EL RIESGO EN LA BANCA ELECTRÓNICA

Feria Domínguez, José Manuel.
Universidad Pablo de Olavide.
Samaniego Medina, Reyes.
Universidad de Sevilla.

Actualmente, la industria bancaria está realizando un gran esfuerzo por conquistar nuevos segmentos de mercado. Dicha situación se encuentra favorecida por los rápidos cambios producidos en el sistema tecnológico (Internet) así como por la globalización de la banca. En este sentido, la banca electrónica se considera una nueva unidad estratégica de negocio dentro de la banca tradicional.

En este trabajo, presentamos los principales riesgos que pueden afectar a las operaciones de banca electrónica, así como la propuesta recientemente emitida por el Comité de Supervisión Bancaria de Basilea para la gestión de tales riesgos.

Nowadays, bank industry is making a big effort in order to take over new market segments. This situation is promoted by rapid changes in the technological system (Internet), as well as the globalization of banking. In that sense, electronic bank is performed as a new strategic business within traditional industry.

In this paper, we present the main risks that could influence electronic bank transactions and the proposal recently issued by the Basle Committee on Banking Supervision in order to manage those risks.

PALABRAS CLAVES: Banca electrónica, riesgo operacional, riesgo reputacional, riesgo legal, valoración del riesgo, gestión del riesgo.
KEYWORDS: Electronic bank, operational risk, reputational risk, legal risk, risk assessment, risk management.

1. INTRODUCCIÓN

Las nuevas tecnologías de la comunicación están incidiendo significativamente en el desarrollo del comercio electrónico, lo cual se traduce en nuevas oportunidades de mercado para el negocio bancario. Buena prueba de ello lo constituye el despegue experimentado por la *banca electrónica*, que hoy en día, ha desplazado los servicios bancarios tradicionales para ofrecer nuevos productos más competitivos y adecuados a las necesidades de los clientes, además de reducir los costes operacionales, aumentado la eficiencia en la gestión y reduciendo los costes de transacción, nacionales e internacionales. Todo ello repercute, sin duda, en un aumento de la productividad y en el bienestar económico en general.

Los comerciantes y particulares han visto incrementada la eficiencia a la hora de mantener relaciones con su banco, disfrutando de una mutua conveniencia. Aún más, la *banca electrónica* ha facilitado el acceso al sistema financiero de los consumidores que, previamente, lo tenían restringido.

El ámbito de este informe se limita a dos aspectos fundamentales:

1. La definición de riesgos exclusivamente bancarios, a pesar de que muchos de ellos pueden afectar tanto a bancos como a emisores no bancarios y proveedores.
2. La gestión del riesgo de la banca electrónica desde una perspectiva de supervisión bancaria.

1.1. Propósito y Organización

El desarrollo de la banca electrónica es algo difícil de pronosticar habida cuenta del grado de incertidumbre existente sobre el futuro tecnológico. A pesar de ello, una reciente encuesta realizada por la Boston Consulting Group señala que la red actual de oficinas bancarias perderá peso en la próxima década en beneficio de los nuevos canales de distribución (banca electrónica, banca telefónica, cajeros automáticos...)

Por su parte, el *Comité de Supervisión Bancaria de Basilea* reconoce que, aparte de los beneficios que indiscutiblemente estas tecnologías proporcionan, existen riesgos obvios para las organizaciones bancarias, y tales riesgos deben ser confrontados con los beneficios. Es por ello por lo

que dicha entidad se encuentra trabajando en el diseño de directrices que puedan ser adoptadas por los organismos de supervisión bancaria dentro del negocio electrónico.

No obstante, es difícil identificar y medir la totalidad de los riesgos asociados a la banca electrónica, ya que su desarrollo está estrechamente vinculado a los avances tecnológicos y a su continua evolución.

Las autoridades competentes deberían animar a los bancos que operan en este segmento a desarrollar procesos de gestión de riesgos que fuesen rigurosos con los riesgos materiales conocidos y suficientemente flexibles para incorporar los cambios necesarios en aquellos riesgos asociados a la banca electrónica. Por consiguiente, el proceso de gestión de riesgos sólo puede ser efectivo si se encuentra en constante evolución.

A medida que la banca electrónica progresa, las interacciones entre los bancos y sus clientes, más allá de las fronteras nacionales, aumentan y dicha relación también es fuente de riesgo.

