POLITECNICO DI TORINO

Corso di Laurea Magistrale

Ingegneria della Produzione Industriale e dell'Innovazione Tecnologica

Tesi di Laurea Magistrale

NUEVAS TECNOLOGÍAS Y SISTEMAS FINANCIEROS

Relatore

Prof. Massimo Rossetto

Candidato

SERGIO MORO SANCHEZ

Ottobre 2014

Nuevas tecnologías y sistemas financieros

ÍNDICE

RESUMEN

La revolución tecnológica ha transformado los sectores económicos de la economía y, por ende, el sector financiero. Además, los sucesos acaecidos en el último ciclo económico recesivo han provocado que el sector financiero realice cambios relevantes. Asimismo, el consumidor ha evolucionado en el nuevo panorama de las nuevas tecnologías de la información y la comunicación y ha tomado nuevas conductas que han motivado la adaptación de las empresas del sector. El sector financiero ha tenido que enfrentarse a la creación de nuevos productos y servicios, a la desconfianza del consumidor final, a las nuevas pautas de comportamiento de los consumidores, a los problemas de seguridad que conllevan las nuevas tecnologías, a la reestructuración interna tanto de capital humano como capital físico, entre otros acontecimientos. Asimismo, se ha visto obligado a adaptarse a nueva regulación, tanto nacional como internacional, y ha visto como, en contradicción con lo anterior, se han introducido nuevos participantes y productos que no provienen de empresas tradicionalmente provenientes del sector financiero. Este trabajo pretende explicar la evolución del sector financiero y el impacto que ha tenido la introducción de las nuevas tecnologías de la información y la comunicación, los desafíos a los que se enfrenta, así como dar unos apuntes sobre la regulación y las perspectivas a las que puede acceder con las herramientas de información de que dispone en la actualidad. Por último, describir el panorama del sector financiero y las tendencias del mismo.

ABSTRACT

The technological revolution has transformed the economic sectors of the economy and, therefore, the financial sector. The events occurred in the last recessive economic cycle have caused, furthermore, the financial sector to carry out significant changes. The consumer has also evolved in the new panorama of the new information and communication technologies, and has taken new behaviors that have motivated the adaptation of the sector companies. The financial sector had to face the creation of new products and services, the suspicion of the final consumer, the consumer's new behavioral patterns, the safety problems that bear the new technologies and the internal restructuring of the human capital as well as the physical capital, among other events.
Also, it has been a required adaptation to the new regulation, both national and international, and it has been necessary, as we can see, and in contradiction to the previous approach, there have been introduced new participants and products that don't come from companies traditionally originated from the financial sector.

This paper aims to explain the evolution of the financial sector and the impact that has had the introduction of the new information and communication technologies, the challenges which it faces, as well as to give a few notes on the regulation and the perspectives you can access with the information tools available to you currently.
Lastly, the paper describes the panorama of the financial sector and it's trends.

1. AGRADECIMIENTOS E INTRODUCCIÓN

En primer lugar quiero agradecer a mi tutor el Dr. David Tanganelli, el cual sin sus enseñanzas y su motivación a la hora de hacer este trabajo, no podría haberlo investigado y por lo tanto no lo habría terminado, el Dr. Tanganelli fue el primer profesor que me impartió una clase docente en la UIC Barcelona, y desde el primer minuto ya asimilamos lo que iba a ser el hecho de ser alumno suyo, con esfuerzo y dedicación podemos con todo lo que tengamos por delante.

También quiero agradecer a todo el equipo que hace posible que UIC Barcelona funcione y obtenga un mayor prestigio año tras año y, es posible en gran parte a los docentes que cada día vienen a trabajar a la universidad para que nosotros los alumnos tengamos un futuro.

Después de un grado de ADE varias personas se incorporan al mundo laboral, y otras como yo y otros compañeros, seguimos estudiando para obtener el master en tecnología y sistemas de producción, el cual sin el no hubiésemos podido a profundizar en un tema tan importante como son las finanzas, en el cual debo dar mi sincera gratitud a Francesc Prior.

Pero para conseguir el máximo beneficio en todos los aspectos tenemos que obtener una calidad optima para ser competitivos en el sector, ya sea alimentario o del automóvil, dado que una menor calidad te produce un mayor coste con la consiguiente reducción de beneficio. Y a su dedicación por todo ello mi agradecimiento a la Jasmina Berbegal y a Joaquim Pous.

No quiero acabar mis agradecimientos sin antes homenajear a mis compañeros de clase y amigos por apoyarme en todos y cada uno de mis días como estudiante, y obviamente a mi familia, a los que están y a los que ya no están, que sin ellos hoy no sería lo que soy, de modo que mi éxito presente y futuro va por ellos.

El sector financiero y, concretamente, la industria bancaria, ha llevado a cabo un proceso de adaptación con el objetivo de aumentar la eficiencia y aprovechar las economías de escala a través de la implementación de la tecnología de la información y comunicación y, por otra parte, la digitalización de sistemas de procesos.

Asimismo, ha debido responder con agilidad a los elementos circunstanciales generados a consecuencia de la crisis económica y financiera, que posteriormente afecto a la totalidad de la economía, con un entorno de políticas económicas por parte de los bancos centrales de tipos de interés, con datos negativos en ocasiones, que han dificultado la obtención de rentabilidad, así como el elevado nivel de morosidad e impago de los clientes, con la consecuente adjudicación de bienes inmuebles y de otro tipo que han lastrado los balances contables bancarios y han generado un colapso de liquidez importante.

El sector financiero ha tenido la agilidad de ser pionero en la incorporación de la Tecnología de la Información y Comunicación (TIC) a su sistema empresarial y productivo. De hecho, es uno de los sectores de la economía que más ha invertido en TIC, liderando los cambios relacionados con los cambios en la sociedad y en el comportamiento de los consumidores en España (Fanjul Suárez & Valdunciel, 2007).

Otro de los aspectos que han transformado el sector financiero ha sido la internacionalización del negocio bancario con instituciones que operan a escala mundial y la pérdida de cuota de mercado de los bancos por la presión de los intermediarios financieros, que, tras la transformación normativa, se han equiparado a la banca.

A consecuencia de la coyuntura cíclica se ha llevado a cabo un efecto de concentración bancaria, tras las quiebras técnicas que han sufrido varias entidades de nuestro país, que ha visto reducir a la tercera parte el número de entidades financieras, fenómeno que no ha concluido.

Por último, el sector financiero se ha tenido que enfrentar a la crisis de reputación y consecuente falta de confianza del sistema bancario, tras las malas prácticas de los mismos en cuanto a venta de activos financieros con elevado riesgo

encubierto, como aquellos vinculados a hipotecas subprime, o la venta de productos de elevada complejidad financiera, como los swaps o preferentes a clientes con niveles de cultura financiera reducida.

La confianza es uno de los elementos claves para la construcción de una relación estable entre cliente y entidad financiera por lo que es un objetivo fundamental recuperar la imagen de entidades "serias" y confiables.

En otro orden de cosas, los desafíos de seguridad cibernética son un aspecto en el que el sector financiero está centrado, teniendo en cuenta el riesgo que conlleva contener la totalidad de datos financieros en sistemas informáticos.

2. ORÍGEN DEL NUEVO SISTEMA FINANCIERO

2.1. Breve exposición de los fundamentos del sistema bancario en España.

El sistema financiero español está formado por la suma de instituciones, medios y mercados, cuyo fin primordial es canalizar el ahorro que generan los prestamistas o unidades de gasto con superávit, hacia los prestatarios o unidades de gasto con déficit, así como facilitar y otorgar seguridad al movimiento de dinero y al sistema de pagos, como labor de intermediación.

El sistema financiero comprende, tanto los instrumentos o activos financieros, como las instituciones o intermediarios y los mercados financieros: los intermediarios compran y venden los activos en los mercados financieros.

El sistema financiero es clave en el desarrollo de un país, puesto que se percibe un mayor crecimiento en los países donde los mercados y las instituciones financieras funcionan mejor. La función principal del sistema financiero es la intermediación entre los agentes económicos que quieran prestar o invertir sus fondos disponibles y aquellos que necesitan dichos fondos para adquirir bienes u otros fines.

Concretamente existen dos tipos de intermediación, la que se realiza a través de entidades bancarias y la que se realiza a través del mercado de valores. El sistema financiero español se ha convertido en las últimas décadas en uno más abierto al exterior, competitivo y más sofisticado.

A pesar de estos cambios, el modelo español sigue caracterizándose por una alta cercanía al cliente. Así, dentro de los países de la UE, España cuenta con una de las menores ratios de habitantes por oficina y un tamaño medio de sucursal de los más reducidos.

En los últimos años está teniendo lugar una reestructuración de nuestro sistema financiero para reforzarlo y hacer frente a las secuelas de la crisis financiera. Esta reestructuración se ha observado tanto en la concentración de entidades a través de la adquisición o fusión, entre otras herramientas de reorganización empresarial. Asimismo, como consecuencia de ello, los grupos bancarios han tenido que reducir la ratio anteriormente citada.

Las entidades financieras más importantes para la financiación de la economía española son las entidades de crédito, concretamente los bancos y las cajas de ahorros, siendo éstas últimas de un número mucho más reducido tras el proceso de cambio en el sector.

Entre las funciones que realizan en la economía están la concesión de préstamos y créditos, los servicios de pagos, la emisión y gestión de otros medios de pago, la intermediación en los mercados interbancarios, así como el asesoramiento y prestación de servicios a empresas en materia de estructura de capital, estrategia empresarial, adquisiciones y fusiones.

El Banco de España, como supervisor del sistema bancario, opera bajo la supervisión del Banco Central Europeo (BCE), que junto con los bancos centrales de los países que han adoptado el euro, constituyen el Euro sistema, el cual define y ejecuta la política monetaria única. Mientras que existan Estados miembros que no hayan

adoptado el euro, es necesario distinguir el Euro-Sistema del Sistema Europeo de Bancos Centrales.

Este sistema está formado por el BCE y los bancos centrales de todos los países miembros de la UE, hayan o no adoptado el euro.

Dentro del sistema financiero español cabe mencionar las bolsas de valores, debido a los cambios que han experimentado y a su crecimiento en los últimos años. En la actualidad, estos mercados canalizan importantes volúmenes de inversión.

El holding Bolsas y Mercados Españoles integra las diferentes empresas que dirigen y gestionan los mercados de valores y sistemas financieros en España, y coordina los mercados de renta variable y fija, derivados y sistemas de compensación y liquidación españoles.

El correcto funcionamiento del sistema financiero de un país condiciona su desarrollo y es pieza clave en la evolución del mismo, es decir, existe cierta causalidad entre su desarrollo financiero y su consiguiente crecimiento económico (Ross Levine, 2004).

2. DESCRIPCIÓN DEL SISTEMA FINANCIERO ACTUAL

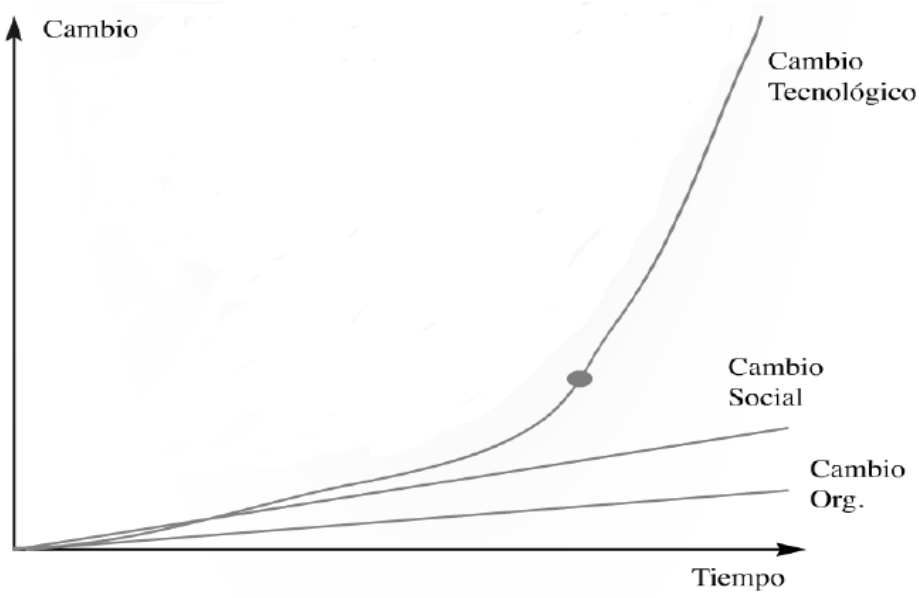
El sistema financiero actual ha experimentado una profunda transformación desde la introducción de las nuevas tecnologías de la información y comunicación y el proceso de globalización, que ha permitido una apertura internacional, transformado ampliamente parámetros tanto económicos como sociales.

Además, la última etapa recesiva de la economía mundial ha contribuido a una reestructuración y cambio de parámetros que generan una amplia distancia entre lo que era el sector financiero en los años noventa y lo que es en la actualidad.

A pesar de ser pionero en la implementación de las nuevas tecnologías en el sistema productivo del sector financiero, el desarrollo de las tecnologías va mucho más rápido que la capacidad de asumir dichas innovaciones.

Según Kurzweil, el ritmo al que se desarrolla la tecnología es exponencial, mientras que la sociedad y, como parte de ella, las organizaciones empresariales tienen un crecimiento tecnológico lineal o con un modelo de crecimiento cercano a la linealidad (gráfico1) (Kurweil, 2006). Según dicho autor, los cambios acaecidos en la tecnología provocarán que se genere una evolución donde desaparecerán métodos y procesos de trabajo y surgirán otros donde se requerirán nuevas capacidades y habilidades tecnológicas.

GRÁFICO 1: MODELO DE CRECIMIENTO DE EVOLUCIO VERSUS SOCIEDAD



Fuente: Kurzweil. (2006).

Como se puede observar en el gráfico, el cambio social se da incluso antes que el cambio de la organización empresarial, pues ésta se va adaptando a las necesidades que percibe de la demanda agregada.

2.1. Sistema bancario español.

El sistema bancario ha experimentado en el ámbito en todos los ámbitos relacionados con el mismo. Cabe destacar el ámbito operativo y el ámbito regulatorio y estructural tras la crisis iniciada a principios de 2007 y las medidas que se han tomado al respecto, las cuales se explicarán en apartados posteriores.

El sistema bancario español está compuesto por el conjunto de instituciones, sistemas de pago y mercados en los que operan. Son varios los segmentos que se pueden diferenciar dependiendo de los entornos de donde proceden.

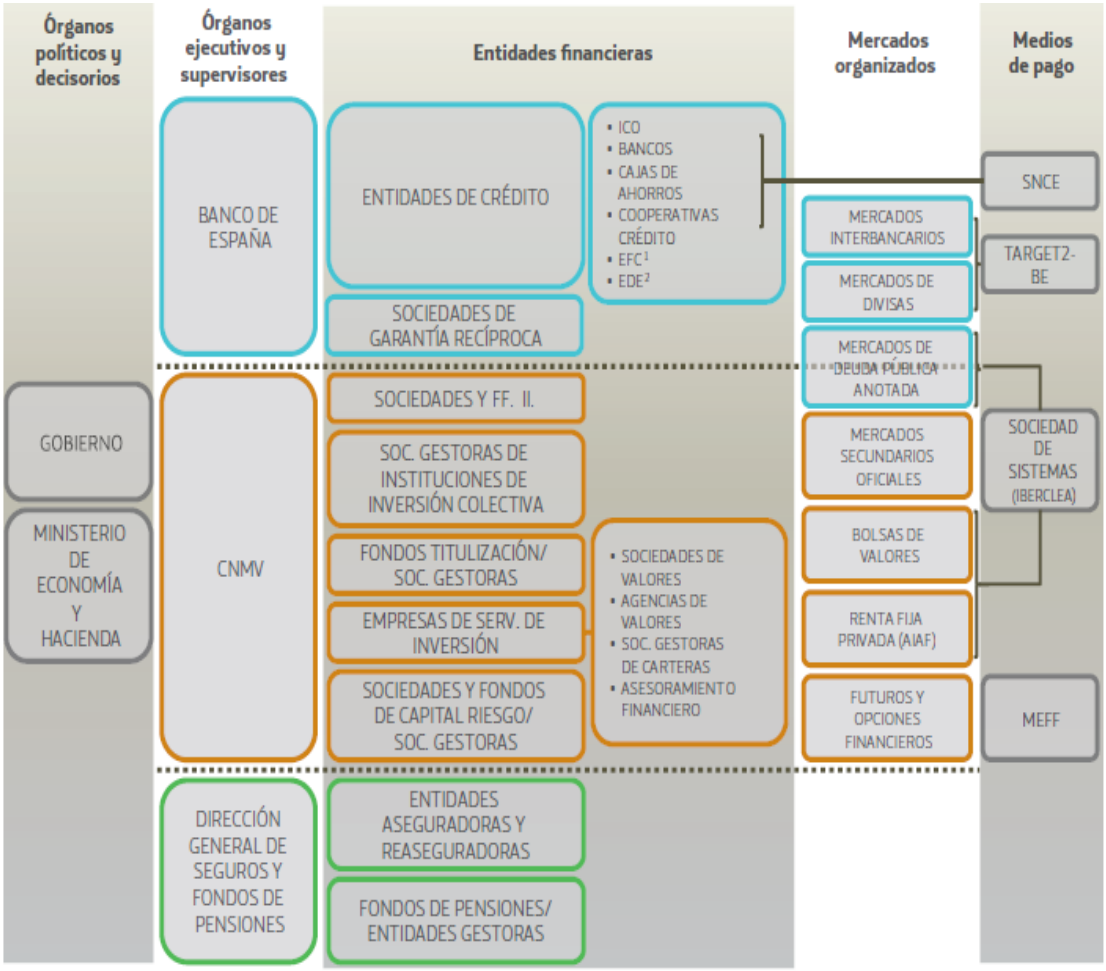
Así en el sistema financiero existen órganos políticos y decisorios, órganos ejecutivos y supervisores, entidades financieras, mercados organizados y organizaciones de medios de pago, como se puede observar en el cuadro 1.

