

Comité de Basilea de Supervisión Bancaria

**Prácticas Sanas para la Administración y
Supervisión del Riesgo Operativo**

Febrero de 2003

Banco de Pagos Internacionales

**Grupo de Administración de Riesgos
del Comité de Basilea de Supervisión Bancaria**

Presidente:

Sr. Roger Cole – Federal Reserve Board, Washington, DC

Banque Nationale de Belgique, Bruselas	Sra. Dominique Gressens
Commission Bancaire et Financière, Bruselas	Sr. Jos Meuleman
Office of the Superintendent of Financial Institutions, Ottawa	Sr. Jeff Miller
Commission Bancaire, Paris	Sr. Laurent Le Mouël
Deutsche Bundesbank, Frankfurt am Main	Sra. Magdalene Heid Sra. Karin Sagner-Kaiser
Bundesanstalt für Finanzdienstleistungsaufsicht, Bonn	Sra. Kirsten Straus
Banca d'Italia, Roma	Sr. Claudio Dauria Sr. Fabrizio Leandri Sr. Sergio Sorrentino
Bank of Japan, Tokio	Sr. Satoshi Yamaguchi
Financial Services Agency, Tokio	Sr. Hirokazu Matsushima
Commission de Surveillance du Secteur Financier, Luxemburgo	Sr. Davy Reinard
De Nederlandsche Bank, Ámsterdam	Sr. Klaas Knot
Banco de España, Madrid	Sr. Guillermo Rodríguez-García Sr. Juan Serrano
Finansinspektionen, Estocolmo	Sr. Jan Hedquist
Sveriges Riksbank, Estocolmo	Sr. Thomas Flodén
Eidgenössische Bankenkommision, Berna	Sr. Martin Sprenger
Financial Services Authority, Londres	Sr. Helmut Bauer Sr. Victor Dowd
Federal Deposit Insurance Corporation, Washington DC	Sr. Mark Schmidt
Federal Reserve Bank of New York	Sra. Beverly Hirtle Sr. Stefan Walter

Federal Reserve Board, Washington DC

Sr. Kirk Odegard

Office of the Comptroller of the Currency,
Washington DC

Sr. Kevin Bailey
Sra. Tanya Smith

European Central Bank, Frankfurt am Main

Sr. Panagiotis Strouzas

European Commission, Bruselas

Sr. Michel Martino
Sra. Melania Savino

Secretariado del Comité de Basilea de
Supervisión de Bancos, Banco Internacional de
Compensación

Sr. Stephen Senior

Índice

Introducción

Antecedentes

Tendencias y Prácticas en el Sector

Prácticas Sanas

Desarrollo de un Entorno Adecuado de Administración de Riesgos

Administración de Riesgos: Identificación, Evaluación, Monitoreo y Mitigación / Control

Papel de los Supervisores

Papel de la Divulgación

Prácticas Sanas para la Administración y Supervisión del Riesgo Operativo

Introducción

1. Este documento detalla un conjunto de principios que suministran un marco para la efectiva administración y supervisión del riesgo operativo. Los bancos y autoridades de supervisión pueden utilizar ese marco en la evaluación de las políticas y prácticas de administración del riesgo operativo.

2. El Comité de Basilea de Supervisión de Bancos (el Comité) reconoce que el enfoque exacto para la administración del riesgo operativo escogido por un banco individual dependerá de una serie de factores, incluyendo el tamaño, nivel de sofisticación, y la índole y complejidad de las actividades del banco. No obstante, a pesar de estas diferencias, los siguientes elementos son de suma importancia para un marco de administración del riesgo operativo para todos los bancos, independientemente de su tamaño y alcance de actividades: estrategias claras y supervisión por el directorio y la alta gerencia, una fuerte cultura del riesgo operativo¹ y una cultura interna de control (incluyendo, entre otras cosas, claras líneas de responsabilidad y segregación de obligaciones, un sistema interno efectivo de presentación de informes, y planes de contingencia). Por lo tanto, el Comité cree que los principios especificados en este documento establecen prácticas sanas que son relevantes para todos los bancos. El anterior documento del Comité *Un Marco para Sistemas de Control Interno en Organizaciones Bancarias* (septiembre de 1998) sostiene su trabajo actual en el área del riesgo operativo.

Antecedentes

3. La desregulación y globalización de los servicios financieros, junto con la creciente sofisticación de la tecnología financiera, están incrementando la complejidad de las actividades de los bancos y por ende, de sus perfiles de riesgo (es decir, el nivel de riesgo entre las actividades y/o categorías de riesgo de la empresa). La elaboración de buenas prácticas para la banca sugiere que a menudo los otros riesgos, que no sean el riesgo de crédito, de la tasa de interés y de mercado, pueden ser significativos. Algunos ejemplos de estos nuevos riesgos crecientes para los bancos son:

- De no ser sujeto a un control adecuado, el mayor uso de tecnologías más automatizadas tiene el potencial de transformar los riesgos relativos a errores en el procesamiento manual en riesgos relativos a fallas del sistema, ya que cada vez más el trabajo se basa en sistemas integrados a nivel mundial;

¹ La *cultura interna del riesgo operativo* significa un conjunto combinado de valores, actitudes, habilidades y conductas individuales y corporativos que determinan el estilo y compromiso de una empresa respecto de la administración del riesgo operativo.

- El crecimiento del e-comercio implica potenciales riesgos (p.ej. fraude interno y externo y problemas relacionados con la seguridad del sistema) que todavía no son totalmente claros;
- Adquisiciones, fusiones, procesos de disolución de fusiones y consolidaciones a gran escala ponen a prueba la viabilidad de sistemas recientemente integrados o nuevos;
- La emergencia de bancos que actúan como proveedores de servicios de gran volumen crea la necesidad de tener un mantenimiento continuo de los controles internos y sistemas de apoyo de calidad superior;
- Los bancos pueden adoptar técnicas de mitigación de riesgos (p.ej. garantías, derivados crediticios, acuerdos de compensación de créditos internos, y reconversión de activos en valores) para optimizar sus niveles de exposición al riesgo de mercado y riesgo de crédito, pero que a su vez pueden generar otras formas de riesgo (p.ej. el riesgo legal); y
- El uso creciente de acuerdos de subcontratación y la participación en sistemas de compensación y liquidación puede mitigar algunos riesgos, pero también puede generar otros riesgos significativos para los bancos.