1.2 Definiciones

La *banca electrónica* puede definirse como el conjunto de productos y procesos que permiten, mediante procedimientos informáticos, que el cliente pueda realizar una serie, cada vez más amplia, de transacciones bancarias sin necesidad de ir a la sucursal[34].

La incorporación de Internet a la banca proporciona una serie de ventajas entre las que destacan:

- La entrada en una nueva unidad estratégica de negocio que ofrece un alto potencial de crecimiento aunque también requiere de fuertes inversiones.
- La reducción de costes de transacción (una transacción realizada vía Internet puede costar a un banco un 1% de lo que vale en la sucursal).
- El acceso a la información general del banco (marketing directo).
- La adecuación de los productos y servicios bancarios a las nuevas necesidades de los clientes, lo cual redunda en su fidelización.

Dos aspectos fundamentales que debemos resaltar en la banca electrónica son, por un lado, la naturaleza del canal a través del cual las actividades se realizan y, por otro, los medios de acceso a dichos canales. Los canales de suministro comunes incluyen tanto a las redes abiertas, como Internet, como a las cerradas (redes locales privadas). La diferencia entre ambas estriba en que éstas últimas restringen el acceso a los participantes (instituciones financieras, consumidores, comerciantes y terceros) en los términos recogidos en el acuerdo, mientras que en las abiertas tales requerimientos de participación no existen.

2. IDENTIFICACION Y ANALISIS DE LOS RIESGOS

Debido a los rápidos cambios en las tecnologías de la información, la lista de riesgos que afectan a la banca electrónica no puede ser exhaustiva. La intención en este documento es describir un grupo de riesgos lo suficientemente significativo como para diseñar una guía general que sirva de apoyo a la gestión de lo mismos.

Hay que advertir que los tipos básicos de riesgo generados en la banca electrónica no son nuevos; la novedad estriba en la forma específica bajo la cual estos riesgos surgen, así como la magnitud de su impacto.

En este sentido, las categorías de riesgo más importantes para la banca electrónica, especialmente para la banca internacional diversificada son:

- riesgo operacional
- riesgo reputacional
- riesgo legal.

[34] (TAMANES, R. y S. GALLEGO. Diccionario de Economía y Finanzas. Alianza Editorial. Madrid, 1994).

2.1. Riesgo Operacional

Este riesgo tiene su justificación en la pérdida potencial derivada de deficiencias significativas en la integridad o confianza del sistema. Las consideraciones de seguridad son importantes, en la medida en que los bancos pueden ser sujetos de ataques externos o internos sobre sus sistemas o productos. El riesgo operacional puede también surgir de un mal uso del cliente, de un diseño inadecuado o de un sistema de banca electrónica mal implantado.

2.1.1. El riesgo de seguridad

El riesgo operacional se encuentra en estrecha relación con el control sobre el acceso a los sistemas de gestión de riesgo y a la contabilidad de un banco. Este control de acceso a los sistemas bancarios se ha convertido en algo tremendamente complejo debido a los avances informáticos, a la dispersión geográfica de los puntos de acceso, y al uso de vías alternativas de comunicación, incluyendo las redes públicas como Internet. A pesar de que la banca en Internet se encuentra implantada en España, sin embargo, la seguridad constituye una de las barreras de entrada para los clientes potenciales. El usuario aún no confía en las medidas de seguridad existentes como por ejemplo la encriptación de datos, aunque todo es cuestión de tiempo y de acostumbrar a los clientes a estos canales de distribución.

Lo cierto es que los accesos no autorizados, ya sean realizados por piratas informáticos (hackers) o por empleados del banco (insiders), pueden dar lugar a pérdidas directas debido al uso y manipulación de información confidencial del cliente. Por esta razón es preciso diseñar sistemas que aseguren la confidencialidad e integridad de cualquier transacción y garanticen la privacidad de la información.

2.1.2 Diseño de sistema. Aplicación y mantenimiento.

Un banco afronta el riesgo de que el sistema por él elegido no se encuentre bien diseñado o implantado. Por ejemplo, un banco está expuesto al riesgo de una interrupción de su sistema de banca electrónica si éste no es compatible o no satisface los requerimientos de sus usuarios.

