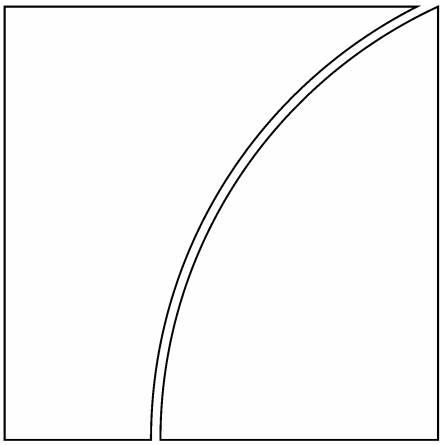
Comité de Supervisión Bancaria de Basilea



Buenas prácticas para la gestión y supervisión del riesgo operativo

Febrero de 2003

BANCO DE PAGOS INTERNACIONALES

Esta publicación puede obtenerse en:

Secretaría del Comité de Supervisión Bancaria de Basilea
c/o Bank for International Settlements
CH-4002 Basilea (Suiza)

E-mail: publications@bis.org

Fax: +41 61 280 9100

Esta publicación se encuentra disponible en la página del BPI en Internet (www.bis.org).

Publicado también en alemán, francés, inglés e italiano.

Grupo para la Gestión del Riesgo del Comité de Supervisión Bancaria de Basilea

Presidente:
Roger Cole, Junta de la Reserva Federal, Washington DC

Banco Nacional de Bélgica, Bruselas	Dominique Gressens
Comisión Bancaria y Financiera, Bruselas	Jos Meuleman
Oficina de Superintendencia de Instituciones Financieras Ottawa	Jeff Miller
Comisión Bancaria, París	Laurent Le Mouël
Deutsche Bundesbank, Frankfurt del Meno	Magdalene Heid Karin Sagner-Kaiser
Bundesanstalt für Finanzdienstleistungsaufsicht, Bonn	Kirsten Straus
Banco de Italia, Roma	Claudio Dauria Fabrizio Leandri Sergio Sorrentino
Banco de Japón, Tokio	Satoshi Yamaguchi
Agencia de Servicios Financieros, Tokio	Hirokazu Matsushima
Comisión de Vigilancia del Sector Financiero, Luxemburgo	Davy Reinard
Banco de los Países Bajos, Amsterdam	Klaas Knot
Banco de España, Madrid	Guillermo Rodriguez-Garcia Juan Serrano
Finansinspektionen, Estocolmo	Jan Hedquist
Sveriges Riksbank, Estocolmo	Thomas Flodén
Eidgenössische Bankenkommission, Berna	Martin Sprenger
Autoridad de los Servicios Financieros, Londres	Helmut Bauer Victor Dowd
Federal Deposit Insurance Corporation, Washington DC	Mark Schmidt
Banco de la Reserva Federal de Nueva York	Beverly Hirtle Stefan Walter
Junta de la Reserva Federal, Washingon, D.C.	Kirk Odegard
Office of the Comptroller of the Currency, Washington DC	Kevin Bailey Tanya Smith
Banco Central Europeo, Frankfurt del Meno	Panagiotis Strouzas
Comisión Europea, Bruselas	Michel Martino Melania Savino
Secretaría del Comité de Supervisión Bancaria de Basilea, Banco de Pagos Internacionales	Stephen Senior

Índice

Buenas prácticas
para la gestión y supervisión del riesgo operativo

Introducción

1. En el presente documento se recoge una serie de principios para una gestión y supervisión eficaces del riesgo operativo, de modo que los bancos y autoridades supervisoras puedan utilizarlos al evaluar políticas y prácticas destinadas a gestionar este tipo de riesgos.

2. El Comité de Supervisión Bancaria de Basilea (el Comité) reconoce que el método concreto para la gestión de riesgos operativos que elija cada banco dependerá de una serie de factores, como son su tamaño y sofisticación así como la naturaleza y complejidad de sus actividades. Sin embargo, a pesar de estas diferencias, son muchos y variados los elementos fundamentales para una gestión adecuada de estos riesgos, sea cual sea el tamaño y ámbito de actuación del banco; a saber, estrategias claramente definidas y seguimiento de las mismas por parte del consejo de administración y de la alta gerencia, una sólida cultura de gestión del riesgo operativo[1] y de control interno (como pueden ser unas líneas inequívocas de responsabilidad y la segregación de funciones), herramientas eficaces para la transmisión interna de información y planes de contingencia. El Comité estima por lo tanto que los principios aquí recogidos ofrecen a todos los bancos las pautas para desarrollar unas buenas prácticas. Su documento anterior, *A Framework for Internal Control Systems in Banking Organisations* (septiembre de 1998) sienta las bases de su labor actual en el ámbito del riesgo operativo.

Antecedentes

3. La desregulación y la globalización de los servicios financieros, junto con la creciente sofisticación de las tecnologías financieras, hacen más complejas las actividades de los bancos y, por ende, aumentan sus perfiles de riesgo (es decir, el nivel de riesgo de las actividades y/o categorías de riesgo de una empresa). Con la evolución de las prácticas bancarias, los bancos se ven expuestos a nuevos riesgos cada vez mayores, aparte de los riesgos de crédito, de tipos de interés y de mercado, como por ejemplo:

- El creciente uso de tecnologías cada vez más automatizadas puede hacer que, si éstas no se someten a los controles adecuados, los riesgos derivados de errores de procesamiento manual se materialicen ahora en fallos en el sistema, al depender en mayor medida de sistemas globalmente integrados;
- El crecimiento del comercio electrónico conlleva ciertos riesgos (por ejemplo, fraude interno y externo y problemas relacionados con la seguridad del sistema) que todavía no se comprenden completamente;
- Las adquisiciones, fusiones, escisiones y consolidaciones a gran escala ponen a prueba la viabilidad de los sistemas nuevos o los recién integrados;
- La creación de bancos que ofrecen servicios a gran escala hace necesario el mantenimiento continuo de controles internos de alto nivel y de sistemas de copias de seguridad;
- Los bancos pueden aplicar técnicas de cobertura del riesgo (por ejemplo, mediante colateral, derivados del crédito, acuerdos de compensación de saldos y titulización de activos) para optimizar su exposición a los riesgos de mercado y de crédito, pero estas coberturas pueden generar a su vez otros tipos de riesgo (ej. riesgo legal); y

[1] Por *cultura de gestión interna del riesgo operativo* se entiende el conjunto de valores, actitudes, competencias y comportamientos individuales y corporativos que conforman el compromiso y estilo de una empresa para la gestión del riesgo operativo.