4. Los diferentes tipos de riesgos indicados arriba pueden ser agrupados bajo el título ‘riesgo operativo’, que fue definido por el Comité como ‘el riesgo de pérdida como resultado de personas, sistemas y procesos internos fracasados o inadecuados o de eventos externos’.² La definición incluye el riesgo legal, pero excluye el riesgo estratégico y el riesgo de reputación.

5. El Comité reconoce que ‘riesgo operativo’ es un término que tiene una variedad de significados en el sector bancario, y por lo tanto, para fines internos (incluyendo en la aplicación del documento sobre Prácticas Sanas), los bancos pueden optar por adoptar sus propias definiciones del riesgo operativo. Sea cual sea la definición exacta, es crítico que los bancos entiendan claramente qué significa el riesgo operativo para una efectiva administración y control de esta categoría de riesgo. También es importante que la definición contemple todos los riesgos operativos relevantes con que se ve enfrentado el banco y que capte las causas más importantes de serias pérdidas operativas. El Comité – en coordinación con el sector – identificó los siguientes tipos de eventos relativos al riesgo operativo como los eventos que pudieran resultar en pérdidas sustanciales:

² Se adoptó esta definición del sector como parte del trabajo del Comité de desarrollar un cargo mínimo de capital regulatorio por el riesgo operativo. A pesar de que este documento no es una parte formal del marco de capital, de todas maneras el Comité espera que los elementos básicos de un marco sano de administración del riesgo operativo definidos en este documento serán útiles para los supervisores cuando están revisando el coeficiente patrimonial del banco, por ejemplo durante el proceso de revisión por el supervisor.

- Fraude interno. Por ejemplo, la presentación a propósito de informes falsos sobre posiciones, robo por empleados, y transacciones internas de un empleado por cuenta propia.
- Fraude externo. Por ejemplo, robo, falsificación, alteración de cheques, y daños causados por *hackers*.
- Prácticas laborales y seguridad en el lugar de trabajo. Por ejemplo, demandas de indemnización de los trabajadores, violación de reglas de salud y seguridad de los empleados, actividades laborales organizadas, demandas por discriminación, y responsabilidad general.
- Clientes, productos y prácticas comerciales. Por ejemplo, infracciones fiduciarias, abuso de información confidencial sobre clientes, transacciones indebidas por cuenta del banco, lavado de dinero, y la venta de productos no autorizados.
- Daños a activos físicos. Por ejemplo, terrorismo, vandalismo, terremotos, incendios e inundaciones.
- Interrupción de las actividades y problemas del sistema. Por ejemplo, deficiencias en el software y hardware, problema de telecomunicación, y cortes de los servicios públicos.
- Administración de procesos, ejecución y entrega. Por ejemplo, errores al ingresar datos, falencias en la administración de garantías prendarias, documentación legal incompleta, acceso no aprobado a cuentas de clientes, mala actuación con personas que no sean clientes, y disputas con vendedores.

Tendencias y Prácticas en el Sector

6. En su trabajo sobre la supervisión de riesgos operativos, el Comité ha tratado de desarrollar una mayor comprensión de las tendencias y prácticas actuales en la industria para administrar el riesgo operativo. Estos esfuerzos implicaron una gran cantidad de reuniones con organizaciones bancarias, estudios sobre prácticas en el sector, y análisis de los resultados. En base a estos esfuerzos, el Comité cree que tiene una buena idea de las prácticas actuales en el sector bancario, al igual que de los esfuerzos en el sector para desarrollar métodos de administración del riesgo operativo.

7. El Comité reconoce que la administración de riesgos operativos específicos no es una práctica nueva; siempre ha sido importante para los bancos intentar evitar fraude, mantener la integridad de los controles internos, reducir los errores en el procesamiento de transacciones, etcétera. Empero, lo que sí es relativamente nuevo es la perspectiva respecto de la administración del riesgo operativo como una práctica integral comparable a la administración del riesgo de crédito y de mercado, no tanto en forma, sino en principio. Las tendencias mencionadas en la introducción de este documento, en combinación con un número creciente de eventos de pérdida operativa de alto perfil en el mundo entero, han dado lugar a que los bancos y supervisores cada vez más ven la administración del riesgo operativo como una disciplina completa, tal como ya ha ocurrido en muchos otros sectores.

8. En el pasado, los bancos se basaron casi exclusivamente en mecanismos de control interno en las líneas de actividad, complementados con la función de auditoría, para administrar el riesgo operativo. A pesar de que estos mecanismos siguen siendo

importantes, recientemente han empezado a emerger estructuras y procesos específicos para administrar el riesgo operativo. En este sentido, un número creciente de organizaciones ha llegado a la conclusión que un programa de administración del riesgo operativo otorga seguridad y solvencia al banco, y por ende, están avanzando en el tratamiento del riesgo operativo como un tipo distinto de riesgo similar al tratamiento del riesgo de crédito y el riesgo de mercado. El Comité cree que es esencial tener un activo intercambio de ideas entre los supervisores y el sector para el desarrollo constante de pautas adecuadas para administrar el riesgo operativo.

9. Este documento está estructurado de la siguiente manera: el desarrollo de un entorno adecuado de administración de riesgo; administración de riesgo: identificación, evaluación, monitoreo y control / mitigación; el papel de los supervisores, y el papel de la divulgación.