Muchos bancos delegan en suministradores de servicios externos y expertos *(outsourcing)* la operativa y el mantenimiento de sus actividades de banca electrónica. Esta delegación puede ser conveniente porque permite al banco desprenderse de aspectos que no puede suministrar de forma eficiente por sí mismo. Sin embargo, el *outsourcing* expone al banco al riesgo operacional, en la medida en que los proveedores de servicios pudieran no estar tecnológicamente preparados para prestar los servicios esperados, o fallar en la actualización de su tecnología. Si esto ocurriera la reputación bancaria se vería seriamente dañada.

Hay que añadir que, debido a los rápidos cambios que caracterizan la tecnología de la información, los bancos se enfrentan también al riesgo de obsolescencia de su sistema. Por ejemplo, el software empleado por la banca electrónica requiere de una actualización constante, pero los canales de distribución de las actualizaciones de software plantean problemas de seguridad para los bancos, ya que pudieran ser interceptados y manipulados. Además, no debemos olvidar una dificultad añadida que estriba en la continua asimilación de las nuevas tecnologías por el banco y su personal.

2.1.3 El mal uso de los productos y servicios por el cliente.

Los malos usos del cliente, tanto intencionados como inadvertidos constituyen otra de las fuentes de riesgo operacional. El riesgo puede ser mayor si el banco no "educa" adecuadamente a sus clientes, sobre las precauciones de seguridad. Además, en ausencia de medidas adecuadas para verificar las transacciones, los clientes podrían anular operaciones que previamente autorizaron, dando lugar a importantes pérdidas financieras para el banco.

El uso personal de información del cliente (como por ejemplo la verificación de información, número de las tarjetas de crédito, número de las cuentas bancarias, etc.) en una transmisión electrónica carente de seguridad permitiría a un experto tener acceso directo a las cuentas de los clientes. Consecuentemente, el banco podría incurrir en pérdidas financieras debido a transacciones de clientes no autorizados.

2.2 El Riesgo reputacional

Es el riesgo de que se forme una opinión pública negativa sobre el servicio bancario prestado. El riesgo reputacional puede derivar en acciones que fomenten la creación de una mala imagen o un posicionamiento negativo en la mente de los clientes, de tal forma que se produzca una migración de fondos hacia otras entidades debido a una pérdida de credibilidad. Este riesgo también aparece vinculado al carácter estratégico de la banca electrónica, es decir, el hecho de no participar en este segmento influye significativamente en la imagen corporativa de la entidad financiera.

El riesgo reputacional puede surgir como respuesta a operaciones realizadas por el banco en sí mismo o como respuesta a acciones emprendidas por terceras partes. Este riesgo aparece cuando los sistemas o productos no funcionan como se esperaba y causan una reacción pública negativa generalizada. En este sentido, una ruptura significativa en la seguridad ofrecida puede dinamitar la confianza pública en un banco. El riesgo reputacional puede también surgir en aquellos casos donde los clientes experimentan problemas con un producto o servicio, y no hayan sido adecuadamente informados sobre el mismo y los procedimientos de resolución del problema.

Los errores, la malversación y el fraude de terceras partes exponen igualmente a los bancos al riesgo reputacional. Por ejemplo, supongamos que se producen fallos en las redes de comunicación que impiden el acceso de los clientes a sus fondos o a la información de sus cuentas, y no existen medios alternativos de acceso a éstas. Del mismo modo, un banco podría incurrir en pérdidas por el simple hecho de que otra institución que ofreciese servicios similares de banca electrónica cometiese frecuentemente errores en la prestación de tales servicios. Por esta razón se afirma que el riesgo reputacional no sólo es importante para un banco en particular, sino para el sistema bancario en su conjunto.

El riesgo reputacional puede aflorar debido a ataques selectivos sobre la imagen de un banco. Por ejemplo, pensemos en un pirata informático que penetre en la página Web de una entidad con el fin de alterarla intencionadamente e incluir información equívoca acerca del banco y sus productos.

2.3. Riesgo Legal

El riesgo legal surge de violaciones e incumplimientos con las leyes, reglas y prácticas, o cuando los derechos y obligaciones legales de las partes respecto a una transacción no están bien establecidos. Dada la relativa nueva naturaleza de muchas de las actividades de banca electrónica, los derechos y obligaciones de las partes respecto a estas transacciones son, en algunos casos, inciertas. Por ejemplo, las aplicaciones de algunas reglas de protección del cliente respecto a la banca electrónica en algunos países no son claras.

