



Munich Personal RePEc Archive

**Sound practices for the management of  
operational risk in financial institutions  
(in Spanish)**

Cristina Pailhé and Miguel Delfiner and Ana Mangialavori

Central Bank of Argentina

January 2007

Online at <http://mpa.ub.uni-muenchen.de/1803/>  
MPRA Paper No. 1803, posted 16. February 2007

# Buenas prácticas para la administración del riesgo operacional en entidades financieras

*Miguel Delfiner, Ana Mangialavori y Cristina Pailhé<sup>1</sup>*

*Enero 2007*

## Resumen

El Comité de Supervisión Bancaria de Basilea (BCBS) definió al riesgo operacional (RO) como el riesgo de pérdidas resultantes de la inadecuación o fallas en los procesos internos, las personas, los sistemas o por eventos externos. Esa definición incluye al riesgo legal, pero excluye el riesgo estratégico y reputacional. Tradicionalmente, la gestión de los ROs individuales ha sido una parte importante del esfuerzo de los bancos por evitar el fraude y mantener la integridad de los controles internos, entre otros aspectos. Sin embargo, lo que resulta relativamente nuevo es considerar a la gestión del RO como una *práctica integral* comparable a la gestión de otros riesgos (como riesgo crediticio o de mercado) a la vez que *medir* las pérdidas provenientes de eventos de RO y *exigir capital regulatorio* para afrontarlas. Habiéndose consolidado el RO como una categoría integral de riesgo, el BCBS ha dictado una serie de principios o buenas prácticas internacionalmente aceptadas para su gestión y supervisión en entidades financieras. Este documento analiza esas *mejores prácticas* y su aplicación en las estructuras de bancos internacionales. Asimismo, se analizan las regulaciones de una muestra de países latinoamericanos que han emitido normas sobre buenas prácticas en la materia. Se debe destacar que los principales países de la región han elaborado normativa tendiente a implementar estructuras de gestión del RO en las entidades financieras, basada en las recomendaciones y principios del BCBS.

---

<sup>1</sup> Miguel Delfiner ([mdelfiner@bcra.gov.ar](mailto:mdelfiner@bcra.gov.ar)) es Analista Principal, Ana Mangialavori ([amangialavori@bcra.gov.ar](mailto:amangialavori@bcra.gov.ar)) es Analista Senior y Cristina Pailhé ([cpailhe@bcra.gov.ar](mailto:cpailhe@bcra.gov.ar)) es Gerente de Investigación y Planificación Normativa, Subgerencia General de Normas, BCRA. Las opiniones vertidas en este trabajo corresponden a los autores y no representan una posición oficial del Banco Central de la República Argentina. Se agradece especialmente a José Rutman por el apoyo brindado para la realización de este trabajo, así como a todos aquellos que contribuyeron con sus opiniones y comentarios a versiones preliminares del documento. Los errores remanentes son exclusiva responsabilidad de los autores.

## Indice

1. [Introducción](#)
2. [Los estándares internacionales](#)
  - 2.1. [Las buenas prácticas de administración y supervisión del RO propuestas por el Comité de Supervisión Bancaria de Basilea](#)
  - 2.2. [Principios Básicos para una Supervisión Bancaria Efectiva](#)
  - 2.3. [El tratamiento del RO en Basilea II](#)
    - 2.3.1. [Pilar I: Criterios de admisión para el uso de los distintos métodos](#)
    - 2.3.2. [Pilar II: Proceso de revisión del supervisor](#)
    - 2.3.3. [Pilar III: Disciplina de mercado](#)
3. [La gestión del RO en las entidades financieras](#)
  - 3.1. [Prácticas observadas en la administración del RO](#)
  - 3.2. [Evaluación del RO a través del uso de datos internos](#)
  - 3.3. [Evaluación del riesgo a través del uso de factores claves del control interno y del entorno de negocios](#)
  - 3.4. [Mitigación del RO y estimación del capital](#)
4. [Las regulaciones sobre \*buenas prácticas\* en países latinoamericanos](#)
  - 4.1. [Brasil](#)
  - 4.2. [Chile](#)
  - 4.3. [Colombia](#)
    - 4.3.1. [Etapas de la administración del RO](#)
    - 4.3.2. [Elementos del sistema de administración del RO](#)
  - 4.4. [México](#)
  - 4.5. [Perú](#)
    - 4.5.1. [Administración de los aspectos que originan el RO](#)
    - 4.5.2. [Requerimientos de información](#)
5. [Conclusiones](#)

[Anexo:](#) Resumen de requisitos establecidos por la Superintendencia Financiera de Colombia

[Referencias bibliográficas](#)

## 1. Introducción

Hasta hace tiempo atrás, era usual que se definiese al *Riesgo Operacional* (RO) de forma imprecisa, comprendiendo a una serie de “otros riesgos” no explícitamente tratados, entendidos y administrados en las entidades financieras de manera integral, como tradicionalmente lo han sido por ejemplo el riesgo de crédito (RC) y el riesgo de mercado (RM). Las ideas y aspectos individuales que están detrás del concepto de RO no son nuevos en el sistema financiero, sino que forman parte de un conocimiento gerencial ya existente y las entidades financieras tradicionalmente han descansado en procesos internos, programas de auditoría, uso de pólizas de seguros y otras herramientas de administración de riesgos, para atacar distintos aspectos que están dentro del ámbito de lo que hoy comprende el concepto de RO.

En los últimos tiempos ha habido una creciente preocupación por el RO y sus consecuencias, tanto por parte de las propias entidades financieras como por parte de los reguladores. El *Comité de Supervisión Bancaria de Basilea* (“el Comité” o “BCBS”, por sus siglas en inglés) ha señalado<sup>2</sup> que la desregulación y la globalización de los servicios financieros, junto con la creciente sofisticación de las tecnologías financieras, han tornado más complejas las actividades de los bancos a la vez que han aumentado sus perfiles de riesgo, lo que hace que se vean expuestos a nuevos riesgos que surgen de factores tales como:

- el uso creciente de tecnologías automatizadas;
- una mayor importancia de la integración de tecnologías informáticas y servicios compartidos entre entidades;
- el crecimiento del comercio electrónico;
- las adquisiciones, fusiones, escisiones y consolidaciones a gran escala;
- la complejidad creciente de productos y servicios;
- la proliferación de técnicas de mitigación de los riesgos de mercado y de crédito;
- la creciente utilización de acuerdos de “*outsourcing*”;
- la mayor participación en los sistemas de compensación y liquidación.

Estos factores, sumados al aumento en todo el mundo de pérdidas generadas por eventos de RO, han llevado a los bancos y supervisores a considerar a la gestión de este tipo de riesgo como una disciplina integral, como ya ha ocurrido en otros sectores de actividad.

En el año 2003 el BCBS publicó una serie de *principios* sobre buenas prácticas para la administración del RO, lo que sentó uno de los principales precedentes del tratamiento del RO como categoría de riesgo. Posteriormente, en junio de 2004, el BCBS publicó el documento “*International Convergence of Capital Measurement and Capital Standards. A revised framework*” (“*Basilea II*” o “*Nuevo Marco de Capitales*”) el cual se ha tornado una referencia ineludible a la hora de hablar y entender el concepto de RO y en el que por primera vez se fija un cargo de capital para atender a las pérdidas provenientes de eventos de RO. En ese documento, el BCBS adoptó una definición específica de lo que se entiende por RO, la cual resultó del consenso de reguladores y la industria: “... *el riesgo operacional es el riesgo de pérdidas resultantes de la inadecuación o fallas en los procesos internos, las personas o los sistemas o por*

---

<sup>2</sup> BCBS (2003).

*eventos externos. Esa definición incluye al riesgo legal, pero excluye el riesgo estratégico y reputacional*”<sup>3</sup>. Además de incluir el aspecto particular de la *medición* del capital regulatorio por RO, Basilea II marca un hito, ya que señala como precondition para la cuantificación de ese riesgo, la *aplicación efectiva de las buenas prácticas* contenidas en el documento de 2003.<sup>4</sup> Adicionalmente, en octubre 2006, el BCBS publicó la versión revisada de los *Principios Básicos para una Supervisión Bancaria Efectiva*,<sup>5</sup> la cual contiene un principio específico dedicado al RO.

Al revisar la evolución de los estándares internacionales y las prácticas de la industria a lo largo de los últimos años, puede afirmarse que son principalmente dos los aspectos que han surgido como novedosos en el tratamiento del RO: el primero, como se expresara anteriormente, es el de considerarlo como una categoría de riesgo bien definida que requiere una gestión integral al igual que ocurre con otros típicos riesgos bancarios. El segundo aspecto que es novedoso es el hecho de *medir* las pérdidas ocasionadas por el RO y requerir capital para afrontarlas. La publicación de Basilea II hizo que muchas veces las discusiones se centraran en el aspecto específico de la medición y en los métodos allí propuestos. Sin embargo, no debe perderse de vista que, como se expresó antes, Basilea II también incorpora la primera de las cuestiones, esto es, la necesidad de contar con buenas prácticas de gestión y supervisión del RO como precondition para aplicar metodologías de medición.

El objetivo de este trabajo es revisar las buenas prácticas sugeridas por los estándares internacionales para la administración y supervisión del RO y la manera en que esos *principios* se han plasmado en la regulación de una serie de países, así como la forma concreta en que se reflejan en la estructura y organización de las entidades financieras. No se profundizará aquí en los aspectos relacionados con la medición del RO en función de los enfoques propuestos por Basilea II, más allá de los aspectos puntuales que se relacionan con las buenas prácticas en la materia.<sup>6</sup>

El documento está organizado de la siguiente manera. En la sección 2 se recopilan las recomendaciones del BCBS, exponiendo los principios específicos aplicables a la gestión y supervisión del RO, como así también lo dispuesto en los *Principios Básicos para una Supervisión Bancaria Efectiva* y el tratamiento que se dispensa a las buenas prácticas de gestión y supervisión del RO en cada uno de los *Pilares* de Basilea II. La sección 3 expone resultados de relevamientos internacionales respecto de las estructuras organizacionales que las entidades financieras han desarrollado para la gestión del RO. Estas estructuras dependen de varios factores, entre ellos de cómo las entidades definen el RO y su vinculación con el ambiente de control del banco. A ello se agrega, una vez definidas las estructuras, la manera en que los bancos pueden medir el RO.

La sección 4 refiere al estudio de la regulación sobre buenas prácticas para la administración y supervisión del RO en una muestra de países latinoamericanos que ha dictado normativa específica al respecto, la mayoría de las cuales recogen los *principios* del BCBS. Por último, en la Sección 5 se exponen las conclusiones.

---

<sup>3</sup> BCBS (2004).

<sup>4</sup> Excepto para el método de medición más sencillo (Enfoque de Indicador Básico) para el cual se *recomienda* la adopción de los principios contenidos en BCBS (2003).

<sup>5</sup> BCBS (2006-a y 2006-b).

<sup>6</sup> Para una revisión de metodologías de medición del RO, ver BCRA (2006-a).

## 2. Los estándares internacionales

### 2.1. Las buenas prácticas de administración y supervisión del RO propuestas por el Comité de Supervisión Bancaria de Basilea

En febrero de 2003 el BCBS publicó el documento “*Sound Practices for the Management and Supervision of Operational Risk*”<sup>7</sup> en donde se establece una serie de principios para una gestión y supervisión eficaz del RO, de modo que los bancos y autoridades supervisoras puedan utilizarlos al evaluar políticas y prácticas destinadas a gestionar este tipo de riesgos. El Comité reconoce que en la práctica, el enfoque exacto elegido por cada entidad para la administración del RO dependerá de una variedad de factores, incluyendo su tamaño y sofisticación y la naturaleza y complejidad de sus actividades. Sin embargo, no obstante esas diferencias, se destaca la existencia de varios elementos que resultan cruciales para un esquema efectivo de administración del RO para bancos de cualquier tamaño y alcance. Esos elementos son:

- **estrategias** claramente definidas y su seguimiento por parte del consejo de administración y de la alta gerencia;
- una sólida **cultura de gestión** del RO y de **control** interno (incluyendo entre otras cosas, líneas claras de responsabilidad y segregación de funciones) y;
- herramientas eficaces para la transmisión interna de **información** y **planes de contingencia**.

A pesar de que existan diferencias de criterio entre los bancos en cuanto a sus definiciones internas del RO, es importante que abarquen el amplio abanico de RO a los que se enfrentan y que recojan las principales causas de pérdidas operativas graves. Los principales *eventos de RO* que ha identificado el BCBS, en conjunto con la banca, como posibles causantes de pérdidas sustanciales son:

- **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

---

<sup>7</sup> BCBS (2003).

acceso no autorizado a las cuentas de los clientes, prácticas inadecuadas de contrapartes distintas de clientes, litigios con distribuidores, etc.

