GESTIÓN DEL RIESGO INFORMÁTICO EN LA BANCA ELECTRÓNICA

Díaz Ramírez Raúl.
Rauldiz38@gmail.com
Universidad Piloto de Colombia

Resumen— En este documento se comentan los aspectos más importantes de la gestión del riesgo informático de la banca electrónica y las actividades con dinero electrónico desde la perspectiva de auditoria interna. Teniendo en cuenta las mejores prácticas a desarrollar para asegurar los servicios en línea.

Abstract— In this paper the most important aspects of IT risk management of electronic banking and electronic money activities from the perspective of internal audit are discussed . Given develop best practices for securing online services.

Índice de Términos— Aseguramiento, Banca Electrónica, Dinero Electrónico, Gestión de riesgos.

I. INTRODUCCIÓN

La transformación digital está afectando a todas las industrias, entre ellas se encuentran las entidades bancarias que tienen un reto importante en la creación de nuevos productos financieros en línea que agreguen valor al consumidor, es por ello que la banca electrónica permite a los bancos ampliar sus mercados para sus actividades tradicionales de recepción de depósitos, otorgamiento de créditos ofrecimiento de productos y servicios, además de fortalecer su posición competitiva en la oferta de servicios de pago existentes. Adicional un factor clave es la reducción de los costos de operación.

En general el desarrollo continuado de la banca electrónica contribuye a mejorar la eficiencia del sistema bancario y de pagos y a reducir el costo de las transacciones con los consumidores a nivel nacional e internacional. Lo que da como resultado un aumento de la productividad y el bienestar económico. Los usuarios bancarios pueden incrementar la eficacia con la que hacen y reciben pagos y disfrutar de una mayor comodidad al respecto. La banca electrónica puede además de permitir el acceso al sistema financiero de aquellos consumidores que tienen un acceso limitado.

El desarrollo y uso de dinero electrónico y de algunas formas de banca electrónica se encuentra todavía en las etapas iniciales. Dada la incertidumbre que existe acerca del desarrollo futuro de la tecnología y de los mercados con relación a la banca electrónica y el dinero electrónico, es importante que las autoridades de supervisión eviten las políticas que podrían obstaculizar la innovación y la experimentación útil. La banca electrónica y las actividades con dinero electrónico conllevan riesgos para las entidades bancarias, y que estos riesgos deben equilibrarse con los beneficios.

II. DEFINICIÓN DE BANCA ELECTRÓNICA Y DINERO ELECTRÓNICO

A. Banca Electrónica

Se refiere al suministro de productos y servicios bancarios para consumidores por medio de canales electrónicos. Estos productos y servicios pueden incluir la recepción de depósitos, préstamos, manejo de cuentas, asesoría financiera, pago electrónico de facturas y el suministro de otros productos y servicios de pago electrónico y dinero electrónico (definido en forma separada más abajo).

Dos de los aspectos fundamentales de la banca electrónica son: las características de los canales de entrega y los medios disponibles a los consumidores para acceder a estos canales. Los canales de entrega más comunes incluyen redes "cerradas" y "abiertas". Las "redes cerradas" limitan el acceso a los participantes (instituciones financieras, consumidores, comerciantes y suministradores de servicios para terceros) que son miembros en virtud de un acuerdo específico. Las "redes abiertas" no tienen estos requisitos de membrecía. Actualmente, los productos y servicios de la banca electrónica

son suministrados a los consumidores por medio de una variedad de dispositivos de acceso, como: terminales en los puntos de venta, cajeros automáticos, teléfonos, computadoras personales, smart cards y otros.

B. Dinero electrónico

Se refiere a un valor almacenado o mecanismos pagados por adelantado para la ejecución de pagos por medio de terminales en el punto de venta, transferencias directas entre dos dispositivos, o mediante redes abiertas de computación, como Internet. Los productos de valor almacenado, incluyen mecanismos de "hardware" y "basados en tarjetas" (también llamados "monederos electrónicos") y mecanismos "software" o "basados en redes" (también llamados "efectivo digital"). Las tarjetas de valor almacenado pueden ser "uni-propósito" o "multi-propósito". Las tarjetas de uni-propósito (por ejemplo, tarjetas para teléfonos) se usan para comprar un sólo tipo de bien o servicios, o productos de un sólo vendedor. Las tarjetas multi-propósito pueden ser utilizadas para una variedad de compras a varios vendedores.

