Banca Electrónica

Milton Eduardo Rodríguez[1]

Introducción

Las mejoras tecnológicas introducen innovaciones en nuestra vida diaria a una velocidad rápida. Uno de los productos innovadores que surgen de estas mejoras es la tecnología de Internet y tiene un uso expansivo. El gasto del consumidor a través de Internet está aumentando a un ritmo significativo. Progresivamente más grupos y organizaciones coinciden en que internet puede ser utilizado para facilitar el desarrollo, aprovechando su fácil acceso a la información y la transferencia de tecnología. El aumento de la competencia en el sector bancario y demanda de los clientes está obligando a los bancos a prestar servicios en línea.

El ímpetu y la expansión de la globalización y el desarrollo de nuevas tecnologías han obligado a los bancos a poner en marcha nuevos canales para buscar ventajas competitivas, reducir sus costos, mejorar sus servicios financieros, ampliar sus bases de datos de clientes, desarrollando su posición financiera a través de productos innovadores y aumentar la lealtad de sus clientes. Hoy en día, los bancos se están cambiando a la distribución multicanal de los servicios financieros a través de internet.

En El Salvador, los bancos tradicionalmente han estado a la vanguardia en la utilización de la tecnología para mejorar sus productos, servicios y eficiencia, aún cuando prevalecen algunas barreras para operaciones interbancarias. Durante un largo tiempo, han estado utilizando canales electrónicos y de telecomunicaciones para la entrega de una amplia gama de productos y servicios de valor agregado. Los canales de distribución han sido directos a través de redes privadas o redes públicas, y los dispositivos incluyen teléfonos, computadoras personales, cajero electrónico automatizado, entre otros. Con la popularidad de las computadoras, el acceso fácil a Internet y la World Wide Web (www), Internet se utiliza cada vez más por los bancos como un canal para recibir las instrucciones y la entrega de sus productos y servicios a sus clientes. Esta forma de la banca se conoce generalmente como la Banca por Internet, aunque la gama de productos y servicios ofrecidos por diferentes bancos varían mucho, tanto en su contenido como su sofisticación.

En el presente documento se expone la banca electrónica en términos de una técnica de distribución multicanal, con el objetivo de examinar la progresión de la Banca Electrónica y la proposición de estrategias para controlar y luchar contra los problemas de riesgo asociados con las actividades de la banca electrónica, este trabajo está organizado de la siguiente manera: la primera parte inicia con la definición del término banca electrónica y su importancia; un detalle de todos los riesgos asociados a tal actividad financiera; luego se mencionan y explican cada uno de los principios de administración de riesgos relacionados emitidos por el Comité de Basilea para la Supervisión Bancaria; se aborda la experiencia internacional relacionada a la materia; en seguida se presenta la experiencia salvadoreña de la banca electrónica y por último se enuncian conclusiones sobre planteamientos normativos que regulen la banca electrónica en el Sistema Financiero nacional de El Salvador.

I. Definición e Importancia

De acuerdo al Comité de Basilea para la Supervisión Bancaria (2003), la 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, como el dinero electrónico[2]".

Basilea considera también que dos de los aspectos fundamentales de la banca electrónica son: las características de los canales de entrega y los medios

1/ Especialista del Departamento de Normas del Sistema Financiero

2/ De acuerdo al documento "Gestión de Riesgos para la Banca Electrónica y Actividades con Dinero Electrónico" (Marzo, 1998) del Comité de Supervisión Bancaria de Basilea, el 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 el Internet.

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 que son miembros en virtud de un acuerdo específico. Estos miembros pueden ser instituciones financieras, consumidores, comerciantes y suministradores de servicios para terceros.

Las "redes abiertas" no tienen estos requisitos de membresía. 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.

Muchas empresas se han adaptado rápidamente a los cambios de Internet y la tecnología para mejorar su eficiencia y la calidad del servicio a través de nuevas aplicaciones en Internet, y así lograr atraer nuevos clientes, cambiando el modelo de negocio de muchas industrias alrededor del mundo como en el caso de la industria bancaria.

El sector bancario es uno de los principales usuarios de las tecnologías de la información y la comunicación en la vida empresarial a raíz de la necesidad de contar con procesos eficientes para el manejo de grandes volúmenes de información. En la búsqueda de esta gestión eficiente de la información la banca se basa en gran medida en la tecnología de la información (TI) para adquirir, procesar y entregar dicha información a todos los usuarios pertinentes. Los bancos saben que tienen que innovar y actualizar sus productos constantemente para retener a sus clientes exigentes y así proporcionarles servicios de calidad, confiables y convenientes según las últimas tendencias tecnológicas.

Cabe destacar que un estudio de investigación conjunta entre GSMA, A.T. Kearney y Wireless Intelligence, muestra que en El Salvador, existen grandes oportunidades para expandir la Banca Electrónica a través de telefonía móvil, tomando en cuenta que en promedio la penetración de esta es hasta del 92.83% de acuerdo al siguiente cuadro de ranking para el año 2010:

Desde la introducción de Internet en 1969, este ha pasado de ser del dominio exclusivo de la red de la computadora y el académico a ser un canal principal de comunicación y un medio actualmente bastante desarrollado para el comercio electrónico. Este rápido crecimiento de Internet ha presentado una nueva serie de oportunidades, así como amenazas serias a los negocios. Hoy en día los celulares permiten al cliente conocer saldos de cuentas y realizar traspasos; el internet facilita el ingreso a los servicios que ofrecen las entidades financieras; las tarjetas de débito/crédito facilitan las transacciones disminuyendo los riesgos y la banca móvil permite mayor interacción entre el cliente y el banco. En este sentido, toma relevancia que para el caso de mercados regulados como el financiero, existan disposiciones específicas relacionadas a la supervisión y regulación de los servicios y productos que se ofrezcan por medio de esta modalidad.