El Comité destaca que la gestión de ROs 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 a la gestión del RO como una práctica integral comparable a la gestión del RC o RM*, aún cuando ello no siempre se manifieste en la práctica. Las tendencias antes mencionadas, unidas al aumento en todo el mundo de casos muy conocidos de pérdidas por RO, 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.<sup>8</sup>

El BCBS subraya que en el pasado, los bancos gestionaban sus ROs 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 RO. En este sentido, son cada vez más las instituciones convencidas de que los programas de gestión del RO proporcionan seguridad y solidez al banco, por lo que están avanzando para tratarlo como un tipo de riesgo específico. El BCBS estima que el intercambio de ideas entre supervisores y banqueros es fundamental para poder desarrollar pautas adecuadas para la gestión de los ROs.

Al desarrollar sus buenas prácticas, el Comité ha partido de su labor anterior sobre la gestión de otros riesgos bancarios significativos, como el RC, riesgo de tasa de interés o de liquidez, convencido de que es necesario tratar al RO con el mismo rigor que se aplica a esos riesgos. Sin embargo, no cabe duda de que el RO difiere de esos otros riesgos bancarios en algunos aspectos 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 repercute en el proceso de gestión. Al mismo tiempo, si el RO no se controla adecuadamente, puede verse afectado el perfil de riesgo de la institución, lo que podría exponerla a pérdidas significativas.

Por “*gestión del RO*” el BCBS entiende a la “*identificación, evaluación, seguimiento y control/cobertura*” de este riesgo. Esta definición contrasta con la que el Comité había adoptado en oportunidades anteriores sobre gestión del riesgo, que hacía referencia a la “*identificación, cálculo, seguimiento y control*” del riesgo. Al igual que en sus trabajos sobre otros riesgos bancarios, el BCBS ha estructurado una serie de *Principios*, agrupados en cuatro áreas:

- desarrollo de un marco adecuado para la gestión del riesgo;
- gestión del riesgo: identificación, evaluación, seguimiento y control /mitigación;
- el rol de los supervisores;
- el rol de la divulgación de información.

---

<sup>8</sup> BCBS (2003).

## Cuadro 1: Buenas Prácticas para la gestión y supervisión del RO<sup>9</sup>

<b>Desarrollo de un marco adecuado para la gestión del riesgo</b>
<p><b>Principio 1:</b> El consejo de administración deberá conocer cuáles son los principales aspectos de los ROs 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 RO válida para toda la empresa y establecer los principios para definir, evaluar, monitorear y controlar o mitigar este tipo de riesgo.</p> <p><b>Principio 2:</b> El consejo de administración deberá asegurar que el marco para la gestión del RO 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 RO.</p> <p><b>Principio 3:</b> La alta gerencia deberá ser la responsable de poner en práctica el marco para la gestión del RO 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 con respecto a la administración del RO. 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.</p>
<b>Gestión del riesgo: identificación, evaluación, seguimiento y cobertura/ control</b>
<p><b>Principio 4:</b> Los bancos deberán identificar y evaluar el RO 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 RO inherente.</p> <p><b>Principio 5:</b> Los bancos deberán vigilar periódicamente los perfiles de RO y las exposiciones sustanciales a pérdidas. La alta gerencia y el consejo de administración deberán recibir información pertinente de forma periódica que complementa la gestión activa del RO.</p> <p><b>Principio 6:</b> Los bancos deberán contar con políticas, procesos y procedimientos para controlar y cubrir los ROs más relevantes. Además, deberán reexaminar periódicamente sus estrategias de control y reducción de riesgos y ajustar su perfil de RO según corresponda, utilizando para ello las estrategias que mejor se adapten a su apetito por el riesgo y a su perfil de riesgo.</p> <p><b>Principio 7:</b> 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.</p>
<b>El rol de los supervisores</b>
<p><b>Principio 8:</b> 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 ROs más relevantes, como parte de su aproximación general a la gestión de riesgos.</p> <p><b>Principio 9:</b> 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 ROs. 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.</p>
<b>El rol de la divulgación de información</b>
<p><b>Principio 10:</b> Los bancos deberán proporcionar información pública suficiente para que los partícipes del mercado puedan evaluar sus estrategias de gestión del RO.</p>

<sup>9</sup> BCBS (2003), versión en español. El Comité aclara que se hace referencia a una estructura de gestión bancaria compuesta por un consejo de administración y una alta dirección, aunque se entiende que los marcos jurídicos y regulatorios difieren entre países en cuanto a las funciones que ostenta cada uno.



## 2.2. Principios Básicos para una Supervisión Bancaria Efectiva <sup>10</sup>

Los *Principios Básicos para una Supervisión Bancaria Efectiva* (“*Basel Core Principles*”, BCP) son considerados un marco de estándares mínimos sobre buenas prácticas de supervisión y son universalmente aplicables y aceptados. El BCBS redactó los BCP y su “*Metodología*” como una contribución para fortalecer el sistema financiero global y han sido utilizados por los países como un “*benchmark*” para evaluar la calidad de sus sistemas de supervisión y para identificar las áreas de trabajo futuro a efectos de alcanzar un nivel sólido de prácticas supervisoras. La experiencia ha demostrado que la realización de autoevaluaciones respecto al grado de cumplimiento de los BCP ha sido útil para que las autoridades identifiquen las fallas y establezcan prioridades para remediarlas.<sup>11</sup>

En este sentido, una de las innovaciones realizadas en el nuevo documento de los BCP publicado en 2006 <sup>12</sup> (que actualiza al original del año 1997), fue la incorporación de un *principio* íntegramente dedicado al RO. Este riesgo es tratado el *Principio N° 15* con una visión *integral* y no como ocurría en los BCP anteriores, en los que formaba parte de un concepto global de riesgo (que incluía riesgos de liquidez, de tasa de interés, etc.).

El *BCP N° 15* establece que: **“Los supervisores deben tener constancia de que los bancos cuentan con políticas y procesos de gestión de riesgos para identificar, evaluar, vigilar y controlar/mitigar el riesgo operacional. Estas políticas y procesos han de ser proporcionales a las dimensiones y complejidad del banco en cuestión”**.

Para la evaluación de este *principio*, el Comité cita como documentos de soporte al analizado en la Sección anterior, “*Sound practices for the management and supervision of operational risk*”<sup>13</sup> y “*Outsourcing in financial services*”, un documento realizado por el Joint Forum.<sup>14</sup>

Como puede verse, el concepto de *gestión* contenido en los BCPs es el mismo que se encuentra en el documento de sanas prácticas del BCBS, en cuanto se refiere a “*identificar, evaluar, vigilar y controlar / mitigar*” al RO, a la vez que los “*Criterios Esenciales*” recogen las buenas prácticas del documento del BCBS del año 2003 (ver Cuadro 2 a continuación).

---

<sup>10</sup> BCBS (2006-a).

<sup>11</sup> BCBS (2006-a y 2006-b).

<sup>12</sup> BCBS (2006-a) y (2006-b).

<sup>13</sup> BCBS (2003).

<sup>14</sup> Joint Forum (2005). El *Joint Forum* fue establecido en 1996 y está conformado por el *Basel Committee on Banking Supervision* (BCBS), la *International Organization of Securities Commissions* (IOSCO) y la *International Association of Insurance Supervisors* (IAIS) para tratar aspectos comunes a los sectores de bancos, valores y seguros, incluyendo la regulación de los conglomerados financieros.

## Cuadro 2: Principio Básico Nro.15 - Riesgo Operacional<sup>15</sup>

<b>Principio básico para una supervisión efectiva del RO</b>
<p><i>“Los supervisores deben tener constancia de que los bancos cuentan con políticas y procesos de gestión de riesgos para identificar, evaluar, vigilar y controlar / mitigar el RO. Estas políticas y procesos han de ser proporcionales a las dimensiones y complejidad del banco en cuestión”.</i></p>
<b>Criterios Esenciales</b>
<ol style="list-style-type: none"><li>1. El supervisor exige que los bancos cuenten con políticas y procesos de gestión de riesgos para identificar, evaluar, vigilar y mitigar el RO. Dichas políticas y procedimientos han de ser acordes a las dimensiones y complejidad de las operaciones del banco, debiendo confirmar el supervisor que se ajustan periódicamente según cambia el perfil de riesgo del banco y las condiciones en el mercado externo.</li><li>2. El supervisor exige que las estrategias, políticas y procesos de los bancos para la gestión del RO sean aprobados y revisados periódicamente por el consejo. También exige que el consejo vigile a la dirección del banco al asegurar que dichas políticas y procesos se aplican adecuadamente.</li><li>3. El supervisor tiene constancia de que la dirección del banco aplica en la práctica la estrategia aprobada y las políticas y procesos significativos para el RO.</li><li>4. El supervisor comprueba la calidad y exhaustividad de los planes de contingencia y de reanudación de la actividad del banco para tener constancia de que en caso de alteraciones graves de la actividad, el banco es capaz de operar sin interrupciones y con pérdidas mínimas (incluidas las que pueden producirse a raíz de alteraciones en los sistemas de pago y liquidación).</li><li>5. El supervisor determina que los bancos cuentan con políticas y procesos adecuados para las tecnologías informáticas sobre aspectos como la seguridad de la información y el desarrollo de los sistemas y que han invertido en dichas tecnologías en proporción al tamaño y complejidad de sus operaciones.</li><li>6. El supervisor exige que haya mecanismos de notificación adecuados que le mantengan al día de cualquier cambio que afecte al RO de los bancos de su jurisdicción.</li><li>7. El supervisor confirma que el riesgo legal se tiene en cuenta en los procesos del banco para la gestión del RO.</li><li>8. El supervisor determina que el banco ha establecido políticas y procesos adecuados para evaluar, gestionar y vigilar las actividades subcontratadas. El programa para gestionar el riesgo de subcontratación deberá:<ul style="list-style-type: none"><li>• aplicar la debida diligencia al seleccionar posibles proveedores de servicios;</li><li>• estructurar el mecanismo de subcontratación;</li><li>• gestionar y vigilar los riesgos relacionados con los mecanismos de subcontratación;</li><li>• asegurar un entorno eficaz de control y;</li><li>• establecer planes de contingencia viables.</li></ul></li></ol>
<p>Las políticas y procesos de subcontratación deben exigir que la institución cuente con exhaustivos contratos y/u otros acuerdos de prestación de servicios que distribuyan claramente las responsabilidades entre la empresa subcontratada y el banco.</p>
<b>Criterios Adicionales</b>
<ol style="list-style-type: none"><li>1. El supervisor determina que las políticas y procesos de gestión de riesgos cubren los principales aspectos del RO, incluyendo un marco adecuado al respecto que se aplica en todo el grupo. Estas políticas y procesos han de incluir otros riesgos que predominan en determinadas actividades con un gran componente operativo, como la actividad de custodia y de correspondencia, al tiempo que deberán cubrir períodos en los que aumente el riesgo operacional.</li></ol>

<sup>15</sup> BCBS (2006-b) versión en español publicada por el Comité.

## 2.3. El tratamiento del RO en Basilea II

### 2.3.1. Pilar I: criterios de admisión para el uso de los distintos métodos

Basilea II incorpora la medición del cargo de capital por RO dentro del Pilar I. Para ello se permite que los reguladores opten por admitir entre tres metodologías de medición, que van desde enfoques muy sencillos hasta modelos de medición avanzados. El Pilar I recoge las *buenas prácticas y principios* emitidos por el BCBS (analizados en la sección anterior de este trabajo) como precondition para la aplicación de dichos enfoques de medición. Estos criterios para calificar para la aplicación de los distintos enfoques, son proporcionales a la complejidad del enfoque elegido y se deja discreción para que, en algunos casos, los reguladores decidan por sí mismos cuáles de los requisitos enumerados serán de aplicación en su jurisdicción. Recordemos que las alternativas de medición del capital por RO contenidas en Basilea II (en orden creciente de sensibilidad al RO) son: i) Enfoque de Indicador Básico; ii) Enfoque Estandarizado (y su variante, el Enfoque Estandarizado Alternativo) y; iii) Enfoques de Medición Avanzada (AMA).

Para el caso del *Enfoque de Indicador Básico*, Basilea II no fija criterios específicos que deban adoptar los bancos en orden a permitirles la aplicación de este método. No obstante, se establece que “...se aconseja a los bancos que utilicen este método que sigan las directrices del Comité recogidas en el documento ‘Sound Practices for the Management and Supervision of Operational Risk’ de febrero de 2003...”<sup>16</sup>

Por su parte, se establece que para la aplicación del *Enfoque Estandarizado*, “...el banco debe demostrar a su supervisor que, como mínimo...”<sup>17</sup>

- su consejo de administración y su alta dirección, según corresponda, participan activamente en la vigilancia del marco de gestión del RO;
- posee un sistema de gestión del RO conceptualmente sólido que aplica en su totalidad y;
- cuenta con recursos suficientes para utilizar la metodología en las principales líneas de negocio, así como en los ámbitos de control y auditoría.

Adicionalmente, un banco con actividad internacional que utilice el *Enfoque Estandarizado* deberá satisfacer también otros criterios:<sup>18</sup>

a) Contar con un sistema de gestión del RO que asigne responsabilidades claras a la unidad de gestión de ese riesgo, quien será responsable del desarrollo de estrategias destinadas a identificar, evaluar, monitorear y controlar/mitigar el RO; codificar las políticas y procedimientos relativos a la gestión y control del RO para toda la entidad; diseñar y aplicar la metodología de evaluación del RO de la institución; y diseñar y aplicar un sistema para transmitir la información sobre el RO.