Prácticas Sanas

10. Al desarrollar estas prácticas sanas, el Comité se ha basado en su trabajo existente sobre la administración de otros riesgos bancarios significativos, como ser el riesgo de crédito, el riesgo de la tasa de interés y el riesgo de liquidez, y el Comité cree que la administración del riesgo operativo se debe tratar con un nivel similar de rigor. Sin embargo, queda claro que el riesgo operativo es diferente de otros riesgos bancarios, ya que, típicamente, no es un riesgo que se toma a cambio de una recompensa esperada, sino que existe en el curso normal de la actividad empresarial, y que esto afecta el proceso de administración de riesgo.³ Al mismo tiempo, la falta de una adecuada administración del riesgo operativo puede resultar en información errónea sobre el perfil de riesgo de una institución, exponiendo la institución a pérdidas significativas. Para reflejar la índole diferente del riesgo operativo, para los fines de este documento, 'administración' del riesgo operativo se interpreta como la 'identificación, evaluación, monitoreo, y control / mitigación' del riesgo. Esta definición es diferente de la definición que el Comité usó en anteriores documentos sobre la administración de riesgo que habla de 'identificación, medición, monitoreo y control' del riesgo. Al igual que su trabajo sobre otros riesgos bancarios, el Comité ha estructurado este documento sobre prácticas sanas en torno a los siguientes principios:

Desarrollo de un Entorno Adecuado de Administración de Riesgos

³ Sin embargo, el Comité reconoce que en algunas líneas de actividad con un riesgo de crédito o de mercado mínimo (p.ej., administración de activos, y pago y liquidación), la decisión de exponerse al riesgo operativo o de competir en base a la capacidad de administrar y fijar un precio para este riesgo, es una parte integral del cálculo de riesgo / recompensa del banco.

Principio 1: El directorio⁴ debería estar consciente de los principales aspectos de los riesgos operativos del banco como una categoría diferente de riesgo a ser administrado, y debería aprobar y revisar periódicamente el marco de administración del riesgo operativo del banco. El marco debería proporcionar una definición a lo largo de la empresa del riesgo operativo y especificar los principios para la identificación, evaluación, monitoreo y control / mitigación del riesgo operativo.

Principio 2: El directorio debería asegurar que el marco de administración del riesgo operativo del banco sea sujeto a una auditoría interna efectiva e integral por personal competente, independiente desde el punto de vista operativo y con una adecuada capacitación. La función de auditoría interna no debería tener la responsabilidad directa por la administración del riesgo operativo.

Principio 3: La alta gerencia debe ser responsable por la implementación del marco de administración del riesgo operativo aprobado por el directorio. El marco se debe implementar de forma coherente a lo largo de toda la organización bancaria, y todos los niveles del personal deberían entender sus responsabilidades respecto de la administración del riesgo operativo. La alta gerencia también debería ser responsable por el desarrollo de políticas, procesos y procedimientos para administrar el riesgo operativo en todos los productos, actividades, procesos y sistemas más importantes del banco.

Administración de Riesgos: Identificación, Evaluación, Monitoreo y Mitigación / Control

Principio 4: Los bancos deberían identificar y evaluar el riesgo operativo inherente en todos los productos, actividades, procesos y sistemas importantes. Los bancos también deberían asegurar que, antes de introducir o emprender productos, actividades, procesos y sistemas nuevos, el riesgo operativo inherente en los mismos sea sujeto a procedimientos adecuados de evaluación.

Principio 5: Los bancos deberían implementar un proceso para monitorear regularmente los perfiles del riesgo operativo y las exposiciones importantes a pérdidas. La información pertinente se debería presentar regularmente a la alta gerencia y el directorio que apoya la administración proactiva del riesgo operativo.

⁴ Este documento se refiere a una estructura directiva compuesta por un directorio y alta gerencia. El Comité está consciente que hay diferencias significativas en los marcos legislativos y regulatorios entre los diferentes países en relación con las funciones del directorio y la alta gerencia. En algunos países, el directorio tiene la principal, pero no exclusiva, función de supervisar el ente ejecutivo (la alta gerencia, la gerencia general) para verificar el cumplimiento con sus tareas. Por este motivo, en algunos casos, se conoce como el directorio supervisor. Esto significa que el directorio no tiene funciones ejecutivas. En otros países, el directorio tiene una responsabilidad más amplia ya que define el marco general para la gerencia del banco. Debido a estas diferencias, los términos ‘directorio’ y ‘alta gerencia’ tal como se emplean en este documento no se utilizan para identificar construcciones legales sino para identificar dos funciones de toma de decisiones en un banco.

Principio 6: Los bancos deberían tener políticas, procesos y procedimientos para controlar y/o mitigar riesgos operativos importantes. Los bancos deberían hacer una revisión periódica de sus estrategias de limitación y control de riesgos y deberían ajustar su perfil de riesgo operativo de acuerdo con ello utilizando estrategias apropiadas, a la luz de su perfil y apetito general de riesgo.

Principio 7: Los bancos deben tener planes de contingencia y de continuación de las actividades para asegurar su capacidad de operar de forma constante y limitar sus pérdidas en caso de una seria interrupción de las actividades.

Papel de los Supervisores

Principio 8: Los supervisores bancarios deberían exigir que todos los bancos, independientemente de su tamaño, tengan un marco efectivo para identificar, evaluar, monitorear y controlar / mitigar riesgos operativos importantes como parte de un enfoque general para la administración de riesgos.

Principio 9: Los supervisores deberían llevar a cabo, directa o indirectamente, evaluaciones independientes regulares de las políticas, procedimientos y prácticas de un banco respecto de los riesgos operativos. Los supervisores deberían asegurar que haya mecanismos adecuados que les permiten estar al tanto de evoluciones en los bancos.

Papel de la Divulgación

Principio 10: Los bancos deben divulgar suficiente información al público para que los participantes en el mercado puedan evaluar su enfoque para la administración del riesgo operativo.

Desarrollo de un Entorno Adecuado de Administración de Riesgos

11. Si no se entiende y administra el riesgo operativo, que está presente en prácticamente todas las transacciones y actividades del banco, puede incrementar considerablemente la probabilidad de que algunos riesgos no se reconocen y por ende no se controlan. Tanto el directorio como la alta gerencia son responsables por la creación de una cultura organizacional que da máxima prioridad a una efectiva administración del riesgo operativo y el cumplimiento de controles operativos sanos. La administración del riesgo operativo es más efectiva si la cultura de un banco enfatiza altos estándares de conducta ética en todos los niveles del banco. El directorio y la alta gerencia deberían promover una cultura organizativa que determina - a través de acciones y palabras - las expectativas de integridad para todos los empleados al efectuar las actividades del banco.

