

## “Requerimiento de Capital por Riesgo Operativo.

### Referencia al caso Uruguayo.”

*“Los hombres pasan, los recuerdos  
quedan, como quedan las obras de los  
que algo hacen”*

Víctor Montenegro (Escritor Argentino)

Trabajo de Investigación Monográfico realizado para la  
obtención del título de Contador Público – Plan 1990

**Autores:**

Alejandra Correa Vilizzio CI: 4.350.811-0

Graciela Galione Klot CI: 3.398.951-6

**Tutor:**

Cr. Rubén Rodríguez

Cátedra: Contabilidad Bancaria

*Agradecemos en primer lugar a nuestras familias y amigos, por el apoyo incondicional brindado a lo largo de nuestra carrera. Agradecemos también a nuestro tutor, Rubén Rodríguez por su dedicación y atención en la elaboración del presente trabajo, así como a los entrevistados.*

## **ABSTRACT**

El objetivo del presente trabajo de investigación monográfica se basó en el estudio de las recomendaciones establecidas en el Nuevo Acuerdo de Capitales “Basilea II”, para la implementación de una eficiente administración de Riesgo Operacional (RO). En especial nos enfocamos en el requerimiento de capital, tanto a nivel internacional como local.

A partir del análisis realizado, observamos que todos los países estudiados han incorporado en mayor o menor medida los lineamientos señalados en este Acuerdo. En particular, destacamos que Uruguay si bien sigue esta línea, viene a paso lento. Para la plaza financiera local, entendemos que el análisis debería dividirse en dos, la gestión y el requerimiento de capital por RO. Consideramos que debería emitirse una norma preceptiva que guíe a los Bancos hacia una misma dirección, implantando pautas para su gestión pero sin exigir una reserva de capital al respecto.

Por último, concluimos que sería recomendable la creación de un Consorcio de Datos mediante el cual, las entidades intercambien información valiosa redundando en una mejor Gestión Integral de Riesgos. Lamentablemente, hoy por hoy los Bancos se encuentran reacios a compartir sus datos internos y no demostraron predisposición a participar en este tipo de Consorcios, haciendo poco viable su implementación.

## INDICE

### Capítulo 1 – Marco Conceptual

1.1.	Introducción .....	8
1.2.	Antecedentes a Basilea II – Destacadas Crisis Financieras.....	10
1.2.1	Caso del Bank of Credit and Commerce (BCCI - 1991).....	12
1.2.2	Caso del Banco de Barings (1995).....	14
1.2.3	Crisis Financiera en Uruguay y la región (2002).....	16
1.2.3.1	Banco Comercial.....	17
1.2.3.2	Banco de Montevideo.....	21
1.3.	Origen y desarrollo del Riesgo Operacional.....	23
1.4.	Conceptos generales. Definiciones y alcances de las mismas.....	26
1.4.1	Definición de Riesgo.....	26
1.4.2	Definición de Riesgo operativo.....	26
A.	Definición de Riesgo Legal.....	27
B.	Definiciones de Riesgos Estratégico y Reputacional .....	28
B.1	Riesgo Reputacional.....	28
B.2	Riesgo Estratégico.....	28
1.5.	Importancia de la Gestión y Administración del RO.....	30
1.6.	Tratamiento del Riesgo Operacional en Basilea II.....	34
1.6.1	Pilar I: Requerimientos mínimos de capital.....	34
1.6.2	Pilar II: Examen del Supervisor.....	43
1.6.3	Pilar III: Disciplina de Mercado.....	44
1.7.	Elementos a considerar para gestionar adecuadamente el RO.....	46
1.7.1	Buenas prácticas para la gestión del RO.....	46
1.7.2	Gobierno Corporativo.....	46
1.7.3	Teoría de la Agencia.....	50

**Capítulo 2 – Observaciones realizadas sobre la aplicación de Basilea II en diversos países**

2.1. Trabajos realizados por Levy, Samandari & Simoes en Bancos Internacionales (Revista Mckinsey, Quarterly 2006).....	55
2.2. Observaciones realizadas por el BCBS en su trabajo con Bancos .....	56

**Capítulo 3 – Administración del Riesgo Operacional en países de interés**

Brasil.....	63
Chile.....	68
Argentina.....	75
México.....	79
Estados Unidos.....	87
España.....	89

**Capítulo 4 – Administración del Riesgo Operacional en Uruguay**

.....	98
-------	----

**Capítulo 5 – Críticas a la Administración del Riesgo Operativo**

.....	110
-------	-----

**Capítulo 6 – Trabajo de Campo en la plaza Uruguaya**

6.1. Estudio realizado en Bancos Privados y Públicos.....	117
6.2. Estudio realizado al Ente Regulador (BCU).....	131

**Capítulo 7 – Conclusiones del trabajo realizado**

.....	134
-------	-----

<b>Bibliografía</b> .....	139
<b>ANEXO I</b> .....	143
<b>ANEXO II</b> .....	145
<b>ANEXO III</b> .....	146
<b>ANEXO IV</b> .....	149
<b>ANEXO V</b> .....	150

# **CAPÍTULO 1**

## **MARCO CONCEPTUAL**

## 1.1. Introducción

El mundo se encuentra constantemente amenazado por crisis financieras de distintas especies. Esto en buena parte se debe a las rápidas mutaciones que viene sufriendo el sector bancario, cuyas prácticas han ido evolucionado en forma acelerada hacia una mayor competencia para acompañar la complejidad de las técnicas que están siendo utilizadas.

“El deterioro de la coyuntura económica ha vuelto más difícil pero también más necesaria la adaptación de los bancos a esta nueva situación”.<sup>1</sup>

“En efecto, la mayoría de los países tienen un sector bancario cuya organización data de hace algunos años y no corresponde con las necesidades de hoy en día. El mundo está “sobre bancarizado” y..., sea cual sea su tamaño, sea cual sea su *know how*, no pueden obtener ingresos suficientes solamente de las operaciones bancarias tradicionales, y por lo tanto han buscado otras fuentes.”<sup>2</sup>

A pesar de que los sistemas financieros se han ido desarrollando de diversas maneras en cada uno de los países, parecen haber seguido la misma tendencia: mayor desreglamentación lo que permitía a los bancos diversificar sus actividades. Lo mencionado anteriormente, sumado a la continua evolución de la tecnología dio lugar al surgimiento de nuevas herramientas como los “productos derivados”, entre otros.

---

<sup>1</sup> Según Babette Stern - "Les banques françaises dans la tourmente", Le Monde, 95.08.22 en el documento "Productos derivados y bancos a la deriva: El caso "BARINGS" – Autor: Dr. Gerard Verna – Director de la Cátedra de Ética en los Negocios, Instituto de Empresa, Madrid, Profesor de gestión internacional de empresas, Universidad Laval, Québec

<sup>2</sup> Según Aldo Olcese - "El drama de la alta finanzas", El Mundo, 95.03.22 en el documento "Productos derivados y bancos a la deriva: El caso "BARINGS" – Autor: Dr. Gerard Verna – Director de la Cátedra de Ética en los Negocios, Instituto de Empresa, Madrid, Profesor de gestión internacional de empresas, Universidad Laval, Québec

“Pero con los productos derivados los mercados financieros tal vez hayan inventado la bomba que les hará explotar”.<sup>3</sup>

Sin embargo, esto solo debería haberse aceptado bajo dos condiciones, las cuales no siempre se encontraban presentes: primero, que la administración de los bancos individuales fuese lo suficientemente capaz ejerciendo un control adecuado de dichas operaciones, y segunda, que cada banco pudiese ser efectivamente supervisado por el Banco Central (u otro organismo de contralor).

Por esta razón se dice que la evolución estructural del sector bancario puede desempeñar un papel sumamente significativo en lo que respecta al surgimiento de crisis financieras.

Es recién a partir del año noventa cuando se pone de manifiesto lo expuestas que se encontraban las entidades financieras a sufrir pérdidas muy elevadas por causas que no procedían ni del riesgo crediticio ni de la volatilidad inherente a los mercados en los cuales éstas se desenvolvían, sino que correspondían a otro tipo de riesgo mucho más imperceptible y por esta razón quizás también más perjudicial que los anteriores.

En efecto, las sucesivas crisis financieras que han y continuarán sucediendo a lo largo de la historia, dejan en evidencia marcadas carencias existentes en los controles administrativos de las operaciones que se llevan a cabo. Las fallas frecuentemente se reducen a: supervisión deficiente, malas estrategias, administración débil, sistemas de control inadecuados, fallas operacionales y

---

<sup>3</sup> Según Bruno Abescat : "La banque qui secoue la planète", L'Express, 95.03.09 en el documento "Productos derivados y bancos a la deriva: El caso "BARINGS" – Autor: Dr. Gerard Verna – Director de la Cátedra de Ética en los Negocios, Instituto de Empresa, Madrid, Profesor de gestión internacional de empresas, Universidad Laval, Quebec

fraudes. Esto de alguna manera resume lo que posteriormente Basilea II denomina *Riesgo Operacional (RO)*.

## **1.2. Antecedentes a Basilea II – Destacadas Crisis Financieras**

Para introducirnos en el tema del riesgo operacional en Basilea II, nos gustaría comenzar haciendo mención a los orígenes de la misma así como al surgimiento de la necesidad de considerar los riesgos operacionales dentro de un marco regulatorio. Debido a esto último, comentaremos brevemente algunas crisis financieras que son relevantes para visualizar en qué aspectos se evidenciaban las carencias de controles sobre estos riesgos.

El Comité de Basilea de Supervisión Bancaria fue creado en 1975 por los gobernadores de los Bancos Centrales de los países del Grupo de los Diez (G10), sean éstos Alemania, Bélgica, Canadá, Estados Unidos, Japón, Holanda, Italia, Francia, Reino Unido, Luxemburgo, Suecia y Suiza.

En 1988 este Comité publica su primer Acuerdo de Capitales (Basilea I), promoviendo sistemas bancarios más seguros y sólidos y brindado de esta manera, un marco normativo para la comunidad financiera internacional. Su principal aporte fue la introducción de nuevos métodos para calcular los requerimientos de capital mínimo que se debería exigir a las entidades financieras tomando en consideración sus perfiles de riesgos, es decir, básicamente en función de sus riesgos de crédito y de mercado.

Según el documento publicado por el Banco Central del Uruguay (en adelante BCU) acerca de los Estándares Mínimos de Gestión, el *Riesgo de Crédito* se define como la posibilidad de que la entidad vea afectadas sus ganancias o su

patrimonio debido a la incapacidad del deudor de cumplir con los términos del contrato firmado con la institución, o de actuar según lo pactado.

En cuanto a los *Riesgos de Mercado*, los define como aquellos por los cuales el valor de las posiciones dentro y fuera de balance pueden verse adversamente afectadas debido a movimientos en las variables de mercado (tasa de interés y tipos de cambio entre divisas), con el consiguiente impacto en las utilidades y patrimonio de las instituciones financieras.

Tal como lo mencionamos anteriormente, a continuación citamos algunos casos de las crisis financieras más renombradas de los últimos tiempos.

El caso más reciente y uno de los más importantes ocurridos durante los últimos 25 años, es la quiebra del Banco Inversor americano “LEHMAN BROTHERS”. Sin embargo, a pesar del protagonismo que ha adquirido este caso en los medios de la actualidad debido a que sus repercusiones están afectando al mundo entero, debemos resaltar que ya en 1996 el Fondo Monetario Internacional (FMI) estimaba que alrededor de 130 países habían sido víctimas de crisis bancarias desde la década de los 80 y era probable que aún en ese momento, un 30% de ellos estuviesen atravesando una crisis con estas características.

Podemos citar dos de los casos más importantes ocurridos en el Reino Unido durante los años 90:

- 1 La Quiebra del Bank of Credit and Commerce (BCCI);
- 2 y la Quiebra del Barings Brothers Bank.

Antes de proceder a detallar cada uno de ellos, consideramos relevante destacar que el Reino Unido ha sido uno de los países más eficientes en evitar y amainar

grandes crisis o quiebras en los bancos más importantes, ya que el costo de los diversos incidentes para el Banco de Inglaterra, significó solo el 0.02% del PBI anual.

Uno de los principios básicos que ha adoptado este banco, es que el apoyo sólo debe darse en situaciones en que el riesgo de contagio sea significativo, ya que de lo contrario, pueden existir circunstancias en las que sería más saludable permitir que un banco caiga y se liquide antes que intentar rescatarlo, por un tema de costo-beneficio.

### **1.2.1 Caso del Bank of Credit and Commerce (BCCI - 1991)**

En Julio de 1991, el Bank of Credit and Commerce (BCCI) (establecimiento anglo-pakistani), fue acusado de participar en todo tipo de actividades delictivas como ser: tráfico de armas, terrorismo, extorsión y lavado de dinero entre otras.

Ésta representó la quiebra bancaria más importante a la que se tuvo que enfrentar el Reino Unido ya que el BCCI era un banco que apostaba a marcar presencia en el mundo y ya había entablado subsidiarias en más de 50 países.

El gran problema de supervisión que tenía este banco, radicaba principalmente en la distancia existente entre las compañías a través de las cuales se realizaban sus negocios internacionales (instaladas en Luxemburgo y las Islas Caimán) y sus accionistas (localizados en Abu Dhabi y Londres), debido a que esta internacionalización dificultaba el control.

A pesar de que el Banco de Inglaterra estaba al tanto de algunos problemas que tenía el BCCI, decidió apoyarlo recapitalizándolo, pero con la condición de supervisarlo con más atención.

Fue recién cuando el BCCI solicitó a una firma de contadores que elaboraran un informe especial, que quedó al descubierto la verdadera magnitud de los problemas existentes y en esa instancia se iniciaron investigaciones más profundas. El resultado fue un informe donde se plantearon una serie de críticas y recomendaciones al débil control que estaba ejerciendo el Banco de Inglaterra. Las mismas fueron adoptadas no sólo por el Banco de Inglaterra (instalando nuevas unidades de investigación) sino que además fueron recogidas por el Comité de Supervisores de Basilea (estableciendo estándares internacionales más estrictos y dando apoyo legislativo a la Unión Europea y al mundo).

