LA TECNOLOGÍA EN LA BANCA

Jesús Marquina Cogolludo [1]

1. Introducción

El negocio de la banca es un negocio tan antiguo como el dinero; asirios, romanos, cartagineses, ya hablaban de negocios y en ellos se empezaba a dibujar los albores de lo que estaba llamado a ser con los años la *industria bancaria*. En el libro de las maravillas de Marco Polo ya se hablaba de *Xeques* y *Pagares*, para que los comerciantes pudiesen viajar mas seguros. Por referirnos a España, podemos citar algunos hitos relevantes de la historia como la aparición en el siglo XVI de las primeras letras de cambio en las ferias de Medina del Campo, coincidiendo con la aparición de las primeras Cajas de Ahorro, con origen en los erarios públicos propugnados por Valle de la Cerda, o incluso desde 1776, fecha en que se fundó el banco mas antiguo de España, el denominado Sobrinos de José Pastor, precursor del actual Banco Pastor. Desde entonces, un largo camino de fundaciones bancarias, encabezadas en 1856 por el Banco de España, en 1857 el Banco Mercantil de Santander, seguidos por un largo y conocido etcétera.

No había entonces base tecnológica que soportase o impulsase el desarrollo del negocio bancario, que se podía realizar sólo de forma manual, en volúmenes escasos y sobre actividades sencillas. Desde entonces hasta nuestros días, la historia de la banca ha tenido un desarrollo vertiginoso; los productos y servicios ofrecidos se han ido *complejizando* y *sofisticando*, hasta alcanzar en los albores del siglo XXI unos niveles de complejidad que solo es posible imaginarse al amparo de una vertiginosa evolución de lo que denominaremos las TIC (tecnologías de la información y comunicación).

Cabe por tanto afirmar, refiriéndonos al negocio bancario en su conjunto, que su evolución viene siendo paralela a la evolución tecnológica, y que lo que antes era un negocio de manejo de dinero, se ha convertido en los últimos tiempos en un negocio de gestión y proceso de información. No hace tanto tiempo, en los albores de la informática, su aplicación al negocio bancario se hacia con una perspectiva de soporte, de lo que se llamaba *mecanización* en busca de unas determinadas cotas de productividad, eficiencia o de reducción de costes; hoy la tecnología ha dejado de ser *soporte* para estar totalmente integrada en el negocio y ser el motor del mismo, indivisible, consustancial con él, hasta el punto de afirmar con rotundidad que no se puede hacer banca sin tecnología.

1 Director de Sistemas Informáticos de Bankinter.

Artículo publicado en el núm. 8 de la Colección Mediterráneo Económico: "Los restos de la industria bancaria en España"
ISBN: 84-95531-28-3 - Depósito Legal: AL-400-2005
Edita: Caja Rural Intermediterránea, Cajamar - Producido por: Instituto de Estudios Socioeconómicos de Cajamar

Para empezar a situar en su contexto este artículo me referiré al alma del negocio bancario, el *cliente*, ese ente caprichoso y voluble, sobre el que todo está basado en cualquiera de sus formas, sea particular, de bajo o alto nivel, o empresa , pequeña mediana grande o multinacional. Todos sin excepción se acercan a la banca para demandar un mundo de servicios que se reclaman disponibles 24 horas al día, 7 días a la semana, 365 días al año, y, naturalmente, desde cualquier lugar donde se encuentre el cliente: en el trabajo, en el coche, en el aeropuerto, en cualquier parte que uno pueda imaginar.

No voy a entrar en la diversidad de productos financieros ni en la complejidad de los mismos, pues describir cualquiera de ellos nos ocuparía mas espacio del que disponemos para este capítulo, aunque creo que a nadie se le escapa que la mayoría de ellos no era posible, siquiera imaginarlos, hace bien pocos años. El acceso a mercados de valores, de derivados, etc., permiten diseñar productos en los que el factor tiempo, medido en décimas de segundo, es determinante para el resultado de la operación, y eso es algo que sólo es realizable bajo el concepto de *tiempo real*, que requiere el uso intensivo de la tecnología, y concretado en grandes capacidades de proceso y unas redes de telecomunicación rápidas y fiables.

Para una mayor concreción voy a focalizar este capítulo en la relación banco-cliente y el papel que las TIC puede jugar en ella desde una doble perspectiva, como es el nivel de servicio prestado por la entidad y percibido por el cliente, así como los requerimientos tecnológicos de la entidad financiera para satisfacer la demanda. También analizaremos la evolución de la relación, medida por elementos diferenciales que ya no son los productos, pues la tecnología nos permite copiar cualquier idea en muy poco tiempo, sin embargo lo que no resulta tan copiable, lo único que realmente va a perdurar y va a conseguir diferenciar una oferta de otra es la *calidad de servicio*, conseguir que nuestra oferta este accesible para los clientes 24 horas al día 7 días a la semana, en la forma en que el cliente la necesite, y con procesos adaptados al canal.

Esta situación nos aboca a diversificar la oferta. Ya no tiene sentido una banca que sólo tenga oficinas; se impone llegar al cliente por múltiples canales para poder satisfacer sus necesidades. Dedicaremos una apartado de este capítulo a la multicanalidad, elemento fundamental en la banca de hoy que no podría ni imaginarse sin el concurso de una tecnología pujante.

Ante un universo tan heterogéneo de clientes, la primera condición que se nos viene a la mente es que no es posible sobrevivir en este negocio con una oferta universal de productos. Es preciso adaptar los productos a los clientes, para lo cual es necesario saber cuanto más mejor del cliente, saber de su actividad, de sus necesidades financieras, de sus hábitos de gasto, de su consumo, de su forma de vida, para poder anticiparse a sus necesidades y poderle hacer una oferta adecuada justo antes de que él sienta la necesidad, o, cuando menos, antes de que lo haga la competencia; y eso requiere:

1. Criterios organizativos claros que permitan la *segmentación* de los mismos en grupos homogéneos que nos permitan canalizarles la oferta más idónea mediante especialistas.

