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

Fascículo II

Agosto
2004

Introducción

En el año 2001 se creó en el ámbito de la Superintendencia de Entidades Financieras y Cambiarias la **Comisión de e-Banking**. Los objetivos establecidos por la Comisión contemplan el análisis de la información relacionada con el desarrollo de la banca electrónica a nivel internacional y de la normativa emitida por los principales organismos reguladores en materia de sanas prácticas y controles de la actividad de e-Banking.

Como producto de la labor realizada, en el mes de enero de 2003 se emitió el fascículo **"e-Banking: Sanas prácticas"**, que fue remitido a las entidades financieras y a los principales actores del mercado de comercio electrónico. En dicha publicación, el análisis estaba dirigido a la identificación preliminar de los estándares de seguridad y las estructuras de controles a aplicar, así como la adecuación de tales requisitos a la realidad del sistema financiero argentino.

En esta oportunidad, la expectativa de la Comisión se centra en avanzar sobre algunos aspectos genéricos que impactan en la actividad tecnológica:

- en primer lugar, un breve desarrollo de los principales aspectos del proceso de tercerización, cuya importancia creciente merece destacarse;

- en segundo lugar, se comentan aspectos claves relacionados con el riesgo operacional, su consideración por el Comité de Basilea y, especialmente, su impacto en las actividades de e-banking; se adjunta además un breve sumario de las publicaciones realizadas por el Comité de Basilea, en relación con los aspectos de tecnología informática a ser contemplados por las entidades financieras;

- siguiendo con la identificación de estándares de seguridad mencionados en nuestro primer fascículo, se incorporan en esta publicación el análisis de la seguridad en redes y la exposición de información crítica, así como un glosario de términos de tecnología informática, y

- por último, se incorpora una sección con datos e indicadores de la actividad de e-Banking en las entidades financieras de nuestro país.

Cabe recordar a los lectores, que estos fascículos no pretenden definir conceptos técnicos específicos o brindar estándares relativos a e-Banking, especialmente considerando que corresponde a las entidades financieras 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 de rápidos cambios.

Por otra parte, y dado el balance positivo desde su implementación, es deseo de la Comisión continuar con el desarrollo del canal de comunicación oportunamente habilitado a través de la cuenta **comision.ebanking@bcra.gov.ar**. Las entidades interesadas en acceder a las actualizaciones y/o avisos sobre novedades y documentación relevante podrán dirigirse a esta dirección.

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

Outsourcing: “La Delegación en Terceros”

Introducción

Hoy en día las organizaciones se enfrentan a una cantidad de cambios y tendencias sin precedentes. Estos cambios incluyen la necesidad de ser globales, crecer sin utilizar más capital, responder a las amenazas y oportunidades de la economía, al envejecimiento de la fuerza laboral, la reducción de costos, y la batalla por lograr información sobre los intereses del consumidor.

La estrategia de tercerización apunta a que empresas de todo tamaño logren estructurar la asignación de sus recursos. Dicha estrategia podría traer beneficios productivos de importancia, o un crecimiento inmediato de la flexibilidad y agilidad necesarias para permanecer competitivos.

Cuando cumple los objetivos estratégicos planeados, la tercerización es la respuesta a una pregunta frecuente que se hacen las organizaciones para proporcionar un mejor servicio a los clientes: ¿producir o comprar? En combinación con otras técnicas, la tercerización permite la creación de un nuevo ambiente en la relación cliente-proveedor.

La tercerización surge cuando una organización transfiere la propiedad de un proceso de negocios a un proveedor. Se basa en el desprendimiento de alguna actividad, que no forme parte de sus habilidades principales, a un tercero especializado. Se entienden como habilidades principales o centrales a todas aquellas que conforman el negocio y en las que se tienen ventajas importantes con respecto a la competencia.

La tercerización: algunas definiciones

La tercerización es una importante tendencia en las decisiones administrativas y operativas de los últimos años en una gran cantidad de organizaciones del ámbito mundial. Según sus características puede definirse como:

- La transferencia de la propiedad de un proceso de negocios a un proveedor; la clave de esta definición es el aspecto de la transferencia de control.
- El uso de recursos externos a la organización para realizar actividades tradicionalmente ejecutadas con personal y recursos internos. Es una estrategia de administración por medio de la cual una organización delega la ejecución de ciertas actividades a organizaciones altamente especializadas.
- La delegación ó contratación a largo plazo de uno o más procesos no críticos del negocio a través de un proveedor más especializado, con el fin de conseguir una mayor efectividad, que permita orientar los esfuerzos de una compañía a las necesidades neurálgicas para el cumplimiento de una misión.
- La contratación externa de recursos anexos, mientras la organización se dedica exclusivamente a la razón o actividad básica de su negocio.
- Productos y servicios ofrecidos a una organización por proveedores independientes de cualquier parte del mundo, siempre que las leyes se lo permitan.

En un contexto de globalización de mercados, las organizaciones intentan dedicarse a innovar y concentrar sus recursos en el negocio principal. Por ello la tercerización ofrece una alternativa a ser analizada.

Básicamente se trata de una modalidad según la cual determinadas organizaciones, grupos o personas ajenas a la compañía son contratadas para hacerse cargo de “parte del negocio” o de un servicio puntual dentro de ella. La compañía delega la gerencia y la operación de uno de sus procesos o servicios a un prestador externo, con el fin de agilizarlo, optimizar su calidad y/o reducir sus costos.

Transfiere así los riesgos a un tercero que pueda dar garantías de experiencia y seriedad en el área. En cierto sentido, este prestador pasa a ser parte de la organización, pero sin incorporarse formalmente. Esta transferencia nunca debe entenderse como la delegación de la responsabilidad primaria de la organización que decide tercerizar las actividades. En otras palabras, la responsabilidad es indelegable.

La metodología de “tercerizar” es parte de la toma gerencial de decisiones. Esta toma de decisiones incluye los pasos de todo proceso de evaluación, planeamiento y ejecución; ayuda a planear y fijar expectativas de negocios e indica aquellas áreas donde se necesitan conocimientos especializados para realizar las distintas actividades.

Es preciso aclarar que la tercerización es diferente de las relaciones de negocios y contratación. En éstas últimas, el contratista es propietario del proceso y lo controla; es decir, le dice al proveedor qué y cómo quiere que se desempeñen y se fabriquen los productos o servicios comprados, por lo que el proveedor no puede variar las instrucciones en ninguna forma. Por el contrario, en el caso de la tercerización, el comprador transfiere la propiedad al proveedor; es decir, no instruye al mismo en como desempeñar una tarea sino que se enfoca en la comunicación de qué resultados quiere, y le deja al proveedor el proceso de obtenerlos.

Haciendo un poco de historia...

Después de la Segunda Guerra Mundial, las organizaciones trataron de concentrar en sí mismas la mayor cantidad posible de actividades, para no tener que depender de los proveedores. Sin embargo, esta estrategia que en principio resultara efectiva, fue haciéndose obsoleta con el desarrollo de la tecnología, ya que los departamentos de una organización nunca podían mantenerse tan actualizados y competitivos como lo hacían las organizaciones independientes especializadas en un área. Además, su capacidad de servicio para acompañar la estrategia de crecimiento era insuficiente.

El concepto de tercerización comienza a ganar credibilidad en el mundo al inicio de la década del 70', enfocándose sobre todo en las áreas de información tecnológica de las organizaciones. Las primeras organizaciones líderes en brindar servicios de tercerización fueron EDS e IBM.

De esa época data la denominación de “outsourcing” o tercerización, para describir la creciente tendencia de grandes compañías que estaban transfiriendo sus sistemas de información a proveedores.

El proceso de tercerización no sólo ha sido aplicado a los sistemas de producción o de explotación tecnológica, sino que ha alcanzado a la mayoría de las áreas de la organización. Los ejemplos más comunes contemplan la tercerización de:

- la administración de los recursos tecnológicos;
- la explotación integral de los sistemas de información;
- los sistemas financieros;
- los sistemas contables;
- las actividades de mercadotecnia;
- los servicios del área de recursos humanos,

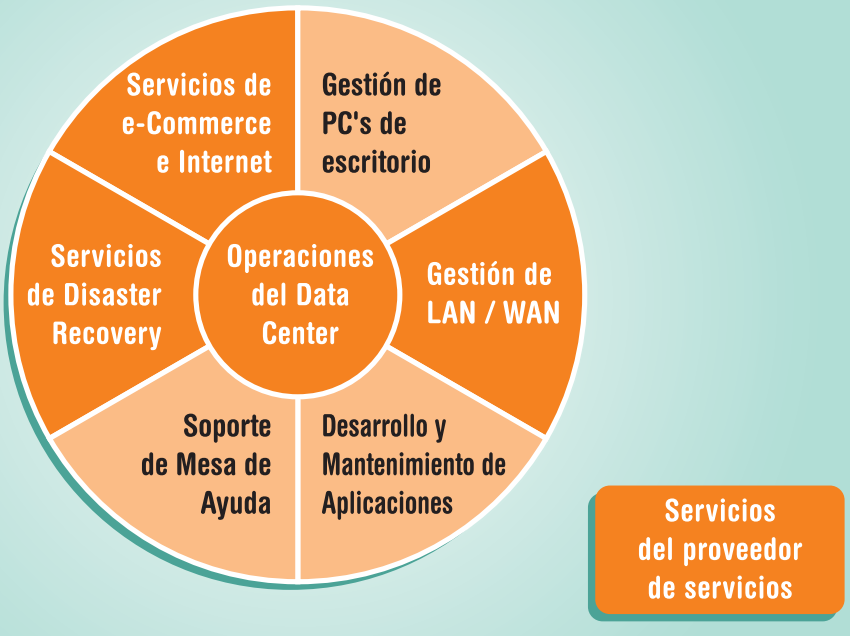
  y

- los sistemas administrativos.

El gráfico siguiente refleja componentes de los servicios informáticos que podrían ser transferidos a proveedores de servicios externos:

FUENTE: IDC

Componentes de la tercerización de los servicios de información



¿Por qué utilizar terceros?

Hasta hace poco tiempo, esta práctica era considerada como un medio para reducir los costos. Sin embargo, en los últimos años se ha demostrado como una herramienta útil para el crecimiento de las organizaciones por razones tales como:

- economía, reducción y/o control del gasto de operación;
- concentración en los negocios y disposición más apropiada de los recursos, debido a la reducción de la utilización de los mismos en funciones no relacionadas con la razón de ser de la compañía;
- disposición de personal altamente capacitado, y
- mayor eficiencia.

Todo esto permite enfocarse ampliamente en asuntos organizacionales y del negocio, acceder a recursos especializados, acelerar los beneficios de la reingeniería, compartir riesgos y destinar recursos para otros propósitos.

Algunas ventajas de la tercerización

Los partidarios de implementar una estrategia de tercerización aducen que la organización contratante (o "el comprador") obtendrá beneficios ya que logrará, en términos generales, una "funcionalidad mayor" a la que tenía internamente, con "costos inferiores" en la mayoría de los casos, en virtud de la economía de escala que obtienen los proveedores contratados.

En estos casos la organización debería preocuparse exclusivamente por definir la funcionalidad de las diferentes áreas de su organización, dejando que el prestador se ocupe de decisiones de tipo tecnológico, manejo del proyecto, implementación, administración y operación de la infraestructura.

En resumen, un adecuado proceso de tercerización podría permitir:

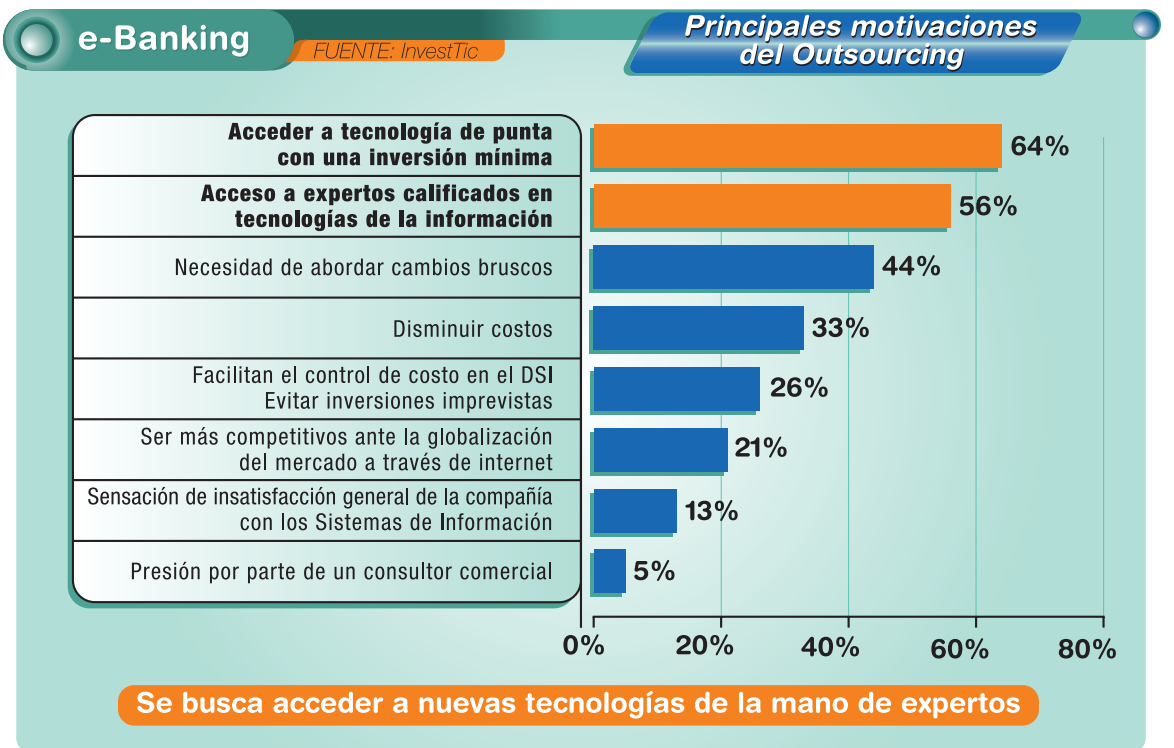
- aplicar el talento y los recursos de la organización en las áreas claves;
- aumentar la rentabilidad a través de la reducción de costos;
- transformar costos fijos en variables flexibilizando su estructura;
- ayudar al enfrentamiento de los cambios en las condiciones de los negocios respondiendo con rapidez;
- obtener los beneficios de la especialización en áreas de negocio;
- acceder a recursos de tecnología avanzada sin la necesidad de entrenar personal de la organización;
- disponer de servicios de información en forma rápida considerando las presiones competitivas, y
- contribuir a redefinir la organización.

Algunas desventajas de la tercerización

En todo proceso existen aspectos negativos que forman parte integral del mismo. La tercerización no queda exenta de esta realidad.

Algunas desventajas que podrían presentarse son:

- la organización pierde contacto con las nuevas tecnologías que ofrecen oportunidades para innovar los productos y procesos;
- el proveedor externo debe aprender y tener conocimiento del negocio en cuestión, existiendo la posibilidad de que los utilice para impulsar su propia industria y se convierta en un competidor;
- el costo ahorrado con el uso de terceros puede no ser el esperado;
- alto costo en el cambio de proveedor en caso de que el seleccionado no resulte satisfactorio, y
- pérdida parcial del control sobre el negocio.



Estrategias de tercerización

Cuando una organización decide llevar a cabo un proceso de tercerización, debe definir una estrategia que guíe dicho proceso.

Hay dos tipos genéricos de estrategia: la periférica y la central. La periférica surge cuando la organización requiere los servicios de proveedores externos para que se ocupen de las actividades de poca relevancia estratégica. La central surge cuando las organizaciones contratan el desarrollo de actividades consideradas de gran importancia y larga duración para obtener el éxito.

La estrategia debe definirse claramente, de manera que asegure que el proceso esté regido por las políticas generadas por la organización en relación con la tercerización. Dichas políticas deben ser conocidas por los empleados involucrados en el proceso y estar ampliamente respaldadas por la Alta Gerencia.

Otros de los aspectos a considerar dentro del proceso estratégico es el tipo de relación que se establecerá entre la organización que contrata y el proveedor. En esta relación existen dos componentes: uno interpersonal, que establece como interaccionan el equipo responsable dentro de la organización con el equipo del proveedor; y el componente corporativo, que define las interacciones a nivel directivo entre ambas partes.

En la actualidad las organizaciones buscan relaciones más formales y a largo plazo, donde el equipo interno asume un rol de socio estratégico, lo que permite un mejor entendimiento del desarrollo de la estrategia del proveedor. La ventaja de este tipo de relación es que permite a ambas partes familiarizarse con el personal y el estilo operativo de la otra organización y ayuda a que el proveedor pueda satisfacer las expectativas del contratante de manera más efectiva en términos de comunicación y frecuencia en los reportes.

Otra clave del proceso estratégico es la medición del desempeño del proveedor seleccionado en términos de tiempo, adherencia al presupuesto y al éxito del proyecto medido sobre la base del logro de los objetivos planteados. Si los niveles de desempeño no pueden medirse numéricamente, se pueden crear escalas de medición subjetivas acordadas con el proveedor.

Es recomendable compartir los resultados obtenidos con el proveedor, especialmente si se

desean tener relaciones de largo plazo. Debe dejarse claramente establecido que cuando se comparten estos resultados no se trata de una forma de castigo o reclamo al proveedor, sino un medio para la búsqueda de áreas de mejora.

La estrategia debe definir la integración del equipo de tercerización, estableciendo las habilidades mínimas necesarias. Un equipo de este tipo generalmente está compuesto por personas de áreas comerciales, técnicas, y financieras, entre otras. Sin embargo, la composición del equipo varía dependiendo del alcance del proyecto y la actividad a delegar al tercero.