Cabe destacar que esta estructura se incluye dentro de una mucho más amplia, a consecuencia de la pertenencia a la Unión Europea. El Banco Central Europeo es, en última instancia, quien establece el marco regulatorio, que posteriormente se introduce en la regulación de los Estados Miembros.

Asimismo, el Banco Central Europeo determina la política monetaria de la Unión Europea, así también realiza propuestas y previsiones sobre las economías de los países pertenecientes a la Unión Europea.

Desde la unificación de la política económica y monetaria de los Estados Miembros, el Banco Central Europeo traza las líneas en estas materias para que la trayectoria seguida por los Bancos Centrales sea desde el mismo enfoque, para lograr los objetivos trazados por la Unión misma.

CUADRO 1: ESTRUCTURA INSTITUCIONAL DEL SISTEMA FINANCIERO ESPAÑOL.



Fuente: Afi (2008). Guía del sistema financiero español.

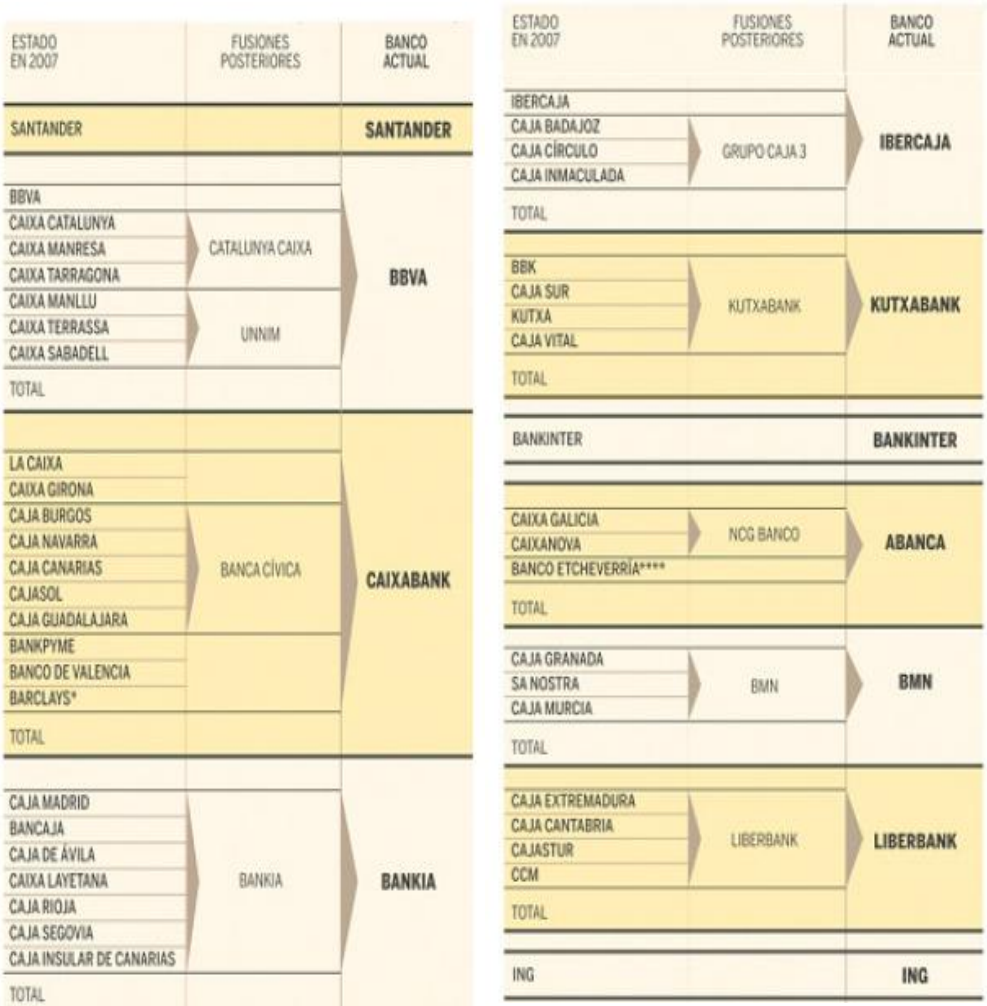
El efecto dominó de transformaciones que se produjo a partir de 2007 ha provocado un cambio profundo en el sistema financiero español. En esta transformación, las decisiones gubernamentales llevadas a cabo para evitar el colapso del sector han sido cruciales. Las fusiones y adquisiciones se han llevado a cabo con el objetivo de mantener la competitividad, aumentar su posición de liderazgo y contribuir a evitar la quiebra de entidades, situación que habría perjudicado gravemente la imagen de la totalidad de las entidades.

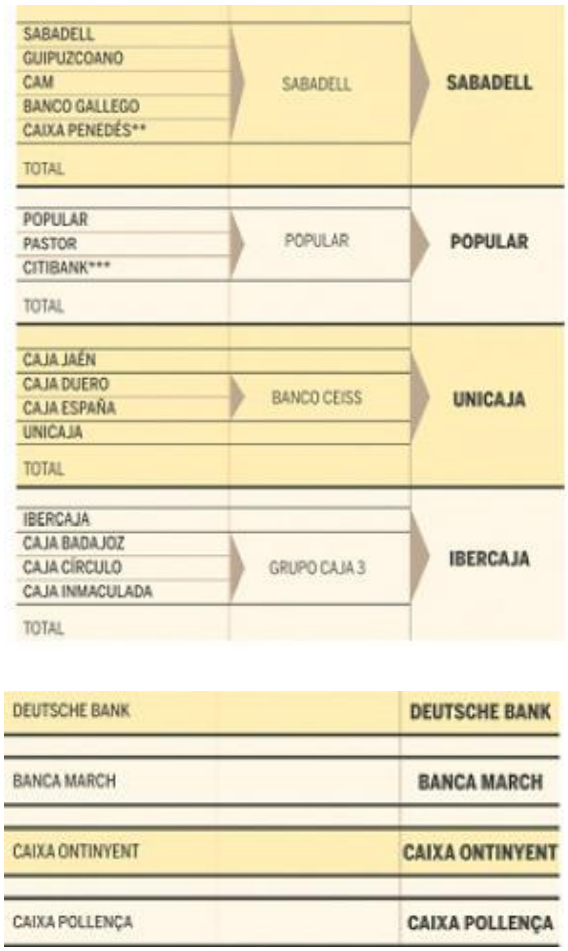
Las cajas de ahorros y las cooperativas de crédito se han transformando en bancos. En 2010, una vez aprobado el Decreto-Ley 11/2010, donde se impulsó la

bancarización de las cajas, aunque se permite que ejerzan su actividad financiera a través de un banco. Dicho Decreto, liberalizó el régimen regulatorio y dotó de potestad a las cajas para realizar las mismas operaciones y prestar los mismos servicios que los bancos.

En el siguiente cuadro se observan las transformaciones que se han llevado a cabo en las entidades financieras españolas a través de las acciones de reestructuración. Como se puede observar, el número de las entidades que se han mantenido tras la reestructuración se ha reducido dos tercios del número total.

CUADRO 2: REAGRUPACIÓN DE LAS ENTIDADES FINANCIERAS TRAS LA CRISIS DE 2007.





Fuente: Romani. Expansión.com. (2015).

Siguiendo a Méndez (2015), la respuesta del sistema financiero español de reestructuración está en línea con la propuesta de dirección política marcada por el Consejo Europeo, que planteó como solución a la crisis direccionar al sector hacia una unión bancaria, económica y fiscal, lo que va acompañado de una profundización en la legitimidad democrática, y por tanto también en la unión política.

En esta línea se sitúan las principales novedades que experimenta el BCE a raíz de la crisis, ya que el Eurobanco ha sido y continua siendo protagonista y objeto de importantes reformas (Méndez, 2015).

A la estructura anterior del sistema financiero ha de añadirse una contribución por parte del Gobierno, con la aprobación del Real Decreto Ley de Reestructuración y Resolución de Entidades de Crédito, en donde se creó una sociedad de gestión para aislar los activos tóxicos de las entidades financieras y posibilita la liquidación de

bancos inviables, conocida como “banco malo” o SAREB. Junto con la creación de esta entidad se incluye una nueva regulación del FROB para reforzar sus intervenciones en fases de gestión de crisis en entidades.

El objetivo de esta entidad es adquirir los activos dañados de los bancos para contribuir al saneamiento de los balances de las entidades financieras que han sido intervenidos por el estado.

En otro orden de cosas, la reestructuración de las entidades financieras y la reducción de beneficios del sector generaron otro efecto que ha transformado el mapa de sucursales en España. En el cuadro 3, se observa el número de entidades de crédito, el número de oficinas y el número de empleados entre 20058 y 2015, y su variación.

CUADRO 3: REDUCCIÓN DE LA CAPACIDAD INSTALADA EN ENTIDADES DE CRÉDITO.

	4T 2015	4 T 2008	VARIACIÓN
Entidades de crédito	262	362	-27,62%
Bancos y cajas	217	286	-24,13%
Nº de oficinas	31.087	46.065	-32,51%
Nº Empleados en España	202.959	278.301	-27,07%

Fuente: Banco de España. (2016).

Como se puede observar, se ha producido una disminución del 27,62% de entidades de crédito en España desde 2008 hasta 2015. Esto influye directamente en una reducción de la capacidad instalada del 32,51% en disminución del número de oficinas (este ajuste continuara ya que la situación actual de tipos bajos, la digitalización, ventas digitales, posibles fusiones o absorciones, márgenes más ajustados, etc) y una caída del 22,07% en empleados con 75.342 trabajadores menos.

A pesar de que este proceso de reestructuración no ha sido solamente en España, sino en toda la Unión Europea, en nuestro país ha habido más cierres de oficinas bancarias, llegando a una reducción del 27,62%. Cabe decir que, como se ha expuesto en apartados anteriores, España ha sido uno de los países con mayor capacidad instalada, es decir, número de oficinas por habitante, gracias, entre otras cosas, a las numerosas cajas de ahorros y por ello, tras la reestructuración, ha habido este descenso.

Según el BCE los países de la eurozona cerraron entre 2009 y 2013 20.539 oficinas, de las cuales más del 50% fueron en España.

En otro orden de cosas, y como consecuencia de las acciones tomadas tras la crisis originada en 2007, se lleva a cabo la construcción de una unión bancaria dentro de un nuevo diseño institucional de la Unión Económica y Monetaria (UEM). El Banco Central Europeo desempeña desde el 4 de noviembre de 2014 tareas de supervisión prudencial de las instituciones de crédito.

Anteriormente a esta fecha dichas tareas le correspondían a cada Banco Central o autoridad nacional competente. En la actualidad, están unificadas con el fin de garantizar la solidez del sistema bancario para intentar aumentar la integración financiera de la eurozona y su estabilidad.

La unión bancaria se compone de un Mecanismo Único de Supervisión (MUS), y de procedimientos comunes de reestructuración y resolución bancaria y de garantía de depósitos. El objetivo último de este nuevo poder consiste en que todos puedan recuperar la confianza en el sistema bancario.

El BCE desempeña estas tareas en el marco de un MUS integrado por el BCE y las autoridades nacionales competentes del área euro. El BCE con este sistema supervisa directamente a 3.600 Incorporación de las Nuevas Tecnologías al Negocio Bancario en España, es decir, las “Fintech” bancos, pertenecientes a 18 Estados miembros, en el marco de un único sistema.

Otro enfoque del proyecto de unión bancaria en Europa es el Mecanismo Único de Resolución (MUR). En él, se igualan las normas y procesos para intervenir y liquidar entidades en quiebra y se crea un fondo de resolución único con aportaciones de todos los bancos de la eurozona.

Su ámbito de aplicación es el de los Estados miembros del área euro, pero admite que puedan adherirse al mismo los Estados de la UE que no han adoptado el euro a través de un acuerdo de cooperación estrecha.

2.2. Evolución del sistema bancario.

El sistema financiero español debe comprenderse como una parte integrante del sistema financiero internacional, puesto que, en la actualidad, es complejo separar los sistemas financieros de los distintos países, ya que existen políticas económicas, regulación y organismos de supervisión financiera internacionales que afectan directamente al sistema financiero español.

Haciendo historia, el sistema financiero, en concreto el bancario, tenía ciertos inconvenientes puesto que la intermediación bancaria se limitaba a la disponibilidad horaria y la información que poseía el cliente era reducida por el restringido acceso a la información financiera que existía.

Este hecho provocaba varios efectos. Por un lado, las transacciones económicas de todo tipo se veían acotadas a la apertura de los bancos. Por otro lado, las entidades bancarias poseían un papel privilegiado de dominio en la economía a consecuencia de lo anterior.

Asimismo, las operaciones de préstamo en los bancos, como las operaciones de seguros en las entidades aseguradoras, asumían un riesgo añadido a lo propiamente estipulado de la operación, puesto que existían dificultades de contrastar determinada información de los sujetos que las solicitaban.

Una de las primeras y principales innovaciones en el sector bancario fue la constitución de los cajeros automáticos y los puntos electrónicos de venta. Los cajeros automáticos fueron los primeros elementos computerizados de acceso remoto al banco.

Esto permitió que, progresivamente, se realizaran cada vez más operaciones en puntos de autoservicio, ampliando la franja horaria a 24 horas y reduciendo la dependencia de los servicios bancarios.

Junto a éste, el dinero de plástico o tarjeta de débito y crédito y la introducción de terminales de punto de venta (TPV) contribuyeron a la agilización de transacciones comerciales de consumo. Dichos terminales se extendieron con rapidez por los establecimientos comerciales de todo tipo, permitiendo al cliente prescindir de dinero en efectivo, con la seguridad de corroboración de capacidad de pago por parte del usuario. En la actualidad, es difícil acceder a un establecimiento que carezca de esta tecnología de pago.

Hay que destacar la importancia del sistema de pago de tarjeta, elemento clave para el desarrollo de las dos innovaciones descritas en los párrafos anteriores. La rapidez con que se desarrollan las transacciones a través de este medio de pago ha transformado las costumbres de consumo en la sociedad.

Asimismo, a través de su numeración, con la introducción de operaciones online, que se detallarán más adelante, se permite realizar transacciones desde un terminal móvil de última generación, hecho que ha revolucionado el comportamiento de los consumidores.

2.2.1. Desde los años sesenta hasta finales de siglo XX.

El sector financiero ha sido pionero en la implementación de innovaciones y nuevas tecnologías de la información, no sólo con el objeto de adaptarse a la transformación de los hábitos de los consumidores, aspecto de vital importancia sobre todo para el sistema bancario, sino también para mejorar el funcionamiento interno y la eficiencia productiva.

La introducción de la tecnología en la banca se ha dado progresivamente conforme se han producido innovaciones a lo largo del tiempo (FUNDESCO, 1988).

Ésta ha acompañado el proceso de innovación financiera y se puede dividir en varias fases (Sarriá, 1994).

La primera fase se da durante los años sesenta, buscando los objetivos de reducir los costes, mejorar la productividad y aumentar la seguridad. En aquella etapa todavía existían restricciones que limitaban el desarrollo productivo del sector a consecuencia de las limitaciones informáticas y las dificultades para encontrar profesionales con formación en el sector, que impedía que se diera un crecimiento empresarial más acelerado que el que se dio durante este periodo de tiempo.

En una segunda etapa, durante los años setenta, se introduce en el sector bancario el teleproceso buscando el objetivo de ofrecer un servicio mejorado a los clientes y lograr agilidad interna en cuanto a la gestión. La aplicación de esta innovación al sistema bancario encontró limitaciones el cuanto a la infraestructura de telecomunicaciones que carecía de envergadura y en cuanto a la normativa y homologación de los servicios ofrecidos.

La siguiente etapa se sitúa durante los años ochenta, se invierte en la introducción del sistema de banca electrónica en el sector bancario español con el objetivo de conseguir mayor autonomía, aumentar los puntos de venta, introducir la ofimática y los sistemas de información.

Las limitaciones en esta etapa surgen de los obstáculos derivados de los servicios telemáticos, de las dificultades halladas en cuanto a compatibilidad de equipos informáticos y software y de los vacíos legales existentes a causa de tan novedoso sistema.

Otro periodo destacado es el comprendido durante los años noventa, donde comienza a introducirse el sistema de la banca online o virtual. Con esta innovación se pretende lograr una descentralización y agilización de determinadas funciones, la reducción de puntos de venta y la comunicación y distribución a través de la rede. Las limitaciones en este periodo aparecen por la falta de profesionales cualificados y vacíos legales en materia de seguridad (Casilda, 1997).

2.2.2. Desde comienzo de siglo XXI hasta la actualidad.

A partir de comienzos de siglo la evolución del sistema financiero en España está muy relacionada con la evolución de las TIC. De hecho, se podría incluso hablar de la transformación experimentada por el sector financiero como el paso del negocio de manejo de dinero al negocio de la gestión y procesamiento de información.

De hecho, si el sistema financiero ni hubiera sido proactivo en la implementación de las innovaciones en su proceso productivo, muchos de los avances a nivel social y en otros ámbitos de la economía no habrían podido ser factibles.

Efectivamente, es complicado imaginar al negocio financiero evolucionar sin la parte esencial que supone en la actualidad el medio de las TIC. Sin embargo, no existe una motivación de vincular ambos sectores, el financiero y el de la tecnología, per se sino más bien a consecuencia de la elevada competencia del sector financiero, en constante crecimiento, así como también el impulso de la innovación productiva y tecnológica.

