arranca el Seguro de Dependencia en España?" 2014/2015.
- 183.- Pedro Antonio Escalona Cano: "La estafa de Seguro. Creación de un Departamento de Fraude en una entidad aseguradora" 2014/2015.

- 184.- Eduard Escardó Lleixà: "Análisis actual y enfoque estratégico comercial de la Bancaseguros respecto a la Mediación tradicional" 2014/2015.
- 185.- Marc Esteve Grau: "Introducción del Ciber Riesgo en el Mundo Asegurador" 2014/2015.
- 186.- Paula Fernández Díaz: "La Innovación en las Entidades Aseguradoras" 2014/2015.
- 187.- Alex Lleyda Capell: "Proceso de transformación de una compañía aseguradora enfocada a producto, para orientarse al cliente" 2014/2015.
- 188.- Oriol Petit Salas: "Creación de Correduría de Seguros y Reaseguros S.L. Gestión Integral de Seguros" 2014/2015.
- 189.- David Ramos Pastor: "Big Data en sectores Asegurador y Financiero" 2014/2015.
- 190.- Marta Raso Cardona: "Comoditización de los seguros de Autos y Hogar. Diferenciación, fidelización y ahorro a través de la prestación de servicios" 2014/2015.
- 191.- David Ruiz Carrillo: "Información de clientes como elemento estratégico de un modelo asegurador. Estrategias de Marketing Relacional/CRM/Big Data aplicadas al desarrollo de un modelo de Bancaseguros" 2014/2015.
- 192.- Maria Torrent Caldas: "Ahorro y planificación financiera en relación al segmento de jóvenes" 2014/2015.
- 193.- Cristian Torres Ruiz: "El seguro de renta vitalicia. Ventajas e inconvenientes" 2014/2015.
- 194.- Juan José Trani Moreno: "La comunicación interna. Una herramienta al servicio de las organizaciones" 2014/2015.
- 195.- Alberto Yebra Yebra: "El seguro, producto refugio de las entidades de crédito en épocas de crisis" 2014/2015.
- 196.- Jesús García Riera: "Aplicación de la Psicología a la Empresa Aseguradora" 2015/2016
- 197.- Pilar Martínez Beguería: "La Función de Auditoría Interna en Solvencia II" 2015/2016
- 198.- Ingrid Nicolás Fargas: "El Contrato de Seguro y su evolución hasta la Ley 20/2015 LOSSEAR. Hacia una regulación más proteccionista del asegurado" 2015/2016
- 199.- María José Páez Reigosa: "Hacia un nuevo modelo de gestión de siniestros en el ramo de Defensa Jurídica" 2015/2016
- 200.- Sara Melissa Pinilla Vega: "Auditoría de Marca para el Grupo Integra Seguros Limitada" 2015/2016
- 201.- Teresa Repollés Llecha: "Optimización del ahorro a través de soluciones integrales. ¿cómo puede la empresa ayudar a sus empleados?" 2015/2016
- 202.- Daniel Rubio de la Torre: "Telematics y el seguro del automóvil. Una nueva póliza basada en los servicios" 2015/2016
- 203.- Marc Tarragó Diego: "Transformación Digital. Evolución de los modelos de negocio en las compañías tradicionales" 2015/2016
- 204.- Marc Torrents Fábregas: "Hacia un modelo asegurador peer-to-peer. ¿El modelo asegurador del futuro?" 2015/2016
- 205.- Inmaculada Vallverdú Coll: "Fórmulas modernas del Seguro de Crédito para el apoyo a la empresa: el caso español" 2015/2016