El aporte más importante que dejó el informe sobre la regulación internacional del Comité de Basilea, podemos resumirlo en:

- La posibilidad de rechazar o revocar una autorización bancaria a aquellos bancos que por su estructura de grupo no les sea posible ser supervisados efectivamente;
- establecimiento del requisito de que la oficina matriz de una entidad financiera se encuentre situada en el mismo Estado donde esté registrada su oficina;
- mejores “puentes de acceso” para compartir información entre las entidades reguladoras, contadores y organismos contra el fraude;
- y la obligación para los auditores y demás expertos de informar actividades sospechosas a los supervisores.

### **1.2.2 Caso del Banco de Barings (1995)**

Creado en 1762 y dirigido por los hermanos Barings, este Banco fue uno de los más importantes y antiguos de Gran Bretaña y entre sus clientes se encontraban algunos tan prestigiosos como la Reina de Inglaterra.

En sus inicios, se dedicaba principalmente a la financiación del negocio de la lana pero luego su actividad se expandió hacia otros sectores del comercio internacional. Pero fue cuando este banco incursionó en el mercado de instrumentos financieros tales como “derivados”, que comenzó el principio del fin.

Un funcionario de Barings, comprometió al banco en operaciones financieras que se arbitraban en función del índice de Nikkei y a medida que éste caía, en lugar de retirarse del mercado, realizaba nuevas operaciones para cubrir las pérdidas, es decir duplicaba su apuesta aunque el mercado estuviese en caída.

Esto derivó en la inevitable quiebra del Banco Barings Brothers, cuyas pérdidas ascendieron a 1.4 billones de dólares.

Sin embargo, aunque esta persona fue la principal responsable de los hechos, debemos destacar la indiferencia que demostró el Banco de Inglaterra frente a esta situación. En efecto, la evidencia demuestra que existieron fallas graves en los controles internos y externos del Banco Barings, lo cual facilitó en buena medida las maniobras de fraude interno.

Entre las fallas de los controles internos, se encontraron:

1. Falta de organización dentro de los departamentos del Banco.
2. Exceso de libertad: este funcionario era responsable de las operaciones y también del nivel de riesgos asumidos. Es decir, tomaba las decisiones y las controlaba para prevenir los riesgos.
3. Confianza ciega depositada por la dirección del banco en este funcionario.

Según expertos en la materia, para poder contener los riesgos que conllevan las operaciones en los incipientes mercados financieros es indispensable mantener una clara separación entre los operadores y los que cierran los acuerdos, así como también deberían tener personal capacitado para valorar y gestionar el riesgo.

En lo que respecta a los controles externos, se mencionan los siguientes:

1. Falta de coordinación entre los organismos de contralor para compartir la información y reaccionar rápidamente.
2. Supervisión insuficiente y fallas en la gestión del Banco de Inglaterra.
3. Personal de organismos de contralor con carencias en la capacitación del negocio financiero: no conocen lo que están controlando.
4. Flexibilidad del Banco de Inglaterra en cuanto a la aplicación de la consolidación única, lo cual aumenta la probabilidad de que pasen inadvertidas grandes transferencias internas.

Lo que salta a la vista es que, para poder contar con un sector bancario más seguro y transparente se debían definir nuevas reglas de funcionamiento interno, de reclutamiento de dirigentes y de controles externos.

Según surge de una editorial del Economist:

*“El papel de los gobiernos no es impedir a la gente tomar riesgos, pero sí asegurarse que cuando las cosas salen mal son los jugadores quienes deben pagar y no el público”.*<sup>4</sup>

### **1.2.3 Crisis Financiera en Uruguay y la región (2002)**

Durante el transcurso del año 2002, el sistema financiero Uruguayo se vio sumergido en una de las peores crisis de la historia, la cual acarreó severas consecuencias para el país: el cierre de cuatro bancos importantes (Banco Comercial, Banco de Montevideo, Caja Obrera y Banco de Crédito) una Cooperativa de Intermediación Financiera (CAYCU) y una Institución Financiera Externa (Compañía General de Negocios). En el presente trabajo nos centraremos solo en los dos primeros bancos mencionados.

Para lograr desarrollar los puntos que vienen a continuación sobre la base de una fuente confiable, obtuvimos autorización por parte de la Secretaría de la Cámara de Representantes de la Republica Oriental del Uruguay, para acceder a la Carpeta número 2450/2002 referente a la “Comisión Investigadora sobre diversas actuaciones relacionadas con el Sistema Financiero y Bancario”. Obtuvimos también acceso a la sentencia judicial sobre “Insolvencia societaria fraudulenta”, decretada contra los directivos del Banco de Montevideo (Resolución N°1424 del 11 de septiembre de 2008).

Por lo tanto, obtuvimos una vasta recopilación de material al respecto, el cual trataremos de sintetizar para poder explicar brevemente la relación causal que

---

<sup>4</sup> Según "The bank that disappeared", The Economist, 1995.03.04 en el documento "Productos derivados y bancos a la deriva: El caso "BARINGS" – Autor: Dr. Gerard Verna – Director de la Cátedra de Ética en los Negocios, Instituto de Empresa, Madrid, Profesor de gestión internacional de empresas, Universidad Laval, Québec

existió entre la administración del Riesgo Operativo que llevaban estas entidades y el posterior cierre de las mismas.

### **1.2.3.1. Banco Comercial**

Según surge del material consultado:

El Banco Central del Uruguay constató irregularidades que se estaban llevando a cabo en el Banco Comercial. A continuación nombramos algunas de ellas:

1. Desaparición de títulos de deuda emitidos por el Gobierno Argentino.
2. Desviaciones de fondos hacia inversiones no autorizadas por los clientes a través de una compañía off-shore.
3. Operativa crediticia del banco otorgando créditos a personas físicas y jurídicas vinculadas al mismo grupo económico.
4. Operativa de compraventa de valores a futuro para disfrazar balances.

Con respecto al primer punto, según el inventario de valores del Banco Comercial, éste debía tener depositados en custodia en el Banco General de Negocios de la República Argentina (en adelante BNG) al 31 de diciembre de 2001, valores públicos y privados, propios y de terceros, por un total estimado de US\$ 500.000.000. Sin embargo, el Banco Central Argentino (en adelante BCA) le certifica al BCU que el BGN posee en custodia por cuenta y orden del Banco Comercial títulos de deuda argentinos por aproximadamente US\$ 300.000.000. Según memorando del BCU de fecha 2 de febrero de 2002 denominado “Banco Comercial S.A – Análisis del faltante de valores públicos y otros activos y eventuales necesidades de capitalización”, el faltante de valores públicos y privados expresados a valor nominal del 31 de diciembre de 2001 ascendía a

US\$ 218.307.079, correspondiendo US\$ 199.392.952 a valores propios y US\$ 18.914.127 a valores de terceros.

La operación consistía en que el Banco Comercial captaba depósitos al 4% y transfería este dinero al BGN para comprar bonos argentinos que rendían un 8% o 10 %. Estos valores quedaban depositados en custodia del BGN y el Banco Comercial recibía a título de comprobante, la certificación de que los valores estaban en custodia e incluso certificados de la Caja Nacional de Valores de la República Argentina. Lo que no se constataba era que efectivamente se adquirieran estos bonos.

El Banco Comercial luego de ser vendido, pasó a formar parte del mismo grupo económico que el BGN.

Según la documentación consultada, antes de que el Banco Comercial fuera vendido, no se invertía en bonos argentinos y la resolución de hacerlo se tomó en Comités de Inversiones de los cuales no se llevaba actas o registros de las decisiones tomadas y éstas eran transmitidas de forma verbal. Asimismo, las órdenes de compra no eran incluidas en las transacciones de la mesa de cambios del Banco Comercial, si o que eran realizadas directamente entre los representantes del Banco Comercial y el del BGN.

De la documentación consultada surge claramente la existencia de un faltante de valores, pero lo que no queda tan claro es si dicho faltante se originó internamente en el Banco Comercial o si fue externamente por parte del BGN.

De todos modos, existieron grandes fallas operativas dentro del Banco Comercial ya que, por ejemplo, éste no obtenía certificados fehacientes sobre la compra de los valores.

En cuanto al segundo punto, según la documentación de la Comisión Investigadora, cuando el Banco Comercial se fusionó con el Banco ING, continuó

con la operativa que venía realizando éste a través de ING Curacao, que ahora se convierte en Comercial Investment Curacao (en adelante CI). Es a través de esta sociedad, que el Banco Comercial colocaba el dinero de los ahorristas en el exterior (Ámsterdam). Ni la sociedad, ni su operativa se encontraban registradas en el Banco Central.

El Banco Comercial les ofrecía a sus clientes la opción de invertir en el exterior, suscribiendo con el cliente un contrato de administración de inversiones. Los recursos recibidos diariamente por sus clientes para ser radicados en ING Amsterdam los acumulaban en una partida única que se transfería a ING Amsterdam para la cuenta de CI. Por lo tanto, la cuenta de CI funcionaba como una cuenta colectiva, lo que facilitaba que el cliente perdiera el control de su dinero.

Ya a partir de octubre del 2000, sin que los clientes fueran alertados, el Banco Comercial comenzó a cambiar la composición de las inversiones de la cuenta de CI, vendiendo los bonos uruguayos y comprando bonos argentinos: U.S Treasury Strips Zero Cupon, entre otras inversiones. Según se desprende del memorando del BCU de fecha 6 de febrero de 2002, en la medida que los depósitos de CI en ING respondían a un mandato fiduciario de los clientes, se entiende que el haber desviado esos fondos hacia otras inversiones constituyó una falta grave ya que no se respetó el encargo del cliente.

Desde el punto de vista de Basilea II estaríamos frente a una práctica no recomendada.

Respecto del tercer punto, si tenemos en cuenta que la operativa crediticia con vinculadas se encuentra prohibida por el BCU según los Artículos 38.7, 38.11 y 38.13 de la Recopilación de Normas de Regulación y Control del Sistema Financiero, podemos señalar que el Banco Comercial realizaba actividades no autorizadas.

Según lo analizado se constataron: créditos otorgados en forma irregular (según exigencias del BCU, en carpetas de crédito para personas físicas y jurídicas) a vinculadas al grupo económico; ausencia de análisis previos a la concesión de créditos, información del deudor y de su capacidad de repago; inconsistencia de los datos que surgen de las carpetas y créditos de volúmenes desmedidos en relación con la capacidad económica del deudor y sus garantías; préstamos destinados a actividades especulativas de alto riesgo; concentración del riesgo país (Argentina) e incertidumbre sobre la recuperabilidad de los mismos. Estos créditos, incobrables para el Banco Comercial, alcanzaban aproximadamente la suma de 80 millones de dólares.

Por último, respecto de la compraventa de valores a futuro, se detecta que el Banco Comercial las realizaba con otras empresas del mismo grupo con el objeto de calzar posiciones activas en valores, en su mayoría argentinos, ante una baja del valor de mercado de los mismos.

Lo que se hacía era acordar con un corredor una opción de venta de dichos valores, a precios que se encontraban muy por encima del valor de mercado de los mismos. Por otro lado, el mismo corredor acordaba una opción inversa con otra empresa del mismo grupo de forma tal, que la operación quedara financieramente cuadrada.

Todo esto se hacía con propósitos meramente contables, por lo que estaríamos frente a un típico caso de “maquillaje contable”.

### **1.2.3.2. Banco de Montevideo**

Según la Sentencia anteriormente mencionada, a principios del año 2002 el BCU comienza a notar un aumento del riesgo en empresas vinculadas al grupo (operativa no autorizada por el BCU), además de irregularidades en la documentación de los créditos.

En tal sentido, el 7 de marzo de 2002 el BCU emitió la resolución “D/110/2002”, en la cual ordena al Banco de Montevideo (BM) cesar de inmediato con la concesión de créditos directos o contingentes a personas físicas o jurídicas vinculadas. Asimismo dispuso por la misma resolución, que debían cancelarse en el plazo de 30 días, los créditos concedidos a empresas o personas del grupo, y a presentar un informe con las medidas a adoptar para recomponer la situación patrimonial al estado anterior a la concesión de los créditos.

El Banco Montevideo hace caso omiso a las instrucciones del Banco Central y sigue con la operativa de créditos a vinculadas.

El Tarde and Commerce Bank era una de las empresas vinculadas al Banco Montevideo, éste venía actuando en Uruguay desde hacía muchos años a través de TCB Mandatos S.A., que había sido autorizada por el BCU con el objeto “prestar servicio de asesoramiento y asistencia técnica con el fin de preparar, promover, o facilitar negocios para sus representados” (Art. 450 de la Recopilación de Normas de Regulación y control del Sistema Financiero).

El Banco Montevideo ofrecía a sus clientes participaciones en certificados de depósitos que él mismo realizaba en el TCB Caimán.

Según se expone en la Sentencia, el TCB desde febrero del 2003 no era solvente, ya que no podía cumplir con sus obligaciones. Pese a ello, el BM seguía ofreciendo esta operativa “off shore”, invocando falsamente que el TCB y el BM eran la misma institución y creando la apariencia de que la operativa era rentable y confiable.

Posteriormente, encontramos un apartado en la sentencia que establece que en el TCB existía una cuenta del grupo al que pertenecía el BM (cuenta N° 5000), a la cual se desviaban los fondos que remitía el BM y de otras empresas vinculadas. Los fondos de esta cuenta se destinaban a uso personal de las empresas del grupo, no siendo declarada en el balance del TCB, constatándose que existía un doble juego de libros. Según declaraciones efectuadas, entre los años 1988 y 2002, se desviaron hacia esa cuenta entre \$ 500.000.000 y \$ 700.000.00.

