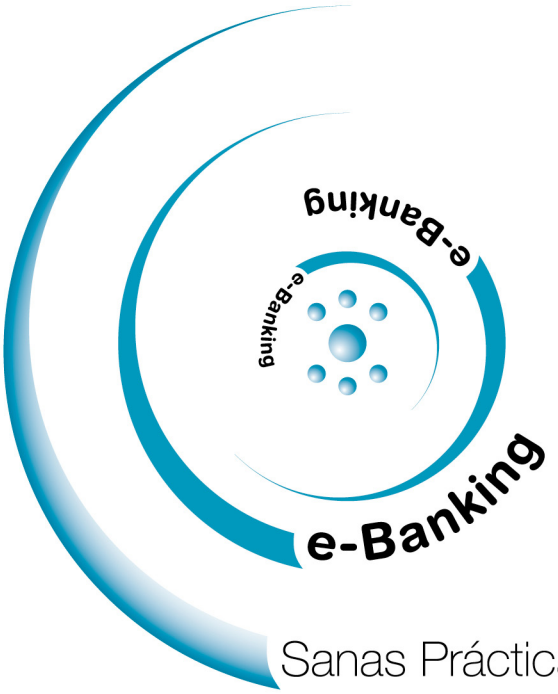
Banco Central de la República Argentina
Superintendencia de Entidades Financieras y Cambiarias
Comisión de e-Banking



Sanas Prácticas

Enero
2003

Introducción

Este documento intenta interiorizar a sus lectores sobre la realidad actual de la Banca Electrónica y por Internet en el entorno financiero. Para ello, se ha ordenado de forma tal de proveer al nivel gerencial de conceptos que ayuden al entendimiento de las tecnologías que se encuentran directamente relacionadas con estos servicios, una aproximación al análisis de los riesgos asociados a las operaciones involucradas y por último, sin pretender ser una guía a seguir en cuanto a seguridad informática, una serie de conceptos y lineamientos generales para su administración.

Se espera que el presente trabajo permita el acercamiento de los niveles no especializados técnicamente a los principales conceptos y aspectos de e–Banking, poniendo énfasis en la difusión de los desafíos de administración del riesgo de estas actividades a nivel del Directorio y la Gerencia.

No se pretende definir conceptos técnicos específicos o brindar estándares relativos a e–Banking, especialmente considerando que corresponde a las entidades analizar en profundidad la naturaleza de estas actividades y el impacto en su perfil global de riesgo, así como evaluar las acciones más adecuadas para su gerenciamiento en un entorno con rápidos cambios.

Asimismo, es deseo de esta comisión brindar a las entidades un canal de comunicación que permita en el futuro hacerles llegar actualizaciones y/o avisos sobre novedades y documentación relevante. Las entidades interesadas en acceder a la información antes mencionada podrán dirigirse a la dirección de mail: **comision.ebanking@bcra.gov.ar**

Integrantes de la
Comisión de e–Banking
Superintendencia de Entidades Financieras y Cambiarias
Banco Central de la República Argentina

Dr. Rubén Marasca
Subgerente General de Análisis y Auditoría

Dr. Marcelo D. Fernández
Gerente de Auditoría Externa de Sistemas

Dra. Silvia Núñez
Inspectora General de Control de Auditorías

Lic. Marcelo H. González
Inspector General de Auditoría Externa de Sistemas

Lic. Carlos A. Bianco
Inspector de Auditoría Externa de Sistemas

Indice

Breve descripción de la evolución de los entornos tecnológicos de procesamiento 9

Canales electrónicos 11

Internet 13

La evolución de la Banca Electrónica 15

Riesgos en e–Banking 29

Administración del riesgo 37

Controles internos de tecnología en e–Banking 41

Sanas Prácticas 45

Conclusiones finales 57

Glosario 59

Fuentes de documentación 61

Breve descripción de la evolución de los entornos tecnológicos de procesamiento

Etimológicamente, "tecnología" se define como arte de la generación; por extensión, se concluye que "tecnología informática" se considera al arte de la generación de servicios de información y telecomunicaciones. Estos servicios deberán ser controlados en forma íntegra, adecuada y eficiente.

Durante las décadas del 70 y 80, los riesgos de Tecnología Informática (T.I.) se reducían al espacio físico del centro de procesamiento de datos. En esas décadas, la ventaja determinante del procesamiento era la rapidez en la generación de información contable versus la convivencia con registros contables manuales.

Se verificaba una casi inexistente segregación de responsabilidades en la prestación de los servicios de análisis, diseño, programación, operación, gerenciamiento y seguridad informática, siendo el principal usuario de dichos servicios el personal interno de la entidad, y no se evidenciaba la existencia de sistemas de información de gestión.

Con el advenimiento masivo a mediados de la década del 80 de redes de microcomputadores LAN (Local Area Network) en nuestro país, el inicio del cableado y la conectividad a través de dispositivos de comunicación aún rudimentarios, se ampliaron los riesgos de seguridad física y lógica existentes.

En ese momento comenzaron a surgir evidencias de una clara separación de responsabilidades entre administración de seguridad, desarrollo y programación. La ventaja determinante en esta etapa fue la reducción de tareas por la distribución de las redes para la realización de labores de oficina y complementarias al procesamiento central.

Seguidamente, comenzó la complementación de datos compartidos entre el "host" central y los microcomputadores interconectados, disminuyendo en forma paulatina la existencia de registros contables manuales y ampliándose la índole y cantidad de usuarios de los servicios de procesamiento dentro del personal interno de la entidad.

A fines de la década del 80 se produjo un cambio estructural de los entornos de T.I. con el despegue de las telecomunicaciones globales.

Durante la década del 90 se hizo masiva la creación de redes WAN (Wide Area Network), iniciándose la convivencia de la antigua arquitectura "host", cuyos datos estaban físicamente centralizados, con una nueva arquitectura "cliente / servidor", donde un servidor (lugar donde se localizan los datos) distribuye a quien lo solicite los datos que se actualizan en una gran base. De esta manera, se modifica la filosofía tecnológica de "archivo físico" a una nueva filosofía definida como "base de datos".

Este momento determina el inicio de la comunicación satelital masiva. Con la reducción notoria del cableado, la conectividad pasa a tener un rol principal. Se generan auditorías especializadas, se determinan nuevos objetivos de control, se observa una mutación de los perfiles de riesgo tradicionales, y se incrementa la importancia relativa de la seguridad informática.

La existencia de registros contables totalmente manuales sólo es aceptable bajo condiciones contingentes, y fundamentalmente se amplía la índole, cantidad y conocimientos de usuarios de los servicios de procesamiento dentro y fuera de la entidad financiera, avanzando en la implementación de nuevas técnicas de administración, gerenciamiento y sistematización de la información de gestión para la toma de decisiones.

Internet, ideado en la década anterior, surge en nuestro país a principios de la década del 90. Este suceso, y la proliferación de diversos recursos tecnológicos que han sido los facilitadores de la integración de los procesos de negocio (computación portátil, computación móvil y otros) conlleva a una evolución continua del área de tecnología informática, mejoran las comunicaciones locales y se integran a las telecomunicaciones globales, generando un solo conjunto heterogéneo de las distintas conectividades, redes y arquitecturas mencionadas.

Canales electrónicos

Se entiende por canal electrónico al conjunto de dispositivos tecnológicos, que permiten una interfase con el cliente, posibilitando el transporte de información y una comunicación remota de dicho cliente con el ambiente de tecnología de información del banco para la generación de transacciones.

Debe considerarse que no importarán las características del canal electrónico en particular, sino que las transacciones sean imputadas "online", a una base de datos común y con dígitos identificatorios únicos, que distingan cuál ha sido el canal utilizado para su concertación.

Dentro de los canales electrónicos relevantes se encuentran:

PC Banking

Si bien su uso se encuentra en retroceso, este canal se conforma de un aplicativo desarrollado por la entidad, que le permite al cliente el acceso a su información financiera, consultas y transferencias.

El cliente debe poseer un "modem" y una línea telefónica. Presenta como ventaja que el usuario puede bajar la información necesaria y trabajar "off line". Su desventaja es el mayor costo para el cliente por mantenimiento, distribución e implementación de nuevas versiones de la aplicación.

Banca Telefónica

En la actualidad, este canal es el más utilizado por los clientes para realizar operaciones financieras. Es altamente dependiente de la tecnología de comunicaciones: la mayoría de las llamadas se envían a contestadores inteligentes, sin necesidad de instalación de "call centers" físicos.

Es la alternativa ideal para aquel cliente que no posea otros canales, al no requerir un software para acceso a los productos o actualizaciones. Es de fácil acceso y de bajos costos transaccionales en relación con la banca física.

Cajero Automático (ATM)

Canal electrónico conformado por un dispositivo que, conectado a una red propietaria, envía y recibe información de un computador central que lo identifica y procesa.

Este canal ha tenido un crecimiento exponencial durante los últimos años. Puede conectarse directamente a entornos de procesamiento centrales o a sistemas de sucursales.

Tanto el hardware como el software se implementan de forma modular, por lo que su actualización no requiere la sustitución de la unidad. Esto permite un costo de mantenimiento reducido y puede ser configurado remotamente.

Su utilización supone un ahorro en personal e incluso en el número de oficinas bancarias, y en la actualidad, las entidades los utilizan como una importante herramienta de marketing.

Video kiosco

Sistema interactivo, que permite al cliente ver y comunicarse con un gestor del banco a través de video y monitor.

Si bien éste canal aún no ha avanzado en nuestro país, se le augura un prometedor futuro, debido a su capacidad para atraer un alto número de usuarios y a sus bajos costos relativos.

Tarjetas inteligentes

Si bien su uso aún no está instalado en nuestro país, se trata de tarjetas multifuncionales que, incorporando un microprocesador, podrán abarcar distinta información del titular de las cuentas; dentro de ellas cabe destacar el "monedero electrónico" (e-Money).

E.D.I. (electronic data interchange)

Este canal permite el intercambio de información entre empresas de manera segura. Las empresas pueden ser pymes o corporativas, con tecnologías distintas pero compatibles entre sí.

Actualmente su principal servicio es el de intercambio de facturas, órdenes de compra, etc., y su comunicación se establece sobre líneas privadas o redes propietarias.

Muestra como ventaja la reducción de los tiempos de gestión y los costos de producción, y como debilidades, que el número de empresas que utilicen este canal deberá ser masivo para lograr una mayor eficiencia, situación que en la actualidad no se presenta.

Para grandes clientes, ciertas entidades financieras ponen a disposición este canal electrónico a través de la instalación del hardware y software necesarios para la conexión interna de dichos clientes con el centro de procesamiento de datos de la entidad.

P. o. S. (point of sale)

Dispositivo utilizado para la automatización en grandes comercios minoristas. Tiene como objetivo facilitar la venta al consumidor. En general se lo utiliza como "input" de transacciones comerciales con tarjetas de crédito/débito.

Tiene la ventaja de reducir el tiempo de aprobación de la transacción comercial, y como debilidad, los problemas de seguridad, disposición física y confidencialidad.

Banca Móvil (m–Banking)

Este canal puede ofrecer diversos servicios a través de celulares, "handies" y "pagers"; puede ser utilizado como receptor de mensajes financieros, y como un canal de soporte de tecnología "sin cable" que le permitirá al cliente operar vía Internet, pudiendo conformar lo que se denomina en la actualidad como PAN (Personal Area Network – Red de Area Personal).

Su principal ventaja es la facilidad otorgada por la movilidad, y su debilidad, similar a la banca telefónica, es su gran dependencia de la homogeneización global de los avances de las comunicaciones.

Internet banking

Puede definirse como el conjunto de servicios utilizados por los clientes, a fin de acceder a sus cuentas y a cualquier otra información o producto ofrecido por las entidades financieras, mediante el uso de herramientas informáticas, a través del canal de Internet.

Internet

Internet tiene sus orígenes a comienzos de la década del '70, como una red denominada Arpanet, establecida por la Agencia de Proyectos de Defensa de los EE.UU.

A finales de esa década surgieron otras redes globales, como la UUCP (Unix to Unix Copy Protocol), que era un conjunto de miles de computadoras Unix. Ya en la década del 80 aparecen mega redes como Bitnet, Csnet y otras.

Este conjunto de redes privadas (Cerfnet, Bitnet), gubernamentales (Arpanet, Nsfnet, Scnet) y otras (UUCP), iniciaron un proyecto conjunto y llegaron a ser conocidas como *INTERNET*, mediante un proyecto que se inició en la National Science Foundation (NSF), la cual creó una red de supercomputadores conectados a lo largo y ancho de EE.UU., siendo los usuarios iniciales científicos e investigadores. La red de alta velocidad que conectó la NSF fue el embrión de Internet en EE.UU.

Actualmente se configura en "links" (conexiones) de alta capacidad, usando líneas telefónicas, microondas, láser, fibra óptica y satélites conectados a redes, sitios computarizados y usuarios a través del mundo.

También se consideran sus orígenes en 1989, en un laboratorio Europeo de Física de Partículas (CERN). Los investigadores querían un método único que realizara la actividad de encontrar cierta información, la trajera a la computadora, y les permitiera ver algún documento y/o gráfico a través de una interfase única, eliminando la complejidad de diversas herramientas.

Cuando Internet se hizo visible más allá de las comunidades científicas y de investigación, un grupo de compañías privadas, proveedoras de distintos servicios, consideró su existencia.

Estos proveedores son los que a fines de la década del 80 construyeron la gran mayoría de líneas de entrada a la comunicación de los usuarios de Internet.

A finales de 1990, los investigadores ya tenían "browsers" (navegadores de Internet) en modo texto y muy pocos en modo gráfico.

En 1992 se difunden para el público en general y a medida que fueron avanzando, se agregaron interfases a otros servicios, entre ellos los bancarios.

La comunidad de Internet adoptó rápidamente esta herramienta y comenzó a crear sus propios servidores de www (World Wide Web) para publicar información.

A finales de 1993 los "browsers" se habían desarrollado para una gran variedad de computadoras y sistemas operativos, y desde allí a la fecha, la Web es una de las formas más populares de acceder a los recursos de la red.

Para acceder a la Web se debe ejecutar en la computadora cliente un "browser": ésta es una aplicación que sabe cómo interpretar y mostrar documentos hipertextuales. Un documento hipertextual es un texto que contiene vínculos con otros textos, gráficos, sonido, video y animaciones.

Cuando recuperamos un documento de la Web, este es con formato y puede ser visto en distintas computadoras. Para asegurar una adecuada imagen existe un formato o lenguaje llamado HTML (Hiper Text Mark-up Language), que es un conjunto de instrucciones sencillas que indican como se estructura ese documento. El "browser" interpreta los comandos HTML y presenta el documento formateado para su visión por el usuario.

La Web convierte el acceso a Internet en algo sencillo para el público en general, lo que permitió que experimentara un crecimiento explosivo.

Es relativamente sencillo recorrer la Web y publicar información en ella. Las herramientas de la Web crecieron a lo largo de los últimos años hasta ser las más populares.

La Web permite unir información que está en un extremo del planeta con otra que se encuentra en lugar distante a través de algo que se denomina hipervínculo. Al hacer "click" sobre éste, nos comunica con el otro sector del documento o con otro documento en otro servidor de información.

Las autopistas de información serán el soporte principal en el futuro de la banca electrónica.

Los principales problemas a evaluar en Internet se basan en la seguridad de las transacciones económicas, afectando elementos fundamentales como los pagos seguros y la confidencialidad de las transacciones.

Actualmente, se están desarrollando herramientas de seguridad para la Red, basadas en sistemas que permitan que los códigos secretos y los números de tarjetas no circulen por la misma, o si lo hacen, sea en forma segura y confidencial.

Con la banca electrónica se pueden prestar servicios de valor agregado que compensen los estrechos márgenes financieros. De igual manera, se plantea el reto de reducir los costos para los clientes menos rentables. Esto implica la ejecución de estrategias para todos los nuevos perfiles que se presenten sobre los riesgos tradicionales.

La evolución de la Banca Electrónica

Entendemos por *Banca Electrónica* al conjunto de facilidades concedidas por las entidades financieras a sus clientes mediante distintos canales electrónicos, a fin de acceder remotamente a los servicios y productos ofrecidos.

El desarrollo de nuevas tecnologías enfrenta a las entidades financieras en un entorno competitivo radicalmente distinto del precedentemente conocido.

La banca a distancia facilita el acceso a las operaciones y disminuye los costos operativos. Con esto se consiguen dos objetivos: mayor comodidad para el cliente y reducción de costos de la administración global de las entidades financieras.

Tiempo atrás, el papel predominante en la captación de clientes era la distribución geográfica. En consecuencia, la sucursal bancaria se consideraba como elemento competitivo fundamental.

Actualmente, la sucursal bancaria está perdiendo peso como único punto de referencia en la distribución bancaria y tiende a ser cada vez más pequeña. Por lo tanto, deja de ser interesante la concentración geográfica.

Una de las misiones de los bancos consiste en ser capaces de anticiparse a los futuros hábitos de compra de los clientes.

La idea de que el cliente bancario valora el contacto personal, va quedando matizada en el sentido de que valora preferentemente el servicio personalizado antes que dicho contacto, siendo los clientes de renta alta y los más jóvenes los que más valoran el precio y la rapidez.

La banca electrónica deberá ser considerada como un nicho de mercado y como un intento de anticipación a los cambios que se están produciendo.

El principal riesgo de la anticipación en banca electrónica es equivocarse con la tecnología escogida o errar en el “timing”.

El éxito de la banca electrónica va a depender cada vez más de la capacidad de la entidad financiera para ofertar sus productos de forma eficiente y eficaz, ofreciendo operaciones sencillas, que puedan resultar de uso masivo, pues las elevadas inversiones en tecnología llegan a ser rentables sobre la base de un alto número de clientes y de transacciones.

Un riesgo crítico que plantea la banca a distancia en las entidades financieras, desde el foco de estrategia comercial, es que se produzca una sobreoferta y superposición de productos, al venderse a través de diferentes canales de distribución con objetivos similares.

También, dependiendo del medio tecnológico que la entidad financiera utilice para proyectarse al exterior, pueden surgir distintos riesgos desde el punto de vista de la estrategia operacional.

Actualmente, en la Argentina, la banca a distancia se utiliza únicamente como complemento a los canales de distribución tradicionales.

Para conseguir la complementariedad de los distintos canales, el banco deberá hacer un esfuerzo para formar a sus empleados, transmitir correctamente a los clientes las ventajas de estas nuevas modalidades, manejar adecuadamente los riesgos tradicionales y los nuevos perfiles que presentan éstos, y establecer prácticas y procedimientos para utilizar los canales emergentes.