---

<sup>16</sup> BCBS (2004), párrafo 651.

<sup>17</sup> BCBS (2004), párrafo 660. Versión en español publicada por el BCBS.

<sup>18</sup> BCBS (2004), párrafo 663. Se establece que los supervisores nacionales deben decidir cuáles de estos criterios serán de aplicación puesto que algunos pueden no resultar apropiados en su jurisdicción (pp.100).

b) Como parte integrante del sistema de evaluación interna del RO del banco, éste deberá analizar de manera sistemática la información disponible sobre dicho riesgo, incluidas las pérdidas relevantes en cada línea de negocio. Su sistema de evaluación del RO deberá estar integrado dentro de los procesos de gestión del riesgo del banco. Los resultados que arroje dicho sistema deberán ser parte integral del proceso de seguimiento y control del perfil de RO del banco. Por ejemplo, esta información debe ser parte importante de la presentación de información sobre el riesgo y su gestión, así como para el análisis del riesgo. El banco deberá implantar técnicas que generen incentivos para mejorar la gestión del RO en toda la entidad.

c) Deberá existir un sistema periódico que informe sobre la exposición al RO, incluidas las pérdidas operativas más importantes, que esté dirigido a la dirección de las unidades de negocio, a la alta dirección y al consejo de administración. El banco deberá contar con procedimientos que permitan adoptar las acciones necesarias de acuerdo con el tenor de la información contenida en los informes de gestión.

d) El sistema de gestión de RO deberá estar bien documentado. El banco deberá contar con un mecanismo que permita garantizar regularmente el cumplimiento de un conjunto documentado de políticas, controles y procedimientos internos relativos al sistema de gestión del RO, que deberá incluir políticas para el tratamiento de los aspectos que se incumplen.

e) Los procesos de gestión y sistemas de evaluación del RO deberán someterse a un procedimiento de validación y a un examen periódico independiente. Estos exámenes deberán incluir tanto las operaciones de las unidades de negocio como las actividades de la unidad de gestión del RO.

f) El sistema de evaluación del RO (incluidos los procesos de validación interna) deberá someterse a exámenes periódicos realizados por auditores externos y/o por los supervisores.

Por último, los criterios de admisión establecidos para los *Enfoques de Medición Avanzada (AMA)* son los más exigentes, en función de la mayor complejidad asociada a ellos. Para estos métodos, se establecen i) criterios generales; ii) criterios cualitativos; iii) criterios cuantitativos y; iv) aspectos de mitigación del riesgo, que deben satisfacer las entidades a efectos de que se les permita el uso de los AMA. Sin tratar de hacer una enumeración exhaustiva de las condiciones establecidas por Basilea II<sup>19</sup>, algunos de los principales aspectos se enumeran a continuación.

#### *i) Criterios generales*

A los efectos de poder utilizar los AMA, el banco deberá demostrar a su supervisor que, como mínimo:

- su consejo de administración y su alta dirección, según corresponda, participan activamente en la vigilancia del marco de gestión del RO;
- posee un sistema de gestión del RO conceptualmente sólido que aplica en su totalidad y ;

---

<sup>19</sup> Las cuales pueden consultarse en BCBS (2004) párrafos 664 a 679.

- cuenta con recursos suficientes para utilizar la metodología en las principales líneas de negocio, así como en los ámbitos de control y auditoría.

El AMA estará sometido a un período de seguimiento inicial por parte del supervisor antes de que pueda utilizarse a efectos de capital regulatorio, lo que permitirá al supervisor determinar si el método es adecuado. El sistema de medición interna de un banco deberá estimar de forma razonable las pérdidas inesperadas, combinando datos relevantes de pérdidas tanto internos como externos, análisis de escenarios, así como el entorno del negocio y los factores de control interno que son específicos al banco. El sistema de medición del banco también deberá poder llevar a cabo la asignación de capital económico por RO entre las distintas líneas de negocio de un modo que genere incentivos para la mejora de la gestión del RO en esas líneas.

#### *ii) Criterios cualitativos*

Los bancos deberán satisfacer los siguientes criterios cualitativos antes de poder ser autorizados a emplear un AMA a efectos de calcular el capital por RO:

a) Contar con una unidad de gestión del RO que se encargue del diseño y aplicación del marco de gestión del RO de la entidad. Esta unidad será la encargada de compilar las políticas y procedimientos de la entidad en su conjunto relativos a la gestión y control del RO; de diseñar y aplicar la metodología de medición del RO en la institución; de diseñar y aplicar un sistema de información y de desarrollar estrategias encaminadas a identificar, estimar, observar y controlar / reducir el RO.

b) El sistema de medición interna del RO deberá estar perfectamente integrado dentro de los procesos habituales de gestión del riesgo del banco. Los resultados que arroje dicho sistema deberán utilizarse activamente en el proceso de seguimiento y control del perfil de RO del banco. Por ejemplo, esta información debe ser parte importante de la presentación de informes sobre el riesgo y su gestión, así como de la distribución interna del capital y del análisis del riesgo. El banco deberá contar con técnicas que distribuyan el capital por RO entre las principales líneas de negocio y que generen incentivos para mejorar la gestión del RO en toda la entidad.

c) Deberá informarse periódicamente a la dirección de las unidades de negocio, a la alta dirección y al consejo de administración acerca de las exposiciones al RO y del historial de pérdidas debidas a este riesgo. El banco deberá contar con procedimientos que permitan adoptar las acciones necesarias en función de la información contenida en estos informes de gestión.

d) El sistema de gestión del RO deberá estar bien documentado. El banco deberá contar con un mecanismo que permita garantizar regularmente el cumplimiento de un conjunto documentado de políticas, controles y procedimientos internos relativos al sistema de gestión del RO, que deberá incluir políticas para el tratamiento de los aspectos que se incumplen.

e) Los auditores externos y/o internos deberán llevar a cabo exámenes periódicos de los procesos de gestión y sistemas de medición del RO. Estos exámenes deberán incluir

tanto las operaciones de las unidades de negocio como las actividades de la unidad independiente de gestión del RO.

f) La validación del sistema de medición del RO que lleven a cabo los auditores externos y/o las autoridades supervisoras deberá incluir los siguientes aspectos:

- comprobación del buen funcionamiento de los procesos de validación interna y;
- comprobación de la transparencia y accesibilidad del flujo de datos asociados al sistema de medición del riesgo y de su procesamiento. Es preciso que los auditores y las autoridades supervisoras puedan acceder fácilmente a las especificaciones y a los parámetros del sistema, siempre que lo estimen necesario y en el marco de los procedimientos oportunos.

### *iii) Criterios cuantitativos*

Estos criterios de admisión corresponden a las características que deben tener los modelos de medición interna para que sean aceptados por el supervisor. Dado que en este trabajo el foco no es el análisis de la medición del RO, simplemente mencionaremos que estos criterios cuantitativos refieren, en primer lugar, a lo que Basilea II llama *criterios de solidez de los AMA*, para luego establecer una serie de criterios cuantitativos de aplicación a las medidas de RO generadas internamente, así como los requisitos asociados a cada uno de los cuatro elementos que conforman un AMA: datos internos, datos externos, análisis de escenarios y factores relacionados con el entorno de negocio y con el control interno.<sup>20</sup>

### *iv) Mitigación del riesgo*

Se establecen criterios específicos referidos a las condiciones que deben cumplir las pólizas de seguro para que se permita que el banco reconozca el efecto mitigador del RO.<sup>21</sup>

## 2.3.2. Pilar II: Proceso de revisión del supervisor

Este Pilar analiza los principios básicos de la revisión del supervisor, la gestión del riesgo y la transparencia y responsabilidad de la supervisión con respecto a los riesgos bancarios. El proceso de revisión del supervisor no sólo tiene como objetivo que las entidades posean un capital adecuado para cubrir todos los riesgos de su negocio, sino que impulsa a los bancos a que desarrollen y utilicen mejores técnicas de gestión de riesgos para su seguimiento y control<sup>22</sup>. El rol del supervisor será el de evaluar si las entidades cuantifican sus necesidades de capital en función de sus riesgos, interviniendo cuando fuera necesario. Esta interacción tiene la intención de fomentar un diálogo entre las entidades y los supervisores de modo tal que cuando se identifiquen deficiencias, se puedan tomar acciones rápidas a efectos de reducir el riesgo o restituir el capital.

---

<sup>20</sup> Para una descripción de los criterios cuantitativos, ver BCBS (2004) párrafos 667 a 676. Cabe aclarar que los requisitos allí contenidos deberían ser considerados como la guía de buenas prácticas para aplicación de los AMA.

<sup>21</sup> BCBS (2004), párrafos 677 a 679.

<sup>22</sup> BCBS (2004).

El Comité identificó cuatro principios básicos que complementan aquellos definidos en los *Principios Básicos para una Supervisión Bancaria Eficaz*.<sup>23</sup>

***Principio 1: Los bancos deberán contar con un proceso para evaluar la suficiencia de su capital total en función de su perfil de riesgo y con una estrategia para el mantenimiento de sus niveles de capital.***

Las características más importantes de un proceso incluyen:

- vigilancia por parte del consejo de administración y la alta dirección;
- evaluación rigurosa del capital;
- evaluación integral de los riesgos;
- seguimiento e información;
- examen de los controles internos.

Todos los riesgos que enfrenta una entidad deberían tenerse en cuenta en el proceso de evaluación del capital, incluyendo por supuesto al RO. Aunque el Comité reconoce que no todos los riesgos pueden medirse con exactitud, es necesario desarrollar un proceso que los estime.

Refiriéndonos estrictamente al RO, en este tema debería aplicarse un rigor similar al utilizado para gestionar otros riesgos significativos<sup>24</sup>. La entidad debe desarrollar un marco para gestionar el RO y evaluar la suficiencia de capital en ese marco. El mismo deberá cubrir la propensión y tolerancia del banco al RO, incluyendo el grado y modo en que el RO es transferido fuera de la entidad. Deberá incluir además, políticas a seguir por la entidad para identificar, evaluar, monitorear y controlar / mitigar el riesgo.

***Principio 2: Los supervisores deberán examinar y evaluar las estrategias y evaluaciones internas de la suficiencia de capital de los bancos, así como la capacidad de éstos para vigilar y garantizar el cumplimiento de los ratios de capital. Los supervisores deben intervenir cuando no estén satisfechos con el resultado de este proceso.***

El supervisor deberá regularmente revisar el proceso por el que una entidad evalúa la suficiencia de capital, la posición de riesgo, los niveles de capital resultante y la calidad del capital mantenido. Los supervisores también deberán evaluar en qué medida los bancos cuentan con un sólido proceso interno de evaluación de la suficiencia de capital. El análisis deberá centrarse en la calidad de gestión y control del riesgo de la entidad y no podrá suponer que los supervisores realicen las funciones de la dirección de la entidad.

***Principio 3: Los supervisores deberán esperar que las entidades operen por encima del ratio mínimo de capital regulatorio y deberán ser capaces de exigirles que mantengan capital por encima de este mínimo.***

En este sentido, existen varias razones por las cuales los bancos deberán mantener este margen, tales como que la entidad decida, por una cuestión de competitividad, operar por encima de los niveles mínimos; en el curso de la actividad bancaria el volumen y

---

<sup>23</sup> Además de en las restantes guías de buenas prácticas emitidas por el BCBS.

<sup>24</sup> BCBS (2004), párrafo 736.

tipo de actividades irán cambiando, al igual que los diferentes tipos de exposición al riesgo, lo que generará fluctuaciones en el coeficiente de capital de la entidad; el hecho de obtener capital adicional puede ser costoso para las entidades especialmente si ello se hace en un momento donde las condiciones del mercado son desfavorables, entre otros.

***Principio 4: Los supervisores deberán intervenir con prontitud para prevenir que el capital descienda por debajo de los niveles mínimos requeridos para cubrir las características de una entidad determinada y deben requerir acciones correctivas inmediatas si el capital no se mantiene en el nivel requerido o no se recupera ese nivel.***

Los supervisores deberán considerar diversas alternativas en el caso que crean que la entidad no pueda cumplir los requisitos incorporados en los principios de supervisión. Deberán contar con discrecionalidad para utilizar los instrumentos que mejor se adapten a las circunstancias de la entidad y a su entorno operativo.

Además de cumplir con estos principios, el supervisor deberá evaluar el requerimiento de capital generado por el Pilar I para asegurar que aporta una imagen coherente del funcionamiento individual del banco. Para tal fin, el supervisor debe tener en cuenta el documento de Basilea sobre “*Buenas prácticas para la Administración y Supervisión del RO*”<sup>25</sup> y tener en consideración los bancos de tamaños y operaciones similares.

Dentro del proceso de supervisión existen elementos discrecionales, es por ello que los supervisores deberán esforzarse por cumplir sus obligaciones de manera transparente y responsable. Deberán hacerse públicos los criterios que utilizarán los supervisores para examinar las evaluaciones internas de capital de las entidades. Si el supervisor no está conforme con los cálculos del requerimiento de capital por RO realizados por la entidad, puede tomar medidas tales como solicitar a la entidad que tenga un mayor requerimiento de capital por RO, que reduzca la exposición a las actividades que implican un alto RO, que mejore la planificación de contingencias, actualice los sistemas informáticos, entre otras posibilidades. En el caso que se fijen requerimientos de capital superiores al mínimo para una determinada entidad, el supervisor deberá explicar cuáles fueron las características de riesgo específicas que dieron origen a esos requerimientos, como así también cualquier medida correctiva.