Penetración Móvil				
País	Ranking 2010	Ranking 2008	Puntaje 2010	Puntaje 2008
Panamá	1	1	100.00	100.00
Uruguay	2	2	96.96	97.81
Argentina	3	3	94.18	97.01
El Salvador	4	4	92.83	91.12
Jamaica	5	5	91.13	88.95
Chile	6	6	89.64	88.80
Brasil	7	7	70.11	72.74
Ecuador	8	8	68.91	71.98
Venezuela	9	9	67.02	66.70
Colombia	10	10	57.94	54.40
República Dominicana	11	11	56.99	53.26
Paraguay	12	12	56.09	52.71
Guatemala	13	13	53.18	52.49
Honduras	14	14	53.15	50.57
México	15	15	43.70	42.32
Perú	16	16	43.18	37.01
Bolivia	17	17	34.72	34.52
Costa Rica	18	18	30.88	12.93
Nicaragua	19	19	18.30	4.02
Haití	20	20	0.00	0.00

Fuente: Observatorio Móvil de América Latina 2011

II. Riesgos relativos a la Banca Electrónica

Un aspecto muy importante que hay detrás de la rápida propagación de la banca electrónica por todo el mundo es su aceptación como un canal de distribución muy rentable de los servicios bancarios en comparación con otros canales existentes. Sin embargo, Internet no se considera un medio de comunicación del todo benigno para el sector bancario, ya que junto a la reducción en el costo de las transacciones, ha sobrevenido una nueva orientación a riesgos, incluso nuevas formas de riesgos a los que los bancos comúnmente se han visto expuestos. En general, las autoridades monetarias y financieras de todo el mundo están preocupadas debido a que, mientras los bancos deben seguir siendo eficaces y rentables, estos también deben estar muy conscientes de los diferentes tipos de riesgos que esta otra actividad de la banca conlleva y que deben disponer de sistemas para la gestión de la misma. El objeto de la actuación reguladora en el control de riesgos ha sido la de identificar los riesgos en términos generales y así asegurar que los bancos cuentan con sistemas mínimos establecidos para abordar el mismo, y que tales sistemas se revisan de forma continua de acuerdo con los cambios en la tecnología.

En los párrafos que siguen, un conjunto genérico de riesgos se discuten como base para la formulación de las directrices de control de riesgos generales que de una u otra forma están vinculados a la actividad financiera de la banca electrónica.

a) Riesgo operacional:

El riesgo operativo, también conocido como riesgo transaccional, es la forma más común de riesgo asociado con la banca electrónica. Toma en cuenta el procesamiento inexacto de las transacciones, no cumplimiento de los contratos, compromisos en la integridad de los datos, la privacidad y confidencialidad de datos, el acceso no autorizado o intrusión a sistemas y operaciones, entre otros. Tales riesgos pueden surgir como consecuencia de deficiencias de los bancos en el diseño, ejecución y supervisión de sus sistemas de información. Además de las deficiencias en la tecnología, los factores humanos como la negligencia por parte de los clientes y empleados, la actividad fraudulenta de los empleados y hackers pueden llegar a ser una fuente potencial de riesgo operacional. A menudo hay una delgada línea de diferencia entre el riesgo operativo y riesgo para la seguridad y ambas terminologías se utilizan casi indistintamente.

De acuerdo a BNAMERICAS (2012): "Además de los delitos vinculados a la suplantación de identidad, las amenazas o riesgos que más vienen creciendo son los fraudes internos cometidos por empleados de las instituciones. Ya sea por infracciones deliberadas o por una fuga accidental de los datos, donde los empleados conforman un canal creciente de filtración de información. Esos riesgos están incrementando las inversiones. "Donde hay más inversión en tecnología de punta es en la prevención de fraudes internos", dice Sánchez Berián, de everis. La tendencia más fuerte hoy es la implantación interna de monitorización activa de empleados mediante la utilización de predictivos; se usan los mismos elementos que para el marketing proactivo, pero aplicados contra el fraude.

Si bien los desembolsos en tecnologías para reducir los fraudes internos son crecientes, no son tan visibles como los aplicados para brindar seguridad a los canales transaccionales. ¿La razón? A diferencia de los ataques de phishing (obtención en forma ilegal de información confidencial, personal y financiera simulando que la solicitud proviene de una organización confiable y reconocida) y códigos maliciosos que afectan las cuentas de los clientes, en los fraudes internos la víctima es la propia institución, y la mayoría de las entidades prefiere no dar a conocer estos hechos".

b) Riesgo de seguridad

Internet es una red pública de computadoras que facilita el flujo de datos o información y al que se puede acceder sin restricciones. Los bancos que utilicen este medio para las transacciones financieras deben tener la tecnología y los sistemas adecuados en su respectiva ubicación, con

un entorno seguro para este tipo de transacciones.

El riesgo de seguridad es latente debido a un acceso no autorizado a los almacenes de información crítica de un banco como el sistema de contabilidad, sistema de gestión de riesgos, sistema de gestión de cartera, entre otros. Una violación de la seguridad podría resultar en pérdidas financieras directas a un banco. Por ejemplo, los piratas que operan a través de Internet, podrían acceder, recuperar y utilizar la información confidencial de los clientes y también podrían implantar virus. Esto puede resultar en la pérdida de datos, robo o manipulación de información de los clientes, la desactivación de una parte importante del sistema informático interno del banco negando así el servicio, fuertes desembolsos por la reparación de estos, entre otros. Otros riesgos asociados son la pérdida de la reputación, violación de la privacidad de los clientes y sus implicaciones legales. Por lo tanto, el control de acceso es de suma importancia.

El control de acceso al sistema de los bancos se ha vuelto más complejo en el entorno de Internet, un acceso no autorizado podría emanar de cualquier fuente y de cualquier parte del mundo, con o sin intención criminal. Los ataques podrían ser por parte de piratas, vendedores sin escrúpulos, empleados descontentos o incluso, puros amantes de la adrenalina. Por lo tanto, es necesario que los bancos evalúen críticamente todos los sistemas interrelacionados con sus actividades y productos e implementar medidas de control de acceso en su locación física y en cada uno de ellos.

Además de los ataques externos los bancos están expuestos a los riesgos de seguridad a partir de fuentes internas por ejemplo fraude de los empleados. Los empleados están familiarizados con los diferentes sistemas y sus debilidades se convierten en amenazas potenciales de seguridad en un entorno poco controlado. Ellos pueden llegar a adquirir los datos de autenticación para acceder a las cuentas de clientes que causarían pérdidas al banco.

A menos que estén específicamente o adecuadamente protegidos, toda la transferencia de datos o información a través de Internet puede controlarse o ser leída por personas no autorizadas. Hay programas como "sniffers", que se pueden configurar en los servidores web o de otros lugares críticos para recopilar datos como números de cuenta, contraseñas y números de cuenta de tarjetas de crédito. Problemas de privacidad de datos y confidencialidad son relevantes, incluso cuando los datos no se transfieren a través de la red. Los datos que residen en los servidores web o los sistemas internos, son susceptibles a la corrupción si no se aíslan correctamente a través de los servidores de seguridad de Internet.