Además, el riesgo legal puede derivar de la incertidumbre respecto a la validación de algunos acuerdos relativos a los medios electrónicos.

Otra fuente de riesgo legal es la asociada a la protección de la privacidad. Aquellos clientes que no han sido adecuadamente informados sobre sus derechos y obligaciones pueden acometer contra el banco.

2.4. Otros riesgos

Los riesgos tradicionales de la banca, tales como el riesgo de crédito, el riesgo de liquidez, el riesgo de tipo de interés, y el riesgo de mercado, pueden también aparecer en la banca electrónica, aunque sus consecuencias prácticas podrían ser de menor magnitud.

El *riesgo de crédito* es el riesgo de que la contraparte no cumpla su obligación por su entero valor. Los bancos que operan en el segmento de banca electrónica pueden extender créditos a través de canales no tradicionales, y expandir su mercado más allá de las fronteras geográficas tradicionales.

La utilización de procedimientos inadecuados para determinar la capacidad crediticia de los prestatarios que piden créditos *en remoto* puede elevar el riesgo de crédito.

Los bancos que operan en programas de pago con dinero electrónico afrontan el riesgo de crédito si una tercera parte intermediaria incumple sus obligaciones con respecto al pago. De igual forma, los bancos que compran dinero electrónico de un emisor para revenderlo a sus clientes están también expuestos al riesgo de crédito (en el caso de que el emisor falle en sus obligaciones para redimir el dinero electrónico).

El *riesgo de liquidez* surge de la incapacidad del banco para cumplir con sus obligaciones cuando éstas le sobrevienen, sin incurrir en pérdidas. Esto sucede en aquellos casos donde el banco no puede atender los reembolsos y la demanda de liquidación por parte del cliente, en un momento determinado del tiempo. Además la iliquidez, en cierta manera, da lugar a acciones legales contra la institución bancaria con el consecuente daño reputacional.

El *riesgo de tipo de interés* se refiere a la exposición del banco a movimientos adversos en los tipos de interés. Los bancos que emiten dinero electrónico pueden verse afectados de forma importante por este tipo de riesgo, cuando movimientos adversos en el tipo de interés disminuyan el valor de los activos con relación a los pasivos de dinero electrónico que se mantienen.

El *riesgo de mercado* es el riesgo de pérdidas en caso de movimientos en los precios de mercado, incluyendo los tipos de cambio. Los bancos que aceptan moneda extranjera en pago de dinero electrónico están sujetos a este tipo de riesgo.

2.5. Transnacionalidad

La banca electrónica está basada en las tecnologías diseñadas para cubrir amplias áreas geográficas. La expansión del mercado puede extenderse más allá de las fronteras nacionales, haciendo surgir ciertos riesgos.

A pesar de que los bancos, normalmente, afrontan los riesgos enumerados con anterioridad, en las transacciones nacionales, es importante destacar que inciden también de forma importante, en la banca electrónica transnacional.

Los bancos deben cumplir diferentes requerimientos legales cuando trabajan con clientes más allá de sus fronteras. Por ejemplo, para la banca a través de Internet, existen actualmente lagunas respecto a estos requerimientos en determinados países. Además, hay ambigüedades jurisdiccionales con relación a las responsabilidades de las diferentes autoridades nacionales. Estas consideraciones pueden exponer a los bancos a un riesgo legal asociado con el incumplimiento de las diferentes leyes nacionales, como son las leyes de protección al consumidor, los requerimientos de comunicación, las reglas de privacidad, etc.

El riesgo operacional podría surgir para un banco que trata con un suministrador de servicios localizado en otro país, el cual, por esta razón, es más difícil de controlar. Los bancos están sujetos al *riesgo país* ya que las partes extranjeras pueden llegar a ser incapaces de cumplir sus obligaciones debido a factores políticos, económicos, sociales, etc.

Un banco que ofrece servicios a través de redes abiertas (Internet) está expuesto al riesgo de crédito, ya que la petición de crédito por clientes de otros países puede resultar más difícil de evaluar. De igual forma, los bancos que aceptan monedas extranjeras para el pago de dinero electrónico se encuentran sujetos al riesgo de mercado debido a variaciones en los tipos de cambio.