En el futuro, la banca deberá contar con múltiples puntos de acceso para los clientes, sin importarle tanto dónde se encuentren sino su disponibilidad a través de los diferentes medios: el usuario valorará menos el hecho de tener un banco cerca, que el saber que puede acceder a los servicios del banco en cualquier momento.

Se buscará una mayor satisfacción del cliente, y la captación de nuevos clientes mediante el abaratamiento del producto virtualizado, y de esta forma se irá introduciendo masivamente el canal de comunicación con el banco convencional, por medio de Internet y de los diferentes dispositivos y canales electrónicos que permitan su integración.

Como ejemplo, cada transacción efectuada a través de cajero automático se estima como un tercio del costo que supondría su ejecución por un

empleado. Con los nuevos dispositivos se sugiere un ahorro mucho mayor, dada la transferencia de los costos tecnológicos de los puntos de consulta a los clientes, pues en muchos casos estos dispositivos son de propiedad de los mismos clientes y se utilizan para fines variados.

Los nuevos canales de distribución electrónica conducen hacia el micromarketing, basado en la capacidad tecnológica de cada grupo de clientes, a quienes se les remite la información segmentada que conduzca a la satisfacción de sus necesidades concretas.

Esta tendencia puede verse incrementada por la creciente desintermediación y por la menor importancia de las fronteras, pudiendo aparecer ofertas segmentadas por diversos motivos: culturales, religiosos, ideológicos u otros de índole similar.

Crecimiento de e–Banking

Existen numerosos factores de mercado que están motivando a las entidades a evaluar su tecnología y analizar profundamente los efectos de la incorporación de productos y servicios relacionados con e–Banking y comercio electrónico en la definición de sus estrategias. Entre dichos factores del mercado se incluyen:

La competencia

Los estudios muestran que la presión competitiva es la fuerza conductora del uso creciente de tecnología de e–Banking, posicionándose delante de la reducción de costos y del acrecentamiento de las ganancias. Los bancos ven al e–Banking como un camino estratégico para mantener los clientes existentes y atraer a los nuevos.

Eficiencia de costos

Las entidades financieras tienen la posibilidad de entregar los distintos servicios de e–Banking a un costo transaccional menor que el de las sucursales “de ladrillos” tradicionales.

Los costos actuales para ejecutar una transacción variarán dependiendo del canal de entrega utilizado.

Los bancos tienen importantes razones para desarrollar tecnologías que permitan asistir en la entrega de productos y servicios bancarios mediante los canales más rentables.

El Directorio deberá incluir en sus decisiones el desarrollo y la revisión continua de los costos asociados con un nuevo producto o servicio, incluyendo tecnología informática, marketing, mantenimiento, y funciones de soporte al cliente. Esto ayudará a que la gerencia lleve a cabo una adecuada administración, tome decisiones con más información y mida el éxito de su emprendimiento comercial.

Alcance geográfico

El e–Banking permite expandir el contacto con el cliente a través de un mayor alcance geográfico y canales de entrega a costo más bajo.

Un punto crítico a considerar por parte del management será definir cuál es la combinación óptima entre operación virtual y sucursal física “de ladrillos” tradicional.

Demografía del cliente

El e–Banking permite a las entidades financieras ofrecer un amplio rango de opciones a sus clientes.

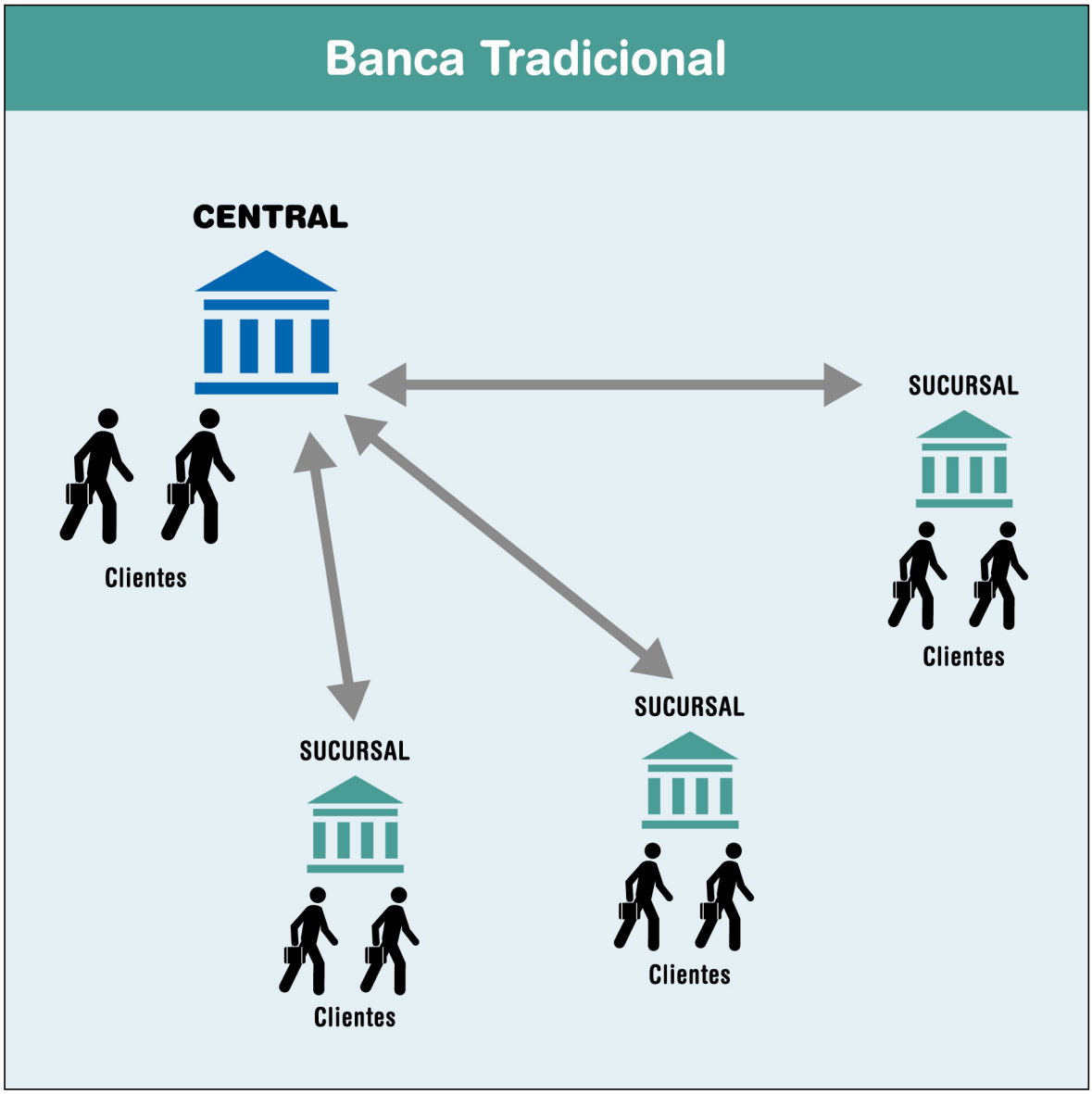
Algunos de ellos confiarán en las sucursales tradicionales para conducir sus negocios bancarios, considerando que ésta es la forma más segura de concretarlos o privilegiando el contacto personal.

Otros usuarios han adoptado en forma temprana las nuevas tecnologías que llegan al mercado. Estos clientes fueron los primeros en obtener computadoras personales y los primeros en emplearlas en la conducción de sus negocios.

La demografía de dichos clientes se mantiene en un proceso de mutación continuo. El desafío actual para las entidades financieras es evaluar y comprender la integración de su base de clientes y encontrar la mejor combinación de canales para entregar los productos y servicios en forma segura y rentable para sus diferentes segmentos del mercado.

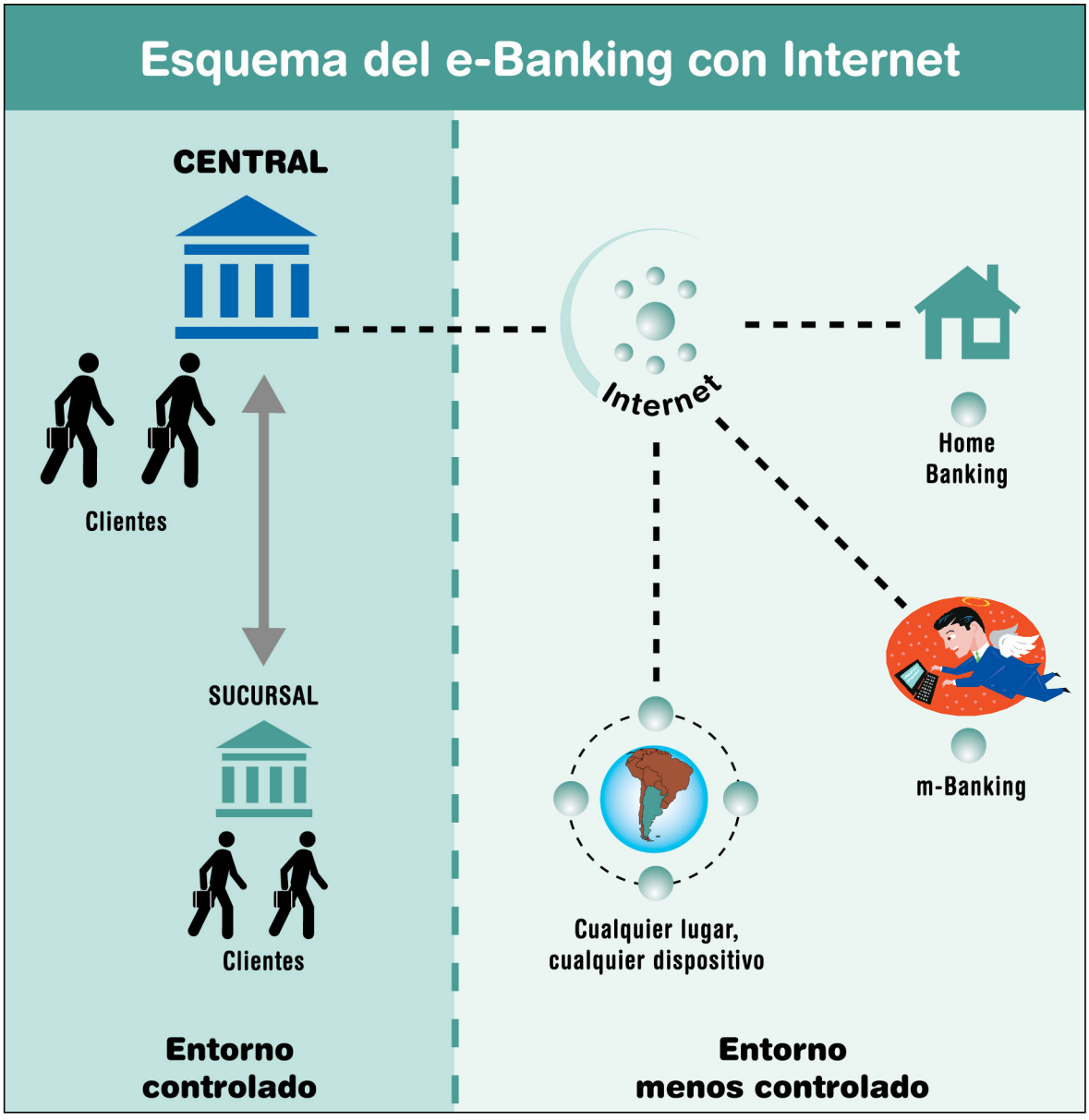
Esquema tradicional del e–Banking

Dentro del esquema tradicional del e–Banking, las entidades financieras establecen las relaciones comerciales con sus clientes dentro de un ambiente controlado, ya que tanto su sede central como las sucursales son el ámbito natural donde los clientes se desenvuelven.



Esquema del e–Banking con Internet (Internet Banking):

Dentro del esquema de e–Banking con Internet las entidades financieras pierden el control fehaciente de los puntos en donde se establecen las relaciones comerciales con sus clientes, y además es muy difícil mantener un esquema de control de todos los actores (intermediadores de Internet) que intervienen.



e–Banking en Argentina

En la actualidad, la mayoría de las entidades financieras en el país cuentan con alguna clase de presencia de e–Banking por medio de Internet. No obstante, no muchas son las que han implementado las mismas alternativas de negocio sobre la Web como las que poseen en su sucursal tradicional.

Se evidencia que el crecimiento que se ha presentado en los últimos años, tanto en volumen como diversificación de canales electrónicos alternativos, ha sido, comparativamente, muy importante.

Hoy, en Argentina, podemos encontrar una importante provisión de servicios bancarios sobre Internet. Al mismo tiempo, se observa un mayor grado de tecnificación en los mecanismos de atención a los clientes en las mismas sucursales bancarias tradicionales. Estas dos situaciones, en algunos casos, han provocado una disminución de la dotación de personal de atención en las entidades.

Existen bancos que incentivan la utilización de los distintos canales electrónicos, sean internos en las sucursales o externos a ella, mediante un cargo adicional al cliente cuando éste realiza sus transacciones en el mostrador tradicional de la entidad.

Se espera que este desarrollo de canales alternativos vaya en aumento a medida que bajen los costos de las tecnologías actuales, y aparezcan nuevos dispositivos portables con capacidades de conexión a las infraestructuras tecnológicas de las entidades financieras.

Actualmente, un conjunto de entidades financieras permiten realizar consultas y transferencias, por medio de los navegadores Web, de los teléfonos celulares "WAP" y de los dispositivos "Palm". La mayoría de las que poseen presencia en Internet permiten la realización de consultas de diversa índole sobre cualquier dispositivo portable con capacidad de navegación Web.

Los servicios que generalmente se ofrecen son:

- Consulta del estado de cuentas.
- Pagos de servicios (e-Pagos).
- Pagos de tarjetas de crédito (e-Pagos).
- Transferencia entre distintas cuentas.
- Concertación de certificados de plazo fijo.
- Solicitudes de chequeras.
- Consulta, simulación y/o inicio de adjudicación de préstamos.
- Compra de acciones, bonos u otros papeles.

Visto desde el ámbito de la seguridad de dichas operatorias, la utilización de firmas digitales y certificados digitales enmarcados en la ley 25.506 es uno de los principales elementos que fortalecen el esquema.

Sitios de e–Banking

La comprensión de los distintos productos de e–Banking existentes en el mercado permitirá identificar los riesgos inherentes involucrados.

Actualmente, las denominaciones clásicas empleadas para designar las diversas clasificaciones de sitios de servicios son:

- ***Sitios que proveen sólo información:***

  Este es un nivel básico, en donde la entidad financiera brinda información sobre productos y servicios a través de un servidor aislado de la red (stand alone).

  El riesgo es relativamente bajo, dado que en general el sistema de información no pasa a través de la red interna.

  Este nivel puede ser provisto por el banco o estar tercerizado.

  Mientras que el riesgo para el banco es bajo, el servidor y/o el sitio web son susceptibles de intrusión, por lo tanto deben aplicarse controles para prevenir alteraciones no autorizadas sobre los mismos.

- ***Sitios de intercambio de información:***

  Esta clase de sitio permite cierto grado de interacción entre los clientes y los sistemas del banco. Dicha interacción puede estar limitada al correo electrónico, solicitud de saldos de las cuentas propias, aplicaciones de préstamos, actualización de datos por cambios de dirección y otros.

  Dado que se accede a la información mediante la red interna de la entidad, el riesgo se incrementa, por lo tanto serán necesarios mecanismos tendientes a prevenir, monitorear y alertar al administrador de los intentos de acceso no autorizados a la red interna.

  El control de virus se convierte en un factor crítico en este entorno.

- ***Sitios transaccionales:***

  Este nivel permite a los clientes realizar operaciones transaccionales. Se parte de la existencia de un pasaje del requerimiento desde el servidor hacia la red interna; por lo tanto, se deberán aplicar los controles más estrictos, dado que las transacciones incluyen pago de servicios, acceso a las cuentas, transferencias de fondos y otros.

- ***Banca Virtual:***

  Se deja de lado la concepción tradicional del banco de “ladrillo” y se adopta la estrategia de conducir las operaciones únicamente a través de Internet.

  En este caso, se amplía la magnitud de los riesgos inherentes, y su control requiere el desarrollo de nuevas herramientas y procedimientos aplicables a operatorias virtuales, cuyas condiciones contractuales escapan a las prácticas de mercado.

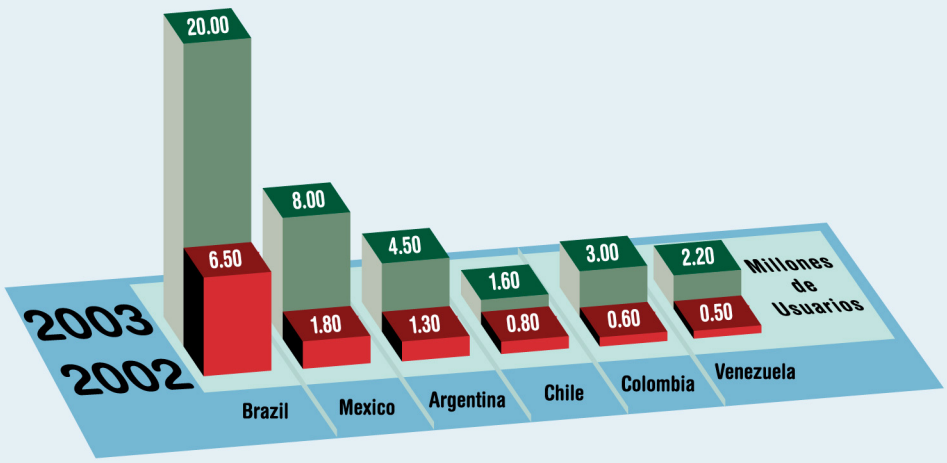
Las Entidades Financieras Argentinas y su relación con los sitios de e–Banking y el ente regulador

Dado que los servicios bancarios ofrecidos a través de Internet aún se encuentran en los estadios iniciales de masificación, el Banco Central de la República Argentina entiende que no sería apropiado recomendar estándares normativos que potencialmente pudieran restringir la innovación tecnológica.

Con el avance del proceso y la criticidad de los objetivos de control se estudiará la necesidad de contar con la regulación pertinente para cada uno de ellos.