### 2.3.3. Pilar III: Disciplina de mercado

El propósito del tercer *Pilar* es complementar los requerimientos de capital mínimo y el proceso de revisión del supervisor, estableciendo las mejores prácticas aplicables respecto a la divulgación de información. El fomentar la disciplina de mercado mediante el desarrollo de requisitos de divulgación permite a los agentes del mercado evaluar información clave sobre el ámbito de aplicación, capital, exposición al riesgo, y procesos de evaluación de riesgo. Ello se considera de mayor relevancia en los casos en los cuales las entidades utilizan metodologías internas de medición, las que por su naturaleza son más “opacas” hacia el público y hacen que las entidades tengan discreción en la evaluación de sus requerimientos de capital. El dar a conocer información basada en este esquema común a las entidades se considera un medio

---

<sup>25</sup> BCBS (2003).



efectivo para informar al mercado sobre la exposición de un banco a ciertos riesgos y provee un marco consistente, lo cual facilita hacer comparaciones.

Para cada área de riesgo (incluyendo la dedicada a RO), los bancos deben describir sus objetivos y políticas de gestión de riesgo, lo que incluye:<sup>26</sup>

- estrategias y procesos;
- estructura y organización de la unidad encargada de la gestión de riesgo;
- alcance y naturaleza de los sistemas de medición de riesgos;
- políticas de cobertura y / o mitigación del riesgo y las estrategias y procesos para controlar la continua eficiencia de las coberturas.

Ajustándonos estrictamente al RO, además de los requisitos antes mencionados sobre divulgación cualitativa, se requiere:

- cantidad de capital necesario por RO y el método utilizado;
- descripción del AMA, en caso que la entidad lo utilice, incluyendo un análisis de los factores internos y externos relevantes considerados en el método de medición del banco. En el caso de uso parcial, el ámbito y cobertura de los distintos métodos utilizados;
- para los bancos que utilicen el AMA, una descripción del uso de seguros para cubrir el RO.

### **3. La gestión del RO en las entidades financieras**

Este capítulo desarrolla las prácticas en la administración del RO desde el punto de vista de las propias entidades bancarias, habiéndose recogido en gran medida la experiencia de consultoras internacionales y el Comité de Basilea en su trabajo con los bancos. Se destacan ciertas prácticas observadas, motivaciones, como así también las limitaciones organizacionales detectadas. Como se ha mencionado anteriormente, las entidades han ido incrementando paulatinamente los recursos asignados a la administración del RO, pasando de la simple mejora en los sistemas de control al desarrollo de modelos de medición y gestión del RO que intentan obtener una estimación del impacto de futuras pérdidas.<sup>27</sup>

Una motivación importante para ello<sup>28</sup> es que un programa de administración del RO puede ayudar a las entidades a alcanzar sus objetivos organizacionales.<sup>29</sup> En tal sentido, se destaca que algunos bancos ya han logrado remover costos excedentes de sus operaciones, dejando poco margen para futuros ahorros por esta vía; el próximo paso consistiría en eliminar los ROs innecesarios de las operaciones. También cabe destacar

---

<sup>26</sup> BCBS (2004), párrafo 824.

<sup>27</sup> Nieto Giménez (2005).

<sup>28</sup> Ver por ejemplo KPMG (2003).

<sup>29</sup> A modo de ejemplo, cuando se aplica un análisis del RO a los procesos de desarrollo de productos, un banco debe asegurarse que los riesgos involucrados sean entendidos y tenidos en consideración. Por otra parte muchas entidades reconocen que la administración tradicional del RO (que trata los componentes del RO en forma discreta, p.ej. a través de mejoras en los controles internos, seguros o auditoría interna), no le permite a su Directorio contar con un panorama integral del RO y, por ende, no resulta efectivo para prevenir pérdidas severas.

que los ahorros resultantes en algunos procesos debidos a una reducción en la tasa de errores pueden sobrepasar en gran medida los beneficios generados a través de una política tradicional de reducción de costos.<sup>30</sup>

### 3.1. Prácticas observadas en la administración del RO

En un trabajo realizado con bancos internacionales, Levy, Samandari & Simoes<sup>31</sup> han observado que la infraestructura de esas entidades suele estar más orientada en *medir* el RO que en *mitigarlo*. Son poco frecuentes los procedimientos para afrontar prácticas de negocio riesgosas y en caso de haberlos, suelen no ser sistemáticos. Los aspectos *cualitativos*, como los aspectos culturales del “*front-office*”, o los puntos de vista de los principales “*stakeholders*” del banco no son frecuentemente considerados en la forma debida. Por otro lado destacan cierta complacencia a nivel de unidad de negocio como consecuencia de la centralización de las funciones de riesgo. Los autores destacan las limitaciones organizacionales para gestionar exitosamente el RO (ver cuadro 3).

**Cuadro 3: Limitaciones organizacionales para el desarrollo de un sistema de administración exitoso del RO<sup>32</sup>**

<b>Promoción organizacional</b>	Si las autoridades del banco sólo visualizan la administración del RO como un requisito regulatorio, y no como una iniciativa que agrega valor a la empresa, los esfuerzos de implementación se verán dificultados.
<b>Recursos y aceptación por parte de las líneas de negocio</b>	Los gerentes de las líneas de negocio suelen ser escépticos respecto a iniciativas corporativas que requieren tiempo y recursos, pero no tengan como contrapartida beneficios tangibles. Por ello es importante que a cambio de su participación reciban “feedback” en cuanto a los beneficios de las iniciativas implementadas.
<b>Función centralizada de RO</b>	La centralización de la función de control de riesgo observada en muchos bancos sin la participación activa de las gerencias involucradas puede dificultar respuestas rápidas frente a necesidades cambiantes.
<b>Cultura orientada al riesgo</b>	Falta de una cultura orientada al riesgo. Para imponerla en la organización resulta importante remunerar los esfuerzos orientados a mitigar los riesgos, por ejemplo a través de una reducción del capital económico imputado al área.
<b>Coordinación con iniciativas de control ya existentes</b>	Las iniciativas existentes pueden incluir procesos de revisión y control de riesgos, auditoría interna, “ <i>compliance</i> ” con IFRS, SOX <sup>33</sup> y otros requisitos regulatorios.

Se señalan tres aspectos a ser mejorados en las prácticas de negocios vinculados a RO<sup>34</sup>:

- la identificación y tratamiento de nuevos riesgos;
- la evaluación constante de los principios y prácticas habituales;
- el tratamiento de los aspectos culturales que dificultan una administración orientada al riesgo.

Por otro lado, un reciente informe del BCBS<sup>35</sup> destaca ciertas prácticas observadas en las entidades financieras vinculadas con la administración del RO<sup>36</sup>. En lo referido a la **participación del directorio**, se observan grandes variaciones entre los bancos: abarcan desde un compromiso absoluto, hasta un mínimo esfuerzo orientado al mero

<sup>30</sup> McKinsey (2006).

<sup>31</sup> Mc Kinsey (2006).

<sup>32</sup> KPMG (2003).

<sup>33</sup> IFRS: International Financial Reporting Standards, SOX: Sarbannes Oxley Act 2002.

<sup>34</sup> Mc Kinsey (2006).

<sup>35</sup> BCBS (2006-c).

<sup>36</sup> El estudio comprende a aquellos bancos que se están orientando a implementar métodos avanzados para la medición del RO (AMA).

cumplimiento regulatorio. En muchas entidades, el directorio ha delegado la responsabilidad de administrar el RO a un subcomité. Algunas de las acciones tomadas por los bancos para demostrar el compromiso de la alta dirección en la administración del RO incluyen la creación y comunicación de políticas integrales que detallan todos los aspectos del marco de administración del RO. También han implementado programas de reportes que permiten al directorio recibir informes periódicos de las unidades de negocio, de la función centralizada de administración de RO y de la auditoría interna.

En cuanto a la **independencia** de la función de administración del RO, ese mismo estudio del BCBS destaca que la mayoría de los bancos tienen una unidad estructuralmente independiente de las unidades de negocio generadoras de RO. Esa unidad es responsable del diseño e implementación del marco de RO. En gran parte de las entidades hay líneas de reporte formal y fuerte cooperación entre dicha función y las unidades de negocio y, en ciertos casos, también tienen acceso directo al comité de auditoría del directorio. En la mayoría de los bancos esta división es la que acumula los datos de pérdida de las unidades de negocio y la que prepara reportes regulares para la alta dirección. En algunos casos también recolecta indicadores clave de riesgo (“*Key Risk Indicators*” o *KRIs* en inglés).

En lo referente a una **auditoría independiente** del sistema de administración del RO, todavía parece ser demasiado temprano para describir una práctica usual entre las entidades. Por ahora la mayoría se apoya en consultorías externas y otras han desarrollado soluciones internas temporarias para ser usadas hasta que logren capacitar al staff que conducirá tests efectivos y tareas de verificación.<sup>37</sup>

Un aspecto importante es la creencia en cuanto a que las consecuencias de los RO finalmente se verán reflejadas en los “*buckets*” ya existentes para riesgo crediticio o de mercado. En consecuencia, no resultaría necesaria una categoría separada de RO. Esta creencia es completamente errónea, ya que estos riesgos tienen una estructura diferente y, en consecuencia, requieren respuestas diferentes por parte de la administración. Hay circunstancias que pueden llevar a confundir eventos de RO con otros riesgos, lo cual puede tener consecuencias considerables. El supuesto de que el riesgo de crédito y de mercado no están correlacionados con el RO es un supuesto que a primera vista pudiera parecer razonable. Sin embargo, los errores operacionales pueden causar problemas en la estimación del nivel de esos otros riesgos. La integración del análisis de los tres tipos de riesgos probablemente tomará tiempo. No obstante, puede ayudar el hecho de ir construyendo una base de datos que integre la información referida a estos tres tipos de riesgo. El BCBS observa<sup>38</sup> que los bancos conceptualmente tienen claros -en general- los límites entre el RO y los demás riesgos. A modo de ejemplo, destaca que las pérdidas generadas por “*traders*” que violan límites se tratan como eventos de RO y no como riesgo de mercado a efectos del cálculo del capital regulatorio. En cambio, en el caso de pérdidas asociadas a préstamos causadas por eventos operativos, como pueden ser procesos inadecuados o fallidos, se observa cierta tendencia en asociarlas al riesgo crediticio.

---

<sup>37</sup> BCBS (2006-c).

<sup>38</sup> BCBS (2006-c).

### 3.2. Evaluación del RO a través del uso de datos internos

En un esquema de administración del RO, la constitución de una **base interna de eventos operativos** es una práctica estandarizada. Para cualquier institución, la recopilación de esos eventos debería contribuir al objetivo de reducción de incidentes y montos de pérdidas y por sobretodo, para mejorar la calidad del servicio y de los productos. Un proceso de recolección de datos internos de RO debería tener una serie de incentivos y controles para asegurar un alto nivel de cobertura y calidad de los datos.

A fin de generar una base de datos internos se requiere de políticas y procesos que garanticen la consistencia y completitud de los mismos. Lo más importante es que éstas sean claras y que sean aplicadas consistentemente a través de sus productos, ubicación y categoría de riesgos. Los datos que superen determinado umbral, incluyendo pérdidas indirectas, *casi-pérdidas* y costos de oportunidad, deberían ser verificados e ingresados a las bases de pérdidas. Cambios posteriores en los montos de pérdida, pagos posteriores de pólizas de seguro y reclamos de compensación adicionales deberían ser agregados en una forma auditable.

Entre los beneficios de construir una base de datos interna se debe destacar que:

- permite tomar conciencia de que las exposiciones al RO pueden ser potencialmente negativas para la organización;
- el cuantificar la exposición ayuda a focalizar los recursos para su mitigación;
- al analizar las causas básicas de los eventos, las ocurrencias repetidas pueden indicar áreas para ser mejoradas.

Por su parte, el **proceso de recopilación de eventos** podría dividirse en tres etapas:

- *Infraestructura*: creación de una infraestructura para detectar y registrar los eventos operativos e incorporarlos en un proceso de administración de riesgo. Los eventos son típicamente capturados a través de sistemas existentes con el propósito de eliminar errores y procesos adicionales y a través de un proceso de entrada manual.
- *Ejecución*: comprende la detección, recopilación, validación y reporte de los eventos. Este proceso comienza con el dónde y cómo detectar el evento. Luego, debe procederse al registro del mismo y posteriormente un proceso de “recupero” donde se corrige la operación. Los eventos son valuados, o sea que se determina el monto de la pérdida.
- *Monitoreo y control*: esta última etapa tiende a asegurar que el proceso de recopilación de eventos es íntegro y acertado. El primer paso en el monitoreo es un análisis por el grupo de administración de RO. Un control adicional es la Auditoría Interna, división independiente de la unidad de RO.