2. Formas de analizar mediante plataformas especificas de tratamientos masivos de datos, los datos del cliente para descubrir hábitos y comportamientos que permitan discriminar y preparar ofertas personalizadas. A estas plataformas denominadas comúnmente como *CRM* (*customer relationship management*) nos referiremos en este documento.

No pasaremos por alto un aspecto que me parece relevante para cuantificar de forma rotunda e inequívoca la importancia de la tecnología para una entidad financiera, como es la cantidad de dinero que dedica anualmente, en términos relativos, al desarrollo y mantenimiento de la plataforma tecnológica, que es sin duda relevante en el conjunto general de sus costes como después veremos.

Por último y por poner el contrapunto nos referiremos al lado oscuro de la evolución tecnológica a esos aspectos que pueden frenar la evolución y el desarrollo de un negocio como el bancario y que son los aspectos relacionados con la seguridad. La evolución tecnológica también llega a ladrones, estafadores y gentes de mal vivir permitiéndoles el desarrollo de virus, gusanos y demás clases de programas maliciosos, que si bien no resultan en general efectivos contra las instituciones bancarias, por disponer de importantes infraestructuras de seguridad, si pueden afectar a los clientes y las relaciones que ambos mantienen, por lo que nos referiremos a ellas a lo largo de este documento.

2. La arquitectura de aplicaciones

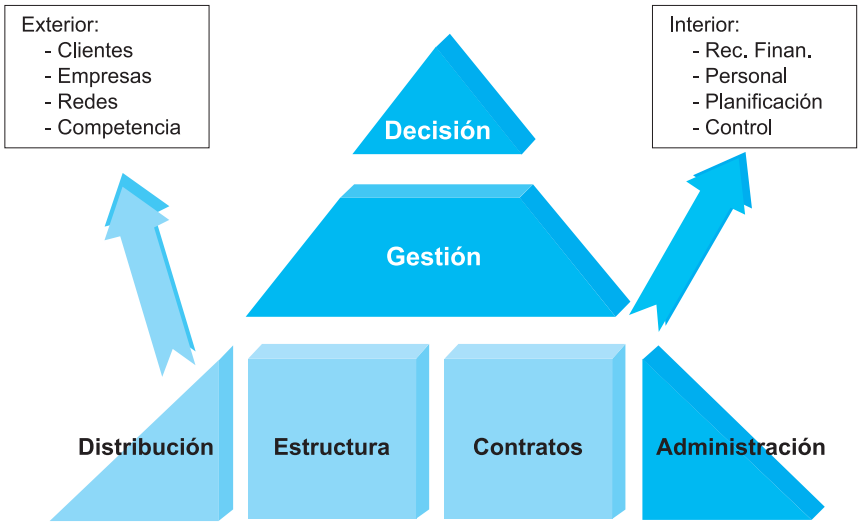
Estar preparado para afrontar el reto descrito pasa por disponer de unas plataformas tecnológicas adecuadas y de unas infraestructuras de telecomunicaciones en línea con la evolución que ambas vienen desarrollando año tras año, que están disponibles para todos y que son adquiribles en el mercado, aunque no profundizaremos en ellas pues hay ofertas para todos los gustos, y la elección de cualquiera de ellas estaría plenamente justificada, sin embargo, hay un factor estratégico y diferencias que son las que hacen que unas entidades puedan sacar mayor partido que otras a las inversiones que hacen en tecnología, algo que no se improvisa, que se puede comprar sólo a nivel conceptual, pero que su implantación en general es larga y compleja como es el disponer de una *arquitectura de aplicaciones* adecuada, soportada por un *modelo de datos* acorde a la misma.

¿Que es una *arquitectura de aplicaciones*? Para definir ese concepto debemos remontarnos al de *sistemas*. La tecnología aplicada a una industria como la financiera requiere

además de potentes ordenadores, complejas redes de telecomunicaciones, un conjunto de aplicaciones, que a su vez no son más que grupos especializados de programas de ordenador, los cuales recogen el conocimiento de todas las prácticas bancarias, de todas las relaciones entre los diferentes elementos que participan en el negocio, empezando por el cliente y terminando por el *regulador*, en nuestro caso el Banco de España o el Ministerio de Hacienda, entes que supervisan y controlan la práctica bancaria, definiendo los procedimientos, elementos de información y control necesarios para que ésta sea adecuada transparente y efectiva dentro de los niveles de riesgo correctos.

Pondremos un ejemplo de forma grafica para ilustrar este concepto:

Figura 1. Modelos procesos áreas básicas



Podríamos definir la *arquitectura de aplicaciones* de una entidad financiera como una pirámide a tres niveles, siempre haciendo abstracción, como ya he dicho, de la topología física de ordenadores que puedan soportarlo, y considerando que todos los bloques tienen *personalidad propia* pero deben a su vez de ser capaces de intercambiar contenidos con los integrantes del resto de la pirámide.

2.1. Nivel operativo

En la base, constituyendo el nivel que podríamos denominar operativo, se recogen las piezas básicas sobre las que descansa la arquitectura: nos encontraríamos con 4 áreas que trataremos de describir a continuación:

Area de distribución:

Incluye los elementos de SW necesarios para poder comunicarnos con el cliente a través de los diferentes canales por medio de los cuales el cliente y el banco puedan entrar en relación. Un buen diseño de este módulo permite a la entidad financiera ser realmente multicanal y ofrecer servicios a través de un canal nuevo en un breve espacio de tiempo y con un coste razonable, pues todo lo demás resulta igualmente valido y sólo requiere modificaciones en estas piezas de *software*.

Area de estructuras:

Construir *software* es una industria que requiere eficiencia, que requiere efectividad y garantía y estar totalmente seguro de que las cosas son como se quiere que sean. En la industria bancaria existen elementos de *software* que se utilizan en múltiples aplicaciones y para garantizar, además de la eficiencia en la gestión, que los procesos son siempre iguales; conviene aislarlos en un modulo que denominaremos soporte en el que se incluirán tratamientos contables, analíticos, liquidadores, etc.