Principio 1: El directorio debería estar consciente de los principales aspectos de los riesgos operativos del banco como una categoría diferente de riesgo a ser administrado, y debería aprobar y revisar periódicamente el marco de administración del riesgo operativo del banco. El marco debería proporcionar una definición a lo largo de la empresa del riesgo operativo y especificar los principios para la identificación, evaluación, monitoreo y control / mitigación del riesgo operativo.

12. El directorio debe aprobar la implementación de un marco a lo largo de la empresa para la administración explícita del riesgo operativo como un riesgo diferente que pone en peligro la seguridad y solvencia del banco. El directorio debería suministrar pautas y directrices claras a la alta gerencia respecto de los principios subyacentes del marco y aprobar las políticas correspondientes desarrolladas por la alta gerencia.

13. Un marco de riesgo operativo debería basarse en una definición adecuada del riesgo operativo que articula claramente qué es lo que constituye riesgo operativo en ese banco. El marco debería cubrir el apetito y tolerancia del banco respecto del riesgo operativo, de acuerdo con lo especificado en las políticas para administrar ese riesgo y la priorización por el banco de actividades en torno a la administración del riesgo operativo, incluyendo la medida en que y la forma en que, el riesgo operativo se transfiere afuera del banco. También debería incluir políticas que definen el enfoque del banco para identificar, evaluar, monitorear y controlar / mitigar el riesgo. El grado de formalidad y sofisticación del marco de administración del riesgo operativo del banco debería ser coherente con el perfil de riesgo del banco.

14. El directorio es responsable por la creación de una estructura gerencial capaz de implementar el marco de administración del riesgo operativo de la empresa. Ya que un aspecto importante de la administración del riesgo operativo está relacionado con el establecimiento de controles internos fuertes, es especialmente importante que el directorio defina líneas claras de responsabilidad gerencial y para la presentación de informes. Además, debería haber una separación de responsabilidades y líneas para la presentación de informes entre las funciones de control del riesgo operativo, líneas de negocios y funciones de apoyo a fin de evitar conflictos de interés. El marco también debería articular los procesos clave que se necesitan en la empresa para administrar el riesgo operativo.

15. El directorio debería revisar regularmente el marco para garantizar que el banco esté administrando los riesgos operativos resultantes de cambios en el mercado externo y otros factores del entorno, al igual que los riesgos operativos asociados con productos, actividades o sistemas nuevos. Este proceso de revisión también debería tener como propósito la evaluación de las buenas prácticas en el sector en la administración del riesgo operativo que son adecuadas para las actividades, sistemas y procesos del banco. De ser necesario, el directorio debería asegurar que el marco de administración del riesgo operativo se revise a la luz de este análisis, para que se capten los riesgos operativos más importantes en el marco.

Principio 2: El directorio debería asegurar que el marco de administración del riesgo operativo del banco sea sujeto a una auditoría interna efectiva e integral por personal competente, independiente desde el punto de vista operativo y con una adecuada capacitación. La función de auditoría interna no debería tener la responsabilidad directa por la administración del riesgo operativo.

16. Los bancos deberían tener estructuras adecuadas de auditoría interna para verificar si las políticas y procedimientos se han implementado efectivamente.⁵ El directorio (o bien directamente o bien indirectamente a través de su comité de auditoría) debe asegurar que el alcance y la frecuencia del programa de auditoría sean adecuados considerando la exposición a riesgo. La auditoría debería verificar periódicamente si el marco de administración del riesgo operativo de la empresa se está implementando efectivamente en toda la empresa.

17. En la medida en que la función de auditoría participa en la supervisión del marco de administración del riesgo operativo, el directorio debería asegurar que se mantenga la independencia de la función de auditoría. Esta independencia puede correr peligro si la función de auditoría está involucrada directamente en el proceso de administración del riesgo operativo. La función de auditoría puede suministrar input valioso a los encargados de la administración del riesgo operativo, pero en sí no debe tener responsabilidad directa por la administración del riesgo operativo. En la práctica, el Comité reconoce que la función de auditoría en algunos bancos (sobre todo en los bancos más pequeños) puede tener la responsabilidad inicial por el desarrollo de un programa de administración del riesgo operativo. Si esto es el caso, los bancos deben asegurar que la responsabilidad por la administración diaria del riesgo operativo sea transferida oportunamente a otra división.

Principio 3: La alta gerencia debe ser responsable por la implementación del marco de administración del riesgo operativo aprobado por el directorio. El marco se debe implementar de forma coherente a lo largo de toda la organización bancaria, y todos los niveles del personal deberían entender sus responsabilidades respecto de la administración del riesgo operativo. La alta gerencia también debería ser responsable por el desarrollo de políticas, procesos y procedimientos para administrar el riesgo

⁵ El documento del Comité, *La Auditoría Interna en Bancos y la Relación del Supervisor con los Auditores* (agosto de 2001) describe el papel de la auditoría interna y externa.

operativo en todos los productos, actividades, procesos y sistemas más importantes del banco.

18. La gerencia debe traducir el marco de administración del riesgo operativo fijado por el directorio en políticas, procesos y procedimientos específicos que se pueden implementar y verificar en las diferentes unidades de negocio. Mientras que cada nivel de administración es responsable por la conformidad y efectividad de las políticas, procesos, procedimientos y controles dentro de su ámbito de trabajo, la alta gerencia debe asignar la autoridad, responsabilidades y relaciones de presentación de informes para promover y mantener el sistema, y asegurar que haya los recursos necesarios para administrar efectivamente el riesgo operativo.

19. La alta gerencia debe asegurar que las actividades del banco sean llevadas a cabo por personal calificado con la experiencia y capacidad técnica requerida y con acceso a recursos, y que el personal responsable por el monitoreo y imposición de la política de riesgo de la institución tenga autoridad independiente de las unidades bajo su supervisión. La gerencia debe asegurar que la política de administración del riesgo operativo del banco se haya comunicado claramente al personal en todos los niveles en las unidades expuestas a riesgos operativos importantes.