3. LA GESTIÓN DE RIESGO

Cada vez más, los bancos consideran estratégico operar en el segmento de la banca electrónica, ya que aumenta la eficiencia del banco y del sistema de pago, beneficiando a particulares y comerciantes. Sin embargo, se incurre en los riesgos anteriormente comentados. En este sentido, el Comité de Basilea sostiene que los bancos deben sopesar, por un lado, beneficios y riesgos reportados

por la banca electrónica y, por otro, ser capaces de gestionar y controlar los riesgos, así como absorber cualquier pérdida derivada si fuera necesario.

Aunque la banca electrónica puede representar una pequeña proporción sobre el conjunto de la actividad bancaria, El Comité de Basilea requiere a las autoridades competentes el aseguramiento del sistema financiero con el fin de que éste no se vea amenazado por la exposición al riesgo.

Las autoridades, a su vez, confían en que los bancos diseñen procesos que les permitan responder a los riesgos corrientes y ajustarse a los nuevos. Un proceso de gestión de riesgo debe incluir los tres elementos básicos de: valoración, control de la exposición y seguimiento de los riesgos. Los bancos deben emplear tales procesos cuando se comprometan con nuevas actividades de banca electrónica y cuando evalúen los compromisos existentes con estas actividades. Es esencial que tengan un proceso de gestión de riesgo compresivo para que puedan suministrar una visión apropiada a los directivos. En la medida en que los nuevos riesgos en la banca electrónica sean identificados y valorados, los directivos se mantendrán informados constantemente sobre estos cambios.

3.1. Valoración del Riesgo

Es un proceso continuo que engloba tres puntos:

1. Un banco debe encontrarse involucrado en un proceso analítico para identificar riesgos y, si fuera posible, cuantificarlos. En el caso de que los riesgos no pudieran ser cuantificados, la gestión podría identificar como los riesgos potenciales y establecer los pasos que hay que tomar para tratarlos y limitarlos. La gestión bancaria debería emitir un juicio razonable de la magnitud del impacto que tendría en el banco cualquier riesgo (incluyendo el impacto máximo potencial) y la probabilidad de que tal suceso ocurriese.
2. Un segundo paso en la valoración del riesgo es la determinación de la tolerancia al riesgo del banco, basado en una valoración de las pérdidas que el banco podría permitirse en el caso de que un problema dado en el sistema se materializase.
3. Finalmente, los gestores pueden estudiar, por un lado la tolerancia al riesgo y, por otra, la valoración del riesgo, y compararla para ver si la exposición al riesgo está dentro de los límites de tolerancia.

3.2 Gestión y Control de Riesgo

Una vez realizada la valoración y la tolerancia al riesgo, la gestión bancaria debería gestionar y controlar dicho riesgo. Esta fase incluye actividades tales como la aplicación de medidas de seguridad, coordinación de la comunicación interna, evaluación de productos y servicios, implantación de medidas para asegurar que los riesgos externos son controlados y gestionados, suministrar información al respecto al cliente y desarrollar planes de contingencias.

Se debería asegurar que el departamento encargado de hacer cumplir los límites de riesgo tenga una autoridad independiente de la unidad de negocio dedicada a la banca electrónica. Los bancos aumentan su habilidad para gestionar y controlar los riesgos inherentes a cualquier actividad cuando las políticas y procedimientos son establecidos en documentación escrita y están disponibles para todo el departamento.

3.2.1. Las Políticas y medidas de seguridad.

Entendemos por *seguridad* una combinación de sistemas, aplicaciones y de controles internos utilizados para salvaguardar la integridad, autenticidad y confidencialidad de los datos y procesos operacionales. Una buena seguridad descansa en el desarrollo y aplicación de adecuadas políticas y medidas de seguridad en los procesos internos del banco, y en la comunicación con terceros ajenos a él. Las políticas y medidas de seguridad pueden limitar el riesgo de ataques internos y externos en la banca electrónica, así como el riesgo reputacional producido por rupturas de seguridad.

Una política de seguridad debe velar por la salvaguarda de la información bancaria y suministrar una explicación sobre cómo se estructura dicha seguridad en el banco. También debe establecer parámetros que definan la tolerancia al riesgo del banco. La política puede definir responsabilidades en el diseño y aplicación, así como garantizar el cumplimiento de las medidas de seguridad y establecer procedimientos para evaluar la ejecución de la política, medidas disciplinarias y comunicar las violaciones de seguridad.