Area de contratos:

No es difícil imaginar su contenido, pues debe recoger todos los programas de la entidad financiera en cuanto a productos y servicios. El catálogo de productos de la entidad convertido a *software*. Éste es el único elemento realmente especifico de una entidad financiera; todos los demás podrían, al menos en teoría, ser comunes.

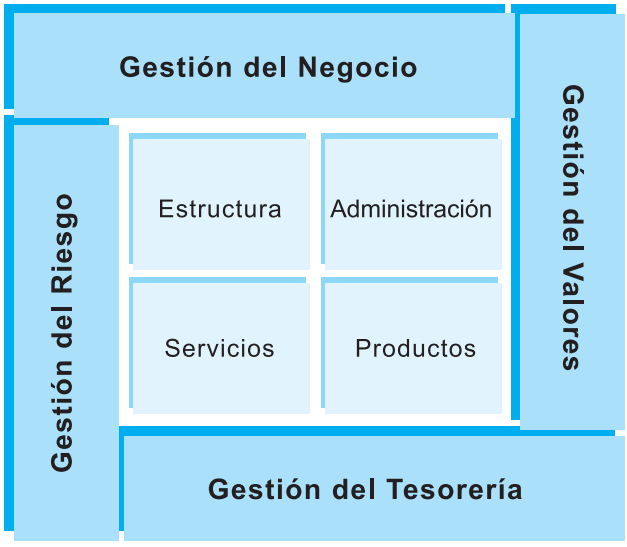
Área de administración:

Cualquier entidad financiera está obligada a hacer cuentas, a presentar resultados, a llevar unos libros y a rendir cuentas a entidades reguladoras o de control. Todo el *software* que de respuesta a estas necesidades podríamos incluirlo en este módulo.

2.2. Nivel de gestión

Situados sobre el nivel operativo, y formando un anillo que lo envuelve como se representa en el grafico siguiente, los sistemas de gestión toman la información producida a nivel operativo y la elaboran en cuatro bloques distintos:

Figura 2. Gestión de tesorería



Gestión de tesorería

Representa un área muy particular de los bancos, con una problemática muy especifica, y para cuya resolución, además de un *software* complejo y muy especializado, se requieren equipos especiales de integración de fuentes de información y la más sofisticada de las tecnologías de tratamiento de la misma.

Gestión del riesgo

En una entidad financiera el riesgo es la base del negocio. Anticiparse a una situación de morosidad o fallo y conceder los créditos dentro de los niveles de riesgo que el banco desee asumir en cada momento, así como el tratamiento automatizado de estos sistemas de sanción y alerta, tendrían su lugar en este modulo.

Gestión de ventas

Bajo este concepto integraremos en este módulo todo el *software* que nos habilite una relación adecuada en tiempo y forma con los clientes, permitiéndonos realizar la oferta adecuada en el momento adecuada y por el canal favorito del cliente.

Gestión del negocio

Operativa, administración, riesgos, etc. sobre todas estas áreas funcionales debemos situar, los elementos de *software* necesarios para gestionar el negocio, analizar rentabilidades,

éxitos o fracasos de la actividad de la entidad a nivel del cliente, producto o segmento. Éstos deben poder ser analizadas mediante las aplicaciones que a tal efecto seamos capaces de gestionar en este módulo.

2.3. Nivel decisión

Si disponemos de una buena base de información a nivel operativo, si éste está rodeado por una capa de gestión especializada y completa, cabe pensar que seremos capaces de preparar un conjunto de herramientas que ayuden a la cúpula directiva a tomar decisiones, y si es así los situaremos en este bloque.

2.4. Modelo de datos

Una buena arquitectura de aplicaciones debe ser complementada con un modelo de datos adecuado, que nos permita una visión única de la información. Cada dato debe ser único y debe tener definidos los caminos de actualización para poder garantizar la consistencia del mismo ocurra lo que ocurra, sea cual sea el camino por el cual se realiza, y naturalmente de forma transparente a su implantación en un conjunto de sistemas que, como ya hemos citado, pueden ser de diversa índole o condición; pero cumpliendo estos requisitos podemos garantizar que darán a la entidad financiera el nivel de soporte adecuado y le permitirá competir con garantías en un mercado cada vez mas difícil, proporcionando al cliente un acceso multicanal y de calidad a la entidad.

3. Multicanalidad y CRM

Ya nos hemos referido con anterioridad a estos conceptos, claves desde nuestro punto de vista en la relación cliente-entidad financiera y en el despliegue tecnológico que ésta debe realizar para satisfacer la demanda del primero.

Una vez entendido el porqué de una arquitectura de aplicaciones, no resulta difícil comprender estos conceptos. Si las aplicaciones son siempre las mismas, si los datos son únicos, la entidad financiera puede afrontar con garantías un planteamiento de negocio en el cual, el cliente, en la medida en la que sea capaz de acercarse a las TIC, puede utilizar los servicios bancarios en cualquier momento o lugar y en la forma que más le conviene.

