

**GESTION DE RIESGOS PARA LA**

**BANCA ELECTRONICA**

**Y**

**ACTIVIDADES CON DINERO ELECTRONICO**

**Comité de Basilea para la Supervisión Bancaria**

**Basilea**

**Marzo de 1998**

## INDICE

<b>1.</b>	<b>Introducción</b>	<b>1</b>
1.1.	Finalidad y Organización	2
1.2	Definición de Banca Electrónica y de Dinero Electrónico	4
<b>2.</b>	<b>Identificación y Análisis de Riesgos</b>	<b>5</b>
2.1	Riesgo Operativo	6
2.2.	Riesgo de Reputación	8
2.3	Riesgo Legal	10
2.4	Otros Riesgos	12
2.5	Asuntos Transterritoriales	13
<b>3.</b>	<b>Gestión de Riesgos</b>	<b>14</b>
3.1	Evaluación de los Riesgos	15
3.2	Control de los Riesgos	16
3.3	Riesgos de Seguimiento	21
3.4	Gestión de los Riesgos Transterritoriales	22
<b>Anexo:</b>	<b>Ejemplos de Posibles Riesgos y Medidas para la Gestión de Riesgos en la Banca Electrónica y Dinero Electrónico para Consumidores</b>	<b>24</b>

## **Gestión de Riesgos para la Banca Electrónica y las Actividades con Dinero Electrónico**

### **1. Introducción**

Los medios de pago electrónico tendrán un lugar preponderante en el desarrollo del comercio electrónico y los servicios y productos bancarios electrónicos para consumidores, incluyendo el dinero electrónico, podrían crear nuevas oportunidades para los bancos. La banca electrónica podría permitir a los bancos ampliar sus mercados para sus actividades tradicionales de recepción de depósitos y otorgamiento de créditos, y ofrecer nuevos productos y servicios o fortalecer su posición competitiva en la oferta de servicios de pago ya existentes. Además, la banca electrónica podría reducir los costos de operación de los bancos.

En general, el desarrollo continuado de la banca electrónica y del dinero electrónica podría contribuir a mejorar la eficiencia del sistema bancario y de pagos y a reducir el costo de las transacciones con los consumidores a nivel nacional e internacional. Esto podría dar como resultado un aumento de la productividad y del bienestar económico. Los consumidores y los comerciantes podrían incrementar la eficiencia con la que hacen y reciben pagos y disfrutar de una mayor comodidad al respecto. La banca electrónica podría además permitir el acceso al sistema financiero, de aquellos consumidores que anteriormente tenían un acceso limitado.

El alcance de este informe es necesariamente limitado en dos aspectos. Primero, trata sobre la gestión de riesgos de la banca electrónica y de las actividades con dinero electrónico desde la perspectiva de la supervisión bancaria solamente y no aborda, por ejemplo, las consecuencias monetarias. En segundo lugar, si bien muchos de los riesgos descritos en el informe se relacionan tanto con los emisores como con los proveedores bancarios y extra bancarios, este informe se refiere solamente a los bancos.

## **1.1 Finalidad y Organización**

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

La finalidad de este documento es proporcionar una orientación para las autoridades de supervisión y las organizaciones bancarias relacionada con los métodos de identificación, evaluación, gestión y control de los riesgos asociados con la banca electrónica y el dinero electrónico. El Comité de Basilea ve este documento como un paso inicial en el análisis y deliberación en curso de los asuntos de supervisión y respuestas relacionadas con los avances tecnológicos de los productos y servicios electrónicos para consumidores.

El Comité de Basilea distribuye el presente documento a los supervisores del mundo entero con la esperanza que facilitará el desarrollo de sistemas apropiados de supervisión para la gestión de riesgos en la banca electrónica y las actividades con dinero electrónico. Los supervisores podrán hacer circular este documento entre las instituciones bajo su supervisión.

Las deliberaciones sobre este tema son generales ya que la tecnología de la banca electrónica y dinero electrónico cambia rápidamente y los productos y servicios del futuro podrán ser muy diferentes de los disponibles en el presente. En esta fase inicial de desarrollo de algunas actividades de la banca electrónica y dinero electrónico, no se pueden medir algunos aspectos de los riesgos. Un sistema de reglamentación prematuro podría paralizar la innovación y la creatividad en estas áreas. Por lo tanto, los supervisores deberían incitar a los bancos a que desarrollen un proceso de gestión de riesgos que sea lo suficientemente riguroso y amplio como para tratar los riesgos importantes, que se conocen, y los suficientemente flexibles como para acomodar cambios en el tipo e intensidad de los

riesgos asociados con sus actividades de banca electrónica y dinero electrónico. Este proceso de gestión de riesgos será eficiente en la medida en que evolucione en forma constante.

Las restantes secciones de este documento están organizadas de la siguiente manera. La sección después de la Introducción presenta definiciones de banca electrónica y dinero electrónico y se refiere al rol que podrán tener los bancos como participantes en las actividades de dinero electrónico. La identificación y el análisis de los riesgos no pretenden ser exhaustivos, sino que la intención es llegar a una discusión ilustrativa de los tipos de problemas que pueden presentarse a los bancos. De estos problemas, los estudios sugieren que los riesgos más probables son el de operaciones, de la reputación y legal.<sup>1</sup>

A medida que se progresa en el desarrollo de la banca electrónica y dinero electrónico, es probable que aumente la interacción entre bancos y sus clientes internacionales. Dichas relaciones podrán plantear aspectos diferentes y riesgos para los bancos y para los supervisores. En este sentido, la Sección II considera los riesgos transterritoriales.