Una muestra de la rapidez con la que se han desarrollado los acontecimientos en esta etapa son los siguientes:

- El número de tarjetas emitidas, ha crecido constantemente: en el año 2009 había casi 77 millones en España, un 59,1% más que en el año 2000.
- Como cabe esperar, el incremento de tarjetas ha venido acompañado a incremento de los aparatos que las aceptan, concretamente en 2009 había 1.392.805 terminales de punto de venta (TPV) en España, un 25,5% más que al comenzar la década.
- En la misma fecha se contaba con 61.374 cajeros automáticos.
- Existían 37.628 terminales para tarjetas monedero.

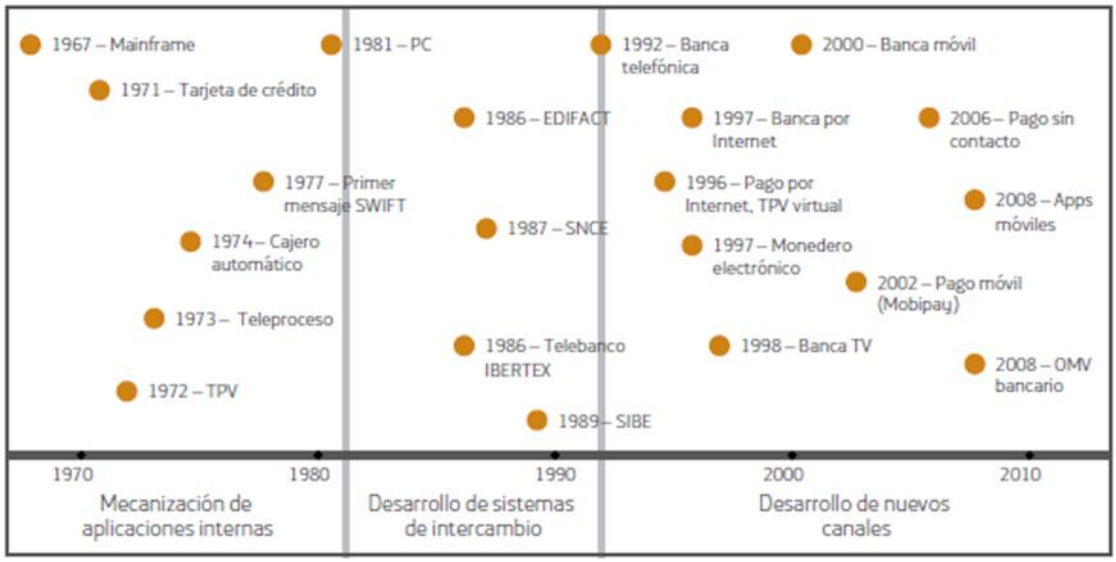
Por otro lado, los mercados financieros también han experimentado un fuerte crecimiento, el cual ha sido evaluado tanto por el número y volumen de ofertas públicas

de venta (OPV), como por el nivel de contratación o la capitalización bursátil. Así, la capitalización de las acciones cotizadas en la Bolsa de Madrid era de 550 miles de millones de euros en febrero del 2011, 6,8 veces más que en diciembre de 1989.

En el gráfico siguiente se muestran las innovaciones aplicadas a la banca desde 1970 hasta 2010. Cabe destacar la importancia y cantidad de los mismo, pero también la rapidez con que unas innovaciones han descartado a otras. Esto evidencia la necesidad de mantenerse a la vanguardia de los nuevos descubrimientos para evitar quedarse obsoleto y, por otra parte, muestra la capacidad visionaria que debe haber por parte de las entidades en cuanto a inversión en innovación.

Este último punto es relevante ya que existen elevados costes de implementación y de re-conducción de los clientes a nuevos métodos y operativa, por lo que es crucial apostar por aquellas innovaciones que tienen recorrido de desarrollo a lo largo del tiempo (Lozano Lázaro & Sebastián Cermeño, 2006).

GRÁFICO 2: LOGROS TECNOLÓGICOS EN EL SECTOR FINANCIERO.



Fuente: Lozano y Sebastián. (2006)

Es evidente que estos datos muestran una nítida importancia de la evolución tecnológica en el sistema financiero, datos que no habrían podido darse sin la introducción de las tecnologías de la información y la comunicación.

Así, un estudio del Ministerio de Industria (García García, 2004) muestra cómo el sector financiero es el segundo sector económico, después del de informática e I+D, que tiene una mayor penetración de las TIC. También revela que ha coincidido el periodo de máximas ganancias de productividad en la banca española con el desarrollo e implementación de la banca por Internet

En el siguiente cuadro, se observa el incremento de clientes de las entidades bancarias más importantes de España, así como otros datos de interés que cabe destacar de cada entidad, datos referenciados al año 2015.

Se puede observar en los datos expuestos, que los bancos contienen en sus objetivos captar clientes de banca online. Las cifras de crecimiento de los clientes online son constantes y crecientes.

CUADRO 4: CLIENTES DIGITALES EN PRINCIPALES BANCOS ESPAÑOLES, REFERENCIADOS SEGÚN SU BASE MUNDIAL DE CLIENTES

BANCO	CLIENTES DIGITALES	CLIENTES BANCA MÓVIL	OTROS DATOS
Grupo Santander	• Jun-15: 15 m (1,9 m España, 575 k USA) • Objetivo 2016: 20,0 m • Objetivo 2018: 30,0 m (4,2 m España)	• Jun-15: 5,5 m • Objetivo 2018: 16 m	• 117 millones de clientes, 12,8% digital • 36,7% móvil/digital 1H15, 53,3% en 2018 • Crecimiento digital 1H15-2016: 33%
BBVA Grupo	• Jun-15: 13,5 m • Jun-14: 11,2 m • Objetivo 2015 15,0 m	• Jun-15: 7,0 m • Jun-14: 11,2 m • Objetivo 2015 15,0 m	• 52% móvil/digital • Crecimiento digital 21% • Crecimiento móvil 59%%
CaixaBank	• Jun-15: 4,2 m	• Jun-15: 2,6 m	• 61,9% móvil/digital • Penetración de clientes online del 33,8% • 13,8 m de clientes.
Sabadell	• Jun-15: + 2,2 m	• Jun-15: 900 k	• 40,9% móvil/digital. • 38% clientes activos utilizan recurrentemente online y móvil
Bankia	• Sept-15: 1,12 m	• 762 k	• 68% móvil/digital • 7,8 m de clientes
Popular	• Mayo-15: 831 k	• Mayo-15: 143 k	• Crecimiento cliente móvil 44% • Penetración banca Internet empresas 70%
Bankinter	• Marzo-15: 350 k	• 1T15: 160 k	• 1T2015: 25,9% clientes usan app móvil • 2014: 62,9% clientes emplean canal internet
ING Direct	• 3,1 millones clientes banco online	• 1 millón estimado móvil/ digital del 33%	• Móvil/digital estimado considerando 1 millón descargas Google Play

Fuente: Estudio de Banca Digital España 2015.

Sin embargo, comparativamente con el resto de la Unión Europea, según Eurostat, en diciembre de 2014, el 37% de la población española entre 15 y 74 años usa la banca por Internet, lo que supone 13 millones de usuarios de la banca online en España. En base a esta información, España está a la cola de Europa en el uso de la banca por Internet, lejos del 49% de la UE-15 o del 57% de UK, o del 89% de Noruega.

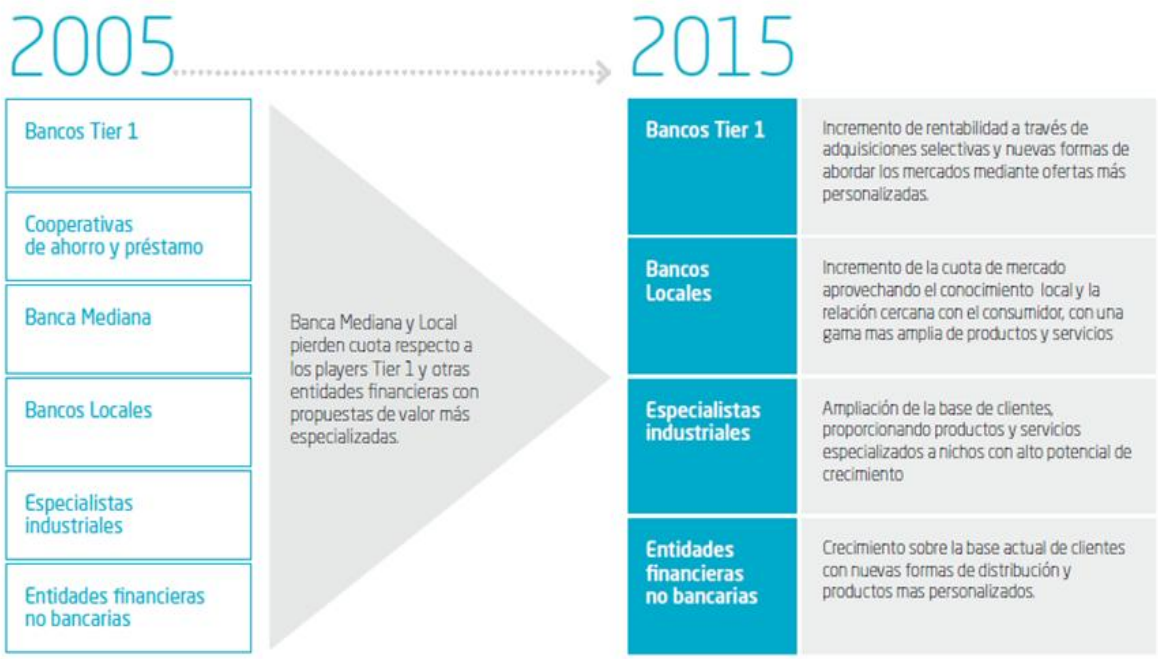
En España, en 2015 había 34,6 millones de smartphones con banda ancha móvil, un 78% de la población, lo que constituye una fortaleza para la bancarización digital de España, líder a nivel europeo.

España lidera en Europa la penetración de uso de la banda ancha móvil como medio de acceso a Internet, con un 77% de los usuarios que usaron Internet en el año 2015 lo hicieron a través de banda ancha móvil, frente a la media UE-15 del 60%, o países como UK con el 69%, Francia con el 59%, o Alemania con el 56%.

La penetración de usuarios de banca por Internet se correlaciona con la penetración del uso de Internet en España, y en la banca online ocupamos el lugar que nos corresponde. La promoción de la banca digital en España también se puede observar desde la perspectiva del incremento de la conectividad a Internet, y explotando fortalezas como la elevada penetración del smartphone y la conectividad de banda ancha móvil.

El cuadro 5 hace referencia de la evolución que han vivido las entidades financieras desde 2005 y 2015 y los cambios que han experimentado a lo largo de ese periodo, a consecuencia de los cambios acaecidos a lo largo de ese periodo.

CUADRO 5: EVOLUCIÓN DEL SISTEMA FINANCIERO ENTRE 2005 Y 2015



Fuente: IBM Institute for Business Value (2016).

Como se puede observar, las cooperativas de ahorro y préstamo desaparecen y toman mayor valor otro tipo de entidades con mayor especialización.

En otro orden de cosas, es importante tener en cuenta que las nuevas tecnologías van de la mano del acceso al público objetivo. En el siguiente cuadro se observa la previsión que existe de los canales de distribución de los servicios vinculados a las tecnologías de la información y la comunicación en los próximos años (los datos expuestos en el cuadro son de 2016).

Queda evidenciado que la relación banca cliente va a ser eminentemente virtual, gracias a las mejoras y los avances tecnológicos en cuanto a aplicaciones y banca online. Este hecho provoca la reducción de oficinas, sin que se considere un número

voluminoso, puesto que el cierre de un número considerable de oficinas puede vincularse a la falta de solvencia del banco o la necesidad de reducir costes.

La tendencia del manejo de efectivo y la necesidad de extracción del mismo en puntos habilitados para ello, va a ser cada vez menor, puesto que se están implantando otros métodos de pago cada vez más sencillos y vinculados a las innovaciones tecnológicas.

CUADRO 6: PREVISIÓN DE LOS EVOLUCIÓN DE CANALES DE DISTRIBUCIÓN

	0-3 AÑOS	4-7 AÑOS	8-10 AÑOS
Móvil / Tablet	Se consolida para consultas. Solo es transaccional en pagos. *Social Banking* le dan aún mayor impulso.	Plenamente funcional para transacciones vía Apps y *Social Banking*.	Indispensable pues aporta funcionalidad no alcanzable en otros canales (real time, banca contextual, etc.).
Oficinas	Continua la progresiva reducción de oficinas. 1er *downgrade* de un gran banco por su pesada infraestructura física.	La reducción de oficinas se convierte en estrategia declarada pues da "mala imagen".	Oficinas muy focalizadas (Flagship, hubs especializados, etc.).
ATM & Efectivo	ATMs y Efectivo decrecen al mismo ritmo.	ATMs son un centro de coste cada vez más insostenible. Integración con el móvil.	Se maneja muy poco efectivo y los puntos de extracción de efectivo comienzan a escasear.
Contacto Remoto	Básicamente telefónico. *Call center* para resolución de incidencias (reactivo) convive con *call center* comercial (proactivo).	La voz da paso a la imagen. La telepresencia se empieza a generalizar vía diferentes dispositivos (móvil, *tablet* y *smart TV*).	La telepresencia online y offline es vía principal de atención tanto para resolución de incidencias como para asesoramiento comercial.

Pagos	Pago móvil P2P sustituye a tarjetas. Proliferan comparadores y herramientas de gestión de finanzas personales.	La mayoría de los pagos se hacen por móvil y banco y NJ empiezan a enriquecer la experiencia de pago (antes, durante y después).	Desaparece el acto físico de "pasar por caja". Los productos están monitoreados (Rfid, etc.) y se cargan a nuestra cuenta, previa aceptación. Experiencia de pago enriquecida.
Cloud	Bancos Tier 1 siguen sin funcionar 100% en cloud, aunque comienzan a transformar sus sistemas. Solo NJ y Tier 3.	Grandes proyectos de renovación tecnológica en bancos Tier 1 y 2. Muchos servicios cloud de valor añadido para PyMEs.	Todos los players en el sector de banca funcionan cloud. Externalización de muchas áreas internas vía cloud.
Analytics	Los pilotos empiezan a entrar en producción. Bancos toman consciencia del "tsunami" *Social Banking*. Muchos fracasos y dinero tirado por la borda.	El cliente acepta que el banco utilice sus datos porque percibe que, ahora sí, resulta en su propio beneficio. Penaliza al banco que no los maneja bien.	Bancos rentabilizan sus datos también para retailers. Los datos de valor añadido son "oro" por lo que se compran y se comercializan a terceros una vez procesados.
Seguridad	No hay una solución definitiva / universal, por lo que sigue siendo un *stopper*.	Hay distintas soluciones que resuelven técnicamente el problema por lo que es un tema gestionable.	Se desarrollan nuevos sistemas biométricos muy avanzados y los problemas de seguridad quedan "definitivamente" superados.
Análisis Riesgo	Empiezan a introducirse soluciones de Big Data, aunque sólo como contraste. Grandes proyectos de *Risk Data Aggregation*.	Big Data es la herramienta principal para las entidades más avanzadas y convive el sistema antiguo. Los préstamos *collateral driven* pierden fuerza vs. *customer driven*.	Unos pocos referentes en riesgo inteligente (Bancos y/o NJ) proveen análisis de riesgo en la nube al resto (*comoditización*).
Fuentes de Financiación Bancaria	Estrechamiento generalizado de márgenes de intermediación. Sólo PayPal y algunas tarjetas prepago drenan pasivo bancario.	Se consolida estrechamiento de márgenes de intermediación. Progresiva desaparición de efectivo. Ganan peso las tarjetas prepago (filosofía de-banked) en países emergentes y clase media-baja de países avanzados. Más difícil captar pasivo "gratis".	Los bancos pelean por captar pasivo con otras firmas de reconocido prestigio. Financiación bancaria se encarece.

Fuente: IBM Institute for Business Value (2016).

3. NUEVAS TECNOLOGÍA EN EL SECTOR FINANCIERO.

En la nueva era digital la tecnología ya no es simplemente un soporte a negocio sino que pasa a ser un elemento clave de la estrategia de transformación. Las entidades financieras necesitan las tecnologías digitales para personalizar y adaptar la experiencia del cliente al individuo.

Los beneficios de la digitalización se obtienen a través de la incorporación de arquitecturas abiertas y plataformas de colaboración que faciliten la redefinición de los modelos de negocio del sector, siendo la escalabilidad y la flexibilidad las premisas básicas que presentan para continuar con el desarrollo digital.

Las entidades deben adaptarse y adoptar nuevos modelos habilitados por el uso de las tecnologías digitales, abrir su tecnología a terceros y a socios, e incorporar la tecnología al negocio para la incrementar la simplicidad operacional y mejorar la eficiencia operativa, tanto interna como externa.

Cabe decir, que dicho enfoque está realizado desde la introducción de la inteligencia virtual al negocio a través de la explotación de los datos para trabajar con sistemas predictivos, analíticos, y de validación y control. Este es uno de los activos más valiosos con los que se encuentran las entidades financieras, puesto que tienen la capacidad de acceder a información amplia y valiosa tanto de sus clientes como de aquellos que todavía no lo son.

El sector financiero está siendo pionero en el uso de Internet como nuevo canal de distribución y es uno de los sectores en los que es posible analizar con más claridad su impacto. Es de esperar que el desarrollo del canal Internet, mantenga un crecimiento sostenido, debido a que la distribución de productos financieros no requiere un intercambio físico de bienes, ya que desde hace mucho tiempo el dinero es, principalmente, un bien electrónico.