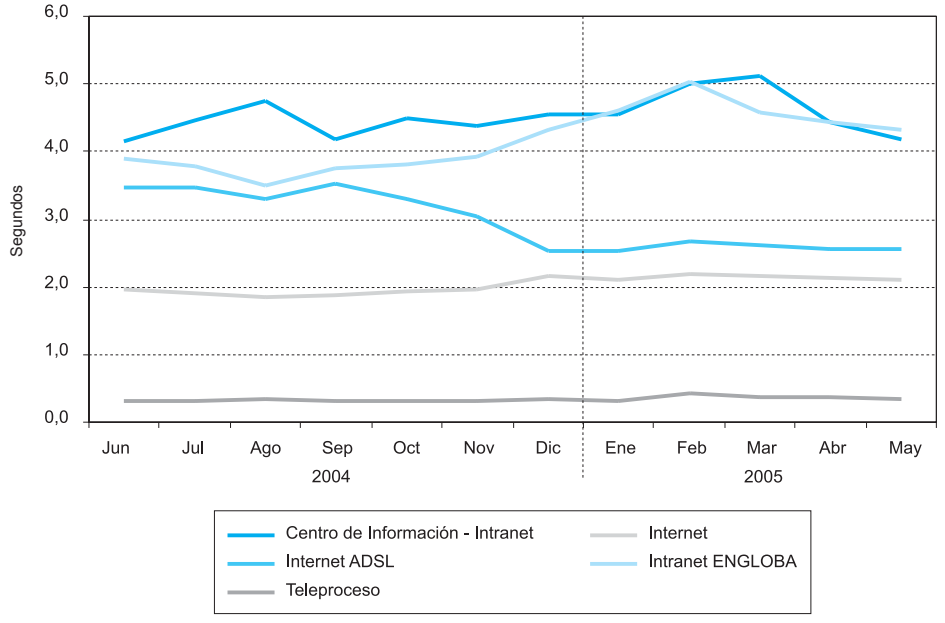
Para el banco que tenga una buena arquitectura como la definida, la preparación de las infraestructuras no debe constituir una grave dificultad técnica ya que sólo debe preocuparse de adecuar en cada caso la *interfaz* y el tipo de diálogo a las características del dispositivo que haya que usar en cada momento, ya que no es igual utilizar un teléfono convencional, un ordenador personal, un teléfono móvil o una combinación de cualquiera de ellos, en lo que se viene a denominar comunicaciones multimodales, y que no son sino la mezcla de los diferentes canales en una misma iteración cliente-entidad financiera aprovechando los últimos adelantos tecnológicos.

Calidad de Servicio

Es, sin duda, el elemento diferencial entre las entidades financieras y el único que marca realmente las diferencias.

Una vigilancia constante y precisa de los niveles de servicio prestados por la entidad en cada uno de sus canales o redes, y concretada en elementos objetivos como tiempos de respuesta o disponibilidad de los servicios, nos permitirá gestionar mejor al cliente, en línea con sus expectativas que pueden ser *pulsadas* periódicamente con encuestas.

Gráfico 1. Evolución Calidad de los Servicios



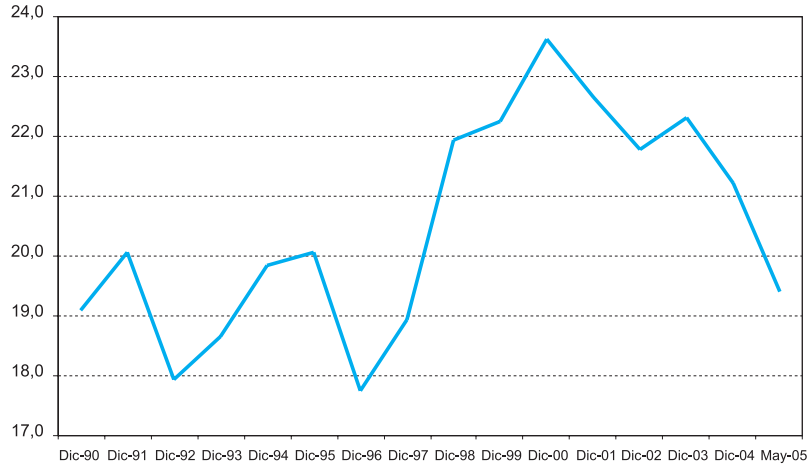
3.1. CRM

Una vez que disponemos de una adecuada plataforma, de una buena arquitectura de aplicaciones y de una estructura multicanal, ya sólo nos falta una cosa para llegar al éxito: vender, ser capaz de ofrecer al cliente el producto que necesita en tiempo y forma y eso sólo lo podemos conseguir una vez más, mediante una nueva aplicación de las TIC, lo que podríamos denominar CRM o gestor de relaciones con clientes. De acuerdo a la arquitectura de aplicaciones descrita, disponemos de muchísima información de la vida de nuestros clientes a través de sus domiciliaciones y del uso que hacen de sus tarjetas de crédito, o de los pagos de impuestos que realizan a través nuestro; podemos tener idea de sus hábitos de consumo, sus necesidades y su nivel de renta. Con todo ello, y la potencia de simulación de las TIC, no es difícil generar algoritmos que nos permitan hacer la mejor oferta en el momento adecuado, con una razonable probabilidad de éxito. Esto es el CRM y se constituye en una tremenda herramienta de ayuda a la *población comercial*.

4. Impacto económico de las TIC en la banca

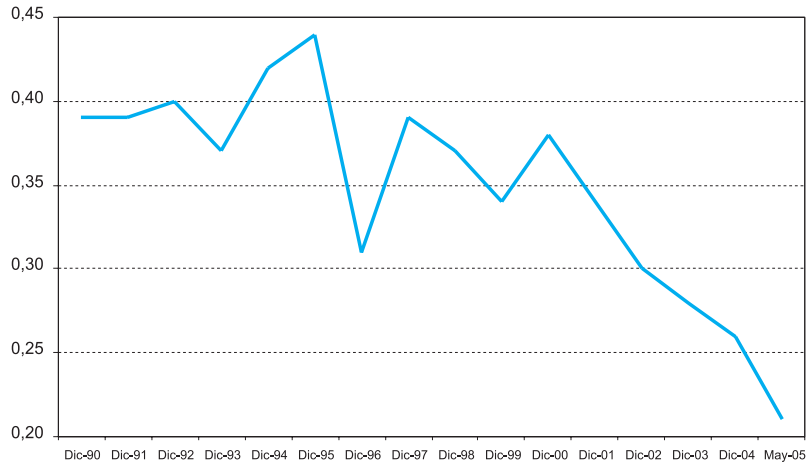
No se puede dogmatizar, ya que depende mucho del tipo de entidad, pero, por poner en magnitud, utilizaremos los datos de una entidad media como Bankinter, y lo haremos mostrando la evolución de este gasto en relación con los activos totales medios o los costes de transformación del banco tal como muestran los gráficos.