El trabajo del BCBS<sup>39</sup> antes mencionado sobre prácticas de la industria, dedica una sección a temas vinculados con datos internos. Comienza tratando el tema del registro de la *fecha de ocurrencia* de un evento operativo, destacando que los bancos tienden a favorecer el día de ocurrencia o el día del descubrimiento del evento por encima del

---

<sup>39</sup> BCBS (2006-c).

correspondiente a su registro contable. Una excepción notable son los litigios judiciales, en cuyo caso se tiende a usar la opción contable. Con respecto a los métodos para evaluar el **monto de pérdida** por daños materiales a activos físicos, los bancos se hallan divididos en forma homogénea entre los que eligen registrarlos a su valor de libros, a su valor de mercado o a su costo de reposición. Muchas entidades validan estas pérdidas conciliándolas con el mayor general o a través de una auditoría interna. Otro tema considerado es el de los eventos de pérdida que *se materializan a lo largo del tiempo*; la práctica habitual entre las entidades es retrotraer todas las pérdidas sucesivas a la fecha de ocurrencia del incidente. Respecto a la asignación de un evento a una línea de negocios, los bancos han elegido entre: i) asignar toda la pérdida a la línea de negocios más afectada o ii) asignar las pérdidas sobre una base pro-rata en las líneas de negocio afectadas

En cuanto al tratamiento de los **recuperos** a efectos de determinar la pérdida asociada a un evento, se destaca que pueden ocurrir inmediatamente o años después de ocurrido el evento de RO. El neteo de los recuperos sería el procedimiento adecuado en el caso de tener certeza respecto a ellos. La mayoría de los bancos registra en sus bases la pérdida bruta neteada de los recuperos obtenidos durante un período previamente especificado (el que suele ser desde uno hasta algunos días de ocurrido el evento). En casos en donde se obtiene un recupero total, algunos bancos registran una casi-pérdida (“*near miss*”). Los bancos que registran estos datos no los usan para *cuantificar* el riesgo, aunque algunos los incorporan para la construcción de escenarios. Generalmente estos datos son usados para identificar *tendencias* en el RO y con otros propósitos de administración del riesgo.

En lo referente al uso de **umbrales mínimos** para el registro de una pérdida por RO, se debe tener en cuenta que su elección afecta a las distribuciones de pérdidas y a las estimaciones de pérdidas inesperadas. La mayoría de los bancos se apoya en opiniones expertas para fijar estos umbrales y suelen elegir los mismos umbrales para todos los tipos de evento, aunque unas cuantas entidades han decidido adaptar los umbrales a las distintas líneas de negocio.

Un tema fundamental es el de la **validación** de los datos internos de pérdida, esto es, los pasos que los bancos deben realizar para garantizar la integridad y completitud de los datos de pérdida interna y de los procesos de recolección de datos. Dado que la mayoría de los bancos recientemente han comenzado a recolectar datos, los procesos de validación todavía se encuentran en etapa de desarrollo y se deberá esperar para observar una práctica común en esta área. Las siguientes prácticas son usadas por las entidades financieras a tales efectos:

- conciliación con el mayor general;
- elaboración de informes de la función de control de riesgo, incluyendo chequeos de consistencia entre varios reportes internos;
- auditorías internas y externas;
- revisión de inconsistencias de datos internos entre líneas de negocio o filiales;
- uso de una función centralizada para ingresar los datos al repositorio de datos.

Cuando las entidades juzgan insuficientes sus datos internos a efectos de administrar sus riesgos, recurren a **datos externos o análisis de escenarios**, lo cual implicará un trabajo adicional de validación.

### 3.3. Evaluación del riesgo a través del uso de factores claves del control interno y del entorno de negocios

A pesar del rol fundamental de las bases de datos internas, éstas tienen limitaciones<sup>40</sup>, entre ellas, el hecho de que los controles se van mejorando con el paso del tiempo a la luz de las experiencias de pérdida. Con ello resultaría que el RO actual es menor al estimado a partir de los datos históricos ya que estos no reflejan las acciones posteriores de mitigación y prevención del RO que implementa la entidad bancaria. Por otro lado, muchas veces los datos en sí mismos no permiten establecer claramente las causas que generaron la pérdida. Otra dificultad de carácter conductual reside en el tema de los incentivos: pueden existir desincentivos para informar eventos relevantes, p.ej. si estos tienen como consecuencia aumentar el cargo de capital a la línea de negocios reportante. Por otro lado, ciertos agentes internos (RRHH, auditoría, o el área legal) pueden estar incentivados en reportar eventos o casi-pérdidas, si ello tiene como consecuencia realzar la importancia de sus tareas.

Todas estas circunstancias pueden haber motivado a que el BCBS recomiende que la metodología de estimación del RO del banco también incluya el uso de *información complementaria* a los datos de pérdida, entre los que se encuentran *factores claves del control interno y del entorno de negocios*. Ello contribuye a una evaluación del riesgo más “*forward-looking*”, reflejando mejor la calidad de los controles del banco y su entorno operativo, ayudando a alinear la estimación del capital económico con los objetivos de administración del RO del propio banco.

La evaluación del RO provee al banco un criterio para identificar potenciales riesgos de naturaleza severa a través del diseño de escenarios estructurados con representantes de todas las líneas de negocio. Como una herramienta que permite la identificación –y en forma limitada, hasta una posible cuantificación del RO– es complementaria al proceso de recolección de datos. Efectivamente, permite cerrar la brecha de conocimiento entre datos históricos de pérdida (generalmente escasos) de carácter “*backward-looking*” e intentos de establecer métodos “*forward-looking*” sensibles al riesgo para la identificación del RO. A pesar que los detalles varían, generalmente la estructura básica de la evaluación del riesgo es universal. Está basada en un conjunto de matrices que identifican y evalúan el RO y sus subcomponentes en términos de su probabilidad de ocurrencia e impacto. El perfil de riesgos resultante presenta un panorama de áreas de riesgos por unidad de negocio, gerencia u otro nivel de agregación.

Un elemento clave en la evaluación del RO son los *KRIs*; factores que pueden proveer señales de alerta temprana respecto a sistemas, procesos, productos, personas y entornos más amplios. Al igual que los datos de pérdida, están basados en datos existentes pero, a diferencia de éstos, no se concentran en el valor nominal de la información, sino que a través de ellos se busca predecir determinados comportamientos futuros (p.ej. la rotación de personal, variable que no está asociada con alguna pérdida actual, pero sí con potenciales pérdidas futuras vinculadas con la renuncia de personal clave). Identificar los *KRIs* puede ser una tarea ardua, dado que la presunta correlación con exposiciones actuales sólo puede ser verificada a lo largo del tiempo usando datos de

---

<sup>40</sup> Power, M (2003).

pérdida reales. Para simplificar su uso, muchos bancos sólo usan una serie genérica limitada de *KRIs* para cada unidad de negocio.

### 3.4. Mitigación del RO y estimación del capital

Una vez identificados y cuantificados los riesgos, debería implementarse una estrategia para su *mitigación* a través de políticas, procedimientos, sistemas y controles. El proceso de mitigación de riesgos es un proceso continuo e iterativo, dado que al momento de implementar una nueva táctica, las otras deben ser revisadas.

El banco que deba estimar el capital económico requerido deberá definir los datos de entrada, las técnicas estadístico-matemáticas a emplear y las hipótesis que usará para medir el RO, definir el modelo y finalmente validarlo. El objetivo de la estimación es obtener las pérdidas *esperadas*, a efectos de incluirlas en el “*pricing*” de los productos, como también la estimación de pérdidas *inesperadas* (p.ej. a través del “Valor a Riesgo”) para las cuales se dispondrá de un capital para su potencial absorción. Un aspecto clave es la validación del modelo y los datos, dado que se incluyen potenciales eventos de pérdida con bajísima frecuencia. Actualmente las técnicas de cálculo más difundidas son el “*Loss distribution approach*” (LDA)<sup>41</sup>, los *KRIs* y el enfoque basado en escenarios. Dado que han sido designados para ayudar a los bancos a calificar para los AMA, usan intensivamente los componentes exigidos para su empleo, esto es, datos de pérdida interna, datos de pérdida externa, escenarios y factores de ambiente laboral y de control.

## 4. Las regulaciones sobre *buenas prácticas* en países latinoamericanos

Los reguladores de varios países de la región han emitido normas referidas a las buenas prácticas de gestión del RO, recogiendo los *principios* del documento del BCBS del año 2003. Existe conciencia en el sentido que el primer punto para avanzar en el tema es cubrir los aspectos cualitativos para la gestión de RO, siendo otra de las principales preocupaciones la necesidad de conformar bases de datos con eventos de pérdidas por RO. A continuación se presenta un estado de situación de aquellos países latinoamericanos que han emitido regulaciones respecto a buenas prácticas de administración y supervisión del RO.

### 4.1. Brasil

En junio de 2006 el *Banco Central de Brasil* (BCB) dictó una *Resolución*<sup>42</sup> por la que estableció que las instituciones financieras y demás instituciones autorizadas a funcionar por el BCB deben implementar una estructura de gerenciamiento del RO, definiendo a ese riesgo y a una clasificación de eventos operativos de acuerdo con lo establecido en Basilea II.

En línea con las buenas prácticas para la gestión y supervisión del RO sugeridas por el BCBS, el BCB establece que la *estructura de gerenciamiento* de RO debe prever:

---

<sup>41</sup> BCRA (2006-a)

<sup>42</sup> BCB (2006), Resolución 3.380.

- la identificación, evaluación, monitoreo, control y mitigación del RO;
- documentación y almacenamiento de información referida a pérdidas por RO;
- elaboración -con una periodicidad mínima anual- de informes que permitan la identificación y corrección de las deficiencias de control y gerenciamiento del RO. Estos deberán ser remitidos al directorio, que deberá manifestarse acerca de las acciones a ser implementadas a efectos de corregir eventuales defectos;
- realización de tests de evaluación de los sistemas de control implementados;
- elaboración y diseminación de la política de administración del RO al personal de la entidad y a los proveedores de servicios tercerizados, estableciéndose roles y responsabilidades;
- existencia de planes de contingencia conteniendo las estrategias a ser adoptadas para asegurar la continuidad de las operaciones y limitar pérdidas graves resultantes de eventos de RO.

La política de gerenciamiento debe ser aprobada y revisada por lo menos anualmente por el directorio de la entidad. Se debe designar un director responsable del gerenciamiento del RO en la entidad, aunque se admite que el mismo pueda desarrollar otras funciones. Se establece que la administración del RO deberá ser ejecutada por una unidad específica, segregada de la división de auditoría interna.

Esta estructura de gerenciamiento deberá ser implementada antes del 31 de diciembre de 2007, siguiendo el siguiente cronograma:

- antes de diciembre de 2006 se deberá designar al director responsable y se deberá definir la estructura organizacional que llevará a cabo la implementación;
- antes de junio de 2007 se deberán definir la política institucional, procesos, procedimientos, y los sistemas necesarios para su efectiva implementación;
- antes de diciembre de 2007 deberá estar implementada la estructura de administración del RO.

## 4.2. Chile

En agosto de 2005, la *Superintendencia de Bancos e Instituciones Financieras de Chile* (SBIF) elaboró disposiciones<sup>43</sup> relativas a la clasificación que la SBIF debe mantener en forma permanente respecto a las instituciones financieras, según su nivel de solvencia y gestión<sup>44</sup>. Adicionalmente se incorporan aspectos esenciales de gestión del capital incluidos en el acuerdo de Basilea II, considerando al RO como una categoría distinta de los riesgos bancarios tradicionales.

La evaluación de una entidad se realiza a través de visitas de inspección, por lo menos una vez al año. En ella se revisan los controles internos, los sistemas de información para la toma de decisiones, el seguimiento oportuno de los riesgos y su clasificación así como la capacidad para enfrentar escenarios de contingencia. La evaluación se efectúa por temas, uno de los cuales es específicamente la administración del RO.<sup>45</sup>

<sup>43</sup> SBIF (2005), Circular N° 3.328.

<sup>44</sup> Existen tres niveles (A, B y C) para cada ítem.

<sup>45</sup> Las restantes incluyen administración del riesgo de crédito y gestión global, de la estrategia de negocios y gestión del capital, transparencia, prevención del lavado de activos, etc.



En lo que respecta a la evaluación de la administración del RO, la SBIF adopta los criterios propuestos por el BCBS. En este contexto, evalúa el rol asumido por el directorio y la alta administración y la aprobación que han dado a la estrategia a utilizar en su administración, entendiendo a este riesgo como una categoría distinta de los riesgos bancarios tradicionales. La estrategia a utilizar en la administración del riesgo, teniendo en cuenta la importancia relativa y el volumen de las operaciones de la entidad, debe contemplar una definición clara de RO y establecer los principios para identificar, evaluar, controlar y mitigar el riesgo. En la evaluación a realizar por la SBIF, interesa observar la compatibilidad entre las políticas y procedimientos establecidos por la entidad con respecto al volumen, sofisticación y naturaleza de sus actividades. Asimismo, se examina la manera en que se han establecido las políticas y la forma en que la dirección del banco participa en su aprobación y supervisa su cumplimiento.