Sobre la base de la identificación y el análisis de riesgos, la Sección III presenta los pasos principales de un proceso de gestión de riesgos para bancos que se dedican a la banca electrónica y a las actividades de dinero electrónico. Este proceso comprende tres pasos principales: evaluación de los riesgos, ejecución de medidas de control de riesgos y seguimiento de los riesgos.

---

<sup>1</sup> Los bancos podrán también enfrentarse a riesgos que podrían afectar el valor de sus intereses como accionistas. Por ejemplo, ante la selección de una de varias nuevas tecnologías, la administración del banco corre el riesgo de escoger una cuyo uso no es luego generalizado y, por lo tanto, no tiene éxito, o puede escoger una que no se adapta adecuadamente a otros productos y servicios. Como ocurre con cualquier decisión tomada por la administración, los riesgos para el éxito financiero, que presentan la banca electrónica y el dinero electrónico, son una preocupación primordial para la administración y los dueños del banco. Sin embargo, como las autoridades de supervisión están encargadas de la protección del sistema bancario, pero no de su rentabilidad, dichos asuntos relacionados con el "valor de las acciones" no constituyen una preocupación directa para los supervisores, al menos que la viabilidad de una institución se vea amenazada. Por lo tanto, el presente documento no asume esta perspectiva de los riesgos del dinero electrónico y de la banca electrónica.

## 1.2 Definición de Banca Electrónica y Dinero Electrónico

1.2.1 La *banca electrónica* se refiere al suministro de productos y servicios bancarios para consumidores por medio de canales electrónicos.<sup>2</sup> Estos productos y servicios pueden incluir la recepción de depósitos, préstamos, manejo de cuentas, asesoría financiera, pago electrónico de facturas y el suministro de otros productos y servicios de pago electrónico, como ser, dinero electrónico (definido en forma separada más bajo).

Dos de los aspectos fundamentales de la banca electrónica son: las características de los canales de entrega y los medios disponibles a los consumidores para acceder a estos canales. Los canales de entrega más comunes incluyen redes "cerradas" y "abiertas". Las "redes cerradas" limitan el acceso a los participantes (instituciones financieras, consumidores, comerciantes y suministradores de servicios para terceros) que son miembros en virtud de un acuerdo específico. Las "redes abiertas" no tienen estos requisitos de membresía. Actualmente, los productos y servicios de la banca electrónica son suministrados a los consumidores por medio de una variedad de dispositivos de acceso, como ser, terminales en los puntos de venta, cajeros automáticos, teléfonos, computadoras personales, *smart cards* y otros.

1.2.2 El *dinero electrónico* se refiere a un valor almacenado o mecanismos pagados por adelantado para la ejecución de pagos por medio de terminales en el punto de venta, transferencias directas entre dos dispositivos, o mediante redes abiertas de computación, como ser el Internet.<sup>3</sup> Los productos de valor almacenado, incluyen

---

<sup>2</sup> Este documento se concentra en la banca electrónica para consumidores y servicios de pago electrónico. Los pagos electrónicos de gran valor y otros servicios para transacciones interbancarias quedan fuera del alcance de este documento.

<sup>3</sup> Varios órganos oficiales han emitido su propia definición de dinero electrónico. Como lo indica un informe reciente del Grupo de los Diez sobre el dinero electrónico, una definición precisa de dinero electrónico es difícil, en parte porque las innovaciones tecnológicas hacen confusa la distinción entre diferentes formas de mecanismos electrónicos de pago anticipado. (Ver *Electronic Money: Consumer protection, law enforcement, supervisory and cross-border issues*, Grupo de los Diez, abril de 1997, lista de dichos estudios). El presente documento está basado tanto en el informe del Grupo de los Diez, como en *Security of Electronic Money*, Bank for International Settlements, agosto de 1996, para establecer una definición del dinero electrónico. Este último informe explica las diferencias en la representación técnica del dinero en productos de valor almacenado. Los productos "basados en los saldos" son dispositivos que manejan un libro de cuentas numérico de manera tal que las transacciones se

mecanismos de "hardware" y "basados en tarjetas" (también llamados "monederos electrónicos") y mecanismos "software" o "basados en redes" (también llamados "efectivo digital"). Las tarjetas de valor almacenado pueden ser "uni-propósito" o "multi-propósito".<sup>4</sup> Las tarjetas de uni-propósito (por ejemplo, tarjetas para teléfonos) se usan para comprar un sólo tipo de bien o servicios, o productos de un sólo vendedor. Las tarjetas multi-propósito pueden ser utilizadas para una variedad de compras a varios vendedores.<sup>5</sup>

Los bancos pueden participar en los esquemas de dinero electrónico como emisores, pero pueden, también, realizar otras funciones. Estas incluyen la distribución de dinero electrónico emitido por otras entidades; el rescate de las ganancias de las transacciones en dinero electrónico para los comerciantes, el manejo del procesamiento, compensación y liquidación de las transacciones de dinero electrónico; y el manejo de registros de transacciones.