Gráfico 2. Evolución porcentual
Gastos informáticos / Costes de transformación



Fuente: Cuenta de resultados según CNMV.

Gráfico 3. Evolución porcentual
Gastos informáticos / Activos Totales Medios



Fuente: Cuenta de resultados según CNMV.

Estos datos varían mucho como decíamos en relación con le tamaño de la entidad, aunque la media del sector está en algo mas del 50% de los datos reflejados, lo que indica la erraticidad del mismo.

5. Seguridad de la Información en los Procesos de Negocio Financiero

Tras todo lo hablado, no podemos olvidarnos del lado oscuro. Qué impacto puede originar en la actividad financiera el paralelo avance al desarrollo de las TIC, el avance sin freno del desarrollo de *software* malicioso que puede atentar contra la confidencialidad de la información y contra la propia *integridad* de la misma. Es por esto que podemos encontrar en el Reglamento 460/2004 de la Unión Europea, referente a la creación de la Agencia Europea de Seguridad de las Redes y de la Información (ENISA -European Network and Information Security Agency), la siguiente introducción:

> *"…las redes de comunicaciones y los sistemas de información se han convertido en un factor esencial del desarrollo económico y social. La informática y las redes se están convirtiendo en recursos omnipresentes, tal y como ha ocurrido con el suministro de agua y electricidad. Por consiguiente, la seguridad de las redes de comunicación y de los sistemas de información y en particular su disponibilidad, es un asunto que preocupa cada vez más a la sociedad."*

Esta declaración, siendo importante por constituir uno de los fundamentos de la creación de esta Agencia Europea de Seguridad, no es otra cosa que plasmar por escrito lo que constituye una realidad fácilmente constatable en la vida ordinaria.

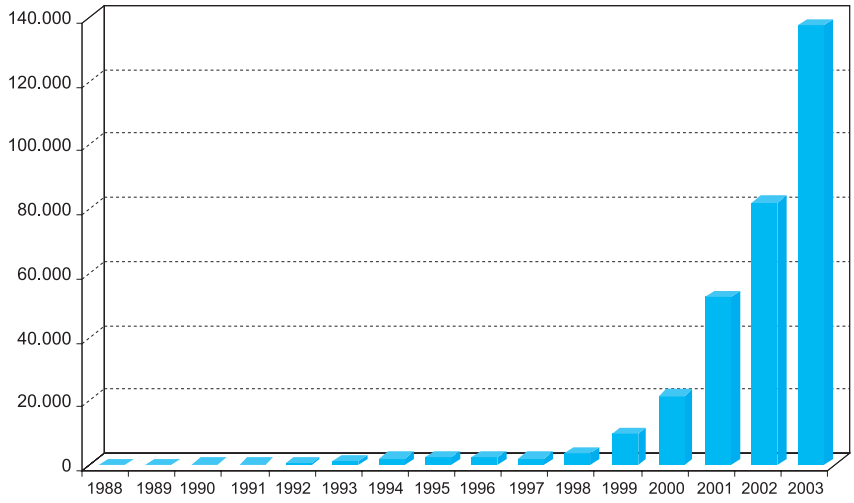
La seguridad de los procesos que son definidos como esenciales para la vida económica debería ser una obviedad inseparable. Su propia condición de *esenciales* ha de llevar implícitas unas garantías de funcionamiento, tanto en lo que se refiere a su explotación exenta de riesgos, como a la ausencia de debilidades en su funcionamiento que dejen estos suministros en manos de la posible mala intención de terceros, como, muy especialmente, garantías sobre su continuidad de funcionamiento. Continuando con el símil que propone la Agencia Europea, sería inconcebible un suministro de agua que no tuviera implícitas, por definición, garantías de salubridad, o un servicio de electricidad que no pudiera garantizar un funcionamiento ordinario sin sobrecargas.

Este funcionamiento seguro lleva implícita la necesidad de que las condiciones de seguridad estén fuertemente *embebidas* en todo el conjunto de procesos de generación de los suministros. No pueden ser un añadido posterior ni estar sujetas a variabilidad por factores externos, sino que deben constituirse en una parte fundamental e inseparable del proceso. En las TIC esto no ha sido así históricamente, de modo que podríamos afirmar que el reconocimiento de la importancia de la seguridad en estos procesos es un hecho relativamente reciente (como puede indicar, sin ir más lejos, el hecho de que la creación de la Agencia Europea que estamos utilizando como ejemplo date de 2004).

El desarrollo y la implementación de la seguridad en las TIC tiene una clara correlación con el creciente número de incidentes y problemas detectados, que ponen de manifiesto la existencia de debilidades. El impacto de los incidentes y problemas de seguridad aumenta también cualitativamente en la misma medida que crecen las expectativas de funcionamiento y prestaciones de las TIC. Nuestra vida ordinaria y nuestras actividades profesionales están cada vez más condicionadas por hechos que consideramos naturales: que un dato sea recogido correctamente, que un correo electrónico llegue a su destino, que una fuente de datos esté accesible, que nuestros medios de trabajo funcionen. Estos hechos, lejos de ser naturales, son en realidad un cúmulo de sincronismos entre dispositivos que han de funcionar siempre perfectamente para que las cosas ocurran y sobre los que cada día existen más y mayores amenazas.

El CERT (Computer Emergency Response Team) publica una serie de estadísticas que nos pueden ilustrar sobre el incremente en el número de incidentes de seguridad en los últimos años [http://www.cert.org/stats/cert_stats.html].