El riesgo de alteración de datos, con o sin intención, pero no autorizado, es real en un entorno de red, cuando se están transmitiendo datos o se están almacenando. Un control de acceso estricto y adecuado junto con el uso de herramientas tecnológicas para garantizar la integridad de los datos es de suma importancia para toda institución financiera y empresas en general. Otro aspecto importante a evaluar es si los sistemas están óptimamente configurados para detectar rápidamente cualquier alteración y así disparar una alerta. La identificación de una persona que presenta una solicitud de un servicio o una transacción como cliente es crucial para la validez jurídica de una transacción y es una fuente de riesgo para un banco. Una computadora conectada a Internet se identifica por su dirección IP (Protocolo de Internet). Los atacantes disponen de métodos para hacer pasar un equipo como otro, comúnmente conocidas como "IP Spoofing". Del mismo modo la identidad del usuario puede ser tergiversada. Por lo tanto, el control de la autenticación es un paso esencial de seguridad en cualquier sistema de banca electrónica.

El no repudio implica la creación de una prueba de comunicación entre dos partes, por ejemplo el banco y su cliente, que no puede negarse más tarde. Los sistemas de los bancos deben estar tecnológicamente equipados para manejar estos aspectos que son fuentes potenciales de riesgo.

Según BNAMERICAS(2012) "Los delitos informáticos son la prin-

cipal fuente de inseguridad para las entidades financieras. Códigos maliciosos (virus, troyanos y gusanos que se introducen en los programas para robar información), phishing y fraudes internos aumentan con fuerza en América Latina.

Desafío en la seguridad móvil

Dentro de los múltiples canales por los cuales se puede ofrecer el servicio de banca electrónica, en la modalidad de telefonía móvil los riesgos son más altos porque buena parte de los usuarios ya sabe que, así como no pueden tener un PC sin protección, tampoco es posible tener un móvil protegido de ataque. Pero esa convicción aún no ha llegado al móvil. BNAMERICAS(2012) menciona que "el uso de las redes sociales y de servicios de mensajería como WhatsApp, que procesa 2.000 millones de mensajes al día, o de sistemas de pago como Google Wallet, está convirtiendo al móvil en un blanco creciente de ataques".

BNAMERICAS también destaca que este foco de vulnerabilidad está apurando las inversiones en investigación. En el mismo documento se resalta que:

"La línea de inversión en investigación que más está creciendo es la incorporación de mecanismos biométricos para la identificación del usuario de banca móvil; empieza a haber celulares con dispositivos como los de lectura de huellas, pero, sobre todo, lo que más se busca es aprovechar las cámaras de los celulares para aplicar sistemas de reconocimiento de rostro.

Las proyecciones indican que esos ataques seguirán creciendo. Los dispositivos móviles serán uno de los principales objetivos de ataques en 2012 en América Latina, particularmente aquellos que utilizan la plataforma Android, según un estudio de Eset. Existe, por ejemplo, una aplicación para Android que aparece como Generador de Token (Token Generator) para hacerse con información, como nombre de usuario y claves secretas, de los usuarios de banca móvil. Esta aplicación se descarga a los celulares a través de correos electrónicos, mensajes de texto, sitios web y enlaces que aparentan provenir de los bancos".

c) Riesgo de la arquitectura del sistema y su diseño

Un control y una apropiada arquitectura del sistema son factores importantes en el manejo de diversos tipos de riesgos operativos y de seguridad. Los bancos enfrentan el riesgo de una mala elección de la tecnología, el diseño inadecuado del sistema y los procesos de control inadecuados. Por ejemplo, si el acceso a un sistema se basa en sólo una dirección IP, cualquier usuario puede acceder al hacerse pasar por un usuario legítimo de la suplantación de direcciones IP de un usuario genuino. Numerosos protocolos se utilizan para la comunicación a través de Internet. Cada protocolo está diseñado para tipos específicos de transferencia de datos. Un sistema que permite la comunicación con todos los protocolos, por ejemplo HTTP (Hyper Text Transfer Protocol), FTP (Protocolo de transferencia de archivos) , Telnet , entre otros, es más propenso a ser atacado que un sistema que permita comunicación sólo con HTTP.

La elección de la tecnología adecuada es otro aspecto potencial de riesgo para los bancos. Una tecnología anticuada, no escalable o no probada podría infligir al banco la pérdida de inversiones, tener un sistema vulnerable y llegar a ofrecer un servicio ineficiente con los riesgos operativos y de seguridad latente, así como también la pérdida de negocio.

Muchos bancos confían en los proveedores de servicios externos para implementar, operar y mantener sus sistemas de banca electrónica. Aunque esto puede ser requerido cuando los bancos no tienen la experiencia necesaria, esto es un aspecto que se suma al riesgo operacional. El hecho de que los proveedores de servicios tengan acceso a toda la información crítica del negocio y los sistemas técnicos del banco, hace el sistema vulnerable. En tal escenario, la elección del proveedor, el acuerdo contractual para la prestación del servicio, entre otros, se convierten en componentes críticos de la seguridad de los bancos.

Las entidades deben educar a su propio personal y demás dependencias respecto a este tipo de proveedores que se deben evitar en la medida de lo posi-

ble. No actualizar el sistema del banco de acuerdo con la tecnología que cambia rápidamente, aumenta el riesgo operacional, ya que deja agujeros en el sistema de seguridad del mismo. Además, el personal puede no comprender plenamente la naturaleza de la nueva tecnología empleada. Así, la educación del personal, como de los usuarios, desempeña un papel importante para evitar riesgos operativos. Estos incluyen el control de acceso, el uso de servidores de seguridad, técnicas criptográficas, el cifrado de clave pública, la firma digital, entre otros.

d) Riesgo reputacional

El riesgo de reputación es el riesgo de contraer significativamente la opinión pública negativa, lo que puede resultar en una pérdida crítica de financiación (o altos costos financieros) o de clientes. Estos riesgos se derivan de acciones que causan una mayor pérdida de la confianza pública en la capacidad de los bancos para llevar a cabo funciones críticas o poner en peligro la relación banco - cliente. Puede ser debido a la propia acción de los bancos o debido a la acción de terceros.