Las medidas de seguridad son combinaciones de herramientas de hardware, software y gestión de personal que contribuyen a construir sistemas seguros. Los bancos pueden elegir entre una variedad de medidas para prevenir o mitigar los ataques internos y externos y malos usos en la banca electrónica. Estas medidas pueden incluir, por ejemplo, la password, control de virus, registro del empleado, etc. La password, la contraseña y los números de identificación personal son técnicas para controlar el acceso e identificar al usuario. Los *firewalls* son combinaciones de hardware y software que controlan y limitan el acceso interno y externo a sistemas conectados en redes como Internet. Los firewalls pueden separar segmentos de redes internas utilizando la tecnología de Internet (intranet). Su tecnología puede ser un medio efectivo para controlar el acceso y salvaguardar los datos confidenciales. Un diseño bien planificado debería incluir requerimientos de seguridad amplios, claros procedimientos de operación, separación de deberes, y selección de personal de confianza que fuera responsable de la configuración y operación de un firewall.

Aunque los firewalls investigan los mensajes que entran, no necesariamente protegen de la infección de virus bajados de Internet. Como consecuencia, se deberían desarrollar controles preventivos y de detección para reducir la probabilidad de ataques de virus y de destrucción de datos.

Los programas para mitigar el riesgo de virus pueden incluir controles de la red, seguimiento de los usuarios, software antivirus, etc. No todas las amenazas de seguridad son externas; la banca electrónica debe estar salvaguardada con respecto a actividades no autorizadas llevadas a cabo por los empleados presentes y pasados. Para proteger la seguridad del sistema hay que tomar precauciones, controlando a los nuevos empleados, a los temporales y a los consultores.

3.2.2. Comunicación interna

Los riesgos operacional, reputacional, etc., pueden ser controlados si los gestores comunican al departamento de control de riesgo la importancia de la banca electrónica sobre el conjunto de objetivos del banco. Al mismo tiempo, el departamento técnico debería comunicar claramente cómo está diseñado el sistema para que funcione, así como sus debilidades y amenazas. Tales procedimientos pueden reducir el riesgo operacional de estructuras de diseño limitado, incluyendo la incompatibilidad de sistemas dentro de la organización bancaria; problemas de integridad de datos; el riesgo reputacional asociado a la insatisfacción del cliente con relación al funcionamiento del sistema; y riesgo de liquidez y de crédito. Para asegurar la adecuada comunicación interna, todas las políticas y procedimientos deberían ser suministrados de forma escrita. Además, los gestores deberían adoptar una política corporativa de educación y potenciación de perfiles y conocimientos, coherente con las innovaciones tecnológicas, con el fin de limitar los riesgos operacionales derivados de una carencia de gestión experta. La implantación del sistema puede incluir un curso técnico de trabajo, así como tiempo para que el departamento se adapte a la evolución del mercado.

3.2.3. Evaluación (test de productos o servicios)

La evaluación de productos y servicios antes de que sean lanzados definitivamente al mercado puede también contribuir al control del riesgo operacional y reputacional, en la medida en que la validación permite conocer si el sistema funciona correctamente y produce los resultados deseados. Los programas pilotos y los prototipos resultan muy útiles en el desarrollo de nuevas aplicaciones.

3.2.4. Outsourcing

Una tendencia creciente en la industria bancaria consiste en centrarse estratégicamente en sus competencias principales y delegar a terceros expertos otras actividades. Aunque estos acuerdos pueden ofrecer beneficios tales como la reducción de costes y las economías de escala, sin embargo no liberan al banco de la última responsabilidad en cuanto al control de riesgo en sus operaciones. Consecuentemente, los bancos deberían adoptar políticas para limitar los riesgos derivados de estos proveedores de servicios. Por ejemplo, la gestión bancaria debería llevar un seguimiento de la ejecución operacional y financiera de sus proveedores de servicios; asegurar que las relaciones contractuales entre las partes, así como las obligaciones de cada una de ellas, son claramente entendidas y definidas por escrito, y mantener un acuerdo de contingencia para cambiar de proveedor de servicio rápidamente si fuera necesario.