Por último, se debe cerrar la elaboración de la estrategia haciendo partícipes de la misma no sólo a los directores, sino también a los gerentes experimentados en las actividades a delegar, ya que pueden proporcionar los aspectos operacionales claves para la estrategia.

Contratos de tercerización

Al considerar la negociación de un contrato de tercerización deberían tenerse en cuenta ciertos aspectos tales como:

- decisiones iniciales,
- definir la terminología,
- estructura del contrato,
- personal,
- locales e instalaciones,
- hardware,
- software,
- términos de cargos y pagos,
- identificar las responsabilidades del proveedor,
- identificar la responsabilidad del cliente, y
- seguridad.

A continuación se incluye una guía con algunas preguntas que contemplan estos aspectos:

Decisiones iniciales

Definir que sistemas y/o servicios van a subcontratarse.

Confirmar la viabilidad financiera del proveedor.

Observar qué tipo de indemnización existirá por fallas del proveedor.

¿Quién iniciará la elaboración del contrato: el proveedor o el cliente?

¿Qué recursos deberán utilizarse en la elaboración del contrato y su negociación?

Por ejemplo:

- Administración funcional
- Experiencia técnica
- Administración de contratos
- Asesoría legal interna
- Asesoría legal externa

Decidir la fecha de inicio para el contrato.

Decidir la fecha de transición para el inicio de los servicios de tercerización.

¿Cuál será la duración del contrato?

Definir la terminología

Definir los términos apropiados para un acuerdo particular de tercerización, por ejemplo, los servicios y el nivel de servicios.

¿Se han identificado y cuantificado las actividades claves?

Identificar los establecimientos donde se realizaran los servicios.

Identificar los equipos que se usarán para proveer los servicios.

Identificar el software que se utilizará para los servicios si se va a subcontratar tecnología informática.

Estructura del contrato

¿Sería apropiado integrar en el contrato documentos de invitación a licitación y respuesta a licitación, o ha cambiado la situación desde que se elaboraron los documentos?

¿Va a haber un solo contrato o será más pertinente tener contratos múltiples? La última opción podría ser una forma práctica para estructurar el contrato si puede dividirse en etapas definidas, como por ejemplo, tercerización de servicios operativos seguidos por el desarrollo de nuevos servicios, o si formará parte de los acuerdos una transferencia de activos.

Personal

¿Formarán parte del arreglo de tercerización algunos miembros del personal actual del cliente, y en caso de ser así, por transferencia temporal o transferencia definitiva?

¿Se aplica la reglamentación existente en cuanto a protección del empleo?

¿Cuál es el grado de indemnización de cada parte en caso de demandas relacionadas sobre cuestiones de empleo?

Locales e instalaciones

¿Dónde se efectivizarán las prestaciones del contrato, en las instalaciones del proveedor o del cliente?

¿Se venderían o se rentarían al proveedor instalaciones que requieran un contrato distinto por las propiedades?

¿Debe negociarse una venta , leasing o alquiler?

Hardware

El proveedor ¿es responsable de proporcionar el equipo para el funcionamiento operativo de los servicios en sus propias instalaciones?

El proveedor ¿va a utilizar el equipo del cliente en las instalaciones del cliente?

¿Se transferirá equipo de las instalaciones del cliente a las del proveedor?

¿Se ha definido la responsabilidad para asegurar que se obtengan todos los permisos y licencias de terceras partes que tiene un interés legal en el equipo?

¿Es necesario un contrato separado para dirigir la transferencia de propiedad?

¿Quién será responsable de los seguros?

¿Quién será responsable de los arreglos y pagos de mantenimiento?

¿Se requerirá un contrato separado para el mantenimiento?

Software

¿El proveedor utilizará software propio?

¿El cliente otorgará la licencia de su propio software para que lo utilice el proveedor en el outsourcing?

¿Ha obtenido el proveedor las licencias para el uso de software de terceros?

¿Quién poseerá los derechos del software que se desarrolle en los arreglos de tercerización?

Términos de cargos y pagos

¿Cómo se calculan los cargos por el servicio?

¿Pueden producirse volúmenes y controlarse con suficiente exactitud para que sea viable un cargo fijo?

Los cargos ¿Se calcularán en función del tiempo y recursos?

¿Están los cargos relacionados directamente con el desempeño en el nivel de servicio?

¿Habrá un sistema de penalización / descuento por incumplimiento de los niveles de servicio que no estén dentro de los criterios acordados?

¿Habrá alguna limitación en variaciones en los niveles por cargos a pagar?

¿Habrá algún trabajo de desarrollo? ¿Cómo se reglamentará?

¿Con qué frecuencia se revisarán los cambios?

¿Hay alguna limitación en los criterios para la revisión, como algún índice de precios en particular, estudios de salarios en computación, etc.?

¿Existe alguna posibilidad de que disminuyan los cargos con el tiempo?

¿Cuáles van a ser los métodos de pago?

Identificar las responsabilidades del proveedor

Auxiliar en la evaluación de los niveles de servicio.

Cumplir los niveles de servicios.

Nombrar un representante.

Revisar regularmente los arreglos de tercerización.

Cumplir las normas del cliente en materia de higiene y seguridad.

Identificar la responsabilidad del cliente

¿Quién asistirá a las reuniones?

¿Cuáles serán los procedimientos especiales para los problemas no resueltos en las reuniones?

¿Se prevé que existan auditorias independientes del sistema?

Seguridad:

¿Es necesaria la confidencialidad en el desempeño de los contratos?

¿Está preparado el proveedor para dar una garantía de cumplimiento de protección de los datos?

¿Se someterá el proveedor a las disposiciones legales o reguladoras que debe cumplir la organización que lo contrata?

Claves para una adecuada tercerización

Claridad de objetivos

El elemento más importante en el éxito de una relación de tercerización a largo plazo es la claridad de objetivos. La organización debe tener muy bien definidas las metas que se pretenden alcanzar con la tercerización. Con igual o mayor importancia aún, las metas deben estar adecuadamente expresadas, habiéndose comprometido el proveedor a ser medido en su desempeño basándose en ellas.

Expectativas realistas

La tercerización sólo es un medio, una herramienta; como tal, tiene limitaciones. Es importante entonces fijar su frontera dentro de los límites de lo posible. Debe existir un parámetro que fije las expectativas de ambos lados al entrar en una relación de tercerización.

Definición detallada de la cartera de servicios incluidos

En muchas ocasiones, el proveedor tiende a definir vagamente la cartera de servicios incluidos en el costo básico de una relación de tercerización. Más aún, estas vaguedades son muchas veces utilizadas exitosamente como estrategia de penetración del cliente: se gana al cliente con precios artificialmente bajos para luego sacar la carta secreta de “los servicios no contemplados” en el costo.

Una vez firmado el contrato y concluida la transferencia de las operaciones al proveedor, comienza la letanía de excepciones o servicios no incluidos que originan innumerables cargos adicionales. Para evitar este mal, casi endémico, es sumamente importante la definición clara y precisa de todos los servicios incluidos.

Definición adecuada de niveles y modelos de servicio

En este rubro se incluyen los criterios mínimos a considerar en cuanto a los servicios prestados como parte de una relación de tercerización entre las partes.

Cada servicio debe tener asociado tanto el modelo de prestación adoptado, como los parámetros de aceptación y medición de su desempeño. Así, el cumplimiento de la relación puede ser controlado por una batería de indicadores, los cuales sirven tanto para señalar si la relación es adecuada, como para tomar medidas preventivas y/o correctivas en caso de que algunos servicios muestren tendencias a la degradación antes de convertirse en problemas críticos.

Flexibilidad financiera

El éxito de una relación de tercerización tiene como fundamento el beneficio económico de ambas partes. Como medida de prevención, los contratos deben incorporar suficiente flexibilidad financiera como para adaptarse a condiciones cambiantes que puedan afectar el costo total de la relación comercial entre las partes, garantizando de alguna manera el beneficio económico buscado originalmente.

Compromiso del proveedor

Una de las ventajas competitivas más fuertes de la tercerización es la disponibilidad, por parte del proveedor, de recursos altamente calificados para resolver los problemas operativos en la infraestructura informática del cliente. Como tal, el proveedor debe comprometerse a mantener la disponibilidad prometida a lo largo de la relación. Como toda relación exitosa de negocios, es necesario que el proveedor garantice una continuidad y calidad mínima en los recursos humanos asignados a la atención y cumplimientos de los compromisos contraídos.

Conformidad gerencial

El éxito de todo proyecto a largo plazo depende, en gran medida, de la continuidad del equipo gerencial responsable del mismo. Este requisito se acentúa más aún en el caso de la tercerización, dado que las condiciones generales de la relación se fijan justo antes de su comienzo formal, en el momento de la negociación y firma del contrato de prestación de servicios.

A partir de allí, el éxito de la relación depende de la adecuada interpretación y el seguimiento de las cláusulas establecidas en el contrato. Por ello, es esencial que los equipos gerenciales responsables del proyecto por ambas partes, se involucren plenamente en las negociaciones contractuales. Ésta es, ciertamente, una garantía importante para el éxito de la relación a largo plazo.

Flexibilidad tecnológica

Las relaciones de tercerización generalmente se expresan en contratos de prestación de servicios a largo plazo. Por lo tanto, para evitar problemas causados por obsolescencia tecnológica no prevista en la transacción original, ésta debe incorporar definiciones y procedimientos de actualización tecnológica (por ejemplo, criterios básicos de evaluación e incorporación de nuevas tecnologías a los servicios prestados). Tales salvaguardas garantizan una de las premisas básicas de la tercerización: la tecnología, manejada por expertos redituando beneficios reales al negocio.

Flexibilidad operativa

Uno de los objetivos más importantes de la tercerización es profesionalizar la operación informática del cliente. Más allá de compromisos formales y definiciones exactas de servicios prestados, el resultado esperado de una solución de tercerización es, generalmente, el mejoramiento y eficiencia de la operación debido a la variedad de situaciones y cambios de condiciones operativas que puedan ocurrir durante el transcurso de la relación.

Es muy importante que la relación original incorpore suficientes elementos de flexibilidad que puedan ser utilizados posteriormente para cambiar los términos operativos (inclusive la definición de los servicios prestados), sin necesidad de recurrir a tortuosas renegociaciones del contrato.

Los riesgos de la tercerización

Los riesgos involucrados en las actividades tercerizadas fluctúan entre los riesgos operacionales y los riesgos estratégicos. Entre los riesgos de la tercerización se pueden mencionar:

- no negociar adecuadamente el contrato;
- inadecuada selección del contratista;
- incremento en el nivel de dependencia de entes externos;
- inexistente control sobre el personal y/o actividades del contratista;
- incremento en el costo de la negociación y monitoreo del contrato, y
- pérdida de confidencialidad.

La tercerización en las entidades financieras de la República Argentina

Actualmente, para efectuar ciertas actividades vinculadas con sus sistemas de información y/o tecnologías informáticas, se observa una tendencia de las organizaciones bancarias a la utilización de servicios provistos por otras empresas, o su transferencia a dependencias de la organización controlante, dentro de su ámbito local o a escala internacional.

Esta manera de concretar las actividades descentralizándolas, implica un nuevo panorama, cuyas consecuencias deben ser analizadas desde el punto de vista de las dificultades para la definición de los alcances que surgen para los entes de contralor, y además, la posible disminución de las necesidades de recursos laborales locales, en el caso de descentralizaciones en el exterior del país.

El surgimiento de riesgos producto de la tercerización, debe ser adecuadamente considerado por las entidades contratantes, toda vez que dicho proceso implica la delegación de una actividad ó función, pero nunca supone el traspaso de la responsabilidad a quien suministra el servicio o la actividad delegada.

Un riesgo crítico inherente al proceso es el que pudiera surgir de la entrega de información confidencial o estratégica a un tercero (sobre la clientela, registros contables, etc.), o por la creación de una relación dependiente ante el mismo (proveedor) que básicamente sustituirá a la entidad financiera involucrada.

A efectos de prevenir los riesgos a que se alude en los párrafos precedentes, se entiende necesario establecer sanas prácticas a ser observadas en las organizaciones financieras que decidan optar por descentralizar y/o tercerizar sus funciones tecnológicas.

En esa línea aparece como condición la necesidad de que la relación se formalice mediante la suscripción de un contrato, que cuente con cláusulas que delimiten con precisión los alcances de las funciones que constituyen su objeto.

También debe contemplarse el detalle de las responsabilidades de ambas partes, el sometimiento de la prestadora a la potestad de la entidad financiera de revisar el contrato, renegociarlo y hasta rescindirlo unilateralmente de verificarse apartamientos de los compromisos asumidos.

Dentro de dichos compromisos se encuentra la adecuación a las normas establecidas por la Ley de Entidades Financieras y por el B.C.R.A., en caso de que sus tareas comprendan aspectos que formal o esencialmente se le impongan al intermediario autorizado, así como a la aceptación del ejercicio de la supervisión del Ente Rector para auditar periódicamente su cumplimiento.

A tales fines debe asegurarse la existencia de un fluido canal de comunicación entre la entidad financiera y el órgano descentralizado o proveedor, así como la aplicación de controles y mecanismos independientes de validación.

Para ello, tanto la auditoría interna como la externa, deben tener acceso a la información y datos relevantes, tales como la formulación de planes de contingencias frente a algún inconveniente en el desempeño del proveedor.

Parece obvio que la satisfacción de las antedichas exigencias conlleva la disposición de capacidad técnica y administrativa, familiaridad con la actividad financiera y facultad para adecuarse a las innovaciones tecnológicas, condiciones indispensables para que los terceros (proveedores en el ámbito local u otras organizaciones vinculadas en el exterior), puedan ser elegidos por las entidades financieras.

Existe actualmente un conjunto normativo que establece las prácticas que las entidades financieras deben procurar cuando determinen delegar en terceros actividades relacionadas a la tecnología informática y a los sistemas de información dentro de la Republica Argentina.

Primariamente se estipulaban los aspectos de control interno que las entidades debían procurar con sus prestadores de servicios de tecnología informática y sistemas de información, mediante la Comunicación “A” 2659, que en síntesis requería:

> *“La existencia de contratos formalmente establecidos con los proveedores externos de software, procesamiento y/o servicios, en donde se contemplen aspectos tales como: el procedimiento por el cual la entidad pueda obtener los datos, los programas fuentes, los manuales y la documentación técnica de los mismos, ante cualquier situación que pudiera sufrir el proveedor por el cual dejara de operar o de prestar sus servicios en el mercado, a fin de poder asegurar la continuidad de procesamiento.*
>
> *Además, los contratos o acuerdos de prestación de servicios, deben establecer claramente la no existencia de limitaciones para la Superintendencia de Entidades Financieras y Cambiarias, en cuanto al acceso a los datos y a toda documentación técnica relacionada (diseño de archivos, tipo de organización, etc.).”*

Ya en esa primera etapa, se formulaba la responsabilidad primaria del control a la entidad, mediante el enunciado siguiente:

> *“Las entidades deben contar con recursos humanos técnicamente capacitados para ejercer un control eficiente sobre las tareas que desarrolla el proveedor externo, ya sea a través de agentes bajo relación de dependencia o que no estén vinculados con los proveedores externos.”*

Con el transcurso del tiempo, a medida que se apreció un mayor grado de delegación de tareas en terceras partes, se amplió el aspecto normativo, mediante la Comunicación “A” 3149, donde se establecen los recaudos que las entidades deben cumplir antes y durante los procesos de tercerización y/o descentralización de actividades de tecnología informática y sistemas de información, tanto cuando el ámbito de la tercerización fuera en el territorio de la República Argentina, como en el exterior.

El Riesgo Operacional

Introducción

Desde hace algunos años, el tema de la administración de riesgos ha captado, cada vez con mayor énfasis, la atención de las instituciones financieras y los organismos regulatorios en todo el mundo. Se ha publicado profusa bibliografía sobre el tema, desde artículos especializados hasta el desarrollo de complejos modelos de estimación de riesgos. Las autoridades de contralor han definido para cada una de sus regiones, en mayor o menor medida, los estándares de administración del riesgo que deben atender las instituciones financieras.

En este contexto, y como uno de los principales actores en el desarrollo de regulaciones para la banca, el Comité de Supervisión Bancaria de Basilea emitió en Junio 1999 una propuesta de mejora del marco de suficiencia del capital (aún en estado de documento consultivo), más conocida como "Basilea II" o "Nuevo Acuerdo de Capital de Basilea".

Según lo manifestado por el Comité, el objetivo al que se enfoca el Nuevo Acuerdo de Capital es poner énfasis en la gestión del riesgo y fomentar mejoras continuas en la capacidad de los bancos para evaluar riesgos. Dichos objetivos podrían ser logrados a través del acercamiento de los requerimientos de capital a las prácticas de administración de riesgos más utilizadas, o en otras palabras, aumentando la sensibilidad al riesgo de los requerimientos de capital.

De acuerdo con las definiciones de "Basilea II", el nuevo marco se apoya en tres Pilares: los requisitos de capital mínimo, el proceso de examen por parte de la supervisión bancaria y la utilización eficaz de la disciplina de mercado. La combinación de estos tres elementos debería permitir, tanto a entidades financieras como a organismos reguladores, una mejor administración del riesgo.