Las principales razones de este riesgo podrían ser que el sistema o los productos no funcionan con las expectativas de los clientes, deficiencias críticas del sistema, importantes fallos de seguridad (debido a ataques, internos o externos), la falta de información a los clientes sobre el uso de los productos y los procedimientos de resolución de problemas, problemas significativos con las redes de comunicación que impiden el acceso de los clientes a sus fondos o información de cuenta, sobre todo si no existen medios alternativos de acceso. Tales situaciones pueden provocar en el cliente, la interrupción de la adquisición del producto o de los servicios contratados. Los clientes directamente afectados pueden dejar el banco y otros podrían tomar la misma decisión al darse cuenta por experiencias ajenas de la mala calidad del producto o servicio financiero ofrecido.

Entre las posibles medidas para evitar este tipo de riesgo se plantea, probar el sistema antes de la implementación, facilidades de recuperación de datos, planes de contingencia, incluidos los planes para hacer frente a problemas de los clientes durante las interrupciones del sistema, la implementación de análisis de virus, la práctica del "ethical hacking[3]" para tapar las lagunas y otras medidas de seguridad.

e) El Riesgo Legal

El riesgo legal surge ante la posibilidad de incumplimiento de leyes, normas, reglamentos o prácticas prescritas, o cuando los derechos y obligaciones de las partes en una transacción no están bien establecidos. Dado lo compleja que resulta la banca por Internet, los derechos y obligaciones en algunos casos son inciertos y la aplicabilidad de las leyes y normas es incierta o ambigua, lo que provoca el riesgo legal, sin embargo, la entidad no se exime de responsabilidades deducidas de los casos anteriormente señalados.

Otras razones de los riesgos legales son la incertidumbre sobre la validez de algunos acuerdos formados a través de medios electrónicos y la ley con respecto a las revelaciones de los clientes y la protección de la vida privada. Un cliente, indebidamente o poco informado acerca de sus derechos y obligaciones, no puede tomar las debidas precauciones en el uso de los productos o servicios de banca por Internet, lo que lleva a transacciones en disputa u otras sanciones reglamentarias. En el entusiasmo de mejorar el servicio al cliente, el banco podría tener un enlace a su sitio de Internet a otros sitios también. Esto puede incurrir en el riesgo legal, porque un hacker podría utilizar el sitio vinculado para estafar a un cliente de un banco.

f) Riesgo de lavado de dinero

A medida que se realizan las transacciones de banca por Internet de forma remota los bancos pueden tener dificultades para aplicar el método tradicional para la detección y prevención de actividades delictivas indeseables. La aplicación de las normas de lavado de dinero

3/ Simulación de probables escenarios en donde se reproducen ataques, con pruebas de intrusión, a la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos, servidores, entre otros, de manera controlada con el fin de comprobar vulnerabilidades en estos.

también pueden ser inapropiadas para algunas formas de pagos electrónicos. Así, los bancos se exponen al riesgo de lavado de dinero. Esto puede dar lugar a sanciones legales por incumplimiento de "conozca a su cliente". Para evitar esto, los bancos tienen que diseñar la identificación adecuada del cliente y una técnica de selección; desarrollo de pistas de auditoría, llevar a cabo revisiones periódicas de cumplimiento; políticas y procedimientos para detectar e informar de actividades sospechosas en las transacciones por Internet

g) Riesgos transfronterizos

La banca por Internet se basa en una tecnología que, por su propia naturaleza, está diseñada para ampliar el alcance geográfico de los bancos y los clientes. Esta expansión del mercado puede extenderse más allá de las fronteras nacionales. Esto provoca diversos riesgos. Incluye los riesgos legales y regulatorios, ya que puede haber incertidumbre acerca de los requisitos legales en algunos países y las ambigüedades de jurisdicción con respecto a las responsabilidades de las distintas autoridades nacionales. Tales consideraciones pueden exponer a los bancos a riesgos legales asociados con la falta de cumplimiento de las distintas leyes y normas nacionales, incluidas las leyes de protección al consumidor, el mantenimiento de registros y requisitos de presentación de informes, las reglas de privacidad y las leyes de lavado de dinero. Si un banco utiliza un proveedor de servicios con sede en otro país, será más difícil de controlar, incurriendo así en riesgos operacionales. Además, el proveedor de servicios establecido en el extranjero o los participantes extranjeros en la banca por Internet, son fuentes de riesgo país en la medida en que las partes extranjeras se convierten en incapaces de cumplir con sus obligaciones debido a factores económicos, sociales o políticos.

Las transacciones transfronterizas acentúan el riesgo de crédito, ya que es difícil de evaluar una solicitud de un préstamo de un cliente en otro país con respecto a un cliente de una base de clientes familiar. Los bancos que aceptan monedas extranjeras en el pago de dinero electrónico pueden ser sometidos al riesgo de mercado, debido a los movimientos en los tipos de cambio.

h) Riesgo Estratégico

Este riesgo está asociado con la introducción de un nuevo producto o servicio. El grado de este riesgo depende de lo bien que la entidad ha abordado las diversas cuestiones relacionadas con el desarrollo de un plan de negocios, la disponibilidad de recursos suficientes para apoyar este plan, la credibilidad del vendedor (si se subcontrata) y el nivel de la tecnología utilizada en comparación con la tecnología disponible, entre otros.

Para reducir este riesgo, los bancos necesitan llevar a cabo un estudio adecuado de la demanda, consulta a expertos de diversos campos, establecer metas alcanzables y monitorear el desempeño. También tienen que analizar la disponibilidad y el costo de los recursos adicionales, la disposición del personal de apoyo, una formación adecuada del mismo y cobertura de seguro idónea. La debida diligencia se debe observar en la selección de proveedores, la auditoría del funcionamiento y establecer arreglos alternativos en caso de una posible incapacidad de un proveedor para cumplir con su obligación. Además de esto, se requieren evaluaciones periódicas de las nuevas tecnologías y la consideración adecuada de los costos de una actualización tecnológica.

i) Otros riesgos asociados

Riesgos bancarios tradicionales tales como el riesgo de crédito, riesgo de liquidez, riesgo de tipo de interés y riesgo de mercado también están presentes en la banca por Internet. Estos riesgos se pueden intensificar debido a la propia naturaleza de la banca por Internet a causa de uso de los canales electrónicos, así como ausencia de límites geográficos. Sin embargo, sus consecuencias prácticas pueden ser de una magnitud diferente para los bancos y los supervisores de los riesgos operacionales, reputacionales y legales. Esto puede ser particularmente cierto para los bancos que se dedican a una variedad de actividades bancarias, en comparación con los bancos o las filiales de bancos

que se especializan en la banca por Internet.