- La creciente utilización de acuerdos de subcontratación y la mayor participación en los sistemas de compensación y liquidación pueden reducir ciertos riesgos, pero también pueden plantear otros muy significativos para los bancos.

4. Los distintos riesgos anteriormente recogidos se pueden agrupar bajo la categoría de "riesgo operativo", que el Comité define como "el riesgo de sufrir pérdidas debido a la inadecuación o a fallos de los procesos, personas o sistemas internos o bien a causa de acontecimientos externos[2]." Esta definición también engloba el riesgo legal pero excluye los riesgos estratégico y de reputación.

5. El Comité reconoce que "riesgo operativo" es un término que representa diferentes conceptos dentro del sector bancario, por lo que los bancos pueden adoptar sus propias definiciones con fines internos (incluida la aplicación del documento Buenas Prácticas). Sea cual sea la definición utilizada, los bancos deben comprender a qué se refiere el riesgo operativo para poder llevar a cabo una administración y un control efectivos de esta categoría de riesgo. También es importante que su definición abarque el amplio abanico de riesgos operativos a los que se enfrentan los bancos y que recoja las principales causas de pérdidas operativas graves. A continuación se recogen los diferentes tipos de riesgo operativo que el Comité, en colaboración con la banca, ha identificado como posibles fuentes de pérdidas sustanciales:

- Fraude interno: Errores intencionados en la información sobre posiciones, robos por parte de empleados, utilización de información confidencial en beneficio de la cuenta del empleado, etc.
- Fraude externo: atraco, falsificación, circulación de cheques en descubierto, daños por intrusión en los sistemas informáticos, etc.
- Relaciones laborales y seguridad en el puesto de trabajo: solicitud de indemnizaciones por parte de los empleados, infracción de las normas laborales de seguridad e higiene, organización de actividades laborales, acusaciones de discriminación, responsabilidades generales, etc.
- Prácticas con los clientes, productos y negocios: abusos de confianza, abuso de información confidencial sobre el cliente, negociación fraudulenta en las cuentas del banco, blanqueo de capitales, venta de productos no autorizados, etc.
- Daños a activos materiales: terrorismo, vandalismo, terremotos, incendios, inundaciones, etc.
- Alteraciones en la actividad y fallos en los sistemas: fallos del *hardware* o del *software*, problemas en las telecomunicaciones, interrupción en la prestación de servicios públicos, etc.
- Ejecución, entrega y procesamiento: errores en la introducción de datos, fallos en la administración del colateral, documentación jurídica incompleta, concesión de acceso no autorizado a las cuentas de los clientes, prácticas inadecuadas de contrapartes distintas de clientes, litigios con distribuidores, etc.

Tendencias y prácticas en el sector

6. Como parte de su labor de supervisión del riesgo operativo, el Comité ha intentado promover un mejor conocimiento de las tendencias y prácticas bancarias actuales para la gestión de este tipo de riesgo. Para ello, se han celebrado numerosas reuniones con organizaciones bancarias, se han realizado encuestas sobre las prácticas en el sector y se han analizado los resultados obtenidos. A partir de estos trabajos, el Comité cree conocer bien las pautas que siguen los bancos en la actualidad y sus esfuerzos por desarrollar nuevos métodos de gestión del riesgo operativo.

[2] El sector bancario adoptó esta definición como parte de la labor del Comité para desarrollar unos requerimientos mínimos de capital regulador para el riesgo operativo. A pesar de que el presente documento no forma parte del acuerdo de capital formalmente, el Comité espera que los elementos fundamentales para una adecuada gestión del riesgo operativo recogidos en este informe orienten al supervisor cuando evalúe la suficiencia del capital bancario, por ejemplo, dentro del proceso del examen supervisor (Pilar 2).

7. El Comité reconoce que la gestión de riesgos operativos concretos no es algo nuevo, sino que siempre ha sido una parte importante del esfuerzo de los bancos por evitar el fraude, mantener la integridad de los controles internos, reducir los errores en las operaciones, etc. Sin embargo, lo que resulta relativamente nuevo es considerar la gestión del riesgo operativo como una práctica integral comparable a la gestión del riesgo de crédito o de mercado en principio, si bien no siempre en la práctica. Las tendencias mencionadas en la introducción de este informe, unidas al aumento en todo el mundo de casos muy conocidos de pérdidas por riesgo operativo, han llevado a los bancos y supervisores a considerar la gestión de este tipo de riesgos como una disciplina integral, como ya ha ocurrido en otros sectores de actividad.

8. En el pasado, los bancos gestionaban sus riesgos operativos utilizando únicamente mecanismos internos de control dentro de sus líneas de negocio, a los que se sumaba la función de auditoría. Aunque estos mecanismos continúan siendo muy importantes, recientemente se han observado nuevos procesos y estructuras destinadas a la gestión del riesgo operativo. En este sentido, son cada vez más las instituciones convencidas de que los programas de gestión del riesgo operativo proporcionan seguridad y solidez al banco, por lo que están avanzando para tratar el riesgo operativo como un tipo de riesgo específico, al igual que ocurre con los riesgos de crédito y de mercado. El Comité estima que el intercambio de ideas entre supervisores y banqueros es fundamental para seguir desarrollando pautas adecuadas para la gestión de riesgos operativos.

9. El presente documento se estructura en las siguientes secciones: desarrollo de un marco adecuado de gestión del riesgo; gestión del riesgo: identificación, evaluación, seguimiento y control/cobertura; la función de los supervisores; y la función de la divulgación de información.