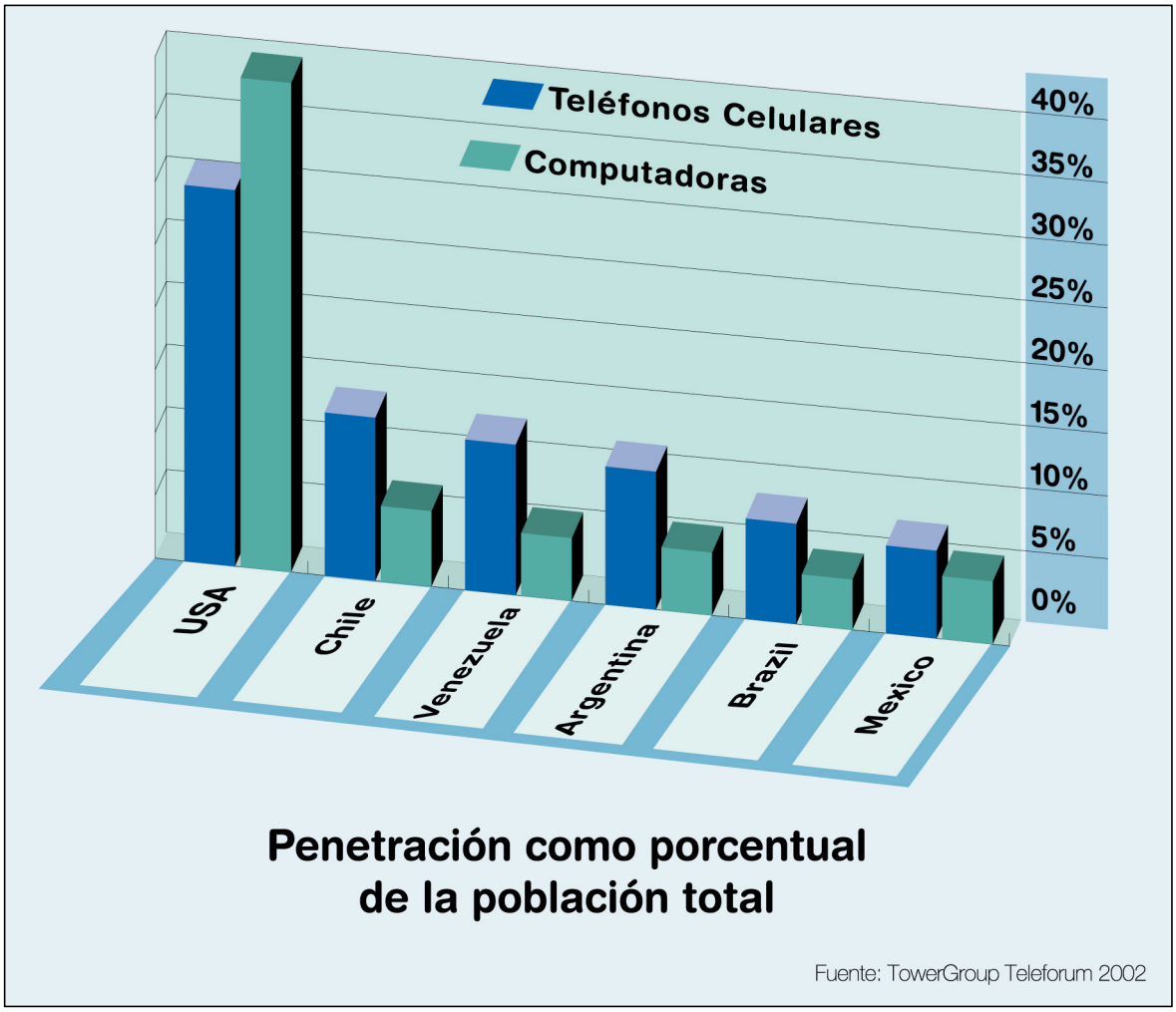
En consecuencia, las acciones futuras estarán orientadas a facilitar la continuidad del análisis y el diálogo que eventualmente conducirá al desarrollo de herramientas de supervisión para las actividades de Internet Banking.

La existencia de estándares razonables de supervisión y administración deberá permitir una conducción segura y adecuada de las actividades, sin obstaculizar la innovación y la competencia que beneficiarán tanto a la industria bancaria como a sus clientes.



Proyección del Crecimiento de Internet en América Latina

Fuente: TowerGroup Teleforum 2002



Comercio electrónico por Internet (e–Commerce)

Para realizar un análisis del *comercio electrónico*, resulta conveniente centrar el estudio en uno o dos subsectores, tal como se efectúa en cualquier industria. No obstante, en el tema que nos ocupa existen varios modelos de negocios que se cruzan entre sí, junto a diversas vinculaciones y transacciones intersectoriales que permiten obtener una mayor comprensión de la dinámica que posee la industria.

Diversos analistas especializados dividen a la industria en cinco tipos de modelos de negocios:

Acceso: Compañías que venden discados de accesos, o conexiones a redes u otros servicios de administración de redes. El modelo de negocio tipo está basado en tarifas mensuales, las cuales son determinadas por la velocidad de la conexión o por el volumen de datos que circula.

Software: Compañías que venden software que facilitan el comercio y la comunicación entre las empresas o a éstas internamente. El tipo de negocio está compuesto por tarifas por licencias de software, mantenimiento, servicios de consultoría, y por distintas tareas operativas.

Contenido: Compañías que proveen el material que se visualiza cuando se está en línea. El tipo de negocio está basado en publicidad, o en algunos casos, tarifas por suscripción.

Comercio: Compañías que venden mercaderías, o facilitan el vínculo entre compradores y vendedores. El tipo de negocio se parece a los catálogos para consumidores. Operan en tres areas: "consumer-to-consumer" (C2C), "business-to-consumer" (B2C) y "business-to-business" (B2B).

Servicios: Compañías que proveen una amplia variedad de servicios necesarios para el trabajo en línea, incluyendo "hosting", alquileres de aplicaciones, procesamiento de transacciones, información de bases de datos y consultoría. El tipo de negocio está basado en tarifas por transacciones, materiales utilizados o por suscripción.

El comercio electrónico por Internet involucra tanto a los productos financieros como a los no financieros, y se está en presencia de un fuerte crecimiento de los mismos. Esto se verifica fácilmente con sólo leer sobre los desarrollos y avances de los distintos productos: dinero-electrónico, pagos electrónicos con tarjetas de crédito y cheques electrónicos.

Teniendo en cuenta las experiencias, el éxito de todo este proceso dependerá no sólo de la tecnología, sino también, en una parte considerable, de la aceptación por parte del consumidor de estos nuevos instrumentos.

Para lograrlo resulta indispensable que los bancos aseguren confidencialidad, disponibilidad e integridad de las transacciones y de la información que ellos procesan.

Las cámaras compensadoras (automated-clearing-houses o ACH) y diversas compañías tecnológicas están invirtiendo importantes esfuerzos en pos de ofrecer a los consumidores una flexibilidad parecida a los documentos emitidos en papel, en términos de oportunidad y cantidad de los pagos, como también en el uso de computadoras personales para los pagos de facturas electrónicas.

Todos estos esfuerzos seguramente continuarán en aumento al tener que considerar la exigencia creciente que los consumidores impondrán a sus entidades bancarias, inclusive en el caso de pequeñas transacciones.

Con lo expresado se evidencia que el comercio electrónico por Internet, con el amplio potencial que cuenta para ofrecer una gran variedad de bienes y servicios a los precios más bajos, llegará a ser el canal principal para convertir pagos realizados en papel en pagos electrónicos.

Es importante recordar que el comercio por Internet no es el único factor que alienta el uso de elementos electrónicos. Los "Automated Teller Machines" (ATMs), denominados en Argentina como Cajeros Automáticos, son instrumentos que ofrecen servicios de suma utilidad.

Es indudable que la vinculación de los ATM con las redes de Internet para ofrecer nuevos productos bancarios es una realidad, que generará seguramente interesantes alternativas para los consumidores.

Es evidente que las entidades financieras persiguen la consigna de reducir la tarifa del servicio al mínimo, estimulando el uso de las computadoras personales, esto se nota en un importante crecimiento de las PC bancarias. Para el desarrollo de distintos productos vinculados con el uso de las "PC banking", será muy importante una precisa y amplia acción de las ACH, como también el desarrollo de "help desks", centros telefónicos para ayudar a los consumidores en su capacitación, y solventar sus dudas y necesidades.

Competencia

Resulta un ejercicio interesante proyectar el ambiente competitivo en el cual estarán los bancos en el futuro con todo este proceso, especialmente en el negocio minorista ("retail"), para lo que se analizarán: (a) la comoditización de los productos bancarios y los nuevos competidores, (b) las estrategias competitivas que desarrollarán los bancos, y (c) la confianza de los consumidores.

Productos bancarios y los nuevos competidores como "Commodities"

Es indudable que con los consumidores usando todos los servicios bancarios con un teléfono, computadora personal o en un ATM, la ubicación geográfica del banco perderá importancia relativa, ya que éstos le darán mayor relevancia a la calidad del servicio y al precio del mismo. Usando "software" inteligentes podrán buscar y ver productos de todos los bancos de una región o un país, haciendo comparaciones de costos, tasas y condiciones. Además ésta comparación electrónica de los productos, no sólo se podrá realizar con un "sentido geográfico", sino que podría realizarse "producto por producto", y como éstos se irán automatizando, algunos analistas hablan de una base "commodity por commodity". Es obvio que esto resulta una amenaza muy importante a la lealtad de los consumidores con sus bancos.

No obstante lo dicho, el principal temor para los bancos es la posible aparición de competidores no bancarios, que ofrezcan diversos productos como ser: tarjetas de crédito, hipotecas, cuentas de ahorro e inversión y préstamos, con precios y calidad muy competitivos.

Estos competidores no bancarios (muchos de ellos serán compañías tecnológicas) tendrán precios interesantes debido a los bajos costos de procesamiento en escala, y a que no deberán mantener los costos fijos de una extensa red de sucursales que tienen la mayoría de los bancos comerciales.

Es por ello que, para contrapesar estas situaciones, los bancos deberán evaluar la realización de las fusiones e integraciones de sus entidades, y además estimular la tercerización en compañías competitivas.

Esta dura batalla competitiva hace imprescindible que las entidades financieras continúen adicionando valor a sus productos financieros, y además, cuando sea necesario, realizar alianzas con otras compañías de alta calidad para que desde su "web-site", y mediante una simple conexión, puedan ofrecer todos los servicios que su cliente pueda necesitar, en forma precisa y eficiente.

Es un momento de cambios, a nivel global, en el negocio del "retail" bancario. El público tiene acceso a cuantiosa información con una velocidad nunca antes conocida.

Para muchos analistas, este nuevo mercado de servicios bancarios de "retail" tendrá características confusas, ya que:

a) los bancos y compañías no bancarias ofrecerán productos similares

b) los bancos y las compañías tecnológicas establecerán alianzas para resolver ciertos problemas, a la vez que los bancos permanecerán preocupados por los objetivos de muchas compañías tecnológicas creativas y competirán con ellas.

Las estrategias competitivas que desarrollarán los bancos

Las entidades financieras, además de invertir y confiar en la nueva tecnología, deberán recortar costos y facilitar los vínculos con los consumidores, evitando competir donde las compañías no bancarias tengan importantes ventajas.

Por ejemplo, más allá de utilizar los canales tradicionales o sitios en Internet y esperar el interés de los consumidores, los bancos abren pequeñas sucursales en cadenas de supermercados, donde confluyen muchas personas, incluidos clientes de sus competidores.

En estos casos, los bancos ubican autoservicios y accesos a aparatos electrónicos cuando puedan realizarlos a bajo costo, y también algunas personas disponibles para consultas y venta de productos con base en el "persona-a-persona".

Atento al importante volumen de información que los bancos poseen de sus clientes en sus bases de datos electrónicas, están comenzando a consolidar esta información en mega bases (warehouses), lo que les permitirá segmentar y clasificar a los consumidores para la comercialización de los productos. De esta forma será factible transmitirle a los clientes en forma electrónica, mensajes personalizados que aparecerán en las pantallas de sus computadoras, cuando estos realicen su rutina normal de negocios.

Para el interés de los bancos, es un tema irreversible que los márgenes de ganancias del negocio del procesamiento de pagos estén disminuyendo drásticamente; no obstante, este tipo de producto tiene una utilidad adicional que es la conformación de bases de datos como herramientas fundamentales en las políticas comerciales de las entidades.

Para muchos banqueros será muy importante en el futuro:

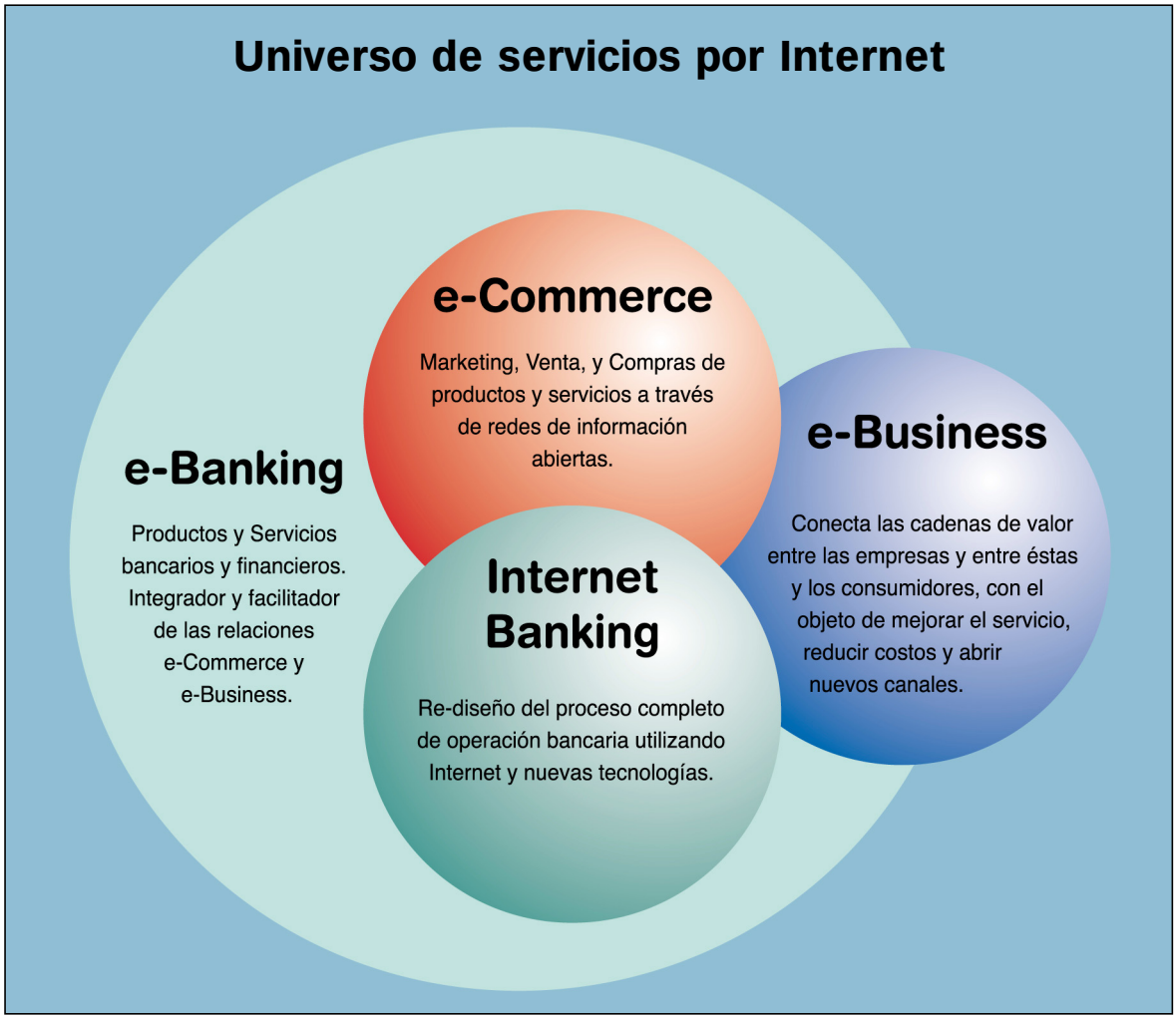
(1) diseñar un sistema de contabilidad de costos, que les permita administrar por individuo sobre todos los productos del banco (y no analizar productos individualmente sobre toda la base de clientes), y

(2) utilizar con eficiencia la tecnología de Internet, sin quedar sometido a ser una operación de "back office" de una compañía tecnológica.

La confianza de los consumidores

Una parte importante del éxito del desarrollo de los productos y servicios bancarios electrónicos dependerá de la reacción que presenten los consumidores ante las propuestas y ofertas que las entidades financieras realicen. Es innegable que dicha reacción está directamente vinculada con la confianza que los clientes vayan adquiriendo en este tipo de operaciones.

Para ello es gravitante que los consumidores, además de comprender los mensajes comerciales sobre las bondades y eficiencias de estos instrumentos, vayan adquiriendo conocimiento sobre la adecuada administración de los riesgos por parte de los bancos.



Productos en el universo de la Banca Electrónica

En la actualidad, los principales productos que las entidades financieras están desarrollando y comercializando son los siguientes:

Instrumentación de portales de Internet

Sitios donde los vendedores exhiben ofertas de productos, los cuales son visitados por un amplio número de posibles compradores. Pueden ofrecerse productos financieros, o éstos combinados con otros no financieros.

Consultoría a pequeñas empresas para el ingreso al e–Commerce

Asesoramiento a empresas en el establecimiento de las estructuras necesarias para el ingreso al e–Commerce.

Servicios de "business-to-business" en el "e-Business"

Diversas corporaciones bancarias internacionales ofrecen a grandes empresas la automatización electrónica total asociada a la adquisición y distribución de mercaderías y servicios entre distintos segmentos industriales.

Para estas corporaciones, se trata de una extensión natural de los servicios tradicionales existentes con el "cash management".

Servicios de gestión de facturación y pagos ("e-Billing")

Se trata de una serie de servicios en desarrollo para completar el vigente "cash management", destinados a grandes empresas con importante volumen de facturación.

Los bancos combinan las capacidades del e-mail para enviar estas cuentas por Internet, y la posibilidad de procesar pagos electrónicos mediante las redes interbancarias de pago, similar al M.E.P. en el sistema financiero argentino.

Verificación de identidades

Diversas compañías ofrecen productos de protección contra fraudes provenientes de falsa representación de identidades a los distintos participantes del e–Commerce.

Dinero y cheques electrónicos ("e-Money")

La mayoría de las computadoras están siendo equipadas con lectores de tarjetas inteligentes, denominadas "smart cards"; para esto, las entidades financieras prevén emitir dinero electrónicamente que será almacenado en esas tarjetas y consumido a través de Internet.