El riesgo crediticio: es el riesgo de que una contraparte no liquide una obligación por su valor total, ya sea a su vencimiento o en cualquier momento posterior. Los bancos pueden no ser capaces de evaluar adecuadamente la solvencia del cliente, mientras que la ampliación de crédito a través de procedimientos de banca a distancia podría aumentar el riesgo de crédito. En la actualidad, los bancos generalmente operan con la base de clientes más familiar. La facilidad de pago electrónico de cuentas en la banca por Internet puede causar el riesgo de crédito si un intermediario tercero no cumpla con sus obligaciones con respecto al pago. Otra variante de la banca por Internet es el dinero electrónico. Trae varios tipos de riesgos asociados. Si un banco adquiere dinero electrónico de un emisor con el fin de transferirlo a un cliente, que se expone al riesgo de crédito en caso de que el emisor caiga en impago de su obligación de reembolso de dinero electrónico.

Riesgo de liquidez: surge de la incapacidad de un banco para cumplir con sus obligaciones a su vencimiento sin incurrir en pérdidas inaceptables, a pesar de que el banco puede en última instancia, ser capaz de cumplir con sus obligaciones. Es importante para un banco dedicado a actividades de transferencia de dinero electrónico, garantice que los fondos son suficientes para cubrir las demandas de canje y liquidación en cualquier momento en particular Si no lo hace, además de exponer al banco a riesgos de liquidez, incluso puede dar lugar a acciones legales y el riesgo de reputación.

Del mismo modo los bancos, manejando dinero electrónico, hacen frente a tasas de interés electrónicas volátiles debido a movimientos adversos en las tasas de interés que causan disminución del valor de los activos en relación con los pasivos pendientes de dinero electrónico. Los bancos también se enfrentan a riesgos de mercado a causa de las pérdidas en las posiciones dentro y fuera de balance, derivados de los movimientos de los precios de mercado, incluidos los tipos de cambio. Los bancos que acepten moneda extranjera para el pago de dinero electrónico también están sujetos a este tipo de riesgo.

Riesgo de la competencia desleal: la banca por Internet intensifica la competencia entre los distintos bancos. La naturaleza abierta de Internet puede inducir a algunos bancos a utilizar prácticas desleales para tomar ventaja sobre sus rivales. Cualquier fuga en la conexión de red o sistema operativo, pueden permitir que interfieran en el sistema de un banco rival. Así, se puede encontrar que junto con los beneficios, la banca por Internet conlleva diversos riesgos para la propia entidad, así como el sistema bancario en su conjunto. El rápido ritmo de la innovación tecnológica es probable que mantenga el cambio de la naturaleza y el alcance de los riesgos que enfrentan los bancos. Estos riesgos deben sopesarse frente a los beneficios. Se requiere que las autoridades encargadas de la supervisión y regulación desarrollen métodos para la identificación de nuevos riesgos, evaluación de riesgos, gestión de riesgos y el control de la exposición al riesgo.

Por lo tanto las autoridades deben alentar a los bancos a desarrollar un proceso de gestión de riesgos rigurosa y lo suficientemente amplio como para hacer frente a los riesgos conocidos y suficientemente flexibles para dar cabida a los cambios en el tipo y la intensidad de los riesgos.

III. Principios de Administración de Riesgos para Banca Electrónica

Principios de Basilea

Los principios de administración de riesgos para la banca electrónica que emitió Basilea caen en tres amplias categorías de aspectos y a veces se traslapan. Sin embargo, estos principios no son ponderados en orden de preferencia o importancia. Si solamente tales ponderaciones pueden cambiar en el tiempo, es preferible que permanezcan neutrales y eviten que se les dé tal prioridad.

Los 14 Principios de Administración de Riesgos para Banca Electrónica

A. Vigilancia de la Junta Directiva y de la Administración (Principios 1 a 3)

La Junta Directiva y la administración superior son responsables de desarrollar la estrategia de negocios de la institución bancaria. Una decisión estratégica explícita debe ser efectuada si la Junta desea que el banco proporcione servicios de transacciones de banca electrónica antes de comenzar a ofrecer tales servicios. Específicamente, la Junta debe asegurarse que los planes de banca electrónica estén claramente integrados dentro de las metas estratégicas corporativas, que se lleve a cabo un análisis de riesgos de las actividades propuestas de banca electrónica, que se establezcan procesos apropiados de mitigación y monitoreo de riesgos para los riesgos identificados, y que se conduzcan revisiones permanentes para evaluar los resultados de las actividades de banca electrónica contra los planes y objetivos de negocios de la institución.

- Θ Principio 1: La Junta Directiva y la administración superior deben establecer una vigilancia efectiva de la administración sobre los riesgos asociados con las actividades de banca electrónica, incluyendo el establecimiento de responsabilidad específica, de políticas y controles para manejar estos riesgos.

- Θ Principio 2: La Junta Directiva y la administración superior deben revisar y aprobar los aspectos claves de los procesos de control de seguridad de banca electrónica.

- Θ Principio 3: La Junta Directiva y la administración superior deben establecer un amplio y constante proceso de vigilancia y debida diligencia para manejar las relaciones de contratación externa del banco y otras dependencias de terceras partes que estén apoyando a la banca electrónica.

Los 14 Principios de Administración de Riesgos para Banca Electrónica

B Controles de Seguridad (Principios 4 a 10)

En tanto que la Junta Directiva tiene la responsabilidad de asegurar que existan procesos apropiados de control de seguridad para banca electrónica, la sustancia de estos procesos necesitan atención especial de la administración debido a los retos de seguridad mejorada impuestos por la banca electrónica. Los siguientes aspectos son particularmente pertinentes:

- Autenticación
- No rechazo
- Integridad de los datos y las transacciones
- Segregación de funciones o tareas
- Controles de autorización
- Mantenimiento de pistas de auditoria
- Confidencialidad de la información bancaria clave

Θ Principio 4: Los bancos deben tomar las medidas apropiadas para autenticar la identidad y la autorización de los clientes con quienes conduzca negocios a través de Internet.