Buenas prácticas

10. Al desarrollar sus buenas prácticas, el Comité ha partido de su labor anterior sobre gestión de otros riesgos bancarios significativos, como el riesgo de crédito, de tipos de interés o de liquidez, convencido de que es necesario tratar el riesgo operativo con el mismo rigor que se aplica a los demás riesgos. Sin embargo, no cabe duda de que el riesgo operativo difiere de otros riesgos bancarios, al no ser un riesgo que se acepte directamente a cambio de un beneficio esperado, sino que es algo que se puede producir en el acontecer diario de la actividad empresarial, y esto repercute en el proceso de gestión del riesgo[3]. Al mismo tiempo, si este riesgo no se controla adecuadamente, puede verse afectado el perfil de riesgo de la institución, con lo que podría verse expuesta a pérdidas significativas. A efectos de este informe y para reflejar la diferente naturaleza del riesgo operativo, por "gestión" del riesgo operativo se entiende la "identificación, evaluación, seguimiento y control o cobertura" del riesgo. Esta definición contrasta sin embargo con la que utilizó el Comité en informes anteriores sobre gestión del riesgo, que hacía referencia a la "identificación, cálculo, seguimiento y control" del riesgo. El Comité, al igual que en sus trabajos sobre otros riesgos bancarios, ha estructurado el presente informe en torno a una serie de principios, a saber:

Desarrollo de un marco adecuado para la gestión del riesgo

Principio 1: El Consejo de administración[4] deberá conocer cuáles son los principales aspectos de los riesgos operativos para el banco, en tanto que categoría de riesgo diferenciada, y deberá aprobar y

[3] No obstante, el Comité reconoce que cuando se trate de líneas de negocio que soportan riesgos de mercado o de crédito mínimos (ej. gestión de activos o pagos y liquidaciones), la decisión de incurrir en riesgos operativos o de competir basándose en su capacidad de gestionar y valorizar adecuadamente el riesgo forma parte del cálculo de riesgos y beneficios del banco.

[4] En el presente documento, se hace referencia a una estructura de gestión bancaria compuesta por un consejo de administración y una alta dirección. El Comité entiende que los marcos jurídicos y reguladores difieren considerablemente en cada país en cuanto a las funciones que ostenta el consejo de administración y la alta dirección. En algunos países, el consejo de administración es el principal (o incluso el único) responsable de supervisar al órgano ejecutivo (alta dirección, dirección general) con el fin de asegurar que éste cumple sus funciones, por lo que en algunos casos se lo conoce como comité de vigilancia. Esto implica que el consejo de administración no posee funciones ejecutivas. En otros países, en cambio, el consejo de administración tiene competencias más amplias, en el sentido de que establece el marco general

revisar periódicamente el marco que utiliza el banco para la gestión de este riesgo. Este marco deberá ofrecer una definición de riesgo operativo válida para toda la empresa y establecer los principios para definir, evaluar, seguir y controlar o mitigar este tipo de riesgos.

Principio 2: El consejo de administración deberá asegurar que el marco para la gestión del riesgo operativo en el banco esté sujeto a un proceso de auditoría interna eficaz e integral por parte de personal independiente, capacitado y competente. La función de auditoría interna no deberá ser directamente responsable de la gestión del riesgo operativo.

Principio 3: La alta gerencia deberá ser la responsable de poner en práctica el marco para la gestión del riesgo operativo aprobado por el consejo de administración. Dicho marco deberá ser aplicado de forma consistente en toda la organización bancaria y todas las categorías laborales deberán comprender sus responsabilidades al respecto. La alta gerencia también deberá ser responsable del desarrollo de políticas, procesos y procedimientos destinados a la gestión de estos riesgos para todos los productos, actividades, procesos y sistemas relevantes para el banco.

Gestión del riesgo: identificación, evaluación, seguimiento y cobertura/control

Principio 4: los bancos deberán identificar y evaluar el riesgo operativo inherente a todos sus productos, actividades, procesos y sistemas relevantes. Además, también deberán comprobar que antes de lanzar o presentar nuevos productos, actividades, procesos o sistemas, se evalúa adecuadamente su riesgo operativo inherente.

Principio 5: Los bancos deberán vigilar periódicamente los perfiles de riesgo operativo y las exposiciones sustanciales a pérdidas. La alta gerencia y el consejo de administración deberán recibir información pertinente de forma periódica que complemente la gestión activa del riesgo operativo.

Principio 6: Los bancos deberán contar con políticas, procesos y procedimientos para controlar y cubrir los riesgos operativos más relevantes. Además, deberán reexaminar periódicamente sus estrategias de control y reducción de riesgos y ajustar su perfil de riesgo operativo según corresponda, utilizando para ello las estrategias que mejor se adapten a su apetito por el riesgo y a su perfil de riesgo.

Principio 7: Los bancos deberán contar con planes de contingencia y de continuidad de la actividad, que aseguren su capacidad operativa continua y que reduzcan las pérdidas en caso de interrupción grave de la actividad.

La función de los supervisores

Principio 8: Los supervisores bancarios deberán exigir a todos los bancos, sea cual sea su tamaño, que mantengan un marco eficaz para identificar, evaluar, seguir y controlar o mitigar sus riesgos operativos más relevantes, como parte de su aproximación general a la gestión de riesgos.

Principio 9: Los supervisores deberán realizar, directa o indirectamente, una evaluación periódica independiente de las políticas, prácticas y procedimientos con los que cuentan los bancos para gestionar sus riesgos operativos. Además, deberán cerciorarse de que se han puesto en marcha los mecanismos necesarios para estar al tanto de cualquier novedad que se produzca en un banco.

La función de la divulgación de información

Principio 10: Los bancos deberán proporcionar información pública suficiente para que los partícipes del mercado puedan evaluar sus estratégicas de gestión del riesgo operativo.

---

para la gestión del banco. Dadas estas diferencias, en este documento las nociones de consejo de administración y alta dirección se utilizan para denominar a los órganos decisorios del banco y no para identificar figuras jurídicas.