20. La alta gerencia debería asegurar que el personal responsable por la administración del riesgo operativo trabaje en efectiva coordinación con el personal responsable por la administración de los riesgos de crédito, mercado, y otros, al igual que con el personal de la empresa encargado de la contratación de servicios externos, como ser seguros y acuerdos de subcontratación. Si no se toma en cuenta esta coordinación, podría haber vacíos o traslapos significativos en el programa general de administración de riesgos del banco.

21. La alta gerencia también debería asegurar que las políticas de remuneración del banco sean coherentes con su apetito de riesgo. Las políticas de remuneración que recompensan al personal que se desvía de las políticas (p.ej. porque sobrepasa los límites definidos) debilitan los procesos de administración de riesgo del banco.

22. Se debe dedicar especial atención a la calidad de los controles de documentación y las prácticas de manejo de transacciones. En particular, deben ser bien documentados y divulgados a todo el personal las políticas, procesos y procedimientos relacionados con tecnologías avanzadas en apoyo de volúmenes altos de transacciones.

Administración de Riesgos: Identificación, Evaluación, Monitoreo y Mitigación / Control

Principio 4: Los bancos deberían identificar y evaluar el riesgo operativo inherente en todos los productos, actividades, procesos y sistemas importantes. Los bancos también deberían asegurar que, antes de introducir o emprender productos, actividades, procesos y sistemas nuevos, el riesgo operativo inherente en los mismos sea sujeto a procedimientos adecuados de evaluación.

23. La identificación de riesgos es esencial para el desarrollo posterior de un sistema viable de monitoreo y control del riesgo operativo. Una efectiva identificación de riesgos

toma en cuenta tanto factores internos (como ser la estructura del banco, la índole de las actividades del banco, la calidad de los recursos humanos del banco, cambios organizativos y rotación del personal) como factores externos (como ser cambios en el sector y avances tecnológicos) que pudieran tener un impacto negativo en el logro de los objetivos del banco.

24. Además de identificar los riesgos de mayor potencial impacto negativo, los bancos deberían evaluar su sensibilidad a estos riesgos. Una efectiva evaluación de riesgos permite al banco entender mejor su perfil de riesgo y asignar más efectivamente los recursos para la administración de riesgos.

25. Algunas de las herramientas que los bancos pueden utilizar para identificar y evaluar los riesgos operativos son:

- Auto-Evaluación o Evaluación del Riesgo: un banco evalúa sus operaciones y actividades frente a un menú de posibles puntos de sensibilidad al riesgo operativo. Este proceso se promueve internamente y, a menudo, incluye listas de control y/o talleres para identificar las fortalezas y debilidades del entorno de riesgo operativo. Por ejemplo, se pueden utilizar tarjetas de puntaje para traducir las evaluaciones cualitativas en parámetros cuantitativos que muestran la posición relativa de diferentes tipos de exposiciones al riesgo operativo. Algunos puntajes pueden estar relacionados con riesgos típicos de ciertas actividades, mientras que otros pueden categorizar riesgos que son comunes en todas las líneas de actividad. Los puntajes pueden referirse a riesgos inherentes, al igual que a los controles para mitigarlos. Además, los bancos pueden utilizar tarjetas de puntaje para asignar capital económico a líneas de actividad de acuerdo con su desempeño en la administración y control de varios aspectos del riesgo operativo.
- Mapeo del Riesgo: en este proceso, se incluyen en un mapa varias unidades de negocio, funciones organizacionales o flujos de proceso por tipo de riesgo. Este ejercicio puede revelar debilidades y puede ayudar a priorizar posteriores acciones a ser tomadas por la gerencia.
- Indicadores de Riesgo: los indicadores de riesgo son estadísticas y/o parámetros, muchas veces financieros, que pueden ayudar a comprender mejor la posición del banco en cuanto al riesgo. Estos indicadores generalmente se revisan periódicamente (por ejemplo, mensualmente o trimestralmente) para avisar a los bancos sobre cambios que podrían indicar un mayor riesgo. Esos indicadores pueden incluir el número de transacciones fracasadas, la tasa de rotación del personal, y la frecuencia y/o seriedad de errores y omisiones.
- Medición: algunas empresas han empezado a cuantificar su exposición al riesgo operativo, utilizando una variedad de enfoques. Por ejemplo, datos sobre la experiencia histórica de pérdidas del banco podrían suministrar información importante para evaluar la exposición del banco al riesgo operativo y desarrollar una política para mitigar / controlar el riesgo. Una forma efectiva para hacer buen uso de esta información consiste en establecer un marco para el registro y seguimiento sistemático de la frecuencia, seriedad y otra información relevante sobre eventos individuales de pérdida. Algunas empresas también han combinado información

sobre pérdida interna con información sobre pérdida externa, análisis de escenarios, y factores de evaluación de riesgo.

Principio 5: Los bancos deberían implementar un proceso para monitorear regularmente los perfiles del riesgo operativo y las exposiciones importantes a pérdidas. La información pertinente se debería presentar regularmente a la alta gerencia y el directorio que apoya la administración proactiva del riesgo operativo.

26. Un proceso de monitoreo efectivo es esencial para poder administrar adecuadamente el riesgo operativo. El monitoreo regular puede tener la ventaja de la rápida detección y corrección de deficiencias en las políticas, procesos y procedimientos de administración del riesgo operativo. La rápida detección y solución de estas deficiencias puede reducir en gran medida la potencial frecuencia y/o seriedad de un evento de pérdida.

27. Además de monitorear los eventos de pérdida operativa, los bancos deben identificar indicadores adecuados de alerta temprana sobre un riesgo incrementado de pérdidas futuras. Esos indicadores (que muchas veces se conocen como indicadores de riesgo clave o indicadores de alerta temprana) deben mirar hacia delante y podrían reflejar potenciales fuentes de riesgo operativo, como ser el crecimiento rápido, la introducción de productos nuevos, la rotación del personal, transacciones cortadas, tiempo de inactividad del sistema, etc. Si los umbrales se vinculan directamente con estos indicadores, un proceso de monitoreo efectivo puede ayudar a identificar los riesgos importantes clave de forma transparente y permitir al banco responder de forma apropiada a esos riesgos.