## **2. Identificación y Análisis de los Riesgos**

Dados los cambios rápidos en la tecnología de información, es imposible hacer una lista exhaustiva. En este sentido, el presente documento pretende describir una serie amplia y representativa de riesgos que sirva de base para una orientación general de la gestión de riesgos. Los riesgos específicos con los que se enfrentan los bancos dedicados a la banca electrónica y a las actividades de dinero electrónico, pueden agruparse de acuerdo con las categorías de riesgo de otros documentos

---

llevan a cabo como débitos o créditos a una cuenta; y los productos "basados en notas", que realizan transacciones transfiriendo la cantidad correcta de "notas electrónicas" (también llamadas "monedas" o "fichas"), que son de denominación fija, de un dispositivo a otro. Las tarjetas de débito y las tarjetas de crédito son mecanismos de pago electrónico para consumidores, pero no son considerados como dinero electrónico porque no son mecanismos pagados anticipadamente.

<sup>4</sup> Las tarjetas de valor almacenado usan ya sea una franja magnética o un chip de computadora incrustada en la tarjeta. Una tarjeta de plástico con un chip de computadora (llamada "smart card") puede realizar operaciones de valor almacenado, además de otras funciones, como las operaciones de débito y crédito.

<sup>5</sup> Los términos multi-propósito y multi-funcional se usan cada vez más para transmitir la idea que la tarjeta, o dispositivo funciona como varios tipos de instrumento de pago (por ejemplo, tarjeta de crédito, tarjeta de débito, tarjeta de valor almacenado), y/o que la tarjeta puede ser utilizada para varios propósitos además de las transacciones financieras (por ejemplo, tarjeta de identificación, depósito de información médica personal). La falta de una terminología uniforme es quizás el reflejo de las rápidas innovaciones tecnológicas.

del Comité de Basilea sobre gestión de riesgos, y, en este sentido, los riesgos no son nuevos.<sup>6</sup> Esta clasificación de riesgos puede ser útil para la identificación sistemática de los riesgos en una organización bancaria. El Anexo presenta ejemplos de los riesgos específicos y problemas de los bancos, relacionados con la banca electrónica y las actividades de dinero electrónico, agrupados en categorías de riesgos.

Si bien los tipos básicos de riesgos generados por las actividades de la banca electrónica y dinero electrónico no son nuevos, la forma específica en que algunos de estos riesgos se genera, así como la magnitud de su efecto en los bancos pueden ser nuevos para los bancos y los supervisores. Algunos de los riesgos y problemas que los bancos deben enfrentar se relacionan tanto con el dinero electrónico, como con la banca electrónica. Sin embargo, habrá, probablemente, diferencias en el grado en que un riesgo específico se aplica a las actividades de dinero electrónico y banca electrónica.

En este momento, parecería que el riesgo operativo, riesgo a la reputación y riesgo legal son las categorías más importantes para la mayoría de las actividades de banca electrónica y dinero electrónico, especialmente para los bancos internacionales y en las tres sub-secciones siguientes se presentan manifestaciones específicas de estos tipos de riesgo. Algunos de los problemas específicos, tocan varias categorías de riesgos. Por ejemplo, una violación de seguridad que permita el acceso no autorizado a información sobre clientes puede ser clasificada como un riesgo operativo, pero dicho evento también expone al banco a un riesgo legal y a un riesgo a la reputación. A pesar de que estos diferentes tipos de riesgo pueden ser generados por un sólo problema, la gestión apropiada de riesgos puede exigir varias acciones correctivas para responder a cada uno de los diferentes riesgos. Otros riesgos pueden también ser importantes para algunas formas de banca electrónica y actividades de dinero electrónico, y estos son tratados a continuación. También se detallan posibles riesgos transterritoriales.

---

<sup>6</sup> Ver, por ejemplo, *Risk Management for Guidelines for Derivatives*, Basle Committee, July 1994, y *Core Principles for Effective Banking Supervision*, Basle Committee, September 1997. Este último documento incluye la presentación básica de las ocho categorías de riesgo: riesgo crediticio, riesgo de país y transferencia, riesgo de mercado, riesgo de la tasa de interés, riesgo de liquidez, riesgo operativo, riesgo legal y riesgo a la reputación. *Payment Systems in the Group of Ten Countries*, Bank for International Settlements, diciembre de 1993 presenta definiciones de los riesgos relacionados con los sistemas bancarios y de pagos.

## **2.1 Riesgo Operativo**

El riesgo operativo se genera del potencial de pérdida debida a deficiencias importantes en la confiabilidad e integridad del sistema. Los aspectos de seguridad son de la mayor importancia, ya que los bancos pueden sufrir ataques externos o internos a sus sistemas o productos. El riesgo operativo puede generarse también por el mal uso de los clientes, y por sistemas de banca electrónica y dinero electrónico mal diseñados o ejecutados. Muchas de las manifestaciones específicas posibles de estos riesgos, se aplican tanto a la banca electrónica, como al dinero electrónico.

### **2.1.1. Riesgos de Seguridad**

El riesgo operativo se genera en relación a los controles del acceso a los sistemas contables y de gestión de riesgos del banco, a la información que transmite a terceros y, en el caso de dinero electrónico, las medidas que utiliza el banco para detectar y controlar dinero falso. Controlar el acceso a los sistemas de los bancos se ha vuelto cada vez más complejo, en vista del crecimiento de las capacidades de los sistemas de computación, la dispersión geográfica de los puntos de acceso, y el uso de varias vías de comunicación, incluyendo redes públicas, como ser el Internet. Es importante hacer notar que en el caso de dinero electrónico, una violación de seguridad puede dar como resultado la creación fraudulenta de obligaciones del banco. En el caso de otras formas de banca electrónica, el acceso no autorizado puede conducir a pérdidas directas, un incremento de las obligaciones de los clientes y otros problemas.