Desarrollo de un entorno adecuado para la gestión del riesgo

11. Si no se comprende y gestiona adecuadamente el riesgo operativo, presente prácticamente en cada operación y actividad bancaria, se puede aumentar la probabilidad de que algunos riesgos pasen desapercibidos o escapen a los controles. Tanto el consejo como la dirección son los responsables de crear una cultura organizativa que conceda gran prioridad a la gestión eficaz del riesgo operativo y al cumplimiento de estrictos controles operativos. La gestión del riesgo operativo resulta más eficaz cuando el banco presta especial atención al cumplimiento de las normas más estrictas de comportamiento ético en todos los niveles de la organización. El consejo y la gerencia deberán fomentar una cultura organizativa que inculque, de palabra y obra, integridad entre todos los empleados a la hora de realizar sus actividades diarias.

Principio 1: El Consejo de administración deberá conocer cuáles son los principales aspectos de los riesgos operativos para el banco, en tanto que categoría de riesgo diferenciada, y deberá aprobar y revisar periódicamente el marco que utiliza el banco para la gestión de este riesgo. Este marco deberá ofrecer una definición de riesgo operativo válida para toda la empresa y establecer los principios para definir, evaluar, seguir y controlar o mitigar este tipo de riesgos.

12. El consejo de administración deberá aprobar la aplicación de un marco, aplicable a toda la empresa, para gestionar explícitamente el riesgo operativo, en tanto que riesgo específico para la seguridad y solidez del banco. El consejo proporcionará a la alta gerencia unas pautas y orientaciones inequívocas sobre los principios en los que se basa este marco y aprobará las políticas correspondientes desarrolladas por la alta gerencia.

13. Dicho marco deberá partir de una definición adecuada de riesgo operativo, que determine sin ambigüedades en qué consiste este riesgo en el banco. Este marco deberá abarcar el apetito del banco por el riesgo operativo así como su tolerancia al mismo, en virtud de sus políticas para gestionar estos riesgos y de sus criterios para establecer prioridades entre las actividades desarrolladas a tal efecto, especificando hasta qué punto y de qué manera se transfiere el riesgo operativo fuera el banco. También deberá incluir las políticas a seguir por el banco para la identificación, evaluación, seguimiento y control o cobertura de este riesgo. El grado de formalidad y sofisticación de este marco deberá ser acorde con su perfil de riesgo.

14. El consejo es responsable de establecer una estructura de gestión capaz de poner en práctica el marco para la gestión del riesgo operativo en la entidad. Dado que uno de los principales aspectos de la gestión de estos riesgos está relacionado con el establecimiento de estrictos controles internos, es especialmente importante que el consejo establezca unas líneas claras de responsabilidad, asunción de responsabilidades e información para la entidad. Asimismo, habrá que delimitar responsabilidades y líneas de autoridad entre las funciones de control de riesgo operacional, las líneas de negocio y los cargos de apoyo con el fin de evitar los conflictos de intereses. Dicho marco también deberá articular los principales procesos que el banco necesita para gestionar el riesgo operativo.

15. El consejo deberá reexaminar este marco periódicamente para cerciorarse de que el banco está gestionando correctamente los riesgos operativos derivados de cambios en el mercado y de otros factores externos, así como los que están asociados a nuevos productos, actividades o sistemas. Este proceso de reevaluación también intentará determinar qué prácticas del sector para la gestión del riesgo operativo se adaptan mejor a las actividades, sistemas y procesos del banco. Si fuera necesario, el consejo se asegurará de que el marco para la gestión del riesgo operativo se revisa a la luz de este análisis, de forma que los principales riesgos operativos queden recogidos en este marco.

Principio 2: El consejo de administración deberá asegurar que el marco para la gestión del riesgo operativo en el banco esté sujeto a un proceso de auditoría interna eficaz e integral por parte de personal independiente, capacitado y competente. La función de auditoría interna no deberá ser directamente responsable de la gestión del riesgo operativo.

16. Los bancos deberán contar con un proceso adecuado de auditoría interna para comprobar que las políticas y procedimientos operativos se han llevado a cabo eficazmente[5]. El consejo, ya sea

[5] El informe del Comité titulado *Internal Audit in Banks and the Supervisor's Relationship with Auditors* (agosto de 2001) describe el papel que desempeñan las auditorías interna y externa.

directamente o indirectamente a través de su comité de auditoría, deberá comprobar que el ámbito y la frecuencia del programa auditor se adaptan a la exposición del banco al riesgo. El auditor deberá comprobar periódicamente que el marco para la gestión del riesgo operativo en el banco se aplica de forma eficaz en toda la empresa.

17. Al participar la auditoría en la vigilancia del marco de gestión del riesgo operativo, el consejo deberá asegurar la independencia del auditor, que puede quedar en entredicho si participara directamente en el proceso de gestión del riesgo operativo. Los auditores pueden proporcionar información muy útil a los responsables de la gestión del riesgo operativo, pero no deben asumir directamente ninguna responsabilidad para la gestión de estos riesgos. En la práctica, el Comité reconoce que en algunos bancos (especialmente en los más pequeños) la auditoría puede estar inicialmente encargada de desarrollar un programa para la gestión del riesgo operativo, en cuyo caso, el banco en cuestión hará todo lo posible por transferir cuanto antes a otro departamento la responsabilidad diaria de esta tarea.

Principio 3: La alta gerencia deberá ser la responsable de poner en práctica el marco para la gestión del riesgo operativo aprobado por el consejo de administración. Dicho marco deberá ser aplicado de forma consistente en toda la organización bancaria y todas las categorías laborales deberán comprender sus responsabilidades al respecto. La alta gerencia también deberá ser responsable del desarrollo de políticas, procesos y procedimientos destinados a la gestión de estos riesgos para todos los productos, actividades, procesos y sistemas relevantes para el banco.

18. La gerencia del banco deberá plasmar el marco para la gestión del riesgo operativo establecido por el consejo de administración en políticas, procesos y procedimientos concretos que puedan aplicarse y comprobarse dentro de las distintas unidades de negocio. Aunque cada grado gerencial es responsable de que estas políticas, procesos, procedimientos y controles sean adecuados y efectivos en el ámbito en el que se aplican, la alta gerencia por su parte debe establecer líneas claras de autoridad, responsabilidad y comunicación para fomentar y mantener la asunción de responsabilidades, al tiempo que deberá asegurar que existen recursos suficientes para gestionar el riesgo operativo de forma eficaz. Asimismo, la alta gerencia también tendrá que evaluar si el proceso de vigilancia gerencial se adapta a los riesgos inherentes a las políticas de cada unidad de negocio.