28. La frecuencia del monitoreo debería reflejar los riesgos involucrados y la frecuencia e índole en el entorno operativo. El monitoreo debería ser una parte integral de las actividades de un banco. Los resultados del monitoreo se deben incluir en los informes regulares para la gerencia y directorio, al igual que las revisiones para verificar el cumplimiento llevadas a cabo por el auditor interno y/o las funciones de administración de riesgos. Los informes elaborados por (y/o para) las autoridades de supervisión también pueden incluir información sobre este monitoreo y deben ser presentados internamente a la alta gerencia y el directorio, de ser aplicable.

29. La alta gerencia debe recibir informes regulares de las áreas pertinentes, como ser las unidades de negocio, funciones, la oficina de administración del riesgo operativo y el departamento de auditoría interna. Los informes sobre el riesgo operativo deberían contener datos financieros, operativos internos y datos sobre el nivel de cumplimiento, al igual que información del mercado externo sobre eventos y condiciones que son relevantes para el proceso de toma de decisiones. Los informes se deben distribuir a los niveles adecuados de gerencia y a las áreas del banco en las que la información reunida pudiera tener un impacto. Los informes deben reflejar plenamente cualquier problema identificado y deben alentar acciones correctivas oportunas para enfrentar los problemas pendientes. A fin de asegurar la utilidad y confiabilidad de esos informes de riesgo y auditoría, la gerencia debe verificar regularmente la oportunidad, exactitud y relevancia de los sistemas de informes y de los controles internos en general. La gerencia también puede utilizar informes preparados por fuentes externas (auditores, supervisores) para evaluar la utilidad y confiabilidad de los informes internos. Los informes se deben analizar con miras a mejorar el desempeño actual

en la administración de riesgo y a desarrollar nuevas políticas, procedimientos y prácticas de administración de riesgos.

30. En general, el directorio debería recibir suficiente información de nivel superior para que pueda entender el perfil general de riesgo operativo del banco y centrarse en las implicaciones materiales y estratégicas para las actividades.

Principio 6: Los bancos deberían tener políticas, procesos y procedimientos para controlar y/o mitigar riesgos operativos importantes. Los bancos deberían hacer una revisión periódica de sus estrategias de limitación y control de riesgos y deberían ajustar su perfil de riesgo operativo de acuerdo con ello utilizando estrategias apropiadas, a la luz de su perfil y apetito general de riesgo.

31. El propósito de las actividades de control es enfrentar los riesgos operativos identificados por el banco.⁶ Con respecto a todos los riesgos operativos importantes que fueron identificados, el banco debería decidir si quiere utilizar procedimientos adecuados para controlar y/o mitigar los riesgos, o si quiere asumir el riesgo. Para los riesgos que no se pueden controlar, el banco debería decidir si quiere aceptar esos riesgos, o si quiere reducir el nivel de las actividades que den lugar a ese riesgo o si quiere retirar esa actividad completamente. Se deben fijar procesos y procedimientos de control y los bancos deben tener un sistema para asegurar el cumplimiento de un conjunto documentado de políticas internas relativas al sistema de administración de riesgos. Algunos elementos de ese sistema podrían ser los siguientes:

- Revisiones en un alto nivel del avance del banco hacia el logro de los objetivos fijados;
- Control de cumplimiento con controles gerenciales;
- Políticas, procesos y procedimientos relativos a la revisión, tratamiento y resolución de problemas de incumplimiento; y
- Un sistema de aprobaciones y autorizaciones documentadas para asegurar que se responda a un nivel gerencial apropiado.

32. A pesar de ser crítico un marco de políticas y procedimientos formales y escritos, debe ser reforzado a través de una fuerte cultura de control que promueve prácticas sanas de administración de riesgos. Tanto el directorio como la alta gerencia son responsables por el establecimiento de una fuerte cultura de control interno en la que las actividades de control son una parte integral de las actividades corrientes del banco. Los controles que son una parte integral de las actividades regulares permiten respuestas rápidas a condiciones cambiantes y evitan costos innecesarios.

33. Un sistema efectivo de control interno también requiere que haya una adecuada segregación de deberes y que el personal no sea asignado a responsabilidades que pueden dar lugar a un conflicto de interés. Asignar obligaciones conflictivas al personal, o a un equipo, puede resultar en que esconden pérdidas, errores o acciones inadecuadas. Por lo

⁶ Para mayores detalles, ver *Marco para Sistemas de Control Interno en Organizaciones Bancarias*, Comisión de Basilea de Supervisión de Bancos, septiembre de 1998.

tanto, las áreas de potenciales conflictos de interés deben ser identificadas, minimizadas y sujetas a un proceso independiente y cuidadoso de monitoreo y revisión.

34. Además de la segregación de deberes, los bancos deben asegurar que haya otras prácticas internas para controlar el riesgo operativo. Algunos ejemplos:

- Monitoreo de cerca de la observancia de umbrales o límites de riesgo asignados;
- Mantener medidas de protección para el acceso a, y uso de, registro y activos bancarios;
- Asegurar que el personal tenga experiencia y capacitación adecuadas;
- Identificar líneas o productos en los que el retorno parece ser incoherente con expectativas razonables (p.ej. en caso de actividades de bajo riesgo y baja ganancia con un alto retorno, puede surgir la pregunta si ese retorno se ha logrado como resultado de la violación de controles internos); y
- La verificación y reconciliación regulares de transacciones y cuentas.

La no-implementación de esas prácticas ha dado lugar a pérdidas operativas significativas en algunos bancos en años recientes.