El impacto de Internet en la distribución de productos financieros es doble: se trata de un nuevo canal para distribuir productos tradicionales y, al mismo tiempo,permite la aparición de nuevas áreas de negocio.

Internet, entendido como nuevo canal de distribución, supone la eliminación de una importante barrera de entrada para nuevos competidores potenciales. De hecho, Internet se está convirtiendo en la vía de entrada preferida de las entidades financieras extranjeras que desean acceder al mercado español de banca comercial, ejerciendo a su vez una mayor presión sobre los precios.

Además, existe el riesgo de que los bancos sean reemplazados como distribuidores de productos financieros y aparezcan nuevos distribuidores: los portales verticales y los agregadores de información. Como consecuencia de esta fuerte competencia se producirá, además, una pérdida de volúmenes en favor de los nuevos participantes.

De acuerdo con el estudio España Online (Martínez León, Olmedo Cifuentes, & Reyes Contreras, 2007), Internet está contribuyendo a acelerar la transición de los bancos como organizaciones basadas en productos hacia organizaciones basadas en el consumidor. Cada vez tiene mayor importancia la innovación, el talento, la calidad del servicio y la eficiencia.

El acceso al cliente potencial a través de Internet ha generado que la competitividad aumente vertiginosamente y, en la actualidad, los bancos ya no compiten con otros bancos, sino con todo tipo de entidades que ofrezcan servicios financieros: brokers online, portales generalistas, aseguradoras y bolsas de valores, entre otros.

Para los bancos tradicionales es muy importante establecer una presencia en la red de calidad, una reputación online de calidad, variada y competitiva en precio. Los recién llegados no corren el riesgo de canalizar sus negocios tradicionales, lo que les está permitiendo ser más agresivos y rápidos que los bancos establecidos.

Además, estos nuevos competidores ya acceden sin elevados costes fijos de redes de oficinas y empleados y, desde otra perspectiva, no necesitan reeducar a su cliente tradicional para re-direccionarlo hacia la banca virtual, sino que acceden directamente a público objetivo que sabe manejarse, lo que conlleva menos costes.

Por otra parte, Internet permite desarrollar nuevas áreas de negocio como la negociación de acciones por Internet. El cliente ahora no sólo es capaz de dar órdenes directamente por Internet, sino que dispone de información en tiempo real, análisis, noticias, alertas, consulta de órdenes y acceso a bolsas internacionales, entre otros servicios.

Este innovador escenario ha dado paso a la aparición de un nuevo segmento de mercado, del que se han beneficiado nuevas compañías de Internet, así como algunas sociedades de valores que han transformado su estructura empresarial, convirtiéndola en completamente online.

Los bancos tradicionales españoles gozan de una posición privilegiada para aprovechar el potencial de Internet, ya que cuentan con dos ventajas: los clientes y una red establecida de sucursales y cajeros automáticos que les permite dar un servicio

añadido que la nueva competencia no va a poder ofrecer. Por ello, aunque Internet representa una amenaza sustancial para las entidades financieras establecidas, también es una oportunidad para aquellas que entiendan el reto que supone y realicen una apuesta decidida por impulsar este canal dentro de su organización.

En principio, para las entidades financieras existen ventajas importantes que justifican la realización de las operaciones bancarias por Internet. Parece evidente que prescindir de la red de oficinas supone una reducción de costes para la banca.

Si la reducción de costes que se obtiene de la eliminación de las sucursales es mayor que la consiguiente reducción de ingresos y no se producen aumentos significativos de otros gastos, entonces, la banca por Internet será rentable para las entidades financieras tradicionales.

Sin embargo, en la práctica, todavía no se puede saber si Internet podrá aprovechar todas las ventajas mencionadas anteriormente. Por una parte, los bancos que han desarrollado el modelo de negocio de banca online, que son principalmente canales no presenciales, son relativamente nuevos, por lo que es posible que el ciclo de las economías de aprendizaje todavía no se hayan agotado.

3.1. EL SECTOR FINANCIERO TECNOLÓGICO.

Las ofertas por Internet de las instituciones financieras pueden ser clasificadas en forma amplia en tres grandes grupos con distintos perfiles de riesgo:

- Informativas: Son herramientas que ofrecen información acerca de los productos y servicios del banco (“brochureware”) y son de bajo riesgo.
- Comunicativas: Ofrecen información relacionada con las cuentas y posiblemente también actualizaciones de los datos estáticos, como los datos del cliente. Como se permite el acceso a los sistemas principales del banco, el riesgo es material.
- Transaccionales: Permiten a los clientes ejecutar transacciones financieras y suponen el mayor riesgo. Algunos modelos transaccionales

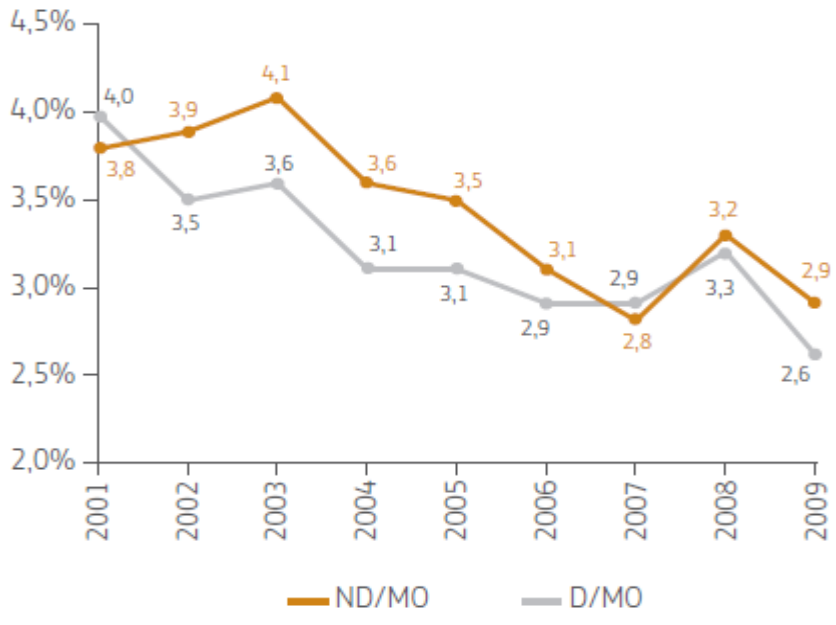
contienen riesgos muy elevados, sobretodo en el caso de que el cliente no haya visitado jamás una sucursal del banco durante toda su relación y prefiere llevar a cabo todas sus transacciones en forma remota.

Durante la última década se estima que el esfuerzo en TIC de las entidades ha oscilado entre los 3.000 y 4.000 millones de euros (BCE, 2010b), con una distribución por partidas. Dentro de este gasto, es interesante distinguir entre el gasto discrecional, es decir, aquel que la entidad puede decidir, tal como las nuevas adquisiciones, el desarrollo de nuevas aplicaciones o el mantenimiento evolutivo de las aplicaciones existentes; y el gasto no discrecional, entendido como aquel que es necesario para el funcionamiento diario de la entidad y está condicionado por la regulación o las decisiones pasadas (Accenture, 2010).

En esta categoría podría entrar el mantenimiento del hardware, el software y las comunicaciones, así como la operación de la infraestructura, la administración, y el mantenimiento correctivo y normativo (Honohan, 2008).

En el siguiente gráfico se observa el gasto invertido por parte del sector bancario en gasto discrecional y no discrecional.

GRÁFICO 3: EVOLUCIÓN DEL GASTO EN TIC DE LAS ENTIDADES FINANCIERAS.



Fuente: Accenture. (2010).

Como se puede observar en el gráfico, el gasto discrecional es el que se ve más reducido en periodos de crisis. En este sentido, el conjunto de costes TIC de la banca creció de manera sostenida entre los años 2002 y 2008, con la consecuente reducción a partir del comienzo del periodo de decrecimiento económico.

Sin embargo, si se vinculan estos datos de gasto con el margen ordinario de las entidades financieras, se observa (gráfico 3), una tendencia a la baja, lo que se justifica con el argumento de que las TIC contribuyen a la productividad de las entidades financieras. Así también, tiene sentido la reducción de inversión en TIC, ya que la implantación de innovaciones requiere inversiones elevadas en el principio pero posteriormente las inversiones son menores (Kendall, Mylenko, & Ponce, 2010).

Los incrementos de productividad pueden producirse por diversas vías: el aprovechamiento de economías de escala, las mejoras asociadas a la adopción de progreso técnico y tecnológico y las ganancias de eficiencia en la gestión.

Estudios llevados a cabo por investigadores del Banco de España (Banco de España, 2011) demuestran que la adopción de una web transaccional tiene un impacto positivo sobre la rentabilidad de las entidades financieras, aunque su impacto solo es significativo tres años después de la adopción, tanto desde el punto de vista de rentabilidad sobre recursos propios (ROE) como en rentabilidad sobre activos (ROA).

Dichas ganancias de rentabilidad se explicarían fundamentalmente por la reducción de los gastos operativos, y su impacto sería gradual, alcanzando máximos unos dos años y medio después de la puesta en marcha del canal.

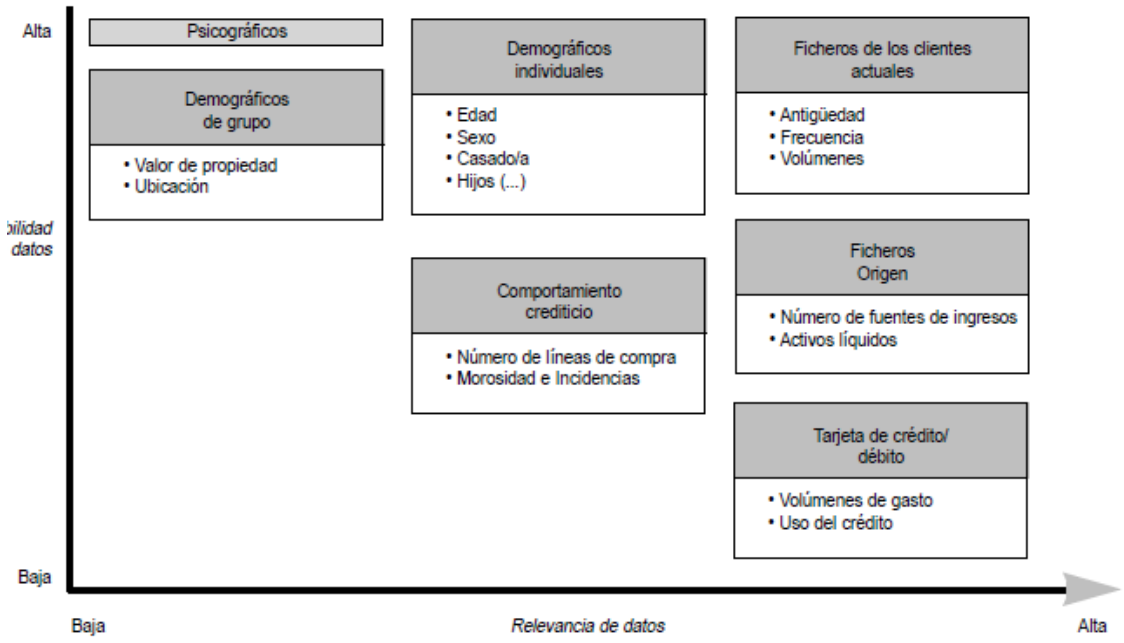
Además, la inversión de un millón de euros en capital TIC equivaldría a sustituir a 25 trabajadores, manteniendo el mismo rendimiento. Sin embargo, no hay evidencia de que las inversiones en TIC incrementen la demanda de crédito o la captación de depósitos (Sánchez Pajares, Martín Enríquez, & Bela Kindelán, 2007).

3.2. EL CAMBIO DEL CLIENTE TIPO.

La profundización financiera que se ha desarrollado en España ha sido esencialmente a través del negocio bancario minorista, a diferencia de lo que ha ocurrido en países como Estados Unidos o Reino Unido, donde los mercados financieros han sido durante años la base de crecimiento del sector.

En el gráfico siguiente se observa el tipo de datos y su grado de importancia de los clientes bancarios que utilizan banca virtual. Estos datos son de suma importancia para el desarrollo de la banca de última generación basada en el cliente.

GRÁFICO 4: DATOS DEL CLIENTE DE BANCA ONLINE.



Fuente: Hernando & Nieto. (2006).

El nuevo entorno marca la necesidad de reinventar el modelo de relación con el cliente hacia un modelo Customer Centric que garantice al cliente una experiencia personalizada e inmediata, que le haga sentirse único, y en el que el banco se anticipe a

sus necesidades y no que le sature con una oferta de productos prediseñada (Fernández de Guevara, 2007).

Para lograr este modelo centrado en el cliente es necesario conocerlo en profundidad para lo que se requiere construir potentes capacidades para integrar toda la información disponible, combinando datos internos con datos externos, datos cuantitativos con datos cualitativos, datos históricos con datos en tiempo real o proyecciones a futuro.

En España, el número de oficinas bancarias en relación con el número de habitantes del país se ha mantenido comparativamente alto con respecto a países de nuestro entorno, algo que podría deberse a la particular idiosincrasia de los españoles, muy apegados al uso de efectivo y al contacto personal.

A pesar de ello, desde el punto de vista del cliente más tecnológico, la realización de las operaciones bancarias por Internet significa mayor comodidad, con reducción del tiempo empleado, evitando desplazamientos y colas, obteniendo información sobre los productos y servicios financieros que ofrece cada entidad y, por último, la posibilidad de recibir una remuneración superior a la del mercado en sus cuentas.

La capacidad de obtener información de diversas entidades en tiempo récord le permite al usuario situarse en una posición privilegiada que anteriormente no tenía, donde su capacidad de negociación es elevada.

La mayoría de los usuarios de banca electrónica señalan la flexibilidad de poder hacer operaciones a cualquier hora del día y, en segundo lugar, el ahorro de tiempo.

Internet también presenta algunos inconvenientes que dificultan su expansión como canal de distribución de servicios financieros. Asimismo, se observa que entre quienes no operan con su banco por Internet, la obtención de un resguardo de la operación realizada constituye el primer freno y, en segundo lugar, el temor al robo de información bancaria. Otro motivo importante para un segmento es el poder contar con la asesoría de un empleado antes de realizar operaciones (Marquina Cogolludo, 2005).

La preocupación por la seguridad, la falta de confianza y el temor por la privacidad todavía suponen barreras significativas a la utilización de estos servicios.

Además, los últimos años se caracterizan por la gran caracterización a los rápidos cambios en la tecnología y por la introducción de servicios de banca corporativa y personal a través de Internet.

La velocidad sin precedentes con la cual se están adoptando las nuevas tecnologías, la ubicuidad y naturaleza global de las redes electrónicas, la integración de plataformas de e-banking con los sistemas anteriores y la creciente dependencia de los bancos respecto de los terceros proveedores de servicios de información, tienden a amplificar dramáticamente la magnitud de los riesgos a los que están expuestos los bancos y que los clientes perciben con recelo.

4. SEGURIDAD

La evolución de las TIC ha generado un profundo cambio en el comportamiento de la sociedad. El uso intensivo de éstas por parte de los ciudadanos, empresas, gobiernos y organizaciones sociales se han acompañado de una serie de riesgos novedosos que han requerido la puesta en marcha de medidas de protección y seguridad de los datos intercambiados y los sistemas y redes conectados.

La creación de un clima de seguridad y confianza digital, que permita reforzar la protección de los organismos públicos y privados y dé forma a una actitud de implicación de los usuarios en el entorno digital es uno de los objetivos de la ciberseguridad.

Este aspecto es crucial, puesto que el pleno desarrollo de la sociedad y la economía en un contexto virtual, depende de que se reduzca al máximo el índice de errores y delitos, que cada vez son más frecuentes, complejos y de mayor magnitud.

Según la Unión Internacional de Telecomunicaciones (UIT), la ciberseguridad se define como “el conjunto de herramientas, políticas, conceptos de seguridad,

salvaguardas de seguridad, directrices, métodos de gestión de riesgos, acciones, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberentorno" (Sector de la Normalización de las Telecomunicaciones de la UIT, 2008).

La ciberseguridad garantiza que se alcancen y mantengan las propiedades de seguridad de los activos de la organización y los usuarios contra los riesgos de seguridad correspondientes en el ciberentorno. Las propiedades de seguridad incluyen una o más de las siguientes: disponibilidad; integridad, que puede incluir la autenticidad y el no repudio; y confidencialidad.

Por lo tanto, la ciberseguridad está definida como un conjunto de directrices, políticas y herramientas que tienen como objetivo crear ese clima de confianza digital, por medio de la protección de los activos de organizaciones y particulares, que tengan soporte TIC.

Además, la necesidad de disponer de una red y entornos seguros está cada vez más presente en el entorno económico y, en concreto en el sector financiero, puesto que cada vez más este sector depende de las nuevas tecnologías para desarrollar su actividad empresarial.

Dado que la ciberseguridad se encuentra estrechamente ligada al uso de la tecnología, las tendencias TIC necesitan desarrollarse de la mano de la ciberseguridad, puesto que no existe mercado alguno que elija implementar un desarrollo tecnológico en su actividad empresarial que lo le asegure un mínimo de seguridad en el servicio.

Un ejemplo de ello es el Cloud Computing. Al ser un componente importante en las arquitecturas de aplicaciones modernas, se considera dentro de las tecnologías emergentes, uno de los principales objetivos de las ciberamenazas. Esto se debe, principalmente, a la gran cantidad de información potencialmente valiosa almacenada y procesada en el Cloud Computing (Parlamento Europeo, 2015).

Los ciberdelincuentes aprovechan las cualidades que ofrece de la computación en la nube por cuestiones de costes, un mejor camuflaje de actividades maliciosas en

sitios legítimos o por razones de rendimiento (Ponemon Institute, 2015). Además, existe todo un mercado de información donde el robo de datos es muy valioso. Los delitos relacionados con el mundo virtual son tan innovadores como el mismo y, constantemente, se crear infracciones que, a priori, son impensables.