Nuevamente, si miramos esta operativa desde el punto de vista de Basilea II estaríamos frente a una práctica no recomendada.

Podemos concluir que al igual que en el caso del BCCI, cuando el problema se origina en la parte superior del organigrama del banco o entre sus accionistas, no hay sistema de control interno que pueda evitar que surjan pérdidas por riesgo operativo. Esto demuestra la importancia de realizar una buena gestión de Gobierno Corporativo.

### 1.3. Origen y desarrollo del Riesgo Operacional

Antes de la publicación del documento “Nuevo Acuerdo de Capitales” de Basilea II (en junio de 2004), el Riesgo Operacional se definía de manera imprecisa comprendiendo riesgos que no eran normalmente tratados y administrados por las entidades financieras.

Dicho riesgo ha ido tomando una importancia creciente en la última década por entre reguladores y entidades financieras. En particular, el Comité de Supervisión Bancaria de Basilea (BCBS) ha señalado que, la desregulación y globalización de los servicios financieros en conjunto con la creciente sofisticación de las tecnologías financieras, han contribuido a que los bancos se encuentren más expuestos a nuevos riesgos que surgen de factores tales como:

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

Todo esto ha desembocado en un sistema financiero significativamente más complejo que da lugar a que estos eventos de riesgo operacional sean más probables y tengan un mayor impacto. Lo anterior, sumado al aumento de pérdidas mundiales generadas por eventos de *Riesgo Operativo*, llevaron a los bancos y supervisores a considerar la gestión de este tipo de riesgo como una disciplina integral.

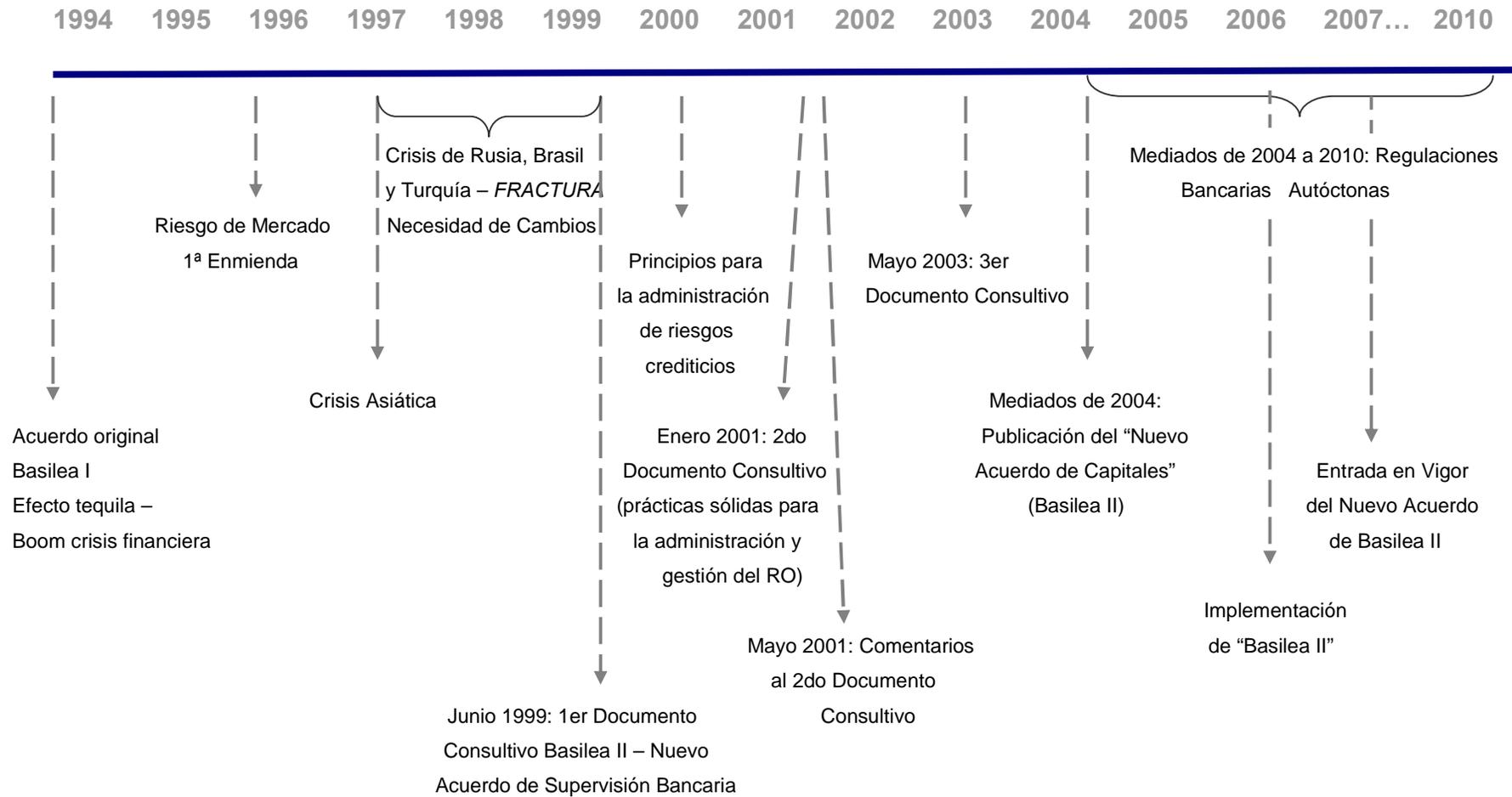
En respuesta a este fenómeno, las entidades han incrementado los recursos asignados a este riesgo ya sea mejorando los sistemas de control o creando nuevas técnicas para lograr un mejor sistema de gestión.

Es a partir de este momento que se comienza a hablar de *Riesgo Operativo* como una categoría separada de riesgo, que al igual que el de Crédito y de Mercado se debe medir y controlar.

Es así, que el Comité de Basilea decide recoger la preocupación e importancia que los supervisores deben otorgar a este riesgo e introduce en el Nuevo Acuerdo de Capital, *exigencias de capital* explícitas por *Riesgo Operacional*.

A continuación detallaremos la evolución histórica de los 2 documentos consultivos de Basilea:

## EVOLUCIÓN HISTÓRICA DE LOS ACUERDOS DE CAPITALES DE BASILEA



## **1.4. Conceptos generales. Definiciones y alcances de las mismas.**

Luego de la introducción al RO realizada en el apartado anterior, corresponde ahora abocarnos a su desarrollo.

### **1.4.1. Definición de Riesgo**

Para poder arribar a una de definición de riesgo operativo, es necesario saber como define la palabra *Riesgo*, algún Diccionario. En tal sentido, la Vigésima segunda edición del Diccionario de La Real Academia Española, lo define como: *“Contingencia o proximidad de un daño”*.

También podemos encontrar otras definiciones tales como: *“Quebranto económico potencial (todavía no realizado) que se deriva de la posible realización de eventos adversos”, “los eventos son adversos respecto de un resultado esperado”*.<sup>5</sup>

### **1.4.2. Definición de Riesgo operativo**

Se entiende que el Riesgo Operacional no es un riesgo “nuevo”, sino que siempre se encontró presente en las instituciones (cualquiera fuese el ramo en el que las mismas se desenvuelven). Sin embargo, es evidente que hasta ahora no existía una acepción única, ya que para algunas entidades el RO abarcaba prácticamente todo aquello que quedaba fuera del riesgo de crédito o mercado, mientras que para otras se reducía a fallas en la operación o proceso, por lo cual era vital desarrollar una definición concreta del mismo.

---

<sup>5</sup> Riesgo operativo de Angel Vilariño, Guatemala, septiembre 2005, Presentación Power Point web: [www.sib.gob.gt/es/presentaciones\\_y\\_conferencias/X1.ppt](http://www.sib.gob.gt/es/presentaciones_y_conferencias/X1.ppt)

Según el documento “International Convergence of Capital Measurement and Capital Standards. A revised framework” (“Basilea II” o “Nuevo Marco de Capitales”), el Comité de Basilea adoptó una definición específica de lo que se entiende por Riesgo Operacional que resultó del consenso de reguladores de 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 eventos externos. Esa definición incluye al riesgo legal, pero excluye el riesgo estratégico y reputacional”.<sup>6</sup>*

### C. Definición de Riesgo Legal

Según Basilea el Riesgo Legal refiere a aquél que surge de la “posibilidad de ser sancionado, multado u obligado a pagar daños punitivos como resultado de acciones supervisoras o de acuerdos privados entre partes”.<sup>7</sup> Como podemos ver toda empresa se encuentra expuesta a este riesgo, ya que son diversas las regulaciones a las que se encuentran sometidas y diversos también, los contratos que suscriben, ya sean con clientes, proveedores, empleados y accionistas.

---

<sup>6</sup> Según el BCBS, en Boletín de Asesoría Gerencial N° 8 – 2008, “Riesgo Legal desde la perspectiva del Riesgo Operacional”, Espiñeira, Seldom y Asociados firma miembro de PriceWaterHouseCoopers

<sup>7</sup> Según el BCBS, en Boletín de Asesoría Gerencial N° 8 – 2008, “Riesgo Legal desde la perspectiva del Riesgo Operacional”, Espiñeira, Seldom y Asociados firma miembro de PriceWaterHouseCoopers

## *D. Definiciones de Riesgos Estratégico y Reputacional*

### *B.1 Riesgo Reputacional*

La “reputación” es un bien intangible que las instituciones proyectan sobre sus inversiones, clientes y empleados, que genera en ellos aceptación, desaprobación o indiferencia.

Según lo antedicho, podemos definir al Riesgo Reputacional como la posibilidad de que una entidad incurra en pérdidas por desprestigio, mala imagen, publicidad negativa, cierta o no, respecto de la institución y sus prácticas de negocio y que, a raíz de esto se pierdan clientes, disminuyan los ingresos o se inicien procesos judiciales que involucren a la entidad.

Es decir que el riesgo reputacional puede surgir de fallas operacionales, del incumplimiento de leyes y reglamentos, o de otras fuentes y puede ser muy dañino para las instituciones en la medida que, dado la naturaleza del negocio, es imprescindible mantener la confianza de los clientes, acreedores y del mercado en general.

En definitiva, podemos decir que el riesgo reputacional nace a partir de la materialización de otras clases de riesgos y en particular del riesgo operacional.

### *B.2 Riesgo Estratégico*

Según especialistas en la materia, el Riesgo Estratégico es uno de los principales elementos que impactan sobre el valor de una institución.

Se lo define como aquél que tiene un impacto destacado sobre las palancas básicas de creación de valor de la organización. Este riesgo depende

mayormente del entorno, tanto interno como externo, en que se desenvuelve la institución y de las estrategias elegidas para la orientación de sus actividades dentro de ese entorno. Es decir que la forma en que se posicionen las entidades financieras en su entorno, influye enormemente en la exposición al riesgo que tendrán que asumir.

Se pueden identificar 2 clases de riesgos estratégicos:

- el sistemático: es aquél al que está expuesta una institución por el simple hecho de competir en un sector determinado;
- y el no sistemático, único o idiosincrásico: es el propio, individual y específico de cada institución.

En definitiva, podemos decir que son 2 los aspectos novedosos que se establecen en el documento de Basilea II para el tratamiento del riesgo operativo:

1. La consideración de este riesgo como una categoría bien definida y separada, que requiere una gestión integral.

El RO difiere de otros riesgos bancarios ya que se produce en el día a día repercutiendo en el proceso de gestión, mientras que los riesgos de crédito y de mercado son aceptados a cambio de un beneficio esperado.

Además, si el riesgo operacional no se controla de forma adecuada, podría verse afectado el perfil de riesgo de la institución, exponiéndola a potenciales pérdidas significativas. Con “perfil de riesgo” nos

referimos al resultado consolidado de la medición permanente de los riesgos a los que se ve expuesta la entidad.

2. El hecho de medir las pérdidas ocasionadas por RO y requerir capital para afrontarlas.

Con respecto a estos dos puntos, podemos agregar que si bien la mayoría de las veces la atención se centra en el aspecto de la “medición” y se le resta importancia al primer aspecto sobre gestión integral del mismo, Basilea II impone la necesidad de contar con buenas prácticas de gestión (contenidas en el documento de 2003), como *precondición* para la aplicación de técnicas de medición y cuantificación del mismo.

### **1.5. Importancia de la Gestión y Administración del RO**

El BCBS puntualiza que anteriormente, los bancos gestionaban sus riesgos operativos únicamente mediante prácticas de control interno y auditorías. Hoy por hoy, se siguen utilizando estos mecanismos pero a su vez se está incursionando en la aplicación de nuevos procesos para gestionarlo, ya que las entidades se han convencido de que éstos proporcionan mayor seguridad y solidez al banco.

El Comité reconoce que en la práctica, el enfoque exacto elegido por cada entidad para la administración de su RO, va a depender de una serie de factores como ser:

- el tamaño;
- la sofisticación tecnológica con que se maneja;

- la naturaleza y complejidad de sus actividades.

No obstante ello, los siguientes elementos son de crucial importancia para bancos de cualquier tamaño y alcance:

- **Estrategias** bien definidas y su seguimiento por parte de la Alta Gerencia y administradores de riesgo;
- una **sólida cultura de gestión** del riesgo operativo y de **control interno** (como ser líneas claras de responsabilidad y segregación de funciones, entre otras);
- herramientas eficaces para la transmisión interna de información y **planes de contingencia**.

Siguiendo esta misma línea, el Comité destaca la importancia de que cada entidad financiera al momento de definir el enfoque anteriormente mencionado, detecte los riesgos operativos a los que se enfrenta y recoja las principales causas que ocasionaron pérdidas graves por este riesgo.