Pueden ocurrir una variedad de problemas específicos de acceso y autenticación. Por ejemplo, los controles insuficientes pueden resultar en un ataque exitoso de usuarios inescrupulosos del Internet, quienes podrían acceder, recuperar y utilizar información sobre clientes del banco y en la introducción de un virus por terceras personas que entran en el sistema del banco.

Además de los ataques externos a los sistemas de dinero electrónico y banca electrónica, los bancos se exponen a riesgos operativos relacionados con fraudes de empleados: los empleados podrían recuperar datos de autenticación a fin de acceder a las cuentas de clientes, o robar tarjetas de

valor almacenado. Los errores involuntarios de los empleados pueden también comprometer los sistemas del banco.

Una de las preocupaciones más importantes de las autoridades de supervisión es la fabricación de dinero electrónico falso, y esta preocupación se intensifica cuando los bancos no incorporan medidas suficientes para detectar y controlar este tipo de actividad delictuosa. El banco se enfrenta a un riesgo operativo generado por la falsificación de dinero, ya que puede ser responsable por el saldo del dinero electrónico falsificado. Además, pueden existir costos asociados con la reparación de un sistema alterado.

### **2.1.2 Diseño, Ejecución y Mantenimiento de Sistemas**

Un banco se enfrenta al riesgo de que los sistemas que selecciona no estén bien diseñados o ejecutados. Por ejemplo, un banco se expone al riesgo de una interrupción o retraso de sus sistemas cuando el sistema de banca electrónica o dinero electrónico que escoge es incompatible con las exigencias de los usuarios.

Muchos bancos confiarán, probablemente, en proveedores externos de servicios y expertos externos para ejecutar, operar y apoyar partes de sus actividades de dinero electrónico y banca electrónica. Esta dependencia puede ser conveniente porque permite a los bancos contratar, fuera de la compañía, ciertos aspectos de la provisión de banca electrónica y actividades de dinero electrónico que no pueden proveer ellos mismos en forma económicamente rentable. Sin embargo, la dependencia de fuentes externas expone al banco a riesgos operativos. Los proveedores de servicios pueden no tener la experiencia necesaria para ofrecer los servicios esperados por el banco, o pueden no actualizar su tecnología en forma oportuna. Las operaciones de un proveedor de servicios pueden ser interrumpidas por problemas con sistemas, o dificultades financieras, impidiendo la entrega de productos o servicios por parte del banco.

El ritmo acelerado que caracteriza los cambios de tecnología de la información representa otro riesgo para los bancos, es decir, el de los sistemas obsoletos. Por ejemplo, los programas de computadora que facilitan el uso por los consumidores de los productos de banca electrónica y

dinero electrónico necesitarán ser actualizados, pero los canales de distribución de los programas actualizados presenta un riesgo para los bancos, ya que criminales o individuos maliciosos pueden interceptarlos y modificarlos. Además, los cambios rápidos de tecnología pueden no dar el tiempo necesario al personal para que comprenda bien los sistemas utilizados por el banco. Esto podría resultar en problemas operativos para los sistemas nuevos o actualizados.

### **2.1.3 Mal Uso por los Clientes de los Productos y Servicios**

Como es el caso con los servicios bancarios tradicionales, el mal uso por los clientes, ya sea intencional o involuntario, es otra fuente de riesgo operativo. Este riesgo puede verse intensificado cuando un banco no educa adecuadamente a sus clientes en cuanto a precauciones de seguridad. Además, ante la ausencia de medidas adecuadas para verificar las transacciones los clientes pueden repudiar transacciones que previamente han autorizado, creando pérdidas financieras para el banco. Los clientes que utilizan información personal (por ejemplo, información sobre la autenticación, números de tarjetas de crédito, o números de cuentas bancarias) en una transmisión electrónica insegura podría permitir a los criminales acceder a las cuentas de clientes. Como consecuencia el banco podrá incurrir en pérdidas financieras debidas a transacciones no autorizadas por los clientes. Otra preocupación es el lavado de dinero como se señala en el informe de abril del Grupo de los Diez: *Electronic Money: Consumer Protection, Law Enforcement, Supervisory and Cross-Border Issues*.

## **2.2 Riesgo a la Reputación**

El riesgo a la reputación es el riesgo de una opinión pública negativa que resulta en una pérdida crítica de clientes. Este riesgo puede incluir acciones que crean una imagen pública negativa permanente de las operaciones generales del banco, de tal manera que el banco se ve imposibilitado de establecer y mantener relaciones con sus clientes. El riesgo de reputación puede también generarse cuando las acciones de un banco causan una pérdida de confianza importante por parte del público en la capacidad del banco de realizar funciones esenciales para la continuación de sus operaciones. El riesgo de reputación puede generarse como respuesta a las acciones del mismo

banco, o en respuesta a las acciones de terceras partes. El riesgo a la reputación puede aumentar a consecuencia de una mayor exposición al riesgo o problemas en otras categorías de riesgo, particularmente el riesgo operativo.

El riesgo a la reputación puede ser el resultado de una deficiencia no esperada de los sistemas o productos, causando una reacción pública negativa. Una violación seria de seguridad, ya sea como resultado de ataques externos o internos al sistema del banco, puede minar la confianza del público en el banco. El riesgo a la reputación también puede ser causado cuando los clientes tienen problemas con un servicio y no se les brinda la información adecuada acerca del uso del producto y procedimientos de solución.