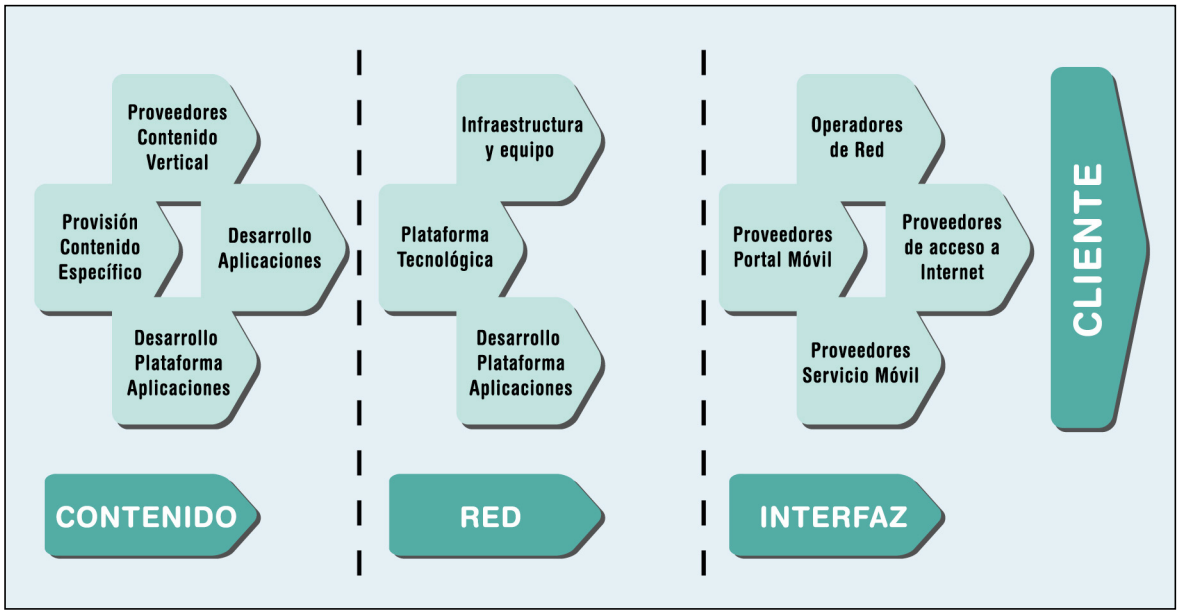
Aún se encuentra en etapa incipiente de implementación la versión electrónica del cheque.

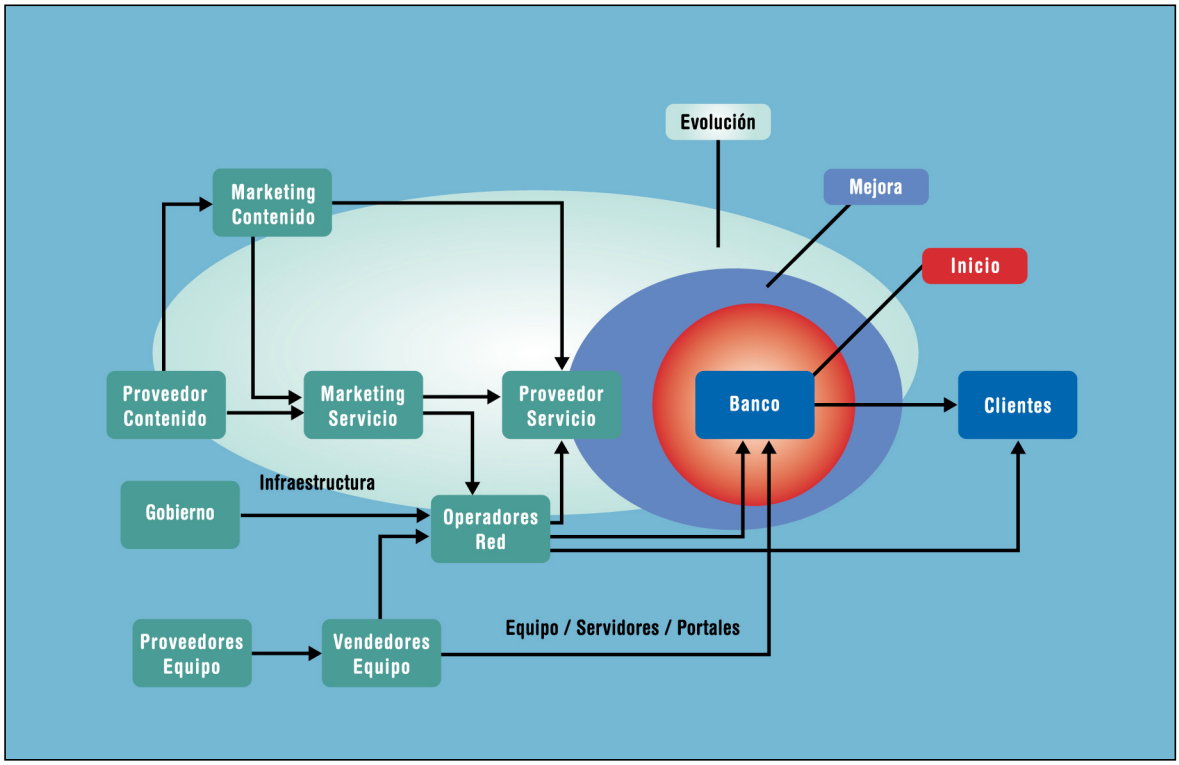
Integración entre las redes de Internet y los ATM´s

Es un proyecto de compleja implementación, pues la integración de estas dos redes implica la aparición de importantes riesgos de seguridad que deben ser adecuadamente monitoreados, al permitir el ingreso a áreas vulnerables en el entorno del "web-site" del banco.

Cadena de valor en la banca electrónica

Las entidades financieras, a medida que van madurando su presencia en los distintos canales de exteriorización, pueden pasar desde ser sólo usuarios de la tecnología a prestadores de diversos servicios a otras organizaciones o entidades financieras:





Riesgos en e–Banking

La rápida expansión del uso de Internet como un canal de distribución de servicios bancarios plantea algunos desafíos extraordinarios para las entidades financieras. Esto es especialmente cierto en el área de administración de riesgos, donde la veloz evolución de las telecomunicaciones y del hardware y software, combinada con el grado de dependencia de los bancos de la tecnología externa de vendedores y proveedores de servicios, continuamente modifican y algunas veces magnifican los riesgos de la banca tradicional.

En la actualidad, se menciona un número de cuestiones que podrían tener impacto en el perfil de los riesgos bancarios:

(i) Significativo incremento en la competencia entre entidades financieras y no financieras dentro de la industria electrónica, con la aparición de nuevos productos y servicios.

(ii) La rápida mejora tecnológica en telecomunicaciones, hardware y software, permitirá aumentar la velocidad del procesamiento de las transacciones.

(iii) La baja experiencia ("expertise") en tecnología y gestión de riesgos en e–Banking, por parte de los niveles directivos y gerenciales de las entidades.

(iv) Mayor confianza en la tercerización y la proliferación de nuevas alianzas con nuevas compañías no financieras.

(v) Potencial incremento del fraude debido a la ausencia de sanas prácticas de negocio para la verificación y autenticación de clientes sobre redes abiertas como Internet.

(vi) Inexistencia y/o ambigüedad de normas y leyes con respecto a la aplicación y jurisdicción de actividades que involucren e–Banking.

(vii) Recolección y almacenamiento de volúmenes significativos de datos de los clientes, que puedan impactar en las políticas de confidencialidad de información manejadas por las entidades.

(viii) Efectividad de la presentación de los avisos legales de las páginas de las entidades versus la eficiencia en la velocidad de navegación a través de las mismas.

Las cuestiones mencionadas son sólo algunos de los puntos que pueden afectar el perfil de los riesgos bancarios tradicionales.

Desde una perspectiva de control, se denomina riesgo a la potencial ocurrencia de eventos, esperados o inesperados, que puedan tener un impacto adverso sobre el capital o las ganancias de una entidad financiera.

Internacionalmente se han definido nueve categorías de riesgo a los efectos de su análisis: riesgo operacional, estratégico, de reputación, de cumplimiento o legal, crediticio, de liquidez, de tasa de interés, de precio y cambiario. Todas estas categorías de riesgo se encuentran, en mayor o menor magnitud, relacionadas también con e–Banking. Sin embargo, las categorías de riesgo sobre las que más impacta son: riesgo operacional, estratégico, de reputación y legal.

Riesgo operacional

Es el riesgo sobre las ganancias o el capital, que surge por la posibilidad de sufrir fraudes, la ocurrencia de errores, o por la incapacidad para brindar servicios o productos.

Si bien este riesgo es evidente en cada producto y servicio ofrecido: desarrollo de sistemas, desarrollo e implementación de productos, procesamiento de transacciones, etc., la operatoria de e–Banking puede generar un alto nivel de riesgo transaccional, particularmente en aquellas líneas de negocios que no hayan sido adecuadamente planeadas, implementadas y monitoreadas.

Los bancos que ofrezcan productos y servicios financieros a través de Internet, deberán obligatoriamente descubrir cuál es la expectativa de sus clientes. También deberán asegurarse de tener el producto correcto y la capacidad para brindarlo en forma adecuada, oportuna y confiable, si es que desean desarrollar un alto nivel de confianza en lo relativo a su marca y prestigio.

Los clientes que hacen negocios a través de Internet se caracterizan por su escasa tolerancia a errores u omisiones de las entidades, que surjan por controles internos inadecuados para administrar su negocio de e–Banking. Adicionalmente, los clientes esperarán la disponibilidad continua del producto, y una página en la Web que sea amigable para su navegación.

Otro factor que representa un grave problema para el acrecentamiento del riesgo transaccional es la ocurrencia de ataques o atentados a los sistemas de las redes y computadoras de las entidades.

Existen estudios que muestran que los sistemas son más vulnerables a ataques internos que a ataques externos. La razón que los justifica es que los operadores y usuarios internos de los sistemas tienen un gran conocimiento sobre sus características y los accesos a los mismos.

Las entidades financieras deberán tener un fuerte programa de ejecución de controles de prevención y detección, a fin de proteger sus sistemas relacionados con Internet, de manera que les permita mitigar tanto riesgos internos como externos.

Se hace necesaria la existencia de planes adecuados de contingencia y de continuidad de negocios, a fin de poder brindar, de forma normal, sus productos y servicios ante el evento de una circunstancia adversa.

Los productos de e–Banking conectados a una red robusta pueden facilitar esta tarea, ya que las capacidades de “backup” pueden ser distribuidas a través de una amplia zona geográfica.

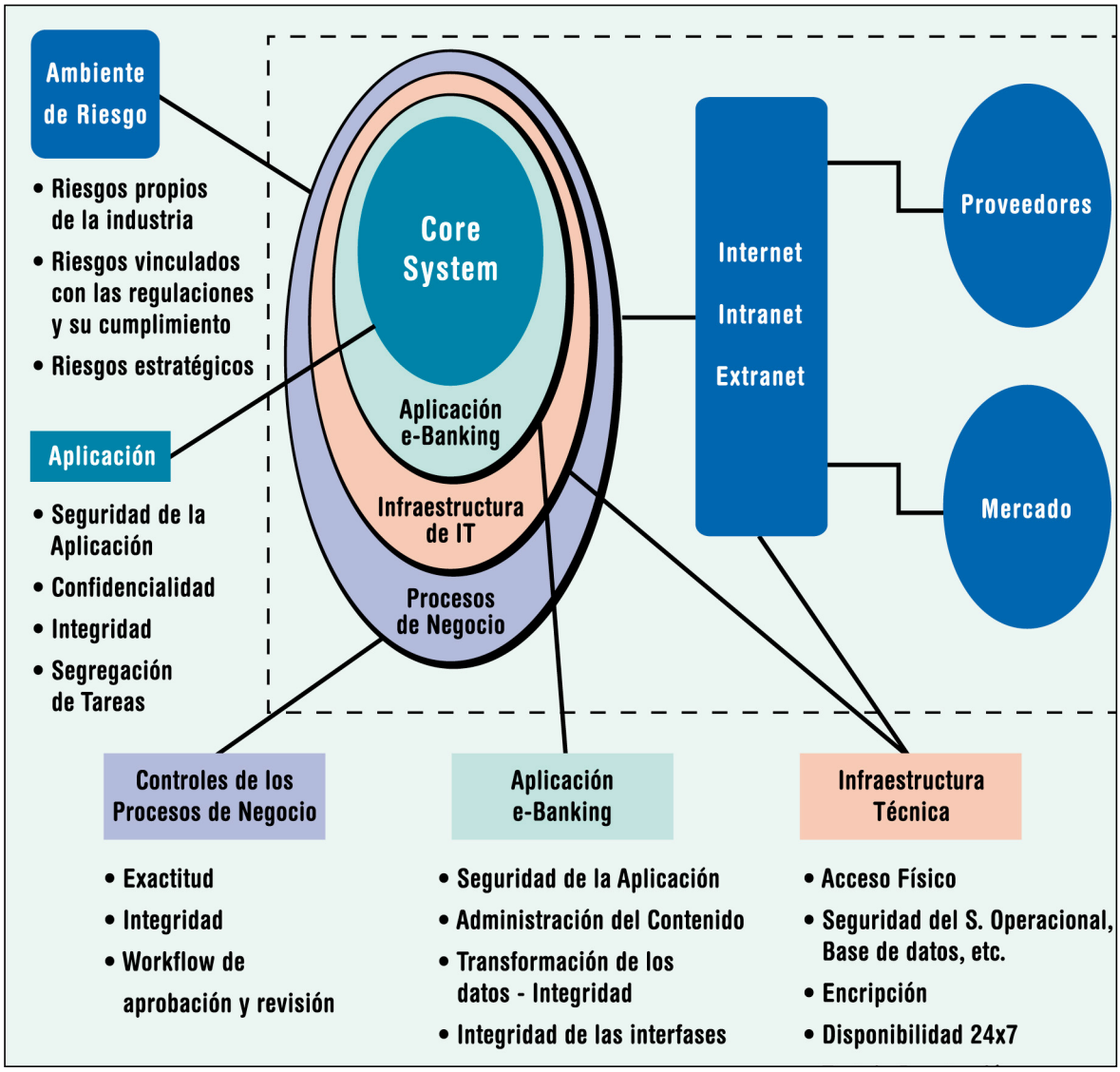
Deben considerarse los objetivos de control críticos de seguridad cuando la entidad desarrolle los planes de contingencia respectivos. La seguridad y los controles internos en la locación de los “backups” deberán ser tan sofisticados como los existentes en el ambiente de procesamiento primario.

Hay que considerar que el cliente posee un alto nivel de expectativa con relación a la disponibilidad y respuesta de los sistemas, y es común el comparar la calidad de los “web sites” de los bancos para decidir la elección del más efectivo.

Los bancos ofrecen cuentas y pagos electrónicos, por lo que necesitan procedimientos y procesos para efectuar transacciones B2B con otras entidades, sus clientes y otros terceros.

Las fallas o errores que impliquen riesgo de transacción también pueden afectar adversamente los riesgos de reputación y de liquidez.

Mapa del riesgo operacional



Riesgo estratégico

Es el riesgo actual o potencial sobre las ganancias o el capital, causado por las adversas decisiones de negocio, la inadecuada implementación de las decisiones, o falta de respuesta a los cambios en la actividad.

Este riesgo es una función de la compatibilidad de los objetivos estratégicos de una organización, de las estrategias de negocio desarrolladas para cumplir con esos objetivos, de los recursos utilizados en dicha tarea, y de la calidad de la implementación.

Los recursos necesarios para llevar a cabo las estrategias de negocios son tangibles e intangibles: incluyen los canales de comunicación, los sistemas operativos, las redes de distribución y las capacidades y habilidades gerenciales.

El Directorio de una entidad financiera deberá entender los riesgos asociados con e–Banking, antes de tomar una decisión para desarrollar un negocio en particular.

Son necesarios niveles suficientes de tecnología y adecuados sistemas de información gerencial (MIS) para soportar este tipo de proyecto.

Debido a que muchos bancos competirán con instituciones financieras más allá de las actuales áreas en las que descansa su negocio, aquellos que se definan por la utilización del e–Banking, deben tener un fuerte vínculo entre las tecnologías empleadas y el proceso de planeamiento de las estrategias del banco.

Antes de introducir un producto de e–Banking, el management debe evaluar si el producto y la tecnología son consistentes con los objetivos de negocio incluidos en el plan estratégico de la entidad.

Además, la entidad debe considerar si cuenta con expertos y con los recursos adecuados para identificar, monitorear y controlar la magnitud del riesgo en el negocio.

El planeamiento y el proceso de toma de decisiones deben centralizarse en cómo es satisfecha la necesidad de un negocio específico a través de e–Banking, más que focalizarse en el producto de banca electrónica como un objetivo independiente del resto.

Los expertos de tecnología del banco, junto con los ejecutivos operativos y de marketing, deben contribuir en la toma de decisiones y en el proceso de planeamiento.

Tienen que asegurase que el plan sea consistente con la generalidad de los objetivos de negocio del banco y que se encuentre dentro del nivel de riesgo tolerado por la entidad.

Las nuevas tecnologías, especialmente Internet, podrán acarrear rápidos cambios en las fuerzas competitivas. De acuerdo con esto, la visión estratégica debe determinar la manera en que la línea de productos y servicios de e–Banking debe ser diseñada, implementada y monitoreada.

Una amenaza importante para las entidades financieras podría ser que se vean envueltas por esos cambios, y no puedan anticiparse a las nuevas metodologías de competencia, o que respondan a ésta de una manera inadecuada.

Puede citarse como ejemplo, la existencia en otros países de bancos que sólo operan “on–line” a través de Internet (bancos virtuales). Dichos bancos operan en Internet sin la carga financiera de soportar los costos relacionados con una red de sucursales físicas; como consecuencia de ello, estos bancos virtuales pueden ofrecer atractivas tasas de interés para préstamos y depósitos, y posiblemente puedan eliminar comisiones de la banca tradicional.

De la misma forma, surgen proveedores financieros “on–line” que podrían expandir sus productos e incluso agregar los normalmente ofrecidos por las entidades financieras clásicas.

Debido a la incertidumbre sobre la potencialidad futura de esta banca virtual, los bancos tradicionales corren el riesgo de subestimar o sobreactuar en esta nueva categoría de competidores. Aquellas entidades que no actúen

rápidamente ante los reflejos del negocio, podrían perder clientes con la llegada de sus rivales "on–line". Por el contrario, algunas entidades podrían invertir grandes sumas para posicionarse en ese mercado y no conseguir la adhesión de los clientes virtuales.

La banca también deberá responder a una nueva presión competitiva creada por firmas no financieras que funcionan como centros adicionales de información en el mercado electrónico, aquellas que ofrecen un servicio de búsqueda, cotizando productos similares contra una gran cantidad de empresas existentes, y dejando evidencia "on–line" de sus logros.

Si los clientes desean realizar compulsas comparativas sobre tasas, hipotecas, cotizaciones, tarjetas y otros productos, podrán obtener dicha información rápidamente de Internet.