En tal sentido, el Nuevo Acuerdo de Basilea clasifica detalladamente posibles pérdidas directamente asociadas a esta categoría de riesgo, con lo cual las entidades deberían asignar sus datos de pérdidas a cada una de las siguientes categorías:

- ***Categorías relacionadas con personas:***

- Fraude interno:

Pérdidas derivadas de algún tipo de actuación destinada a cometer fraude, apropiarse de bienes indebidamente o eludir leyes, reglamentaciones, resoluciones, normativas o políticas empresariales, en las que se encuentra implicado por lo menos una persona interna a la empresa.

- Políticas de empleo y seguridad laboral:

Pérdidas derivadas de actividades incompatibles con la legislación, acuerdos laborales, higiene y seguridad en el trabajo. También se incluye el pago de reclamos por daños al personal, por casos relacionados con la diversidad/discriminación; por aspectos relativos a la remuneración prestaciones sociales, extinción del contrato y la organización laboral.

- ***Categorías relacionadas con procesos:***

- Ejecución, entrega y gestión de procesos:

Pérdidas derivadas de errores en el procesamiento de operaciones o en la gestión de procesos, así como de relaciones con contrapartes comerciales y proveedores. Por incumplimiento en la obligación de informar, documentación extraviada, acceso no autorizado a la información, registro incorrecto de clientes, entre otros.

- Clientes productos y prácticas comerciales:

Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación frente a clientes. También incluye, pérdidas por la naturaleza o diseño de un producto, violación de privacidad de los clientes, el uso inadecuado de información confidencial o la responsabilidad de la contraparte.

- ***Categorías relacionadas con Sistemas:***

- Interrupción de operaciones o fallos del sistema:

Pérdidas derivadas de la interrupción de operaciones o fallos de sistemas.

- ***Categorías relacionadas con fuentes externas:***

- Daños o pérdidas de activo fijo:

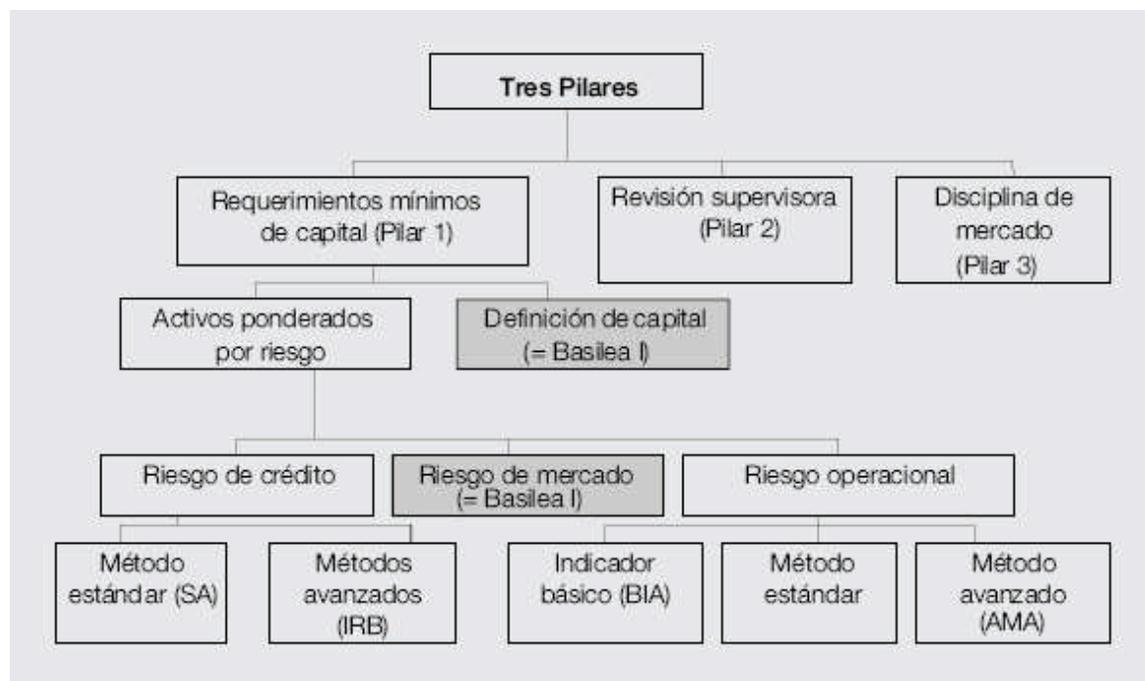
Terrorismo, vandalismo, terremotos, incendios, inundaciones, etc.

- Fraude externo:

Pérdidas derivadas de algún tipo de actuación destinada a defraudar, apropiarse de bienes indebidamente, o eludir la legislación por parte de un tercero, como por ejemplo robo, hurto, falsificación, utilización de cheques sin fondo, entre otros.

## 1.6. Tratamiento del Riesgo Operacional en Basilea II

La estructura del Nuevo Acuerdo de Basilea, se compone de 3 pilares los que detallamos a continuación.



8

### 1.6.1 Pilar I: Requerimientos mínimos de capital

Como ya hemos mencionado en los puntos anteriores, Basilea II brinda un marco de referencia para la gestión integral de riesgos, el cual está siendo progresivamente adoptado, tanto por los supervisores como por las instituciones.

<sup>8</sup> “El Nuevo Acuerdo de -Capital Basilea II- y su transposición europea: El proceso y la implementación”

En este marco, se contemplan 3 grandes riesgos que deben ser considerados al momento de determinar el requerimiento de capital a mantener, siendo éstos: Riesgo de Crédito, Riesgo de Mercado y Riesgo Operacional.

Propone tres métodos de complejidad creciente para el cálculo del requerimiento del capital por RO, a los que llama: *Modelo del Indicador Básico*, *Modelo Estándar* y *Métodos de Medición Avanzados (AMA, sigla en inglés)*.

Los dos primeros se caracterizan por ser sensibles al riesgo, dado que determinan el requerimiento de capital en forma simplificada a través del producto entre los ingresos brutos anuales medios y el coeficiente de exigencia de capital.

En los *AMA* el requerimiento de capital es determinado según la estimación del riesgo operacional al que realmente está expuesta la empresa. Para la realización de esta estimación se deben desarrollar modelos estadísticos de medición interna. Como veremos más adelante, en el marco de Basilea II la posibilidad de utilizar modelos internos está sujeta a la aprobación del supervisor junto con el cumplimiento de requerimientos cualitativos adicionales.

#### Modelo del Indicador Básico (BIA):

Dicho método consiste en multiplicar un porcentaje fijo ( $\alpha$ ) por un indicador de la exposición al riesgo operacional (ingresos brutos). El porcentaje ha sido fijado en un 15%, que es la cifra que relaciona dicho indicador con el nivel deseado de recursos propios en el sistema financiero. El capital requerido en este enfoque es la media de los ingresos brutos anuales (positivos) de los tres últimos ejercicios.

Resumiendo:

$$RC_{BIA} = [\sum (IB_{1...n} \times \alpha)]/n$$

Donde:

$RC_{BIA}$ : Requerimiento de Capital por el Enfoque Básico

IB: ingresos anuales brutos, siempre que los mismos sean positivos en los últimos tres años.

$\alpha$ : 15%

n: número de años, de los tres últimos años con ingresos positivos.

Basilea II define ingresos brutos como los ingresos netos por intereses más otros ingresos netos ajenos a intereses, esta medición excluye las provisiones, los gastos de exportación, los resultados realizados por la venta de valores de la cartera de inversión y los resultados extraordinarios o los ingresos derivados de las actividades de seguros.

El objetivo de este método fue buscar la simplicidad a la hora de medir el requerimiento de capital, y que pudiese ser compatible entre diferentes jurisdicciones.

#### Modelo Estándar (SA):

Sigue la misma línea simplificadora del método anterior, pero con la diferencia de que en este método las entidades quedan obligadas a dividir sus actividades en ocho líneas de negocio. Consiste en multiplicar unos porcentajes fijos ( $\beta$ ) por un

---

<sup>9</sup> “El tratamiento del riesgo operacional en Basilea II”, María Ángeles Nieto Giménez-Montesinos

indicador de la exposición al riesgo operacional (ingresos brutos) en cada una de las líneas de negocio.

Resumiendo:

$$RC_{SA} = \left\{ \sum_{\text{años 1-3}} \max[\sum (IB_{1-8} \times \beta_{1-8}), 0] \right\} / 3$$
<sup>10</sup>

Donde:

RC<sub>SA</sub>: Requerimiento de Capital por el Método Estándar

IB: Ingresos brutos de cada línea de negocio

β: Porcentaje fijo, cuyo valor por cada línea de negocio se detalla a continuación:

(β1) Finanzas corporativas	18%
(β2) Negociación y ventas	18%
(β3) Banca Minorista	12%
(β4) Banca Comercial	15%
(β5) Liquidación y pagos	18%
(β6) Servicios de Agencia	15%
(β7) Administración de Activos	12%
(β8) Intermediación minorista	12%

Es un método de cálculo que requiere por parte de las entidades la realización de una gestión activa de su riesgo operacional. En tal sentido, para poder optar por este método se deberán cumplir ciertos requisitos cualitativos bastante exigentes como ser: la implicación activa de la alta dirección y el consejo de administración; que el sistema de evaluación de riesgo sea sólido y esté

---

<sup>10</sup> "El tratamiento del riesgo operacional en Basilea II", María Ángeles Nieto Giménez-Montesinos

plenamente integrado en la gestión diaria de riesgos de la entidad; y que la entidad cuente con recursos suficientes tanto en las líneas de negocio como en las áreas de control y auditoría. Además, requiere que la entidad cuente con un sistema de evaluación y gestión de riesgo operacional que, primero que nada se encuentre integrado dentro de los procesos de gestión de riesgos de la entidad, se asigne responsabilidades a una unidad de riesgo operacional, se realice un seguimiento de las pérdidas relevantes sufridas en cada línea de negocio, se generen reportes informativos sistemáticos a la dirección de las líneas de negocio, Alta Gerencia y al consejo de administración, con su correspondiente documentación y por último, que sea validado interna y externamente por los auditores y/o supervisores.

Asimismo, existe un *Método Estándar Alternativo (ASA)*, que cumple con el objeto de subsanar algunas deficiencias que presentó el *Método Estándar Tradicional (SA)* al ponerse en práctica. La diferencia consiste en que para las dos líneas de negocios en las que se observó el problema (un doble cómputo en el riesgo de crédito y en el riesgo operacional), que fueron la banca minorista y la banca comercial, se tomó como indicador de riesgo operacional la cifra de los préstamos en balance en lugar de una cifra de margen. Para el cálculo de los requerimientos de capital de estas dos líneas de negocio se multiplica el indicador de cada una de ellas por un coeficiente reductor ( $m$ ) que ha sido fijado en un 3.5% y por sus betas correspondientes.

Es importante que la entidad reflexione a la hora de usar este último método, ya que el Comité de Basilea entiende que el mismo sólo puede ser usado bajo la aprobación del supervisor nacional y una vez que la entidad opta por el ASA, no podrá volver al SA sin autorización del supervisor.

### Métodos Avanzados (AMA):

La novedad y el atractivo de la utilización de los modelos internos como éste, radica en que la entidad puede utilizar el resultado de su propio modelo (que ha sido diseñado según sus necesidades de gestión), a efectos regulatorios.

Existen ciertos requerimientos necesarios para la aplicación de modelos internos:

#### *A. Requerimientos generales*

Basilea II sienta criterios generales cualitativos y cuantitativos muy rigurosos, que deberían cumplir las entidades que quieran adoptar el modelo AMA, para obtener la autorización del regulador a estos efectos.

En síntesis, requiere la implicación activa por parte de la alta dirección y del consejo de administración en la gestión de riesgo operacional; que el modelo interno sea sólido y esté plenamente integrado a los sistemas de medición y gestión de riesgos de la entidad; y que la entidad cuente con recursos suficientes tanto en las líneas de negocio como en las áreas de control y auditoría.

#### *B. Requisitos cualitativos*

Se considera imprescindible que las entidades implanten y mantengan rigurosos procedimientos para la elaboración de sus modelos internos y que exista una validación independiente de tales modelos. En resumen, la entidad deberá cumplir los siguientes requisitos cualitativos:

- Contar con una unidad independiente de gestión del riesgo operacional responsable del desarrollo e implantación de la metodología de cálculo.

- Que el modelo interno de medición de riesgo operacional esté totalmente integrado en los procesos de gestión de riesgos de la entidad.
- Existencia de un sistema de divulgación de información periódico a las direcciones de las líneas de negocio, a la alta dirección y al consejo de administración.
- El sistema debe estar adecuadamente documentado.
- Debe ser validado interna y externamente.

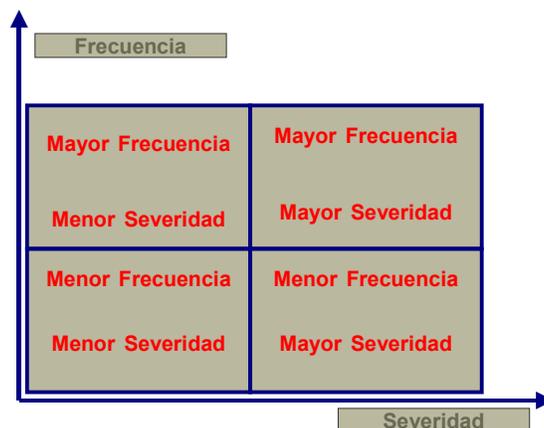
*C. Requisitos cuantitativos:*

Los reguladores exigirán a la entidad que calcule su capital regulatorio como la suma de la pérdida esperada y la inesperada, a menos que pueda demostrar que ya ha efectuado una medición de la pérdida esperada y la está cubriendo de alguna forma.

Todos los modelos AMA deberán utilizar los cuatro elementos que componen un sistema de medición de riesgo operacional, ellos son: datos internos, datos externos, escenarios y factores de control y entorno de negocio.