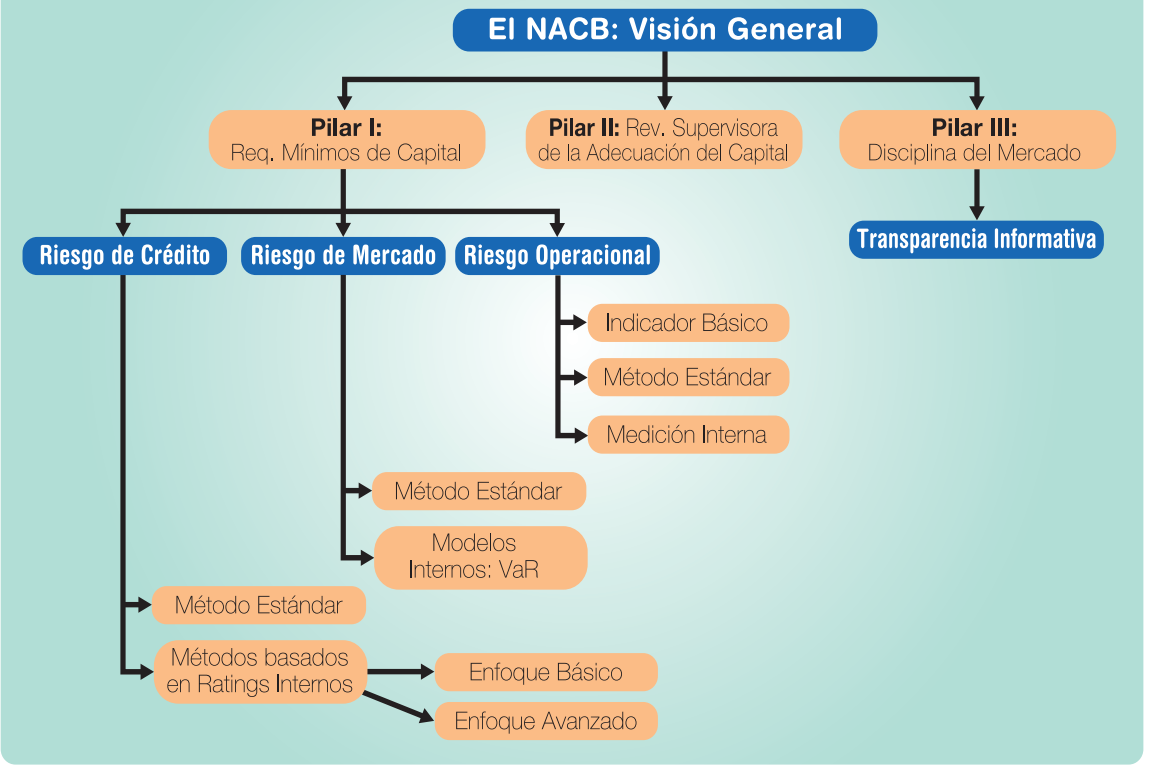
El Nuevo Acuerdo de Capital de Basilea:

La incidencia del riesgo operacional

Como se menciona en la introducción, el Comité de Supervisión Bancaria ha propuesto una modificación al Acuerdo de Basilea de 1988, que determinaba un "colchón" general de capital que respondía tanto a los requisitos por los riesgos medidos (de crédito y de mercado) como al resto de los riesgos no medidos. La nueva propuesta es consecuente con la meta establecida por el Comité de *desarrollar metodologías que reflejen cada vez más un perfil de riesgo particular para cada banco*.

El Nuevo Acuerdo de Capital establece tres pilares: los requisitos de capital mínimo, el proceso de revisión supervisora y la disciplina de mercado (Fig.1). Antes de profundizar en el tema del riesgo operacional, es conveniente comentar brevemente los principales conceptos referidos a estos tres Pilares.

Fig. 1 El Nuevo Acuerdo de Capital de Basilea



El Pilar I

En la propuesta del Nuevo Acuerdo, el coeficiente mínimo de capital requerido del 8% permanece intacto. De esta forma, lo que se modifica es la definición de activos ponderados por su nivel de riesgo, es decir, los métodos utilizados para medir los riesgos a los que se enfrentan los bancos.

El Acuerdo vigente (Basilea 1988) cubre explícitamente tan sólo dos tipos de riesgos al definir los activos ponderados por su nivel de riesgo: (1) riesgo de crédito y (2) riesgo de mercado. Se entiende que el tratamiento de estos dos grandes riesgos cubre implícitamente otros riesgos. La propuesta del Nuevo Capital no prevé ninguna modificación para este tratamiento de los "riesgos no medidos".

En el Nuevo Acuerdo el primer pilar propone cambiar la definición de activos ponderados por su nivel de riesgo, a través de dos elementos principales: (1) modificaciones sustanciales en el tratamiento del riesgo de crédito con respecto al Acuerdo vigente; y (2) **la introducción de un tratamiento explícito para el riesgo operativo**, lo cual resultará en una medición de dicho riesgo que se incluirá en el denominador del coeficiente de capital del banco.

En los dos casos, el Nuevo Acuerdo prevé tres opciones para el cálculo del riesgo de crédito y otras tres para el cálculo del riesgo operativo. La capacidad de las instituciones financieras para cumplir con los criterios específicos que demanda cada opción determinará el marco usado para el cálculo del capital de riesgo.

La inclusión del riesgo operativo es el punto más novedoso de la Propuesta de Acuerdo en cuanto a la definición y cálculo del capital a riesgo, atento a que en forma previa los únicos riesgos contemplados expresamente para su medición eran "crédito" y "mercado". En el Nuevo Acuerdo se prevén tres enfoques de medición del riesgo operacional. Básicamente, los mismos son:

- **Enfoque del Indicador Básico** (Basic Indicator Approach): en este caso, se une la exigencia de capital por riesgo operacional a un indicador de riesgo único. El indicador considerado por Basilea es el ingreso bruto promedio de los últimos tres años. Los bancos que apliquen este enfoque mantendrán capital por riesgo operativo igual a un porcentaje fijo de sus ingresos brutos.

- **Enfoque Estándar** (Standardized Approach): en este enfoque, se toma el método del Indicador Básico como punto de partida y se dividen las actividades del banco en líneas de negocio. La exigencia de capital por cada una de esas líneas surgirá de aplicar un porcentaje fijo a un indicador de riesgo operativo, sin que éstos sean necesariamente los mismos para todas las líneas. La exigencia de capital por riesgo operativo será la suma de las exigencias por cada línea.

- **Enfoque de Medición Interna** (Advanced Measurement Approaches- AMA): este método permite a los bancos que cumplen condiciones de supervisión más estrictas, la utilización de datos internos a fin de la medición del capital por riesgo operativo. Las entidades deberán recopilar información para estimar tres indicadores cuantitativos para cada línea de negocios y tipo de riesgo que representan: i) exposición al riesgo operativo, ii) probabilidad de que se produzcan pérdidas y iii) monto de la pérdida si ésta se produce. Con estos indicadores cuantitativos y un porcentaje fijo establecido por el Comité de Basilea para cada línea de negocios basado en sus análisis de la industria bancaria se determinará el monto de capital regulatorio por el riesgo operativo. La exigencia total de capital por riesgo operativo, como en el Enfoque Estándar, surge de la suma de los requisitos por cada línea de negocios.

Los pilares II y III

El Comité de Basilea entiende que la revisión de los supervisores bancarios y la disciplina de mercado son complementos esenciales de los requisitos de capital mínimo establecidos.

Por un lado, la supervisión bancaria debería enfocarse a analizar si las entidades financieras cuentan con procesos internos de medición de riesgo confiables para evaluar la suficiencia de su capital. En ese proceso debería considerar las habilidades de la Gerencia para valorar adecuadamente la suficiencia del capital, las estrategias para mantener niveles adecuados de capital, y la intervención de los supervisores cuando los resultados de estas evaluaciones no sean satisfactorios.

Por otra parte, la inclusión de la disciplina de mercado como Pilar III está orientada a considerar las posibles implicancias de la utilización de metodologías internas de cada banco, a los efectos del cálculo de los requisitos de capital por riesgo crediticio y riesgo operativo. Dado que el Nuevo Acuerdo prevé esta posibilidad, el Comité de Basilea impulsa a través del Pilar III, la divulgación de las metodologías empleadas a fin de que los participantes del mercado conozcan y comprendan la relación entre el perfil de riesgo de una entidad y su capital.

El riesgo operacional: esbozo de su definición

En nuestra anterior presentación definíamos el riesgo operacional de la siguiente forma:

Los eventos más importantes de riesgo operacional involucran fallas en los controles internos y/o en el "gobierno de las organizaciones" (corporate governance). Tales fallas pueden llevar a grandes pérdidas financieras, que pueden producirse a causa de fraudes y/o incumplimientos (por ejemplo, problemas en la disponibilidad de los sistemas), o pueden generar que los intereses del banco se vean comprometidos debido a conductas de su personal reñidas con la ética o por mal desempeño de sus funciones (por ejemplo, asunción de riesgos no autorizados por la Dirección). Sin embargo, no sólo estos "eventos" involucran riesgo operacional: dentro de éste se consideran también los eventos externos, incluyendo los desastres "naturales" (inundaciones, etc.) así como las consecuencias de, por ejemplo, un ataque terrorista.

e-Banking

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.

Sin embargo, existen numerosas definiciones del riesgo operacional que incluyen, entre otras, las siguientes:

- Riesgo operacional es el asociado a la posibilidad de fallas de los sistemas en un mercado determinado...
- Es el riesgo asociado con errores humanos, procedimientos y/o controles inadecuados, actividades criminales y fraude,...
- Son los riesgos causados por deficiencias tecnológicas y fallas de los sistemas...
- Son todos los riesgos que "no son específicos de la banca" y que derivan de decisiones de negocio, competencia...
- Comprende el riesgo legal y el riesgo estratégico o de negocio, las fallas en cumplir los requerimientos regulatorios y el impacto adverso en la reputación de los bancos...

Inclusive, algún tiempo atrás, algunos bancos definían el riesgo operacional como todo riesgo que no se enmarcara en las definiciones de riesgo de crédito y riesgo de mercado. Actualmente se tiende a utilizar la definición propuesta por Basilea, aunque algunos autores aconsejan a los bancos crear una propia, útil a sus propósitos internos.

Es importante que, cualesquiera sea la definición a utilizar, se considere el rango completo de riesgos operativos que enfrenta cada entidad. Al respecto, en las últimas publicaciones del Comité se incluye una guía de "clasificación de eventos de pérdida por riesgo operacional", algunos de cuyos datos resulta útil conocer:

FUENTE: Comité de Basilea

Clasificación de eventos de pérdida por riesgo operacional

Categorías de tipos de eventos	Definición
Fraude interno y externo	Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o a soslayar regulaciones, por parte de una parte interna de la organización o por terceros. Ejemplos: • Operaciones no autorizadas • Operaciones no reveladas (intencionalmente) • Hurto y fraude • Daños por ataques informáticos • Robo de información
Relaciones laborales y seguridad en el puesto de trabajo	Pérdidas derivadas de actuaciones incompatibles con la legislación y/o acuerdos laborales. Ejemplos: • Cuestiones relativas a remuneración, contratos, etc. • Eventos relacionados con las normas de seguridad en el trabajo
Prácticas con clientes, productos y negocios	Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación profesional frente a clientes concretos, o derivadas de la naturaleza o diseño de un producto. Ejemplos: • Aspectos de divulgación de información de clientes • Violación de privacidad • Defectos de los productos (no autorizado, fallas en diseño, etc.) • Prácticas ajenas a la competencia
Daños a activos materiales	Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos. Ejemplos: • Pérdidas por desastres naturales • Pérdidas por vandalismo, terrorismo
Incidencias en el negocio y fallas en los sistemas	Pérdidas derivadas de fallos en los sistemas. Ejemplos: • Interrupción de suministros de servicios • Problemas de hardware, software, telecomunicaciones, etc.
Ejecución, entrega y gestión de procesos	Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores. Ejemplos: • Comunicaciones defectuosas • Incumplimiento de plazos o de responsabilidades • Inexistencia de autorizaciones de alta / rechazo de clientes • Tercerización de determinados servicios

Si bien surge de la amplia bibliografía existente que la definición antes mencionada (ver recuadro "Riesgo operacional") cuenta con mayor consenso que el resto, en la elaboración de la propuesta de una exigencia regulatoria mínima de capital por riesgo operativo y los documentos relacionados, el Comité de Basilea ha adoptado la siguiente definición: "Riesgo operacional es el riesgo de pérdidas, directas o indirectas, resultante de procesos internos, comportamientos humanos y/o sistemas inadecuados o fallidos, o de eventos externos". A los fines de la determinación de una exigencia regulatoria mínima de capital por riesgo operativo, esta definición incluye el riesgo legal, pero excluye los riesgos estratégico, de reputación y sistémico.

En los fundamentos de la adopción de esta definición, el Comité señala que su objetivo es estimular a la industria bancaria a desarrollar metodologías y a recopilar datos relacionados con la administración del riesgo operacional. Por ello, al formular las propuestas para la definición de un capital regulatorio mínimo por riesgo operativo elige esta definición que se enfoca en las causas del riesgo operacional.

La novedad que traen los enfoques sobre riesgo operacional es el tratamiento de la administración de este riesgo como una disciplina particular, con su propia estructura de controles, herramientas y procesos, distintos de la administración del riesgo de crédito y del riesgo de mercado. El Comité de Basilea refuerza esta tendencia al desarrollar el tema e incorporarlo como punto clave en la determinación de los capitales mínimos de las entidades financieras.

Sin embargo, ha de destacarse que toda esta disciplina se encuentra aún en etapa de desarrollo, inclusive en los sistemas financieros más avanzados. Las causas se encuentran, sobre todo, en la falta de experiencias y antecedentes válidos, aplicables a la mayoría de las entidades, en cuanto a la obtención de un consenso sobre la definición del riesgo operacional, sobre qué se entiende por evento de riesgo operacional, sobre la medición de las pérdidas asociadas a un evento de riesgo operacional, entre otros temas.

Aún teniendo en cuenta la indefinición sobre estas cuestiones, en la actualidad de los mercados financieros, la administración del riesgo operacional se ha convertido en un punto importante a considerar dentro de las "sanas prácticas" que debería contemplar un banco.

Comentarios sobre la situación actual en cuanto al riesgo operacional

A los fines de su trabajo sobre la administración de riesgo operacional, Basilea ha llevado a cabo numerosas reuniones con organizaciones bancarias y autoridades de supervisión. De las discusiones con dichos actores, surgen algunos temas en común que el Comité señala como relevantes:

- El conocimiento y tratamiento del riesgo operacional al nivel de la Dirección y la Gerencia se encuentra en proceso de avance. En la realidad, los bancos que consideran el tema han designado como responsables primarios de la administración del riesgo operacional a los responsables de las líneas de negocio.

  En algunas entidades que están desarrollando sistemas de medición del riesgo operacional, también se ha tratado de incorporar incentivos para la implementación de sanas prácticas de administración de este riesgo por parte de dichos responsables. Estos incentivos contemplarían, entre otros, la inclusión del tratamiento del riesgo operacional dentro del proceso de evaluación de desempeño de los responsables, así como la implementación de reportes en forma directa a la Dirección acerca del detalle de las pérdidas por riesgo operacional y el resultado de las acciones correctivas tomadas.

- La mayoría de las entidades encuestadas por Basilea se encuentran en los estadios menos avanzados de desarrollo de herramientas de medición y monitoreo del riesgo operacional. Asimismo, la consideración del riesgo operacional como una categoría particular es relativamente reciente. La medición y reporte del riesgo operacional en forma periódica sólo era contemplada por algunos bancos.

- Otra de las cuestiones que surge es la relativa a la información sobre riesgo operacional. A diferencia de los riesgos de crédito y de mercado, los factores de riesgo operacional están muy ligados a las particularidades de cada entidad y no existen relaciones claras (matemáticas o estadísticas) entre los factores individuales de riesgo y el volumen o naturaleza de las pérdidas operacionales. Por otra parte, la mayoría de las entidades no cuentan con registros de información acerca de su historia de pérdidas operacionales (volumen, causas, etc.).

En resumen, si bien por un lado se está avanzando en el desarrollo de las herramientas de identificación y medición del riesgo operacional, aún existen numerosos aspectos a definir por parte de los bancos, y por otra parte, el constante crecimiento tecnológico conlleva a la aparición de situaciones que incrementan el riesgo operacional. Algunas de dichas situaciones son:

- La globalización de los servicios financieros incrementa la complejidad de los perfiles de riesgo de las entidades.

- El avance en la utilización de tecnología de la información, sin la implementación de controles adecuados, puede transformar el riesgo de errores de procesamiento manual en riesgos de fallas en los sistemas.

- A los fines de optimizar su exposición a los riesgos de crédito y mercado, los bancos pueden utilizar mecanismos de mitigación (por ejemplo, derivados de crédito) que incrementen el riesgo operacional.

- La tercerización de algunos servicios (outsourcing) permite a las entidades enfocarse en las actividades críticas, pero puede incrementar los niveles de riesgo operacional.

- El crecimiento del e-Commerce conlleva la aparición de situaciones de riesgo (como fraudes externos) cuyos efectos, en algunos casos, no han podido analizarse totalmente (no existen antecedentes, no hay legislación que contemple esas situaciones, etc.).

Como vemos, muchas de estas cuestiones afectan a la operatoria de e-Banking desarrollada por los bancos, si bien existen situaciones que exceden dicha actividad e impactan en la totalidad de operaciones llevadas a cabo por las entidades.

En particular, algunos de los aspectos que en principio podrían incrementar el riesgo operacional en el contexto del sistema financiero en el país son:

- La redefinición de los objetivos de cada entidad como punto de partida del armado de nuevos planes de negocio.

- La consideración de segmentos y productos no trabajados habitualmente en las situaciones previas a la crisis: nuevos productos y procesos, entendiendo como novedad su tratamiento en la entidad, no sólo su aparición en el mercado.