III. DEFINICIÓN DE BANCA ELECTRÓNICA Y DINERO ELECTRÓNICO

El riesgo operativo, riesgo a la reputación y riesgo legal son las categorías más importantes para la mayoría de las actividades de banca electrónica y dinero electrónico, especialmente para los bancos internacionales

Algunos de los problemas específicos, tocan varias categorías de riesgos. Por ejemplo, una violación de seguridad que permita el acceso no autorizado a información sobre clientes puede ser clasificada como un riesgo operativo, pero dicho evento también expone al banco a un riesgo legal y a un riesgo a la reputación. A pesar de que estos diferentes tipos de riesgo pueden ser generados por un sólo problema, la gestión apropiada de riesgos puede exigir varias acciones correctivas para responder a cada uno de los diferentes riesgos que se puedan presentar en un momento determinado en la entidad financiera.

A. Riesgo operativo

El riesgo operativo se genera del potencial de pérdida debida a deficiencias importantes en la confiabilidad e integridad del sistema. Los aspectos de seguridad son de la mayor importancia, ya que los bancos pueden sufrir ataques externos o internos a sus sistemas o productos. El riesgo operativo puede generarse por:

Fraude interno: Errores intencionados en la información sobre posiciones, robos por parte de empleados, utilización de información confidencial en beneficio de la cuenta del empleado, etc.

Fraude externo: atraco, falsificación, circulación de cheques en descubierto, daños por intrusión en los sistemas informáticos, etc.

Prácticas con los clientes, productos y negocios: abusos de confianza, abuso de información confidencial sobre el cliente, negociación fraudulenta en las cuentas del banco, blanqueo de capitales, venta de productos no autorizados, etc.

Daños a activos materiales: terrorismo, vandalismo, terremotos, incendios, inundaciones, etc.

Alteraciones en la actividad y fallos en los sistemas: fallos del hardware o del Software, problemas en las telecomunicaciones, interrupción en la prestación de servicios públicos, etc.

Ejecución, entrega y procesamiento: errores en la introducción de datos, fallos en la administración del colateral, documentación jurídica incompleta, concesión de acceso no autorizado a las cuentas de los clientes, prácticas inadecuadas de contrapartes distintas de clientes, litigios con distribuidores, etc

Adicionalmente también por el mal uso de los clientes, un diseño inadecuado del sistema, o un sistema mal implantado. Entre los ejemplos de riesgo operativo se encuentra: Acceso no autorizados, fraude de empleados, obsolescencia del sistema, ausencia de gestión experta, riesgo del proveedor del servicio, el cliente no cumple las pautas de seguridad, el cliente niega haber realizado una transacción

B. Riesgos 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, 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.

Figura 1. Infografía Pago Seguro
Fuente: Kaspersky Lab

Diseño del 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 se suceden en las tecnologías 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; al mismo tiempo, 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.

El Mal Uso y Servicios por el Cliente

Los malos usos del cliente, tanto intencionado como inadvertido, 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 (hacker) tener acceso directo a las cuentas de los clientes. Consecuentemente, el banco podría

incurrir en pérdidas financieras debido a transacciones de clientes no autorizados.

C. 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. 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, por ejemplo, un banco mundialmente activo experimenta un daño importante a su reputación relacionado con sus negocios de banca electrónica o dinero electrónico, la seguridad de los sistemas de los demás bancos puede también ser cuestionada. En circunstancias extremas, una situación de esta naturaleza puede conducir a interrupciones sistémicas en la banca en general.