19. La alta dirección deberá garantizar que el banco cuenta con personal cualificado que cuenten con la necesaria experiencia, aptitudes técnicas y acceso a recursos, y que la autoridad del personal encargado de controlar y asegurar el cumplimiento de las políticas para la gestión del riesgo no procede de las unidades que vigila. La dirección deberá cerciorarse de que dichas políticas han sido claramente puestas en conocimiento del personal de cualquier unidad que sea susceptible de incurrir en riesgos operativos.

20. La alta dirección deberá comprobar que el personal encargado de la gestión del riesgo operativo se comunica activamente con el que se ocupa de los riesgos de crédito, de mercado y otros, así como con aquellos empleados responsables de contratar servicios externos, como por ejemplo contratación de seguros o subcontratación. De no hacerlo así, podrían producirse vacíos o, todo lo contrario, solapamientos en el programa general de gestión del riesgo en el banco.

21. También deberá garantizar que las políticas de remuneración del banco son acordes con su apetito por el riesgo. Las políticas salariales que recompensan al empleado que se desvía de las políticas establecidas (por ejemplo, excediendo los límites permitidos) socavan los procesos de gestión de riesgos del banco.

22. Habrá que prestar especial atención a la calidad de los controles sobre la documentación y a las prácticas para realizar de las operaciones. En concreto, habrá que documentar detalladamente las políticas, procesos y procedimientos relacionados con las tecnologías avanzadas que facilitan las operaciones de mayor volumen, y dicha documentación deberá ser distribuida entre todo el personal relevante.

Gestión del riesgo: identificación, evaluación, seguimiento y cobertura/control

Principio 4: Los bancos deberán identificar y evaluar el riesgo operativo inherente a todos sus productos, actividades, procesos y sistemas relevantes. Además, también deberán comprobar que antes de lanzar o presentar nuevos productos, actividades, procesos o sistemas, se evalúa adecuadamente su riesgo operativo inherente.

23. La identificación del riesgo operativo es fundamental para el posterior desarrollo de un sistema viable de control y seguimiento del mismo. Para ello, se tienen en cuenta tanto factores internos (la estructura del banco, la naturaleza de sus actividades, la calidad de su capital humano, cambios organizativos y rotación de plantilla) como externos (cambios en el sector y avances tecnológicos) que pudieran obstaculizar el logro de los objetivos del banco.

24. Los bancos, además de identificar los riesgos potenciales más perjudiciales, deberán evaluar su vulnerabilidad ante tales riesgos, para poder así comprender mejor su perfil de riesgo y determinar con mayor precisión qué recursos necesitará para la gestión del mismo.

25. Los bancos pueden identificar y evaluar sus riesgos operativos de diversas maneras:

- Auto-evaluación o evaluación del riesgo: el banco comprueba la vulnerabilidad de sus operaciones y actividades ante el riesgo operativo. Este proceso es interno y a menudo conlleva la utilización de listas de control o de grupos de trabajo para identificar los puntos fuertes y débiles del entorno de riesgo operativo. Los cuadros de mando (*scorecards*), por ejemplo, son un instrumento para transformar las evaluaciones cualitativas en medidas cuantitativas que clasifican de forma relativa los diferentes tipos de exposiciones al riesgo operativo. Algunos indicadores pueden referirse a riesgos específicos a una línea de negocio concreta mientras que otros pueden clasificar jerárquicamente los riesgos que afectan a varias líneas. Además, se puede analizar tanto los riesgos inherentes como los controles necesarios para mitigarlos. Asimismo, los bancos pueden utilizar estos cuadros de mando para asignar el nivel de capital económico que corresponde a cada línea de negocio dependiendo de los resultados de la gestión y control de diversos aspectos del riesgo operativo.
- Asignación de riesgos (*risk mapping*): en este proceso, se agrupan por tipo de riesgo las diferentes unidades de negocio, funciones organizativas o procesos, lo que puede dejar al descubierto ámbitos que presenten deficiencias y ayudar a determinar cuáles son las prioridades para su gestión.
- Indicadores de riesgo: se trata de estadísticas o parámetros, a menudo financieros, que pueden revelar qué riesgos asume cada banco. Estos indicadores suelen ser revisados periódicamente (mensual o trimestralmente) para alertar a los bancos sobre cambios que puedan ser reveladores de problemas con el riesgo. Se suelen utilizar parámetros como el número de operaciones fallidas, las tasas de rotación de asalariados y la frecuencia y/o gravedad de los errores u omisiones.
- Cálculos: algunas empresas han comenzado a cuantificar su exposición al riesgo operativo utilizando diversos métodos. Uno de ellos es utilizar el historial de pérdidas de un banco, que puede revelar datos muy útiles para evaluar la exposición de un banco al riesgo operativo y desarrollar una política para cubrir o controlar el riesgo. Una manera muy eficaz de utilizar correctamente esta información es establecer un marco para registrar y consignar sistemáticamente la frecuencia, gravedad y otros aspectos importantes de cada caso de pérdida. Algunos bancos también combinan los datos sobre pérdidas internas con datos sobre pérdidas externas, análisis de escenarios y factores de evaluación del riesgo.

Principio 5: Los bancos deberán vigilar de forma periódica los perfiles de riesgo operativo y las exposiciones sustanciales a pérdidas. La alta gerencia y el consejo de administración deberán recibir información pertinente de forma periódica que complemente la gestión activa del riesgo operativo.

26. Para gestionar adecuadamente el riesgo operativo es fundamental contar con un proceso de seguimiento eficaz, que realizado periódicamente, puede facilitar la rápida detección y corrección de deficiencias en sus políticas, procesos y procedimientos de gestión del riesgo operativo, lo que a su vez puede reducir sustancialmente la frecuencia y gravedad de la pérdida.