- La creciente tendencia a la tercerización de servicios.

- El crecimiento del volumen de transacciones operadas a través de canales no tradicionales (por ejemplo e-Banking).

- Los cambios en los sistemas, proyectados por las entidades. En algunos casos de grupos financieros, el análisis de costos privilegia el desarrollo de dichos proyectos en el país.

Pautas de administración de riesgo operacional en e-Banking

Dentro de sus publicaciones, el Comité de Basilea ha emitido algunas pautas de administración del riesgo operacional, a través de un documento con 10 Principios (Publicación Nº 96 del Comité de Basilea “Sanas Prácticas para la Administración y Supervisión del Riesgo Operacional”, Febrero 2003). Básicamente, los principios se refieren a cuatro puntos clave: a) el desarrollo de un ambiente adecuado para la administración del riesgo; b) la administración del riesgo: identificación, medición, monitoreo y control; c) el rol de la supervisión; y d) el rol de la divulgación de información.

Dado que el documento citado está orientado a la administración del riesgo operacional en el contexto de la implementación del Nuevo Acuerdo de Capital de Basilea, existen cuestiones que no se relacionan en forma directa con la operatoria de e-banking. Se trata de los puntos c) y d). El primero, referido al rol de la supervisión, como moderador y evaluador de las condiciones que deben cumplir las entidades con el fin de la utilización de modelos internos para la medición del riesgo operacional. El segundo punto, el rol de la divulgación de la información, también se encuentra relacionado con la necesidad de informar públicamente al mercado acerca de los métodos y modelos utilizados para la medición del riesgo operacional. Ambas cuestiones no serán objeto de análisis en este documento.

Desarrollo de un ambiente adecuado para la administración del riesgo

En general, el funcionamiento de una estrategia efectiva de administración del riesgo, cualquiera sea éste (operativo, legal, etc.), en una entidad depende especialmente del compromiso del Directorio y la Gerencia y el proceso de supervisión que aplican sobre el banco.

Una de las principales cuestiones a considerar es el conocimiento del Directorio y la Gerencia, respecto de los principales aspectos del riesgo operativo que enfrenta el banco. Dicho conocimiento debería reflejarse en la estrategia definida para la administración del mismo. Las decisiones de asunción de determinados niveles de riesgo operativo deberían ser explicitadas por la Dirección, quien es responsable de las mismas.

La responsabilidad de la Dirección no sólo se acota a esta definición. Es parte de aquélla la aprobación de una estructura para la administración del riesgo operativo, así como asegurar que la Gerencia asuma sus propias responsabilidades en el proceso.

Al respecto, las entidades con mayores avances en el tema han establecido una función independiente de administración de riesgo operativo a nivel corporativo con una línea de reporte directa a la Alta gerencia (por ejemplo Oficial Jefe de Riesgo Operativo). En otros casos, la Auditoría Interna juega un papel preponderante como líder en la implementación de un proceso de administración del riesgo operativo. En este caso, el liderazgo debería acotarse a las etapas iniciales del proceso, a fin de mantener el criterio de independencia de los auditores.

Las responsabilidades típicas para una función independiente de riesgo operativo incluyen:

- Establecer definiciones consistentes para el riesgo operativo que incluya a todas las unidades de negocio del banco;

- Desarrollar políticas, procedimientos y prácticas a nivel del banco, para asegurar que el riesgo operativo es adecuadamente identificado, monitoreado y controlado;

- Producir informes de exposición del riesgo operativo a nivel del banco y anticipar los riesgos claves e indicadores de desempeño para la Alta Gerencia;

- Supervisar y asegurar la integridad del proceso de evaluación del riesgo operativo dentro de las líneas de negocio;

- Desarrollar estrategias para mitigar el riesgo operativo, posiblemente en combinación con productos de mitigación de riesgos tales como seguros para riesgos operativos, tercerización de actividades, etc.

Como en el caso del riesgo de mercado y del riesgo de crédito, la gerencia de cada una de las líneas de negocio tendrá una mayor comprensión de los procesos del negocio y los puntos de mayor vulnerabilidad que pudieran resultar en exposiciones significativas de riesgo operativo. En algunos bancos, los gerentes de líneas de negocios son responsables por el desarrollo de medidas de vigilancia de las principales fuentes de riesgo operativo, reportando las observaciones o hallazgos a las funciones independientes de administración de riesgos operativos e instalando los controles apropiados.

La Dirección debería, asimismo, revisar la estrategia en forma periódica, para asegurar que se estén contemplando todos los cambios relevantes, que surjan de factores ambientales, o como consecuencia de la incorporación de nuevos productos, actividades o sistemas.

Por ejemplo, aquellas entidades que cuentan con un sitio transaccional deberían contemplar regularmente la revisión de las operaciones permitidas a los clientes así como las eventuales incorporaciones, verificando que se adecuen a las regulaciones vigentes.

Otro de los aspectos a considerar es la existencia de una auditoría interna adecuada, que controle la implementación efectiva de las políticas y procedimientos relacionados con la administración del riesgo operativo. El Directorio, a través de su Comité de Auditoría, debería asegurar que el alcance y frecuencia de las pruebas programadas son apropiados para los riesgos involucrados.

En cuanto a la Gerencia, debe traducir la estrategia de administración de riesgos establecida por el Directorio en políticas, procesos y procedimientos adecuados para la entidad. Asimismo es necesaria la formalización de tales políticas y procesos, así como una adecuada comunicación a todos los niveles organizacionales.

Un punto importante en el proceso de supervisión gerencial es la emisión de reportes periódicos que permitan monitorear la efectividad del sistema de administración del riesgo operativo, tanto por parte de la Gerencia como por el Directorio.

La Gerencia deberá también verificar que las actividades de e-Banking y su monitoreo sean llevadas a cabo por personal calificado con las capacidades técnicas necesarias.

En resumen, a los efectos del desarrollo de un adecuado ambiente de administración del riesgo podrían identificarse como los principales aspectos a considerar los siguientes:

e-Banking

FUENTE: Comisión de e-Banking

Aspectos a considerar para una adecuada administración del riesgo

Administración del riesgo: identificación, medición, monitoreo y control

Identificación y medición

Previo al lanzamiento o introducción de nuevos productos, las entidades deben identificar claramente el riesgo operativo inherente, y prever procedimientos adecuados de evaluación.

La efectiva identificación del riesgo considera tanto factores internos (tales como la complejidad de la estructura del banco, la naturaleza de las actividades del banco, la calidad del personal, los cambios organizacionales y la rotación del personal) y factores externos (tales como condiciones económicas fluctuantes, cambios en la industria y avances tecnológicos) que pudieran afectar adversamente el logro de los objetivos del banco.

Dicho proceso debería incluir también una determinación de los riesgos que son controlables por el banco y de los que no lo son.

Algunos de los ejercicios que pueden llevarse a cabo para identificar adecuadamente los riesgos operativos son:

- Auto-evaluación o evaluación de riesgos: El banco define un menú de posibles eventos de riesgo operativo y evalúa sus actividades contra el mismo, identificando fortalezas y debilidades del ambiente de control.

- Indicadores clave de riesgo: Se establecen estadísticas que pueden proveer una visión de la posición de riesgo del banco, siendo necesaria su revisión periódica para alertar sobre cambios que pudieran implicar problemas de riesgo. Los indicadores podrían incluir, por ejemplo, tasas de rotación del personal, frecuencia de errores, reclamos de clientes, etc.

Los factores de riesgo operativo usualmente identificados por los bancos son más bien medidas de tipo interno como calificaciones de auditoría interna, desempeño, volumen de transacciones, tasas de error, etc., que factores de tipo externo como en el caso de los riesgos de crédito y mercado. De todas formas, hay incertidumbre acerca de que factores son los más importantes, dado que no existe una relación directa entre los factores de riesgo identificados y la dimensión y frecuencia de las pérdidas.

Es por ello que el proceso de medición del riesgo operativo se encuentra, aún en sistemas financieros más desarrollados, en un estadio primitivo. Para cualquier sistema confiable de medición, se necesita recolectar los datos para desarrollar medidas generales de riesgo operativo.

Monitoreo y control

Es esencial un proceso efectivo de monitoreo para administrar adecuadamente el riesgo operativo. Las actividades de monitoreo sobre la marcha pueden ofrecer la ventaja de detectar y corregir rápidamente las deficiencias en las políticas, procesos y procedimientos para administrar dicho riesgo. La frecuencia de monitoreo debería reflejar los riesgos involucrados y la frecuencia y naturaleza de los cambios en el entorno operativo.

Los bancos deberían tener políticas, procesos y procedimientos para controlar o mitigar el riesgo operativo identificado. Para los riesgos que son controlables, el banco debe decidir la extensión con que desea utilizar los procedimientos de control y otras técnicas apropiadas, o soportar el riesgo. Para los riesgos que no pueden ser controlados, el banco debe decidir si aceptar estos riesgos o eliminar o reducir el nivel de la actividad de negocio involucrada.

Se deberían establecer procesos y procedimientos de control y las entidades deberían tener instalado un sistema para asegurar el cumplimiento de un conjunto documentado de políticas internas concernientes al sistema de administración de riesgos.

Los principales elementos de este sistema podrían incluir:

- Revisiones de alto nivel del progreso del banco en la consecución de los objetivos establecidos;

- Verificación del cumplimiento de los controles gerenciales;

- Un sistema de aprobaciones y autorizaciones documentadas para asegurar responsabilidad a un nivel gerencial apropiado.

Para ser efectivas, las actividades de control deberían ser una parte integral de las actividades regulares de un banco, y deberían involucrar a todos los niveles de personal del banco, incluyendo tanto a la Alta Gerencia como al personal de las unidades de negocio. Los controles que son una parte integral de las actividades regulares permiten rápidas respuestas a las condiciones cambiantes y evitan costos innecesarios.

A los efectos de mitigar el riesgo operacional, los bancos utilizan una variedad de técnicas. En general, la existencia de controles internos y un proceso de auditoría interna son vistos como uno de los principales mecanismos que permiten cubrir este objetivo.

En otros casos, algunas entidades tienen establecidos ciertos “límites” de riesgo, usualmente basados en su medición del riesgo operacional, superados los cuales se disparan alertas sobre potenciales problemas.

Como se comentaba precedentemente, los controles internos son vistos como la herramienta más útil para reducir o mitigar el riesgo operacional. Entre dichos controles se destacan la segregación de funciones, el establecimiento de una línea clara de reporte y adecuados procedimientos operativos. A los fines de contemplar una adecuada segregación de tareas y que el personal no tenga asignadas responsabilidades que pudieran crear conflictos de intereses, deberían identificarse las áreas de conflictos potenciales de interés, minimizarse y ser objeto de un cuidadoso monitoreo y revisión independientes.

Las actividades de la auditoría interna también se consideran un importante elemento en la administración de riesgo operacional. Se destacan en particular la identificación de potenciales problemas, la validación de las auto-evaluaciones de la Gerencia y el seguimiento de las situaciones o problemas detectados y las acciones para su resolución. De una encuesta llevada a cabo por Basilea, surge que varios bancos estiman que la mayoría de los eventos de riesgo operacional se encuentran asociados con debilidades de control interno o la inobservancia de los procedimientos de control existentes.

Con respecto a otras estrategias de mitigación de riesgos es necesario evaluar si están reduciendo el riesgo verdaderamente, o sólo transfieren el riesgo a otro sector o área del negocio. Una técnica creciente de mitigación de riesgos es el uso de pólizas de seguro para ayudar a mitigar el riesgo operativo resultante de eventos tales como errores y omisiones, pérdidas físicas de valores, fraude de empleados o terceras partes y desastres naturales. La conveniencia de dicha práctica se encuentra en discusión, dado que se podría estar cambiando el riesgo operacional por riesgo de incumplimiento de la aseguradora.

Los bancos también deberían establecer políticas sólidas para administrar los riesgos asociados con las actividades tercerizadas. La tercerización de actividades tiene el potencial de mejorar el desempeño del banco y puede reducir el perfil de riesgo de la institución transfiriendo actividades a otros que son más expertos y tienen mayor escala para administrar los riesgos asociados con actividades especializadas del negocio. Sin embargo, no deberían descuidarse los aspectos relativos al riesgo residual asociado con los acuerdos de tercerización, incluyendo la interrupción de los servicios o eventuales riesgos de reputación.

Dependiendo de la importancia y criticidad de la actividad, los bancos deberían comprender el impacto sobre sus operaciones y en sus clientes de cualquier deficiencia potencial en los servicios provistos por proveedores y otros terceros suministradores de servicios, incluyendo interrupciones del servicio y la falla o incumplimiento potencial de los negocios de las terceras partes. El alcance de la responsabilidad de las terceras partes y su capacidad financiera para compensar al banco por los errores, negligencias y otras fallas operativas deberían estar consideradas explícitamente como parte de la evaluación de riesgos. Para las actividades críticas, el banco podría necesitar considerar planes de contingencia, incluyendo la disponibilidad de terceras partes externas alternativas y los costos y recursos requeridos para cambiar las terceras partes, potencialmente con muy poco tiempo de aviso.

Las inversiones en apropiada tecnología de procesamiento y seguridad de tecnología informática son también importantes para la mitigación de riesgos. Sin embargo, los bancos deberían ser conscientes de que el aumento en automatización puede transformar las pérdidas de alta frecuencia y baja severidad en pérdidas de baja frecuencia con alta severidad. Esto último puede ser asociado con pérdidas o interrupciones extensas de servicios causadas por factores internos o por factores que están más allá del control inmediato del banco (por ejemplo eventos externos). Tales problemas pueden causar serias dificultades a los bancos y podrían comprometer la habilidad de una institución para llevar adelante las actividades claves del negocio, si no se contara con planes de contingencia adecuados.

En definitiva, a pesar de las diferencias entre entidades (tamaño, naturaleza y complejidad de sus actividades, volúmenes de operaciones, etc.), un buen sistema de información gerencial, una cultura fuerte de control interno y la existencia de planes de contingencia son elementos cruciales para una administración efectiva del riesgo operativo en cualquier entidad.

Algunos eventos de riesgo operacional en e-banking

Algunos ejemplos de eventos de riesgo operacional que afectaron a entidades financieras en distintas regiones del mundo, y se conocieron durante el ejercicio 2003 y el presente año:

FUENTE: Comisión de e-Banking

Algunos eventos de riesgo operacional en e-Banking

Eventos

25 de enero 2003

Según un portavoz del FBI, el flujo mundial de información en Internet se redujo fuertemente el sábado 25/01/2003 durante varias horas, debido a los efectos de un virus de progresión rápida. El problema fue detectado por distintos sitios de control de Internet en el mundo.

La caída del tráfico de Internet afectó el envío y recepción de correos electrónicos y otras transmisiones de información. En Corea del Sur la red Internet de débito quedó bloqueada provocando la peor avería conocida en ese país.

Algunas de las principales víctimas del ataque en EE.UU fueron:

- Countrywide Financial, sus clientes no tuvieron acceso durante más de 48 horas a los servicios bancarios por Internet.
- Bank of America, cuya red de cajeros automáticos e interconexiones bancarias se colapsó totalmente en todo el territorio. En casi 18 mil cajeros automáticos los clientes del BOFA no pudieron sacar su dinero.
- American Express, el acceso al sitio Web de esa tarjeta de crédito y sus servicios bancarios on-line fueron bloqueados totalmente.

Febrero 2003

Un estudiante de 18 años fue detenido en Río de Janeiro como presunto autor de la duplicación de páginas de Internet de entidades bancarias para conseguir los datos necesarios para realizar transferencias.

Se creaban páginas Web idénticas a bancos brasileños, coreanos, peruanos y de EE.UU. Una vez construidos los sitios, semejantes a los que poseen las entidades bancarias, los usuarios accedían a las páginas e introducían sus claves y datos para realizar transferencias. Estos datos eran almacenados y posteriormente utilizados para transferir dinero y realizar compras.

Septiembre 2003

El banco británico Barclays afirmó que piratas informáticos habían mandado un correo electrónico a sus clientes, con un falso logo de la entidad, que incluía un supuesto enlace al portal del banco. A los clientes se le solicitaban sus datos personales, la contraseña o el número de identificación personal (PIN), para poder ser utilizados para retirar efectivo de sus cuentas.

El portavoz del banco expresó públicamente que la entidad no tenía nada que ver con este correo y que ese portal no pertenecía a Barclays, e indicó que unas 400 personas se habían puesto en contacto con el banco diciendo que habían recibido el e-mail. Ocho de estas personas confesaron que habían revelado sus datos personales, y sus cuentas fueron bloqueadas. Barclays anunció que cubriría cualquier pérdida ocasionada por el fraude.

Noviembre 2003

Según News.com, el 5/11/2003 las autoridades brasileñas arrestaron a dieciocho hackers, que operaban desde el estado de Pará en Amazonia hasta Goias, en un intento de disminuir el índice de criminalidad en Internet que disparaban las bandas organizadas que operan en el norte de Brasil.

La operación, bautizada con el nombre de Caballo de Troya, abarcaba a 205 oficiales de policía federal especializada dedicada al rastreo de estos expertos, que habían conseguido robar más de diez millones de dólares en el último año entre sucursales bancarias online y sistemas de clientes. Los ladrones habían conseguido crear programas y sitios de Internet con la capacidad de develar las contraseñas de los clientes que realizaban sus operaciones a través de la Red. Más tarde desviaban los fondos a cuentas de terceros a las que tenían acceso.

FUENTE: Comisión de e-Banking

Algunos eventos de riesgo operacional en e-Banking

Eventos

Enero 2004

Un joven fue condenado por la justicia federal brasileña a 6 años de prisión por hackear las páginas de cuatro bancos. Guilherme Amorim, de sólo 19 años de edad, fue detenido el año pasado en Campo Grande acusado de hackear los sitios Web de cuatro entidades bancarias.