Θ Principio 5: Los bancos deben utilizar métodos de autenticación de transacciones que promuevan el no rechazo y establezcan responsabilidad para las transacciones de banca electrónica.

Θ Principio 6: Los bancos deben asegurarse que existan medidas apropiadas para promover una segregación adecuada de funciones en los sistemas de banca electrónica, en las bases de datos y en las aplicaciones.

Θ Principio 7: Los bancos deben asegurarse que tengan controles apropiados de autorización y privilegios de autorización para los sistemas de banca electrónica, para las bases de datos y aplicaciones.

Θ Principio 8: los bancos deben asegurarse que tengan medidas apropiadas para proteger la integridad de los datos de las transacciones de banca electrónica, de los registros y de la información.

Θ Principio 9: los bancos deben asegurarse de que existan claras pistas de auditoría para todas las transacciones de banca electrónica.

Θ Principio 10: Los bancos deben tomar medidas apropiadas para preservar la confidencialidad de información clave de banca electrónica. Las medidas tomadas para preservar la confidencialidad deben ser conmensuradas con la sensibilidad de la información que esté siendo transmitida y/o almacenada en bases de datos.

Los 14 Principios de Administración de Riesgos para Banca Electrónica

C. Administración de los Riesgos Legales y de Reputación (Principios 11 al 14)

Las leyes y regulaciones sobre privacidad y protección específica del cliente variarán de jurisdicción a jurisdicción. Sin embargo, generalmente los bancos tienen una clara responsabilidad de proporcionar a sus consumidores un nivel de comodidad relativo a la divulgación de información, a la protección de datos de sus clientes y disponibilidad de negocios, que se aproxime al nivel que tendrían si hicieran transacciones de negocios a través de los tradicionales canales de distribución bancaria.

- Principio 11: Los bancos deben asegurarse de que se proporcione información adecuada en sus sitios web de tal forma que permita a los clientes potenciales para que hagan una conclusión informada acerca de la identidad del banco y el estado regulativo del banco, previo a efectuar transacciones de banca electrónica.

- Principio 12: Los bancos deben tomar las medidas apropiadas para asegurar la adherencia a los requerimientos aplicables sobre privacidad del cliente para las jurisdicciones en que el banco esté proporcionando servicios y productos de banca electrónica.

- Principio 13: los bancos deben tener una capacidad efectiva, continuidad de negocios y procesos de planificación de contingencias para ayudar a asegurar la disponibilidad de los servicios y sistemas de banca electrónica.

- Principio 14: los bancos deben desarrollar planes apropiados de respuesta a incidentes para administrar, detener y minimizar los problemas resultantes de eventos inesperados, incluyendo ataques internos y externos, que pudieran impedir la provisión de servicios y sistemas de banca electrónica.

Fuente: Elaboracíon propia en base a documento **"Basel Committee on Banking Supervision, (July, 2003): Risk Management Principles for Electronic Banking"**.

IV. Experiencia Internacional

En los últimos años, las entidades financieras se han esforzado en brindar a los clientes y usuarios los servicios de la banca electrónica, adecuando sus operaciones financieras para ofrecer diversas opciones que permitan al cliente ahorrar tiempo y disponer de fácil acceso a los servicios desde cualquier punto en el que se encuentren sin tener que apersonarse a las instalaciones financieras, aspecto que coadyuva de sobremanera a la bancarización en la región y/o a la inclusión financiera.

De acuerdo a Claudia Casas (2011), a nivel latinoamericano la banca electrónica está muy difundida, principalmente a través del canal de telefonía móvil, siendo las experiencias más destacables las siguientes:

- Brasil: Disponen de servicio desarrollado de e-banking, mobile banking y payment para consultas y transferencias de valores y pagos respectivamente, donde todas las transacciones tienen que estar respaldadas por cuentas bancarias. No existe una regulación establecida.

- Colombia: La banca electrónica está desarrollada, permitiendo efectuar transacciones financieras (transferencias entre cuentas, pago a terceros y consulta de saldos) a cualquier hora a través de teléfonos móviles e internet y cuyas transacciones están respaldadas por una cuenta bancaria. En cuanto a la regulación, la Superintendencia Financiera de Colombia y el Ministerio de Tecnología de Información son los encargados de generar y hacer cumplir las disposiciones normativas y regulatorias que permitan la implementación de productos financieros para servicios financieros móviles, velando por la seguridad y calidad del mismo.

- Costa Rica: La banca electrónica ha crecido en las últimas dos décadas y proporciona al usuario financiero la posibilidad de realizar consultas, transacciones financieras, transferencias y pago de servicios a través del internet. Se dispone además de un servicio de banca móvil que no se encuentra regulado, a través del cual pueden realizar operaciones de: consulta de saldos, compra de divisas, y pago de servicios telefónicos.

- Chile: A partir de la década de los 90 empezó un proceso de masificación de la banca por internet, canales telefónicos y red de cajeros automáticos ATM. Asimismo, las entidades financieras empezaron a ofrecer servicios de banca móvil sustentadas en cuentas bancarias, cuyo servicio permite realizar operaciones como: publicación de abono de sueldo, transferencia de fondos, postergar la cuota de un crédito, abono a la línea de sobregiro, inversiones, pagos de cuentas, avances en efectivo y consulta de movimientos. La Superintendencia de Bancos e Instituciones Financieras es la encargada de brindar seguridad, calidad y regulación en la banca móvil, a través de la normativa sobre transferencia electrónica de información y fondos y externalización de servicios.

- Honduras: A través de la banca por internet se pueden realizar transacciones en cuentas de ahorro, pago de planillas, pago de servicios básicos y su plataforma está al nivel de los países desarrollados. Por medio de convenios con entidades de telefonía celular, las entidades financieras utilizan la interconexión móvil para avisar al beneficiario sobre la disponibilidad de fondos en su cuenta, la misma que se registra como una transferencia doméstica en los libros contables del banco. No dispone de una regulación específica para este tipo de servicios.