En consecuencia, es de esperar que los proveedores de servicios en las nuevas tecnologías incluyan en sus innovaciones controles de seguridad y, en su caso, pautas de comportamiento a los clientes con el fin de desarrollar sus propias estrategias de ciberseguridad.

Otro caso es la herramienta de Internet de las Cosas (IoT, siglas en inglés), puesto que es una implementación ubicua de sistemas y múltiples elementos interconectados.

Esto lleva asociado un perímetro borroso de seguridad que obliga a desarrollar nuevos enfoques para asegurar las funciones de la red y los datos. Los principales riesgos asociados a la seguridad de IoT están relacionados con la complejidad resultante de la convergencia de múltiples plataformas y aplicaciones en sistemas embebidos (ISACA, 2015).

Además, IoT se considera un importante productor de grandes volúmenes de datos en bruto a muy altas velocidades. Como tal, estos datos (Big Data) pueden ser usados para sintetizar la información que es relevante en materia de seguridad, confidencialidad, personal, etc.

Sin embargo, es evidente que la falta de seguridad en el apoyo o el suministro de tecnologías y sistemas tienen el potencial de afectar negativamente a estos grandes sistemas de datos.

En definitiva, el campo de estudio de la ciberseguridad se encuentra íntimamente ligado a la evolución de las tendencias TIC identificadas, dado que como se ha ejemplificado brevemente, el auge en la conectividad, la ubicuidad de los datos o la saturación de los sistemas, entre otros, llevan asociados consigo una serie de vulnerabilidades y riesgos en ciberseguridad que deberán ser estudiados y abordados.

4.1. CARACTERÍSTICAS DE LA CIBERSEGURIDAD.

El sector de la ciberseguridad se presenta como un motor de desarrollo de la Economía Digital. La seguridad y la protección de la información adquieren una gran relevancia en la era actual de la digitalización y la hiperconectividad.

El aumento en el número de vulnerabilidades y riesgos que las empresas, administraciones públicas o los ciudadanos pueden sufrir, requieren de un mayor grado de especialización y capacitación del sector y, más concretamente, de su respuesta ante ellos.

Existen varios programas a nivel internacional que trazan una serie de pautas para el desarrollo del sector de la ciberseguridad. Por ejemplo, el Programa Europeo Horizonte 2020 establece varios aspectos transversales cruciales a desarrollar como la inclusión de la perspectiva de la Ciberseguridad o el Internet de las Cosas, así como el desarrollo de Sociedades Seguras, protegiendo la libertad y la seguridad de Europa y su ciudadanía.

Por ejemplo, el Programa de Sociedades Seguras (2017) se presentan una serie de convocatorias concretas para el desarrollo de proyectos de ciberseguridad enmarcados en ámbitos como la protección de las infraestructuras críticas, seguros y certificaciones para unos sistemas, servicios y componentes TIC más confiables y fiables, servicios y soluciones de ciberseguridad aplicables a pymes, administraciones públicas locales y particulares, seguridad digital de datos médicos, cooperación e intercambio de información entre los miembros de la Unión Europea y otros países sobre investigación, desarrollo e innovación en ciberseguridad, criptografía, ciberinteligencia (Advanced Cybersecurity Threat) y actores implicados, privacidad, protección de los datos e identidades digitales, entre otros.

Otro programa, el Programa Específico de Tecnologías de la Información y las Comunicaciones centra su atención en ámbitos como:

- Una nueva generación de componentes y sistemas. En este ámbito, cobra especial importancia la seguridad de sistemas ciber-físicos y sistemas smart.

- Computación avanzada y Cloud Computing, haciendo hincapié en la protección de sistemas en la nube.

- Internet del Futuro. Incluyéndose especificaciones para la seguridad en dispositivos móviles y el desarrollo de tecnologías de software seguras (seguridad desde el diseño).

- Creación de tecnologías Big Data que intrínsecamente contemplen la privacidad de los datos.

- Robótica y sistemas autónomos.

- Tecnologías clave habilitadoras.

Por último, en el documento de Visión Estratégica elaborado a partir de los grupos de trabajo para desarrollar los Programas de Trabajo del Horizonte 2020 para el próximo periodo 2018-2020, se han identificado 12 ejes impulsores de cambio, entre ellos, el relativo a la Revolución digital. En él, se plantea que la creciente dependencia de los sistemas TIC puede provocar el inicio de ciberguerras, y consecuentemente, la necesidad de poner en marcha mecanismos de vigilancia integral (Baena & del Barrio, 2013).

4.2. EVALUACIÓN DEL RIESGO DE LAS TIC EN EL SECTOR FINANCIERO

El sector financiero y la banca forman parte activa de la revolución digital que está transformando la prestación de los servicios financieros, desde los modelos de negocio tradicionales basados en las relaciones presenciales, hacia nuevos canales

online y móvil para desarrollar la relación con los clientes y aumentar su vinculación y fidelización.

La transformación digital de la banca implica nuevos riesgos, canales y vectores de ataque en el ámbito de la ciberseguridad, que están intentando aprovechar actores con intenciones cibercriminales. Gran parte del fraude más tradicional está también migrando en el ciberespacio, donde están ya activas organizaciones criminales que emplean técnicas avanzadas para cometer fraude contra los usuarios finales, dañado así económicamente y desde el aspecto de confianza a los bancos.

Asimismo, los propios bancos, su marca, su presencia online, sus sistemas IT, su propiedad intelectual e información confidencial están también expuestas a nuevos riesgos por la imparable revolución tecnológica, complejos sistemas IT, redes de proveedores, aplicaciones cloud, los terminales móviles, el uso del Internet y de las redes sociales para establecer la presencia digital de la marca, etc.

Para garantizar la seguridad e integridad de los activos financieros y los servicios que prestan las entidades bancarias se plantean una serie de propuestas de mejora para la ciberseguridad en la banca digital (Calvo, 2012).

En base a los análisis realizados, garantizando a la vez la seguridad e integridad de todos los activos de los bancos, se plantean las siguientes recomendaciones y mejores prácticas en el ámbito de la ciberseguridad en la banca digital (Accenture, 2010):

- Un enfoque proactivo de la ciberseguridad, que ha de avanzar desde las defensas hacia la detección temprana y reacción rápida y eficaz. Se estima que, en 2020, el 60% de los presupuestos de seguridad de las empresas se destinará a la detección y respuesta rápidas, frente a menos del 10% en 2013[1].

- Dotarse de inteligencia de seguridad mediante las alianzas más adecuadas. La banca debe contar con herramientas, soluciones y socios tecnológicos que proporcionen *inteligencia de seguridad*, para conseguir predecir, prevenir, detectar y responder de forma temprana.

[1] Development Trend of Enterprise Security in the Internet Ages – Gartner (2017).

- Realización de test periódicos de vulnerabilidades a lo largo de toda la industria promovidos por las autoridades regulatorias bancarias, que lo incluyan como parte sustantiva de los riesgos operacionales de las entidades. La realización de tests de detección de vulnerabilidades ha de ser de forma continua y persistente, para reducir la ventana de exposición. Los tests que se realizan solo unas pocas veces al año, coincidiendo en muchas ocasiones con auditorías, no son suficientes. La experiencia británica de Waking Shark II de la BBA[2] es un adecuado caso de referencia.

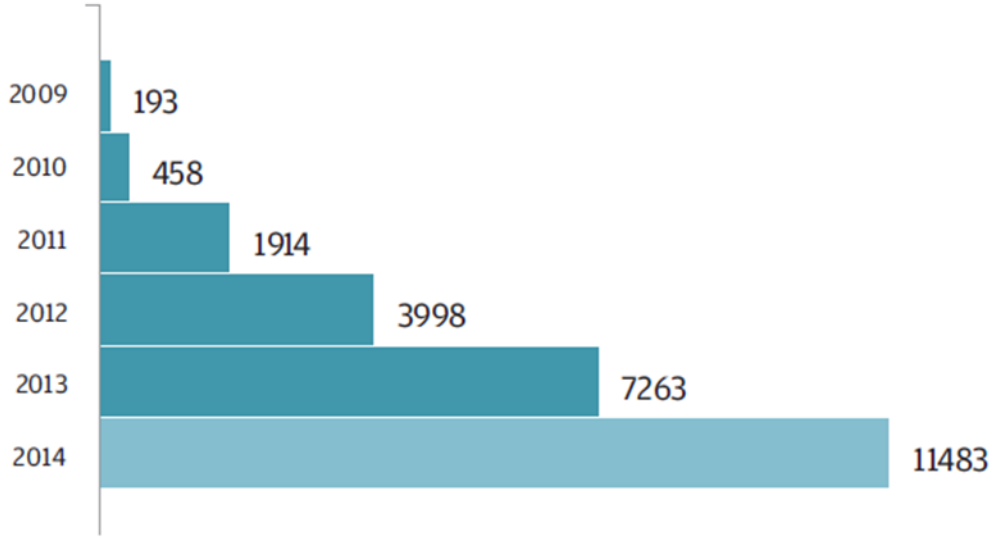
- Separación presupuestaria entre Seguridad e IT, de forma que se evite la habitual lucha por evitar recortes y de este modo poder disponer de visibilidad independiente de cada ámbito en los Executive Boards.

- Mayor foco en el eslabón más débil, el empleado y cliente, aumentando la formación interna, el entrenamiento del personal y la concienciación del usuario de banca mediante sitios web específicos, campañas de difusión, o avisos de alertas de ataques.

El sector financiero sigue siendo uno de sus objetivos primarios, creciendo un 15%[3] la actividad delictiva respecto años anteriores, tal y como reflejan diversos informes de seguridad (Climent & Momparler, 2016). En España, como se puede observar en el siguiente gráfico, se han producido entre Enero y Octubre de 2014 cerca de 12.000 incidentes, de acuerdo a la información facilitada por el CCN-CERT a finales de año.

[2] https://www.bba.org.uk/policy/capital-markets-infrastructure/business-continuity/bankof-england-publishes-operation-waking-shark-ii-generic-scenario-pack/
[3] Mandiant's M-Trends 2014 Threat Report.

GRÁFICO 5: EVOLUCIÓN DE INCIDENTES DETECTADOS POR EL CCN-CERT DESDE 2009 A 2014



Fuente: CCN-CERT.

España es el tercer país que más ciberataques recibe mediante software malicioso o malware instalado en los ordenadores de los usuarios, solo superado por EE.UU. y Reino Unido[4].

Los continuos titulares sobre ataques de ciberseguridad, el caso Snowden y la NSA, Wikileaks, y los más recientes ataques dirigidos contra JPMorgan, Target y Sony entre otros muchos, provocan la desconfianza de los ciudadanos.

Es la misma confianza de los clientes el gran activo que requiere de protección por parte de los bancos y en el que se basa su modelo de negocio. En España, La Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas, prevé la implantación de un Sistema de Protección de Infraestructuras Críticas (Sistema PIC), desarrollado en base a Planes Estratégicos Sectoriales (PES), incluido el que resulta de aplicación al sector financiero, y cuya

[4] http://www.computing.es

estructura contiene: normativa de aplicación, estructura del sector/subsector, estudio de impacto, análisis general de riesgos y propuesta de medidas estratégicas.

Los tres principales factores citados por las entidades financieras en los que aplicar el presupuesto destinado a seguridad de la información son el cumplimiento de los requisitos normativos, la continuidad del negocio y recuperación frente a desastres, y el riesgo reputacional.

La tendencia del sector financiero es de mayor regulación conforme se desarrolle plenamente el Plan Estratégico Sectorial, o la Directiva europea sobre la seguridad de las redes y de la información, por la que las entidades financieras deben adoptar prácticas de gestión de riesgos y comunicar los incidentes significativos de seguridad que se produzcan en relación con la prestación de sus servicios principales, la continuidad del negocio y recuperación frente a desastres, entre otros.

Aun así, las entidades financieras deben modificar su actual aproximación "tradicional" a la gestión de la seguridad, de un enfoque defensivo a otro mucho más proactivo y dinámico, que les permita anticiparse, detectar, reaccionar y recuperarse frente a las amenazas en el menor tiempo posible, admitiendo la posibilidad de que van a ser comprometidas en cualquier momento.

A pesar de que las entidades financieras han adoptado significativas medidas para reforzar sus esfuerzos en ciberseguridad, seguirán siendo desafiadas por la velocidad de los cambios tecnológicos y por la cada vez más sofisticada naturaleza de amenazas.

Las entidades son conscientes de que el panorama de las amenazas está en constante evolución, y les resulta difícil mantenerse al día con los últimos avances, en medio de la presión competitiva que soportan para integrar las nuevas tecnologías dentro de su oferta de productos (Banco de España, 2013c).

Los atacantes y sus metodologías son cada vez más sofisticados. Mientras que el malware12 sigue siendo la mayor amenaza reportada, los atacantes están utilizando con

más frecuencia ataques multivector, lo que dificulta su detección y detención (Sector de la Normalización de las Telecomunicaciones de la UIT, 2008).

Los principales ataques que sufre el sector financiero son los ataques de denegación de servicio (DoS), los robos de datos, el malware avanzado y el fraude interno y externo. Las medidas de seguridad tradicionales ya no son suficientes para hacer frente al rápido ritmo con el que cambia el panorama de los vectores de ataque, metodologías y herramientas.

En la actualidad, las empresas que tienen la capacidad de almacenar y analizar una variedad cada vez mayor de datos (Big DATA) relevantes a efectos de la prevención y detección de vulnerabilidades y ataques, combinado con el análisis forense y la minería de datos personalizados, son las que pueden determinar y analizar las acciones que ejecutan los sofisticados criminales cibernéticos.

Asimismo, pueden crear una verdadera plataforma de inteligencia de seguridad para la detección, prevención y remediación en tiempo real de los ciberataques.

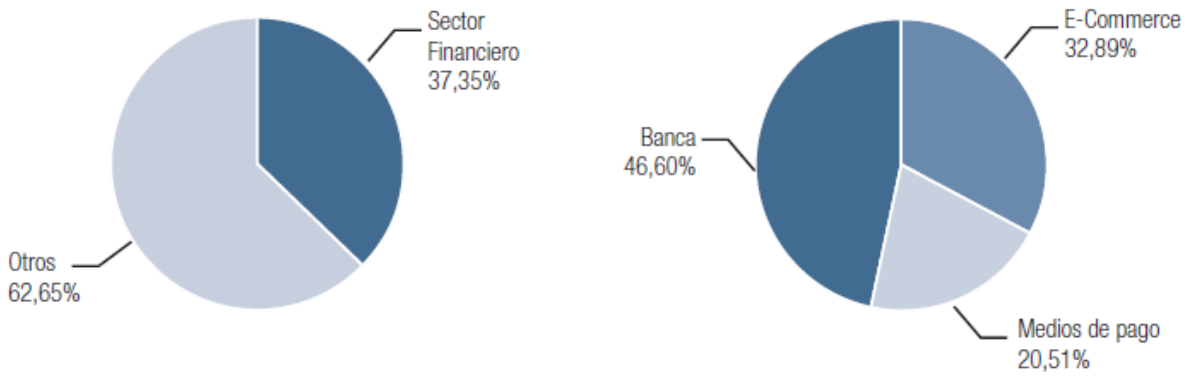
La "Inteligencia" de seguridad está evolucionando muy rápidamente, pasando de sólo reunir, correlacionar y notificar los datos de los dispositivos de seguridad, a enfoques en los que cada vez más se incluyen datos y "inteligencia" provenientes de terceros, de socios o de grupos de intercambio de información especializada, como podría ser el Centro para el Análisis e Intercambio de Información de Servicios Financieros (FS-ISAC).

En otro orden de cosas, se procede a exponer los principales ciberataques que son sometidas las entidades financieras. El primer lugar lo ocupa el fraude online, es decir, ataques contra la infraestructura del banco, clientes o entidades colaboradores, con el fin de realizar transacciones ilícitas o robar dinero. En esta categoría se incluyen como principales amenazas a Phishing, Carding, Malware Bancario, Malware Móvil y Malware de Puntos de Venta:

- Phishing: son ataques basados en técnicas de ingeniería social o de utilización de código malicioso, o la combinación de ambas. El

delincuente se hace pasar por una empresa o institución de confianza, de modo que logra sonsacar información privada al usuario, que utilizará posteriormente con fin malicioso[5]. De los ataques que ha sufrido el sector financiero en 2014, un 37,35% eran phishing[6].

GRÁFICO 6: ATAQUES PHISHING EN 2014.



Fuente: "Financial cyber threats Sept-Dec 2014"; Kaspersky Lab en colaboración con el servicio de con el servicio de Vigilancia Digital de Telefónica.

Uno se los motivos que más promueven este tipo de ataques es la alta rentabilidad que tienen en el mercado negro, con un retorno directo mediante la comisión directa de fraude. La tendencia de este tipo de ataques es al alza por lo que se evidencia la necesidad de definir una estrategia de seguridad en este aspecto concreto.

- Malware bancario: según INCIBE, el malware es un término que se utiliza para referirse a cualquier tipo de software malicioso o molesto que puede instalarse en los sistemas informáticos para llevar a cabo

[5] Instituto Nacional de Ciberseguridad (INCIBE).
[6] Estadísticas de phishing obtenidas del informe "Financial cyber threats Sept-Dec 2014"; Kaspersky Lab en colaboración con el servicio de Vigilancia Digital de Telefónica.

acciones sin el conocimiento del usuario. En el sector bancario, un ejemplo de este tipo de ataques es el denominado Zeus, el cual propaga copias de sí mismo a otros equipos mediante email, redes P2P, mensajería instantánea, entre otros medios virtuales de comunicación. De este modo crea una especie de red de equipos infectados bajo el control del malware y de su administrador. El objetivo de Zeus es el robo de credenciales bancarias e información financiera de los usuarios y puede llevar a cabo un gran número de acciones fraudulentas y perjudiciales como el control de los equipos, el robo de información confidencial, etc. logra registrar lo que teclean los usuarios, interceptan y modifican la comunicación entre los usuarios y la banca online en los navegadores web. En 2014 se recogieron una media del 55% de infecciones en España[7]. La complejidad de detener este tipo de ataque es la capacidad de mutar del programa malicioso.