D. 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. Los sistemas de dinero electrónico pueden ser atractivos para el lavado de dinero cuando ofrecen límites flexibles de saldos y transacciones y disponen una posibilidad limitada de auditoría de las transacciones. La aplicación de reglas de lavado de dinero puede no ser apropiada para algunas formas de pagos electrónicos. Puesto que la banca electrónica puede ser conducida a distancia, los bancos pueden enfrentarse a mayores dificultades para aplicar métodos tradicionales de prevención y detección de la actividad criminal.

Los bancos que se dedican a la banca electrónica y a las actividades de dinero electrónico pueden enfrentarse a riesgos legales relacionados con divulgaciones a los clientes y protección de la confidencialidad. Los clientes que no reciben una información adecuada sobre sus derechos y obligaciones pueden iniciar acciones legales en contra del banco. La falta de una protección de la confidencialidad adecuada puede también someter al banco a sanciones de reglamentación en algunos países.

Los bancos que eligen mejorar su servicio al cliente conectando sus lugares en el Internet a otros lugares, pueden también enfrentar riesgos legales. Un experto en computadoras puede utilizar el lugar para estafar a un cliente del banco, y el banco se enfrentaría a un litigio con dicho cliente.

A medida que se expande el comercio electrónico, los bancos buscan participar en sistemas de autenticación electrónica, como los que utilizan certificados digitales. El rol de autoridad de certificación puede exponer al banco a un riesgo legal. Por ejemplo, un banco que actúa como autoridad de certificación puede ser responsable de pérdidas financieras incurridas por las partes que confiaron en la certificación. Además, el riesgo legal puede presentarse si los bancos participan en sistemas nuevos de autentificación y no se especifican con claridad los derechos y obligaciones pertinentes.

IV. GESTIÓN Y CONTROL DE RIESGOS

Para un número cada vez mayor de bancos, existe una razón estratégica para involucrarse en actividades de banca electrónica y dinero electrónico. Además, un mayor uso de la banca electrónica y dinero electrónico puede incrementar la eficiencia del sistema bancario y de pagos, beneficiando a clientes y comerciantes. Al mismo tiempo, existen riesgos para los bancos que se dedican a actividades de banca electrónica y dinero electrónico. Estos riesgos deben compararse con los beneficios y los bancos deben ser capaces de manejar y controlar los riesgos y absorber toda pérdida asociada, si fuese necesario. Los riesgos que presenta la banca electrónica y el dinero electrónico deben ser evaluados en el contexto de los otros riesgos que enfrenta el banco. Si bien las actividades de banca electrónica y dinero electrónico pueden representar una parte relativamente pequeña de las actividades totales de los bancos, los supervisores pueden aun así exigir a la administración superior.

La seguridad que los sistemas esenciales no se ven amenazados por los riesgos que toma el banco.

El ritmo acelerado de las innovaciones tecnológicas probablemente cambiará las características y el alcance de los riesgos que enfrentan los bancos con relación a la banca electrónica y al dinero electrónico. Los supervisores esperan que los bancos pongan en práctica procesos que permitan a la administración del banco responder a los riesgos actuales y adaptarse a los riesgos nuevos. Un proceso de gestión de riesgo que incluye los tres elementos básicos de evaluación de riesgos, control de riesgos y seguimiento de riesgos ayudará a los bancos y a los supervisores en el logro de estos objetivos. Los bancos pueden emplear un proceso de este tipo al comprometerse con nuevas actividades de banca electrónica y dinero electrónico y al evaluar los compromisos ya existentes.

Es de suma importancia que los bancos pongan en práctica un proceso general de gestión de riesgos, vigilado por el directorio y la administración superior. A medida que se identifican y evalúan nuevos riesgos en la banca electrónica y dinero electrónico, se debe mantener informado al directorio y a la administración superior de estos cambios.

Figura 2. Alinear Estrategia, Control y Gestión
Fuentes: Committe of Sponsoring Organization of the Treadway

Antes de comenzar toda actividad nueva, se debe realizar un análisis amplio para que la administración superior pueda asegurarse que el proceso de gestión de riesgos es adecuado para evaluar, controlar y seguir todo riesgo generado por la nueva actividad propuesta.