Comenzamos por los *datos internos*: son los datos más útiles en un modelo interno debido a que son los que mejor representan la estructura del negocio, los sistemas de control y la cultura de cada organización.

Si clasificamos los datos según su frecuencia y su impacto, obtendríamos el siguiente cuadro<sup>11</sup>:



El problema para las entidades se encuentra básicamente en el cuadrante inferior derecho, ya que el simple hecho de mantener un registro histórico de las pérdidas relacionadas con este tipo de riesgos no es suficiente para modelizar las pérdidas por RO. Por lo anterior, Basilea II entiende que las entidades deberían complementar sus datos internos con datos provenientes de otras entidades, es decir del exterior (*datos externos*).

En la actualidad existen dos tipos de bases de datos externas, una *base de datos pública*, que recopila información suministrada por proveedores tales como empresas de consultoría o compañías aseguradoras, y por otro lado, tenemos la *base de datos de consorcios de entidades de crédito*, ya sea en el ámbito local o internacional.

Incluso cuando la entidad utilice datos internos y externos para mejorar sus estimaciones, estos datos solo proporcionarían información sobre el pasado, y no siempre los datos del pasado son los mejores para predecir el futuro, sobre todo cuando cambia la realidad del negocio. Por lo tanto, el banco deberá

---

<sup>11</sup> "El tratamiento del riesgo operacional en Basilea II", María Ángeles Nieto Giménez-Montesinos

utilizar, adicionalmente *análisis de escenarios*, basados en las opiniones de los directores y expertos en la gestión de riesgos, para poder obtener evaluaciones razonables de pérdidas severas que podrían sufrir.

Por último, cada entidad deberá identificar los factores básicos de su *entorno de negocio* y su *control interno*. El considerar dichos factores les permitirá obtener evaluaciones de riesgo más orientadas hacia el futuro, y que reflejen de forma más directa la calidad de los entornos operativos y de control propios de la institución.

Basilea II establece los requisitos mínimos que deben reunir los datos internos, para asegurar que la base sea suficiente tanto en términos cuantitativos como cualitativos.

Estos requisitos son:

- Los datos de pérdida deben ser completos y recoger la totalidad de las actividades y exposiciones de relevancia en todas las ubicaciones geográficas.
- Se marca un umbral de pérdida, de por ejemplo 10.000 euros, a partir del cual se empieza a recopilar información.
- Una de las dificultades a la hora de crear una base de datos interna es la delimitación del riesgo operacional con respecto a otros riesgos. Un caso frecuente son las pérdidas por riesgos de crédito, que inicialmente se originaron por algún evento de tipo operacional.
- Un caso especial en la recopilación de datos de pérdida es el tratamiento de *eventos múltiples* (son aquellos que siendo un único evento, afectan a varias líneas de negocio) y *eventos prolongados en el tiempo* (por ejemplo un fraude concebido bajo un plan de acción y materializado en

varias operaciones secuenciales). Se deberán establecer sistemas para la recopilación de este tipo de datos.

- Se exige un período mínimo de observaciones de cinco años. No obstante ello, y teniendo en cuenta que la creación de esta base es relativamente reciente, se contemplará que la primera vez que el banco presente el modelo interno a efectos regulatorios, se aceptará un mínimo de tres años de base histórica.
- Finalmente, la entidad deberá ser capaz de asignar los datos recopilados a las categorías supervisoras de eventos de pérdidas y líneas de negocio.

### **1.6.2 Pilar II: Examen del Supervisor**

Este pilar, apunta básicamente a procurar que las entidades evalúen sus necesidades y posiciones de capital en función de sus perfiles de riesgos y que los supervisores examinen y tomen las medidas adecuadas en respuesta a estas evaluaciones. Es importante que tanto los supervisores como las entidades, establezcan procedimientos rigurosos para evaluar sus riesgos ya que esto repercute directamente en la adecuación del capital.

Los sistemas de control y supervisión deben actualizarse continuamente, con monitoreos y revisiones profundas, debido a los constantes cambios de la realidad del entorno y a la creciente complejidad que presentan las instituciones financieras.

### **1.6.3 Pilar III: Disciplina de Mercado**

Basilea II, menciona este pilar como un complemento deseable y necesario de los dos pilares anteriores. Se trata de la difusión de información útil y necesaria para ayudar a los participantes del mercado a evaluar el perfil de riesgo y el nivel de capitalización de los bancos. Esta divulgación de información contribuye a lograr la transparencia de los mercados financieros, dejando en evidencia la exposición al riesgo que mantienen los bancos y facilitando la realización de comparaciones.

#### ***En resumen:***

- El RO es un riesgo no-financiero, que al igual que el de crédito y de mercado, debería ser gestionado y monitoreado.
- Se sub-divide en las siguientes categorías: riesgo de acontecimientos internos, riesgo de sucesos externos y riesgo de acontecimientos en el ámbito de los negocios, en función de la clase de hechos que le den origen. Al momento de tomar una medida para gestionar el riesgo operativo, se debería atender a la categoría de riesgo a la cual nos estamos enfrentando. Estas sub-categorías no son rígidas, es decir que un riesgo operativo que se origine debido a un suceso externo, podría luego convertirse en un riesgo de negocios.
- Existen diversas y contradictorias opiniones acerca de cómo debería ser gestionado este riesgo, y no existe ningún método de cuantificación y medición del mismo con el que todos estén de acuerdo. Hay quienes se inclinan por la prevención de eventuales fallas en los controles internos, enfocándose en la mejora de las prácticas de gestión, y hay otros que

afirman la necesidad de un capital regulador para hacer frente a las consecuencias del acaecimiento de riesgos operativos.

- Entendemos que es imprescindible atender a la estructura y características de cada institución financiera de manera de establecer si es suficiente y viable mantener capital inmovilizado para hacer frente a los riesgos operativos, o si, por el contrario, es más eficiente apuntar a la prevención y mejora de las prácticas de gestión. Dependerá del contexto en el que se nos presente esta disyuntiva.

## **1.7. Elementos a considerar para gestionar adecuadamente el RO**

### **1.7.1 Buenas prácticas para la gestión del RO**

Según el Comité de Basilea, se entiende por *gestión del riesgo operacional*, la identificación, evaluación, seguimiento y control/cobertura de este riesgo, a diferencia de lo que anteriormente había considerado como “identificación, cálculo, seguimiento y control” del riesgo. (*Ver Anexo I: “Buenas Prácticas para la gestión y supervisión del Riesgo Operativo”*)

Este Comité también establece los Principios Básicos para una Supervisión Bancaria Efectiva (“Basel Core Principles” BCP)

Estos principios son considerados un marco de estándares mínimos sobre buenas prácticas de supervisión y son universalmente aplicables y aceptados.

En particular es de destacar el *Principio N° 15*, el cual está enteramente dedicado al riesgo operacional y éste fue incluido en el documento de los BCP publicado en 2006. (*Ver Anexo II: Principio Básico N°15 – Riesgo Operacional*)

### **1.1.2 Gobierno Corporativo**

“Gobernar” proviene del latín “Gubernare” (dirigir un navío), y éste a su vez, tiene su origen en el idioma griego.

Hay varios matices que permitirían arribar a una definición de “Gobierno Corporativo” (GC), por lo que nombraremos algunas definiciones al respecto que resultan de interés.

Se lo relaciona con el campo de estudio de teoría económica que trata los fenómenos que surgen cuando hay separación entre control y propiedad. Esta

separación se da a raíz de que en la evolución de las corporaciones, éstas dejan de ser negocios familiares y pasan a intervenir distintos actores como ser: trabajadores, propietarios o accionistas, acreedores, gerentes, proveedores, entre otros. Cada uno de estos actores persigue distintos propósitos dentro de la organización y es con esta separación de funciones que nace el problema de Gobierno Corporativo. El problema radica en la dispersión de la propiedad dentro de cada organización, ya que aunque cada vez más individuos participan en ellas, el control se concentra en pocas manos lo cual puede beneficiar o perjudicar a muchos individuos, cambiar las condiciones del mercado, afectar distintas zonas geográficas y por todo esto, fomentar o detener el crecimiento de un país.

El Economista Félix Campoverde (Catedrático y Asesor empresarial de Guayaquil-Ecuador), refiere al GC como el conjunto de reglas, políticas, y procedimientos que se utilizan para controlar y dirigir la organización corporativa de una forma equitativa y responsable. Está regido por los siguientes principios:

- Transparencia de la información (disponer de normas contables adecuadas y un sistema efectivo de auditoría externa).
- Igualdad en el tratamiento a los accionistas (gobierno corporativo interno).
- El orden y control de los mercados financieros (gobierno corporativo externo).

En definitiva, el GC conlleva la determinación de reglas claras para todas las partes involucradas en una institución, es decir los grupos de interés o “stakeholders”. De esta forma, se estaría delimitando lo que le corresponde a cada parte y garantizando que todos alcancen el fin perseguido.

Es así que un Buen GC, influye en lograr un equilibrio entre los objetivos económicos y sociales, incentivando el uso eficiente de recursos y exigiendo

rendición de cuentas a los encargados de administrarlos para evitar fraudes que vayan en contra de la entidad, de la comunidad y del Estado.

Siguiendo esta misma línea, podemos decir que las *Buenas prácticas de Gobierno Corporativo*, contribuyen a la mejora en el uso de los recursos de las entidades; a una mayor transparencia contable y mitigan los problemas de información. La ausencia de estas buenas prácticas, se traducen en divulgación de información inoportuna e incompleta, abuso de accionistas mayoritarios, falta de independencia e integridad de los procesos de auditoría y contratación de personal no calificado para desempeñar tareas de importancia, entre otros, lo cual perjudica el manejo eficiente de los recursos y el cuidado del patrimonio de los inversionistas y acreedores.

Según el Comité de Basilea, las entidades financieras deben:

- contar con manuales de las operaciones que realizan, donde se detalle la tolerancia de RO permitida y quienes son los responsables de hacer cumplir las políticas fijadas por la Dirección;
- tener sistemas adecuados en función de sus necesidades, es decir, contar con “sistemas a medida”;
- procurar contratar personal suficiente, con la experiencia y conocimiento adecuado según requieran cada una de sus unidades de negocio;
- tener un sistema adecuado de control de riesgos, ya que una pobre supervisión y conductas inadecuadas en el manejo de los negocios puede desembocar en el fracaso de la administración, poniendo en riesgo el dinero del público;
- hacer un seguimiento diario de las operaciones, cumplir con los requerimientos de información, procesamiento de datos, planes de

contingencia, entre otras prácticas que resulten relevantes para el desarrollo adecuado del negocio;

- establecer un sistema efectivo de control interno;
- imponer un marco de políticas de administración de riesgos que se deben cumplir. Comprender y administrar el riesgo operativo puede ser trascendente para reducir la probabilidad de que algunos riesgos no sean reconocidos y controlados. Es responsabilidad del Directorio y la Alta Gerencia fijar el manejo adecuado del riesgo y la exposición de la entidad.

Resulta relevante agregar, que en junio de 2002, las empresas norteamericanas tuvieron que ajustarse a un nuevo marco regulatorio acerca de GC, como consecuencia de los grandes fraudes corporativos (Enron, Worldcom, etc), que tuvieron lugar en ese tiempo. Es así que entra en vigor la Ley Sabarnes-Oxley (SOX), que obliga principalmente a las organizaciones que cotizan en la Bolsa de EEUU (SEC). Esta ley, cambia las reglas para los directores, auditores y para el resto de la entidad.

Tiene por objeto primordial, la protección del accionista asegurando la transparencia de información en los mercados, exigiendo que la misma sea oportuna, precisa, fiable y comprensible y mediante la prevención de fraudes financieros.

Se dice que es la ley más severa de la historia en cuanto a la regulación para la exposición contable, auditorías y presentación de balances.

Aunque la aplicación de esta normativa significa la asunción de enormes costos para las entidades, la están aplicando también aquellas que no tienen obligación de hacerlo ya que consideran que su aplicación, en el largo plazo, redundará en importantes beneficios debido al máximo nivel de control que ésta representa.

### **1.1.3 Teoría de la Agencia**

El problema de “agencia”, está enmarcada en el Gobierno Corporativo, en el sentido que nace a partir de los conflictos de intereses que se originan entre los diversos agentes que participan en una entidad o “stakeholders”.

Se ha evidenciado que muchas veces la relación de agencia acarrea riesgos que se identifican como la causa subyacente en el surgimiento de pérdidas operativas.

Esta relación de agencia implica la existencia del problema del riesgo moral, y el hecho de que para motivar a una parte (agente) con intereses propios a que realice servicios en beneficio de otra (principal), ésta debe delegar autoridad para que el agente tome decisiones y es entonces cuando el principal pierde el control. Así puede ocurrir que el agente, en su búsqueda de beneficios personales, actúe en perjuicio de los intereses de la entidad.

La importancia de esta teoría radica en que este hecho puede presentarse en cualquier forma de contrato laboral ya que cada trabajador tiene capacidad de decisión acorde al nivel jerárquico en que se encuentra y con esto también tiene poder de desvirtuar o desviar el resultado de su trabajo. De esta forma, es que los accionistas podrían incurrir en costos para supervisar a los directivos o los directivos tomar decisiones que generen pérdida a los accionistas, y esto comprende lo que se denomina “costos de agencia”. Estos costos también pueden originarse entre la Alta Gerencia y el resto de la entidad o en los acreedores de la misma.

Es entonces para minimizar estos costos que los propietarios nombran un Consejo de Administración, quien se va a encargar de supervisar a los directivos.

La existencia de esta situación da origen al gobierno corporativo. El GC es el mecanismo a través del cual se asegura que los “agentes” estén motivados en alinear su comportamiento real con el del principal y demás grupos de interés, evitando divergencia y conflicto de intereses y asimetría de la información. Se debe lograr que las decisiones de los agentes coincidan con los intereses del principal. Es decir que un sistema perfecto de GC, le daría a los directivos todos los incentivos correctos para tomar decisiones de inversión y financiamiento que maximicen el valor de la entidad.