Los bancos afectados por estas estafas a través de Internet son la Caixa Económica Federal, el Banco do Brasil, Itaú y Bradesco. Guilherme era el coordinador de un grupo de piratas informáticos, y tras una investigación detuvieron a otros cinco acusados, que se encuentran a la espera de ser juzgados. En dicho grupo se encuentra el padre del coordinador de la banda, un médico llamado José Geraldo Alves, y dos agentes de la Policía Civil de Mato Grosso.

Amorim retiró dinero de más de cien cuentas corrientes, pero se cree que con la detención se evitó que se llevaran a cabo acciones con las que pretendían hacerse con 150 millones de reales, que equivale a cerca de 55 millones de dólares.

Febrero 2004

En España, sobre las 18 horas del domingo 22/02/2004 se detectó un nuevo envío indiscriminado de e-mails simulando ser un mensaje del Banco Popular, donde se solicitaba a los clientes dirigirse a una dirección de su sitio Web para mejorar la seguridad de sus cuentas. En esta ocasión se destaca que el falso enlace abría 2 ventanas: por un lado la página original del Banco Popular, mientras que en la segunda, donde se producía el robo de la cuenta del cliente, se ocultaba la URL del servidor Web utilizado para el fraude.

Sin duda se trata de otra vuelta de tuerca en las técnicas conocidas como "pishing" (password harvesting fishing), estafas donde se intenta suplantar la identidad de entidades legítimas para engañar a los usuarios, y que en el caso de España está afectando en los últimos tiempos, con especial incidencia, a Banesto y Banco Popular.

El mensaje detectado por Hispasec, y reportado de forma inmediata al Banco Popular, aparece con el nombre de remitente "Validate" y la dirección de correo validate@bancopopular.es. Con el asunto "Apreciado Cliente", el mensaje HTML incluye en su inicio el logotipo del Grupo Banco Popular.

Febrero 2004

El mayor robo de datos conocido hasta la fecha se produjo en Japón, donde los datos de 4,52 millones de suscriptores del mayor proveedor de banda ancha del país fueron robados.
Softbank Corp, el mayor proveedor de acceso de banda ancha en Japón anunció que los datos de 4.520.000 nombres, el 67% de su base de datos del servicio Yahoo BB fueron robados por un par de supuestas redes de extorsión. La empresa también anunció que tiene previsto gastar 4.000 millones de yenes, aproximadamente 36,63 millones de dólares, en concepto de compensación a sus abonados.
La base de datos incluía los nombres de 2,4 millones de clientes actuales así como de los que dejaron el servicio, los que están todavía en proceso de suscripción y los que están en período de prueba gratuita. Según Masayoshi Son, presidente ejecutivo de Softbank: "Lo lamentamos sinceramente, tendremos el máximo cuidado en asegurar que esto no se repita jamás".

Marzo 2004

Dos personas de nacionalidad rusa fueron detenidas en Málaga por presunta implicación en estafas bancarias a través de Internet. Pertenecen presuntamente a una organización que lleva a cabo estafas a través de Internet haciéndose pasar por entidades bancarias. Su forma de operar consiste en el envío masivo de correos electrónicos, en los cuales se hacen pasar por una entidad bancaria y solicitan al usuario que se conecte a una URL indicada, la cual a simple vista parece pertenecer a dicha entidad, sin que sea así.

El usuario introducía de este modo sus datos personales y claves de acceso con el fin de mejorar la seguridad en la comunicación con el banco, no sabiendo que lo que hacía era proporcionar a los estafadores una vía de acceso a sus cuentas. Las personas detenidas utilizaron los datos obtenidos para realizar ciertas transferencias a cuentas de Australia o Rusia.

Exposición de la Información Crítica Seguridad en Redes

Hoy en día, vivir en un mundo interconectado implica que las comunicaciones cumplan un papel fundamental en todos los sistemas, ya que los mismos requieren compulsivamente cada vez más velocidades en los enlaces para que la información llegue a los usuarios, vendedores, clientes, socios, etc.

Esto permite aseverar que no es posible considerar a estos entornos como cajas negras y suponer que los mismos se encuentran seguros al estar dentro de nuestra organización.

La realidad evidencia que casi todos los elementos asociados a la red tienen la posibilidad de conectarse entre sí, de hecho los estragos ocasionados por los famosos virus “Code Red”, “Nimda”, “Love”, etc. son prueba de ello.

Afortunadamente se han implementando soluciones tecnológicas, muchas de las cuales ya forman parte de los estándares que mantienen a las redes segregadas y protegidas.

Es importante resaltar que la auditoría de redes es sólo una “columna” de la estructura que forman junto a la seguridad lógica (aplicativa, operativa y de base de datos), la seguridad física, y la continuidad de negocio, etc., un conjunto de elementos que permiten asegurar los activos de las organizaciones.

Las redes en general, van desde simples LANs conectadas en una única oficina o edificio, hasta otras que pueden alcanzar distintos edificios ubicados en distintas regiones geográficas (en el mismo territorio o en el exterior), con distintos tipos de accesos (privados y/o públicos).

Vulnerabilidades:

Existen tres grandes grupos de vulnerabilidades básicas:

1. **Intercepción:** El dato, al ser transmitido a través de la red, pasa por distintos medios y equipos que, generalmente, son custodiados física y lógicamente por terceras partes sobre las cuales no se posee control. Estos datos pueden ser interceptados, con la consiguiente posibilidad de que alguien los lea, los modifique o los retire, al destruirlos o evitar que sigan su camino. Todo esto produce una pérdida de integridad en la información transmitida, llegando al extremo de ocasionar importantes pérdidas materiales.

2. **Disponibilidad:** a medida que las redes proliferan, es cada vez mayor la cantidad de usuarios remotos que acceden a las aplicaciones. Si las conexiones fallan, o no se encuentran disponibles por alguna razón, se producen pérdidas materiales por interrupción de las operaciones del negocio.

3. **Puntos de entrada o de acceso:** Las redes extienden la utilización de los sistemas, posibilitando la conexión de los usuarios independientemente de la ubicación geográfica en la que se encuentren. Esta ventaja, trae aparejado el riego de que “cualquiera” acceda, vea o transite por la red, y de existir un punto débil en la configuración a través de la misma, pueda vulnerar la estructura de seguridad planteada, permitiendo a los intrusos, el acceso a la información sensible o crítica. Por su configuración inherente, las redes proveen muchos puntos de acceso para intrusos, interceptores, virus, gusanos, troyanos, etc. Esta ventaja, la de permitir la conexión a la red por parte de cualquiera desde cualquier punto, se convierte en desventaja desde el punto de vista de la seguridad. Es por ello que es tan importante encontrar la ecuación que maximice ambos recursos: seguridad y accesibilidad. Afortunadamente, existe una cantidad de soluciones probadas que combinan hardware y/o software para llegar a la situación óptima que requiere cada organización. En este punto, es crítico recordar que “el costo del control no debe superar el valor del bien a resguardar”.

Controles:

Una vez identificadas las vulnerabilidades, analizaremos los controles a tener en cuenta:

Intercepción

El control de la seguridad en la capa física es fundamental por el hecho de permitir controlar la ubicación de los equipos de comunicaciones como primera barrera de seguridad.

Se debe tener especial cuidado en la evaluación de los puntos a controlar, sin dejar de lado el análisis de los puntos de interconexión ante los diferentes sistemas. No obstante, la llegada de las conexiones inalámbricas hace que el control antes mencionado sea de difícil implementación.

La herramienta para la intercepción es la encripción. Ésta elimina la necesidad de husmear la red en busca de datos que circulan por ella, ya que los mismos no pueden ser interpretados por terceros.

En la actualidad existen una cantidad de métodos que realizan encripción tanto a nivel de aplicación, como de comunicación, mediante dispositivos tales como routers, switches, multiplexores, etc. Las VPN (redes privadas virtuales) son un ejemplo del uso de la encripción a nivel de túnel de datos, sobre una red pública o compartida. Otros métodos pueden ser el uso de certificados y/o firmas digitales.

Disponibilidad

El control que asegure la disponibilidad, se consigue a través del establecimiento de una buena arquitectura y monitoreo de las redes.

En el diseño de la red se debe asegurar que entre cada recurso y el punto de acceso, existan caminos redundantes y ruteos automáticos, que redireccionen el tráfico al camino habilitado sin pérdida de tiempo y de datos.

Cada componente de la red debe estar diseñado a prueba de fallas, o construido con ciertos componentes redundantes.

Redes altamente distribuidas o complejas deben ser monitoreadas y administradas, generalmente mediante la utilización de software específico, y en manos de un COR (Centro de Operaciones de Red) que brinde servicios 24/7. Dicho Centro será el encargado de asegurarse que el ancho de banda brindado en cada momento sea el adecuado, sin cuellos de botellas, y brindando la velocidad requerida por los usuarios y las aplicaciones.

Puntos de acceso

Muchos de los controles en las redes se establecen en los puntos de conexión con el "exterior". Estos controles buscan limitar el tipo de tráfico que puede ingresar o salir, o también restringir las direcciones de origen y destino. Por ejemplo, para proveer acceso a un servidor Web dentro de la red a los clientes distribuidos a lo largo del mundo, con el objeto de que puedan cargar órdenes de compra, la red debería aceptar solamente ciertos tipos de protocolos (http), y no otros que permitieran validarse en los servidores (telnet).

En otra situación, en donde un socio o proveedor brindan soporte y/o mantenimiento desde ubicaciones remotas fijas, la red debería aceptar conexiones para ese servicio exclusivamente, que provengan desde locaciones definidas y conocidas.

Todo esto es controlable mediante correctas implementaciones de reglas en los firewalls, o mediante listas de acceso en los routers.

Los sistemas de detección de intrusos (IDS's) y antivirus trabajan en conjunto para detener y actuar en consecuencia junto a los firewalls, tomando medidas correctivas dinámicas ante la ocurrencia de eventos definidos como críticos.

Sanas prácticas a tener en cuenta en el análisis de la seguridad en las redes

1. **Determinación de la extensión de la red:** Es fundamental para el establecimiento de los controles identificar los límites lógicos definiendo que equipos serán considerados internos y cuales externos, y la actualización periódica, manual o mediante software, que mantenga los diagramas actualizados.

2. **Ubicación de la información crítica:** La seguridad aplicada al recurso debe encontrarse en relación al valor del activo a proteger, por lo que es necesario definir e identificar cual será la información considerada confidencial, crítica, sensible, de dominio público interno o externo, etc., a los efectos de aplicar al recurso que la contiene las protecciones y accesos pertinentes.

3. **Evaluar quienes deben tener acceso a los recursos:** Determinar quienes deben tener los permisos para acceder a los recursos y que tipos de accesos deben concedérseles (lectura, escritura, ejecución, etc.).

En este proceso deberían tenerse en cuenta puntos como:

a. ¿Los sistemas deben ser accedidos sólo por los empleados de la organización?

b. ¿Los proveedores y distribuidores deben tener el mismo tipo de acceso que los empleados?

c. ¿Los empleados deben acceder a los mismos recursos tanto cuando se encuentran en la "red interna" como cuando están en la "red externa"?

d. ¿Los clientes deben acceder a aplicaciones específicamente desarrolladas para ser aplicadas a los servidores Web de la extranet, o realizan conexiones mediante acceso remoto directamente con los sistemas de la organización?

4. **Determinar cuales son las conexiones a las redes externas:** Todas las redes que se conectan a Internet lo hacen mediante una conexión brindada por un Proveedor de Internet (ISP).

Las razones para contar con una conexión son: brindar servicios de correo y navegación a los usuarios internos, utilizar servicios de e-Commerce, e-Banking, la publicación de servidores Web y otros. A efectos de la utilización de estos servicios se requerirán en algunos casos vínculos dedicados, dado su alto requerimiento de ancho de banda.

Todos los elementos (gateways, routers, modems, etc.) a través de los cuales estas conexiones son establecidas, son puntos potenciales de riesgo.

"Todo vínculo que ingresa al ámbito de la red interna, sin que se posean los permisos y accesos necesarios para constatar la configuración del equipo que lo vincula, constituye un riesgo potencial".

A esta altura ya estamos en condiciones de reconocer los límites de la red interna, los recursos que contienen la información, en sus distintos niveles de confidencialidad, los permisos asignados a los usuarios y los mecanismos aplicados para acceder a la información dependiendo de la localización del cliente.

5. **¿Cuales deberían ser los mecanismos de protección aplicados?:**

Existen una cantidad de organizaciones que se dedican a informar las vulnerabilidades detectadas por terceros o las informadas por los desarrolladores o fabricantes. Son los denominados "parches" que solucionan ciertos "problemas" en las aplicaciones o sistemas operativos, que al momento de su lanzamiento al mercado no fueron contemplados o debidamente analizados.

Estos “parches” deben ser aplicados a equipos de testeo o desarrollo antes que a los de producción, ya que en ciertas ocasiones se presentan incompatibilidades con desarrollos locales o de terceros realizados “a medida”.

Cuando alguien trata de aprovechar esas vulnerabilidades, utilizan códigos que forman un patrón (firma) que permite ser detectado. Esta propiedad es utilizada por los IDS's para alertar de la ocurrencia de esta clase de eventos al personal encargado de la seguridad, considerándolos como un intento de intrusión.

Una definición de “vulnerabilidad” en términos tecnológicos o de seguridad informática es:

“Falla en la configuración o en la instalación de un programa (software) o de un dispositivo (hardware), que permite obtener acceso de manera no autorizada al programa o hardware”.

Se identifican tres tipos de vulnerabilidad:

- Debido a un error de diseño inicial lógico / físico en un dispositivo o en un programa.

  Ej.: Una aplicación de uso bancario que no requiera contraseñas de uso (por exceso de confianza en los empleados).

- Debido a una metodología incorrecta de diseño, la cual no toma en cuenta el ambiente en el cual el producto va a ser utilizado.

  Ej.: Software que no pueda ser instalado en el ambiente para el cual fue desarrollado.

- Debido a la inducción deliberada de la vulnerabilidad, en cualquier etapa del diseño, con el fin de aprovecharse de la misma para beneficio propio.

  Un empleado disgustado, que altera el generador de números aleatorios en una aplicación de contraseñas, para que las mismas tengan un largo fijo y un número de combinaciones finitas muy pequeño.

La existencia de estas vulnerabilidades hace necesario identificar o conocer si la información resguardada ha sido accedida por personal no autorizado o si existen individuos procurando obtenerla. Esta función de detección es cumplida por los IDS (sistemas de detección de intrusos).

Sistemas de Detección de Intrusos

Estos sistemas forman parte de una pequeña, pero crítica, familia de dispositivos que permiten alertar ante la ocurrencia de eventos identificados como maliciosos.

Dependiendo del lugar aplicado al sensor o la función que desempeña existen distintos tipo de IDSs (sistema de detección de intrusos):

HIDS (Host IDS)

Este tipo de monitor de eventos concentra datos de múltiples fuentes que analizan la actividad sospechosa. Este monitoreo es realizado en tiempo real y las fallas de los sistemas protegidos son detectadas rápidamente, promoviendo su popularidad entre el personal técnico y de seguridad.

IDS de red

Este dispositivo monitorea todo el tráfico que atraviesa el segmento donde el agente está instalado, reaccionando ante cualquier anormalidad o firma de actividad sospechosa. Es un “Sniffer” con actitud. Su magnitud varía entre aquellos simples que se cargan y funcionan, y aquellos que requieren de configuraciones específicas y complicadas. Dependiendo de la velocidad de la red, estos dispositivos no requieren hardware de magnitud.

NNIDS (Network node IDS)

Con el advenimiento de las redes switcheadas y el aumento en la velocidad de transmisión se generaron cuellos de botella para el análisis de los paquetes que circulan, teniendo que descartar gran cantidad de ellos.

Las redes switcheadas permiten que se analicen los paquetes mediante la modalidad de configuración de las placas en modo promiscuo. Siempre existe la posibilidad de definir uno de los puertos del switch para realizar análisis autorizados de la información que circula por la red, mediante algún analizador de protocolo o software específico.

IDS Híbridos (No Promiscuos combinado con el Log de eventos)

Combinando el NNIDS y el Host IDS en un solo paquete, se realiza una buena cobertura teniendo en cuenta la relación o la ecuación cantidad de información y costo, reservándose esta estructura en general para servidores críticos.

Controladores de Integridad

¿Cómo determinar si un archivo ha sido modificado por un atacante en beneficio propio? Cuando un sistema es comprometido, generalmente el atacante altera ciertos archivos clave que le proveen acceso continuo. Los controladores de integridad aplican una serie de algoritmos a la información, que les permite determinar si el contenido de la misma ha variado. Cuando se detectan cambios en las verificaciones periódicas, los controladores disparan alarmas de notificación.

Equipos Trampa (HoneyPots)

Estos equipos son herramientas altamente flexibles con diversas aplicaciones en seguridad. No solucionan un único problema; por el contrario, son aplicables para múltiples usos tales como prevención, detección o simplemente recopilación de la información. Básicamente, todos comparten el mismo concepto: es un recurso de seguridad que no debería tener interacción con los sistemas productivos o actividad autorizada. Esta característica hace simple su utilización.

En general, existen dos tipos: los de producción y los de investigación. Los primeros capturan información limitada y son generalmente usados en compañías y organizaciones. Los segundos son de configuración y mantenimiento más elaborado, capturan cuantiosa información y son comúnmente utilizados por organizaciones militares o gubernamentales.