- Carding: hace referencia al uso específico de herramientas y técnicas como el phishing o el malware con el objetivo de obtener datos de tarjetas bancarias. A pesar de los esfuerzos de seguridad que se llevan a cabo, las filtraciones y robos de gran cantidad de tarjetas bancarias es diaria. El objetivo es la venta de sus datos con destino a mercados indirectos.

El segundo lugar lo ocupa el tipo de ataques que provocan problemas de Marca y Reputación. En este grupo se incluyen los contenidos publicados en canales online con carácter ofensivo o dañino para la imagen de un banco, los ataques online contra la imagen de directivos u otras identidades digitales relacionadas con la entidad, entre otros.

El objetivo criminal en estos casos está centrado en impedir el normal funcionamiento de las entidades bancarias a través de ataques a sus activos que pongan en riesgo la continuidad del negocio.

[7] Estadísticas de malware y malware móvil obtenidas del informe "Financial cyber threats 2014"; Kaspersky Lab en colaboración con el servicio de Vigilancia Digital de Telefónica.

La banca digital es totalmente dependiente de la relación multicanal con los clientes y tiene cadenas de valor cada vez más complejas. Es por esto que la disponibilidad permanente de los canales de comunicación e interacción es una pieza clave para conseguir los objetivos de negocio de las entidades.

Son varias las amenazas que se vinculan a este tipo de ataques:

- Fugas de información: hace referencia a la publicación de información sensible o confidencial de la entidad. En este aspecto las entidades tienen una cuestión de enfoque en los datos: por un lado, los objetivos de seguridad internos y, por otro, los datos internos que son manejados por terceros, como la mensajería, la gestión de red, entre otros. En este aspecto, el sector bancario es responsable de las fugas de información, sin embargo, no pueden configurar completamente los dispositivos que adquieren, y existe una relación directa entre el *major provider* del software genérico y las fugas de datos (ASBANC, 2016).

- Vulneración y publicación de información sobre mecanismos de seguridad: dependiendo de la publicación de información que revele determinadas vulnerabilidades en activos físicos, o las evidencias de que un activo lógico se ha visto comprometido hace necesarios la monitorización y el control de forma continuada. Ejemplos de este tipo de ataques pueden ser burlar un sistema de ataque antirrobo, un vídeo en el que se detalla un ataque de inyección SQL que afecta al site principal del cliente, entre otros. Son tutoriales que permiten que cualquier persona pueda realizar un ataque incluso sin tener conocimientos avanzados.

- Robo de credenciales: la amenaza constante reside en los empleados puesto que son el eslabón más débil en la cadena de seguridad y son susceptibles de ser amenazados por prácticas de ingeniería social mediante correos electrónicos enviados por supuestas personas conocidas que contienen phishing o pharming, así como el aumento de la responsabilidad sobre estos.

- Actividad hacktivista y activista orientada a atentar contra activos del banco: las redes sociales son el canal principal para la coordinación de grupos cuyo propósito sea atentar contra activos concretos de una entidad. Este tipo de ataques no sólo se dirige a los clientes del sector financieros, sino también a la infraestructura y la organización de los bancos.

El tercer lugar lo ocupa el tipo de ataques que impactan en la Continuidad del Negocio, como los robos de credenciales, tanto de empleados como de clientes o proveedores, las fugas de información relacionada con la actividad económica de la entidad, la vulneración de los mecanismos de seguridad empleados por los bancos, la actividad hacktivista y activista, orientada a atentar contra activos del banco (ataques de denegación de servicios, escraches, entre otros).

En concreto, en este tipo de amenazas se hace referencia a la puesta en marcha de actividades que puedan afectar a la reputación de la entidad bancaria o de alguna de las personalidades relevantes de la misma. Las entidades financieras son altamente dependientes de su imagen de marca y su reputación como proveedores de servicios y productos hacia sus clientes, como consecuencia de la globalidad de los mercados y la competencia feroz para capturar nuevas relaciones de confianza.

Las amenazas de este sentido se pueden concretar en:

- Seguimiento de identidades digitales: en este aspecto son varias las amenazas que se aglutinan: la sobreexposición de información desde los perfiles oficiales en redes sociales que puedan suponer una fuga de información; las reacciones negativas en la rede ante declaraciones realizadas desde los perfiles oficiales; la identificación de perfiles fraudulentos en redes sociales; entre otros. Son amenazas que afectan a los perfiles oficiales de las entidades y a las personalidades destacadas de las mismas.

- Búsqueda de contenidos ofensivos: en este aspecto la difamación o la maledicencia en redes sociales se identifica como una de las principales

herramientas para causar daño a entidades financieras. Por ello, la identificación y seguimiento de perfiles de influencia en webs, blogs y redes sociales, enfocados a menoscabar la imagen o reputación del cliente, así como todas aquellas publicaciones que puedan suponer un riesgo y puedan impactarle legalmente o económicamente se convierten en obligatorios.

- Seguimiento de dominios: la amenaza en este sentido el typosquatting, concepto ligado a los dominios de Internet. Se trata de aquellos dominios publicados que, por su similitud con los dominios legítimos del cliente, podrían ser utilizados para suplantar a los dominios originales o redirigir a usuarios del cliente hacia páginas de terceros, a partir del aprovechamiento de los errores tipográficos que cometan los propios usuarios.

4.3. NORMATIVA SOBRE SEGURIDAD

Las medidas legales y las diversas normativas relacionadas de manera directa o indirecta con la seguridad TIC, el impulso a proyectos tractores relacionados con la seguridad, las campañas para la promoción de la seguridad o el impulso a la investigación en estas áreas tienen un impacto decisivo en sobre la oferta y la demanda de seguridad.

Las obligaciones relacionadas con la seguridad TIC, que de una manera directa o indirecta vienen impuestas por la legislación, constituyen un elemento de la máxima importancia a la hora de crear una demanda estable de soluciones de seguridad. Tal es la importancia de esta cuestión que los expertos la identifican como el principal factor de impulso del mercado de la seguridad TIC en España (KASPERSKY, 2016).

Algunas de las disposiciones legales establecen obligaciones directas para todas las empresas y organizaciones en materia de seguridad TIC. Otras normas no establecen directamente obligaciones en materia de seguridad, pero implican para los sujetos destinatarios de la necesidad de adoptar las medidas necesarias para garantizar la seguridad de sus sistemas de información con la finalidad de poder cumplir las obligaciones legales que se les imponen.

Las obligaciones legislativas y normativas han supuesto un aumento de la demanda de seguridad TIC (productos, servicios y profesionales). En España, la Ley Orgánica de Protección de Datos ha tenido un fuerte impacto, principalmente por tratarse de una ley cuya aplicación afecta a prácticamente todas las empresas del país.

También se ha dejado notar el efecto de la Ley Sarbannes-Oxley pues, aunque se trata de legislación estadounidense, están también obligadas a cumplirlo empresas extranjeras que tengan su sede matriz en Estados Unidos, lo que ha llevado a que en España se consuma seguridad TIC orientada al cumplimiento de esta ley (Dirección General de Seguridad, 2014).

Por otro lado, existe una normativa específica para determinados sectores. El sector de la banca ha recibido un fuerte impulso en seguridad TIC de la mano de la adopción obligatoria del Estándar de Seguridad de Datos PCI24 (PCI DSS), normativa que debe cumplirse por todos los negocios que almacenan, procesan y/o transmiten información de tarjetas de crédito/débito.

En definitiva, el cumplimiento normativo aparece como un aspecto clave en la potenciación de la implementación de seguridad TIC a gran escala y como factor de impulso para el mercado. Más adelante, en este apartado se detalla la normativa específica del sector financiero.

Las disposiciones legales pueden agruparse en cuatro categorías: normas que protegen derechos relacionados con la seguridad de la información; normas que establecen obligaciones en materia de seguridad, normas que proporcionan seguridad jurídica en el desarrollo de servicios relacionados con la seguridad TIC y normas que establecen obligaciones de seguridad específicamente para las administraciones públicas.

Asimismo, cabe destacar la importancia que en el ámbito normativo tienen los estándares y la certificación como mecanismos eficientes de promoción de buenas prácticas. La autorregulación mediante acuerdos de uso juega igualmente un importante papel en la difusión e impulso de las buenas prácticas en seguridad TIC.

Toda esta estructura normativa de seguridad supone un importante paso adelante para orientar los esfuerzos de empresas e instituciones en el difícil camino de implantar de forma adecuada las políticas de seguridad TIC.

4.3.1. Normas que protegen derechos relacionados con la seguridad:

Un primer grupo regulatorio lo constituyen las normas que protegen la seguridad TIC y sancionan conductas contrarias a la seguridad de la información. La propia Constitución Española incluye entre los derechos y libertades fundamentales la protección del secreto de las comunicaciones y de la intimidad de las personas frente al uso de medios electrónicos.

En cuanto a la protección penal, el Código Penal establece sanción penal para las conductas más graves, tales como las conductas vulneradoras de la intimidad personal o de la intimidad de los datos personales o constitutivos de estafas que se realicen utilizando las nuevas tecnologías. Asimismo, se tipifican actividades que causen daños deliberados en la información o sistemas informáticos ajenos, el espionaje empresarial instrumentado a través de nuevas tecnologías o acceso ilegítimo a servicios de televisión de pago o similares.

De la misma manera existen medidas de protección civil, mediante sanciones y medidas protectoras para las conductas de menor gravedad que no llegan a constituir ilícitos penales.

Destaca en este ámbito la normativa sobre protección de la propiedad intelectual, que regula aspectos como la protección de los derechos de autor sobre programas de ordenador, concediendo a su titular los derechos exclusivos para su explotación o la

protección de las medidas tecnológicas y de la información para la gestión de derechos, sancionando las conductas que atenten contra estos derechos protegidos.

4.3.2. Normas que establecen obligaciones en materia de seguridad TIC.

Este grupo se compone de las normas que establecen obligaciones en materia de seguridad TIC que representan en la práctica las disposiciones que de una manera más directa contribuyen a desarrollar el mercado de la seguridad TIC y a dotarlo de estabilidad. Este grupo de normas incluye tanto aquellas que imponen obligaciones al sector privado, como las que implican obligaciones relacionadas con la seguridad TIC para el sector público.

En lo que se refiere a las normas que establecen obligaciones directas de seguridad destaca sobre todas ellas la Ley de Protección de Datos Personales. Esta ley es sin duda la norma que ha tenido un impacto más directo en el desarrollo del mercado de la seguridad TIC en España, al establecer todo un conjunto de disposiciones sobre la seguridad de los ficheros informáticos que contienen datos personales de obligado cumplimiento para todos los sujetos públicos y privados titulares de dichos ficheros.

El amplio espectro de la Ley de protección de Datos Personales ha implicado un fuerte dinamismo para el mercado de soluciones de seguridad con incidencia en muchos de los elementos de la cadena de valor desde los fabricantes de equipos y sistemas hardware, el desarrollo de aplicaciones informáticas, la integración de sistemas, los servicios de soporte y mantenimiento, la consultoría e implantación de procedimientos o los servicios de auditoría de seguridad.

Cabe destacar por su importancia la Ley de Medidas de Impulso de la Sociedad de la Información. La ley impone a todas las empresas que presten servicios al público en general de especial trascendencia económica la obligación de facilitar a sus usuarios un medio de interlocución telemática que les permita la realización de diferentes trámites tales como la contratación electrónica de servicios, suministros y bienes, la

consulta de sus datos de cliente, la presentación de quejas, incidencias, sugerencias y, en su caso, reclamaciones, y el ejercicio de sus derechos de acceso, rectificación, cancelación y oposición en los términos previstos en la normativa reguladora de protección de datos de carácter personal. Para ello impone a estas empresas la obligación de garantizar la seguridad mediante el uso de certificados reconocidos de firma electrónica.

La Ley de Medidas de Impulso de la Sociedad de la Información también establece la obligatoriedad de la facturación electrónica en el marco de la contratación con el sector público estatal. Para ello la factura electrónica será un documento electrónico que cumple con los requisitos exigibles a las facturas y que, además, garantiza la autenticidad de su origen y la integridad de su contenido, lo que impide el repudio de la factura por su emisor.

Igualmente se prevé el uso de la factura electrónica en otras relaciones de los ciudadanos con la Administración tales como justificación de ayudas y subvenciones públicas.

Esta ley ha introducido asimismo obligaciones de información sobre seguridad. Se obliga a los proveedores de servicios de acceso a Internet a informar a sus clientes de forma permanente, fácil, directa y gratuita sobre los diferentes medios de carácter técnico que aumentan los niveles de la seguridad de la información y permiten, entre otros, la protección frente a virus informáticos y programas espía y la restricción de los correos electrónicos no solicitados.

Deberán igualmente informar a sus clientes sobre las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios en Internet no deseados o que puedan resultar nocivos para la juventud y la infancia, y también acerca de las posibles responsabilidades en que puedan incurrir por el uso de Internet con fines ilícitos, en particular, para la comisión de ilícitos penales y por la vulneración de la legislación en materia de propiedad intelectual e industrial.

4.3.3. Normas que proporcionan seguridad jurídica en el desarrollo de servicios.

Este grupo de medidas regulatorias lo constituyen las normas que proporcionan seguridad jurídica en el desarrollo de servicios relacionados con la seguridad TIC. Esta clase de normas no establecen obligaciones en sí mismas para la demanda de seguridad, pero sí ofrecen seguridad y confianza para los usuarios sobre determinados segmentos concretos del mercado de la seguridad TIC, dotándolos de cobertura legal, y estableciendo en otros casos requisitos y condiciones a la oferta de las empresas que proporcionan productos o servicios relacionados con la seguridad.

Destaca en este apartado la Ley de Firma Electrónica que ha establecido un marco regulador estable que ha permitido el desarrollo de soluciones de seguridad basadas en firma electrónica en diferentes ámbitos (e-Administración, facturación electrónica, entre otros).

Por otra parte ha establecido las condiciones básicas para regular la actividad de los prestadores de firma electrónica estableciendo de esta manera un marco para el desarrollo de este segmento de la oferta de seguridad TIC. El aspecto esencial de esta norma es equiparar el valor jurídico de la firma electrónica al de la firma manuscrita cuando la primera se produce bajo determinadas condiciones y cumple ciertos requisitos de seguridad.

Una segunda referencia de normas que contribuyen a generar confianza en el mercado de la seguridad TIC ha sido el sistema español de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información. Esta norma permite disponer de un esquema propio para que los fabricantes de productos o sistemas de TI que lo deseen puedan certificar la seguridad de dichos productos, y de esta manera mejorar la confianza de los usuarios en esta clase de soluciones.

Esta norma regula dos aspectos básicos. En primer lugar establece los requisitos que habrán de cumplir los laboratorios de evaluación y los procedimientos para su acreditación. En segundo lugar regula los procedimientos para la certificación de

productos y sistemas, así como los criterios y metodologías para la evaluación de la seguridad.

4.3.4. Normas que protegen la seguridad TIC y sancionan conductas contrarias.

La primera norma marco a la que se ha de hacer referencia es a la Constitución Española de 1978.

En su artículo 18 incluye entre los derechos y libertades fundamentales la protección del secreto de las comunicaciones y de la intimidad de las personas frente al uso de medios electrónicos.

En el artículo 18.3 se garantiza el secreto de las comunicaciones y, en especial, de las postales, telegráficas y telefónicas, salvo resolución judicial. En el artículo 18.4 la ley limita el uso de la informática para garantizar el honor y la intimidad personal y familiar de los ciudadanos y el pleno ejercicio de sus derechos.

En segundo lugar se encuentra la Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, donde se recogen hasta cinco aspectos diferentes de la seguridad TIC relacionados con:

- La protección de la intimidad personal y el acceso a datos de carácter personal en soportes electrónicos.
- Las estafas usando medios electrónicos.
- Las actividades que causen daños deliberados en la información o sistemas informáticos ajenos.
- El espionaje empresarial.
- El acceso ilegítimo a servicios de televisión de pago o similares.

El artículo 197 de la misma norma se prevé “que, para descubrir los secretos o vulnerar la intimidad de otro, sin su consentimiento, se apodere de sus papeles, cartas,

mensajes de correo electrónico o cualesquiera otros documentos o efectos personales o intercepte sus telecomunicaciones o utilice artificios técnicos de escucha, transmisión, grabación o reproducción del sonido o de la imagen, o de cualquier otra señal de comunicación, será castigado con las penas de prisión de uno a cuatro años y multa de doce a veinticuatro meses" (Código Penal, 1995).

Las mismas penas se impondrán al que, sin estar autorizado, se apodere, utilice o modifique, en perjuicio de tercero, datos reservados de carácter personal o familiar de otro que se hallen registrados en ficheros o soportes informáticos, electrónicos o telemáticos, o en cualquier otro tipo de archivo o registro público o privado. Iguales penas se impondrán a quien, sin estar autorizado, acceda por cualquier medio a los mismos y a quien los altere o utilice en perjuicio del titular de los datos o de un tercero.

Se impondrá la pena de prisión de dos a cinco años si se difunden, revelan o ceden a terceros los datos o hechos descubiertos o las imágenes captadas a que se refieren los números anteriores.