**Cuadro 4: Aspectos que determinan la buena gestión del RO (SBIF)**

- La institución tiene una definición de lo que entiende por RO y lo ha reconocido como un riesgo gestionable.
- Existen una función encargada de la administración de RO.
- La entidad mantiene políticas para la administración de los RO aprobadas por el directorio o la administración superior.
- La estrategia de administración del RO es consistente con el volumen y complejidad de sus actividades y tiene en cuenta el nivel de tolerancia al riesgo del banco, incluyendo líneas específicas de responsabilidad.
- Esta estrategia ha sido implementada a través de toda la organización bancaria y todos los niveles del personal asumen y comprenden sus responsabilidades respecto a la administración de este riesgo.
- La entidad administra los RO considerando los impactos que pudieran provocar (severidad de la pérdida) y la probabilidad de ocurrencia de los eventos.
- La entidad evalúa el RO inherente a todos los tipos de productos, actividades, procesos y sistemas.
- Se asegura que antes de introducir nuevos productos, emprender nuevas actividades o establecer nuevos procesos y sistemas, se evalúa el RO inherente.
- El banco ha integrado a sus actividades normales el monitoreo del RO y ha identificado indicadores apropiados que brinden alertas de un aumento del riesgo y de futuras pérdidas.
- La institución es capaz de cuantificar los impactos de las pérdidas asociadas al RO y constituir prudencialmente los resguardos necesarios.
- Los sistemas de información permiten hacer un monitoreo continuo de la exposición a los RO. Poseen la cobertura y profundidad necesarias para servir en forma eficiente al proceso de toma de decisiones de la alta administración y directorio.
- El banco cuenta con políticas para administrar los riesgos asociados a las actividades entregadas a terceras partes y lleva a cabo verificaciones y monitoreos de las actividades de dichas partes.
- El banco realiza inversiones en tecnología de procesamiento y seguridad de la información, que permiten mitigar los RO y que son concordantes con el volumen y complejidad de las actividades y operaciones que realiza.
- La institución cuenta con una adecuada planificación a largo plazo para la infraestructura tecnológica y dispone de los recursos necesarios para el desarrollo normal de sus actividades y para que los nuevos proyectos previstos se concreten oportunamente.
- El banco cuenta con una estructura que permite administrar la seguridad de la información en términos de resguardar su confidencialidad, integridad y disponibilidad.
- El banco considera en sus planes de continuidad del negocio y contingencia, diversos escenarios y supuestos que pudieran impedir que cumpla toda o parte de sus obligaciones y en ese sentido ha desarrollado una metodología formal que considera en sus etapas, la evaluación de impacto y criticidad de sus servicios y productos, la definición de estrategias de prevención, contención y recuperación, así como pruebas periódicas de tales estrategias.
- La institución ha implementado un proceso para controlar permanentemente la incorporación de nuevas políticas, procesos y procedimientos, que permiten detectar y corregir sus eventuales deficiencias de manera de reducir la frecuencia y severidad de los eventos de pérdida. Asimismo, la entidad emite reportes con la información pertinente a la alta administración y directores.
- La entidad bancaria ha adoptado una estrategia y sistema de gestión de calidad respecto de sus productos, servicios, e información que suministra a sus clientes, reguladores y a otros entes.
- La extensión y profundidad de las auditorías es proporcional al nivel de riesgo y al volumen de actividad. La función de auditoría está en posición de evaluar en forma independiente el cumplimiento de las políticas, la eficacia de los procedimientos y los sistemas de información.

### 4.3.Colombia

La *Superintendencia Financiera de Colombia* (SFC) a través de una *Circular Externa*<sup>46</sup> fijó las bases y los lineamientos mínimos que deben ser implementados para el desarrollo de un *Sistema de Administración del Riesgo Operativo* (SARO). Definen al RO como la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en los recursos humanos, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. Esta definición incluye el riesgo legal y (a diferencia de Basilea II) también el riesgo reputacional.

La SFC establece que las entidades sometidas a su supervisión se exponen al RO y por lo tanto deberán desarrollar, establecer, implementar y mantener un SARO, acorde con su estructura, tamaño, objeto social y actividades de apoyo, estas últimas realizadas directamente o a través de terceros, que les permita identificar, medir, controlar y monitorear eficazmente el RO.

#### 4.3.1. Etapas de la administración del RO

Previo a la implementación de las etapas del SARO, las entidades deben establecer las políticas, objetivos, procedimientos y estructura para la administración del RO. El sistema debe estar alineado con los planes estratégicos de cada entidad.

En el desarrollo del SARO, las entidades deben **identificar** el RO al que se exponen, teniendo en cuenta los factores de riesgo definidos por la regulación, para lo cual deben como mínimo:

- identificar y documentar la totalidad de los procesos;
- establecer metodologías de identificación, que sean aplicables a los procesos, con el fin de determinar los eventos de RO. En base a ellas, identificar los eventos de RO potenciales y ocurridos, en cada uno de los procesos;
- la etapa de identificación debe realizarse previamente a la implementación o modificación de cualquier proceso y con anterioridad a la realización de operaciones de fusión, adquisición, cesión de activos, pasivos y contratos, entre otros.

Una vez concluida la etapa de identificación, las entidades deben **medir** la probabilidad de ocurrencia de un evento de RO y su impacto en caso de materializarse. Esta medición podrá ser cualitativa y, cuando se cuente con datos históricos, cuantitativa. Para la determinación de la probabilidad se debe considerar un horizonte de tiempo de un año. En el proceso de medición del RO las entidades deben desarrollar, como mínimo, los siguientes pasos:

- establecer la metodología de medición susceptible de ser aplicada a los eventos de RO identificados. La metodología debe ser aplicable tanto a la probabilidad de ocurrencia como al impacto, en los casos en que el riesgo se materialice;
- aplicar la metodología para lograr una medición individual y consolidada de la probabilidad de ocurrencia y del impacto, en caso de materializarse en la totalidad de los procesos de la entidad;

---

<sup>46</sup> SFC (2006).

- determinar el perfil de riesgo inherente individual y consolidado.

Las entidades deben tomar medidas para **controlar** el riesgo inherente a que se ven expuestas con el fin de disminuir la probabilidad de ocurrencia y/o el impacto en caso de que el riesgo se materialice. Durante esta etapa las entidades deben como mínimo:

- establecer la metodología en función de la cual se definen las medidas de control de los eventos de RO, e implementarlas para cada uno de los eventos de RO;
- determinar las medidas que permitan asegurar la continuidad del negocio;
- determinar el perfil de riesgo residual individual y consolidado.

Sin perjuicio de lo anterior, las entidades podrán decidir si transfieren, aceptan o evitan el riesgo, en los casos en que esto sea posible. Debe tenerse en cuenta que la utilización de ciertas medidas, como la contratación de seguros, puede ser una fuente generadora de nuevos eventos de RO, los cuales deben ser a su vez administrados.

De acuerdo con su estructura, tamaño, objeto social y actividades de apoyo, las entidades deben definir, implementar, probar y mantener un proceso para administrar la **continuidad del negocio** que incluya elementos como: prevención y atención de emergencias, administración de la crisis, planes de contingencia y capacidad de retorno a la operación normal. Los planes de continuidad del negocio deben cumplir, como mínimo, con los siguientes requisitos:

- haber superado las pruebas necesarias para confirmar su eficacia y eficiencia;
- ser conocidos por todos los interesados;
- cubrir por lo menos los siguientes aspectos: identificación de eventos que pueden afectar la operación, actividades a realizar cuando se presentan fallas, alternativas de operación y regreso a la actividad normal.

Las entidades deben hacer un **monitoreo periódico** de los perfiles de riesgo y de las exposiciones a pérdidas. En ese sentido, éstas deben cumplir como mínimo, con los siguientes requisitos:

- desarrollar un proceso de seguimiento efectivo, que facilite la rápida detección y corrección de las deficiencias en su SARO. El seguimiento debe tener una periodicidad acorde con los eventos de RO potenciales y ocurridos, así como con la frecuencia y naturaleza de los cambios en el entorno operativo y debe realizarse con una periodicidad mínima semestral;
- establecer indicadores descriptivos y/o prospectivos que evidencien los potenciales eventos de RO;
- asegurar que los controles estén funcionando en forma oportuna y efectiva;
- asegurar que los riesgos residuales se encuentren en los niveles de aceptación establecidos por la entidad.

#### 4.3.2. Elementos del sistema de administración del RO

Cada una de las etapas y elementos del sistema debe contar con **políticas** claras y efectivamente aplicadas que permitan un adecuado funcionamiento del SARO y se traduzcan en reglas de conducta y procedimientos que orienten la actuación de la entidad para una adecuada implementación y funcionamiento de las etapas y elementos

del SARO. Esas etapas y elementos deben constar en **documentos y registros**, garantizando la integridad, oportunidad, confiabilidad y disponibilidad de la información allí contenida. Para cada uno de estos aspectos, la Superintendencia establece requisitos mínimos que deben ser cumplidos (ver en [Anexo](#)).

Respecto de la **estructura organizacional**, las entidades deben establecer y asignar como mínimo ciertas funciones establecidas por la SFC, a cargo de los órganos de dirección, administración y demás áreas de la entidad en relación con las distintas etapas y elementos del SARO. La regulación establece de manera detallada las funciones que se le requiere a la junta directiva, al representante legal y a la unidad de RO (ver detalles en el [Anexo](#)).

Las entidades deben además construir un **registro de eventos** de RO y mantenerlo actualizado, el que debe contener todos los eventos de RO ocurridos y discriminarlos según:

- generen pérdidas y afecten el estado de resultados de la entidad;
- generen pérdidas y no afecten el estado de resultados de la entidad;
- no generen pérdidas y por ende no afecten el estado de resultados de la entidad.

La SFC establece toda una serie de características mínimas que debe cumplir dicho registro de eventos de RO (ver [Anexo](#)).

También, se deben establecer **instancias responsables de efectuar una evaluación** del SARO, las que informarán, de forma oportuna, los resultados a los órganos competentes. Los órganos de control no deben ser responsables de la administración del RO y serán por lo menos la revisoría fiscal y la auditoría interna o quien ejerza el control interno.

Las entidades, de acuerdo con sus actividades y tamaño, deben contar con la **tecnología** y los **sistemas necesarios** para garantizar el adecuado funcionamiento del SARO. Asimismo se establece que la **divulgación de la información** debe hacerse en forma periódica y estar disponible, cuando así se requiera. Se debe diseñar un sistema adecuado de **reportes** tanto internos como externos, que garantice el funcionamiento de los propios procedimientos y el cumplimiento de los requerimientos normativos.

Por último, se deben diseñar, programar y coordinar **planes de capacitación** sobre el SARO dirigidos a todas las áreas y funcionarios, los que deben cumplir también con los requisitos establecidos por la SFC.

#### 4.4. México

La *Circular Unica de Bancos*, en su Capítulo IV<sup>47</sup> establece que las instituciones deben observar los lineamientos mínimos sobre la *Administración Integral de Riesgos* (AIR) e instituir mecanismos que les permitan realizar sus actividades con niveles de riesgo acordes con su capital neto y capacidad operativa. Clasifica a los riesgos en

---

<sup>47</sup> CNBV (2005).

cuantificables y no cuantificables y, dentro del primer grupo, en discrecionales y no discrecionales.

Se definen los riesgos *no discrecionales* como los resultantes de la operación del negocio, pero que no son producto de la toma de una posición de riesgo. Entre ellos se encuentra el RO, que se define como la pérdida potencial por fallas o deficiencias en los controles internos, por errores en el procesamiento y almacenamiento de las operaciones o en la transmisión de información, así como por resoluciones administrativas y judiciales adversas, fraudes o robos y comprende, entre otros, al riesgo tecnológico y al riesgo legal, en el entendido de que:

- el *riesgo tecnológico* se define como la pérdida potencial por daños, interrupción, alteración o fallas derivadas del uso o dependencia en el hardware, software, sistemas, aplicaciones, redes y cualquier otro canal de distribución de información en la prestación de servicios bancarios con los clientes de la Institución;
- el *riesgo legal* se define como la pérdida potencial por el incumplimiento de las disposiciones legales y administrativas aplicables, la emisión de resoluciones administrativas y judiciales desfavorables y la aplicación de sanciones, en relación con las operaciones que llevan a cabo las instituciones.

En cuanto a la AIR, establece que las instituciones deberán:

- definir sus objetivos sobre exposición al riesgo y desarrollar políticas y procedimientos para la administración de los distintos tipos de riesgo;
- delimitar las diferentes funciones y responsabilidades de los distintos órganos, unidades administrativas y personal de operación y apoyo;
- identificar, medir, vigilar, limitar, controlar, informar y revelar riesgos.

El consejo de cada institución será el responsable de aprobar los objetivos, lineamientos y políticas para administrar los riesgos, los límites de exposición al riesgo y los mecanismos para la realización de acciones correctivas. Además deberá revisarlos cuando menos una vez por año.