La seguridad de la información delicada del banco es de crítica importancia. El acuerdo de *outsourcing* obliga al banco a compartir estos datos reservados con los proveedores de servicios. La gestión bancaria debería evaluar la habilidad del proveedor de estos servicios para mantener el mismo nivel de seguridad que el obtenido para las actividades llevadas desde el banco, a través de una revisión de las políticas y procedimientos encaminadas a proteger esta información por los proveedores de servicios. Adicionalmente, la banca que opte por el *outsourcing* deberá tener el derecho a evaluar la competencia y la ejecución operacional y financiera de los proveedores de servicios.

3.2.5. Demostraciones y educación del cliente

Las demostraciones y la educación o adiestramiento del cliente pueden ayudar al banco a limitar el riesgo legal y reputacional. Se trata de programas para familiarizar al cliente con los nuevos productos y servicios, con las comisiones inherentes a los mismos, y con los procedimientos de resolución de errores y problemas. Todo ello facilita a los bancos cumplir con las leyes de protección al consumidor.

Explicaciones sobre la naturaleza de la relación bancaria incluida en la página web pueden reducir el riesgo legal derivado de problemas con los servicios o productos ofrecidos en la misma.

3.2.6. Planes de Contingencia

Un banco puede limitar el riesgo de ruptura en los procesos internos o en el suministro de un producto/servicio gracias a los planes de contingencia que establecen un curso de acción en el caso de que se produzcan rupturas en la provisión de servicios electrónicos. El plan debería incluir: recuperación de datos, procesos alternativos de datos, servicios de emergencia y de apoyo al cliente... Los sistemas de backup deberían ser testados periódicamente para garantizar su efectividad. En definitiva, los bancos deben asegurar que sus operaciones de banca electrónica son tan seguras como sus operaciones corrientes.

Un importante aspecto de la banca electrónica es la dependencia de otras empresas: vendedores de hardware, software, proveedores de Internet, compañías de telecomunicaciones, etc. La gestión bancaria debe insistir en que tales proveedores de servicios tengan capacidades de bakup.

Además, en la gestión deben pronosticarse acciones compensatorias, que pudieran llevarse a cabo cuando los proveedores de servicios provocasen perjuicios al cliente bancario. Estos planes podrían incluir contratos a corto plazo con otros proveedores y una política que describiese cómo el banco tratará las pérdidas del cliente asociadas con la ruptura del servicio. Los bancos deberían también considerar la facultad de reservarse el derecho de cambiar de proveedores en cualquier momento si fuese necesario.

Los planes de contingencia pueden también contribuir a limitar el riesgo reputacional derivado de las propias acciones del banco, o de problemas experimentados por otras instituciones que ofrecen servicios similares de banca electrónica. Por ejemplo, los bancos podrían establecer procedimientos para tratar los problemas de los clientes durante las interrupciones del sistema.

3.3. Seguimiento del riesgo

Un continuo seguimiento es un aspecto importante de cualquier proceso de gestión del riesgo. En el caso de la banca electrónica el seguimiento es doblemente importante debido a la naturaleza de las actividades (ya que cambian rápidamente a medida que las innovaciones ocurren) y la dependencia de algunos productos de Internet. Dos elementos de este seguimiento son el sistema de vigilancia y comprobación y el sistema de auditoría.

3.3.1. Sistema de vigilancia y comprobación.

La *comprobación* de operaciones del sistema puede ayudar a detectar actividades inusuales y los problemas más graves que se pueden presentar: rupturas y ataques. El test de penetración se centra en la identificación, aislamiento y confirmación de defectos en el diseño y la aplicación de los mecanismos de seguridad a través de intentos controlados para penetrar en un sistema fuera de los procedimientos normales.

La *vigilancia* es una forma de seguimiento en la cual el software y las aplicaciones de auditoría se utilizan para llevar a cabo la actividad. En contraste al test de penetración, la vigilancia se centra en el seguimiento de actividades rutinarias, la investigación de anomalías, y la emisión de continuos informes respecto a la efectividad de la seguridad.