Al derribar las barreras geográficas, el e–Banking permitirá descubrir los términos más beneficiosos para adherirse a productos bancarios, lo que relegará el poder de los bancos que operan por estrategia regional. Como reacción, los bancos deberán considerar la retención de clientes adoptando una estrategia de construcción de productos a la medida de las preferencias individuales de los mismos.

Mientras aquellas empresas que brindan información comparativa transforman los productos bancarios en "commodities", haciendo del precio un parámetro de consideración, los bancos deben cultivar la relación comercial individual con sus clientes e identificar claramente las necesidades de los mismos para satisfacerlas minuciosamente y lograr su adhesión a los nuevos servicios, como el de gerenciar su planeamiento financiero y otros.

Esta identificación previa implica una dificultad, al ser necesario obtener datos relativos a la privacidad del cliente potencial, siendo éste generalmente renuente a divulgar dicha información a los bancos, por temor a que existan fallas en los filtros de seguridad que permitan que esos datos pasen a terceros desconocidos.

Otra área de exposición de los bancos es el llamado riesgo estratégico de ajuste, que se genera ante errores en la decisión estratégica sobre qué sucederá en el mercado con el posicionamiento de la banca electrónica: esto significa si la misma será suplementaria de la banca de redes de sucursales físicas o definitivamente será el e–Banking el reemplazante de la banca tradicional.

En la actualidad, los participantes de la industria bancaria tienen diferentes posiciones en cuanto al curso que tomará el mercado: los que se posicionan en el primer horizonte descreen del cambio total del cliente, al desear siempre la mayor posibilidad de elecciones y servicios. Los que sustentan la teoría del reemplazo, creen que la convivencia de ambas bancas sería imposible por lo oneroso de mantener los dos canales de captura y oferta de información y productos.

Finalmente, las preferencias del cliente y la competencia determinarán cuál será la realidad estratégica que domine las decisiones futuras.

Durante este período, los bancos deberán realizar un ajuste a la variación y al crecimiento del mercado electrónico, de donde surge el riesgo estratégico mencionado.

Podrán elegir una reducción en escala del número de sucursales físicas, implementar sucursales más pequeñas, con menor personal, y una oferta variada de servicios entre los que incluyan la operación virtual.

Deberán decidir si es más conveniente expandirse geográficamente a través de fusiones, una estrategia que genera un aumento notorio de ambos tipos de sucursales y clientes, o expandir su base de clientes a través de Internet, con acceso a productos virtuales y comercio electrónico.

Si el ajuste de sucursales mencionado se efectúa apresuradamente, el riesgo será un posible alineamiento de los segmentos de la base de clientes para el cual éstos no estén preparados, con la consiguiente pérdida de los que aún no deseen operar por e–Banking.

Riesgo de reputación

Es el riesgo actual o potencial sobre las ganancias o el capital, causado por una opinión pública negativa. Esto afectaría la habilidad de la institución de establecer nuevas relaciones o servicios, o mantener las relaciones de servicio actuales.

Este riesgo puede exponer a la institución a litigios, pérdidas financieras o una disminución en su base de clientes.

La exposición al riesgo de reputación está presente en toda área de la organización, e incluye la responsabilidad de tener especial precaución en el trato con los clientes y la comunidad.

La reputación de un banco se puede ver afectada, por ejemplo, si los servicios que provee no son correctos y oportunos. Esto puede incluir la inadecuada provisión de productos a través de sistemas no confiables o ineficientes, la inoportuna respuesta a las consultas de los clientes, o las violaciones a la privacidad de los mismos.

La reputación del banco puede verse dañada si los servicios de Internet Banking son ejecutados de manera inadecuada o están alejados de los intereses de los clientes y del público.

Un marketing bien diseñado es una de las maneras para educar a los potenciales clientes y ayudar a limitar el riesgo de reputación. Los clientes deben entender qué es lo que, en términos razonables, pueden esperar de su producto o servicio, qué riesgos especiales tienen, y qué beneficios pueden obtener usando el sistema.

Las entidades no deberían promover su sistema de Internet Banking basándose en figuras y atributos que el sistema no posea.

Los bancos deben considerar cuidadosamente cómo son presentadas las conexiones con los terceros en sus sitios Web.

Los vínculos de hipertexto usualmente utilizados para permitir a un cliente que se conecte con un tercero, pueden reflejar la apreciación errónea sobre la posibilidad de tener los productos o servicios de la tercera parte.

Debe quedar claro al consumidor, mediante alguna indicación especial, que está saliendo del sitio Web del banco, para que no haya confusión sobre quién es el proveedor de productos y servicios ofrecidos, así como la seguridad y los estándares de privacidad que son aplicables.

De manera similar, deben establecerse mensajes adecuados para que los clientes puedan distinguir entre los productos que cuentan con seguridad de los que no la posean.

Los bancos necesitan asegurarse que los planes de continuidad del negocio incluyan la operatoria de e–Banking.

Las pruebas regulares del plan de continuidad del negocio incluyen las estrategias de comunicación con la prensa y el público. Estas pruebas ayudarán al banco a asegurar que pueda responder efectiva y rápidamente a adversidades provenientes de reacciones del cliente y los medios.

Riesgo de cumplimiento o legal

Es el riesgo sobre las ganancias y el capital que surge por violaciones o incumplimiento de leyes, normativas, regulaciones, prácticas establecidas o estándares éticos. También suele surgir este riesgo en situaciones donde las leyes, normas o procedimientos escritos que posee el banco para brindar sus servicios, productos o actividades de su cartera de clientes, sean ambiguas o no hayan sido adecuadamente relevadas y probadas.

El riesgo de cumplimiento expone a la entidad a penalidades monetarias y puede, además, derivar en daños a la reputación, reducción del valor de sus franquicias y marcas, limitación en la oportunidad de nuevos negocios, reducción de expansiones potenciales y juicios por incumplimientos contractuales.

Los bancos con gran volumen de operaciones necesitarán realizar acciones efectivas que permitan canalizar los reclamos y mensajes de sus clientes que usen e–mail o ingresen al web site, en forma sincronizada con los restantes canales de servicios de la entidad: esto es importante a fin de asegurar una sola comunicación, oportuna y consistente con todos ellos, independientemente del canal que los clientes prefieran.

A medida que se desarrolle el comercio electrónico y la actividad bancaria a través de e–Banking, nuevas normas y leyes regirán las operaciones y el trato con los clientes. Las entidades deberán analizar y evaluar oportuna y adecuadamente toda implicancia y efectos que pueda tener la provisión de servicios y productos a través de estos nuevos canales, y considerar cuidadosamente el impacto de las regulaciones que puedan surgir.

El impacto de la introducción de e–Banking también tiene implicaciones sobre otros riesgos bancarios tradicionales, aunque no necesariamente resulta en un incremento o reducción del perfil de riesgo de las entidades, sino en una transformación del mismo.

Adicionalmente, el suministro de servicios “cross–border” (banca transfronteriza) de e–Banking, no tan extendidos a la fecha, incrementa la necesidad de reevaluar los riesgos que se presentan en los bancos.

Las actividades de e–Banking están basadas en tecnología, por lo que naturalmente están diseñadas para expandir el “virtual” alcance geográfico de los bancos, sin necesariamente requerir una expansión “física” o geográfica similar.

Esta expansión de los mercados puede extenderse más allá de las fronteras, lo que incrementa significativamente los riesgos y los desafíos de cooperación entre países debido entre otras razones a:

1. La potencial facilidad y velocidad con que los bancos localizados en cualquier lugar del mundo pueden dirigir las actividades con sus clientes a través de redes electrónicas interconectadas entre países en los que el banco no está autorizado o supervisado.

2. Las dificultades prácticas que enfrentan las autoridades para monitorear o controlar el acceso al país de sitios de e–Banking originados en otras jurisdicciones, sin la cooperación de las autoridades del país anfitrión.

Administración del riesgo

Es fundamental que el Directorio de la entidad comprenda los riesgos derivados del ofrecimiento de productos y servicios vía Internet.

Las entidades financieras deben contar con un proceso para la administración del riesgo que les permita identificar, medir, monitorear y controlar su exposición al riesgo y en particular, en lo referente al entorno de e–Banking, considerar la exposición manifiesta de los riesgos clásicos relacionados con el ambiente de tecnología informática y comunicaciones.

Uno de los objetivos que se plantea el B.C.R.A. es difundir sanas prácticas para que las entidades financieras puedan comprender si están operando su entorno de productos y servicios de e–Banking de una manera segura y confiable.

Las entidades deberían contar con personal idóneo encargado de determinar si el nivel de riesgo asumido es consistente con el grado de tolerancia al riesgo de la entidad, y medir su habilidad para manejarlo y controlarlo.

La administración del riesgo de las nuevas tecnologías tiene tres elementos esenciales:

- El proceso de planeamiento para el uso de la tecnología.
- La implementación de la tecnología.
- Los mecanismos para medir y monitorear el riesgo.

Planificación del riesgo

El proceso de planificación del riesgo es responsabilidad del Directorio y de la Alta Gerencia.

El Directorio y la Alta Gerencia necesitan contar con las habilidades y conocimientos suficientes para evaluar y administrar el uso de la tecnología de e–Banking y los riesgos asociados.

El Directorio debe revisar, aprobar y monitorear los proyectos referidos a Internet Banking, que puedan tener un impacto significativo en el perfil de riesgo de la entidad.

La Dirección y la Alta Gerencia son los responsables de desarrollar la estrategia de negocio de las instituciones bancarias. Una decisión estratégica debería ser claramente explicitada si la Dirección desea proveer servicios de e–Banking, como paso previo al ofrecimiento de dichos servicios.

Específicamente, el Directorio debería asegurar que los planes de e–Banking están claramente integrados dentro de los objetivos estratégicos de la institución, que se ha efectuado un análisis de riesgo de dichas actividades, que se han establecido procesos apropiados de mitigación y monitoreo de riesgos para aquellos identificados, y que se conducen revisiones continuas para evaluar los resultados de las actividades de e–Banking en relación con los planes de negocio y objetivos de la institución.

La realización de evaluaciones periódicas e independientes sobre la tecnología de e–Banking y sus productos por parte de auditores o consultores externos puede ayudar al Directorio y a la Gerencia a cumplir con sus responsabilidades.

El Directorio y la Alta Gerencia deberían asegurarse que las dimensiones de los riesgos operacional y de seguridad de las estrategias de negocio de e–Banking están apropiadamente consideradas y dirigidas.

La provisión de servicios financieros a través de Internet puede modificar significativamente y/o aún incrementar los tradicionales riesgos bancarios. Deberían tomarse los recaudos que permitan asegurar que los procesos existentes de administración del riesgo, procesos de control de seguridad y procesos de revisión de las relaciones de outsourcing están apropiadamente evaluados, y en su caso, modificados para adecuarlos a los productos y servicios de e–Banking.

Implementación de la tecnología

La implementación de la tecnología es responsabilidad directa del nivel gerencial.

El management debe contar con las habilidades y los conocimientos necesarios para evaluar efectivamente la tecnología y los productos de e–Banking, seleccionar la combinación adecuada para la entidad y verificar que se encuentren instalados de forma apropiada.

Si la entidad no cuenta con expertos para satisfacer internamente esta responsabilidad, debe considerar contactarse con empresas debidamente especializadas en el negocio, o evaluar la realización de alianzas o convenios con proveedores de tecnología complementaria.

En esta etapa, es crítico para las entidades asegurar el conocimiento y experiencia de sus recursos humanos, dada la constante innovación y la rapidez con que se producen los cambios relacionados con e–Banking.

Monitoreo y cuantificación del riesgo

El monitoreo y cuantificación del riesgo es responsabilidad directa del nivel gerencial.

El management debe contar con las habilidades y conocimientos necesarios para identificar, medir, monitorear y controlar los riesgos asociados.

El Directorio debe recibir reportes regulares sobre la tecnología utilizada, los riesgos asumidos, y cómo esos riesgos son administrados.

El monitoreo del rendimiento del sistema es un factor clave del éxito.

Como parte del proceso de diseño, los bancos deberían incluir un efectivo control de calidad y procesos de auditoría en sus sistemas de e–Banking.

Por otra parte, las entidades deberían realizar revisiones periódicas sobre los sistemas para determinar el grado de acercamiento a los estándares de rendimiento pautados.

En suma, es incumbencia del Directorio y la Gerencia de las entidades financieras seguir las acciones necesarias para asegurarse que sus instituciones han revisado, y modificado cuando fuere necesario, las políticas y procesos de administración de riesgo existentes para cubrir las actividades de e–Banking.

El enfoque de administración de riesgo considerado debería integrar todas las actividades desarrolladas por la entidad, y si bien en lo fundamental, las políticas y procedimientos de administración del riesgo no deberían ser diferentes de aquellas aplicadas a las actividades bancarias desarrolladas a través de otros canales, deberían contemplar las adaptaciones al “nuevo” canal de distribución que representa e–Banking.

Las entidades financieras tendrán que desarrollar adecuados procedimientos de administración de riesgo para sus particulares perfil de riesgo, estructura operacional y cultura organizacional, que se encuentren en conformidad con los requerimientos específicos de administración del riesgo y la normativa aplicable.

El perfil de riesgo de cada banco es diferente y requiere un apropiado enfoque de administración, que esté acorde a la escala de operaciones de e–Banking de la entidad, la materialidad de los riesgos presentes, y la disposición y habilidad de la institución para administrar estos riesgos.

Administración de riesgos de seguridad informática

Dentro de la actividad de e–Banking, los controles internos sobre la tecnología informática y los sistemas de información cumplen una función protagónica.

El Directorio tiene la última responsabilidad sobre el nivel de riesgo de seguridad informática tomado por su institución. De esta manera, debe aprobar las estrategias globales sobre el negocio y las tecnologías y el alcance de las políticas de seguridad informática de sus organizaciones.

La activa vigilancia demostrada por los Directorios se verá reflejada en:

- El entendimiento de los tipos de riesgos inherentes de seguridad informática en las actividades de negocios de sus instituciones, y en mantenerse informado sobre el estado de los mismos, al tiempo que los productos y servicios son desarrollados, mejorados y son introducidas nuevas tecnologías y canales de entrega.

- La revisión y aprobación de políticas de seguridad informática para direccionar riesgos inherentes con relación a los créditos, inversiones, fondos, títulos y otras aplicaciones y actividades de procesamiento significativas de una institución.

- El afianzamiento de la importancia estratégica de la seguridad informática a través de la organización, participando en la implantación de una dirección corporativa de seguridad.

- La revisión y aprobación de niveles aceptables de exposición al riesgo de seguridad informática, relacionados con los cambios en las estrategias tecnológicas y de negocio, nuevos productos y servicios, o cambios substanciales en las plataformas tecnológicas, conversiones importantes y arreglos significativos para tercerización.

- La revisión y aprobación de programas de auditoría interna de la institución, con apropiado alcance y frecuencia, conforme a las políticas de seguridad informática.

La Gerencia necesita tomar la administración de sus riesgos de seguridad y ejercer vigilancia gerencial sobre las actividades de seguridad informática, aun cuando este tipo de actividades puedan ser delegadas operativamente a otros.

Para ello la Gerencia deberá:

- Proveer dirección y niveles consistentes de seguridad de la información sobre la organización, estableciendo una función de seguridad informática corporativa y/o designar un oficial local de seguridad informática.

- Poner énfasis en la seguridad informática como un tema relacionado con la estrategia de negocio, más que como un tema meramente técnico.

- Establecer funciones de seguridad con personal competente que tenga el conocimiento apropiado y la experiencia necesaria para dirigir los riesgos asociados con las actividades técnicas y de negocios de la institución.

- Unir la seguridad de la información al rendimiento. El código de conducta de la institución y el proceso de selección de personal debe incluir los requerimientos de seguridad de la información de la institución. De manera similar, los juicios sobre el rendimiento de las unidades de negocio deben considerar los resultados de las auditorías de seguridad informática y demás revisiones.

- Asegurar respuestas oportunas a los cambios en los riesgos de seguridad de la información, que pueden provenir de cambios en la tecnología o innovaciones técnicas. Asegurar que la infraestructura y los controles internos necesarios para administrar los riesgos asociados de seguridad de la información, están funcionando correctamente.

- Asegurar que sean formulados y probados planes de contingencia ante crisis, para aquellos incidentes relacionados con la seguridad de la información.

Controles internos de tecnología en e–Banking

Los controles internos en los sistemas de información y tecnología informática (TI / SI) que dan soporte a e–Banking, deberían estar vinculados con el nivel de riesgo que presentan las transacciones y los productos que por este medio se ofrecen.

Como ocurre en las diversas actividades que conllevan el negocio financiero, la Dirección tiene la responsabilidad primaria del desarrollo, la implementación y el seguimiento de un adecuado sistema de controles internos sobre los productos, los sistemas de información y la tecnología informática de la entidad.

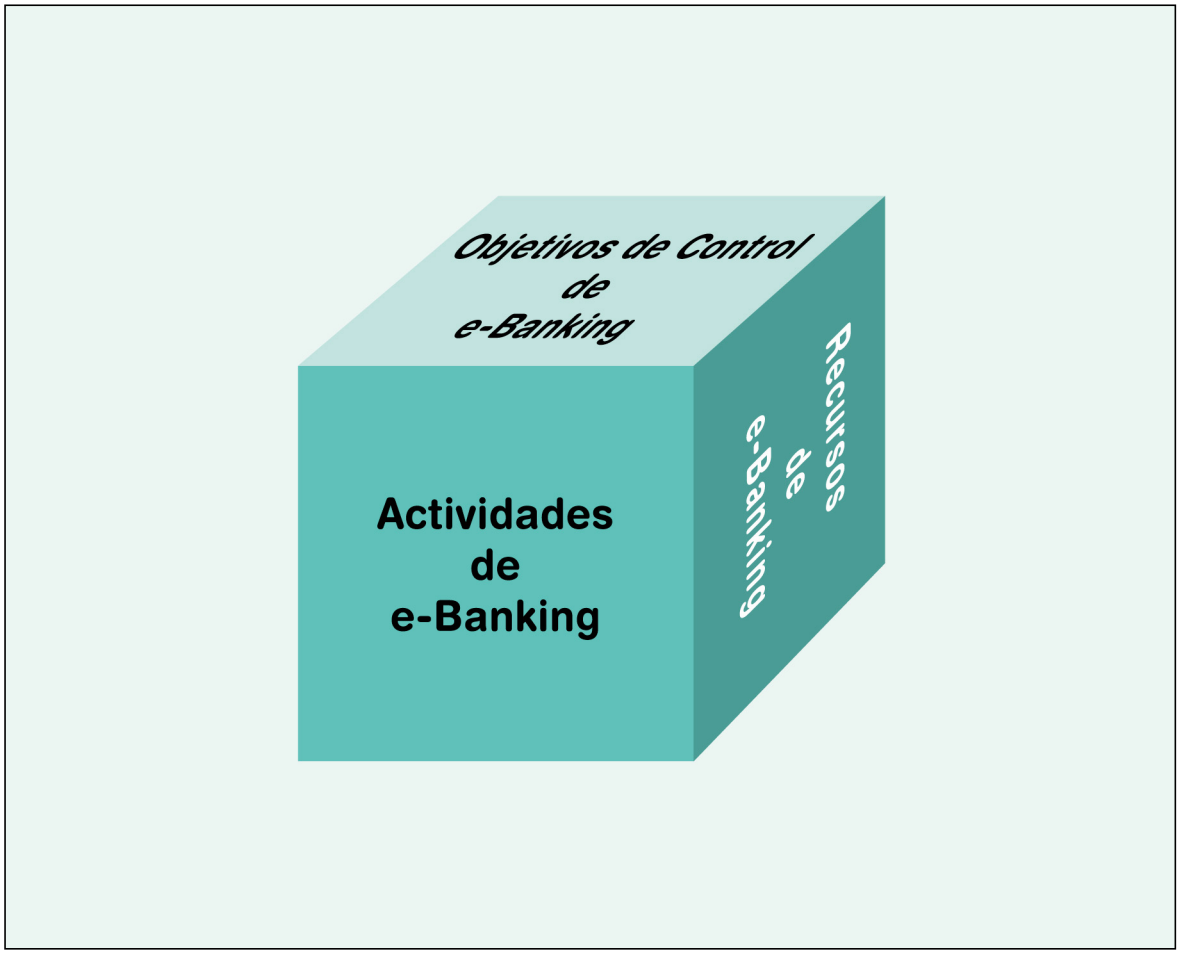
El seguimiento del estado y nivel de desarrollo de los controles internos de los sistemas de información y tecnología informática, se obtendrá con la realización de auditorías informáticas en forma periódica, que permitan asegurar que los controles son los apropiados y funcionan correctamente.