- México: A parte de la banca por internet y la masificación de red de cajeros automáticos, brinda dos tipos de servicios, el primero referido a la banca móvil a través de la implementación del servicio de Smartphone mediante el cual efectúan consulta de saldos, transferencia de

recursos o pago de créditos o servicios, y el segundo relacionado con pago móvil, servicio que está sustentado en la tenencia de una cuenta bancaria, la cual está asociada a un número telefónico y que permite efectuar transacciones desde y hacia otro teléfono móvil. A través de circulares del Banco de México y de la ley de Instituciones de Crédito se regula este servicio, estableciéndose que la entidad bancaria es la responsable de la seguridad en las transferencias y la captación de recursos.

- Perú: La banca electrónica consiste en la realización de operaciones bancarias a través del internet y de teléfonos celulares. Si bien no existe una normativa específica, la Superintendencia de Bancos, Seguros y AFP, a través de circulares define los niveles de intensidad en la relación cliente - banco, la misma que es aplicable también a monederos y dinero electrónico..

- Uruguay: Es ofertado por una entidad de intermediación financiera, la cual mediante los servicios de banca por internet y banca móvil permite efectuar operaciones como: consulta de saldos y movimientos de cuentas, consulta de saldo en tarjeta de crédito, consulta de cuenta de inversiones, pago de tarjetas de crédito, recarga de tarjetas pre pagadas, transferencia entre cuentas propias y con terceros pre contratados, recarga de minutos para celular, consulta de cotización de moneda extranjera y bloqueo de tarjeta de débito. No disponen de una normativa específica y siguen los lineamientos dispuestos en la normativa para bancos.

V. Banca Electrónica en El Salvador

Gracias a la introducción y el desarrollo de la tecnología en El Salvador, en los últimos años se ha registrado un incremento en la oferta y uso del servicio de banca electrónica, lo que ha permitido al cliente y usuario conocer sus saldos de cuentas o hacer transacciones, obtener información personalizada, tener facilidad de compras y permitir una interacción activa con las entidades financieras.

El incremento y mejora de servicios de banca por celular, internet, tarjeta de débito/crédito, cajeros automáticos o banca móvil, han agilizado la atención de los clientes y público en general, permitiendo al usuario ahorrar tiempo y acceder a una variedad de servicios operativos y de control desde cualquier punto geográfico las 24 horas del día.

Hoy en día, es posible realizar desde la residencia, el trabajo o cualquier otro sitio todas las operaciones que antes requerían la presencia física del cliente en la agencia o efectuando una llamada al banco como: monitoreo y control de cuentas, hacer transferencias y transacciones y pago de servicios básicos. Todo ello es posible desde una computadora o un dispositivo móvil, lo que ha vuelto eficiente la bancarización en el país.

Los servicios de banca electrónica ofertados por las entidades bancarias en nuestro país son: banca por internet, operaciones por POS, transferencias, pago de servicios, servicio de swift, back y front office, entre otros.

A nivel regulatorio en primera instancia, las entidades financieras pueden desarrollar y ofrecer servicios y productos de banca electrónica a partir de lo que permite la Ley de Bancos en el Art. 56 literal l) que dicta lo siguiente:

"Que los bancos podrán celebrar operaciones y prestar servicios con el público mediante el uso de equipos y sistemas automatizados, estableciendo en los contratos respectivos las bases para determinar las operaciones y servicios cuya prestación se pacte; los medios de identificación del usuario y las responsabilidades correspondientes a su uso; y los medios por los que se hagan constar la creación, transmisión, modificación o extinción de derechos y obligaciones inherentes a las operaciones y servicios de que se trate.

El uso de los medios de identificación que se establezca conforme a lo previsto en este literal, en sustitución de la firma autógrafa,

producirá los mismos efectos que los que las leyes otorgan a los documentos correspondientes y en consecuencia, tendrán el mismo valor probatorio; cuando estas operaciones se realicen mediante contratos de adhesión, los modelos de dichos contratos deberán ser previamente depositados en la Superintendencia, quien podrá, mediante decisión fundamentada, en un plazo no mayor a treinta días a partir de la fecha del depósito del modelo, requerir los cambios necesarios, cuando contengan cláusulas que se opongan a la legislación o cuando se consideren violatorios a los derechos del cliente. En todo caso el Banco estará obligado a explicar al cliente las implicaciones del contrato, previo a su suscripción".

Por otra parte, la Ley de Supervisión y Regulación del Sistema Financiero en los literales d) y g) del artículo 35 establece que:

"los directores, gerentes y demás funcionarios que ostenten cargos de dirección o administración en los integrantes del sistema financiero, están obligados a cumplir y velar porque las entidades adopten y actualicen políticas y mecanismos para la gestión de riesgos, debiendo entre otras acciones, identificarlos, evaluarlos, mitigarlos y revelarlos acordes a las mejores prácticas internacionales. En dichas políticas se deberán incluir las medidas que se adoptarán para prevenir posibles incumplimientos a requerimientos regulatorios y las que adoptarán en el evento de que haya incurrido en ellos, debiendo definir en ambas situaciones los parámetros que orientarán la actuación y los responsables de implementarlas. Asimismo, a las entidades se les exige el cumplimiento de un eficiente funcionamiento de los sistemas de registro, tratamiento, almacenamiento, transmisión, producción, seguridad y control de los flujos de información".

Por lo que, una Norma que regule la actividad de Banca Electrónica, deberá contemplar los aspectos legales anteriormente expuestos, más la aplicación de estándares internacionales que rigen los temas de seguridad informática en dicha actividad.

VI. Conclusiones

En la presente investigación se destaca que la banca electrónica ofrece ventajas para el consumidor en términos de comodidad, y para el proveedor en términos de reducción de costos y mayor alcance, sin embargo, el servicio en sí plantea una serie de riesgos, que preocupan a los reguladores y supervisores financieros, especialmente los relacionados con:

1. Riesgos operacionales.
2. Operaciones transfronterizas.
3. Protección de los clientes y la confidencialidad.
4. Competitividad y rentabilidad.