35. El riesgo operativo puede ser más pronunciado si los bancos empiezan a trabajar con actividades nuevas o si desarrollan productos nuevos (sobre todo si esas actividades o productos no son coherentes con las estrategias comerciales centrales del banco), ingresan en mercados que no conocen bien, y/o participan en negocios a una considerable distancia geográfica de la oficina central. Además, en muchos de esos casos, las empresas no aseguran que la infraestructura de control de la administración de riesgos siga el ritmo del crecimiento de las actividades. Cierta número de las pérdidas más grandes de más alto perfil en los años recientes ha ocurrido en caso de presentarse una o más de estas condiciones. En este sentido, los bancos tienen la responsabilidad de asegurar que se dedique especial atención a las actividades de control interno en caso de existir esas condiciones.

36. Algunos riesgos operativos significativos tienen una baja probabilidad pero un potencial impacto financiero enorme. Además, no todos los eventos de riesgo pueden ser controlados (p.ej. desastres naturales). Se pueden utilizar herramientas o programas de mitigación de riesgos para reducir la exposición a, o la frecuencia y/o seriedad de esos eventos. Por ejemplo, se pueden utilizar pólizas de seguros, especialmente las con ciertas características, especialmente el pago rápido, para exteriorizar el riesgo de pérdidas de “baja frecuencia, alta seriedad” que pudieran ocurrir como resultado de eventos como ser demandas de terceros como resultado de errores y omisiones, la pérdida física de valores, fraude cometido por empleados o terceros, y desastres naturales.

37. Sin embargo, los bancos deberían considerar las herramientas de mitigación de riesgo como instrumentos complementarios, y no en reemplazo de un detenido control interno del riesgo operativo. La exposición a riesgos puede bajar considerablemente si hay mecanismos para reconocer y rectificar rápidamente errores legítimos del riesgo operativo. También se tiene que analizar cuidadosamente la medida en que las herramientas de

mitigación de riesgo, como ser seguros, realmente reducen el riesgo, ya que a veces transfieren el riesgo a otro sector o área, o incluso crean un riesgo nuevo (p.ej. un riesgo legal o de contraparte).

38. También son importantes las inversiones en la seguridad adecuada de la tecnología de información y tecnología de procesamiento para mitigar el nivel de riesgo. No obstante, los bancos deben estar conscientes que una mayor automatización puede transformar las pérdidas de alta frecuencia y baja seriedad en pérdidas de baja frecuencia y alta seriedad. Éstas últimas pueden estar asociadas con la pérdida o interrupción prolongada de servicios a causa de factores internos o factores más allá del control inmediato del banco (p.ej. eventos externos). Esos problemas pueden dar lugar a serias dificultades para los bancos y podrían poner en peligro la capacidad de la institución de seguir ejecutando sus actividades comerciales clave. Tal como se discute abajo en el Principio 7, los bancos deberían establecer planes de recuperación en caso de desastres y de continuación de las actividades que enfrentan este riesgo.

39. Asimismo, los bancos deberían fijar políticas para administrar los riesgos asociados con las actividades de subcontratación. A través de subcontrataciones, la institución puede bajar su perfil de riesgo, transfiriendo actividades a otros con más experiencia y que trabajan a una mayor escala para administrar los riesgos asociados con actividades especializadas. Sin embargo, si un banco trabaja con terceros, no baja la responsabilidad del directorio y la gerencia por asegurar que las actividades de la parte tercera se lleven a cabo de una manera sana y segura y de conformidad con las leyes aplicables. Los acuerdos de subcontratación deben basarse en contratos y/o acuerdos de provisión de servicios robustos que aseguran una repartición clara de las responsabilidades entre los proveedores externos de servicios y el banco que los subcontrata. Asimismo, los bancos deben administrar los riesgos residuales asociados con los acuerdos de subcontratación, incluyendo la interrupción de servicios.

40. Dependiendo de la escala e índole de la actividad, los bancos deben entender el potencial impacto en sus operaciones y sus clientes de cualquier potencial deficiencia en los servicios suministrados por los vendedores y otros proveedores de servicios que sean de terceros u otras empresas del grupo, incluyendo interrupciones operativas y la potencial quiebra o problemas de las partes externas. El directorio y la gerencia deben asegurar que las expectativas y obligaciones de cada parte estén bien definidas, entendidas y que sean exigibles. El alcance de la responsabilidad y capacidad financiera de la parte externa para compensar al banco por errores, negligencia y otros defectos operativos se debe considerar explícitamente como una parte de la evaluación de riesgo. Los bancos deben hacer un análisis inicial y deben monitorear las actividades de proveedores terceros, especialmente de los que no tienen experiencia en el entorno regulado del sector bancario. Además, deben revisar este proceso (incluyendo re-evaluaciones de la información) regularmente. Para actividades críticas, puede ser que el banco tenga que pensar en planes de contingencia, incluyendo la disponibilidad de partes externas alternativas y los costos y recursos requeridos para cambiar de parte externa, posiblemente de forma muy repentina.

41. En algunos casos, los bancos pueden decidir de o bien retener cierto nivel de riesgo operativo o de auto-asegurarse contra ese riesgo. Si esto es el caso y el riesgo es

considerable, la decisión de retener el riesgo o auto-asegurarse contra el riesgo debe ser transparente dentro de la organización y debe ser compatible con la estrategia comercial y apetito de riesgo general del banco.

Principio 7: Los bancos deben tener planes de contingencia y de continuación de las actividades para asegurar su capacidad de operar de forma constante y limitar sus pérdidas en caso de una seria interrupción de las actividades.

42. Por motivos fuera del control de un banco, un evento serio puede resultar en la incapacidad del banco de cumplir con algunas o todas sus obligaciones, especialmente si está dañada o inaccesible la infraestructura física, de telecomunicaciones, o de tecnología de información del banco. A su vez, esto puede dar lugar a pérdidas financieras significativas para el banco, al igual que a perturbaciones más amplias en el sistema financiero a través de canales como ser el sistema de pagos. En este sentido, los bancos deben establecer planes de recuperación en caso de desastres y de continuación de las actividades que toman en cuenta los diferentes tipos de posibles escenarios a los que puede estar expuesto el banco, de acuerdo con el tamaño y complejidad de las operaciones del banco.