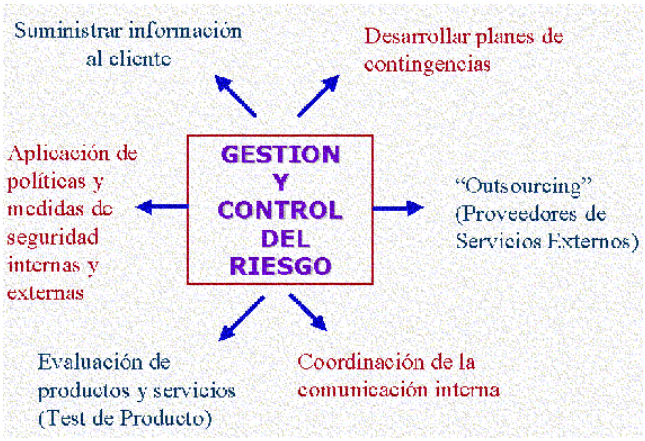

Figura 3. Gestión y Control del Riesgo
Fuente: José Manuel Feria Domínguez, la Banca en Internet, Riesgos Implícitos

A. Evaluación de los Riesgos

La evaluación de los riesgos es un proceso continuo, que comprende, normalmente, tres pasos. Primero, el banco puede realizar un análisis riguroso para identificar los riesgos y, donde sea posible, cuantificarlos. Si los riesgos no pueden ser cuantificados, la administración puede aun así identificar cómo pueden presentarse los riesgos potenciales y los pasos que ha dado para responder y limitar dichos riesgos. La administración del

banco debe formarse un criterio razonable de la magnitud de todo riesgo con respecto, tanto al efecto que podría tener sobre el banco (incluyendo el efecto potencial máximo), como a la probabilidad que dicho evento ocurra.

El segundo paso en la evaluación de riesgos es la determinación por parte del directorio y de la administración superior de la tolerancia al riesgo del banco, basado en la evaluación de las pérdidas que el banco podría sostener en el evento de la materialización de un problema dado.

Finalmente, la administración puede comparar su tolerancia al riesgo con su evaluación de la magnitud del riesgo para confirmar si la exposición al riesgo se adapta a los límites de tolerancia.

B. Manejo y Control de los Riesgos

Habiendo realizado una evaluación de los riesgos y de su tolerancia al riesgo, la administración del banco debe dar pasos para manejar y controlar los riesgos. Esta fase del proceso de gestión de riesgos incluye actividades tales como la ejecución de políticas y medidas de seguridad, la coordinación interna de las comunicaciones, la evaluación y actualización de productos y servicios, la ejecución de medidas para garantizar el control y manejo de los riesgos de contrataciones fuera de la compañía, la provisión de divulgaciones y educación del cliente y la preparación de planes para contingencias. La administración superior debe asegurar que el personal responsable de la aplicación de los límites de riesgo tiene autoridad independiente de las unidades de negocios encargadas de las actividades de banca electrónica y dinero electrónico. Los bancos aumentan su capacidad de controlar y manejar los diferentes riesgos inherentes a toda actividad, cuando las políticas y los procedimientos se incluyen en documentos escritos, puestos a la disposición del personal pertinente.

C. Las Políticas y Medidas de Seguridad

Se entiende 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. De esta forma, se puede 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 establecer los parámetros que definan la tolerancia al riesgo del banco y, así garantizar el cumplimiento de las medidas de seguridad y establecer procedimientos que evalúen la ejecución de la política, las medidas disciplinarias y la comunicación de posibles violaciones en la 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, el password, control de virus, registro del empleado, etc. El 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.

Adicionalmente se debe tener en cuenta los requerimientos de banca móvil de la circular 042 externa de 2012 de la Superintendencia Financiera de Colombia:

Contar con mecanismos de autenticación de dos factores para la realización de operaciones monetarias y no monetarias.