Los Equipos Trampa son una nueva tecnología, con un potencial enorme para la comunidad de la seguridad informática. A diferencia de los Firewalls o de los Sistemas de Detección de Intrusos, estos equipos no resuelven un problema específico. Pueden abarcar en su objetivo desde el descubrimiento de los ataques encriptados en las redes de IPv6 hasta la captura de los datos de intento de fraude en línea, realizados a bases de datos muy extensas.

Un Equipo Trampa es una herramienta utilizada para determinar cuando un recurso es de uso ilícito o no autorizado.

Conceptualmente, la mayoría de los equipos trampa trabajan de la misma manera: no tienen ninguna actividad autorizada ni tienen valores del entorno productivo. Teóricamente, no deberían ver el tráfico de red, al no poseer un perfil que les asigne alguna actividad legítima. Esto implica que cualquier interacción con el equipo trampa probablemente se relacione a una actividad desautorizada o fraudulenta. Cualquier conexión que se intenta a estos dispositivos es probablemente una sonda, un ataque o un intento de comprometer al recurso. Si bien en su concepción parece muy simple, es esta misma simplicidad la que le brinda importantes ventajas.

Las ventajas:

- Pocos datos de alto valor: Los equipos trampa coleccionan cantidades pequeñas de información. En lugar de acumular giga bites de datos por día, anotan sólo mega bites de datos por día. De la misma forma, se reduce notoriamente el número de alarmas generadas. Al capturar sólo la actividad dudosa, cualquier interacción con ellos es probablemente actividad no autorizada o malévola. La información es mínima, pero de alto valor, por lo que el análisis de los datos almacenados en estos equipos brinda ventajas de facilidad y abaratamiento de costos.

- Maleabilidad: Estos equipos pueden capturar un modelo no prefijado de intrusión, incluso herramientas o tácticas no reconocidas.

- Mínimos recursos: Como sólo capturan la actividad fraudulenta, requieren mínimos recursos.

- Encriptación o IPv6: Al contrario de otras tecnologías de seguridad (como los sistemas de Detección de Intrusión) los equipos trampa trabajan bien en ambientes encriptados o con IPv6.

- Simplicidad: No requieren de algoritmos o firmas.

Las desventajas:

Dentro de las debilidades de esta tecnología, se pueden enunciar:

- Vista limitada: El dispositivo puede rastrear y capturar la actividad sólo cuando se interactúa con él. No capturará los ataques contra otros sistemas, a menos que el asaltador o la amenaza también actúe recíprocamente.

- El riesgo: Las distintas tecnologías de seguridad poseen riesgos específicos: un firewall podría ser superado, podría romperse la encriptación, un sensor de IDS tiene el riesgo de no descubrir los ataques. Específicamente, en el caso de los equipos trampa, existe el riesgo de ser tomados por el intruso y usados para dañar otros sistemas, variando la magnitud de dicho riesgo en función del tipo de honeypot utilizado.

Clasificación de los equipos trampa (honeypots)

Los equipos trampa pueden ser clasificados de acuerdo con la interacción que poseen, o sea el nivel de actividad que estos dispositivos le permitan al atacante.

De baja interacción son aquellos que normalmente limitan la actividad y trabajan emulando servicios y sistemas operativos. La principal ventaja de este tipo de equipos es la facilidad de instalación y mantenimiento con un riesgo mínimo. Su desventaja principal es que sólo recolecta una cantidad limitada de información y se lo diseña para capturar sólo un tipo de actividad conocida. Para un asaltador experimentado, es fácil descubrirlos, no importa cuan buena sea la emulación.

Los equipos trampa de alta interacción son generalmente soluciones complejas, involucran sistemas operativos y aplicaciones reales. No existe emulación y el atacante estará actuando sobre el procesamiento real. Ofrece como ventaja el conocimiento, en tiempo real, de la existencia de un ataque, y la posibilidad de análisis, en el momento, de nuevas conductas de comportamiento de intrusión. La desventaja de este tipo de dispositivos es la necesidad de utilizar tecnologías adicionales como instrumento para impedir que el atacante pueda dañar otros sistemas. Adicionalmente, son complejos para su instalación y mantenimiento.

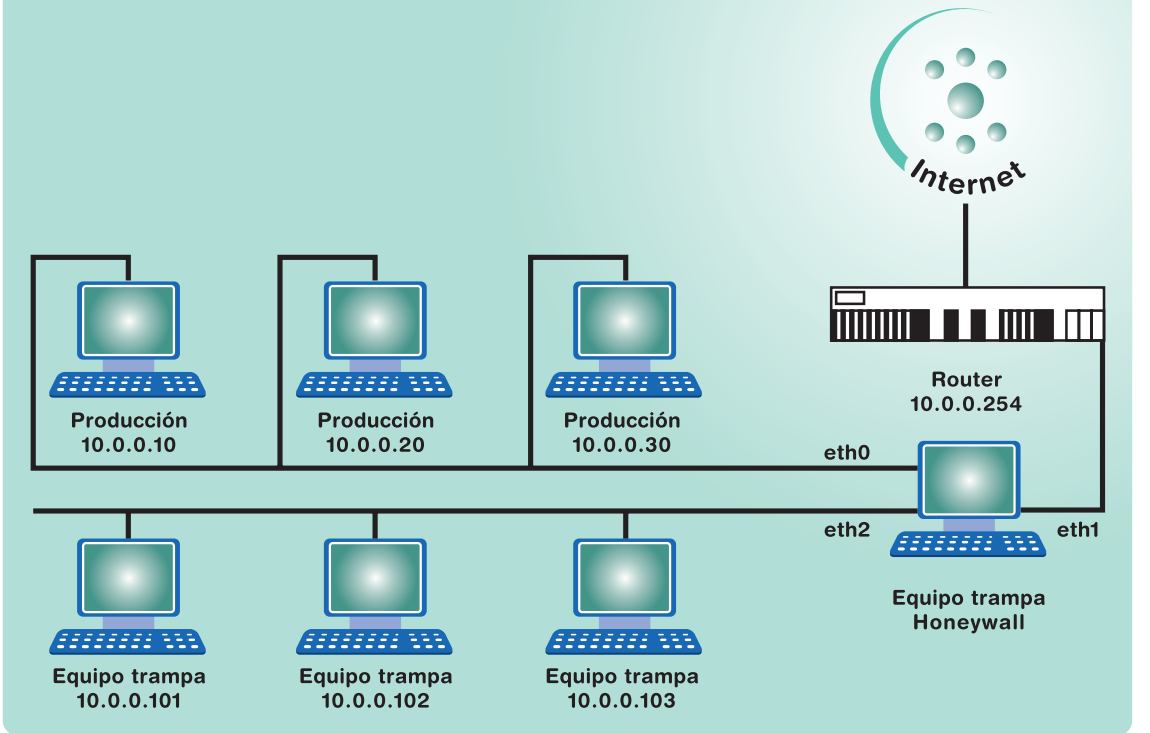
Redes Trampa (Honeynets): El honeypot de la alta-interacción

Las redes Trampa son un ejemplo de equipos trampa de alta-interacción. Se trata de una arquitectura de red, donde toda la actividad es monitoreada y capturada. Dentro de esta red, se instalan intencionalmente a las eventuales “víctimas” junto a las computadoras reales que ejecutan las aplicaciones corrientes. Cuando los intrusos acceden al sistema no comprenden que están dentro de una red trampa. Toda su actividad, las sesiones de SSH encriptadas, los correos electrónicos y los archivos transferidos, son capturados sin que ellos se den cuenta. Esto se logra insertando un módulo en el núcleo de los sistemas operativos de la “víctima”, que captura todas las acciones del asaltador.

Al mismo tiempo, la Red Trampa controla la actividad del asaltador, usando una entrada del Firewall Trampa (Honeywall). Esta entrada permite el tráfico entrante a los sistemas de la “víctima” pero controlando el tráfico que sale, utilizando las tecnologías de prevención de intrusión. Esto da una cierta flexibilidad permitiendo al asaltador actuar recíprocamente con los sistemas de la víctima, pero impide al asaltador dañar otras computadoras del entorno de Redes No-Trampa.

FUENTE: Comisión de e-Banking

Redes trampa (Honeynets): el honeypot de la alta interacción



Aplicación de los equipos trampa

Cuando el honeypot es utilizado con propósitos de producción, el objetivo es proteger a la organización respondiendo a un ataque, lo que debe incluir los conceptos de prevención y alerta.

Cuando el dispositivo es usado con propósitos de investigación, se estará coleccionando información que tiene un valor diferente para cada una de las organizaciones. Algunas de ellas pueden querer estudiar las tendencias en la actividad del asaltador, mientras otras estarán interesadas en dar alerta anticipada y predictiva ante hechos que vayan en contra de las leyes vigentes.

En general, los equipos trampa de baja-interacción se usan para propósitos de producción, mientras que los de alta-interacción se usan con propósitos de investigación.

Cuando se usan en ambientes productivos, los equipos trampa pueden proteger a la organización con el fin de lograr la prevención, el descubrimiento o la respuesta.

Estos equipos ayudan a prevenir los ataques automatizados (como por ejemplo, los gusanos). Dichos ataques se basan en herramientas que, al azar, examinan redes enteras en busca de sistemas vulnerables, con el fin de capturarlos. Los honeypots pueden ayudar a defenderse contra tales ataques, retardando su examinado hasta llegar incluso a detenerlos.

Los equipos trampa también pueden dar protección a su organización contra los asaltadores humanos. El concepto aplicado es el de decepción o disuasión: la idea es confundir al asaltador, para hacerle perder su tiempo y recursos ya que actúa recíprocamente con el equipo trampa. Entretanto, la organización ha descubierto la actividad del asaltador y ha tenido el tiempo suficiente para responder y detener al mismo.

La detección es otra forma en que los equipos trampa pueden ayudar a la protección de las organizaciones. Esta detección es crítica y el propósito consiste en identificar un fracaso o una ruptura, ya que independientemente de cuan segura es una organización, siempre habrá fallas simplemente porque existen personas en el proceso.

Finalmente, otro medio en que los equipos trampa ayudan a proteger a las organizaciones es en la respuesta. Una vez que una organización detecta un ataque surge como interrogante la respuesta. Esto puede ofrecerle al personal de seguridad uno de los más grandes retos, ya que la determinación de la identidad, la forma en que se accedió al sistema y el daño real ocasionado por un atacante, son datos de difícil o casi nula obtención. En general, es prácticamente imposible sacar de línea a los sistemas comprometidos para analizarlos.

Sistemas productivos tales como servidores de mail son tan críticos en la operatoria que es impensado "bajarlos", sacándolos de línea para aplicarles prácticas de análisis forense apropiadas, conformándose con la realización de controles de funcionalidad mientras siguen prestando servicios. Esto reduce la posibilidad de analizar que ocurrió, cuanto daño se produjo, e incluso si el atacante llegó a quebrar otros sistemas.

Otro inconveniente es que si el sistema es sacado de línea es muy difícil determinar las causas que originaron la caída, ya que es complicado identificar, de toda la información almacenada, cuales registros corresponden a la actividad normal del día a día y cuales a las del atacante.

Los equipos trampa ayudan en la resolución de estas debilidades. Al no tener datos productivos, pueden ser retirados del entorno de producción para un análisis forense exhaustivo, sin que esto impacte en las operaciones diarias.

Por último, el uso de los equipos trampa en investigación es considerada una herramienta útil al recopilar información valiosa sobre las amenazas. Los dispositivos coleccionan dicha información, que posteriormente puede utilizarse para una variedad de propósitos, incluso el análisis de tendencias, la identificación de nuevas herramientas o métodos, asaltadores y sus comunidades o motivaciones, y dando alerta anticipada y predicción.

Glosario Tecnológico

Agent - Agente:
En detección de intrusiones, una entidad independiente que realiza labores de monitoreo y análisis de bajo nivel y envía sus resultados a un coordinador o un transmisor-receptor. También conocido como sensor.

Anomaly - Anomalía:
No usual o estadísticamente raro.

Anomaly detection - Detección de anomalías:
Detección basada en la actividad del sistema que coincide con la definida como anormal.

Application log - Registro de aplicación:
En sistemas Windows, es uno de los tres tipos de registros de eventos. Este registro contiene los eventos generados por las aplicaciones.

Application Program Interface - Interfaz de programación de aplicaciones (API):
Conjunto de rutinas, protocolos, y herramientas para la construcción de aplicaciones software.

Artificial Intelligence - Inteligencia artificial (AI):
Ciencia que busca la comprensión de entidades inteligentes.

Assessment system - (Véase **"Vulnerability Scanner"**).

Assessment - Evaluación, estimación.

Attribute - Atributo.

Authentication - Autenticación, autentificación:
Proceso de confirmar la identidad de una entidad de sistema (un usuario, un proceso, etc.).

Authorization - Autorización:
Acción de otorgar el acceso a usuarios, objetos o procesos.

Back door - Puerta trasera:
Mecanismo que permite a un atacante entrar y controlar un sistema de forma oculta. Suelen instalarse justo después de comprometer un sistema. (Véase también **"Vulnerabilidad"**).

Backbone - Eje principal, red troncal, estructura principal.

Bandwidth - Amplitud de banda, ancho de banda:
1. Diferencia en hertzios (Hz) entre la frecuencia más alta y la más baja de un canal de transmisión. **2.** Datos que pueden ser enviados en un período de tiempo determinado a través de un circuito de comunicación. Se mide en bits por segundo (bps).

Batch - Lote:
En informática, programa asignado a un sistema para ser ejecutado de forma desatendida. Los trabajos por lotes suelen ejecutarse en un plano secundario, mientras que los interactivos se ejecutan en primer plano.

Binary Log Format - Formato de registro binario:
Formato de registro utilizado por herramientas basadas en las librerías "libpcap", como por ejemplo "tcpdump". Se aplica para registrar el tráfico de red. Algunas de las ventajas del formato binario sobre el formato ASCII, son su menor necesidad de almacenamiento y que la información que contiene puede ser accedida en menos tiempo.

Bit:
Abreviación de "binary digit". Unidad elemental de información en un sistema informático. Tiene un único valor en formato binario: "0" ó "1". (Véase también **"Byte"**).

Black-hat Community - Comunidad del Sombrero negro:
Aquellos que acceden o intentan acceder a recursos de información a través de Internet sin tener autorización para hacerlo.

Bridge - Puente:
Dispositivo que permite la interconexión de dos redes con igual o distintos interfaces o pila de protocolos. Realiza funciones de encaminamiento de paquetes a nivel de enlace. Un puente multipuerto es prácticamente un conmutador. (Véase también **"Conmutador"**).

Buffer - Búfer, memoria intermedia:
Área de memoria de un sistema reservada para almacenar información de forma temporal. Generalmente se utiliza para compensar las diferencias de velocidad surgidas entre varias señales o procesos.

Buffer Overflow - Desbordamiento de búfer, desbordamiento de la pila:
Técnica que consiste en almacenar más datos en un búfer de los que puede contener. Los datos que no caben pueden invadir zonas adyacentes a la del búfer, corrompiéndolas o sobrescribiéndolas. Este método es ampliamente utilizado para realizar ataques que abren interfaces de comando remotas.

Bug - Error, fallo:
En informática, fallo (o agujero) de seguridad.

Byte - Byte, octeto:
Unidad de información compuesta por ocho bits. Modificando los diferentes bits de un byte se pueden obtener hasta 256 combinaciones diferentes.

Cache - Almacén, ante-memoria, depósito:
Mecanismo especial de almacenamiento de alta velocidad. Puede ser una zona reservada de la memoria principal, o un dispositivo independiente de almacenamiento de alta velocidad.

Checksum - Suma de control, suma de verificación, suma de comprobación:
Algoritmo matemático que genera un número único a partir de un conjunto de datos, utilizado para comprobar la integridad de los mismos.

Composition - Composición:
1. En detección de intrusiones, proceso de combinar información procedente de distintas fuentes en un flujo de datos coherente. **2.** En seguridad informática, combinar un conjunto de componentes en un sistema para obtener los atributos de seguridad del mismo, según las propiedades de dichos componentes.

Compromised - Comprometido, violentado:
Estado de un equipo/sistema cuando un intruso ha ingresado.

Correlation - Correlación:
En detección de intrusiones, relación que se establece entre diferentes fuentes de información.

Crack - Invadir, penetrar.

Data Mining - Minería de datos:
Arte y ciencia de descubrir y explotar relaciones nuevas, útiles y provechosas en grandes cantidades de información.

Datagram - Datagrama:
Mensaje que se envía en una red de comunicaciones por intercambio de paquetes.

DDoS - (Véase **"Distributed Denial of Service"**).

Demilitarized Zone - Zona desmilitarizada, red perimétrica (DMZ):
Máquina o pequeña subred situada entre una red interna de confianza (como una red local privada) y una red externa no confiable (como Internet). Normalmente en esta zona se sitúan los dispositivos accesibles desde Internet, como servidores Web, FTP, SMTP o DNS, evitando la necesidad de acceso desde el exterior a la red privada. Este término es de origen militar y se utiliza para definir un área situada entre dos enemigos.

Deceptive application - Aplicación engañosa:
Aplicación cuya apariencia y comportamiento emulan a una aplicación real. Normalmente se utiliza para controlar acciones realizadas por atacantes o intrusos.

Decoy server - Servidor señuelo o servidor trampa. Véase (**"Honeypot"**).

Denial of Service - Denegación de servicio (DoS):
Estrategia de ataque que consiste en saturar de información a la víctima con información inútil para detener los servicios que ofrece. (Véase también **"Denegación de servicio distribuida"**).