Fuentes consultadas:

- Documento "Productos derivados y bancos a la deriva: El caso "BARINGS" – Autor: Dr. Gerard Verna – Director de la Cátedra de Ética en los Negocios, Instituto de Empresa, Madrid, Profesor de gestión internacional de empresas, Universidad Laval, Québec.
- El escándalo de la BCCI fue el objeto de numerosos estudios y publicaciones. Nosotros nos referimos principalmente a "The BM Affair", informe del Sen. Joseph Kerry (D-Mass.) y Sen. Hank Brown (R-Colo.) para el Comité del Senado para Relaciones Extranjeras (The Senate Committee on Foreign Relations, Subcommittee on Terrorism, Narcotics and International Operations 30 septembre 1992.) Texto completo y consultable en: <http://www.fas.org/irp/congress/>
- "Las causas de las crisis bancarias y su manejo" Autor: Tony Latter 63, Primera Edición, 1998 México, D.F. (Publicado en inglés por el Centro de Estudios de Banca Central, Banco de Inglaterra, Londres EC2R 8AH, julio de 1997).
- MPRA – "Sound practices for the management of operational risk in financial institutions" in spanish. Pailhé, Cristina, Delfiner, Miguel and Mangialavori, Ana Central Bank of Argentina. January 2007. Web: <http://mpra.ub.uni-muenchen.de/1803/> MPRA Paper No. 1803, posted 07. November 2007 / 02:00)
- "La valoración de las empresas a la luz de Basilea 2" Prof. Jorge Soley – Ahmad Rahnama Madrid 11 de Marzo de 2004
- Presentación Power Point: "Como prepararse para la implementación de Basilea 2 en el ámbito bancario" Montevideo 15 de Octubre de 2004 – Dr. Daniel Jorge Biau - Banco de la Nación Argentina) (Segundo doc consultivo dic 2000)
- Circular Externa 041 de Junio de 2007 – Superintendencia Financiera de Colombia – Cap. XXIII Reglas relativas a la administración del Riesgo Operativo.  
Web: [http://www.superfinanciera.gov.co/Normativa/NormasyReglamentaciones/cir100/cap23\\_riesgo-opera.doc](http://www.superfinanciera.gov.co/Normativa/NormasyReglamentaciones/cir100/cap23_riesgo-opera.doc).
- Carta Informativa Semanal 6 de Agosto de 2006– Año 16 N° 904 -Superintendencia de Bancos y Entidades Financieras de Bolivia — Web: [http://www.sbef.gov.bo/archivos/carta\\_informativa06082006.pdf](http://www.sbef.gov.bo/archivos/carta_informativa06082006.pdf)
- "Gestión estratégica de riesgos – Cómo gestionar la incertidumbre"  
Web:<http://turan.uc3m.es/uc3m/inst/FC/posgrado/documents/GestionestrategicadeRiesgos-EF2003-FT.pdf>
- Boletín de Asesoría Gerencial N° 8 – 2008, "Riesgo Legal desde la perspectiva del Riesgo Operacional", Espiñeira, Seldom y Asociados firma miembro de PricewaterhouseCoopers.
- "El tratamiento del riesgo operacional en Basilea II", María Ángeles Nieto Giménez-Montesinos.
- Riesgo operativo de Angel Vilariño, Guatemala, septiembre 2005, Presentación Power Point  
Web: [www.sib.gob.gt/es/presentaciones\\_y\\_conferencias/X/1.ppt](http://www.sib.gob.gt/es/presentaciones_y_conferencias/X/1.ppt)
- "El Nuevo Acuerdo de -Capital Basilea II- y su transposición europea: El proceso y la implementación" Fernando Vargas, Cristina Iglesias Sarria –  
Web: <http://www.bde.es/webbde/es/secciones/informes/be/estfin/numero7/ef0700.pdf>
- Boletín Informativo KPMG "Mito o Realidad" 2008  
Web: <http://www.kpmg.cl/documentos/Boletin%20Informativo%202008.PDF>
- Artículo Félix Campoverde Velez : "Administración de Riesgos – Gobierno Corporativo" - 16 Noviembre, 2007  
Web: <http://www.zonaeconomica.com/gobierno-corporativo>
- Documento de la web: <http://redalyc.uaemex.mx/redalyc/pdf/391/39111110.pdf> "La relación entre la estructura financiera y la estrategia competitiva de la empresa desde el punto de vista del control del riesgo. Una mención especial a la estrategia de diferenciación." Revista Galega de Economía, Junio, año/vol.11 N°001 – 2002
- Documento: "¿Resuelve la Integración Financiera el Problema de Agencia?: El caso de los Grupos Económicos Chilenos." Autores: Ricardo Paredes M. y Ana María Caller - Publicación del Departamento de Economía de la facultad de Ciencias Económicas y Administrativas de la Universidad de Chile, vol.19, N°2, Diciembre de 1992.

## **CAPÍTULO 2**

# **OBSERVACIONES REALIZADAS SOBRE LA APLICACIÓN DE BASILEA II EN DIVERSOS PAÍSES**

A través de datos recogidos por diversas consultoras internacionales y de la información recabada a través de la experiencia obtenida por el Comité de Basilea al trabajar con bancos, se han encontrado ciertas prácticas comunes en la administración del riesgo operativo, motivaciones y también limitaciones organizacionales para implementarlas.

Lo que es claro, es que las entidades financieras han ido evolucionando en la asignación de recursos destinados a la gestión de este riesgo, pasando de simples mejoras en sistemas de control interno al desarrollo de metodologías para medir y cuantificar el requerimiento de capital que se debería exigir según el nivel de riesgo y las prácticas corporativas.

Esto en parte se debe a que, las entidades financieras han notado que el método tradicional de gestión del RO, impide a sus Directorios contar con una visión integral de este riesgo por lo que se les hace muy difícil la prevención de pérdidas importantes.

Adicionalmente, se evidencia que muchos bancos ya han logrado la eliminación de costos excesivos de sus operaciones y lo que restaría sería la eliminación de los riesgos operativos innecesarios de las operaciones. Esta eliminación de costos muchas veces excede a los beneficios obtenidos en ocasión de la aplicación de una política general de reducción de costos, lo cual representa una gran motivación para la aplicación de estas sanas prácticas de gestión de RO.

## **2.1. Trabajos realizados por Levy, Samandari & Simoes en Bancos Internacionales (Revista Mckinsey, Quarterly 2006)**

La revista McKinsey Quarterly, es una revista on-line de Gestión de la estrategia de negocios, de Artículos, encuestas y entrevistas, que abarca “Global Business Strategy”. En el Artículo “Better operational-risk management for banks” publicado en la mencionada revista, el 13 de setiembre de 2006, Cindy Levy y Antonio Simoes (Directores de la Oficina londinense de la revista McKinsey) y Hamid Samandari (Director en la Oficina de Washington DC)<sup>12</sup>, expresan que durante trabajos realizados con bancos internacionales, notaron que éstos se inclinan más en *medir* el RO que en *mitigarlo* ya que rara vez se encontraron con procedimientos para afrontar operaciones riesgosas.

Asimismo, lograron identificar las siguientes limitaciones que presentan las entidades para gestionar adecuadamente su RO, las que se describen a continuación:

- Visualización de la administración de este riesgo como un mero requisito regulatorio por parte de la Dirección y no como una práctica que agregue valor a la entidad.
- Escepticismo de altos directivos en cuanto la asignación de recursos a una iniciativa de la que no se obtengan beneficios tangibles.
- Centralización de la función del control del riesgo operacional sin participación de la Alta Gerencia, lo que enlentece el proceso de respuesta ante el surgimiento de dificultades.

---

<sup>12</sup> [http://www.mckinseyquarterly.com/Financial\\_Services/Banking/Better\\_operational-risk\\_management\\_for\\_banks\\_1835](http://www.mckinseyquarterly.com/Financial_Services/Banking/Better_operational-risk_management_for_banks_1835)

- Ausencia de una cultura organizacional que esté orientada al riesgo.
- Coordinación de las nuevas prácticas de control a implementar con las ya existentes.

## **2.2. Observaciones realizadas por el BCBS en su trabajo con Bancos.**

Por otra parte, el Comité de Basilea en su documento “Basel Committee on Banking Supervision: “Observed range of practice in key elements of Advanced measurement approaches (AMA)”, publicado en Octubre 2006<sup>13</sup>, identificó distintos grados de involucramiento de los Directorios en la gestión del riesgo operativo, que van desde un mínimo esfuerzo hasta un compromiso absoluto. Este último, se evidencia por la creación y comunicación de políticas integrales detallando el marco de administración de este riesgo y la implementación de programas para emitir informes periódicos de la función centralizada encargada de la gestión del RO y de la auditoría interna.

Asimismo, observó que es frecuente que la unidad encargada de la administración del RO se encuentre separada del resto de las unidades de negocio de la organización lo cual le otorga mayor independencia. Esta unidad, en general es la que analiza la información acerca de las pérdidas obtenidas, realizando los correspondientes reportes para la Dirección.

En lo que respecta a auditorías externas de la gestión y administración del riesgo operativo, se encontraron que no podían identificar aún un común denominador

---

<sup>13</sup> MPRA – “Sound practices for the management of operational risk in financial institutions” in spanish. Pailhé, Cristina, Delfiner, Miguel and Mangialavori, Ana Central Bank of Argentina. January 2007. Web: <http://mpra.ub.uni-muenchen.de/1803/> MPRA Paper No. 1803, posted 07. November 2007 / 02:00)

en las prácticas usuales de las entidades. Si pudieron observar que la mayoría se apoya en consultoras externas y sólo algunas han desarrollado soluciones internas de forma provisoria.

Otro aspecto de importancia que han observado, es que los bancos en general tienen claro las diferencias conceptuales entre el riesgo operativo y el de crédito y de mercado, ya que se vieron casos donde las pérdidas generadas por los “traders” que violan límites se trataron como casos de riesgo operativo y no como riesgo de mercado.

No obstante lo mencionado anteriormente, en el caso de pérdidas originadas en la aplicación de procesos inadecuados o fallidos en el manejo de préstamos, generalmente se tiende a asociarlas al riesgo crediticio y no al riesgo operativo cuando todo indicaría que corresponden a eventos de este tipo de riesgo.

La tendencia a la integración de los 3 tipos de riesgos es algo que llevará mucho tiempo en lograrse. Esto es importante porque los errores operacionales pueden causar errores consecuentes en la estimación de los riesgos de crédito y de mercado. Una forma de impulsar esta integración sería a través de la creación de una base de datos que integre la información recabada de los 3 tipos de riesgos.

Aquellas organizaciones financieras que deseen implementar una administración del riesgo operacional, deben tener en consideración la creación de una base de datos interna de eventos operativos que permita la reducción de incidentes y pérdidas económicas y a la vez, contribuya a la mejora de la calidad de productos y servicios realizados.

En definitiva, las ventajas de tener esta base interna de eventos operativos son que: permite a las entidades tomar conciencia de que las exposiciones al riesgo operacional pueden ser muy perjudiciales; al cuantificar la exposición colabora en la asignación de recursos para su mitigación; al analizar la frecuencia en la ocurrencia de eventos se denotan cuáles son las áreas a ser mejoradas.

El Comité detectó que, en la práctica los bancos tienden a tomar como fecha de ocurrencia de un evento operativo, la fecha en que se descubre dicho evento más que la fecha de registro contable del mismo. Sin embargo, en litigios judiciales sí tienden a tomar la fecha de registro contable.

Por otra parte, se ha observado también que los métodos utilizados por los bancos para valuar el monto de pérdida por daños materiales de activos fijos se reducen a:

- Valor de mercado
- Valor de reposición
- Valor en libros

En cuanto a la imputación de pérdidas detectadas, se distinguen dos métodos:

1. Asignar toda la pérdida a la línea de negocios más afectada.
2. Asignar las pérdidas sobre una base pro-rata en las líneas de negocio afectadas.

A su vez, los bancos tienden a contabilizar las pérdidas netas de los recuperos obtenidos durante un tiempo determinado con anticipación (de uno a varios días de ocurrido el evento), y en el caso de que el recupero sea total entonces registran lo que se llama “casi-pérdidas”.

Cabe destacar, que todos estos datos son recogidos internamente a los efectos de evaluar las tendencias del riesgo operacional dentro de la organización y no para cuantificar el mismo.

Para la definición de los umbrales mínimos de pérdidas a la hora de considerarlos en la base de datos interna, la mayoría de los bancos se apoya en expertos en la materia y es usual que se elijan los mismos umbrales para todos los tipos de eventos y sólo algunas entidades optan por definir umbrales específicos a cada unidad de negocio.

Para validar sus datos, las prácticas más usuales son las siguientes:

1. Conciliaciones con el mayor general;
2. elaboración de informes de la función de control de riesgo;
3. auditorías tanto externas como internas;
4. revisión de las inconsistencias generadas en los datos recabados por las distintas líneas de negocio.

Hasta ahora únicamente nos hemos referido a las *ventajas* de crear y mantener una base de datos interna en la cual se registren las pérdidas originadas en eventos de riesgo operacional.

Sin embargo, también se han encontrado algunas *carencias* de este método de control, las que resumiremos a continuación:

- La estimación del riesgo operativo a través de estos datos históricos no tiene en cuenta las acciones de prevención y mitigación de los eventos que dan origen a pérdidas.

Por esta razón, ocurre que el riesgo operativo actual es menor al que se ve reflejado en estos datos y por ende, los datos pierden realidad.

- Muchas veces los datos no reflejan claramente las causas que originaron las pérdidas.
- Existencia de desincentivos para informar eventos que sean relevantes, con lo cual se pierde información.

Debido a estas limitaciones es que el BCBS recomienda que también se incluya el uso de información complementaria a los datos de pérdida, como ser los factores del control interno y del entorno de negocios.