Gráfico 4. Incidentes reportados por el CERT



La Seguridad de la Información es la disciplina que, dentro del área TIC, se ocupa de la gestión de los riesgos dentro de los sistemas informáticos y aporta las respuestas adecuadas, tanto tecnológicas como organizativas y de procedimientos, para hacer frente a las amenazas.

5.1. El contexto general de la Seguridad de la Información

Ninguna medida de seguridad tiene significado en sí misma si no es valorada en el contexto de las amenazas a que intenta dar una respuesta. Así, por ejemplo, si observamos una medida de seguridad concreta: "cerrar la funda de nuestro portátil con un candado", no cabe pensar que esta medida sea apropiada frente a una amenaza de robo, puesto que nada impide que sea robado con funda y todo, o, simplemente, rajando la cubierta. Sí podría ser, por el contrario, una medida adecuada y suficiente si únicamente se pretendiera evitar que algún compañero accediera al portátil. Para conseguir el objetivo de que "ningún ladrón robará mi portátil" posiblemente habría que llegar a usar unas esposas, que aseguraran que estamos en todo momento en contacto directo con él, incluso ante situaciones como tomar un café o ir al baño. Evidentemente, incluso las esposas serán insuficientes si el planteamiento fuera "ningún asesino profesional robará mi portátil". Para protegerse frente al crimen organizado o frente a una potencia extranjera, probablemente habrá que recurrir a un furgón blindado custodiado por guardas armados.

Cualquier medida de seguridad deberá emplearse, por tanto, en un contexto determinado y sólo será válida frente a unas determinadas expectativas. Tan ridículo sería usar el furgón blindado para proteger el portátil de la secretaria, como utilizar un candado si la amenaza proviene de una banda armada. Si el objetivo fuera: "nadie accederá a la información de mi

portátil", en ese caso la medida más apropiada sería el cifrado del disco, ya que aunque el portátil fuera robado, no se conseguiría acceder a la información.

El desarrollo e implantación de medidas de seguridad informática ha de ser, por consiguiente, un continuo ejercicio de gestión del riesgo, de modo que en cada posible situación de amenaza se diseñe y ponga en marcha un conjunto de medidas adecuadas, tanto en razón a su eficacia, como su coste, complejidad, gastos de mantenimiento, facilidad de uso, etc.

5.2. El contexto en el mundo financiero

La creciente relevancia de las TIC en el desarrollo económico tiene uno de sus principales fundamentos en que tales actividades son susceptibles de ser representadas de forma abstracta por información, de tal manera que la gestión de la actividad se enfoca directamente sobre esa representación. Aparece, por consiguiente, una nueva clase de activos a considerar en la empresa -activos de información- cuyo mantenimiento, conservación y adecuación puede resultar tan relevante como cualquier otro aspecto tangible de la actividad. De la misma manera que los edificios, las mercancías, los vehículos, la maquinaria, etc. requieren de procedimientos adecuados que aminoren los riesgos a que puedan estar expuestos, con igual o más intensidad lo deben estar los citados activos de información, que, al constituirse en el corazón de la gestión, pueden condicionar la continuidad general de la propia empresa.

En el contexto financiero, este punto toma especial relevancia ya que los activos de información dejan de ser únicamente una *representación* de la realidad, pasando a ser, en una gran parte de la actividad, la única realidad existente. A nivel general, el flujo financiero ha ido cambiando de forma progresiva e imparable, de modo que las representaciones físicas de los bienes han ido desapareciendo y convirtiéndose en pura información almacenada; a lo largo de los últimos años hemos visto cómo desaparecían del mundo físico la mayoría de las representaciones de propiedad de activos financieros. Así, por ejemplo, los tradicionales certificados de posesión de una participación en una empresa, las *acciones*, han dejado de ser elementos físicos para convertirse en meras anotaciones en cuenta. Aparte de transacciones de gran relevancia, en las que no existe trasiego de dinero físico, incluso el mundo ordinario del consumo ha ido cambiando progresivamente de forma que nuestras compras se realizan por puros adeudos informáticos, mediante sistemas de interconexión entre comercios y bancos. Esta evolución, en la que sin duda aún hemos de ver avances notables, no debería extrañarnos si reparamos que el mismo dinero que tendemos a considerar *físico* no es tal, ya que hace siglos que hemos sustituido un verdadero valor de intercambio por una mera representación en papel, a la que convencionalmente todos atribuimos un valor que en realidad no va más allá de la información que representa. Mientras mantuvimos nuestra tradicional peseta, los billetes informaban de que "El Banco de España pagará al portador…", lo que es la más pura expresión de un soporte que no tiene más contenido real que la información que muestra.