El director general de la institución, será responsable de vigilar que se mantenga la independencia necesaria entre la unidad para la AIR y las *Unidades de Negocio* (UN). Adicionalmente deberá:

- establecer como mínimo programas semestrales de revisión por parte de la unidad para la AIR y de las UN, respecto al cumplimiento de objetivos, procedimientos y controles en la celebración de operaciones, así como de los límites;
- asegurar la existencia de sistemas de almacenamiento, procesamiento y manejo de información;
- difundir y, en su caso, implementar, planes de acción para situaciones de contingencia en las que por caso fortuito o fuerza mayor, se impida el cumplimiento de los límites y niveles de tolerancia al riesgo aplicables;
- establecer programas de capacitación y actualización para el personal de la unidad para la AIR y para todo aquél involucrado en las operaciones que impliquen riesgo para la institución;

- establecer procedimientos que aseguren un adecuado flujo de la información entre las UN y la unidad para la AIR.

A su vez, el consejo deberá constituir un comité que administrará los riesgos y vigilará que la realización de las operaciones se ajuste a objetivos, políticas y procedimientos para administrarlos. El comité de riesgos deberá reunirse cuando menos una vez al mes y todas las sesiones y acuerdos se harán constar en actas debidamente circunstanciadas y suscritas por todos y cada uno de los asistentes. El comité de riesgos para llevar a cabo la AIR contará con una unidad especializada cuyo objeto será identificar, medir, vigilar e informar los riesgos cuantificables que enfrenta la institución en sus operaciones, ya sea que éstos se registren dentro o fuera del balance, incluyendo, en su caso, los riesgos de sus subsidiarias financieras. Esta unidad será independiente de las UN, a fin de evitar conflictos de interés y asegurar una adecuada separación de responsabilidades.

En materia de administración por tipo de riesgo, la Circular establece las funciones que las instituciones deberán desarrollar para la administración del RO. Deberán como mínimo:

- identificar y documentar los procesos que describen el quehacer de cada unidad de la institución;
- identificar y documentar los ROs implícitos a los procesos;
- evaluar e informar por lo menos trimestralmente, las consecuencias que generaría materializar los riesgos identificados e informar los resultados a los responsables de las unidades implicadas;
- establecer los niveles de tolerancia al riesgo para cada tipo de riesgo identificado, definiendo causas, orígenes o factores de riesgo.

Para el registro de eventos de pérdida por RO, incluyendo riesgos tecnológico y legal, deberán:

- clasificar las unidades y líneas de negocio;
- identificar y clasificar los diferentes tipos de eventos de pérdida;
- mantener una base de datos histórica que contenga el registro sistemático de los diferentes tipos de pérdida y su costo, en correspondencia con su registro contable, identificado con la línea de negocio de origen.

También contempla aspectos vinculados con el riesgo legal y el tecnológico, propiciando informes sobre la exposición de riesgo que incluyan una descripción del mismo, posibles causas y consecuencias de su materialización incluyendo en la medida de lo posible una estimación de su impacto financiero y propuestas de acciones a fin de minimizar esa exposición.

#### 4.5. Perú

En enero de 2002 la *Superintendencia de Bancos y Seguros* (SBS) aprobó el *Reglamento para la Administración de los Riesgos de Operación*<sup>48</sup>. Allí se define *riesgo de operación* (RO) como la posibilidad de ocurrencia de pérdidas financieras por

---

<sup>48</sup> SBS (2002-a).

deficiencias o fallas en los procesos internos, en la tecnología de información, en las personas o por ocurrencia de eventos externos adversos. Se determina que el directorio es responsable del establecimiento de políticas y procedimientos generales para identificar, medir, controlar y reportar apropiadamente los riesgos de operación. Corresponderá a la gerencia general la implementación de las políticas y procedimientos generales establecidos por el directorio. La unidad de riesgos es la encargada de administrar los ROs que enfrenta la entidad, pudiendo comprender a alguna unidad especializada para la evaluación de dicho riesgo. Entre las funciones de esta unidad, figuran las de:

- preparar y evaluar las políticas para la administración de los RO;
- desarrollar metodologías para la evaluación cualitativa y/o cuantitativa de los riesgos;
- evaluar los RO, de forma previa al lanzamiento de nuevos productos y ante cambios importantes en el ambiente operativo o informático;
- consolidar y desarrollar reportes e informes sobre la administración de los RO por proceso, o unidades de negocio y apoyo;
- identificar las necesidades de capacitación y difusión para una adecuada administración de los RO.

La entidad deberá contar con una estructura organizacional y administrativa que permita una adecuada administración del RO y deberá establecer políticas y procedimientos claramente definidos y consistentes con el tamaño y naturaleza de la entidad y con la complejidad de sus operaciones y servicios. Dicha estructura deberá establecerse de manera que exista independencia entre la unidad de riesgos y aquellas otras unidades de negocio, así como una clara delimitación de funciones, responsabilidades y perfil de puestos en todos sus niveles. Estos aspectos deberán encontrarse recogidos en el manual de organización y funciones del banco.

El manual de control de riesgos deberá contener una sección especial sobre los riesgos de operación. Dicha sección deberá contemplar por lo menos los siguientes aspectos:

- políticas para la administración de los ROs;
- funciones y responsabilidades en la administración de los ROs;
- descripción de la metodología aplicada para medir y evaluar los ROs;
- la forma y periodicidad con la que se deberá informar al directorio y a la gerencia general, entre otros, sobre la exposición a los ROs;
- el proceso para la aprobación de propuestas de nuevas operaciones, productos y servicios.<sup>49</sup>

#### 4.5.1. Administración de los aspectos que originan el RO

Las entidades deben administrar los riesgos asociados a los **procesos internos** para la realización de sus operaciones y servicios, a efectos de minimizar la posibilidad de pérdidas financieras relacionadas al diseño inapropiado de los procesos críticos, o a políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de

---

<sup>49</sup> Las propuestas deberán contar, entre otros aspectos, con una descripción general de la nueva operación, producto o servicio de que se trate, los riesgos identificados y las acciones a tomar para su control.

los mismos. En tal sentido, podrán considerarse entre otros, los riesgos asociados a las fallas en los modelos utilizados, los errores en las transacciones, la evaluación inadecuada de contratos o de la complejidad de productos, operaciones y servicios, los errores en la información contable, la inadecuada compensación, liquidación o pago, la insuficiencia de recursos para el volumen de operaciones, la inadecuada documentación de transacciones, así como el incumplimiento de plazos y costos planeados.

Del mismo modo deberán administrar apropiadamente los riesgos asociados a la **tecnología de información**, de tal modo que se minimice la posibilidad de pérdidas financieras derivadas del uso de sistemas informáticos inadecuados y tecnologías relacionadas a ellos, que pueden afectar el desarrollo de las operaciones y servicios al atender contra la confidencialidad, integridad y disponibilidad de la información. Para este fin, las entidades podrán considerar los riesgos vinculados a las fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo e implementación de dichos sistemas y la compatibilidad e integración de los mismos, problemas de calidad de información, la inadecuada inversión en tecnología, así como las fallas en la adecuación a los objetivos del negocio, entre otros aspectos. En febrero de 2002 se establecieron criterios mínimos para la identificación y administración de los riesgos asociados a la tecnología de información, donde se amplía sustancialmente este ítem<sup>50</sup>.

Las entidades deben administrar apropiadamente los riesgos asociados a **las personas**, de tal modo que se minimice la posibilidad de pérdidas financieras asociadas a inadecuada capacitación del personal, negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, lavado de dinero y similares.

Además, deberán considerar la posibilidad de pérdidas derivada de la ocurrencia de **eventos externos**, ajenos al control de la entidad, que pudiesen alterar el desarrollo de sus actividades. En tal sentido, entre otros factores, se podrán tomar en consideración los riesgos que implican las contingencias legales, las fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, así como las fallas en servicios críticos provistos por terceros.

#### 4.5.2. Requerimientos de información

Las entidades deberán presentar a la SBS, dentro de los noventa días siguientes al cierre de cada ejercicio anual, un informe referido a la evaluación de los RO que enfrentan, por proceso o unidad de negocio y apoyo. Dicho informe deberá contemplar por lo menos los siguientes aspectos:

- metodología empleada para la administración de los RO;
- identificación de los RO por proceso o unidad de negocio y apoyo;
- evaluación de los RO identificados;
- medidas adoptadas para administrar los RO materiales identificados y plazos para su aplicación, entre las cuales se encuentran, entre otras: evitar, transferir o

---

<sup>50</sup> SBS (2002-b). Ahí se incluyen definiciones, responsabilidades, estructura organizacional y procedimientos, administración de la seguridad de información, subcontratación (*outsourcing*), aspectos de la seguridad de información, administración de las operaciones y comunicaciones, desarrollo y mantenimiento de sistemas informáticos (requerimientos de seguridad), procedimientos de respaldo, planeamiento para la continuidad de negocios, privacidad de la información, entre otros.



retener el riesgo; reducir su probabilidad de ocurrencia o reducir sus consecuencias;

- funcionarios responsables de las actividades de control de riesgo;
- plan de actividades de la unidad de riesgos en lo referente a la administración de los RO.

## 5. Conclusiones

Una serie de factores llevaron a que tanto la comunidad reguladora internacional como la industria financiera comenzaran a manifestar una preocupación creciente por pérdidas provenientes de eventos de RO. Así fue que a lo largo de los últimos años, el RO se ha consolidado como una categoría de riesgo abordada en sí misma, que comprende toda una serie de riesgos que tradicionalmente se trataban de manera parcial. En el año 2003, el BCBS publicó una serie de *principios* sobre buenas prácticas para la administración del RO, lo que sentó uno de los principales precedentes del tratamiento integral del RO como categoría de riesgo. Posteriormente, en junio de 2004 con la publicación de *Basilea II* se marca otro hito importante ya que se fija por primera vez un cargo de capital explícito para atender a las pérdidas provenientes de eventos de RO. Además de incluir el aspecto particular de la *medición* del capital regulatorio, Basilea II señala como precondition para la cuantificación de ese riesgo, a la *aplicación efectiva de las buenas prácticas* dictadas en la materia. Asimismo, la versión revisada de los *Principios Básicos para una Supervisión Bancaria Efectiva*, del año 2006, incorpora un principio específico dedicado al RO.

Al revisar la evolución de los estándares internacionales y las prácticas de la industria a lo largo de los últimos años, puede afirmarse que son principalmente dos los aspectos que han surgido como novedosos en el tratamiento del RO: el primero, es el de considerarlo como una categoría de riesgo bien definida que requiere una gestión *integral* al igual que ocurre con otros típicos riesgos bancarios. El segundo, es el hecho de *medir* las pérdidas ocasionadas por el RO y *requerir capital* para afrontarlas. La publicación de Basilea II hizo que muchas veces las discusiones se centraran en el aspecto específico de la medición y en los métodos allí propuestos. Sin embargo, no debe perderse de vista que, como se expresó antes, Basilea II también incorpora la necesidad de contar con buenas prácticas de gestión y supervisión del RO como precondition para aplicar metodologías de medición.

Este trabajo realizó una recopilación de las buenas prácticas sugeridas por los estándares del BCBS y la manera en que esos *principios* se han plasmado en la regulación de una serie de países, así como la forma en que se reflejan en las estructuras y organización de las entidades financieras. El concepto de *gestión* del RO adoptado por el BCBS comprende a la *identificación, evaluación, monitoreo y mitigación/control* de ese riesgo. Estos cuatro aspectos se reflejan claramente en los principios dictados por el BCBS y son recogidos por las regulaciones de los países latinoamericanos analizados, con algunas variantes. En este trabajo se puso especial atención en aquellos países latinoamericanos que han emitido regulaciones vinculadas con el RO (como es el caso de Brasil, Chile, Colombia, México y Perú), tendientes a implementar procedimientos, documentación, responsabilidades y creación de estructuras adecuadas para una eficiente administración del RO en las entidades financieras; todo ello previo a la instauración de cargos de capital para la cobertura del RO.

Esas regulaciones analizadas de países latinoamericanos, están en línea con las definiciones de RO y los tipos de eventos definidos por el BCBS. En ese sentido, las normas han recogido los principios fundamentales de asignación de responsabilidades concretas para el directorio y la alta gerencia de las entidades como así también la necesidad de que exista una unidad independiente encargada del RO dentro de la organización y el rol de control que corresponde tanto a la auditoría interna como a los supervisores. Se reconoce en la regulación la necesidad de que las entidades tengan estrategias claramente definidas que sean revisadas periódicamente por parte del directorio y de la alta gerencia; una sólida cultura de gestión del RO y de control interno y herramientas eficaces para la transmisión interna de información y planes de contingencia.