La estructura de evaluación del riesgo en general es común a todas las entidades, y básicamente se conforma de matrices que identifican y evalúan el riesgo operacional en función de su probabilidad de ocurrencia y las repercusiones de sus consecuencias sobre la organización.

En particular, se hace mención a los KRIs, que son factores que pueden mostrar las señales de alerta de manera anticipada, acerca de los sistemas, procesos, productos, personas y entorno de los bancos. Es a través de estos factores, que también se basan en datos existentes, que se busca predecir comportamientos futuros, con variables como ser la rotación del personal entre otros, que evidencian potenciales pérdidas en caso de ocurrir determinados sucesos como puede ser la renuncia de personal clave.

Fuentes consultadas:

- MPRA – “Sound practices for the management of operational risk in financial institutions” in spanish. Pailhé, Cristina, Delfiner, Miguel and Mangialavori, Ana Central Bank of Argentina. January 2007.  
Web: <http://mpa.ub.uni-muenchen.de/1803/> MPRA Paper No. 1803, posted 07. November 2007 / 02:00)
- Revista McKinsey Quarterly Artículo “Better operacional-risk management for banks.” Web:  
[http://www.mckinseyquarterly.com/Financial\\_Services/Banking/Better\\_operationalrisk\\_management\\_for\\_banks\\_1835](http://www.mckinseyquarterly.com/Financial_Services/Banking/Better_operationalrisk_management_for_banks_1835)

## **CAPÍTULO 3**

# **ADMINISTRACIÓN DEL RIESGO OPERACIONAL EN PAÍSES DE INTERÉS**

En el presente capítulo trataremos de hacer un resumen acerca de la normativa regulatoria en cuanto a la administración y supervisión del Riesgo Operativo en los siguientes países: Brasil, Chile, Argentina, México, Estados Unidos y España.



## **Brasil**

El 9 de diciembre de 2004, el Banco Central de Brasil (BCB) publica por primera vez una Comunicación que hace referencia al riesgo operacional (Comunicación N° 12.746). La misma establece un cronograma de acción para la correcta implementación de un requerimiento de capital por riesgo operativo. Dicho cronograma posteriormente es ajustado según la Comunicación N° 16.137 del 27 de septiembre del 2007, que plantea lo siguiente:

- Para finales de 2007, se comenzaría a exigir un requerimiento de capital por este riesgo.
- Antes de finales de 2009, se publicarían los puntos claves a tener en cuenta a la hora de desarrollar modelos internos.
- Antes de finales de 2011, se establecerían los criterios exigidos para la adopción de modelos internos, así como la divulgación del procedimiento para solicitar ante el Banco de Brasil la autorización para la aplicación de los mismos.
- Por último, antes de finales de 2012, se iniciarían los procesos de autorización para el uso de estos modelos internos.

El 29 de junio de 2006, se publica la Resolución N° 3.380, que impone a todas las instituciones sujetas a supervisión por parte del Banco Central de Brasil, la

obligación de desarrollar una Estructura de Gerenciamiento del Riesgo Operacional.

Esta Estructura de Gerenciamiento del RO deberá prever:

- La identificación, evaluación, monitoreo, control y mitigación del riesgo operativo;
- documento y archivo de datos concernientes al surgimiento de pérdidas originadas en eventos de riesgo operativo;
- elaborar por lo menos una vez al año, informes que permitan identificar y corregir deficiencias en el mencionado gerenciamiento;
- revisar por lo menos una vez al año los procedimientos de control del RO;
- difusión de las políticas de administración del riesgo operativo al personal interno, así como, a los proveedores de servicios tercerizados para establecer roles y responsabilidades;
- elaboración de un plan de contingencia;
- establecer un proceso estructurado de comunicación e información en toda la organización.

Como podemos observar, estas políticas conjuntamente con la necesidad de nombrar un responsable por el gerenciamiento del riesgo operacional, responden claramente al propósito del Banco Central de Brasil de introducir las recomendaciones de Basilea II dentro de su sistema de normativo.

Dos meses después, el 29 de agosto de 2007, el Banco central de Brasil publica la Resolución N° 3.490. La misma establece que, las instituciones financieras que operen bajo su supervisión deberán en todo momento mantener un Patrimonio de Referencia (PR), que deberá ser siempre superior al llamado Patrimonio de Referencia Exigido (PRE).

El PRE se compone por la suma de los riesgos que se encuentran presentes en la actividad bancaria según Basilea II, sean éstos: el riesgo de crédito, el de mercado y el operacional (POPR).

Lo interesante es que ya en el año 2007 Brasil exigía a sus instituciones que mantuviesen una reserva en su patrimonio para posibles pérdidas ocasionadas por riesgo operativo.

Esta Comunicación entra vigor el 30 de abril de 2008, cuando el BCB publica la Circular N° 3.383 que establece la forma de cálculo del requerimiento de capital por Riesgo Operacional.

Los métodos de medición propuestos por esta Circular son los siguientes:

- El indicador básico.
- Método estándar alternativo.
- Método estándar alternativo simplificado.

El método seleccionado por cada institución debe ser comunicado al Banco de Brasil.

El Artículo 3 de esta norma nos dice que el indicador de exposición al riesgo operacional (IE) para cada período anual, se debe calcular como:

$$IE = \sum (Rentas \text{ de operaciones de intermediación financiera} + Rentas \text{ por servicios prestados} - Pérdidas \text{ por operaciones de intermediación financiera})$$

Agregando posteriormente que el indicador alternativo de exposición al riesgo operacional (IAE), para el período de un año, se calcula como:

$$IAE = \frac{(Sdos\ sem.\ de\ op.\ de\ crédito,\ Arrendamiento\ Mercantil\ y\ Otra\ op.) * 0,035}{2}$$

En el Artículo 4° se exponen diferentes líneas de negocios a ser tenidas en cuenta a la hora de calcular la exposición a este riesgo, esta lista, según surge de un compilado de consultas frecuentes al BCB (publicado en [www.bcb.gub.br](http://www.bcb.gub.br)), no es una lista taxativa.

Cerramos dicho capítulo exponiendo las formas de cálculo, planteadas por el BCB para calcular el requerimiento de capital por riesgo operacional:

- Formula a usar para abordar el método del indicador básico:

$$P_{OPR} = Z \cdot \frac{\sum_{t=1}^3 \max [0,15 \times IE_t; 0]}{n}$$

Donde:

Z: Es un valor que se encuentra publicado en el Art. 8° de dicha Circular.

IE: Indicador de Exposición al Riesgo Operacional en el periodo anual “t”.

n: Número de veces en que el valor IE fue positivo el período de tres años.

- Formula a usar para abordar el Método estándar alternativo:

$$P_{OPR} = Z \cdot \frac{\sum_{t=1}^3 \max \left[ \left( \sum_{i=1}^2 IAE_{i,t} \times \beta_i \right) + \left( \sum_{i=3}^8 IE_{i,t} \times \beta_i \right); 0 \right]}{3}$$

Donde:

Z: Es un valor que se encuentra publicado en el Art. 8° de dicha Circular.

IAE: Indicador Alternativo de Exposición al Riesgo Operacional, en el periodo “t”, para cada línea de negocio “i” mencionadas en el Art. 4 de la norma.

IE: Indicador de Exposición al Riesgo Operacional, en el periodo “t”, para cada línea de negocio “i” mencionadas en el Art. 4 de la norma.

$\beta$ : Factor de ponderación aplicado a cada línea de negocio “i”.

Más adelante la norma define los valores en que se debe situar el factor  $\beta$  según cada línea de negocio.

- Formula a usar para abordar el Método estándar alternativo simplificado:

$$P_{OPR} = Z \cdot \frac{\sum_{t=1}^3 \max \{ [(IAE_t \times 0,15) + (IE_t \times 0,18)]; 0 \}}{3}$$

Donde:

Z: Es un valor que se encuentra publicado en el Art. 8° de dicha Circular.

IAE: Indicador Alternativo de Exposición al Riesgo Operacional, en el periodo “t”, para la suma de las líneas de negocio “i” mencionadas en el Art. 4 de la norma.

IE: Indicador de Exposición al Riesgo Operacional, en el periodo “t”, para la suma de las operaciones incluidas en cada línea de negocio “i” mencionadas en el Art. 4 de la norma.



## Chile

En enero del 2005, la Superintendencia de Bancos e Instituciones Financieras (en Chile el órgano supervisor de los Bancos e Instituciones Financieras es la Superintendencia de Bancos e Instituciones Financieras - SBIF), entregó a los representantes de la industria bancaria y al público en general un documento denominado “Directrices de la hoja de ruta para la transición hacia Basilea II”.

Este documento expone algunas reformas normativas de años anteriores que facilitarán a Chile implementar el Nuevo Acuerdo de Capitales. A continuación citamos algunos ejemplos:

- Han implementado una definición del riesgo operacional para evaluar la gestión, en términos similares a los de Basilea II en julio de 2004.
- Existe un informe del Fondo Monetario Internacional y del Banco Mundial, que encontró que más del 80% de los Principios de Supervisión Bancaria Efectiva, están siendo aplicados en Chile.

Más adelante en el mismo documento, se hace énfasis en que la transición va a ser gradual y que el Banco Central de Chile y la SBIF, trabajaran coordinadamente en este proceso.

En una primera etapa solo se permitirá el enfoque estandarizado para los riesgos de créditos y operacional. Luego en una segunda etapa, se avanzará hacia un enfoque de modelos internos, siempre y cuando, se hayan adquirido las competencias necesarias y se disponga de suficiente información como para validar los modelos.

La normativa financiera de Chile la podemos encontrar en dos documentos de suma importancia, que se encuentran publicados en la pagina web de la SBIF,

siendo éstos: la Ley General de Bancos (LGB) y la Recopilación de Actualizada de Normas (RAN).

La LGB plantea un modelo particular de clasificación de Bancos. En su Artículo 59 establece que “la Superintendencia mantendrá permanentemente la clasificación de gestión y solvencia de los bancos e instituciones financieras, realizada conforme al procedimiento señalado en los Artículos siguientes”. Esta clasificación deberá efectuarse periódicamente (al menos una vez al año) y será comunicada a todos los bancos dentro de los cinco días siguientes a la fecha de su realización.

En esta tarea encomendada a la SBIF, podemos ver el intento por párete de la banca chilena de llegar a la tan recomendada transparencia de mercado (Pilar III de Basilea II).

Nos interesa destacar cómo va a clasificar la SBIF a las diferentes instituciones, es por esto que a continuación transcribimos el Art. 62 de la LGB, para comentarlo posteriormente:

*“Artículo 62.- Para los efectos de lo señalado en los Artículos anteriores, los bancos se clasificarán según su gestión en los siguientes niveles:*

*Nivel A: Incluye a las instituciones no clasificadas en los niveles B y C siguientes.*

*Nivel B: Incluye a las instituciones que reflejan ciertas debilidades en los controles internos, sistemas de información para la toma de decisiones, seguimiento oportuno de riesgos, clasificación privada de riesgo y capacidad para enfrentar escenarios de contingencia, las que serán*

*corregidas por la propia institución durante el período que preceda al de la próxima calificación para evitar un deterioro paulatino en la solidez de la institución. También se considerarán las sanciones aplicadas a la empresa, salvo las que se encuentren con reclamación pendiente.*

*Nivel C: Incluye a las instituciones que presentan deficiencias significativas, en alguno de los factores señalados en el Nivel anterior, cuya corrección debe ser efectuada con la mayor prontitud para evitar un menoscabo relevante en su estabilidad”.*

En resumen, la Banca Chilena a la hora de la clasificación, prestará primordial atención, a la efectiva gestión de riesgos, al sistema de control interno y a la capacidad del ente de enfrentar las contingencias propias del mercado financiero.

Asimismo, según la RAN estos procesos clasificatorios se realizarán a través de:

- visitas de inspección;
- análisis y evaluación de información acerca del banco;
- y de reuniones para estar al corriente de los acontecimientos, que inciden o pueden incidir en la marcha normal de la institución.

El apartado 3.3 de la RAN, habla específicamente de la Administración del Riesgo Operativo, por lo cual en adelante centraremos nuestra atención el mismo.

Comienza diciendo que, resultará de interés para la evaluación que realizará la Superintendencia, el rol asumido por el Directorio y la alta administración, así como, la aprobación que los mismos han dado a la estrategia de riesgo

operativo. Entendiendo a éste como una categoría separada de los riesgos bancarios tradicionales.

Esta estrategia debe contemplar una definición clara, de lo que se considera como riesgo operacional y establecer los principios para su identificación, evaluación, control y mitigación. En este sentido, si la exposición al riesgo es significativa, cobra relevancia la existencia de definiciones precisas de lo que se entiende por pérdidas operacionales esperadas y pérdidas operacionales inesperadas, por cuanto los tratamientos de mitigación son diferentes en uno u otro caso.

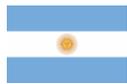
Más adelante la norma establece situaciones y hechos que revelan una buena gestión del riesgo operacional, como ejemplos plantea los siguientes:

- El banco tiene una definición de lo que entiende por riesgo operacional y cuenta con una función encargada de la administración de este tipo de riesgo.
- Mantiene políticas para la administración de los riesgos operacionales, aprobada por el Directorio o la administración superior.
- La estrategia de administración del riesgo operacional definida por el banco, es consistente con el volumen y complejidad de sus actividades.
- La entidad administra los riesgos operacionales considerando los impactos que pudieran provocar en el banco (severidad de la pérdida) y la probabilidad de ocurrencia de los eventos.