Para ello, la Dirección es responsable de la implementación de un adecuado modelo para el seguimiento, el control y la auditoría de todas las funciones y recursos que estén involucrados en las operaciones de e–Banking.

En la actualidad, existen dos clases de modelos de control disponibles, aquellos configurados para el “control de los objetivos del negocio”, y los del tipo “modelo enfocado a tecnología informática”.

El concepto fundamental es que la Dirección adopte un modelo que se enfoque al control de tecnología informática y sistemas de información para el entorno de negocio en e–Banking.

Este modelo debería ser capaz de brindar la información necesaria para dar soporte a los procesos de negocio y relacionar la tecnología y los sistemas con las actividades, los recursos y los objetivos de control de e–Banking.



Criterios requeridos

Los objetivos de control interno para los sistemas de información y tecnología informática de e–Banking deben satisfacer los requerimientos de:

Efectividad

Se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta y consistente.

Eficiencia

Se refiere a la provisión de información a través de la utilización óptima, más productiva y económica de recursos.

Confidencialidad

Se refiere a la protección de información sensible contra divulgación no autorizada.

Integridad

Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.

Disponibilidad

Se refiere a la disponibilidad de la información cuando esta es requerida por el proceso de negocio ahora y en el futuro. También se refiere a la salvaguarda de los recursos necesarios y capacidades asociadas.

Cumplimiento

Se refiere al cumplimiento de aquellas leyes, regulaciones y acuerdos contractuales a los que el proceso de negocios está sujeto, por ejemplo, criterios de negocios impuestos externamente.

Confiabilidad

Se refiere a la provisión de información apropiada para la administración con el fin de operar la entidad y para ejercer sus responsabilidades de reportes financieros y de cumplimiento.

Recursos Intervinientes

La totalidad de los criterios precedentemente mencionados debe ser aplicada a cada uno de los recursos intervinientes en los procesos de tecnología informática. Estos son:

Datos

Los elementos de datos en su más amplio sentido, (por ejemplo, externos e internos) estructurados y no estructurados, gráficos, sonido, etc.

Sistemas de aplicación

Abarcan la suma de procedimientos manuales y programados.

Tecnología

Que comprende el hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etc.

Instalaciones

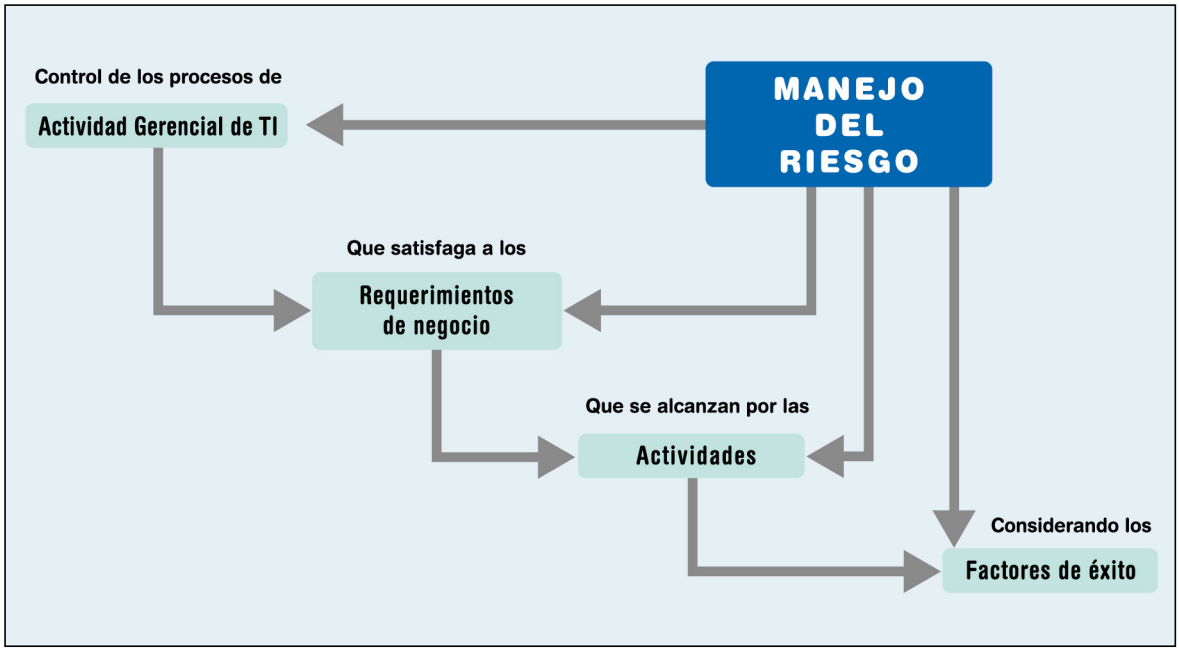
Recursos para alojar y dar soporte a los sistemas de información.

Personal

Habilidades del personal, conocimiento, conciencia y productividad para planear, organizar, adquirir, entregar, soportar y monitorear servicios y sistemas de información.

Manejo del Riesgo

La Dirección es la responsable de poseer un conocimiento integral de la operatoria, a efectos de poder evaluar la adecuada combinación y suficiencia de controles internos para el manejo del riesgo.



Control Interno: Componentes y Categorías

De acuerdo con la "Information System Audit and Control Association" (ISACA), los componentes de control interno básicos comprenden:

Controles internos contables

Usados para salvaguardar los activos y la confiabilidad de los registros financieros.

Controles operacionales

Utilizados para asegurar que los objetivos de negocio son tenidos en cuenta. Estos controles incluirían planes y presupuestos operativos, comparados contra la ejecución de lo planificado.

Controles administrativos

Empleados para asegurar la eficiencia operacional y la adhesión a las políticas y procedimientos de la entidad. Estos controles incluirían la realización de auditorías externas e internas en forma periódica.

Adicionalmente, ISACA separa los controles internos en tres categorías generales.

Estas categorías pueden ser localizadas en los controles internos básicos señalados anteriormente:

Controles preventivos

Son aquellos que previenen la ocurrencia de algún riesgo (por fraude o error). Un ejemplo de este tipo de control es la aplicación de un software de control de accesos lógicos que autorice el ingreso a la red sólo al personal autorizado.

Controles de detección

Identifican la ocurrencia de una acción. Ejemplo de ello sería un software de detección de intrusos que dispare un alerta o una alarma.

Controles correctivos

Corrigen una situación una vez que ha sido detectada. Un ejemplo sería un software de "backup" que pudiera ser usado para recobrar un archivo corrupto, o una base de datos.

Como participantes significativas en el mercado, las entidades financieras están siendo cada vez más agresivas en la adopción de las capacidades de los servicios de e–Banking, que incluyen sistemas de banca remota y programas de valor agregado.

Este proceso es altamente dinámico a medida que las tecnologías emergentes producen una variedad de alternativas de entrega de productos y servicios de innovación.

Las oportunidades de negocio por medio del e–Banking, pueden poseer riesgos significativos para una entidad financiera, como los que ya se han enunciado precedentemente; no obstante, estos riesgos pueden ser mitigados mediante la adopción de un programa de administración y gerenciamiento del riesgo y la aplicación de sanas prácticas.

Los componentes básicos de sanas prácticas que ayuden a mantener un alto grado de confianza pública dentro de un entorno de red abierta, como es Internet, incluyen como mínimo:

Provisión de políticas y procedimientos generales para los productos y servicios de e–Banking

Es importante que se definan e implementen políticas y procedimientos en relación a la incorporación de clientes por medio de Internet, sobre los medios o mecanismos de autenticar la identidad de los clientes, los criterios de privacidad de los datos pertenecientes a los clientes y recolectados por las entidades financieras, contemplando los aspectos legales que sean de aplicación.

Otros aspectos relevantes de la presencia en Internet y que deben estar pautados en las políticas y procedimientos, es la utilización de enlaces (links), donde es importante que quede claramente resaltado la desvinculación de la entidad en la responsabilidad de lo operado en el sitio web que se ingresa, si es que no pertenece a la entidad.

Dentro de los servicios presentes en Internet, los financieros y bancarios son los que más dinamismo presentan, por ello mantener un adecuado control de los cambios que se realizan tanto en su diseño como en los programas que realizan las funciones del negocio, es de vital importancia para minimizar los riesgos de fallas operativas en las modificaciones efectuadas.

Contar con procedimientos, que detallen los diferentes pasos y controles a efectuar durante estas modificaciones y/o actualizaciones, se transforma en una faceta muy relevante para el control.

Selección de la arquitectura tecnológica y su configuración

Deben existir mecanismos de seguridad y de procedimientos, los cuales tomados conjuntamente, constituyan una arquitectura de seguridad para el e–Banking.

Deben existir medidas para asegurar la adecuada elección de los protocolos de comunicación correctos para el ambiente y la aplicación, así como el adecuado uso y explotación de sus características y compensación de sus limitaciones.

Una arquitectura de seguridad de información es una descripción de todas las medidas de seguridad implementadas entre el conjunto de los usuarios y los recursos que gestionan la información. Más específicamente, la arquitectura es un diseño conceptual que trata sobre la función, la ubicación, los recursos, y los procedimientos para realizar la implementación de las medidas de seguridad que se hayan definido.

Para completar la arquitectura se deben tratar tanto los requerimientos técnicos como los de negocios. A su turno, las demandas técnicas de seguridad dependen fuertemente de la infraestructura de tecnología.

Implementación de mecanismos de control que alerten las fallas y minimicen las vulnerabilidades que la arquitectura puede presentar frente a la exposición a Internet

Deben existir mecanismos corta fuegos (Firewalls) para mediar entre la red pública, Internet, y la red privada de la organización, que garanticen la no–intromisión y reconozcan las vulnerabilidades de seguridad cuando estas se evidencien, como ser la detección de intrusos (Intrusion Detection).

Debe existir un mecanismo para proteger de la presencia, en el ambiente de e–Banking y sus redes privadas de soporte, de virus de computadora y prevenir su propagación a otros clientes.

La Web ciertamente es el aspecto más accesible y utilizado de la Internet. Todo el mundo es direccionado desde un explorador Web (browser). Los exploradores Web se comunican con los servidores Web utilizando el protocolo HTTP. Este protocolo rápidamente llegó a fijarse en la memoria de cualquier usuario de Internet mediante el uso de la sigla por Protocolo de Transferencia de Hipertexto (Hypertext Transfer Protocol) en la dirección de cualquier servicio Web de Internet.

Entender los temas de seguridad de la Web es esencial para minimizar los riesgos comunes, que incluyen:

Riesgo de intercepción

El HTTP comunica la información desde el cliente al servidor y lo hace en un texto claro o de forma no encriptada. Consecuentemente, es posible que la información sea vista y posiblemente modificada, en cualquier punto entre el cliente y el servidor.

Redirección

Las páginas de un servidor Web están formateadas en HTML – lenguaje de hipertexto realzado (Hyper Text Markup Language). Este lenguaje ofrece muchas opciones para unir las páginas, tanto dentro de un sitio, como de múltiples sitios. Este también soporta la redirección entre los diferentes sitios de una manera enteramente transparente para la mayoría de los usuarios. Consecuentemente, es relativamente fácil para alguien personificar un servicio Web o representar un sitio u organización falsamente. Esto a menudo se refiere como “spoofing” (burla).

Temas de identificación

Una página Web transaccional vincula a un cliente y a un negocio o posiblemente a dos o más negocios. Existe solamente limitado control sobre la verdadera identificación de cualquiera de las partes; esta es relativamente una medida trivial para asumir cualquier identidad que uno quiera escoger sobre Internet. Esto significa que en la conducción de transacciones por Internet, uno tiene que ejercer un extremo cuidado para verificar la identidad de sus clientes.

Débil seguridad del cliente

Mientras que las organizaciones que ofrecen transacciones a través de un servidor de Internet pueden estar en capacidad de manejar el riesgo dentro de su propio ambiente, usualmente no sucede lo mismo desde el lado del cliente.

Algunos de estos temas de seguridad de Web se deben a las debilidades en el diseño de los protocolos HTTP y HTML. Para ayudar a tratar estos temas, han emergido otros protocolos que realizan una mejora sustancial, como ser SSL (Secure Sockets Layer) y una versión de SSL en sí misma ha sido creada como TLS (Transport Layer Security); también el IPSec, en modo túnel o transporte, siendo éstas solo algunas de las opciones más seguras.

Otras de las medidas es la instalación de "Firewall", que es un dispositivo de red con dos o más interfases. Más específicamente, es una combinación de hardware y software que se levanta entre Internet y una organización interna, incluyendo sus redes de área local y computadores.

Su función más elemental es prevenir el tráfico de mensajes desde las partes fuera de la organización, y los accesos no autorizados a la red privada. Además, este traslada el protocolo interno de Internet (IP) emitido de forma tal que un potencial intruso no conozca la dirección interna ni el acceso a ella.

Para el mundo exterior, viniendo a través de Internet, la única dirección percibible es aquella del "Firewall", y si está adecuadamente configurado, no permitirá que personas desconocidas ingresen a través de la red interna.

Provisión de procedimientos y controles que brinden una adecuada seguridad en las aplicaciones de e–Banking

Debe existir una adecuada separación y controles de seguridad entre las aplicaciones que brinden servicio e–Banking y las que se utilizan en la red interna (Intranet).

Deben existir adecuados controles de los cambios o modificaciones que se realicen en las aplicaciones que brinden servicios de e–Banking.

Debe existir un programa regular de auditoría y evaluación de la seguridad de los ambientes de e–Banking y sus aplicaciones, a fin de proporcionar seguridad sobre la presencia de los controles y su efectividad.

Cualquier cambio, pero particularmente los cambios de complejidad en la tecnología interdependiente podría causar resultados inesperados y amenazar la disponibilidad.

La estrategia de separación de ambientes de prueba para minimizar los riesgos de cambios es prácticamente de alta criticidad. Además, la posibilidad de efectuar cambios es un resultado deseable para muchas de las personas que habitualmente atacan a los sitios de Internet y a otras redes públicas. En consecuencia, la seguridad de procesos de cambios en sí misma es de vital importancia.

Por lo tanto, la revisión independiente y la auditoría de sistemas se hacen más esenciales para asegurar que el nivel deseado de protección haya sido logrado.

Provisión de mecanismos que permitan la contabilización y auditoría de las transacciones de e–Banking

Las aplicaciones de e–Banking deben mantener un registro (log) de su uso, el cual debe ser controlado por personal responsable.

En las aplicaciones de e–Banking deben existir mecanismos que permitan reconstruir la actividad procesada por una aplicación.

Debe mantenerse una asociación entre una transacción de e–Banking y la persona que la ingresó.

La existencia de "logs" y pistas de auditoría que puedan ser usados para identificar el origen de los problemas es esencial en cualquier aplicación. Esta necesidad se incrementa porque los problemas pueden no ser detectados hasta algún tiempo después de la ocurrencia del incidente.

El registro efectivo (logs) de los sistemas de e–Banking puede ser difícil de lograr principalmente debido al gran número de servicios de red, a los componentes envueltos en una solución de e–Banking, y a la carencia de integración de sus capacidades de registro; por lo cual, es conveniente que cada uno de los componentes involucrados sea administrado y auditado a fin de asegurar sus condiciones y los períodos de retención adecuados.

Para posteriores revisiones, es importante mantener una asociación entre una transacción de e–Banking y la persona que la ingresó. Esto se logra mediante los servicios de "no – repudio", que proveen evidencia irrefutable de una acción específica ocurrida.

El "no–repudio" de origen protege contra cualquier intento que haga el iniciador de un mensaje de rechazar el envío del mismo.

El "no–repudio" no es un concepto nuevo. Las firmas digitales son usadas frecuentemente para proveerlo.

Consideración sobre la infraestructura de Telecomunicaciones

Debe considerarse si la arquitectura de la red adoptada es apropiada para la naturaleza y magnitud necesarias para el funcionamiento bancario.

Los protocolos de la red usados deben ser apropiados para el uso específico (por ejemplo, si se realizan pagos o transferencias, deben usarse los protocolos seguros).

El banco debe tener un proceso eficaz para evaluar la suficiencia de controles físicos en el lugar para restringir el acceso a los servidores y componentes (Firewalls, routers, switches, etc).

Se deben implementar adecuados mecanismos de descubrimiento de intrusión, sistemas y procedimientos para el control de virus.

Se deben realizar adecuadas pruebas de penetración en las redes internas y/o externas.

Se deben tomar las precauciones de enlaces mediante una red privada virtual (VPN) y técnicas de encriptación relacionadas para los casos en donde se consideren necesarios

Administración y control de procesos parcial o totalmente tercerizados

Un acuerdo para la provisión de servicios de T.I. por terceros, será adecuado, en la medida que considere:

Un nivel adecuado de inclusión, participación, compromiso y disponibilidad acordados y formalizados de todos los recursos técnicos y humanos necesarios para la ejecución positiva, oportuna y eficaz de cada objetivo, procedimiento y tarea que componen el servicio.