27. Además de vigilar los casos de pérdidas operativas, los bancos deberán identificar indicadores que les avisen con antelación en caso de aumentar el riesgo de sufrir pérdidas en el futuro. Estos indicadores (a menudo llamados indicadores clave o indicadores de alerta temprana) deberán ser anticipatorios y reflejar las fuentes potenciales de riesgo operativo, como pueden ser un crecimiento acelerado, el lanzamiento de nuevos productos, la rotación de los efectivos, interrupciones en las operaciones, interrupciones en el sistema, etc. Cuando estos indicadores se asignan a unos límites máximos, un proceso de seguimiento eficaz puede ayudar a identificar los

principales riesgos de forma transparente y permitir que el banco reaccione ante los mismos de forma adecuada.

28. La frecuencia con la que se realice el seguimiento debe ser acorde con los riesgos potenciales así como con la frecuencia y naturaleza de los cambios en el entorno operativo. Este seguimiento deberá insertarse en las actividades del banco y sus resultados deberán incluirse en los informes presentados periódicamente a la gerencia y al consejo, al igual que debe ocurrir con los estudios sobre el cumplimiento realizados por los auditores internos y/o por los gestores de riesgos. Los informes generados por (o para) las autoridades supervisoras también pueden incluir este seguimiento y deberán distribuirse internamente entre los miembros de la alta gerencia y el consejo, según sea el caso.

29. La alta dirección deberá recibir periódicamente informes de los departamentos que corresponda, como unidades de negocios, funciones de grupo, la oficina de gestión del riesgo operativo y la auditoria interna. Estos informes sobre riesgo operativo deberán recoger información interna sobre aspectos financieros, operativos y de cumplimiento, así como información externa sobre acontecimientos y condiciones que sean pertinentes para la toma de decisiones. Los informes se distribuirán entre los niveles de gerencia adecuados y entre las áreas del banco que puedan verse afectadas. Además, deberán recoger detalladamente cualquier problemática identificada y activar una acción correctora oportuna cuando corresponda. En aras de garantizar la utilidad y fiabilidad de estos informes sobre riesgo y de auditoría, la gerencia deberá comprobar periódicamente la exactitud, precisión y relevancia de las líneas de autoridad y de los controles internos en general. También podrá utilizar informes preparados por fuentes externas (auditores, supervisores) para determinar la utilidad y fiabilidad de los informes internos. Será necesario analizar los informes con el fin de mejorar los sistemas de gestión de riesgo actuales así como para desarrollar nuevas políticas, procedimientos y prácticas a tal efecto.

30. En líneas generales, el consejo de administración deberá recibir información de alto nivel que sea suficiente para poder formarse una opinión acerca del perfil de riesgo operativo general del banco y estudiar las implicaciones estratégicas y sustanciales para su actividad.

Principio 6: Los bancos deberán contar con políticas, procesos y procedimientos para controlar y cubrir los riesgos operativos más relevantes. Además, deberán reexaminar periódicamente sus estrategias de control y reducción de riesgos y ajustar su perfil de riesgo operativo según corresponda, utilizando para ello las estrategias que mejor se adapten a su apetito por el riesgo y a su perfil de riesgo.

31. Las actividades de control están diseñadas para gestionar los riesgos operativos que el banco haya identificado[6]. El banco deberá decidir, para cada riesgo operativo sustancial que haya sido identificado, si va a utilizar procedimientos de control y/o cobertura de riesgos o bien si prefiere asumirlo. En el caso de aquellos riesgos que no se puedan controlar, el banco tendrá que decidir si los acepta, si reduce el nivel de actividad en el sector al que afectan o si cesa dicha actividad completamente. Habrá que establecer procesos y procedimientos de control y los bancos deberán contar con un sistema que asegure el cumplimiento de un conjunto de políticas internas perfectamente documentadas para la gestión del riesgo. Para ello, habrá que tener en cuenta una serie de factores básicos:

- Estudios de alto nivel sobre el progreso realizado por el banco para alcanzar los objetivos descritos;
- Comprobación del cumplimiento de los controles gerenciales;
- Políticas, procesos y procedimientos para el análisis, tratamiento y resolución de casos de incumplimiento; y
- Un sistema de aprobaciones y autorizaciones documentadas que aseguren la asunción de responsabilidades ante la categoría directiva más adecuada.

[6] Para saber más al respecto, véase *Framework for Internal Control Systems in Banking Organisations*, Basel Committee on Banking Supervision, septiembre de 1998.

32. Aunque es fundamental contar con un marco de políticas y procedimientos formales por escrito, éste debe reforzarse mediante un estricto control que promueva unas buenas prácticas de gestión del riesgo. Tanto el consejo de administración como la alta gerencia deberán establecer una sólida cultura de control interno, en la que las actividades de control formen parte integral de la actividad diaria del banco, de modo que pueda responderse rápidamente ante cualquier cambio de circunstancias y evitar costes innecesarios.

33. También es necesaria una correcta segregación de las ocupaciones, de modo que ningún empleado asuma responsabilidades que puedan generar un conflicto de intereses, ya que en ese caso, sería más fácil encubrir pérdidas, errores o actuaciones impropias. Por lo tanto, habrá que identificar qué áreas pueden generar conflictos de intereses para intentar reducirlos al máximo y aplicar estrictas medidas de seguimiento y comprobación independientes.

34. Además de la segregación de funciones, los bancos deberán garantizar la existencia de otras prácticas internas igualmente adecuadas para controlar el riesgo operativo, como pueden ser:

- Comprobación minuciosa del respecto a los límites o máximos asignados para el riesgo;
- Establecimiento de salvaguardias para acceder a los activos y archivos del banco y utilizarlos;
- Personal con la experiencia y formación adecuadas;
- Identificación de líneas de negocio o productos en los que el rendimiento se aleje bastante de lo razonablemente esperado (por ejemplo, cuando una operación que supuestamente conlleva poco riesgo y escaso margen genera un alto rendimiento, de modo que se pueda poner en duda si se han alcanzado estos beneficios infringiendo algún control interno); y
- Comprobación y conciliación periódicas de las operaciones y de las cuentas.

En los últimos años, algunos bancos han sufrido importantes pérdidas operativas por no haber llevado a cabo estas prácticas adecuadamente.