Para operaciones monetarias individuales o que acumuladas mensualmente por cliente superen dos SMMLV, implementar mecanismos de cifrado fuerte de extremo a extremo para el envío y recepción de información confidencial de las operaciones realizadas, tal como: clave, número de cuenta, número de tarjeta, etc. Esta información, en ningún caso, podrá ser conocida por los proveedores de redes y servicios de telecomunicaciones ni por cualquier otra entidad diferente a la entidad financiera que preste el servicio a través de este canal.

Dicha información tampoco podrá ser almacenada en el teléfono móvil.

Cualquier comunicación que se envíe al teléfono móvil como parte del servicio de alertas o notificación de operaciones no requiere ser cifrada, salvo que incluya información confidencial.

Para las operaciones monetarias individuales o que acumuladas mensualmente por cliente sean inferiores a dos SMMLV y que no cifren la información de extremo a extremo, la entidad deberá adoptar las medidas necesarias para mitigar el riesgo asociado a esta forma de operar, el cual debe considerar los mecanismos de seguridad en donde la información no se encuentre cifrada. La Superintendencia Financiera de Colombia (SFC) podrá suspender el uso del canal cuando se advierta que existen fallas que afecten la seguridad de la información.

Contar con medidas que garanticen la atomicidad de las operaciones y eviten su duplicidad debido a fallas en la comunicación ocasionadas por la calidad de la señal, el traslado entre celdas, etc.

Los servicios que se presten para la realización de operaciones a través de Internet, en sesiones originadas desde el dispositivo móvil, deben cumplir con los requerimientos establecidos en el numeral 4.9 Internet, los cuales son:

Implementar los algoritmos y protocolos necesarios para brindar una comunicación segura.

Realizar como mínimo dos veces al año una prueba de vulnerabilidad y penetración a los equipos, dispositivos y medios de comunicación usados en la realización de operaciones monetarias por este canal. Sin embargo, cuando se realicen cambios en la plataforma que afecten la seguridad del canal, deberá realizarse una prueba adicional.

Promover y poner a disposición de sus clientes mecanismos que reduzcan la posibilidad de que la información de sus operaciones monetarias pueda ser capturada por terceros no autorizados durante cada sesión.

Establecer el tiempo máximo de inactividad, después del cual se deberá dar por cancelada la sesión, exigiendo un nuevo proceso de autenticación para realizar otras operaciones.

Informar al cliente, al inicio de cada sesión, la fecha y hora del último ingreso a este canal.

Implementar mecanismos que permitan a la entidad financiera verificar constantemente que no sean modificados los enlaces (links) de su sitio Web, ni suplantados sus certificados digitales, ni modificada indebidamente la resolución de sus DNS.

Contar con mecanismos para incrementar la seguridad de los portales, protegiéndolos de ataques de negación de servicio, inyección de código malicioso u objetos maliciosos, que afecten la seguridad de la operación o su conclusión exitosa.

Las entidades que permitan realizar operaciones monetarias por este canal deben ofrecer a sus clientes mecanismos fuertes de autenticación.

D. Comunicación Interna

La gestión de los riesgos operativos, a la reputación, legales y otros se facilita cuando la administración superior comunica al personal pertinente la forma en que la provisión de banca electrónica y dinero electrónico pretende apoyar los objetivos generales del banco. Al mismo tiempo, el personal técnico debe comunicar a la

administración superior cómo funcionan los sistemas, así como los puntos fuertes y las debilidades de los mismos. Estos procedimientos pueden disminuir los riesgos operativos del diseño deficiente de sistemas, incluyendo la incompatibilidad de diferentes sistemas dentro de una organización bancaria; problemas de integridad de la información; riesgo a la reputación asociado con la insatisfacción de los clientes; y riesgos crediticios y de liquidez. Para asegurar una comunicación interna adecuada, todas las políticas y procedimientos deberían ser dados por escrito. Además, la administración superior debería poner en práctica, como política general, la educación y actualización constante del personal de acuerdo con el ritmo de la innovación tecnológica. Estas actividades de capacitación podrían incluir cursos técnicos en el trabajo, así como tiempo para que el personal se mantenga informado sobre los acontecimientos importantes del mercado.