Los errores, hechos delictivos y fraude de terceras partes pueden también exponer al banco a este tipo de riesgo. El riesgo a la reputación puede surgir de problemas en las redes de comunicación que impiden a los clientes el acceso a sus fondos, o información sobre las cuentas, particularmente si no existen alternativas a este acceso. Las pérdidas substanciales causadas por errores de otra institución que ofrece el mismo, o similar, producto o servicio de banca electrónica o dinero electrónico, pueden levantar sospechas de los clientes del banco en cuanto a sus productos o servicios, aunque el banco no enfrente los mismos problemas. El riesgo a la reputación puede también generarse con motivo de ataques dirigidos a un banco particular. Por ejemplo, la penetración del lugar en la red del banco con fines delictivos para alterarlo y diseminar intencionalmente información sobre el banco o sus productos.

El riesgo a la reputación puede no sólo ser significativo para un banco, sino para todo el sistema bancario. Si, por ejemplo, un banco mundialmente activo experimenta un daño importante a su reputación relacionado con sus negocios de banca electrónica o dinero electrónico, la seguridad de los sistemas de los demás bancos puede también ser cuestionada. En circunstancias extremas, una situación de esta naturaleza puede conducir a interrupciones sistémicas en la banca en general.

### **2.3 Riesgo Legal**

El riesgo legal surge de las violaciones o incumplimientos de las leyes, reglas, reglamentos o prácticas establecidas, o cuando los derechos y obligaciones legales de las partes de una transacción no están bien definidos. Dada la relativa novedad de las actividades de banca electrónica y dinero electrónico, los derechos y obligaciones de las partes de dichas transacciones son, en algunos casos, poco precisas. Por ejemplo, la aplicación de algunos reglamentos de protección del consumidor a la banca electrónica y las actividades de dinero electrónico pueden no ser claras en algunos países. Además, el riesgo legal puede resultar de la incertidumbre en cuanto a la validez de los acuerdos suscritos por medios electrónicos.

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

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

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

A medida que se expande el comercio electrónico, los bancos probablemente buscarán participar en sistemas de autenticación electrónica, como ser los que utilizan certificados digitales.<sup>7</sup> El rol de autoridad de certificación puede exponer al banco a un riesgo legal. Por ejemplo,

---

<sup>7</sup> El objetivo de un certificado digital emitido por una autoridad de certificación competente es garantizar que una firma digital

un banco que actúa como autoridad de certificación puede ser responsable de pérdidas financieras incurridas por las partes que confiaron en la certificación. Además, el riesgo legal puede presentarse si los bancos participan en sistemas nuevos de autenticación y no se especifican con claridad los derechos y obligaciones pertinentes.

## 2.4 Otros Riesgos

La banca electrónica y las actividades de dinero electrónico también presentan riesgos tradicionales, como ser el riesgo crediticio, el riesgo de liquidez, riesgo de la tasa de interés y riesgos de mercado. Sin embargo, las consecuencias prácticas de estos riesgos pueden ser diferentes a las de los riesgos operativos, de la reputación y legales. Esto es especialmente evidente en el caso de los bancos que tienen una variedad de actividades bancarias, comparados con aquellos bancos o sucursales que se especializan en actividades de banca electrónica y dinero electrónico.

*2.4.1 El riesgo crediticio* es el riesgo que una contraparte no cancele totalmente una obligación de pago, ya sea en el momento de su vencimiento o en cualquier momento de ahí en adelante. Los bancos que se dedican a actividades de banca electrónica pueden dar créditos por vías no tradicionales y ampliar su mercado más allá de los límites geográficos tradicionales. Las deficiencias en los procedimientos utilizados para determinar la solvencia de los prestatarios que solicitan crédito a distancia, pueden intensificar el riesgo crediticio de los bancos. Los bancos que ofrecen programas de pago electrónico de facturas pueden enfrentarse a riesgos crediticios si un intermediario externo no cumple con sus obligaciones con respecto al pago. Los bancos que compran dinero electrónico de un emisor para revenderlo a sus clientes, también se exponen a un riesgo crediticio, en el caso que un emisor no cumpla con sus obligaciones para recuperar el dinero electrónico.

---

dada es efectivamente generada por un firmante dado. El banco que decide actuar como autoridad de certificación puede ser considerado como suministrador de servicios a clientes, similares a los asociados con la provisión de un dispositivo de acceso a cuentas, o como notario público. La firma digital es una serie de datos anexados a un mensaje electrónico, cuyo propósito es identificar exclusivamente el remitente al destinatario. En la actualidad, la mayoría de las firmas digitales se generan utilizando un algoritmo criptográfico, en el que el remitente utiliza una función matemática para crear la firma y el destinatario utiliza una función matemática diferente, pero asociada a la primera, para verificar la firma. Normalmente las firmas digitales proveen además un mecanismo para verificar la integridad del mensaje.

*2.4.2 Riesgo de liquidez* es el riesgo que resulta de la incapacidad del banco de cumplir con sus obligaciones en el momento de su vencimiento, sin incurrir en pérdidas inaceptables, aún cuando el banco pueda, en última instancia, cumplir con dichas obligaciones. El riesgo de liquidez puede ser significativo para los bancos que se especializan en actividades de dinero electrónico, cuando dichos bancos son incapaces de asegurar que los fondos son suficientes para cubrir las exigencias de recuperación y liquidación en un momento dado. Además, el hecho de no cumplir en forma oportuna con las exigencias de liquidación puede tener como consecuencia una acción legal contra la institución y un daño a su reputación.