Distributed Denial of Service - Denegación de servicio distribuida (DDoS):
Estrategia de ataque que coordina la acción de múltiples sistemas para saturar a la víctima con información inútil para detener los servicios que ofrece. Los sistemas utilizados para el ataque suelen haber sido previamente comprometidos, pasando a ser controlados por el atacante mediante un cliente DDoS. (Véase también "Denegación de servicio").

DMZ - (Véase **"Demilitarized Zone"**).

DoS - (Véase **"Denial of Service"**).

Encryption - Cifrado:
Proceso mediante el cual se toma un mensaje en claro, se le aplica una función matemática, y se obtiene un mensaje codificado.

Ethernet:
Sistema de red de área local de alta velocidad.

Exploit - Ardid, artificio:
Implementación de un fallo de seguridad utilizado para comprobar y demostrar la existencia del fallo, o bien para comprometer al sistema de forma ilícita.

False negative - Falso negativo:
En detección de intrusiones, error producido cuando el sistema diagnostica como ataque una actividad normal. También conocido como error de tipo II.

False positive - Falso positivo:
En detección de intrusiones, error producido cuando el sistema diagnostica como actividad normal un ataque. También conocido como error de tipo I.

File Transfer Protocol - Protocolo de transferencia de ficheros (FTP):
Protocolo que permite a un usuario de un sistema acceder a otro sistema de una red, e intercambiar información con el mismo.

Fingerprint - Huella dactilar, huella digital.

Firewall
Herramienta de seguridad que proporciona un límite entre redes de distinta confianza o nivel de seguridad, mediante el uso de políticas de control de acceso de nivel de red.

Flag - Indicador.

Free Software - Software libre:
Código que otorga libertad a los usuarios para ejecutar, copiar, distribuir, estudiar, cambiar y mejorar el mismo. (Véase también **"Código abierto"**).

FTP - (Véase **"File Transfer Protocol"**).

Gateway - Pasarela, puerta de enlace.

Hash Function - Función resumen:
Función de cifrado que permite detectar cambios en objetos.

HID - (Véase **"Host based intrusion detection"**).

Honeynet - Red trampa:
Es un tipo de sistema trampa. Red de sistemas reales diseñada para ser comprometida.

Honeypot - Equipo o Sistema trampa:
Recurso de sistema de información cuyo valor reside en el uso no autorizado o ilícito de dicho recurso.

Honeywall:
Equipo dentro de la red trampa que actúa como pasarela/puente, y donde se instalan las utilidades de control y captura de datos (iptables, ebtables, snort, sebek, etc.).

Host - Anfitrión, máquina anfitriona, puesto.

Host based - Basado en máquina:
Que controla información de fuentes internas a una máquina.

HTTP - (Véase **"Hypertext Transfer Protocol"**).

Hub - Concentrador:
Dispositivo que permite la interconexión de las estaciones de trabajo entre sí. No realiza funciones de encaminamiento; lo que recibe por un puerto lo reenvía a través del resto. (Véase también **"Repetidor"**).

Hypertext Transfer Protocol - Protocolo de Transferencia de Hipertexto (HTTP):
Protocolo usado para la transferencia de documentos www. (Véase también **"www"**).

Identification and authentication - Identificación y autenticación (I&A):
Mecanismo de seguridad que asigna una identidad única a cada usuario (identificación) y la comprueba (autenticación).

IDS - (Véase **"Intrusion Detection System"**).

IETF - (Véase **"Internet Engineering Task Force"**).

In-line mode - Modo en línea:
Método de intercepción del tráfico de red, que consiste en hacer pasar todo el tráfico a través de un monitor o rastreador, generalmente configurado como puente, para minimizar el impacto sobre el rendimiento de la red y dificultar su detección.

Integration - Integración:
En ingeniería de sistemas, combinación de componentes en una entidad coherente.

Integrity checker - Comprobador de integridad:
Herramienta de seguridad que utiliza funciones resumen basadas en algoritmos de cifrado, para detectar alteraciones en objetos del sistema.

Internet Engineering Task Force - Grupo de trabajo de ingeniería de internet (IETF):
Una de las principales organizaciones encargadas de la formulación de estándares en Internet.

Internet Protocol Security - Seguridad de protocolo Internet (IPSec):
Conjunto de protocolos desarrollados por el IETF para soportar el intercambio seguro de paquetes en el nivel IP. IPsec se utiliza ampliamente para implementar Redes Virtuales Privadas (VPNs).

Internet Protocol version 6 - Protocolo Internet versión 6:
Revisión del protocolo Internet que viene a sustituir a la tradicional versión 4. Cuenta con nuevas características, como mejoras en las direcciones, simplificación de la cabecera, nuevo soporte de extensiones y opciones, etiquetado de tráfico, y capacidades de autenticación y privacidad.

Interoperability - Interoperabilidad:
Capacidad de un sistema para trabajar con otros sin que sean necesarios grandes esfuerzos por parte del usuario.

Intrusion - Intrusión:
Violación intencionada de las políticas de seguridad de un sistema.

Intrusion detection - Detección de intrusiones:
Proceso que controla los eventos de un sistema o red, en busca de signos que indiquen problemas de seguridad.

Intrusion Detection System - Sistema de detección de intrusiones (IDS):
Sistema que controla redes y sistemas en busca de violaciones de políticas de seguridad. Está compuesto por tres elementos fundamentales: fuentes de información, motor de análisis y mecanismos de respuesta.

Intrusion Prevention System - Sistema de prevención de intrusiones (IPS):
Sistema que combina las capacidades de bloqueo de un firewall y las de análisis de un IDS. Está diseñado para detener ataques antes de que tengan éxito.

Intrusive monitoring - Monitoreo de intrusión:
En análisis de vulnerabilidades, obtener información mediante la realización de comprobaciones que afectan al estado del sistema, llegando en algunos casos a provocar su caída.

IPS - (Véase **"Intrusion Prevention System"**).

IPsec - (Véase **"Internet Protocol Security"**).

IPv6 - (Véase **"Internet Protocol versión 6"**).

Isolation - Aislamiento.

Libpcap:
Interfaz independiente del sistema para la captura de paquetes de nivel de usuario, desarrollada en el "Lawrence Berkeley National Laboratory".

Log - Registro, historial.

Logger - Gestor de registro de actividades:
Componente del sistema encargado de las labores de registro de actividad.

Mainframe - Gran computadora, servidor corporativo, computadora central, macrocomputadora.

Man-in-the-middle attack - Ataque por interceptación:
Estrategia de ataque en la que el atacante intercepta una comunicación entre dos partes, substituyendo el tráfico entre ambas a voluntad y controlando la comunicación.

Masquerade - Enmascaramiento, falseamiento de identidad.

Masquerader - Enmascarado:
Atacante que accede a un sistema utilizando identificadores de usuario y contraseñas de usuarios legítimos.

Masquerading - Enmascaramiento, mimetización.

Message digest - Resumen de mensaje. (Véase **"Función resumen"**).

Misuse - Uso indebido:
Actividad o comportamiento conocida como mala o inapropiada.

Misuse Detection - Detección de usos indebidos:
Detección basada en la actividad del sistema que coincide con la definida como mala.

Monitor - Monitor, monitoreo:
Cualquier mecanismo o método utilizado por un sistema de detección de intrusiones para obtener información.

Monitoring policy - Política de monitoreo:
Conjunto de reglas que definen la forma en que se debe capturar e interpretar la información.

Multi-host based - Basado en multi-máquina:
Que controla la información de fuentes internas a múltiples máquinas. (Véase también **"Basado en Máquina"**).

Multihost - Multi-máquina.

Network based - Basado en red:
Que controla información de fuentes de red, generalmente captura de paquetes.

Network hop - Salto de red:
Estrategia de ataque en la que el atacante intenta ocultar su identidad realizando sus actividades desde otros sistemas comprometidos.

Network management - Gestión de redes:
Controlar diversos aspectos de una red para optimizar su eficiencia. Las cinco categorías de gestión de red son: seguridad, fallo, auditoría, configuración y gestión de rendimiento.

Network Node Intrusion Detector - Detector de Intrusiones de Nodo de Red:
Detector de intrusiones basado en red que se instala en una máquina. Esta medida ayuda a solventar problemas como los asociados a entornos conmutados o cifrado en las comunicaciones.

Network Tap - Dispositivo de escucha de red:
Dispositivo de aspecto externo similar a un concentrador o un conmutador, que permite a un rastreador interceptar el tráfico de red entre dos segmentos sin ser detectado. Además, apenas afecta al rendimiento de la red.

NID - (Véase **"Network Intrusion Detection"**).

NNID - (Véase **"Network Node Intrusion Detection"**).

Non credentialed analysis - Análisis sin acreditaciones:
En análisis de vulnerabilidades, enfoque de control pasivo en los que las contraseñas u otro tipo de credenciales no son necesarias. Normalmente implica el lanzamiento de ataques contra el sistema, provocando algún tipo de reacción.

Non intrusive monitoring - Monitoreo de no intrusión:
En análisis de vulnerabilidades, obtener información mediante la ejecución de una lista de comprobaciones de los atributos del sistema.

Open Source - Código abierto:
Software que cumple los criterios descritos por la iniciativa "Open Source". Este término no implica el acceso al código fuente. (Véase también **"Software Libre"**).

Open Systems Interconnection - Interconexión de Sistemas Abiertos (OSI):
Estructura de protocolos en siete niveles propuesta por ISO (International Standardization Organization) e ITU-T (International Telecommunication Union Telecommunication Standardization Sector).

OS fingerprinting - Identificación de sistema operativo:
Conjunto de técnicas utilizadas para determinar la identidad del sistema operativo de un sistema remoto. Generalmente se logra mediante el envío de determinados datos de red y el posterior análisis de las respuestas recibidas.

OSI - (Véase **"Open Systems Interconnection"**).

Packet - Paquete:
Estructura de datos con una cabecera que puede estar o no lógicamente completa. Más a menudo, se refiere a un empaquetamiento físico de datos que lógico. Se utiliza para enviar datos a través de una red conmutada de paquetes.

Passive response - Respuesta pasiva:
Respuesta en la que el sistema simplemente registra e informa de la intrusión o ataque, delegando en el usuario las acciones subsecuentes.

Password cracker - Destructor de contraseñas:
Herramienta de seguridad diseñada para descubrir las contraseñas de los usuarios. En la mayoría de los casos se utilizan diferentes aproximaciones para obtenerlas.

Patch - Parche:
En seguridad informática, código que corrige un fallo (agujero) de seguridad.

Plug-in - Accesorio, añadido, módulo.

Polymorphic shell - Interfaz de comandos polimórfica:
Interfaz de comandos cuyo código cambia con cada ejecución. Esto se hace para evadir los detectores de intrusión basados en reglas. En la mayoría de los casos se utilizan durante ataques de desbordamiento del búfer.

Polymorphic virus - Virus polimórfico:
Virus informático que cambia de aspecto con cada ejecución. Esta característica tiene el objeto de evitar a los detectores de virus.

Port scan - Sondeo de puertos, escaneo de puertos:
Barrido de puertos generalmente usado para determinar qué servicios ofrece un sistema. Es uno de los métodos más comunes entre los atacantes para obtener información de sus objetivos. (Véase también **"Escaneo Sigiloso de Puertos"**).

Privilege - Privilegio:
Nivel de confianza perteneciente a un objeto del sistema.

Promiscuous mode - Modo promiscuo:
Respecto a una interfaz de red, el modo de operación que genera una interrupción por cada actividad de red detectada. Esto permite a la interfaz recoger todo el tráfico de red de su segmento y entregárselo al detector de intrusiones.

Protocol stack - Pila de protocolos:
Conjunto de protocolos que se implementan en un determinado sistema.

Race condition - Condición de carrera:
Comportamiento anómalo provocado por una dependencia excesiva del tiempo relativo transcurrido entre diferentes eventos.

Real-time analysis - Análisis en tiempo real:
Análisis realizado de forma continua, con resultados obtenidos en un tiempo en que permita alterar el estado actual del sistema.

Record - Informe, historial.

Repeater - Repetidor:
Dispositivo que regenera la señal que pasa a través de la red, permitiendo extender la distancia de transmisión. Un repetidor multi-puerto se conoce como un concentrador. (Véase también **"Concentrador"**).

Router - Encaminador, enrutador:
Dispositivo que reenvía paquetes de datos entre redes. Permite conectar al menos dos redes. Los puntos de conexión con el "encaminador" son las puertas de enlace de cada red.

Rule base - Base de reglas:
Conjunto de reglas utilizadas para analizar los registros de datos.

Rule based - Basado en reglas:
En detección de intrusiones, que utiliza patrones de actividad (generalmente ataques conocidos) para reconocer una intrusión.

Scalability - Escalabilidad:
Forma en que la solución a un determinado problema se comporta cuando el tamaño del problema crece.

Scan - Escanear. (Véase **"Port scan"**).

Script - Guión:
Lista de comandos que puede ser ejecutada sin interacción por parte del usuario. Un lenguaje de "script" es un lenguaje de programación sencillo que puede ser utilizado para escribir guiones.

Script Kiddie:
Alguien que no tiene especiales conocimientos técnicos, que busca aleatoriamente debilidades en Internet para poder acceder a un sistema. No comprende realmente qué debilidad está explotando porque la debilidad fue descubierta por otro. Un "script kiddie" no busca una información o compañía en concreto, sino que más bien utiliza el conocimiento de la vulnerabilidad para encontrar una víctima en Internet que posea dicho fallo de seguridad.

Secure Shell - Interfaz de comandos segura (SSH):
También conocida como "Secure Socket Shell", es una interfaz de comandos basada en UNIX y un protocolo, para acceder de forma segura a una máquina remota. Es ampliamente utilizada por administradores de red para realizar tareas de gestión y control. SSH es un conjunto de tres utilidades: slogin, ssh y scp; versiones seguras de las anteriores utilidades de UNIX: rlogin, rsh y rcp.

Secure Socket Layer - Capa de conexión segura (SSL):
Protocolo creado por Netscape para permitir la transmisión cifrada y segura de información a través de la red.

Security - Seguridad:
1. Según un enfoque práctico, la seguridad implica que un sistema se comporte de la manera esperada. Esta definición depende de los niveles de confianza. **2.** Según un enfoque formal, consiste en el cumplimiento de la "tríada de conceptos": confidencialidad, integridad y disponibilidad.

Security log - Registro de seguridad:
En sistemas Windows, es uno de los tres tipos de registros de eventos. Este registro contiene los eventos considerados como relevantes en materia de seguridad.

Security policy - Política de seguridad:
1. Conjunto de estatutos que describen la filosofía de una organización respecto a la protección de su información y sistemas informáticos. **2.** Conjunto de reglas que ponen en práctica los requisitos de seguridad del sistema.

Segment - Segmento:
Unidad lógica de datos, en particular un segmento de TCP es la unidad de datos transferida entre dos módulos de TCP.

Sensor - Sensor:
En detección de intrusiones, una entidad que realiza labores de control y obtención de datos de las fuentes de información. También conocido como agente. En muchos IDS, el sensor y el analizador forman parte del mismo componente. (Véase también **"Agente"**).

Server Message Block - Bloque de mensajes de servidor (SMB):
También conocido como "Session Message Block", NetBIOS y LanManager. Es un protocolo utilizado por sistemas Windows para compartir ficheros, impresoras, puertos serie y otras entidades de comunicación entre ordenadores.

Session creep - Deslizamiento sigiloso de sesión:
Técnica utilizada por un usuario que consiste en modificar gradualmente su comportamiento para entrenar al detector de anomalías. De esta forma, se consigue que el detector diagnostique como actividad normal un posible ataque.

Shadow Password - Contraseña oculta.

Shell - Interfaz de comandos.

Signature - Firma, patrón:
En detección de intrusiones, patrones que indican los usos indebidos de un sistema.

Simple Mail Transfer Protocol - Protocolo simple de transferencia de correo:
Protocolo de comunicaciones para la transmisión de correo electrónico entre computadoras.

SMB - (Véase **"Server Message Block"**).

SMTP - (Véase **"Simple Mail Transfer Protocol"**).

Sniffer - Rastreador:
Dispositivo capaz de capturar todos los paquetes de datos que viajan por el segmento de red al que está conectado. Cuenta con una interfaz de red en modo promiscuo.

Sniffing cable - Cable de rastreo, cable de sólo recepción:
Cable de red modificado para imposibilitar el envío de datos, permitiendo exclusivamente su recepción.

Spanning port - Puerto de extensión, puerto abarcador:
Puerto especial con el que cuentan algunos conmutadores avanzados. Está programado para poder recibir una copia del tráfico destinado a uno o varios puertos del conmutador.

Spoofing - Falseamiento, enmascaramiento:
Modificación de la identidad de origen real durante una comunicación. El método más común consiste en alterar directamente la dirección origen de cada paquete de la comunicación.

SSH - Véase (**"Secure Shell"**).

SSL - Véase (**"Secure Socket Layer"**).

Stack - Pila:
Área de datos o búfer utilizada para almacenar peticiones que deben ser atendidas. Tiene una estructura FILO (primero en entrar, último en salir) o LIFO (último en entrar, primero en salir).

Stack smashing - Desbordamiento de la pila:
Caso especial del desbordamiento del búfer, en el que el objetivo es la pila del sistema. (Véase también **"Pila"** y **"Desbordamiento de Búfer"**).

Statistic Anomaly Filter - Filtro de anomalías estadísticas:
Filtro que permite la detección de actividades y comportamientos poco usuales o comunes.

Stealth port scan - Escaneo sigiloso de puertos:
Barrido de puertos mediante diversas técnicas con el fin de evadir los métodos de detección comunes. Algunas de estas técnicas implican un escaneo intencionadamente lento, o el envío de paquetes especiales aprovechando particularidades del protocolo. (Véase también **"Escaneo de Puertos"**).