Cuestiones de riesgo operacional

El fácil acceso y disponibilidad de la tecnología mediante la arquitectura abierta de Internet expone a los sistemas de los bancos. La dependencia de estos en terceros proveedores coloca el conocimiento de sus sistemas en un dominio público y los deja en una situación vulnerable ante empresas relativamente pequeñas que tienen una alta rotación de personal. Además, hay ausencia de pistas de auditoría convencionales como también lo relativo al anonimato de las transacciones debido al acceso remoto. Es imperativo que la seguridad y la integridad de las transacciones estén protegidas de modo que el potencial para la pérdida resultante de actividades delictivas, como el fraude, el blanqueo de dinero, evasión de impuestos, entre otros, y una interrupción en los sistemas de suministro, ya sea por accidente o por diseño, se mitiguen. Las respuestas de supervisión para gestionar los asuntos de riesgo operacional incluyen el tema de la orientación adecuada sobre el riesgo (incluyendo riesgo de outsourcing) el control y el mantenimiento de registros, exigibilidad de las normas mínimas de la tecnología y de seguridad adecuadas para el ejercicio de la actividad transaccional, la extensión de "conozca a su cliente", reglas para las transacciones en Internet, y la insistencia en la divulgación apropiada y visible para informar a los clientes de los riesgos que enfrentan en hacer negocios en Internet.

En los próximos años, la tendencia es que muchos de estos riesgos provengan sobre todo de los dispositivos móviles, pues la alta

penetración de la telefonía celular promete acelerar la bancarización en buena parte de los países latinoamericanos. Pero para que ese potencial se concrete, las inversiones en seguridad en los sistemas deberán cobrar un impulso aún mayor.

En lo relativo a cuestiones transfronterizas

La banca electrónica no tiene fronteras, y los bancos pueden ser fuente de depósitos de jurisdicciones en la que no tienen licencia o no ser supervisados y tener acceso a los sistemas de pago. Los clientes pueden potencialmente parquear sus fondos en jurisdicciones en las que las autoridades nacionales no tienen acceso a los registros. Las cuestiones de jurisdicción, la territorialidad y el recurso se vuelven aún más borrosa en el caso de los bancos virtuales. Cuestiones transfronterizas también entran en juego cuando los bancos deciden ubicar sus centros de procesamiento, registros o copias de seguridad en diferentes jurisdicciones.

La protección de los clientes y las cuestiones de confidencialidad:

La pérdida de la confidencialidad del cliente puede suponer un riesgo para la reputación de los bancos y el sistema financiero en su conjunto. Realizar transacciones comerciales en Internet expone los datos que se envían a través de Internet a la interceptación por parte de agentes no autorizados, que podrán luego utilizar los datos sin el consentimiento de los clientes. También se ha producido la incidencia, donde los fallos se han desarrollado en los sitios web que permiten a los clientes acceder a las cuentas de cada uno. Para hacer frente a estos riesgos, los clientes necesitan ser educados a través de la divulgación adecuada de estos riesgos.

Cuestiones de competitividad y rentabilidad:

Aunque se espera que la banca electrónica pueda reducir sustancialmente el costo de hacer transacciones en el largo plazo, el limitado negocio está haciendo que en internet se tenga que pagar por la infraestructura en la que los bancos han invertido. Esto incluye las alianzas con empresas de tecnología en la creación de vías de pago, portales y soluciones de Internet (aplicaciones móviles). Sin embargo, los próximos años pueden acudir a un escenario en el que los márgenes de los bancos convencionales se ven presionados por la competencia de la banca electrónica. Estas cuestiones tienen que ser tomadas en cuenta por las autoridades financieras mientras se decide el enfoque regulatorio de banca electrónica.

Por último, el automatizar y tecnificar electrónicamente la banca en el país ha permitido a las entidades financieras ofrecer mejores, rápidos y seguros servicios que se adaptan a las necesidades de los clientes, sin importar el tiempo y lugar geográfico en el que se encuentren, proporcionando un acceso continuo y permanente a las operaciones financieras y disminuyendo sus costos operativos.

La innovación y mejora en los servicios financieros posibilita que las entidades proporcionen un valor agregado a sus clientes, permitiendo que la población pueda acceder a una variedad de servicios financieros sin tener que aproximarse a un determinado punto de atención físico para realizar sus transacciones, lo que conlleva también al fortalecimiento del proceso de bancarización dentro del país.

Es deseable que todos los bancos, que proponen ofrecer servicios transaccionales a través de Internet obtengan al menos la no objeción de sus modelos de negocios, a través de esta modalidad, de las autoridades financieras correspondientes antes de iniciar estos servicios. La solicitud del banco para tales permisos debería indicar, al menos, su plan de negocio, análisis de costo y beneficio operacional, ajustes a realizar como la tecnología adoptada, socios comerciales y de servicios de terceros, los proveedores y los sistemas y procedimientos de control del banco que propone adoptar para la gestión de riesgos, entre otros. La regulación relativa a esta actividad es conveniente que incluya aspectos de remisión de información a la autoridad supervisora, así como cualquier cambio material en los componentes, servicios y productos relacionados a la banca electrónica que ella ofrece.

Referencias Bibliográficas

Basel Committee on Banking Supervision, (July, 2003): "Management and Supervision of Cross-Border Electronic Banking Activities"

Basel Committee on Banking Supervision, (October, 2000): "Electronic Banking Group Initiatives and White Papers"

Basel Committee on Banking Supervision, (June, 2011): "Principles for the Sound Management of Operational Risk".

Basel Committee on Banking Supervision, (July, 2003): "Risk Management Principles for Electronic Banking".

Comité de Supervisión Bancaria de Basilea, (Marzo, 1998): "Gestión de Riesgos para la Banca Electrónica y Actividades con Dinero Electrónico".

Comité de Supervisión Bancaria de Basilea, (Febrero, 2003): "Buenas prácticas para la gestión y supervisión del riesgo operativo".

Comité de Supervisión Bancaria de Basilea, (Enero, 2014): "Adecuada gestión de los riesgos relacionados con el blanqueo de capitales y la financiación del terrorismo".

Claudia Casas. FELABAN, (2011) "Operaciones y prestación de Servicios de Banca Móvil".

Revista BNAMERICAS, (Julio 2012) "Las TI y su papel en seguridad bancaria".

Ley de Supervisión y Regulación del Sistema Financiero, contenida en Decreto Legislativo número 592, publicada en el Diario Oficial número 23 Tomo 390 de fecha 2 de febrero de 2011.

Ley de Bancos, contenida en Decreto Legislativo número 697, publicada en el Diario Oficial número 181 Tomo 344 de fecha 30 de septiembre de 1999, con su última reforma contenida en Decreto Legislativo número 592, publicada en el Diario Oficial número 23 Tomo 390 de fecha 2 de febrero de 2011.

Observatorio Móvil de América Latina (2011): "Impulsando el desarrollo económico y social a través de la banda ancha móvil". www.wirelessintelligence.com