E. Evaluación y Perfeccionamiento

La evaluación de productos y servicios antes de su comercialización generalizada puede también ayudar a limitar los riesgos operativos y a la reputación. La realización de pruebas comprueba que los equipos y sistemas funcionan adecuadamente y producen los resultados deseados. Los programas piloto o los prototipos pueden ser útiles para el desarrollo de nuevas aplicaciones. El riesgo de la interrupción de los sistemas puede también ser disminuido con políticas de revisión regular de las capacidades del "hardware" y "software" existentes.

F. Outsourcing

Existe una tendencia cada vez mayor de concentrarse estratégicamente en las actividades principales y confiar a terceros las actividades que no entran en las competencias del banco. Si bien este tipo de acuerdos ofrece ciertos beneficios, como ser, la reducción de costos y economías de escala, no liberan al banco de su responsabilidad final en el control de los riesgos que afectan sus operaciones. En consecuencia, los bancos deberían formular políticas para limitar los riesgos que resultan de la dependencia de suministradores externos de servicios. Por ejemplo, la administración del banco debe seguir de cerca el rendimiento operativo y financiero de sus suministradores de servicios; asegurar que las relaciones entre las partes del contrato, así como las expectativas y obligaciones de cada parte son bien comprendidas y contenidas en contratos escritos con fuerza legal; y mantener un plan de contingencia para cambiar los suministradores de servicios rápidamente, si fuera necesario.

La seguridad de la información sensible del banco es de importancia fundamental. Las contrataciones fuera de la empresa pueden obligar al banco a compartir datos confidenciales con los suministradores de servicios. La administración del banco debe evaluar la capacidad del suministrador de servicios para mantener el mismo nivel de seguridad, como si las actividades fueran conducidas por el banco mismo. Esto se puede lograr examinando las políticas y procedimientos del suministrador de servicios para la protección de datos confidenciales. Adicionalmente, los supervisores podrían exigir el derecho de evaluar en forma independiente la competencia y el rendimiento operativo y financieros de los suministradores de servicios.

G. Divulgaciones y Educación del Cliente

Las divulgaciones y educación al cliente pueden ayudar a un banco a limitar el riesgo legal y a la reputación. Las divulgaciones y programas de educación para clientes sobre el uso de nuevos productos y servicios, cargos por servicios y productos y procedimientos de solución de problemas y errores pueden asistir a los bancos en su cumplimiento con las leyes y reglamentos de protección al cliente y de confidencialidad. Las divulgaciones y explicaciones sobre el tipo de relación del banco con un lugar en la red, pueden reducir el riesgo legal de un banco generado por problemas con servicios o productos del lugar conectado a la red.

H. Planes de Contingencia

Un banco puede limitar el riesgo de interrupciones de los procesos internos o en la entrega de servicios o productos, elaborando planes de contingencia donde se establece el curso de las acciones en caso de una interrupción del

suministro de servicios de banca electrónica y dinero electrónico. Este plan puede incluir la recuperación de datos, formas alternativas de procesamiento de datos, personal de emergencia y apoyo al servicio al cliente. Los sistemas de respaldo deben ser verificados periódicamente para comprobar su eficiencia. Los bancos deben garantizar que sus operaciones de contingencia son tan seguras como sus operaciones normales.

Un aspecto importante de la banca electrónica y dinero electrónico es la dependencia de entidades externas, como ser vendedores de "hardware", proveedores de "software", proveedores de servicios Internet y compañías de telecomunicaciones. La administración del banco podría insistir que dichos proveedores de servicios cuenten con capacidades de respaldo de sus actividades. Además, la administración podría considerar las acciones de compensación que podría desarrollar en caso que los suministradores de servicios se vean imposibilitados de cumplir con sus obligaciones. Estos planes podrían incluir la contratación, a corto plazo, de otros proveedores y una política describiendo la forma en que el banco trataría las pérdidas de sus clientes, asociadas con la interrupción del servicio. Los bancos deberían también tener en cuenta la conveniencia de reservarse el derecho de cambiar de proveedores de servicios, en forma rápida, si fuese necesario.