3.3.2. La auditoría

La auditoría (interna y externa) suministra un mecanismo independiente de control para detectar deficiencias y minimizar riesgos en el suministro de servicios bancarios electrónicos. El papel de un auditor es asegurar que las políticas y procedimientos desarrollados son los adecuados, y que el banco se adhiere a ellos. El personal auditor debe tener la suficiente experiencia para llevarlo a cabo. Un auditor interno debería estar separado e independiente de los empleados que toman decisiones de riesgo, por ello la gestión debería buscar auditores externos cualificados, tales como consultores de seguridad informática y otros profesionales de relevante experiencia, que proporcionen una valoración independiente de la banca electrónica.

3.4. La gestión del riesgo transnacional

Los riesgos transnacionales son más complejos que los afrontados por la banca en su país de origen; por ello merecen una especial atención.

Los bancos que eligen diferentes mercados nacionales en los que operar necesitan conocer los diferentes requerimientos legales de esos mercados y desarrollar una apreciación de las diferencias en las expectativas del consumidor y su conocimiento sobre los productos y servicios. Además, los gestores deberían asegurarse de que los sistemas de extensión de crédito y gestión de la liquidez tienen en cuenta las dificultades potenciales derivadas de las actividades transnacionales. Es necesario valorar el riesgo país y desarrollar planes de contingencia que contemplen las rupturas de servicios debidos a problemas en el clima político y económico exterior. En el caso de que los bancos deleguen en suministradores de servicios extranjeros, las autoridades nacionales querrán valorar la accesibilidad a la información de dichos suministradores de servicios.

Las autoridades nacionales pueden jugar un papel importante en la identificación y discusión de las ambigüedades jurisdiccionales, así como dirigir sus esfuerzos hacia el desarrollo de medidas para detectar prácticas ilegales e inseguras. Finalmente, pueden potenciar los esfuerzos para compartir información sobre innovaciones en los productos y servicios de la banca electrónica.

4. CONCLUSIONES

1. El futuro para el negocio bancario se encuentra vinculado, sin lugar a dudas, a los canales alternativos de distribución, entre ellos la banca electrónica.
2. La fidelización de la clientela, la diversificación de la actividad bancaria y el ahorro de costes son las principales ventajas que ofrece la banca en remoto.
3. La moneda única y la aplicación de las nuevas tecnologías de la comunicación aumentarán la integración de la banca en el marco europeo, lo cual repercutirá en una mayor competencia y reducción de los precios de los productos y servicios financieros.
4. A pesar de los beneficios que reporta la banca electrónica, la operativa en este segmento no está exenta de riesgo. El Comité de Basilea define una serie de riesgos inherentes a las transacciones electrónicas: riesgo operacional, el riesgo reputacional y el legal, los cuales deben ser identificados, medidos y gestionados por los bancos para evitar incurrir en pérdidas económicas directas.
5. La monitorización de estos riesgos implica adoptar una posición proactiva que se concrete en campañas de difusión y sensibilización para adiestrar al cliente, elaboración de planes de contingencia y establecimiento de medidas de seguridad, formación de personal cualificado, actualización constante de las tecnologías, etc.
6. La seguridad es uno de los aspectos que más preocupan tanto a bancos como a clientes. Sin embargo, pensamos el verdadero problema se trasladará, con el tiempo, desde aspectos tecnológicos a factores estratégicos, es decir, el riesgo asociado a no operar en el segmento de banca electrónica o no estar lo suficientemente actualizado dentro del sector.

BIBLIOGRAFÍA.

Risk management for electronic banking and electronic money activities. Basle Committee on Banking Supervision .

Naranjo, Laura. *La Banca electrónica abarata los costes y fideliza las pymes.* Mercado de Riesgos, nº 37, septiembre 1998.

Pérez-Ocerin, Javier. *Realidad y Futuro de Internet en los Servicios Electrónicos Bancarios.* Banca y Finanzas, nº. 27, noviembre 1997.

Montoya, Andrés. Nuevos Servicios Bancarios. *La Banca electrónica.* Dirección y Progreso, nº 136 (1994).

Charro Pastor, Alberto Manuel. *La Función de Tesorería en la Empresa Banca Electrónica y Cash Management.* Boletín de Estudios Económicos, Vol. 1.1, nº. 157, Abril 1996.

Guillen, Imanol. *Los tecnicismos de 1992.* Directivos Nueva Banca, 1988.

Steinhardt, Ricardo J.M. *Marketelematica, La Nueva Estrategia de la Banca Electrónica.* Alta Dirección, 1986.