*2.4.3 Riesgo de tasa de interés* se refiere a la exposición de la situación financiera del banco a los movimientos adversos de las tasas de interés. Los bancos que se especializan en la provisión de dinero electrónico pueden enfrentar un riesgo de tasa de interés considerable, en la medida en que los movimientos adversos de las tasas de interés disminuyan el valor de los activos en relación a los pasivos pendientes de dinero electrónico.

*2.4.4. Riesgos de mercado* es el riesgo de pérdidas en las posiciones en y fuera del balance debidas a cambios en los precios de mercado, incluyendo tasas de cambio de divisas. Los bancos que aceptan monedas extranjeras, como pago de dinero electrónico, están sujetos a este tipo de riesgo.

*2.4.5. Asuntos transterritoriales.*

Las actividades de la banca electrónica y de dinero electrónico se basan en una tecnología que, por naturaleza, está diseñada para extender el alcance geográfico de los bancos y sus clientes. Esta expansión del mercado puede ir más allá de las fronteras nacionales, y, por lo tanto, puede aumentar ciertos riesgos. Si bien los bancos se enfrentan actualmente a riesgos similares en la banca internacional, es importante notar que estos riesgos están también relacionados con el comportamiento transterritorial de la banca electrónica y dinero electrónico. Los bancos pueden enfrentarse a exigencias legales y de reglamentación diferentes, al tratar con clientes transnacionales.

Para las nuevas formas de banca electrónica para consumidores, como ser las actividades bancarias en el Internet, y para el dinero electrónico, pueden existir incertidumbres con respecto a las exigencias legales de algunos países. Además, puede haber una ambigüedad en cuanto a jurisdicciones de las diferentes autoridades nacionales. Estos aspectos pueden exponer a los bancos a un riesgo legal asociado con el incumplimiento con diferentes leyes y reglamentos nacionales, incluyendo las leyes de protección del consumidor, exigencias de mantención de registros y presentación de informes, reglas de confidencialidad y leyes relacionadas con el lavado de dinero.

Los bancos que tratan con un suministrador de servicios ubicado en otro país pueden enfrentarse con un riesgo operativo que, por la misma razón, es más difícil de controlar. Los bancos pueden enfrentarse con otros riesgos a medida que se involucran en el suministro de servicios de banca electrónica y dinero electrónico en otros países. Los bancos que tratan con suministradores de servicios instalados en otros países, o con participantes extranjeros en actividades de banca electrónica y dinero electrónico, están sujetos al riesgo de país en la medida en que las partes extranjeras no pueden cumplir con sus obligaciones debido a factores económicos, sociales o políticos. Un banco que ofrece servicios por redes abiertas, como el Internet, puede estar expuesto a un riesgo crediticio, ya que la solicitud de crédito de clientes en otros países puede ser más difícil de evaluar con procedimientos diseñados para una clientela más conocida. Los bancos que aceptan divisas extranjeras como pago de dinero electrónico pueden estar sujetos a riesgo de mercado debido a los movimientos de las tasas de cambio de divisas.

### **3. Gestión de Riesgos**

Para un número cada vez mayor de bancos, existe una razón estratégica para involucrarse en actividades de banca electrónica y dinero electrónico. Además, un mayor uso de la banca electrónica y dinero electrónico puede incrementar la eficiencia del sistema bancario y de pagos, beneficiando a clientes y comerciantes. Al mismo tiempo, y como se mencionó anteriormente, existen riesgos para los bancos que se dedican a actividades de banca electrónica y dinero electrónico. Estos riesgos deben compararse con los beneficios y los bancos deben ser capaces de manejar y controlar los riesgos y absorber toda pérdida asociada, si fuese necesario. Los riesgos que presenta la banca electrónica y el dinero electrónico deben ser evaluados en el contexto de los otros

riesgos que enfrenta el banco. Si bien las actividades de banca electrónica y dinero electrónico pueden representar una parte relativamente pequeña de las actividades totales de los bancos, los supervisores pueden aún así exigir a la administración superior la seguridad que los sistemas esenciales no se ven amenazados por los riesgos que toma el banco.

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

Es de suma importancia que los bancos pongan en práctica un proceso general de gestión de riesgos, vigilado por el directorio y la administración superior. A medida que se identifican y evalúan nuevos riesgos en la banca electrónica y dinero electrónico, se debe mantener informados al directorio y a la administración superior de estos cambios. Antes de comenzar toda actividad nueva, se debe realizar un análisis amplio para que la administración superior pueda asegurarse que el proceso de gestión de riesgos es adecuado para evaluar, controlar y seguir todo riesgo generado por la nueva actividad propuesta.

### **3.1 Evaluación de los Riesgos**

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

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

El segundo paso en la evaluación de riesgos es la determinación por parte del directorio y de la administración superior de la tolerancia al riesgo del banco, basado en la evaluación de las pérdidas que el banco podría sostener en el evento de la materialización de un problema dado. Finalmente, la administración puede comparar su tolerancia al riesgo con su evaluación de la magnitud del riesgo para confirmar si la exposición al riesgo se adapta a los límites de tolerancia.

### **3.2 Manejo y Control de los Riesgos**

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

#### **3.2.1 Medidas y Políticas de Seguridad**

La seguridad es la combinación de sistemas, aplicaciones y controles internos utilizados para salvaguardar la integridad, autenticidad y confidencialidad del procesamiento de datos y de los procesos de operación. Una seguridad adecuada depende de la formulación y ejecución de políticas acertadas y medidas de seguridad para los procesos del banco y para la comunicación entre el banco y las partes externas. Las políticas y medidas de seguridad pueden limitar el riesgo de ataques

externos e internos a los sistemas de banca electrónica y dinero electrónico, así como también el riesgo a la reputación generado por las violaciones de seguridad.