El artículo 248 tipifica como reos del delito de estafa a los que, con ánimo de lucro, y valiéndose de alguna manipulación informática o artificio semejante consigan la transferencia no consentida de cualquier activo patrimonial en perjuicio de tercero. La misma pena se aplicará a los que fabricaren, introdujeren, poseyeren o facilitaren programas de ordenador específicamente destinados a la comisión de las estafas.

El artículo 264 castiga con la pena de prisión de uno a tres años y multa de doce a veinticuatro meses al que por cualquier medio destruya, altere, inutilice o de cualquier otro modo dañe los datos, programas o documentos electrónicos ajenos contenidos en redes, soportes o sistemas informáticos.

El artículo 278 se refiere al espionaje empresarial y establece que el que, para descubrir un secreto de empresa se apoderare por cualquier medio de datos, documentos escritos o electrónicos, soportes informáticos u otros objetos que se refieran al mismo, o empleare alguno de los medios o instrumentos señalados en el apartado 1 del artículo

197, será castigado con la pena de prisión de dos a cuatro años y multa de doce a veinticuatro meses.

El artículo 286 tipifica como delito aquellas acciones que, sin consentimiento del prestador de servicios y con fines comerciales, faciliten el acceso inteligible a un servicio de radiodifusión sonora o televisiva, a servicios interactivos prestados a distancia por vía electrónica, o suministre el acceso condicional a los mismos, considerado como servicio independiente.

En otro orden de cosas, el Real Decreto legislativo 1/1996 por el que se aprueba el texto refundido de la ley de Protección Intelectual también contempla regulación sobre las TIC.

En sus artículos 95 a 104 regula la protección de los derechos de autor sobre programas de ordenador concediendo a su titular los derechos exclusivos para su explotación. Tendrán la consideración de infractores de los derechos de autor quienes, sin autorización del titular de los mismos:

- Pongan en circulación una o más copias de un programa de ordenador conociendo o pudiendo presumir su naturaleza ilegítima.

- Tengan con fines comerciales una o más copias de un programa de ordenador, conociendo o pudiendo presumir su naturaleza ilegítima.

- Pongan en circulación o tengan con fines comerciales cualquier instrumento cuyo único uso sea facilitar la supresión o neutralización no autorizadas de cualquier dispositivo técnico utilizado para proteger un programa de ordenador.

Por su parte, los artículos 160 a 162 de la ley regulan la protección de las medidas tecnológicas y de la información para la gestión de derechos, y permiten adoptar medidas de protección contra quienes, a sabiendas o teniendo motivos razonables para saberlo, eludan cualquier medida tecnológica eficaz, así como respecto de aquellos que fabriquen o distribuyan cualquier dispositivo, producto o componente para eludir dichas medidas.

Asimismo se prevé la posibilidad de solicitar medidas de protección contra quienes, a sabiendas y sin autorización lleven a cabo alguno de los actos siguientes:

- Supresión o alteración de toda información para la gestión electrónica de derechos.

- Distribución, importación para distribución, emisión por radiodifusión, comunicación o puesta a disposición del público de obras o prestaciones protegidas en las que se haya suprimido o alterado sin autorización la información para la gestión electrónica de derechos.

Por su parte,la Ley de Firma Electrónica constituye una norma de gran importancia para el mercado español de la seguridad TIC. A diferencia de la LOPD no establece obligaciones directas en materia de seguridad TIC con un impacto directo en la demanda (con la salvedad de la regulación relativa al eDNI).

Sin embargo sí ha establecido un marco regulador estable que ha permitido el desarrollo de soluciones de seguridad basadas en firma electrónica en diferentes ámbitos (e-Administración, facturación electrónica…). Por otra parte ha establecido las condiciones básicas para regular la actividad de los prestadores de firma electrónica estableciendo de esta manera un marco para el desarrollo de este segmento de la oferta de seguridad TIC.

El aspecto esencial de esta norma es equiparar el valor jurídico de la firma electrónica al de la firma manuscrita cuando la primera se produce bajo determinadas condiciones y ciertos requisitos de seguridad. No obstante no niega validez a la firma electrónica que no alcance dichos mínimos de seguridad.

La norma no establece requisitos técnicos obligatorios ni técnicas, dejando al mercado la definición del nivel de seguridad de los productos y servicios de firma electrónica en atención a las necesidades de los usuarios y a las tecnologías disponibles.

Desde la perspectiva de impacto directo en el mercado el aspecto más relevante es la regulación del DNI electrónico y en concreto lo previsto en el artículo 15.2 de la norma que obliga a todas la personas físicas o jurídicas, públicas o privadas, a reconocer la eficacia del documento nacional de identidad electrónico para acreditar la identidad y los demás datos personales del titular que consten en el mismo, y para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica en él incluidos.

Otro aspecto a reseñar desde el punto de vista del mercado de la seguridad TIC es la creación en la ley de un esquema de certificación de prestadores de firma electrónica y de dispositivos de creación de firma electrónica. No obstante, el alcance cuantitativo de esta previsión es limitado dado el reducido número de prestadores de servicios de certificación existentes en los mercados nacionales.

Se trata de un aspecto cualitativamente relevante al constituir una primera aproximación legal a la certificación de los productos y servicios de seguridad TIC.

En este caso la ley ofrece a los prestadores y productos certificados la presunción de cumplimiento de los requisitos de seguridad exigibles para la plena eficacia legal de la firma, lo que en caso de litigio permite acreditar de manera directa el cumplimiento de los mismos.

Otra norma de relevancia es la Orden PRE/2740/2007 que aprueba el Reglamento de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

Se trata de un paso importante para la consolidación del mercado de la seguridad TIC en España, que permite disponer de un esquema propio para que los fabricantes de productos o sistemas de TI que lo deseen puedan certificar la seguridad de dichos productos. Al mismo tiempo se establecen las condiciones para facilitar que las entidades públicas o privadas que quieran ejercer de laboratorios de evaluación de la seguridad de las TI en el marco del Esquema puedan desarrollar su actividad en España, creando un mercado en este ámbito.

Esta norma regula dos aspectos básicos. En primer lugar establece los requisitos que habrán de cumplir los laboratorios de evaluación y los procedimientos para su acreditación. En segundo lugar regula los procedimientos para la certificación de productos y sistemas, así como los criterios y metodologías para la evaluación de la seguridad.

Los criterios de evaluación serán los recogidos en las siguientes normas:

a) Common Criteria for Information Technology Security Evaluation.

b) ISO/IEC 15408, Evaluation Criteria for IT Security.

c) Information Technology Security Evaluation Criteria (abreviado, ITSEC). Office for Official Publications of the European Communities.

Actúa como organismo de certificación de todo el esquema el Centro Criptológico Nacional. Dicho organismo se constituye al amparo de la Ley 11/2002, de 6 de mayo, reguladora del Centro Nacional de Inteligencia, que encomienda a este centro el ejercicio de las funciones relativas a la seguridad de las tecnologías de la información, y según lo dispuesto en el Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, entre cuyas funciones está la de constituir el Organismo de Certificación del Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información.

En la Ley Orgánica 15/1999, de Protección de Datos Personales (LOPD) se halla uno de los determinantes que más han influido en el desarrollo del mercado de la seguridad TIC en España.

Como cuestión inicial es necesario señalar que las disposiciones de la ley no se refieren de una manera específica o exclusiva a la protección de datos personales contenidos en soportes electrónicos sino que es de aplicación a toda clase de soportes de los ficheros correspondientes.

Es el Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la LOPD, la norma que establece los requisitos concretos para los titulares de ficheros o sistemas de información que realicen almacenamiento o tratamiento de datos personales tanto en formato electrónico como en papel.

Este reglamento establece tres niveles de seguridad en función de la naturaleza de los datos personales de que se trate y más que requisitos técnicos concretos, recoge obligaciones de carácter organizativo y de gestión para cada tipo de datos como las siguientes:

- Documento de seguridad que incluya funciones y obligaciones del personal.
- Registro de incidencias.
- Sistema de identificación y autenticación de usuarios y de control de acceso a los datos.
- Obligación en cuanto a la gestión de soporte de los datos, copias de respaldo y recuperación.
- Auditoría de los sistemas de información y de los soportes.
- Cifrado de datos cuando se transmitan por redes de telecomunicaciones.

Esta ley además de su efecto directo sobre las empresas y el sector público ha dado lugar a todo un conjunto de efectos indirectos, asociados a otras disposiciones

legales que imponen al sector público o privado obligaciones de almacenamiento de datos.

A título de ejemplo y por su relevancia puede citarse la Ley 25/2007 de Conservación de datos relativos a las Comunicaciones Electrónicas y a las Redes Públicas de Comunicaciones, que tiene por objeto la regulación de la obligación de los operadores de conservar los datos generados o tratados en el marco de la prestación de servicios de comunicaciones electrónicas o de redes públicas de comunicación, así como el deber de cesión de dichos datos a los agentes facultados siempre que les sean requeridos a través de la correspondiente autorización judicial con fines de detección, investigación y enjuiciamiento de delitos graves contemplados en el Código Penal o en las leyes penales especiales. En esta norma se obliga a estos operadores a garantizar la seguridad de los datos almacenados.

En la Ley 56/2007, de 28 de diciembre, de Medidas de Impulso de la Sociedad de la Información, además de las previsiones sobre uso de la factura electrónica en los ámbitos público y privado recogidas en esta norma legal, la ley establece una serie de obligaciones para un número significativo de empresas del sector privado muy relacionadas con la seguridad TIC.

La Ley impone, en su artículo 2, a todas las empresas que presten servicios al público en general de especial trascendencia económica la obligación de facilitar a sus usuarios un medio de interlocución telemática que les permita la realización de diferentes trámites tales como la contratación electrónica de servicios, suministros y bienes, la consulta de sus datos de cliente, la presentación de quejas, incidencias, sugerencias y, en su caso, reclamaciones, y el ejercicio de sus derechos de acceso, rectificación, cancelación y oposición en los términos previstos en la normativa reguladora de protección de datos de carácter personal.

Para ello impone a estas empresas la obligación de garantizar la seguridad del uso de estos medios mediante el uso de certificados reconocidos de firma electrónica.

Por otra parte en su disposición adicional tercera prevé un plan de mejora de los niveles de seguridad y confianza en Internet, que habrá de ser elaborado por el Gobierno y que incluirá directrices y medidas para aumentar la seguridad frente a las amenazas de Internet y proteger la privacidad online. Este plan se revisará periódicamente para poder responder al escenario de amenazas en continua evolución.

La Ley General de Telecomunicaciones dedica el Capítulo III de su Título III a regular el secreto de las comunicaciones y la protección de los datos personales en este ámbito.

El artículo 33 de la ley establece la obligación de los operadores de redes y servicios de comunicaciones electrónicas a garantizar el secreto de las comunicaciones de conformidad con los artículos 18.3 y 55.2 de la Constitución, debiendo adoptar las medidas técnicas necesarias para ello.

Asimismo se les obliga a la interceptación legal de las comunicaciones de acuerdo con la legislación vigente, adoptando para ello a su costa las soluciones técnicas necesarias. El alcance de las obligaciones de interceptación previstas en este artículo ha sido ampliado y detallado en la Ley 25/2007.

El artículo 34 establece que los operadores deberán garantizar la protección de los datos personales adoptando para ello las medidas técnicas y de gestión adecuadas para preservar la seguridad en la explotación de su red o en la prestación de sus servicios.

El artículo 35 se refiere al cifrado en las redes y servicios de comunicaciones electrónicas, reconociéndose con carácter general el derecho a proteger la información mediante sistemas de cifrado.

Asimismo se prevé la posibilidad de que se podrá imponer la obligación de facilitar a un órgano de la Administración General del Estado o a un organismo público los algoritmos o cualquier procedimiento de cifrado utilizado. No obstante dicha previsión no se ha concretado por el momento.

Por su parte, la Ley de Servicios de la Sociedad de la Información contempla tres aspectos relacionados con la seguridad TIC. En primer lugar, establece determinadas obligaciones de colaboración de los prestadores de estos servicios de la Sociedad de la Información con las autoridades al objeto de facilitar la persecución de actividades o conductas ilícitas o impedir su realización.

En segundo lugar recoge una serie de previsiones en relación con el envío de comunicaciones comerciales no solicitadas (spam). Por último recoge previsiones sobre la información a los usuarios relacionada con la seguridad TIC.

Respecto de la primera de estas cuestiones, el artículo 11 establece un deber general de colaboración de los prestadores de servicios de intermediación, al objeto de hacer efectivas las resoluciones de las autoridades para ordenar la interrupción de un servicio o la retirada de un contenido ilícito proveniente de otros prestadores de servicios.

Por su parte, en su artículo 12 se regula una obligación de retención de datos de tráfico. Se obliga a los operadores de redes y servicios de comunicaciones electrónicas, los proveedores de acceso a redes de telecomunicaciones y los prestadores de servicios de alojamiento de datos a retener los datos de conexión y tráfico generados por las comunicaciones establecidas durante la prestación de un servicio de la Sociedad de la Información por un período máximo de doce meses.

Asimismo, están obligados a adoptar las medidas de seguridad apropiadas para evitar su pérdida o alteración y el acceso no autorizado a los mismos. No obstante ese artículo no ha sido objeto de desarrollo reglamentario por lo que hasta la fecha no ha tenido una aplicación práctica. En todo caso la aprobación de la Ley 25/2007 de conservación de datos ha venido a establecer un régimen legal más detallado y completo en esta materia.

La segunda de las cuestiones relevantes en materia de seguridad TIC recogidas en esta ley es la relativa a las comunicaciones comerciales por vía electrónica a las que se dedica el Título III, en sus artículos desde el 19 al 22.

En este aspecto la ley puede ser considerada como garantista al establecer la prohibición del envío de comunicaciones publicitarias o promocionales por correo electrónico u otro medio de comunicación electrónica equivalente que previamente no hubieran sido solicitadas o expresamente autorizadas por los destinatarios de las mismas, lo que se conoce como el Modelo Opt-In.

Se recoge en la norma una excepción a este principio general por imposición de la normativa comunitaria para los casos en que exista una relación contractual previa, siempre que el prestador hubiera obtenido de forma lícita los datos de contacto del destinatario y los empleara para el envío de comunicaciones comerciales referentes a productos o servicios de su propia empresa que sean similares a los que inicialmente fueron objeto de contratación con el cliente, que es el modelo Opt-Out.

Asimismo se reconoce una serie de derechos a los destinatarios como el de revocar en cualquier momento el consentimiento prestado o derechos en relación con el tratamiento de datos personales.

Por último, la Ley de Medidas de Impulso de la Sociedad de la Información ha introducido, en su artículo 4.6, determinadas modificaciones en la Ley 34/2002, entre las que destaca la introducción de un nuevo artículo, el 12bis, relativo a obligaciones de información sobre seguridad. Se obliga los proveedores de servicios de acceso a Internet a informar a sus clientes de forma permanente, fácil, directa y gratuita sobre los diferentes medios de carácter técnico que aumenten los niveles de la seguridad de la información y permitan, entre otros, la protección frente a virus informáticos y programas espía, y la restricción de los correos electrónicos no solicitados.

Deberán igualmente informar a sus clientes sobre las herramientas existentes para el filtrado y restricción del acceso a determinados contenidos y servicios en Internet no deseados o que puedan resultar nocivos para la juventud y la infancia, y también acerca de las posibles responsabilidades en que puedan incurrir por el uso de Internet con fines ilícitos, en particular, para la comisión de ilícitos penales y por la vulneración de la legislación en materia de propiedad intelectual e industrial.

Asimismo, estos proveedores de acceso a Internet y los prestadores de servicios de correo electrónico deberán informar a sus clientes de forma permanente, fácil, directa y gratuita sobre las medidas de seguridad que apliquen en la provisión de los mencionados servicios.

Estas obligaciones de información vendrán a mejorar sin lugar a dudas la sensibilización de los usuarios y en especial de los usuarios residenciales sobre la seguridad TIC y las soluciones y productos existentes para prevenir y resolver posibles problemas relacionados con la misma, actuando en consecuencia sobre uno de los problemas básicos identificados entre las barreras para el desarrollo del mercado de la seguridad TIC en España.

Por su parte, la Unión Europea ha implementado normativa y respalda la cooperación operativa, como parte de la Estrategia de Ciberseguridad de la Unión. Por un lado, se ha desarrollado normativa para la protección frente al cibercrimen como la Directiva 2013 relativa a Ataques contra Sistemas de Información, o la Directiva sobre Privacidad y Comunicaciones Electrónicas del año 2002.

Por otro lado, la Comisión Europea ha jugado un papel clave en el desarrollo del Centro Europeo del Cibercrimen (EC3), en el que se ponen en común los conocimientos de ciberdelincuencia para apoyar las investigaciones de delitos de los Estados miembros.

4.3.5. Normativa específica del sector financiero en materia de ciberseguridad.

En cuanto a la regulación relativa a la Seguridad de la información en el sector financiero destacan las siguientes normas reguladoras:

- Normativa del Banco Central Europeo: Recomendaciones para la seguridad de los pagos por internet, recomendaciones para los servicios

de acceso a una cuenta de pago. Ley 8/2011, de 28 de abril, por la que se establecen medidas para la protección de las infraestructuras críticas.

- PCI-DSS. Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago. Con respecto al funcionamiento de los medios de pago y de las entidades que emiten medios de pago, así como las relaciones entre dichas entidades y los usuarios de los medios de pago se encuentran regulados en la Ley 16/2009, de 13 de noviembre de Servicios de Pago. La Ley de Servicios de Pago establece de manera expresa una serie de actividades excluidas de su ámbito de aplicación, de tal forma que no son necesarias ni la autorización para prestar y ejecutar los servicios de pago ni la supervisión del Banco de España.

- En relación al Comercio Electrónico, hay que tener en cuenta las directrices de la Agenda Digital europea y española y el Plan de Confianza en el ámbito Digital lideradas por el gobierno donde se establece un ámbito de colaboración público-privada.