35. El riesgo operativo puede ser más grave cuando los bancos realizan actividades nuevas o lanzan nuevos productos (especialmente cuando así contradicen las estrategias de los principales negocios del banco), participan en mercados que desconocen o realizan negocios en lugares lejanos. Asimismo, en muchos de estos casos, las empresas no pueden garantizar que la infraestructura para la gestión del riesgo pueda seguir el ritmo de crecimiento de la actividad bancaria. En los últimos años, se han producido enormes pérdidas muy conocidas por la existencia de una o más de estas circunstancias. En estos casos, por lo tanto, les compete a los bancos comprobar que se presta especial atención a las actividades de control interno

36. Algunos riesgos operativos significativos tienen pocas probabilidades de producirse, pero sus repercusiones financieras podrían ser enormes, a lo que se añade que no todos los eventos de riesgo están controlados (ej. desastres naturales). Se pueden utilizar herramientas o programas de cobertura del riesgo para reducir la exposición a los mismos, así como su frecuencia y gravedad. Por ejemplo, las pólizas de seguros, especialmente las que contienen cláusulas de pronto pago o de pago garantizado, pueden ayudar a externalizar el riesgo de que se produzcan pérdidas “poco frecuentes y de enorme gravedad” por reclamaciones de terceros a raíz de de errores u omisiones, extravíos de títulos valores, fraude por parte de empleados o terceros y desastres naturales.

37. Ahora bien, los bancos deben utilizar estas herramientas de cobertura de riesgos como un complemento (y no un sustituto) de las medidas de control interno del riesgo operativo. Si se cuenta con los mecanismos adecuados para reconocer los errores operativos rápidamente y subsanarlos, es posible reducir considerablemente la exposición a este tipo de riesgos. Además, también habrá que considerar cuidadosamente hasta qué punto este tipo de coberturas ante riesgos (como los seguros) realmente reducen el riesgo o más bien lo trasladan a otros sectores de actividad del banco o incluso generan nuevos riesgos (ej. riesgo legal o de contraparte).

38. Para mitigar estos riesgos, también es importante invertir en tecnologías adecuadas para el procesamiento y tratamiento de la información, así como en sistemas de seguridad. Sin embargo, los bancos deben ser conscientes de que una mayor automatización puede transformar las pérdidas más frecuentes y de mayor gravedad en pérdidas menos frecuentes pero de extrema gravedad, que pueden derivarse de suspensiones o interrupciones prolongadas de los servicios a causa de factores internos o a factores que escapen al control inmediato del banco (ej. acontecimientos externos). Estos problemas pueden poner en serias dificultades a los bancos y hacer peligrar la capacidad de la

institución para desempeñar sus principales actividades. Tal y como se especifica en el Principio 7, tras un desastre los bancos deben establecer planes de recuperación y de continuidad de la actividad para poder sobreponerse a estos riesgos.

39. Los bancos también deberán establecer políticas para la gestión de los riesgos derivados de las actividades de subcontratación. La subcontratación puede mejorar el perfil de riesgo de la institución al transferir actividades a otras empresas con mayor experiencia y en mejor disposición de gestionar los riesgos que llevan consigo estas actividades especializadas. Sin embargo, la utilización de terceros por parte del banco no disminuye la responsabilidad del consejo de administración ni de la alta gerencia de asegurar que la tarea subcontratada se realiza de forma correcta y segura, de conformidad con las leyes vigentes. Los acuerdos de subcontratación se pueden plasmar en contratos vinculantes o en acuerdos de provisión de servicios que aseguren una clara distribución de tareas entre los proveedores del servicio y el banco que subcontrata. Además, éste último tendrá que gestionar los riesgos residuales que llevan asociados este tipo de acuerdos, incluida la interrupción del servicio.

40. Dependiendo de la importancia y naturaleza de la actividad en cuestión, los bancos tendrán que conocer qué repercusiones podría tener para sus operaciones y sus clientes una deficiencia cualquiera en los servicios prestados por sus proveedores o por proveedores externos o intragrupo, como podría ser un fallo operativo o la quiebra o incumplimiento por parte de un tercero. El consejo y la gerencia deberán comprobar que se hayan definido y comprendido claramente las expectativas y obligaciones de cada una de las partes y que su cumplimiento haya quedado asegurado. Durante la evaluación de riesgos, también habrá que considerar explícitamente los límites de la responsabilidad de terceros frente al banco, así como su capacidad financiera para indemnizarlo en concepto de errores, negligencia o cualquier otro fallo operativo. Los bancos, por su parte, deberán realizar una prueba preliminar para comprobar la debida diligencia y controlar las actividades de los proveedores externos, especialmente aquellos con menos experiencia en cuanto a regulación bancaria, y tendrán que revisar este proceso (incluyendo el análisis de la debida diligencia) de forma periódica. En el caso de actividades críticas, el banco tal vez deba elaborar planes de emergencia en los que se detalle la disponibilidad de recursos externos alternativos y los costes y recursos necesarios para transferirles la actividad, posiblemente con muy poca antelación.

41. En algunos casos, los bancos pueden optar por aceptar cierto nivel de riesgo operativo o bien por asegurarse frente a éste por sí mismo. Cuando así sea, si el riesgo en cuestión es sustancial, la decisión de aceptar el riesgo o asegurarse frente al mismo deberá ser adoptada con total transparencia en el seno de la organización y deberá estar en la línea de la estrategia general del banco y de su apetito por el riesgo.

Principio 7: Los bancos deberán contar con planes de contingencia y de continuidad de la actividad, que aseguren su capacidad operativa continua y que reduzcan las pérdidas en caso de interrupción grave de la actividad.

42. Por razones ajenas al banco, un acontecimiento grave puede impedirle cumplir alguna de sus obligaciones (o todas), especialmente cuando se hayan visto afectadas sus estructuras físicas, informáticas o sus telecomunicaciones. Esto, a su vez, puede provocar pérdidas significativas para el banco e incluso afectar al sistema financiero en general a través de su sistema de pagos, por lo que los bancos deben establecer tras una catástrofe planes de recuperación y de continuidad de la actividad que consideren distintos supuestos factibles que hagan más vulnerable al banco; estos planes deberán ser acordes al tamaño y complejidad de sus operaciones.