43. Los bancos deberían identificar procesos comerciales críticos, incluyendo los que dependen de vendedores externos o terceros, y para los que la rápida reanudación de los servicios sería sumamente crítica. Para estos procesos, los bancos deberían identificar mecanismos alternativos para reanudar los servicios en caso de una interrupción. Se debe dedicar especial atención a la posibilidad de restablecer los registros electrónicos o físicos necesarios para reanudar las actividades. Si hay back-ups de esos registros en otro lugar, o si las operaciones del banco se deben reubicar a otro lugar, es importante que esos lugares se encuentren a una distancia adecuada de las operaciones interrumpidas para minimizar el riesgo de que tanto los registros primarios como los registros de back-up estén indisponibles simultáneamente.

44. Los bancos deben hacer una revisión periódica de sus planes de recuperación en caso de desastres y de continuación de las actividades para ver si son coherentes con las operaciones y estrategias comerciales del banco. Además, esos planes deben ser probados periódicamente para asegurar que el banco pueda ejecutar los planes en el evento poco probable de una seria interrupción de las actividades.

Papel de los Supervisores

Principio 8: Los supervisores bancarios deberían exigir que todos los bancos, independientemente de su tamaño, tengan un marco efectivo para identificar, evaluar, monitorear y controlar / mitigar riesgos operativos importantes como parte de un enfoque general para la administración de riesgos.

45. Los supervisores deben exigir que los bancos desarrollen marcos de administración del riesgo operativo que son coherentes con las pautas en este documento y con el tamaño, complejidad y perfiles de riesgo de los bancos. En la medida en que los riesgos operativos amenazan la seguridad y solvencia de los bancos, los supervisores tienen la responsabilidad

por alentar a los bancos a desarrollar y utilizar mejores técnicas para administrar esos riesgos.

Principio 9: Los supervisores deberían llevar a cabo, directa o indirectamente, evaluaciones independientes regulares de las políticas, procedimientos y prácticas de un banco respecto de los riesgos operativos. Los supervisores deberían asegurar que haya mecanismos adecuados que les permiten estar al tanto de evoluciones en los bancos.

46. Algunos ejemplos de lo que una evaluación independiente del riesgo operativo por los supervisores debería verificar son:

- La efectividad del proceso de administración de riesgo del banco y el entorno de control general respecto del riesgo operativo;
- Los métodos que el banco utiliza para monitorear e informar sobre su perfil de riesgo operativo, incluyendo datos sobre pérdidas operativas y otros indicadores sobre el potencial riesgo operativo;
- Los procedimientos del banco para la resolución oportuna y efectiva de eventos y vulnerabilidad al riesgo operativo;
- El proceso de controles internos, revisiones y auditorías del banco para asegurar la integridad del proceso general de administración del riesgo operativo;
- La efectividad de los esfuerzos de mitigación del riesgo operativo del banco, como ser la contratación de seguros;
- La calidad e integridad de los planes del banco de recuperación en caso de desastres y de continuación de las actividades;
- El proceso del banco para evaluar el coeficiente patrimonial general para el riesgo operativo en relación con su perfil de riesgo, y, de ser apropiado, sus metas de capital internas.

47. Los supervisores también deben tratar de asegurar que, en caso de bancos que forman parte de un grupo financiero, haya procedimientos para asegurar que el riesgo operativo sea administrado de una forma apropiada e integrada a lo largo del grupo. Al realizar esta evaluación, puede ser necesaria la cooperación y el intercambio de información con otros supervisores, de acuerdo con procedimientos definidos. Algunos supervisores pueden optar por utilizar auditores externos en estos procesos de evaluación.

48. Las deficiencias identificadas durante la revisión por el supervisor se pueden enfrentar con una variedad de acciones. Los supervisores deben utilizar los instrumentos más adecuados para las circunstancias específicas del banco y su entorno de operación. Para que puedan recibir información actualizada sobre el riesgo operativo, los supervisores podrían establecer mecanismos para la presentación de informes directamente con los bancos y auditores externos (por ejemplo, los informes gerenciales internos sobre el riesgo operativo se podrían poner a disposición de los supervisores de forma rutinaria).

49. En vista del reconocimiento general que los procesos integrales de administración del riesgo operativo todavía se están desarrollando en muchos bancos, los supervisores

deberían desempeñar un papel activo en el fomento de esos esfuerzos mediante el monitoreo y evaluación de las mejoras recientes y planes de evoluciones prospectivas del banco. Estos esfuerzos se pueden comparar con los de otros bancos para suministrar retroalimentación útil sobre el estado de sus propios esfuerzos. Además, en la medida en que hay razones identificadas por qué ciertos esfuerzos han resultado inefectivos, esa información se debería suministrar en términos generales para apoyar el proceso de planificación. Asimismo, los supervisores deben centrarse en la medida en que un banco ha integrado el proceso de administración del riesgo operativo a lo largo de la organización para asegurar una efectiva administración del riesgo operativo en las diferentes líneas de negocio, para tener líneas claras de comunicación y responsabilidad y para promover la activa auto-evaluación de las prácticas existentes y la consideración de posibles mejoras en la mitigación del riesgo.

Papel de la Divulgación

Principio 10: Los bancos deben divulgar suficiente información al público para que los participantes en el mercado puedan evaluar su enfoque para la administración del riesgo operativo.

50. El Comité cree que la divulgación pública oportuna y frecuente de información relevante por los bancos puede resultar en una mejor disciplina de mercado y, por ende, una administración de riesgo más efectiva. La cantidad de la divulgación debe ser de acuerdo con el tamaño, perfil de riesgo y complejidad de las operaciones del banco.

51. El área de la divulgación del riesgo operativo todavía no está bien desarrollada, en primer lugar porque los bancos siguen en proceso de desarrollo de las técnicas de evaluación del riesgo operativo. Sin embargo, el Comité cree que un banco debería divulgar su marco de administración del riesgo operativo de una forma que permite a los inversionistas y contrapartes determinar si el banco identifica, evalúa, monitorea y controla / mitiga efectivamente el riesgo operativo.

Traducción de la Superintendencia de Bancos y Entidades de Bolivia.