La *política de seguridad* refleja la voluntad de la administración para apoyar la información sobre seguridad y proporciona una explicación de la organización de seguridad del banco. Además, esta política establece principios directivos que definen la tolerancia al riesgo de seguridad del banco. Puede también definir las responsabilidades del diseño, ejecución y aplicación de medidas de información sobre seguridad, así como establecer procedimientos para evaluar el cumplimiento con las políticas, aplicar medidas de disciplina e informar sobre violaciones de seguridad.

Las *medidas de seguridad* son una combinación de herramientas de hardware y software, y administración de personal, que contribuyen a la elaboración de sistemas y operaciones seguras. La administración superior debe analizar la seguridad como un proceso amplio que es tan fuerte como la parte más débil del proceso. Los bancos pueden escoger de una variedad de medidas de seguridad para prevenir o mitigar los ataques internos o externos para el mal uso de la banca electrónica. Estas medidas, incluyen, criptogramas, claves, *firewalls*, controles de virus, y pre-selección de empleados. Para los criptogramas se utilizan algoritmos criptográficos para codificar datos claros de textos en textos cifrados para evitar observaciones no autorizadas.<sup>8</sup> Las palabras claves, frases claves, números de identificación personal, fichas basadas en el "hardware", y la biometría son técnicas que se usan para controlar el acceso e identificar a los usuarios.

Los *firewalls* son combinaciones de "hardware" y "software" que seleccionan y limitan el acceso externo a los sistemas internos conectados a redes abiertas como el Internet. Los *firewalls* pueden también separar segmentos de las redes internas utilizando tecnología de Internet (*Intranets*). La tecnología de los *firewalls*, cuando es diseñada y ejecutada en forma correcta, puede ser un medio efectivo para controlar el acceso y salvaguardar la confidencialidad e integridad de la información. Dado que esta tecnología es de diseño complejo y costoso, sus puntos fuertes y capacidades deben ser proporcionales a la sensibilidad de la información a ser protegida. Un diseño bien planificado debería incluir requisitos de seguridad para toda la empresa, procedimientos de

---

<sup>8</sup> Ver *Security of Electronic Money*, Bank for International Settlements, agosto de 1996, especialmente la sección 4.1.2. sobre criptografía para más detalles.

operación claros, separación de funciones, y selección de personal confiable responsable de la configuración y operación del *firewall*.

Si bien los *firewalls* seleccionan los mensajes que son recibidos, no necesariamente protegen contra los programas con virus que son recuperados del Internet. Consecuentemente, la administración debe elaborar controles de prevención y detección para reducir las probabilidades de un ataque de virus y la destrucción de datos, particularmente en el caso de la banca a distancia. Los programas normalmente utilizados para mitigar el riesgo de una infección por virus pueden incluir controles de red, políticas para el usuario final, entrenamiento de los usuarios y programas para la detección de virus.

No todas las amenazas a la seguridad provienen del exterior. Los sistemas de banca electrónica y dinero electrónico deben también ser protegidos, hasta donde sea posible, contra las autoridades no autorizadas de los empleados actuales y anteriores. Como es el caso con las actividades tradicionales de la banca, la verificación de los antecedentes de nuevos empleados, empleados temporales y consultores, así como los controles internos y la separación de funciones son precauciones importantes para la protección del sistema.

En el caso del dinero electrónico, existen medidas de seguridad adicionales que pueden ayudar a evitar los ataques y el mal uso, incluyendo la falsificación y el lavado de dinero.<sup>9</sup> Estas medidas podrían incluir una comunicación interactiva con el usuario o con un operador central; el seguimiento de las transacciones individuales; el mantenimiento de registros acumulables en una central de datos; el uso de dispositivos a prueba de alteraciones incorporados en las tarjetas de valor almacenado y en el "hardware" comercial; y el uso de límites de valor y fechas de vencimiento en las tarjetas de valor almacenado.

### **3.2.2 Comunicaciones Internas**

---

<sup>9</sup> El informe *Security of Electronic Money, Bank for International Settlements*, abril de 1996, detalla las medidas de seguridad aplicables al dinero electrónico. Este informe concluye que es preferible una combinación de medidas de seguridad, a una medida única para prevenir los problemas de seguridad del dinero electrónico.

La gestión de los riesgos operativos, a la reputación, legales y otros se facilita cuando la administración superior comunica al personal pertinente la forma en que la provisión de banca electrónica y dinero electrónico pretende apoyar los objetivos generales del banco. Al mismo tiempo, el personal técnico debe comunicar a la administración superior cómo funcionan los sistemas, así como los puntos fuertes y las debilidades de los mismos. Estos procedimientos pueden disminuir los riesgos operativos del diseño deficiente de sistemas, incluyendo la incompatibilidad de diferentes sistemas dentro de una organización bancaria; problemas de integridad de la información; riesgo a la reputación asociado con la insatisfacción de los clientes; y riesgos crediticios y de liquidez.

Para asegurar una comunicación interna adecuada, todas las políticas y procedimientos deberían ser dados por escrito. Además, la administración superior debería poner en práctica, como política general, la educación y actualización constante del personal de acuerdo con el ritmo de la innovación tecnológica. Estas actividades de capacitación podrían incluir cursos técnicos en el trabajo, así como tiempo para que el personal se mantenga informado sobre los acontecimientos importantes del mercado.