Que el acuerdo permita la medición cuantitativa y cualitativa de la ejecución de los procesos, minimice la exposición a daño o perjuicio de la entidad en la continuidad del negocio y la integridad de la información, y subordine el control y auditoría de los procesos a las prácticas de la entidad y las que establezcan los organismos de control.

La implementación de mecanismos y procedimientos que otorguen confidencialidad e integridad de los datos estáticos y en tránsito, y una adecuada autenticidad y autenticación de los participantes intervinientes en las transacciones de e–Banking que posibiliten el no–repudio de las mismas.

Debe existir un medio que asegure la confidencialidad e integridad de los datos residentes en las bases de datos, y de los datos comunicados entre la entidad y los clientes, y en el caso de aplicarse, entre los clientes.

Debe existir un proceso por el cual los participantes en una transacción de e–Banking puedan ser única y positivamente identificados.

Debe existir un mecanismo por el cual el iniciador de una transacción de e–Banking pueda ser únicamente asociado con esta.

Debe existir una infraestructura para manejar y controlar los pares de claves públicas, privadas y certificados.Los procesos definidos en las transacciones de e–Banking, deben proporcionar la autenticación necesaria entre partes; garantizar la confidencialidad de la información sensible (número de tarjeta o cuenta, fecha de caducidad, etc.), y preservar la integridad de la información que contienen las transacciones.

Aunque estos aspectos son importantes en cualquier red de transmisión de datos, su vulnerabilidad causa una preocupación mucho mayor cuando se relacionan con Internet u otra red pública de datos, por su ubicuidad y desconocimiento de todas las partes actuantes.

Cómo se logra la implementación en los procesos de autenticación, confidencialidad e integridad enunciados anteriormente:

La autenticación de las partes se consigue mediante la emisión de certificados y la generación de firmas digitales.

La confidencialidad (no vulnerabilidad de la información) se alcanza mediante la encripción de los mensajes.

La integridad de los datos se consigue mediante el uso de firmas digitales.

Los algoritmos criptográficos empleados para los procesos de encripción, emisión de certificados y generación de firmas digitales son de doble naturaleza. Por un lado, se define un algoritmo de clave privada, de probada fortaleza y excelente rendimiento: DES (Data Encryption Standard), en uso desde 1977.

Por otro lado, se hace imprescindible contar con un algoritmo que permita el intercambio de claves en una red pública, con total seguridad, entre múltiples participantes sin ninguna relación previa. Un algoritmo como el descripto se define

de clave pública, y generalmente se emplea el diseñado por Rivest, Shamir y Adleman, cuyas iniciales componen su nombre: RSA.

Esencialmente, cada algoritmo criptográfico permite la implementación de una función determinada. DES se emplea para garantizar la confidencialidad de los mensajes transmitidos; RSA se utiliza para garantizar la integridad de los datos y la autenticidad de los participantes. RSA desempeña todavía una función adicional, que es posible gracias a su definición como algoritmo de clave pública (también se conoce como algoritmo asimétrico, por emplear dos claves diferentes, una para la encripción y otra para la desencripción): permite la distribución y utilización de una clave secreta entre participantes sin ninguna relación previa y, lo que es más importante, sobre canales (vínculos de comunicación) no asegurados.

Clave privada vs. Clave pública

DES, como algoritmo de clave privada (este tipo de algoritmos también recibe la denominación de algoritmos simétricos – Figura 1) requiere que las partes intervinientes en un proceso de encripción/desencripción compartan la misma clave.

Esto plantea, como cabe suponer, problemas de distribución de claves en entornos no seguros, como es el caso de Internet.

A nadie se le ocurriría distribuir una clave DES mediante un mensaje de correo electrónico, o por teléfono. Sólo la entrega en mano garantiza que una clave no sea divulgada durante la distribución.

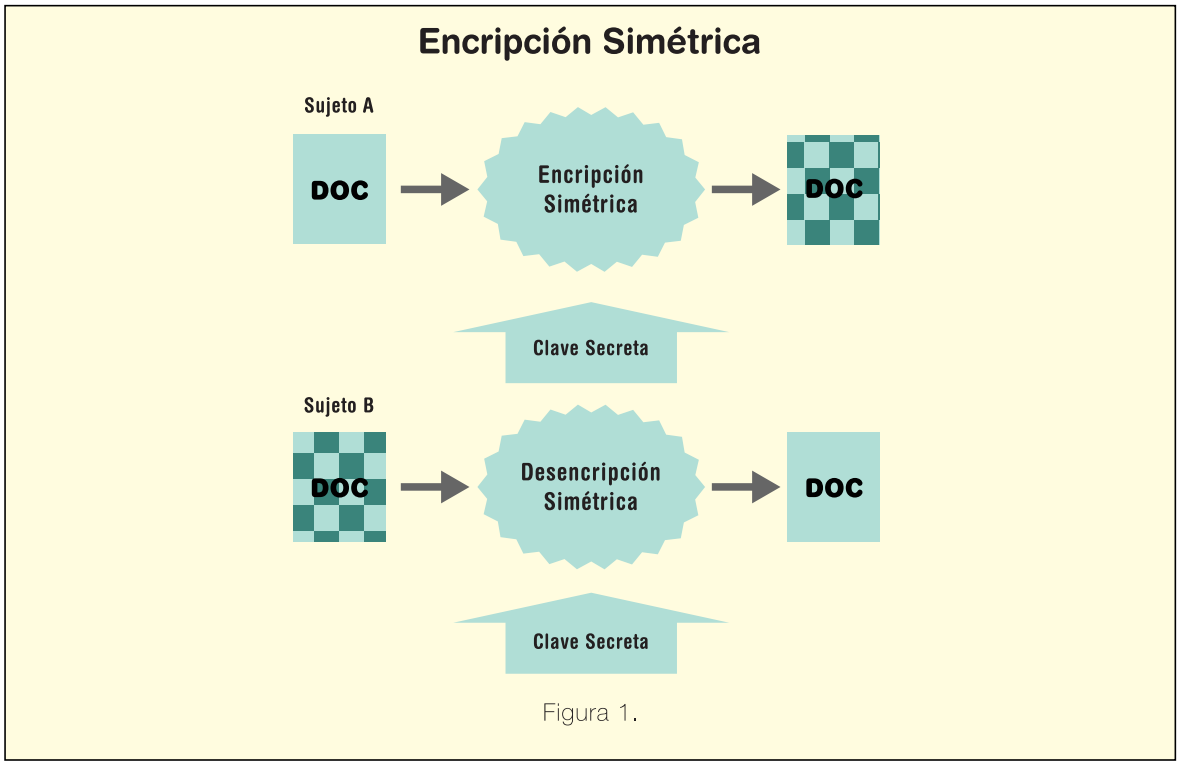


Figura 1.

Los algoritmos de clave pública, como RSA (también denominados algoritmos asimétricos – Figura 2), están sustentados en una base matemática tal, que cada una de las partes intervinientes dispone de un par de claves: una se denomina clave pública, y está destinada a ser distribuida libremente.

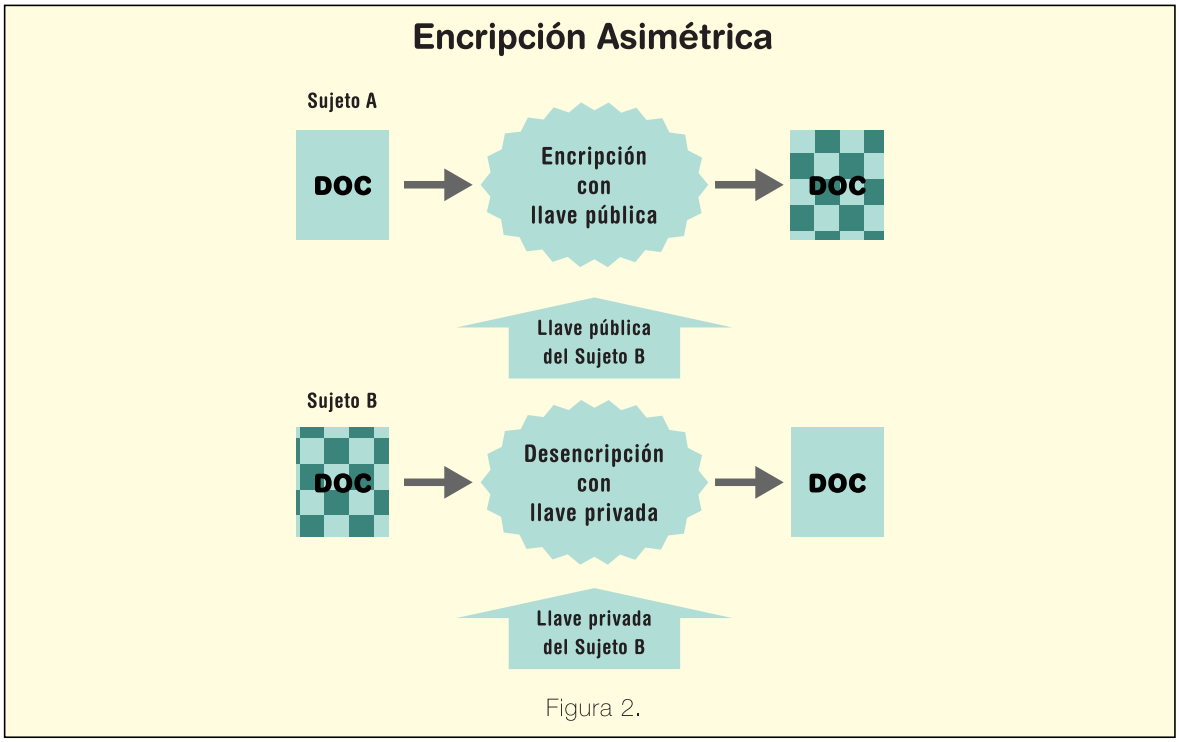


Figura 2.

En este caso, cuanto más ampliamente se haya distribuido esta clave, más garantías existen que no sea posible la "suplantación de identidad". La otra clave, la clave privada, será conocida solamente por su legítimo propietario, y debe ser custodiada con el mismo cuidado con el que se haría para una clave DES. La base matemática aludida anteriormente permite que, mientras que un mensaje puede ser encriptado con la clave pública, sea necesaria la clave privada para su desencripción.

El mensaje original es encriptado con la clave pública del destinatario; éste podrá obtener el mensaje original después de aplicar su clave privada al mensaje cifrado.

Se resuelve así el problema de la distribución de claves sobre canales no seguros, pero siempre aparecen nuevos problemas, uno de ellos es el relativo a la "suplantación de identidad".

Veamos en que consiste: Sujeto "A" y Sujeto "B" son usuarios de un sistema de criptografía basado en RSA, Sujeto "A" obtiene la clave pública de Sujeto "B" de una página Web generada por ésta última; sin embargo Sujeto "C" ha sustituido la clave pública original de Sujeto "B" por la suya propia. Cuando Sujeto "A" envía un mensaje a Sujeto "B", cifrado con su clave pública, en realidad está utilizando la de Sujeto "C", que puede así intervenir estos mensajes. Para no levantar sospechas, Sujeto "C" reenvía el mensaje original a Sujeto "B", esta vez con la clave pública original de ésta ultima.

Para resolver este problema potencial, en el contexto de los sistemas criptográficos de clave pública se ha diseñado la figura de la Autoridad Certificadora (*Certifying Authority*, CA), que se trata de entidades independientes que garantizan, mediante la emisión de certificados electrónicos, la autenticidad de las claves públicas de los usuarios (particulares y empresas), y custodian la integridad de las mismas.

Confidencialidad de los mensajes

La confidencialidad de los mensajes está soportada primariamente por la utilización de claves simétricas para cifrar el contenido de los mismos. Estas claves, generadas de forma aleatoria, son cifradas a su vez con el componente público del par de claves asimétricas del destinatario.

La unión de la clave simétrica cifrada, junto con los datos del mensaje cifrados con esta, se conoce como sobre electrónico (digital envelope), (Figura 3.)

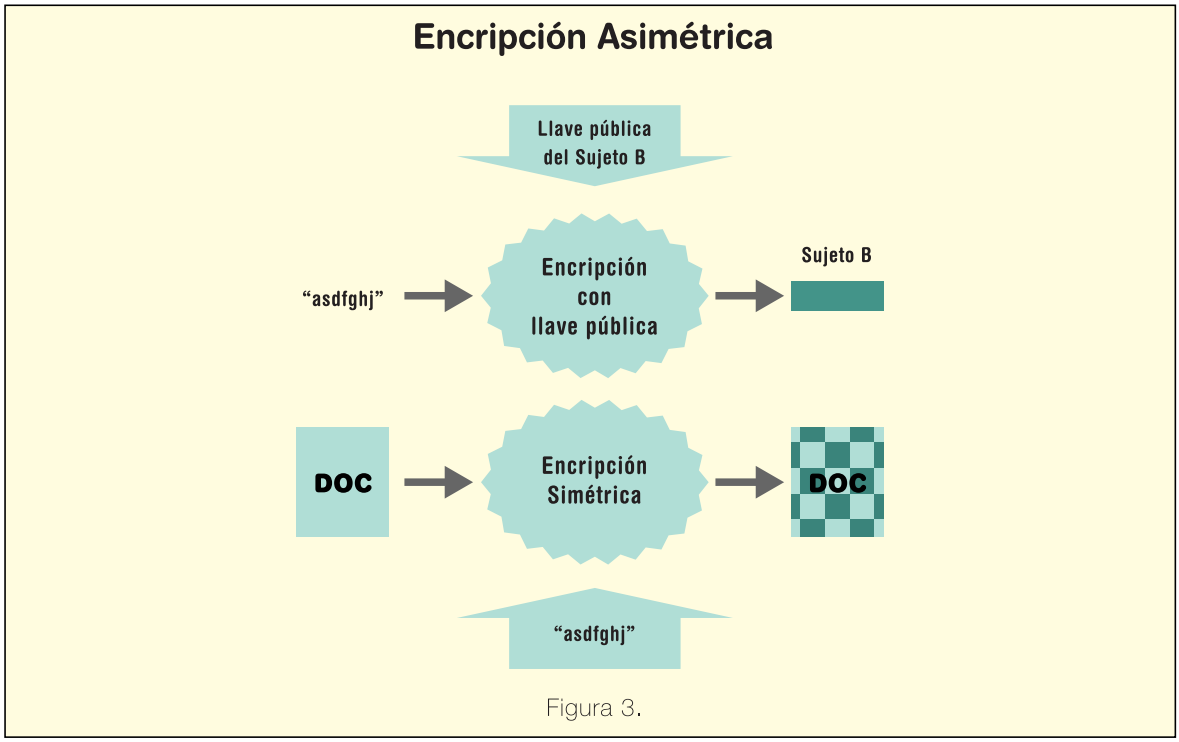


Figura 3.

A su recepción, el destinatario utiliza el componente privado de su par de claves asimétricas para descifrar la clave simétrica, que a su vez permitirá descifrar los datos del mensaje, Figura 4. La generación de las claves simétricas aleatorias es un proceso de gran importancia. La programación y métodos empleados para ello deben garantizar que tales claves no sean inferidas del contenido del mensaje, ni del entorno en el que se han producido.

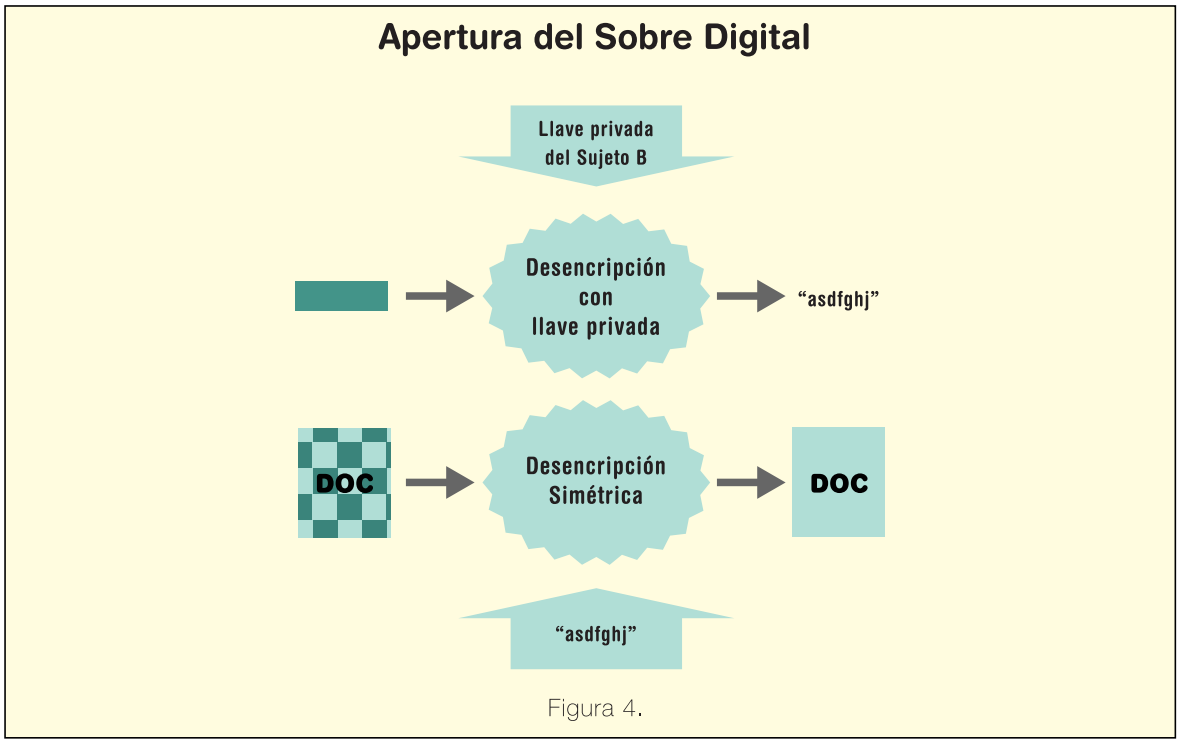


Figura 4.

Firmas electrónicas. Integridad y autenticidad de los mensajes

La *integridad*, como garantía de que el contenido de los mensajes no ha sido alterado de forma fraudulenta, y la *autenticidad*, que garantiza que las partes intervinientes en el proceso representan a quienes realmente dicen ser, se basan en la generación de firmas electrónicas (*digital signatures*).

La firma electrónica resulta de las relaciones matemáticas entre las claves pública y privada del algoritmo asimétrico utilizado. Así, un mensaje cifrado con una de las claves sólo puede ser descifrado con la otra. El remitente de un mensaje cifra su contenido con su propia clave privada; el destinatario puede descifrarlo con la correspondiente clave pública y determinar así la autenticidad del origen del mensaje.