## Anexo

### Resumen de requisitos establecidos por la Superintendencia Financiera de Colombia

#### Colombia: Requisitos mínimos establecidos por la SFC

Políticas	Procedimientos	Documentos y registros
a. Impulsar a nivel institucional la cultura en materia de RO.	a. Instrumentar las diferentes etapas y elementos del SARO.	a. El Manual de RO que debe contener, como mínimo:
b. Evidenciar el deber de los órganos de administración, de control y de sus demás funcionarios, de asegurar el cumplimiento de las normas internas y externas relacionadas con la administración del RO.	b. Identificar los cambios y la evolución de los controles y los perfiles de riesgo.	i. Las políticas para la administración del RO.
c. Permitir prevenir y resolver conflictos de interés en el acopio de información en las diferentes etapas del SARO, especialmente para el registro de eventos de RO.	c. Adoptar las medidas por el incumplimiento del SARO.	ii. Las metodologías para la identificación, medición y control y los niveles de aceptación del RO.
d. Permitir la identificación de cambios en los controles y los perfiles de riesgo.		iii. La estructura organizacional del SARO, como también los roles y responsabilidades de quienes participan en la administración del RO.
e. Desarrollar e implementar planes de continuidad del negocio.		iv. Las medidas necesarias para asegurar el cumplimiento de las políticas y objetivos del SARO.
		v. Los procedimientos que deben implementar los órganos de control frente al SARO.
		vi. Las estrategias de capacitación y divulgación del SARO
		b. Los procedimientos para identificar, medir, controlar y monitorear el RO.
		C. Los documentos y registros que evidencien la operación efectiva del SARO.
		d. Los informes de la Junta Directiva, el Representante Legal y los órganos de control.

#### Colombia: Características mínimas que debe cumplir el registro de eventos de RO

- a. Cada entidad debe tener su propio y único registro de eventos de RO. La entidad con matriz internacional debe tener disponible y centralizada en Colombia, la información relacionada con los eventos de RO locales.
- b. Comprender la totalidad de los eventos de RO.
- c. Contener los siguientes campos mínimos, que corresponden a la información de los eventos de RO :
  - i. Código interno que relacione el evento en forma secuencial.
  - ii. Fechas en que se inicia, finaliza, se descubre, y se registra contablemente el evento.
  - iii. Moneda extranjera en la que se materializa el evento.
  - iv. El monto de dinero a que asciende la pérdida.
  - v. El monto de dinero recuperado por acción directa de la entidad, discriminando el monto recuperado por coberturas a través de un seguro.
  - vi. Producto o servicio afectado.
  - vii. Cuentas del “Plan Único de Cuentas” (PUC) afectadas.
  - viii. Identificar el proceso afectado.
  - ix. Tipo de pérdida según el registro de eventos por RO de la entidad.
  - x. Descripción detallada del evento: canal de servicio o atención al cliente (cuando aplica), y zona geográfica
  - xi. Identificación de la línea operativa donde se produjo el evento según clasificación suministrada por la SFC (coincide con la que fue propuesta por Basilea).

## Colombia

### Estructura organizacional: funciones requeridas por la SFC

Junta Directiva	Representante Legal	Unidad de RO
<ul style="list-style-type: none"> <li>▪ Establecer las políticas relativas al SARO.</li> <li>▪ Aprobar el Manual de RO y sus actualizaciones.</li> <li>▪ Hacer seguimiento y pronunciarse sobre perfil de RO de la entidad.</li> <li>▪ Establecer las medidas relativas al perfil de riesgo, teniendo en cuenta el nivel de tolerancia al riesgo de la entidad.</li> <li>▪ Pronunciarse respecto de cada uno de los puntos que contengan los informes periódicos que presente el Representante Legal.</li> <li>▪ Pronunciarse sobre la evaluación periódica del SARO, que realicen los órganos de control.</li> <li>▪ Proveer los recursos necesarios para implementar y mantener en funcionamiento, de forma efectiva y eficiente, el SARO.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Diseñar y someter a aprobación de la Junta Directiva u órgano que haga sus veces, el Manual de RO y sus actualizaciones.</li> <li>▪ Velar por el cumplimiento efectivo de las políticas establecidas por la Junta Directiva.</li> <li>▪ Adelantar un seguimiento permanente de las etapas y elementos constitutivos del SARO que se llevan a cabo en la entidad.</li> <li>▪ Designar el área o cargo que actuará como responsable de la implementación y seguimiento del SARO – (Unidad de RO).</li> <li>▪ Desarrollar y velar porque se implementen las estrategias con el fin de establecer el cambio cultural que la administración de este riesgo implica para la entidad.</li> <li>▪ Adoptar las medidas relativas al perfil de riesgo, teniendo en cuenta el nivel de tolerancia al riesgo, fijado por la Junta Directiva.</li> <li>▪ Velar por la correcta aplicación de los controles del riesgo inherente, identificado y medido.</li> <li>▪ Recibir y evaluar los informes presentados por la Unidad de RO.</li> <li>▪ Velar porque las etapas y elementos del SARO cumplan, como mínimo, con las disposiciones señaladas en la presente Circular.</li> <li>▪ Velar porque se implementen los procedimientos para la adecuada administración del RO a que se vea expuesta la entidad en desarrollo de su actividad.</li> <li>▪ Aprobar los planes de contingencia y de continuidad del negocio y disponer de los recursos necesarios para su oportuna ejecución.</li> <li>▪ Presentar un informe periódico, como mínimo semestral, a la Junta Directiva sobre la evolución y aspectos relevantes del SARO, incluyendo, entre otros, las acciones preventivas y correctivas implementadas o por implementar y el área responsable.</li> <li>▪ Establecer un procedimiento para alimentar el registro de eventos de RO.</li> <li>▪ Velar porque el registro de eventos de RO cumpla con los criterios de integridad, confiabilidad, disponibilidad, cumplimiento, eficiencia y confidencialidad de la información allí contenida.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Tener conocimiento en materia de administración de RO.</li> <li>▪ Ser organizacionalmente de alto nivel y tener capacidad decisoria.</li> <li>▪ No depender de los órganos de control, ni de las áreas de operaciones o de tecnología, ni relaciones que originen conflictos de interés.</li> <li>▪ Tener los recursos suficientes según el tamaño de la entidad.</li> <li>▪ Definir los instrumentos, metodologías y procedimientos tendientes a que la entidad administre efectivamente su RO, en concordancia con los lineamientos, etapas y elementos, mínimos previstos en esta norma.</li> <li>▪ Desarrollar e implementar el sistema de reportes, internos y externos, del RO de la entidad.</li> <li>▪ Administrar el registro de eventos de RO.</li> <li>▪ Coordinar la recolección de la información para cargar el registro de RO.</li> <li>▪ Evaluar el impacto de las medidas de control potenciales para cada uno de los eventos de riesgo identificados y medidos.</li> <li>▪ Establecer y monitorear el perfil de riesgo individual y consolidado de la entidad, e informarlo al órgano correspondiente.</li> <li>▪ Realizar el seguimiento permanente de los procedimientos y planes de acción relacionados con el SARO.</li> <li>▪ Desarrollar los modelos de medición del RO.</li> <li>▪ Desarrollar los programas de capacitación relacionados con el SARO.</li> <li>▪ Realizar el seguimiento a las medidas adoptadas para mitigar el riesgo inherente, con el propósito de evaluar su efectividad.</li> <li>▪ Reportar semestralmente al Representante Legal la evolución del RO, los controles implementados y el monitoreo que se realice sobre el mismo.</li> </ul>

**Colombia**  
**Instancias responsables de efectuar una evaluación del SARO**

---

- a. **Revisoría Fiscal:** deberá elaborar un reporte al cierre de cada ejercicio contable en el que informe acerca de las conclusiones obtenidas en el proceso de evaluación del cumplimiento de las normas e instructivos sobre el SARO. A su vez debe poner en conocimiento del Representante Legal los incumplimientos del SARO sin perjuicio de la obligación de informar sobre ellos a la Junta Directiva u órgano que haga sus veces.
  - b. **Auditoría Interna o quien ejerza el control interno:** deberá evaluar periódicamente la efectividad y cumplimiento de todas y cada una de las etapas y los elementos del SARO con el fin de determinar las deficiencias y sus posibles soluciones. Así mismo debe informar los resultados de la evaluación a la Unidad de RO y al Representante Legal. También debe realizar una revisión periódica del registro de eventos de RO e informar al Representante Legal sobre el cumplimiento de las condiciones señaladas en los registros de eventos de RO.
- 

**Colombia**  
**Divulgación de la información**

---

- a. *Información interna:* Como resultado del monitoreo deben elaborarse reportes semestrales que permitan establecer de forma individual y consolidada el perfil de riesgo residual de la entidad. Los administradores de la entidad en su informe de gestión al cierre de cada ejercicio contable deben incluir una indicación sobre la gestión adelantada en materia de administración de RO.
  - b. *Información externa:* en concordancia con las disposiciones legales vigentes sobre la materia las entidades deben suministrar al público la información necesaria con el fin de que el mercado pueda evaluar las estrategias de gestión del RO adoptadas por la entidad. Las características de la información divulgada estarán relacionadas con el volumen la complejidad y el perfil de riesgo de las operaciones de la entidad.
  - c. *Revelación contable:* los eventos de RO cuando no afecten el estado de resultados deben ser revelados en cuentas de orden de acuerdo con la metodología para su cuantificación establecida por cada entidad. Las pérdidas cuando afecten el estado de resultados deben registrarse en cuentas de gastos en el período en el que se materializó la pérdida. En las notas a los estados financieros se deben señalar las causas que originaron los eventos de RO revelados en cuentas de orden o registrados en el estado de resultados.
- 

**Colombia**  
**Planes de capacitación**

---

- a. Periodicidad anual.
  - b. Ser impartidos durante el proceso de inducción de los nuevos funcionarios.
  - c. Ser impartidos a los terceros, cuando exista una relación contractual con éstos.
  - d. Ser constantemente revisados y actualizados.
  - e. Contar con los mecanismos de evaluación de los resultados obtenidos para determinar la eficacia de los programas y el alcance de los objetivos propuestos.
-

## Referencias bibliográficas

- BCB (2006) Banco Central de Brasil: “*Resolución 3.380*”.
- BCRA (2006-a): “*Sistemas de Información para la Administración del Riesgo Operativo: Estudio de los sistemas de información requeridos para la medición del Riesgo Operativo*”. Gerencias de Investigación y Planificación Normativa y de Régimen Informativo, Octubre.
- BCRA (2006-b): “*Sistemas de Información para la Administración del Riesgo Operativo: Relevamiento en el sistema financiero argentino*”. Gerencias de Investigación y Planificación Normativa y de Régimen Informativo, Octubre.
- BCBS (2002) Basel Committee on Banking Supervision: “*Operational Risk Data Collection Exercise*”.
- BCBS (2003) Basel Committee on Banking Supervision: “*Sound practices for the management and supervision of operational risk*” y versión en español: “*Buenas prácticas para la gestión y supervisión del riesgo operativo*”, Febrero.
- BCBS (2004) Basel Committee on Banking Supervision: “*International Convergence of Capital Measurement and Capital Standards. A revised framework*”, updated June 2006.
- BCBS (2006-a) Basel Committee on Banking Supervision: “*Core Principles for Effective Banking Supervision*”, October.
- BCBS (2006-b) Basel Committee on Banking Supervision: “*Core Principles Methodology*”, October.
- BCBS (2006-c) Basel Committee on Banking Supervision: “*Observed range of practice in key elements of Advanced measurement approaches (AMA)*”, October.
- Cepparo, Germán (2006): “*Basilea II y el riesgo operacional en las entidades financieras*”. Tesis final del Master en Administración Financiera, Universidad de Buenos Aires.
- CNVB (2005) Comisión Nacional Bancaria y de Valores de México: “*Circular Única de Bancos – Capítulo IV – Administración de Riesgos*”. Diciembre 2005 y complementarias.
- Cruz, Marcelo (2002): “*Modeling, Measuring and Hedging Operational Risk*”, John Wiley & Sons LTD, Reprinted August 2005.
- FSI (2006) Financial Stability Institute: “*Implementation of the new capital adequacy framework in non-Basel Committee member countries*”, Occasional Paper N°6, October.
- FSI Connect.

- Joint Forum (2005): “*Outsourcing in financial services*”, February.
- KPMG (2003): “*Basel II – A closer look: managing operational risk*”. KPMG Financial Services.
- McKinsey (2006) (Levy, Samandari & Simoes): “*Better operational-risk management for banks*”, McKinsey Quarterly Bulletin, August.
- Nieto Giménez-Montesinos, María Angeles (2005): “*El tratamiento del Riesgo Operacional en Basilea II*”, Estabilidad Financiera N.º 8, Banco de España, Mayo.
- Operational Risk & Compliance Magazine: *varios números*, Incisive Media Investments Ltd.
- Power, M (2003): “*The invention of operational Risk*”, ESCR Center for analysis of risk and regulation, London School of Economics Discussion Paper 16, June.
- SBIF (2005) Superintendencia de Bancos e Instituciones Financieras de Chile: “*Circular N° 3.328. Capítulo 1-13 Bancos y Financieras*”, Agosto.
- SBS (2002-a) Superintendencia de Banca y Seguros (Perú): “*Resolución N°6-2002*”.
- SBS (2002-b) Superintendencia de Banca y Seguros (Perú): “*Circular N° G-105-2002*”.
- Seivold, A. , S. Leifer, S. Ulman (2006): “*Operational Risk Management: An evolving discipline*”, Supervisory Insights, Summer 2006. Federal Deposit Insurance Corporation (US).
- Seminario “*Riesgo Operativo en Basilea II*” (2006), FSI / ASBA, México.
- SFC (2006) Superintendencia Financiera de Colombia: “*Circular Externa 049*”, Diciembre.