### **3.2.3 Evaluación y Perfeccionamiento**

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

### **3.2.4 Contratación de Servicios fuera de la Empresa**

Existe una tendencia cada vez mayor de concentrarse estratégicamente en las actividades principales y confiar a terceros las actividades que no entran en las competencias del banco. Si bien

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

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

### **3.2.5 Divulgaciones y Educación al Cliente**

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

### **3.2.6 Planificación de Contingencias**

Un banco puede limitar el riesgo de interrupciones de los procesos internos o en la entrega de servicios o productos, elaborando planes de contingencia donde se establece el curso de las acciones en caso de una interrupción del suministro de servicios de banca electrónica y dinero electrónico. Este plan puede incluir la recuperación de datos, formas alternativas de procesamiento de datos, personal de emergencia y apoyo al servicio al cliente. Los sistemas de respaldo deben ser verificados periódicamente para comprobar su eficiencia. Los bancos deben garantizar que sus operaciones de contingencia son tan seguras como sus operaciones normales.

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

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

### **3.3 Riesgos de Seguimiento**

Un seguimiento constante es un aspecto importante en todo proceso de gestión de riesgos. En el caso de la banca electrónica y del dinero electrónico el seguimiento es particularmente

importante, ya que la naturaleza de estas actividades puede cambiar rápidamente a medida que se producen innovaciones y debido a la dependencia de ciertos productos del uso de redes abiertas, como el Internet. Dos elementos importantes del seguimiento son la verificación y la auditoría de los sistemas.

### **3.3.1 Verificación y Vigilancia de los Sistemas**

La verificación de la operación de los sistemas puede ayudar a detectar actividades inusuales y advertir problemas, interrupciones y ataques importantes al sistema. Las pruebas de penetración se dirigen a la identificación, aislamiento y confirmación de fallas en el diseño y ejecución de los mecanismos de seguridad mediante intentos controlados de penetrar el sistema fuera de los procedimientos normales. La vigilancia es una forma de seguimiento para la cual se utilizan aplicaciones de "software" y auditoría para controlar la actividad. Contrariamente a las pruebas de penetración la vigilancia se concentra en el seguimiento de operaciones de rutina, la investigación de anomalías y la formulación de criterios relacionados con la eficiencia de la seguridad, verificando el cumplimiento con las políticas de seguridad.

### **3.3.2 Auditorías**

Las auditorías (internas y externas) brindan un mecanismo de control independiente para detectar deficiencias y reducir, a un mínimo, los riesgos que comporta el suministro de servicios de banca electrónica y dinero electrónico. El rol de un auditor es velar por la elaboración de normas, políticas y procedimientos apropiados, y confirmar el compromiso del banco con los mismos. El personal de auditoría debe tener la experiencia necesaria para llevar a cabo un análisis preciso. El auditor interno debe ser independiente de los empleados que intervienen en la toma de decisiones relacionadas con la gestión de riesgos. Para completar la auditoría interna, la administración puede hacer uso de auditores externos calificados, como ser, consultores en seguridad u otros profesionales, para obtener una evaluación independiente de las actividades de banca electrónica o dinero electrónico.

### **3.4 Gestión de Riesgos Transterritoriales**

Los riesgos transterritoriales pueden ser más complejos que los riesgos a los que se enfrenta un banco en su país de origen. Por lo tanto, los bancos y los supervisores tendrán que dedicar tiempo a la evaluación, control y seguimiento de los riesgos a la reputación, legal y otros generados por las actividades de banca electrónica y dinero electrónico transterritoriales.

Los bancos que proveen servicios a sus clientes en varios mercados nacionales, deberán comprender las diferentes exigencias legales y apreciar las diferencias nacionales en las expectativas de los clientes y conocimiento de los productos y servicios. Además, la administración superior debe asegurarse que los sistemas de otorgamiento de créditos y administración de liquidez, toman en cuenta las dificultades potenciales de las actividades transterritoriales. El banco tendrá que evaluar el riesgo país y elaborar planes de contingencia que tomen en cuenta las interrupciones de servicio causadas por problemas políticos y económicos en el exterior. El banco puede además enfrentarse a dificultades relacionadas con el cumplimiento de las obligaciones por el suministrador de servicios extranjero. En el caso de bancos que dependen de suministradores de servicios ubicados en el exterior, los supervisores nacionales deberán evaluar la facilidad de acceso a la información de los suministradores de servicios transnacionales, así como las actividades de los mismos, caso por caso.

Los supervisores nacionales pueden tener un rol importante en la gestión de estos riesgos identificando y deliberando sobre las ambigüedades de jurisdicción. Además, pueden continuar sus esfuerzos de elaboración de medidas para la detección de prácticas inseguras e ilegales. Finalmente los supervisores nacionales pueden continuar y fortalecer los esfuerzos conjuntos para compartir información sobre innovaciones de productos y servicios y prácticas de la industria.

## **ANEXO**

### **Ejemplos de Posibles Riesgos y Medidas para**

## **la Gestión de Riesgos en la Banca Electrónica y Dinero Electrónico para Consumidores**

La matriz presentada a continuación da ejemplos de los posibles riesgos para los bancos que se dediquen a actividades de banca electrónica y dinero electrónico, e indica las posibles medidas a ser utilizadas para manejar dichos riesgos. Esta lista es representativa más que exhaustiva. Las posibles medidas de gestión de riesgos no deben ser interpretadas como el reflejo de una política nacional o internacional de supervisión.

*Traducción de la Superintendencia de Bancos y Entidades Financieras de Bolivia.*