- En el ámbito bancario, hay que destacar la Gestión de Identidad para evitar Suplantaciones y Fraudes y para ello hay que apoyarse en las medidas técnicas disponibles (doble factor de autenticación, Open ID Connect como el Mobile Connect, entre otros), así como en la Concienciación del Consumidor y de los Trabajadores.

- El Real Decreto 421/2004, de 12 de marzo, por el que se regula el Centro Criptológico Nacional, y se dota de capacidad para llevar a cabo un seguimiento exhaustivo de la evolución de dichos activos financieros que cada vez están siendo más populares.

5. EL FUTURO DEL DINERO FIDUCIARIO Y LAS CRIPTOMONEDAS

El dinero fiduciario es cada vez menos utilizado en las transacciones comerciales, puesto que la utilización de las tarjetas, los monederos virtuales y demás elementos de pago están limitado su uso.

Asimismo, aunque es pronto para afirmarlo, el dinero fiduciario puede llegar a tener su fin en menor tiempo del que se podría imaginar. Un hecho que revela su capacidad para ser sustituido es la criptomoneda.

Además, cabe decir que el dinero fiduciario funciona del mismo modo que ésta, ya que la paridad con las reservas de oro de los bancos nacionales dejó de funcionar.

Por otro lado, en la actualidad las transacciones entre la mayoría de los agentes de la economía son meros apuntes contables que no implican el movimiento real de dinero.

Con todo esto, cabe dedicar unas líneas a la forma de pago emergente vinculada a las TIC que está revolucionando el sistema de pago a nivel mundial.

El Bitcoin, y el resto de criptomonedas o monedas virtuales, surgieron como alternativa a las monedas convencionales y al actual sistema de divisas. Se sustentan en el protocolo P2P como medio de pago con dinero virtual para comprar productos y servicios online.

Las diferencias de estas monedas respecto a las tradicionales son varias. Primeramente, no pertenecen a ningún Estado o país y pueden usarse en todo el mundo por igual. Están descentralizadas: no son controladas por ningún Estado, banco, institución financiera o empresa. No hay intermediarios: las transacciones se hacen directamente de persona a persona. Se pueden cambiar bitcoins a euros u otras divisas y viceversa, como cualquier moneda.

Pero la gran disrupción se encuentra en la tecnología distribuida que soporta de estas monedas, el denominado Blockchain, mediante la cual se puede transferir

cualquier activo entre dos usuarios sin la necesidad de una entidad central o de compensación.

Esta revolución financiera está generando un cambio profundo en el sistema financiero y están apostando por ella fondos de inversión, startups especializadas, entidades financieras y organismos públicos. Entre estos últimos cabe destacar el Banco de Inglaterra o la Comisión Europea, que están estudiando la posibilidad de emitir en el futuro una moneda digital propia y las consecuencias que ello tendría.

Además esta tecnología basada en el Blockchain puede ahorrar muchos millones de euros al sector financiero pero también podría convertirse en un competidor muy disruptivo.

Sin embargo, desde la Comisión Nacional del Mercado de Valores han destacado que estos activos no tienen la consideración legal de dinero ni de depósitos y, por tanto, no se benefician de las protecciones y garantías contempladas en la normativa de productos bancarios o de inversión.

Destacan su carácter especulativo, la ausencia de respaldo por parte de los organismos supervisores y las vulnerabilidades que presentan tanto por el lado del fraude como por el de la posible manipulación de precios. Y hacen hincapié en los problemas de liquidez que pueden presentar.

Independientemente de las alertas de este tipo de activo financiero por parte de los organismos públicos españoles el interés por la materia crece exponencialmente. Desde su aparición en el año 2009, el número de criptoactivos ha aumentado de forma sostenida hasta llegar a sobrepasar las 1.500 iniciativas. Además, su valor de mercado se ha multiplicado más que cualquier otro activo sujeto a cotización.

Estos hechos se añaden a la amplitud de las modalidades de su comercialización, que pueden ser comercializadas directamente, a través de contratos por diferencias o por medio de otros productos estructurados como contratos con futuros o swaps; esto favorece una mayor diversidad de usos y hace que las economías de todo el mundo estén cada vez más expuestas a sus riesgos.

Si bien es cierto que su peso relativo sigue siendo pequeño con apenas el 1% del PIB mundial, se constata que los criptoactivos van ganando atractivo entre el inversor minorista.

Este hecho, unido a su volatilidad extrema y a las fuertes pérdidas que han experimentado a consecuencia de fallos operativos y de otras amenazas cibernéticas, expone un panorama ante el que resulta apremiante que las autoridades tomen medidas.

Los entes reguladores están focalizados en las posibles repercusiones para la estabilidad financiera, incluyendo las ramificaciones que puedan tener sobre la protección de la clientela, la protección de datos, la integridad del mercado, la evasión fiscal o la elusión de controles sobre el blanqueo.

Al tratarse de un fenómeno de carácter global, la efectividad de cualquier medida pasa por apostar por un enfoque cooperativo, cuestión en la que España está plenamente involucrada tanto en Europa como en otros foros multilaterales. En concreto, uno de los compromisos destacados del Consejo de Estabilidad Financiera (FSB, siglas en inglés) y de la Comisión Europea para el ejercicio 2018 es la identificación de las necesidades de información y la formulación de unos indicadores adecuados que permitan reforzar las tareas de seguimiento y medición de los riesgos emergentes.

Este esfuerzo por aumentar la transparencia y trazabilidad de la operativa que tiene lugar con criptoactivos debe ser visto como un primer paso dentro de una estrategia más ambiciosa que aspire a evaluar con más precisión los posibles riesgos, sin descartar en última instancia que se produzcan cambios normativos que den respuesta a las vulnerabilidades detectadas, eliminen las oportunidades para el arbitraje y provean un fundamento sólido para el desarrollo de una industria compatible con la existencia de un sistema financiero global seguro.

6. EL SECTOR FINANCIERO Y EL BIG DATA.

Las entidades financieras están experimentando a una revolución tecnológica sin precedentes, que está transformando el mundo en términos de lo que se puede hacer y del coste al que puede hacerse. En consecuencia estos cambios impactan de forma sustancial en la actividad del sector. Dicha revolución se manifiesta tanto en la generación y el acceso a la información como en su almacenamiento, procesamiento y modelización.

Por un lado, la velocidad a la que se genera la información se está incrementando de forma vertiginosa. Según la Federal Big Data Commission, el volumen total de datos en el mundos e duplica cada 18 meses. Estos datos son mayoritariamente digitales, el 50% se puede consultar mediante Internet, el 80% son desestructurados (Federal Big Data Commission, 2014). La mayoría de estos datos provienen de fuentes como las redes sociales, logs de actividad, entre otros.

Es por esto que el fenómeno Big DATA se está caracterizando por una explosión de las tres uves: volumen, variedad de fuentes y velocidad de generación de datos.

Por otro lado, se observa también una explosión del acceso a la información mediante dispositivos móviles. El mercado de móviles global se acerca al punto de saturación y el de smartphones alcanzó el 51% de cuota en 2016[8]. Es evidente el crecimiento decreciente de ambos subsectores, lo que hace prever que surgirá una nueva tecnología de reemplazo en el corto plazo, donde se incluirán Internet delas Cosas y los dispositivos Wearables con tecnología integrada (European Banking Authority, 2014).

En otro orden de cosas, la capacidad de almacenamiento crece de forma exponencial y su coste unitario desciende del mismo modo. Por ejemplo, almacenar un 1GB de datos en 1980 costaba 10 millones de dólares, en la actualidad es menos de 10 centavos de dólar (Authority, 2014). Esto ha llevado a que la cantidad de información almancenada sea masiva.

[8] International Telecommunication Union.

El mismo fenómeno se da en el procesamiento: la capacidad de ejecutar instrucciones por segundo por cada 1.000 dólares de procesador se ha multiplicado por casi 300 desde el año 2000 (Kurzweil, 2014). El desarrollo de la computación distribuida permite paralelizar las operaciones en numerosos núcleos y, una vez en manos de gigantes tecnológicos como Google, se perfila como el futuro del procesamiento.

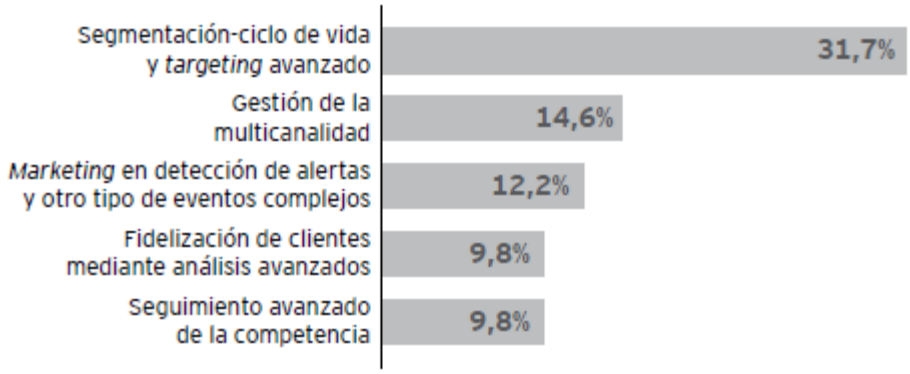
En el sector financiero, la banca digital y los requerimientos del mundo de la información hacen que las entidades necesiten mayores capacidades de procesamiento y por ello se proveen de máquinas de alto rendimiento y computación distribuida.

Por último, las capacidade de modelización están evolucionando con rapidez, impulsadas por las nuevas tecnologías y la disponibilidad de información. El número de decisiones que se toman de forma automática empleando modelos en las entidades financieras se multiplica cada año con el consecuente aumento de beneficios desde la eficiencia obtenida.

La industria financiera es una de las más beneficiadas por la adopción del data science. De hecho, es el sector qu maneja la mayor cantidad y calidad de información de sus clientes para extraer conocimiento e incorporarlo en su propuesta de valor.

En el gráfico siguiente se observan las oportunidades percibidas por parte del sector de la banca del Big DATA.

GRÁFICO 7: OPORTUNIDADES ESTRATÉGICAS DEL BIG DATA EN LAS ENTIDADES BANCARIAS.



Fuente: Análisis EY, FrontQuery y Teradata.

La principal oportunidad está constituida por la segmentación avanzada de clientes. La incorporación de nuevas fuentes de datos a las segmentaciones tradicionales posibilita la obtención de una visión y un entendimiento más completos de los clientes de las entidades, lo que lleva aparejada la definición de propuestas de valor más adaptadas a los diferentes perfiles de clientes (KASPERSKY, 2016).

Conocer mejor a los clientes permite realizar un targeting más ajustado, y esto se traduce en mayor eficiencia y rendimiento de las acciones comerciales.

Por otro lado, la fidelización de clientes se perfila como la segunda aplicación de estas técnicas, especialmente relevante en las entidades financieras. Tras una profunda crisis del sector, que ha llevado a una fuerte pérdida de confianza por parte de los clientes, detectar el abandono con suficiente antelación y definir acciones de retención eficientes ha pasado a ser una prioridad para las entidades, área en el cual Big DATA y Analytics pueden ayudar a mejorar.

En otro orden de cosas, una mejor gestión de la *omnicanalidad*, aspecto muy importante en un contexto en el que las nuevas tecnologías ponen a disposición de los clientes un mayor número de canales de comunicación mejorados y alta capacidad de transacción con las empresas, y la definición de estrategias de pricing dinámico por segmento de cliente, en un contexto que se acerca al real time, aparecen también en puestos destacados cuando se pregunta por las principales áreas de aplicación de Big DATA.

En definitiva, el Big DATA es uno de los ámbitos de las TIC que mayor recorrido tiene que ofrecer para el sector financiero que, desde la buena gestión, puede desarrollar un tipo de negocio personalizado y de alta eficiencia.

8. CONCLUSIONES

Las nuevas tecnologías han revolucionado el panorama económico y social a nivel mundial. La rapidez con la que se llevan a cabo cambios tecnológicos de envergadura que convierten en obsoletos programas y aplicaciones recientes es vertiginoso y abrumador. Sin embargo, para el sector financiero, que sigue muy de cerca los cambios en las nuevas tecnologías, es una gran oportunidad para reinventar su modelo de negocio.

Al tiempo que las relaciones entre entidad y cliente cambian, los productos y servicios son cada vez más tecnológicos y aparecen activos virtuales como las criptomonedas, también el riesgo y el cibercrimen se une a dicho crecimiento.

La legislación, a pesar de su intento por mantenerse ágil a los cambios de la sociedad tecnológica y de establecer marcos regulatorios con el fin de proteger a los usuarios de las TIC, se encuentra en retraso constante.

En muchas ocasiones la norma aparece posterior al crimen. Este hecho es un punto débil en la estructura financiera, puesto que el volumen de datos confidenciales que maneja la industria bancaria es muy suculento y los ciberdelincuentes están constantemente tratando de anticiparse a la norma.

En definitiva, el sector financiero está a la cabeza en cuanto a implementación de TIC en su modelo de negocio, aspecto que afecta directamente a la evolución de la sociedad tecnológica. Puede seguir siendo uno de los sectores de la economía que más beneficios obtenga del Big DATA y de la interconectividad de la sociedad.

9. BIBLIOGRAFÍA

Accenture. (2010). Estudio de costes de tecnologías de la información en las entidades financieras. *Centro de Alto Rendimiento de Accenture*, 457.

Authority, E. B. (2014). *Guidelines on common procedures and methologies for the supervisory review and evaluation process.* SREP: SREP.

Baena, V., & del Barrio, G. (2013). *Impacto de la adopción de internet como canalde distribución en el sector bancario español: Evolución y perspectiva del futuro.* Madrid: Boletín Económico del ICE Nº3035.

BCE, B. C. (2010b). Statistical Data Warehouse. *EU Banking Structures*, 42.

Calvo, A. (2012). *Ética y sistema financiero: reflexiones a la luz de las crisis bancarias en España.* Madrid: CEU Ediciones.

Casilda, R. (1997). Realidades y alternativas, el futuro de la banca. La banca virtual. *Esic-Market*, 53.

Climent, F. J., & Momparler, A. (2016). *La situación de la banca online en España.* Boletín Económico del ICE: ICE.

Commission, F. B. (2014). *Demistifying big data, a practical guide to transforming the business of Governmment.* New York: FBDC.

económicos, D. d. (2016). *Estudio de transacciones por banca móvil e internet.* Madrid: ASBANC.

España, B. d. (2011). Boletín Estadísitco. *Banco de España*, 56.

España, B. d. (2013c). *Entidades de dinero electrónico.* Madrid: Banco de España.

ESPAÑA, P. D. (2014). *Informe anual de Seguridad Nacional.* Madrid: Gobierno de España.

Europeo, P. (2015). *Cibersecurity in the European Union and Beyond: Exploring the Threats and Policy Responses.* Bruselas: Directorate-General for Internal Policies.

Fanjul Suárez, J. L., & Valdunciel, L. (2007). *Un paradigma de la nueva economía: el sector financiero en España.* León: Facultad de ciencias Económicas y Empresariales. Universidad de León.

Fernándezde Guevara, J. (2007). La mejora de la productividad bancaria en España: crecimiento y progreso técnico. *Instituto Valenciano de Investicaciones Económicas*, 54.

FUNDESCO. (1988). *Las nuevas tecnologías de la información y el futuro del sistema financiero español. Definicion de tendencias y futuro lógico.* Madrid: Informe final de la Fase II, D.O.P. Nº3.

García García, C. R. (2004). La expansión de la banca online en España. *Información Comercial Española, ICE*, 89.

Honohan, P. (2008). Cross-Country Variation in Houshold Access to Financial Services. *JOurnal of Bankikg & Finance*, 2482.

Institute, P. (2015). *Global Encryption & Key Management Trends Study.* Traverse City: Ponemon Institute.

ISACA. (2015). *Global Cybersecurity Status Report.* Chicago: ISACA.

KASPERSKY. (2016). *Las predicciones de Kaspersky Lab en ciberseguridad.* ..: KASPERSKY.

Kendall, J., Mylenko, N., & Ponce, A. (2010). Measuring financial access around the world. *World bank Policy Research*, 5253.

Kurweil, R. (2006). *The Singularity is Near: When Humans Trascend Biology.* New York: Penguin Books.

Kurzweil, R. (2014). *The accelerating power of technology.* Boston: Pingdom.

Lozano Lázaro, M., & Sebastián Cermeño, J. (2006). *Las TIC en el sector financiero español.* Madrid: Tribuna Fundación Telefónica.

Marquina Cogolludo, J. (2005). La tecnología en la banca. *Colección Mediterráneo Económico: Los retos de la industria bancaria en España*, 87.

Martínez León, I. M., Olmedo Cifuentes, I., & Reyes Contreras, Y. (2007). Importancia del conocimiento en la Banca Online. *Universidad Politécnica de Cartagena*, 25.

Méndez, E. (2015). *Las instituciones europeas ante la crisis económica: Análisis y propuestas para politizar y democratizar el proceso de tomad de decisioens a nivel europeo.* Madrid: UGR.

Penal, C. (1995). *Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal.* Madrid: BOE Nº281, de 24 de noviembre de 1995.

Sánchez Pajares, E., Martín Enríquez, A., & Bela Kindelán, J. (2007). Iniciativas para fomentar el uso de los servicios bancarios a distancia. *Ekonomiaz: Revista vasca de economía*, 194.

Sarriá, N. (1994). Las tecnologías de la información como factor de competitiviad en las entidades financieras. *Papeles de Economía Español*, 58.

Sector de la Normalización de las Telecomunicaciones de la UIT, U. (2008). *Serie X: Redes de Datos, Comunicaciones de Sistemas Abiertos y Seguridad (X.1205).* Naciones Unidas: Recomendación UIT-T.1205.