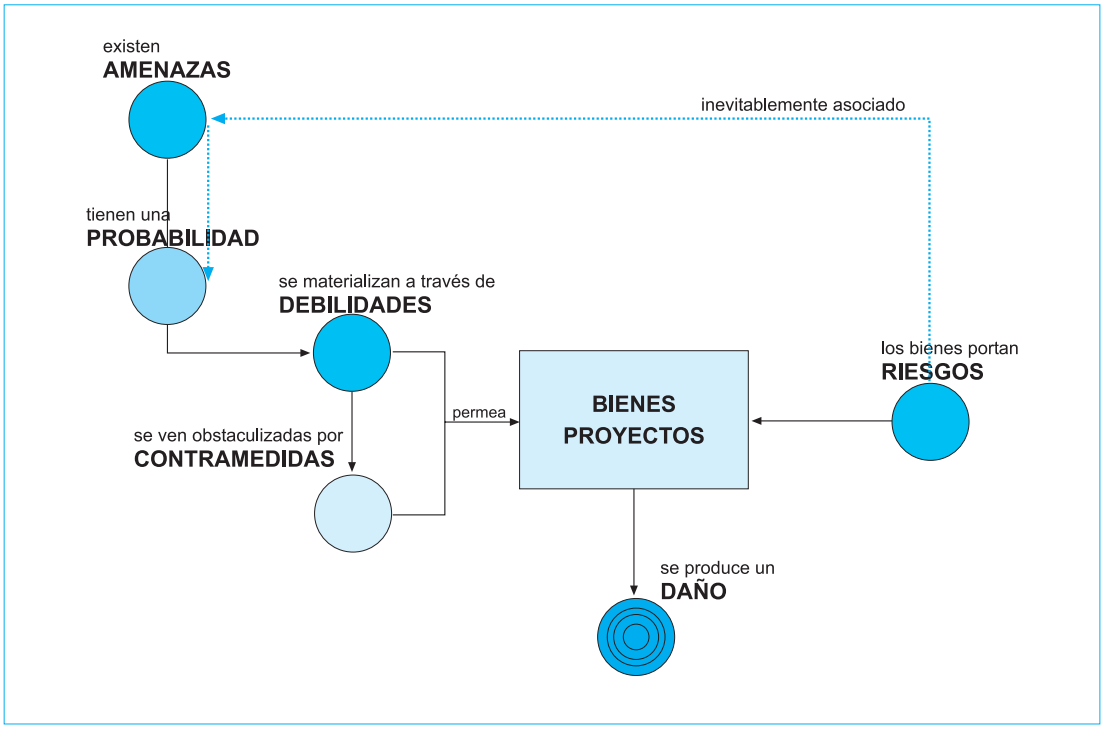
En este contexto, en el que los activos de información son los únicos y verdaderos activos que se manejan, está claro que las tecnologías que se ocupan de su tratamiento, las TIC, son un aspecto tan fundamental como lo podrían ser los hornos de fundición en una siderurgia. La seguridad de tales tecnologías, que son la esencia del negocio, pasa por tanto a adquirir una importancia *dramática*.

Otro aspecto a considerar, dentro del mundo de la banca y las finanzas, es el verdadero motor que subyace en su propia existencia, que no es otro que la confianza. De hecho podríamos llegar a afirmar que todo el entramado económico a nivel mundial está basado casi exclusivamente en la existencia de unas grandes cantidades de confianza, desde el mismo momento en que el principal instrumento de intercambio, el dinero, no es más que una promesa a futuro, es decir, una información. La persistencia de la confianza y su continua renovación es un mecanismo natural, es decir, no necesita ser estimulada de forma artificial. Dado que, por ejemplo, lo único que hace moverse la bolsa es la confianza implícita de que mañana también va a haber bolsa, no es algo que requiera ser reafirmado. Simplemente se da por sobreentendido. No obstante, sí que resulta relativamente sencillo erosionar esa confianza en modo local y limitado, es decir, que solamente afecte a un determinado individuo o empresa. Indudablemente también se dan casos de pérdida de confianza a nivel de país, o incluso región, pero su dimensión hace que el problema adquiera más tintes políticos que meramente prácticos y por tanto salen del ámbito de estos comentarios. La confianza en la banca tiene que ser preservada en base a que no existan episodios que la pongan en duda. Tal como decimos, no es necesario que un banco demuestre cada día que es digno de confianza, pero sí puede llegar a ser vital que no le ocurran cosas que la pongan en peligro. Esta desconfianza de dimensión local, cuando ocurre, puede tener consecuencias catastróficas, dado que su propagación y efectos tienen un *tamaño crítico* de forma que, cuando se supera, deja de ser importante el que existan causas verdaderas y objetivas. Basta con que una ola de desconfianza se reparta adecuadamente para que se produzca la conocida paradoja de la *profecía autocumplida*, es decir, la información sobre la existencia de una crisis, aunque sea mentira, es capaz por sí misma de desencadenar tal crisis.

En el mundo financiero y de la banca, por consiguiente, la Seguridad de la Información es un aspecto vital de la continuidad de la empresa; y la ausencia de incidentes que pudieran comprometer esa imagen de seguridad, pasa a tener una dimensión varios órdenes de magnitud superior que en otras actividades más convencionales en este sentido. Por consiguiente, la relevancia, inversión y atención que han de tener los temas de seguridad-TIC tendrán que estar de acuerdo con estos principios y no pueden ser considerados en ningún momento una actividad de segundo orden.

5.3. La gestión de la seguridad

La determinación de las medidas adecuadas de seguridad en cualquier entorno y negocio ha de ser un proceso racional, de tal forma que se puedan tener en cuenta los riesgos, su posible impacto y el coste de aminoración. En ningún caso se puede asumir que el objetivo sea una eliminación de los riesgos al 100%, sino reducir el riesgo a niveles aceptables. Este proceso de análisis de riesgos puede tener muchas formas de realización, desde las más formalistas y completas, que se basan en un análisis exhaustivo en el seno de la empresa de todos los procesos, activos, etc., dejando posteriormente una extensa documentación sobre todo ello; o bien análisis más parciales, más guiados por el conocimiento previo y la determinación de lo realmente relevante, que, si bien no dejan posteriormente el mismo nivel de evidencias de su consecución, suelen conducir más rápidamente al logro de soluciones prácticas. En cualquier caso, el procedimiento a seguir, ya sea completo y riguroso, ya sea más basado en una actuación por excepción, ha de tener siempre los mismos principios.



Básicamente podemos afirmar que los activos, sea cual sea su materialización concreta (bienes, información, proyectos…) pueden llevar en sí mismos una serie de *riesgos* asociados, o pueden estar sujetos a determinadas *amenazas*, genéricas o específicas para el bien de que se trate. El objetivo fundamental del análisis, y por tanto de las medidas de seguridad que finalmente se han de adoptar, es evitar que el *daño* se materialice. Para ello se deberán tener en cuenta las *probabilidades* de que las *amenazas* tomen cuerpo, la posible existencia de *debilidades* en el sistema bajo análisis que provoquen un aumento en la posibilidad de ocurrencia, y, por lo tanto, deben ser evitadas, y las posibles *contramedidas* que aminoren la *amenaza* o las consecuencias de su materialización.