Steganography - Esteganografía:
Arte de transmitir información de modo que la presencia de la misma pase inadvertida. Se suele hacer camuflando los datos en el interior de un texto, imagen, o fichero multimedia.

Stream - Corriente, flujo.

Subnet - Subred.

Switch - Conmutador:
Elemento utilizado para interconectar máquinas a una red. Tiene funciones de encaminamiento básico de tráfico de red, y permite subdividir las redes en segmentos, de forma similar a un puente. (Véase también **"Puente"**).

Switched environment - Entorno conmutado:
Entorno de red en el que predomina el uso de conmutadores.

System log - Registro de sistema:
1. En sistemas Windows, es uno de los tres tipos de registros de eventos. Este registro contiene los eventos generados por los componentes de sistema. **2.** en sistemas UNIX, ficheros de eventos del sistema y aplicaciones, que suelen consistir en ficheros de texto consistentes en una línea por cada evento.

Tap mode - Modo de escucha.

Target based - Basado en objetivo:
Que controla la información de determinados objetos, generalmente utilizando métodos de cifrado como funciones resumen para permitir la detección de cambios.

TCP/IP - Véase (**"Transmission Control Protocol / Internet Protocol"**).

Tcpdump:
Herramienta de control y adquisición de datos que realiza labores de filtrado, recopilación, y visualización de paquetes.

Testing by exploit - Probar mediante explosión:
Método de comprobación de seguridad que consiste en lanzar ataques conocidos contra el objetivo y estudiar los resultados. (Véase también **"Análisis de Vulnerabilidades"**).

Thread - Hebra, hilo (de mensajes o de ejecución), flujo de control o flujo de ejecución.

Threat - Amenaza:
Situación o evento con que puede provocar daños en un sistema.

Token based - Basado en testigo:
Sistemas que emplean elementos especiales como tarjetas inteligentes, llaves, o discos para la autenticación de usuario.

Trail - Rastro, registro.

Transmission Control Protocol / Internet Protocol - Protocolo de Control de Transmisión / Protocolo Internet (TCP/IP):
Conjunto de protocolos básicos sobre los que se fundamenta Internet. Se sitúan en torno al nivel tres y cuatro del modelo OSI.

Trojan Horse - Caballo de Troya, troyano:
Programa informático de aspecto inofensivo que oculta en su interior un código que permite abrir una "puerta trasera" en el sistema en que se ejecuta. (Véase también **"Puerta Trasera"**).

Trust - Confianza:
Esperanza firme de que un sistema se comporte como corresponde.

Trusted processes - Procesos de confianza:
Procesos que sirven para cumplir un objetivo de seguridad.

Trusted systems - Sistemas de confianza:
Sistemas que emplean las suficientes medidas para cumplir los requisitos necesarios para su uso en el proceso de información sensible o clasificada.

Type I error - Error de Tipo I:
En detección de intrusiones, error producido cuando el sistema diagnostica como ataque una actividad normal. También conocido como falso positivo. (Véase también **"Falso Positivo"**).

Type II error - Error de Tipo II:
En detección de intrusiones, error producido cuando el sistema diagnostica como actividad normal un ataque. También conocido como falso negativo. (Véase también **"Falso Negativo"**).

User-agent - Agente de usuario.

Virtual Private Network - Red privada virtual (VPN):
Red generalmente construida sobre infraestructura pública, que utiliza métodos de cifrado y otros mecanismos de seguridad para proteger el acceso y la privacidad de sus comunicaciones.

VPN - (Véase **"Virtual Private Network"**).

Vulnerabilities - Vulnerabilidades:
Debilidades en un sistema que pueden ser utilizadas para violar las políticas de seguridad.

Vulnerability analysis - Análisis de vulnerabilidades:
Análisis del estado de la seguridad de un sistema o sus componentes mediante el envío de pruebas y recogida de resultados en intervalos.

Vulnerability scanner - Escáner o analizador de vulnerabilidades:
Herramienta diseñada para llevar a cabo análisis de vulnerabilidades.

Web - Malla, telaraña:
Servidor de información www. Se utiliza también para definir el universo www en su totalidad. (Véase también **"www"**).

Wireless - Inalámbrico.

World Wide Web - Malla mundial, telaraña mundial:
Sistema de información distribuido, basado en hipertexto. La información puede ser de diferente naturaleza, como por ejemplo texto, gráfico, audio, o vídeo. (Véase también **"Web"**).

Worm - Gusano:
Programa informático que se auto-duplica y auto-propaga. A diferencia de los virus, suelen estar diseñados para redes.

Wrapper - Envoltura, empacador:
Software que complementa las características de otro software para mejorar determinados aspectos como compatibilidad, o seguridad.

www - (Véase **"World Wide Web"**).

Apéndice

Publicaciones del Comité de Basilea

El Comité de Supervisión Bancaria de Basilea emite periódicamente documentos guía para las actividades relacionadas con la administración de riesgos en el entorno financiero. Específicamente en relación con la operatoria de e-Banking y sus riesgos, las publicaciones vigentes a la fecha son:

- ***"Principios de administración del riesgo en e-Banking" (Documento Nº 98, julio de 2003)***

Este documento desarrolla 14 Principios de Administración del Riesgo para e-Banking, identificados por el Comité de Basilea para ayudar a las instituciones bancarias a desarrollar las políticas y procesos para el manejo del riesgo que permitan cubrir sus actividades de este tipo.

En el mes de mayo de 2001 el Comité había publicado, con carácter consultivo, el Documento Nº 82 "Principios de Administración del Riesgo en e-Banking", cuyos temas no difieren básicamente de la versión final, que se emitió con posterioridad al análisis de los comentarios y sugerencias recibidas de la comunidad bancaria.

- ***"Administración y supervisión de las actividades de e-Banking Transfronterizas" (Documento N° 99, julio de 2003):***

Este documento enfoca dos áreas en particular: la primera, la identificación de las responsabilidades de los bancos en la administración del riesgo respecto de las actividades de e-Banking transfronterizas. En este punto, la publicación complementa los conceptos del Documento N° 98 arriba citado, en cuanto a la necesidad de que los bancos integren la administración de riesgos derivados de las operaciones "cross-border" en e-Banking dentro del proceso general de administración de los riesgos.

El segundo objetivo es focalizar la atención en la necesidad de una supervisión efectiva de las actividades "cross-border" de e-Banking en el país de origen ("home country supervision"), así como promover la cooperación entre supervisores de los distintos países involucrados.

Siguiendo el proceso de emisión de documentos generalmente utilizado, el Comité había publicado en el mes de octubre de 2002 y con carácter consultivo, el Documento N° 93 "Administración y Supervisión de las Actividades de e-Banking Transfronterizas", cuyos temas no difieren básicamente de la versión final. La misma se emitió con posterioridad al análisis de los comentarios y sugerencias recibidas durante el período de consulta.

Las dos publicaciones antes citadas tienen sus orígenes en los análisis iniciados por el Grupo de e-Banking del Comité de Basilea (el EBG), cuyos primeros trabajos fueron los Documentos N° 35 "Administración del Riesgo para Actividades de e-Banking y Dinero Electrónico" del mes de marzo de 1998, y N° 76 "Iniciativas del Grupo de e-Banking del Comité de Basilea" del mes de octubre de 2000.

Cabe agregar que el primer trabajo de Basilea en relación con actividades a través de computadores, se emitió en el mes de julio de 1989 con el nombre de "Riesgos en los Sistemas de Computación y Telecomunicaciones" (Documento N° 6).

Por otra parte, con relación al manejo del riesgo operacional, el Comité ha publicado lo siguiente:

- ***"Sanas Prácticas para la Administración del Riesgo Operacional" (Documento N° 96, febrero de 2003):***

Este documento desarrolla 10 Principios de Administración del Riesgo Operacional, concebidos por el Comité de Basilea como guía en el proceso de tratamiento del riesgo operacional por parte de los bancos, y su impacto especialmente en la determinación del capital mínimo de las entidades financieras.

Los antecedentes de esta publicación son los Documentos N° 86 y 91 de "Sanas Prácticas para la Administración y Supervisión del Riesgo Operacional", de los meses de septiembre de 1998 y diciembre de 2001 respectivamente, que corresponden a las dos etapas consultivas del documento antes de su emisión final.

Previo a éstos, y como inicio de las discusiones sobre el tema, se emitieron el Documento N° 42 "Administración del Riesgo Operacional" del mes de septiembre de 1998, y el Trabajo N° 8 "Tratamiento Regulatorio del Riesgo Operacional" del mes de septiembre de 2001.

En lo que respecta al tratamiento particular de enfoques de medición avanzada (AMA) aplicados a entidades con subsidiarias en el exterior, el Comité ha emitido la publicación N° 106 en Enero/2004,y en cuanto a las "Consideraciones prácticas de la implementación de Basilea II" se ha emitido la publicación N° 109 de Julio/2004.

En resumen, los documentos emitidos hasta la fecha son los siguientes:

e-Banking

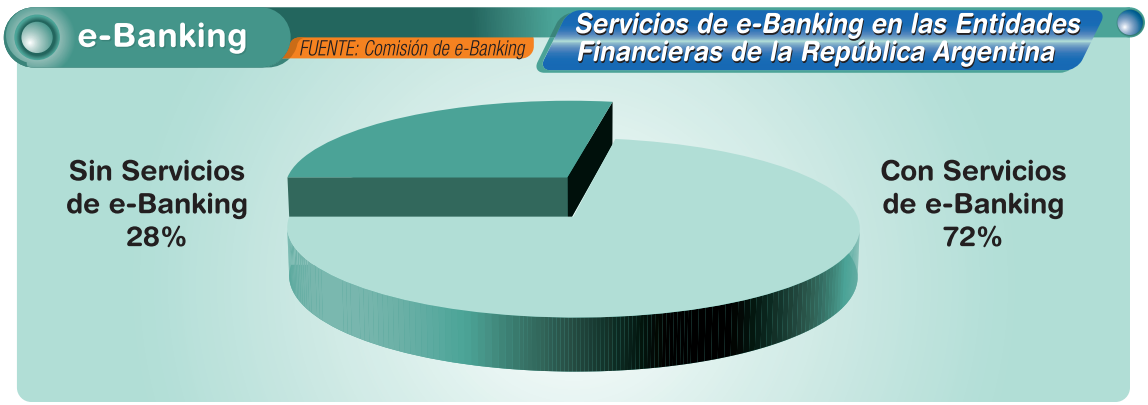
FUENTE: Comisión de e-Banking

Tema	Documentos de Basilea vigentes a la fecha	Documentos emitidos — Antecedentes Documentos Consultivos
Administración del riesgo en e-Banking	Nº 98, Julio 2003	Documento Nº 82, Mayo 2001 Documento Nº 76, Octubre 2000 Documento Nº 35, Marzo 1998
Operaciones "cross-border" en e-Banking	Nº 99, Julio 2003	Documento Nº 93, Octubre 2002 Documento Nº 76, Octubre 2000 Documento Nº 35, Marzo 1998
Riesgo operacional (conceptos básicos)	Nº 96, Febrero 2003	Documento Nº 91, Diciembre 2001 Documento Nº 86, Septiembre 1998 Documento Nº 42, Septiembre 1998 Working paper Nº 8, Septiembre 2001
Otros temas de riesgo operacional	Nº 106, Enero 2004 Nº 109, Julio 2004	

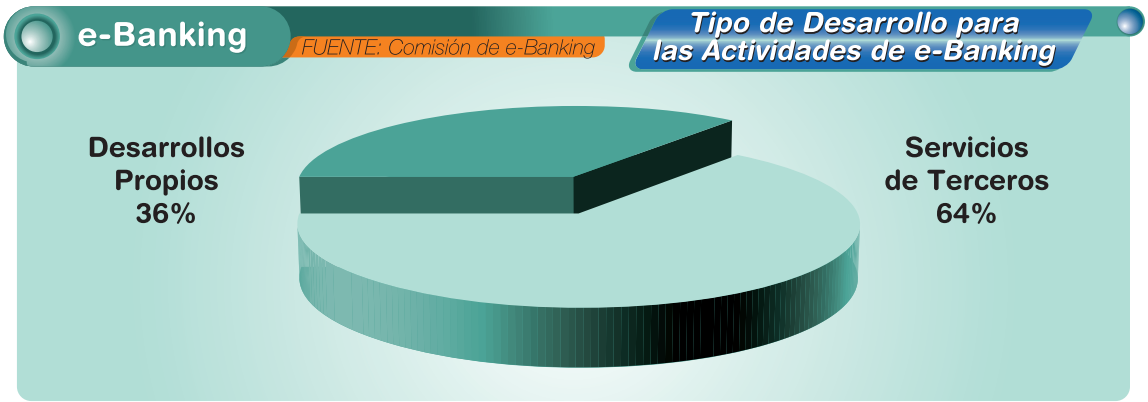
Indicadores actuales de e-Banking en el Sistema Financiero Argentino

De acuerdo a un relevamiento efectuado por esta Comisión durante el primer trimestre del año 2004, basado en un requerimiento preliminar efectuado a las entidades financieras sobre la infraestructura tecnológica para las operatorias de e-Banking (Com. "A" 4007), se lograron obtener en un primer análisis de la información relevada las siguientes conclusiones:

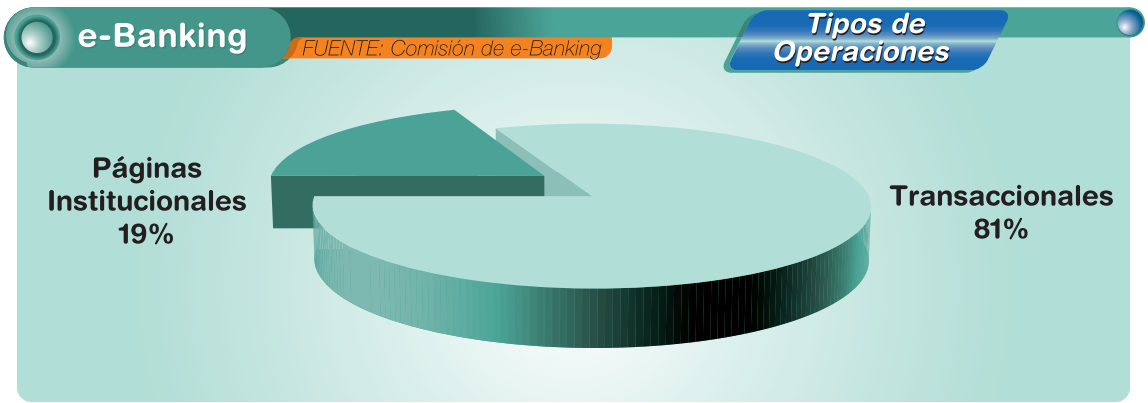
• el 72% de las entidades financieras argentinas brinda servicios específicos para las actividades de e-Banking;



• el 36% de las entidades financieras de la República Argentina posee desarrollos propios para las actividades de Banca Electrónica, y el 64% utiliza servicios tercerizados;



• el 81 % de las páginas de las entidades financieras cuentan con la posibilidad de realizar operaciones transaccionales, y el resto sólo brinda información institucional;



• la cantidad mensual estimada de transacciones procesadas asciende a 8.500.000, y

• el volumen monetario aproximado es de 3.500.000.000 pesos.

Fuentes de documentación

- **"Operational Risk Control with Basel II: Basic Principles and Capital Requirements"**
  Dimitris Chorafas, Publisher: Butterworth-Heinemann, ISBN: 0750659092

- **"Sound Practices for the Management and Supervision of Operational Risk"**
  Basel Committee on Banking Supervision - February 2003

- **"Risk Management Principles for Electronic Banking"**
  Basel Committee on Banking Supervision - July 2001

- **"Modeling, Measuring and Hedging Operational Risk"**
  Marcelo G. Cruz, Publisher: John Wiley & Sons, ISBN: 0471515604

- **"Operational Risk: Regulation, Analysis and Management"**
  Carol Alexander, Publisher: Financial Times Prentice Hall, ISBN: 0273659669

- **"Strategic Outsourcing: A Structured Approach to Outsourcing Decisions and Initiatives"**
  Maurice F. Greaver, Publisher: AMACOM, ISBN: 0814404340

- **"Intelligent IT Outsourcing: Eight Building Blocks to Success"**
  Sara Cullen and Leslie Willcocks - Publisher: Butterworth-Heinemann, ISBN: 0750656514

- **"The IT Outsourcing Guide"**
  Rob Aalders, Publisher: John Wiley & Sons, ISBN: 0471499358

- **"Outsourcing for Radical Change: A Bold Approach to Enterprise Transformation"**
  Jane C. Linder, Publisher: AMACOM, ISBN: 0814472184

- **"Banks and the Possibilities of E-Commerce"**
  Marcelo Héctor González, CISA - Control Journal ISACA magazine v4, 2001

- **"Computer Security Handbook 4th Edition"**
  Edited by Seymor Bosworth and M.E. Kabay, Publisher: John Wiley & Sons; 4th edition, ISBN: 0471412589

- **"Inside Network Perimeter Security-The Definitive Guide to Firewalls, VPNs, Routers and Intrusion Detection Systems"**
  Stephen Northcutt, Lenny Zeltser, Scott Winters, Karen Kent Frederick and Ronald W. Ritchey, Publisher: Que, ISBN: 0735712328

- **"Hackers Beware: Defending Your Network From the Wiley Hacker"**
  Eric Cole, Publisher: Que, ISBN: 0735710090

- **"Fundamentals of Network Security"**
  John E. Canavan, Publisher: Artech House, ISBN: 1580531768

Notas

Editado por Invercas S.A.