Para garantizar la integridad del contenido del mensaje, y al mismo tiempo acelerar el tratamiento del mismo, se incorpora un proceso adicional consistente en generar un valor único y representativo de los datos. Este proceso, denominado valor numérico resumen del mensaje (*message digest*) consiste en hacer pasar los datos a través de una función irreversible (*one–way hash function*), que produce un valor *Hash* (valor numérico resumen del mensaje) del original que es único para un contenido dado.

Es imposible a nivel computacional producir el mismo *Hash* a partir de dos mensajes diferentes. El *Hash* del mensaje se cifra con la clave privada del remitente, y el resultado se añade al mensaje original que se envía, constituyendo la firma electrónica del mismo, Figura 5.

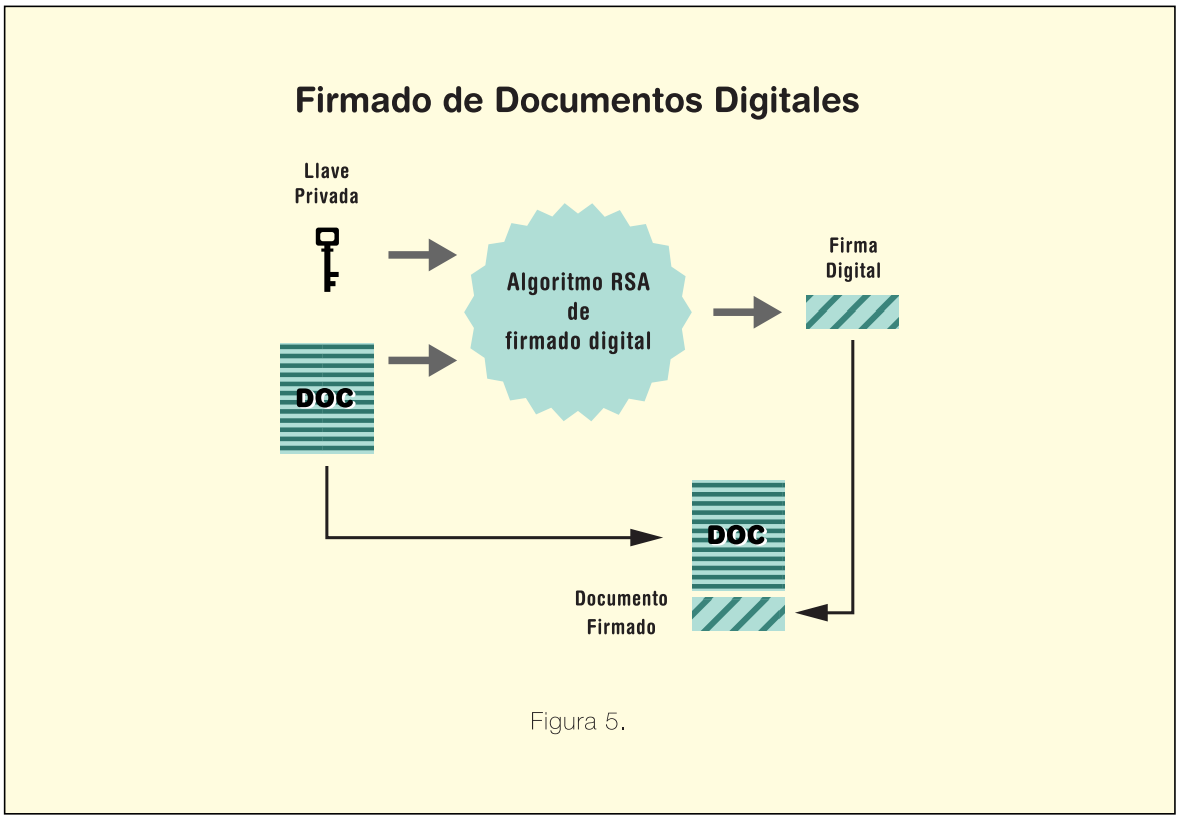


Figura 5.

El destinatario del mensaje descifra el *Hash* con la clave pública del remitente, aplica la misma función al mensaje original y compara ambos resultados. Si son iguales, la *integridad* y *autenticidad* del mensaje son correctas. Si el proceso de descifrado no es satisfactorio, el remitente no puede ser autenticado; si el *Hash* generado no es coincidente con el extraído de la firma electrónica, se ha producido una modificación en el contenido del mensaje, figura 6.

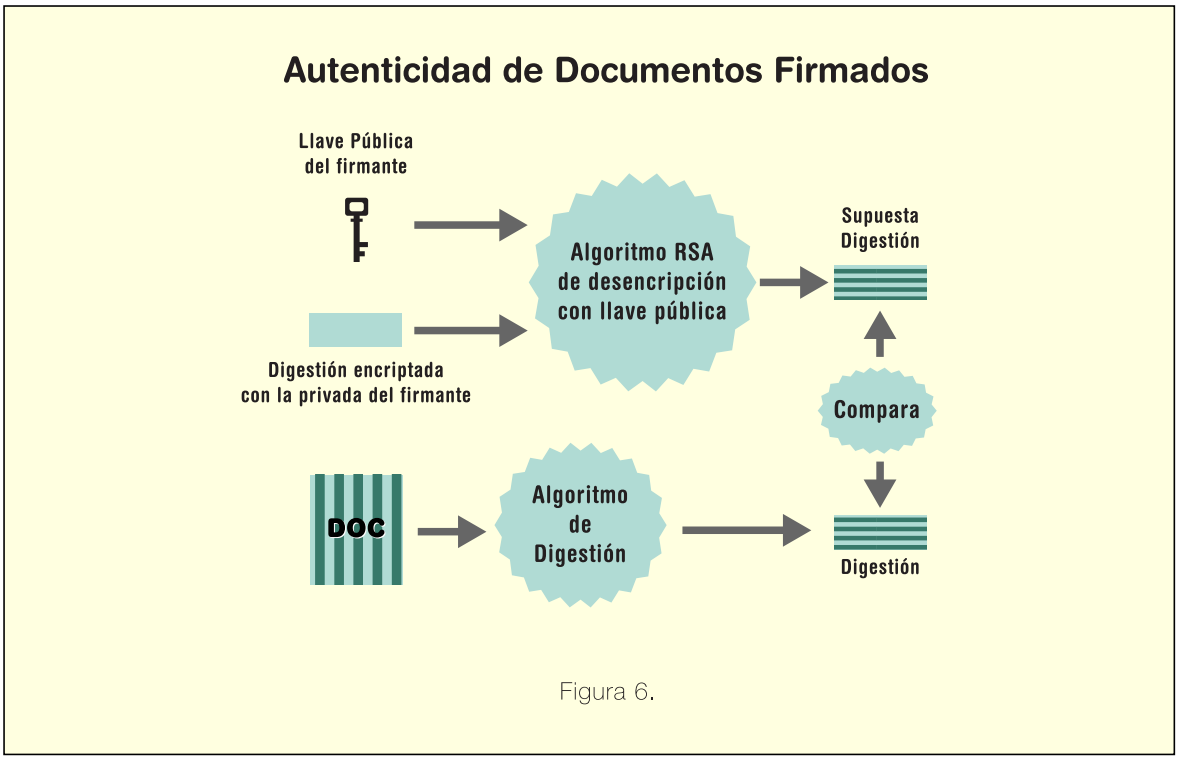


Figura 6.

Certificados de Autenticidad

La firma electrónica garantiza la autenticidad del remitente y la integridad de los datos contenidos en el mensaje. No obstante, aún es posible que se haya producido una suplantación de identidad del remitente, si su clave pública ha sido alterada de forma fraudulenta por una tercera persona. Una posible solución para el problema de la suplantación de identidad, es el intercambio de claves públicas mediante canales seguros. Sin embargo esto no es viable en la mayoría de los casos, y especialmente cuando los participantes no guardan una relación anterior, como se da en el comercio electrónico.

Una alternativa al intercambio seguro de claves es la utilización de certificados de autenticidad emitidos por entidades de confianza para todas las partes intervinientes. Tales entidades se denominan Autoridades Certificadoras (*Certificate Authorities*, CA). Un certificado de autenticidad contiene la clave pública de la persona o entidad para la que se emite, junto con información propia, y todo ello firmado electrónicamente por la CA. Como la clave pública de la CA está ampliamente distribuida, no existe riesgo de suplantación de identidad.

Existencia de controles preventivos y correctivos definidos para asegurar la disponibilidad permanente de actividades sujetas a servicios de e–Banking y el acceso a los datos

Debe existir un plan y procedimientos para continuar las actividades de e–Banking en caso de una interrupción prolongada de los medios requeridos para el procesamiento normal.

Deben existir procedimientos que garanticen la custodia y recuperación de los datos de las operaciones y transacciones de e–Banking.

Como la arquitectura y la tecnología del e–Banking consisten de dispositivos electrónicos para la gestión de mensajes y datos trabajando todos juntos (ruteadores de mensajes por medio de la red, dispositivos de entrada y computadoras), si el diseño de éstas redes no contempla la necesidad de la alta disponibilidad para los fines del negocio, entonces la falla de un componente técnico se equipara a cerrar el negocio.

Lo que se necesita es la duplicación de ciertos componentes críticos y la estructura que podrá estar en rápida capacidad de sobreponerse a la falta o el mal funcionamiento de los dispositivos cuando uno de ellos falle.

Algunos componentes son más críticos que otros para el e–Banking:

- La Internet en sí misma – es el “sine qua non” del e–Banking.

- Proveedores de servicios de Internet – dado que algunas veces los ISPs están fuera de servicio o no se encuentran disponibles, es importante para una compañía tener por lo menos dos, para que uno provea acceso en una emergencia. La otra propuesta utilizada por algunas organizaciones, es la de mantener su propia presencia en Internet con un ISP como respaldo.

- Los servidores Web – es esencial que haya más que un servidor Web disponible, preferentemente en diferentes ubicaciones.

- Bases de datos – es importante tener duplicación de bases de datos para soportar la falla, cuando se produzca, de forma transparente para el negocio.

La sola duplicación no es suficiente; debe haber una infraestructura de software que redireccione el tráfico del e–Banking fuera de los componentes dañados hacia aquellos aún activos, y mantenga una sincronización de las operaciones en todo momento.

Además, se deberán prever las funciones de gerenciamiento necesarias para estos casos de emergencias.

Conclusiones finales

El impacto que protagoniza el desarrollo de e–Banking se verifica tanto en las entidades financieras como en la sociedad en general.

Para aquellas entidades que exploten completamente su potencial, esta nueva forma de comunicación ofrece la posibilidad de grandes cambios que modifiquen radicalmente las expectativas de los clientes y redefinan el mercado, o creen mercados completamente nuevos.

Todas las organizaciones, incluidas aquellas que ignoran las nuevas tecnologías, sienten el impacto de estos cambios en el mercado y en las expectativas de los clientes. A su vez, los miembros de la sociedad se enfrentan con formas totalmente nuevas de adquirir bienes y servicios, acceder a la información e interactuar entre partes.

La seguridad de la información y las sanas prácticas de controles internos son temas con una tendencia creciente de criticidad debido al incremento de la tecnificación, la diversidad de las redes de computación, la explotación de los servicios más variados por Internet, el acelerado advenimiento del negocio financiero por distintos canales electrónicos (e–Banking, Internet Banking, m–Banking, etc.), y el mayor número de negocios que dependen de la información para sus operaciones diarias.

Una adecuada política de seguridad y de control será un requerimiento infaltable para la salud de cualquier entidad financiera.

"La sana administración de los riesgos,

asociada con la prestación íntegra de los servicios electrónicos

y el empleo de una seguridad efectiva,

será la clave para el mantenimiento de la confianza del público."

Glosario

Terminologías y conceptos aplicados a e–Banking

Amenaza. Llámase a la combinación del riesgo, su consecuencia, y la posibilidad de que el evento negativo vaya a suceder.

Autenticación. Verificación de la identidad de una persona o de un proceso para acceder a un recurso o poder realizar determinada actividad.
También se aplica a la verificación de identidad de origen de un mensaje.

Certificado. Pareja de clave privada y clave pública.
Físicamente son dos archivos que unidos, permiten definir un conjunto de claves de encriptación y una identidad certificada.
La clave privada nunca abandona el servidor, por lo que nadie obtiene esta información, y nadie podrá suplantar la identidad del servidor certificado.

Clave privada. Es la clave que tan sólo es conocida por el receptor y que se utiliza para desencriptar el mensaje que el emisor envía encriptado con la clave pública del receptor del mismo.
Este sistema de clave pública y clave privada se conoce como sistema asimétrico.

Clave pública. Es la clave que estará al alcance de todo el mundo para que un mensaje encriptado nos pueda ser remitido. También con ella puede desencriptarse lo que es encriptado con nuestra clave privada.

Confidencialidad. Los mensajes sólo podrán ser leídos por el emisor y el receptor.
En algunos países ya se han dado casos de denuncias contra la intimidad por intrusión en los lectores de correo electrónico y violación de correspondencia.

Cracker. Persona que intenta acceder a un sistema informático sin autorización. Se diferencian de los hackers por su clara identificación delictiva, y suele por lo general disponer de gran cantidad de mecanismos y estrategias que le posibilitan la intrusión en un sistema.

Criptoanálisis. Rama del conocimiento que se encarga de descifrar los mensajes encriptados sin conocer sus llaves.
Se dice que determinada clave ha sido “rota” cuando alguien logra descifrar un mensaje sin conocer la clave que le dio origen.

Criptografía. Ciencia que se ocupa de la escritura secreta, originada en el deseo humano por mantener ciertos temas bajo confidencialidad.

Denegación de Servicio. (DoS – Denial of Service): En Internet, un DoS o ataque de denegación de servicio es un incidente en el cual un usuario o una organización se ven privados de un recurso que normalmente podrían usar.
Habitualmente, la pérdida del servicio supone la indisponibilidad de determinado servicio de red, como el correo electrónico, o la pérdida temporal de toda la conectividad y todos los servicios de red.
Aunque normalmente es realizado de forma intencionada y maliciosa, este tipo de ataques suele ocurrir de forma accidental.

e–Business. (negocio electrónico) Cualquier tipo de actividad empresarial realizada a través de tecnologías de la Información y comunicaciones.

Firewalls.	Usados frecuentemente en los sistemas de e–Banking como una medida de seguridad para proteger redes internas. Deberían ser considerados en toda instalación conectada a alguna red externa. Los "firewalls" son sistemas que combinan la utilización de hardware y software, y se encuentran ubicados entre las redes que intercambian información teniendo en cuenta la dirección del flujo de la misma, lo que provee una puerta que resguarda el acceso no autorizado a la red interna.
Hacker.	Persona que tiene un conocimiento profundo acerca del funcionamiento de redes y que puede advertir los errores y fallas de seguridad del mismo. Al igual que un cracker busca acceder por diversas vías a los sistemas informáticos pero con fines de protagonismo.
Identidad del receptor.	No deben quedar dudas de quien es el destinatario del mensaje, un receptor anónimo o que suplante a otro puede utilizar la información en su propio beneficio.
Identidad del remitente.	Conocer con certeza quién es el emisor de un mensaje, tal como las órdenes de cargo en cuenta o de transferencias bancarias.
Integridad.	Toda manipulación no autorizada en un mensaje debe ser detectada para rechazar el mismo.
Intrusion Detection.	La detección de intrusos (IDS – Intrusion Detection Software) es otro ingrediente esencial en el ambiente de seguridad de Internet. Mientras el Firewall actúa como un cerco protector alrededor de la red corporativa, el IDS actúa como un sistema de monitoreo por video y alarma contra ladrones. Aunque se considera un sistema relativamente nuevo y su tecnología y diseño aún continua madurando, un servidor con un IDS estratégicamente colocado, se transforma en un factor crítico que proporciona protección adecuada para el ambiente de la Internet.
Protocolo.	Descripción formal de formatos de mensaje y de reglas que dos computadores deben seguir para intercambiar dichos mensajes.
Trojan Horse.	(Caballo de Troya) programa informático que lleva en su interior la lógica necesaria para que el creador del programa pueda acceder al interior del sistema que lo procesa.
WWW, Web o W3.	(World Wide Web). La Web es la parte de Internet a la que se accedes a través del protocolo HTTP mediante Browsers gráficos ó navegadores.

Fuentes de documentación

- **"Mobilize Your Enterprise: Achieving Competitive Advantage through Wireless Technology"**
  (Patrick Brans, Prentice Hall Professional, September 2002)

- **"Get–Started Guide to M–Commerce and Mobile Technology"**
  (Danielle Zillox, Amacom, June 2002)

- **"M–Commerce: Technologies, Services, and Business Models"**
  (Norman M. Sadeh, Wiley, John & Sons, Inc, March 2002)

- **"Wireless Internet and Mobile Business"**
  (Harvey M. Deitel, Paul J. Deitel, Tem Nieto, Kate Steinbuhler, Prentice Hall Professional, December 2001)

- **"Electronic Commerce 2002: A Managerial Perspective"**
  (Efraim Turban, Chung, David King, Merrill Warkentin, Jae Lee, Pearson Education, November 2001)

- **"E–Finance: The Electronic Revolution in Financial Services"**
  (Erik Banks, Wiley, John & Sons, August 2001)

- **"Electronic Banking: The Ultimate Guide to Online Banking"**
  (SCN Education BV, Vieweg Verlag/Morgan Kaufmann Publishers, April 2001)

- **"Risk Management Principles for Electronic Banking"**
  (Basel Committee on Banking Supervision – May 2001)

- **"e–Commerce Security Enterprise Best Practices"**
  (The Information Systems Audit and Control Association)

- **"Digital Signature – Security and Controls"**
  (The Information Systems Audit and Control Association)

- **"The Internet and the National Bank Charter – Comptroller's Corporate Manual"**
  (Office of the Comptroller of the Currency - January 2001)

- **"Risk assessment tools and practices for information system security"**
  (FFIEC Information Systems Examination Handbook – 2000)

- **"Electronic Finance: Reshaping the Financial Landscape around the World"**
  Stijn Claessens, Thomas Glaessner and Daniela Klingebiel (World Bank September 2000)

- **"Internet Banking - Comptroller's Handbook I-IB "**
  (Office Comptroller of the Currency Administrator of National Banks 1999)

- **"Treatment of material on overseas Internet World Wide Web sites accessible in the UK but not intended for investors in the UK"**
  (Financial Services Authority – 1998)

- **"Electronic Banking Group's Phase I Summary Report: Supervisory Issues and recommendations relating to electronic banking developments"**
  (Basel Committee on Banking Supervision – June 2000)

- **"Electronic Commerce - The New Business Perspective" extraido del Control Journal de I.S.A.C.A. Noviembre de 2000.**
  (Marcelo Héctor González, ASS, CISA)

Editado por Invercas S.A.