El equilibrio adecuado entre estos factores, y, por supuesto, un enfoque realista y ceñido a los aspectos realmente prácticos y relevantes en cada caso, es lo que conducirá al diseño de sistemas y procedimientos de seguridad adecuados, tanto en eficacia como en el coste que representen.

5.4. El análisis de riesgos (de seguridad) como condicionante de negocio

En un entorno de TIC, en el que una de las actividades más importantes es la resolución de demandas de negocio, y cuya materialización en *sistemas* o *aplicaciones* termina con frecuencia constituyéndose en el negocio en sí mismo, la valoración de riesgos y el diseño de medidas no puede ser una actividad posterior al diseño, ni puede estar condicionada por completo por los requerimientos de negocio.

La evolución de la banca y finanzas en el uso de TIC en los últimos decenios ha caminado hacia un uso intensivo de las capacidades de interconexión y servicios a distancia, aspectos que han tomado una dimensión mucho más extensa y popular a medida que las redes de intercomunicación han ido quedando al alcance de una gran masa de público a través de Internet. Lo que hace unos quince o veinte años ya constituía un avance notable en el uso de redes para intercambio de transacciones financieras entre bancos, como puede ser la red *Swift* o el sistema de compensación interbancario, alcanza hoy en día una dimensión totalmente popularizada en el mundo de la banca por Internet, o el incipiente mundo del móvil.

Estos cambios suponen un aumento notable de los riesgos en los procesos TIC. Nada tiene que ver, en una valoración de amenazas, la situación que vivíamos en los años 80, en donde disponíamos de un único ordenador, sin conexiones externas, altamente protegido físicamente y con un muy escaso personal suficientemente conocedor de sus interioridades, con la situación actual, en la que un funcionamiento ordinario orientado a resolver transacciones *on-line* exige la presencia de centenares de ordenadores, cada uno de ellos con sus peculiaridades, vulnerabilidades y amenazas; todo el mundo conectado con todo el mundo a través de una red pública en la que tenemos la certeza de que existen elementos dispuestos a provocar

daños, en ocasiones por el simple placer intelectual de conseguirlo, y, últimamente, y cada vez con más claridad, con el objetivo de conseguir beneficios económicos.

En este entorno que a priori ha de considerarse *potencialmente hostil* en el más frío de los análisis, la puesta en marcha de nuevas iniciativas de negocio no puede estar al margen de un análisis de riesgos, y, probablemente, deba de buscarse un equilibrio entre las potenciales funcionalidades, la comodidad en su uso y los nuevos riesgos a que podrían estar sometidos esos nuevos negocios.

Por otra parte, como la realidad demuestra de forma recalcitrante, y recordando lo ya comentado en cuanto a la *confianza*, la generalidad del público siempre se resistirá a aceptar nuevas formas de relación y negocio que no perciba como seguras. A la dificultad natural de necesidad de adaptarse a un nuevo medio, que en sí mismo puede ser un obstáculo nada despreciable, no se puede añadir una percepción de inseguridad. Sencillamente, el público no aceptará ese nuevo medio o tecnología y le dará la espalda. El que se pueda llegar a determinar la verdadera causa, y que ésta quede establecida precisamente en *la falta de seguridad*, no es algo que se alcance fácilmente; para el mismo usuario resulta en ocasiones difícil que identifique qué es lo que le frena o le impide aficionarse a una determinada forma de hacer.

La sensación de seguridad, al ser precisamente una *sensación*, puede incluso no estar ligada necesariamente a la seguridad real. Con mucha frecuencia los usuarios más habituales son perfectamente desconocedores de los entramados, protocolos y sistemas internos de los que hacen uso, motivo por el que suele tener poca eficacia poner el acento en su excelencia. Los criterios de un usuario común son, por lo general, tan sencillos como sus propias expectativas, lo que obliga a que, para destacar un aspecto de seguridad de un sistema, las explicaciones y argumentarios deban huir de complicaciones técnicas. Ahora bien, esto, aparentemente más sencillo que tener que descender a profundas disquisiciones, hace el problema increíblemente más complejo de resolver. El usuario no quiere saber si utilizamos un cifrado simétrico de 128 bits, sino que quiere que se le responda a una pregunta mucho más simple ¿esto es seguro?, ¿sí o no?

Responder a esa pregunta es un ejercicio en sí mismo que puede llevar a absolutas y tremendas complicaciones. Algunas de ellas sólo pueden ser resueltas si esta conciencia se ha tenido clara desde el mismo nacimiento del proyecto, y, en todo caso, si se ha conseguido que los condicionantes de negocio, de *usabilidad*, o de *comodidad*, no han provocado que los proyectos lleven implícitos riesgos de difícil aminoración. La seguridad de las TIC, por consiguiente, han de ser un elemento esencial en el diseño de nuevos negocios, especialmente en los que tales tecnologías tienen un uso masivo y principal. La presencia de los criterios de seguridad tendrán, en una mayoría de casos, la apariencia de obstáculos o aminoraciones de la posible comodidad, pero, en caso de no ser resueltos satisfactoriamente, sencillamente los proyectos serán finalmente rechazados por el público.

6. Conclusión final

Creo que tras lo expuesto se puede concluir que:

- Las TIC no sólo son necesarias para la realización del negocio bancario, sino que sin ellas no es posible hacer banca ya que este es un negocio que ha mutado convirtiéndose en un negocio de tratamiento de información mas allá del tratamiento de dinero.

- Para poder realizar una gestión efectiva de las TIC es necesario disponer de una *arquitectura de aplicaciones* soportada en un modelo de datos único.

- La *calidad de servicio* es al único aspecto no copiable que permite diferenciar a una entidad de otra.

- Disponer de una tecnología adecuada requiere de políticas de desarrollo de las TIC de forma continuada, con significativas inversiones a lo largo del tiempo.

- La seguridad de la información es tan importante como la del propio dinero y puede condicionar la viabilidad de los negocios que utilicen tecnología de forma intensiva.