43. Los bancos deberán identificar cuáles son sus procesos más críticos, incluidos aquellos en los que se dependa de distribuidores externos u otras terceras partes, para los cuales será fundamental la reanudación inmediata del servicio. Para estos procesos, el banco deberá identificar mecanismos alternativos para reanudar el servicio en caso de una interrupción del mismo, prestando especial atención a la capacidad de recuperar archivos físicos o electrónicos indispensables para la reanudación de la actividad. Cuando se realicen copias de seguridad de estos archivos en un lugar externo al banco o cuando éste deba trasladar sus operaciones a una nueva instalación, habrá que intentar que estos lugares se encuentren a una distancia adecuada del lugar que se ha visto afectado, para evitar que ambas instalaciones estén fuera de servicio al mismo tiempo.

44. Los bancos deberán comprobar periódicamente sus planes de recuperación y de continuidad del negocio para catástrofes, para que estén en la línea de las operaciones actuales del banco y de sus estrategias de negocio. Asimismo, estos planes deberán ser puestos a prueba cada

cierto tiempo para comprobar si el banco sería capaz de reanudar su actividad en el improbable caso de que se produjera una alteración grave de su negocio.

La función de los supervisores

Principio 8: Los supervisores bancarios deberán exigir a todos los bancos, sea cual sea su tamaño, que mantengan un marco eficaz para identificar, evaluar, seguir y controlar o mitigar sus riesgos operativos más relevantes, como parte de su aproximación general a la gestión de riesgos.

45. Los supervisores deberán exigir que los bancos desarrollen marcos para la gestión del riesgo operativo que sean acordes con las pautas recogidas en este informe y con su tamaño, complejidad y perfil de riesgo. En la medida que los riesgos operativos ponen en peligro la seguridad y solidez de los bancos, los supervisores tienen la obligación de instar a los bancos a desarrollar y utilizar las mejores técnicas posibles para la gestión de estos riesgos.

Principio 9: Los supervisores deberán realizar, directa o indirectamente, una evaluación periódica independiente de las políticas, prácticas y procedimientos con los que cuentan los bancos para gestionar sus riesgos operativos. Además, deberán cerciorarse de que se han puesto en marcha los mecanismos necesarios para estar al tanto de cualquier novedad que se produzca en un banco.

46. Cuando los supervisores evalúen independientemente el riesgo operativo, deberán examinar los siguientes aspectos:

- La eficacia del proceso de gestión del riesgo del banco y de su entorno de control global del riesgo operativo;
- Los métodos que utiliza el banco para vigilar e informar sobre su perfil de riesgo operativo, incluidos los datos sobre pérdidas operativas y otros indicadores de posibles riesgos operativos;
- Los procedimientos que sigue el banco para solucionar rápida y eficazmente los casos de riesgo operativo y subsanar su vulnerabilidad ante el riesgo.
- Los controles, auditorías y exámenes internos que realiza el banco para garantizar la integridad de la gestión general del riesgo operativo.
- La eficacia de los esfuerzos del banco para mitigar estos riesgos, por ejemplo mediante la utilización de seguros;
- La calidad y minuciosidad de los planes del banco para recuperarse de una catástrofe y continuar con sus actividades; y
- El proceso que sigue el banco para determinar si sus niveles de capital son adecuados para hacer frente al riesgo operativo teniendo en cuenta su perfil de riesgo y, si procede, sus límites internos de capital.

47. Los supervisores también deberán cerciorarse de que los bancos que forman parte de un grupo financiero cuentan con procedimientos que garanticen una gestión del riesgo operativo adecuada e integrada en todo el grupo. Para ello, puede ser necesario cooperar y compartir información con otros supervisores, en virtud de los procedimientos establecidos, e incluso algunos supervisores pueden decidir que sean auditores externos los que lleven a cabo estos procesos de evaluación.

48. Si se detectan deficiencias durante este examen supervisor, podrán subsanarse mediante una serie de mecanismos, utilizando los supervisores los que mejor se adapten a las circunstancias concretas del banco y a su entorno operativo. Para poder recibir la información reciente sobre el riesgo operativo, los supervisores podrán establecer mecanismos de transmisión de información directa con bancos y auditores externos (por ejemplo, se puede poner periódicamente a disposición de los supervisores los informes sobre la gestión interna del riesgo operativo en un banco).

49. En general, se reconoce que muchos bancos todavía están desarrollando procesos para la gestión de sus riesgos operativos, por lo que los supervisores deben promover activamente el continuo desarrollo interno de estos controles mediante su seguimiento y evaluación de los últimos avances de los bancos y de sus planes de desarrollo. Estos esfuerzos se pueden comparar después con los que estén realizando otros bancos, de modo que se obtenga así una clara impresión del estado en el que se encuentra su labor actual. Asimismo, teniendo en cuenta que se han identificado

algunas causas por las que los esfuerzos de algunos bancos no han dado sus frutos, se podría ofrecer dicha información en términos generales para ayudar a desarrollar el proceso de planificación. Además, los supervisores deberán comprobar hasta qué punto el banco ha integrado sus procesos para la gestión del riesgo operativo en su organización con el fin de asegurar una correcta gestión de estos riesgos en todos los niveles organizativos, presentar unas líneas inequívocas de comunicación y responsabilidad, así como fomentar la auto-evaluación activa de sus prácticas y la consideración de posibles mejoras para la cobertura de riesgos.

La función de la divulgación de información

Principio 10: Los bancos deberán proporcionar información pública suficiente para que los partícipes del mercado puedan evaluar sus estratégicas de gestión del riesgo operativo.

50. El Comité estima que, cuando los bancos divulgan información relevante de forma frecuente y oportuna, se mejora sustancialmente la disciplina de mercado y, por ende, se consigue una gestión de riesgos más eficaz. Para determinar cuánta información se debe que divulgar, habrá que tener en cuenta el volumen, perfil de riesgo y complejidad de las operaciones del banco.

51. Este ámbito de divulgación todavía no está bien asentado, principalmente porque los bancos todavía están desarrollando sus técnicas de evaluación de riesgos operativos. Sin embargo, el Comité considera que los bancos deben informar acerca de su marco para la gestión de esos riesgos, de modo que los inversionistas y las contrapartes puedan determinar si dicho banco es eficaz a la hora de identificar, evaluar, vigilar y controlar o cubrir sus riesgos operativos.