La planificación de contingencias puede también contribuir a limitar el riesgo a la reputación generado por las acciones del propio banco, o por problemas sufridos por otra institución que ofrece productos o servicios de banca electrónica o dineros electrónicos, idénticos o similares. Por ejemplo, los bancos podrían establecer procedimientos para atender los problemas de los clientes durante la interrupción del sistema.

V. SEGUIMIENTO

Un seguimiento constante es un aspecto importante en todo proceso de gestión de riesgos. En el caso de la banca electrónica y del dinero electrónico el seguimiento es particularmente importante, ya que la naturaleza de estas actividades puede cambiar rápidamente a medida que se producen innovaciones y debido a la dependencia de ciertos productos del uso de redes abiertas, como el Internet. Dos elementos importantes del seguimiento son la verificación y la auditoria de los sistemas.

A. Verificación y Vigilancia de los Sistemas

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.

B. Auditorías

Las auditorías (internas y externas) brindan un mecanismo de control independiente para detectar deficiencias y reducir, a un mínimo, los riesgos que comporta el suministro de servicios de banca electrónica y dinero electrónico. El rol de un auditor es velar por la elaboración de normas, políticas y procedimientos apropiados, y confirmar el compromiso del banco con los mismos. El personal de auditoría debe tener la experiencia necesaria para llevar a cabo un análisis preciso. El auditor interno debe ser independiente de los empleados que intervienen en la toma de decisiones relacionadas con la gestión de riesgos.

Para completar la auditoría interna, la administración puede hacer uso de auditores externos calificados, como ser, consultores en seguridad u otros profesionales, para obtener una evaluación independiente de las actividades de banca electrónica o dinero electrónico.

VI. CONCLUSIONES

La Banca Electrónica está orientada a brindar servicios Financieros en la Nube permitiendo realizar transacciones en línea y evitando desplazamientos de los clientes hacia las oficinas, por lo anterior las entidades bancarias deben contar con una infraestructura tecnológica robusta y segura para evitar posibles fraudes y estafas.

Los tipos de riesgos que deben mitigar y minimizar las entidades financieras son: Operativo, Seguridad, Reputacional y Legal.

Las entidades financieras deben contar con un plan de gestión de riesgos integral que permita tener una óptima administración y tratamiento de los riesgos.

Las entidades financieras deben contar con un plan de gestión de riesgos integral que permita tener una óptima administración y tratamiento de los riesgos.

Las entidades financieras deben tener un plan de seguimiento e implementación de acciones de mejora de los riesgos.

REFERENCIAS

[1] Comité de Basilea para la supervisión Bancaria (Marzo de 1998) disponible en: http://www.asba-supervision.org/aml-cft/doc_download/1439-gestion-de-riesgos-para-la-banca-electronica-y-las-actividades-con-dinero-electronico.

[2] Tendencias metodológicas de gestión de riesgo informático y continuidad del negocio (Septiembre 01 de 2010) disponible en: http://portal.uexternado.edu.co/pdf/6_DerechoDeLosNegocios/adelaGarz%C3%83%C2%B3n.pdf.

[3] José Manuel Feria Domínguez. La Banca en Internet: Riesgos Implícitos disponible en:http://thales.cica.es/rd/Recursos/rd98/Economia/02/texto3.html.

[4] Peligros de la Banca Online: Infografía (28 de septiembre de 2012) disponible en: http://www.ticbeat.com/tecnologias/los-peligros-de-la-banca-online-infografi/

[5] Buenas prácticas para la supervisión y gestión del riesgo operativo disponible en: http://www.bis.org/publ/bcbs96esp.pdf.

[6] Circular 042 de 2012 Superintendencia Financiera de Colombia disponible en: http://www.certicamara.com/download/correspondencia/20121005_Anexos_12_circular_042_de_2012.pdf.