- La entidad realiza evaluaciones del riesgo operacional inherente a todos los tipos de productos, actividades, procesos y sistemas. Asimismo, se asegura que antes de introducir nuevos productos, emprender nuevas actividades, o establecer nuevos procesos y sistemas, el riesgo operacional inherente a los mismos esté sujeto a procedimientos de evaluación.
- El banco ha integrado a sus actividades normales el monitoreo del riesgo operacional y ha identificado indicadores apropiados que marcan alertas de un aumento del riesgo y de futuras pérdidas.
- El banco es capaz de cuantificar los impactos de las pérdidas asociadas al riesgo operacional y constituir prudencialmente los resguardos necesarios.
- Los sistemas de información permiten hacer un monitoreo continuo de la exposición a los riesgos operacionales. 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 a las mismas.
- El banco realiza inversiones en tecnología de procesamiento y seguridad de la información, que permiten mitigar los riesgos operacionales y que son concordantes con el volumen y complejidad de las actividades y operaciones que realiza.

- El banco 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, con el objeto 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.
- El banco 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.
- 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.

Podemos concluir entonces que la Banca Chilena se encuentra caminando hacia la implementación integral de Basilea II a pasos adelantados en comparación con algunos de sus vecinos Latinoamericanos.



## Argentina

En el año 2007 el Banco Central de la República Argentina (BCRA) publica la llamada “Hoja de ruta para la implementación de Basilea II”. En este documento se establece que en lo que refiere a la exigencia de capital por riesgo operacional, el BCRA considera conveniente seguir analizando entre las alternativas disponibles para su medición, con el objeto de identificar la de mejor adaptación al sistema financiero local. No obstante, plantea además que propiciará la adopción de buenas prácticas en materia de administración de este riesgo.

Más adelante, el 20 de octubre de 2008, el BCRA publica la Comunicación N° 4.854 llamada: “Lineamientos para la gestión del riesgo operacional en las entidades financieras”.

Este documento plantea que a cada entidad le corresponderá implementar una administración eficiente del RO, con lo cual debe existir un responsable por el gerenciamiento de dicho riesgo. Esta persona deberá demostrar un alto grado de compromiso, tendiente a mantener una sólida cultura de gestión de RO, en la cual las actividades relacionadas con ese riesgo formen parte de los procesos diarios de la entidad financiera.

En dicha Comunicación, se establecen los roles y tareas que corresponden al personal superior de la entidad.

Por un lado, se plantea que el Directorio será el responsable de que la entidad cuente con una estrategia adecuada para la gestión de riesgo operacional y para ello deberá:

- Aprobar el sistema que se utilizará para la gestión de RO, cuya periodicidad mínima de revisión será anual, a no ser que se produzcan hechos de relevancia al respecto.
- Tener claro conocimiento de los procedimientos desarrollados a los efectos de gestionar y controlar este riesgo.
- Asegurarse de que el sistema de RO esté sujeto a auditoría interna.
- Aprobar políticas de difusión del sistema de gestión de RO y de capacitación, dirigidas a todas las áreas y funcionarios de la organización.
- Establecer políticas de gestión de RO relacionadas con actividades subcontratadas y con servicios prestados por proveedores.
- Aprobar políticas de difusión a terceros de la información que corresponda sobre el sistema de gestión de RO.
- Garantizar que la entidad cuente en todo momento con personal capacitado, así como con los recursos necesarios para llevar adelante el sistema de gestión de RO.
- Verificar que los encargados de la gestión del RO no desarrollen otras tareas que puedan interferir y generar conflictos de intereses con su función.

Por otro lado, se establece que la Gerencia General o alguna autoridad equivalente tendrán las siguientes responsabilidades:

- Implementación, reporte y control de los procesos y procedimientos para la puesta en práctica y funcionamiento del sistema de gestión aprobado por el Directorio.
- Será la encargada de que existan procesos y procedimientos para cada unidad de negocio.
-

- Deberá establecer líneas claras de autoridad, responsabilidad y comunicación con las distintas gerencias.
- Asegurar la existencia de recursos suficientes para la gestión.
- Deberá evaluar si el proceso de vigilancia gerencial se adapta a los riesgos inherentes a las políticas de cada unidad de negocio.
- Recibirá reportes de la Unidad de RO o persona responsable, con el objeto de controlar la gestión de RO.
- Informará al Directorio como mínimo semestralmente, sobre los principales aspectos relacionados con la gestión de este riesgo.

Más adelante, la norma plantea que las gerencias serán responsables de aplicar en las distintas unidades de negocios los procesos y procedimientos concretos definidos en el sistema de gestión de RO.

Asimismo, informarán a la Unidad de RO o persona responsable, acerca de los resultados de la ejecución de procesos y procedimientos, con la periodicidad definida por la entidad.

Por último, según la norma, la estructura de la unidad encargada de la gestión de riesgo operacional (Unidad de RO o persona responsable) contemplará las siguientes características:

- Se adecuará al tamaño de la institución, naturaleza y complejidad de sus productos y procesos y a la magnitud de sus operaciones.
- Dependerá de la Gerencia General u equivalente.
- No podrá estar a cargo de la Auditoría Interna.
- Podrá incorporar personal de otras áreas siempre que las responsabilidades asignadas no impliquen conflictos de intereses entre sus funciones.

- Existirá independencia entre la unidad o persona responsable de la gestión de RO y las unidades de negocios involucradas, así como una clara delimitación de funciones, responsabilidades y perfil de puestos de trabajo en todos sus niveles.
- Deberá articular los principales procesos para gestionar el RO, adoptando los mecanismos que permitan una comunicación, interacción y coordinación efectiva con los responsables de los otros riesgos y con los responsables de contratar servicios externos.
- Recibirá de las gerencias informes con los resultados de la ejecución de los procesos y procedimientos.
- Informará a la Gerencia General la detección de las posibles deficiencias que se produzcan en la aplicación de las políticas, procesos y procedimientos de gestión de riesgo operacional y las pertinentes propuestas para su corrección.

Las entidades podrán cubrirse de la exposición a riesgos operacionales significativos usando herramientas o programas de cobertura de riesgos, como por ejemplo, las pólizas de seguros. Las mismas deberán ser usadas como complemento de las medidas de control interno adoptadas para esos riesgos, pero no serán sustitutos de la gestión de RO.

Finaliza la norma, diciendo que las entidades financieras deberán contar con planes de contingencia y de continuidad operacional. Para ello deberán identificar sus procesos más críticos y mecanismos alternativos, a los efectos de reanudar el servicio en caso de interrupción.



## México

Para analizar la normativa de este país, nos basaremos en la recopilación de normas vigentes, llamada “Disposiciones de carácter general aplicables a las Instituciones de Crédito”. Publicada originalmente por “La Comisión Nacional Bancaria y de Valores” (ente supervisor en México) en el Diario Oficial de la Federación de México, el 2 de diciembre de 2005, y modificada posteriormente por diferentes Circulares.

Centraremos nuestra atención en el “Titulo Segundo – Capítulo 4º” de la misma, por ser el que plantea la forma en que las Instituciones Financieras deben administrar sus riesgos.

En el Artículo 66, se dividen los riesgos a los que se enfrentan las instituciones financieras en dos grandes categorías: cuantificables y no cuantificables.

La norma define a cada una de estas categorías de riesgos, de la siguiente manera:

### 1. Riesgos cuantificables:

Estos riesgos a su vez se separan en: discrecionales y no discrecionales.

- Los riesgos discrecionales “son aquéllos para los cuales es posible conformar bases estadísticas que permitan medir sus pérdidas potenciales”, dentro de esta categoría tenemos el riesgo de crédito, el de mercado y el de liquidez.
- Por su parte, los riesgos no discrecionales “son aquéllos resultantes de la operación del negocio, pero que no son producto

de la toma de una posición de riesgo, tales como el riesgo operacional”. Podemos ver en la norma, que al definir este riesgo no se aleja de la definición aportada por Basilea II.

## 2. Riesgos no cuantificables:

En esta categoría de riesgos se encuentran aquéllos derivados de eventos imprevistos para los cuales no se puede conformar una base estadística de datos que permita medir las pérdidas potenciales derivadas de los mismos.

Posteriormente, el Artículo 67 establece que para llevar adelante una correcta Administración Integral de Riesgos, las instituciones deberían:

- Definir sus objetivos sobre la exposición al riesgo y desarrollar políticas y procedimientos para la administración de los mismos, sean éstos cuantificables o no.
- Delimitar claramente las diferentes funciones, actividades y responsabilidades en materia de Administración Integral de Riesgos en toda la organización.
- Identificar, medir, vigilar, limitar, controlar, informar y revelar los riesgos cuantificables y no cuantificables a los que se encuentra expuesta la institución.
- Agrupar, considerando a sus Subsidiarias Financieras, los distintos tipos de riesgo a que se encuentran expuestas, por unidad de negocio o por factor de riesgo.

Más adelante, la norma nos dice que, el Consejo de cada institución será responsable de: aprobar los objetivos, lineamientos y políticas para la Administración Integral de Riesgos, marcar los límites de exposición a los mismos y establecer los mecanismos para la realización de acciones correctivas. En complemento de lo anterior, se permite que el Consejo delegue al Comité de riesgos la facultad de aprobar los límites específicos de exposición a los diferentes riesgos, los cuales serán revisados por lo menos una vez al año.

El Comité de riesgos, para llevar a cabo la mencionada Administración Integral de Riesgos, contará con una unidad especializada, cuyo objeto será: identificar, medir, vigilar e informar sobre los riesgos cuantificables a los que se enfrenta la institución, ya sea que éstos se registren dentro o fuera del balance, incluyendo, en su caso, los riesgos de sus Subsidiarias Financieras.

Por otro lado, el Director General de la institución, será el responsable de vigilar que se mantenga la Independencia necesaria entre la unidad de Administración Integral de Riesgos (AIR) y las distintas Unidades de Negocio.

En el Artículo 78, la norma plantea que las Instituciones deberán contemplar en sus objetivos, lineamientos y políticas para la AIR por lo menos los siguientes aspectos:

- El perfil de riesgo, así como los objetivos de exposición al mismo.
- La estructura organizacional.
- Las facultades y responsabilidades de aquellas personas que desempeñan cargos que implican la toma de riesgos para la institución.
- La clasificación de los riesgos por tipo de operación y línea de negocios.

- Los límites tanto globales como específicos de la exposición al riesgo.
- La forma y periodicidad con la que se deberá informar al Consejo, al Comité de riesgos, al Director General y a las unidades de negocio, sobre la exposición al riesgo de la institución en general y de cada unidad de negocio en particular.
- Las medidas de control interno, así como las medidas para corregir las desviaciones que se observen sobre los límites de exposición al riesgo y niveles de tolerancia al mismo.
- El proceso para aprobar operaciones, servicios, productos y líneas de negocio nuevas para la institución.
- Los planes de acción para reestablecer el negocio en caso de presentarse eventos fortuitos o de fuerza mayor.
- El proceso para obtener la autorización a exceder de manera excepcional los límites de exposición al riesgo y niveles de tolerancia al mismo.

Las modificaciones que se pretendan efectuar a los objetivos, lineamientos y políticas de la Administración Integral de Riesgos deberán ser propuestas por el Comité de riesgos y aprobadas por el Consejo.

Más adelante, en la “sección cuarta - apartado B”, se expone el tratamiento a dar a los riesgos no discretionales. En tal sentido, las instituciones deberán como mínimo desarrollar las siguientes funciones:

1. En materia de administración del RO:

- Identificar y documentar los procesos que se desarrollan en la institución.
- Identificar y documentar los riesgos operacionales implícitos en dichos procesos.
- Evaluar e informar por lo menos trimestralmente, las consecuencias que sobre el negocio generaría la materialización de los riesgos identificados e informar los resultados a los responsables de las unidades implicadas, a fin de que se evalúen las diferentes medidas de control de dichos riesgos.
- Establecer los niveles de tolerancia al riesgo para cada tipo de riesgo identificado, definiendo sus causas y orígenes.
- Las instituciones deberán llevar un registro histórico de eventos de pérdida por riesgo operacional.

2. En materia de administración del riesgo tecnológico:

Las Instituciones deberán evaluar las circunstancias que en materia de riesgo tecnológico pudieran influir en su operación ordinaria, las cuales se sujetarán a vigilancia permanente a fin de verificar el desempeño del proceso de AIR.

3. En materia de administración del riesgo legal:

- Establecer políticas y procedimientos para que en forma previa a la celebración de actos jurídicos, se analice la validez y se procure la adecuada instrumentación legal de éstos, incluyendo la formalización de las garantías en favor de la institución, a fin de evitar vicios en la celebración de las operaciones.
- Estimar el monto de pérdidas potenciales derivado de resoluciones judiciales o administrativas desfavorables, así como la posible aplicación de sanciones, en relación con las operaciones que se lleven a cabo.
- Analizar los actos que realice la institución cuando se rijan por un sistema jurídico distinto al nacional y evaluar las diferencias existentes entre el sistema de que se trate y el nacional.
- Dar a conocer a sus directivos y empleados, las disposiciones legales y administrativas aplicables a las operaciones.
- Realizar, cuando menos anualmente, auditorías legales internas.
- Mantener una base de datos histórica sobre las resoluciones judiciales y administrativas, sus causas y costos.

Corresponderá al Comité de riesgos de la institución el cumplimiento de las funciones relativas al riesgo tecnológico y al riesgo legal a que hacen referencia los incisos anteriores, pudiendo auxiliarse con el área que se estime conveniente, siempre y cuando ello no se suscite conflictos de intereses.

Más adelante en la norma, nos encontramos con el Artículo 87, el cual plantea que las instituciones deberán contar con informes que se basen en datos íntegros, precisos y oportunos, relacionados con su Administración Integral de Riesgos y que como mínimo contengan lo siguiente:

- La exposición por tipo de riesgo en los casos de riesgos discrecionales, así como los niveles de incidencia e impacto en el caso de los riesgos no discrecionales. Los informes sobre la exposición de riesgo deberán incluir análisis de sensibilidad y pruebas bajo condiciones extremas.
- El grado de cumplimiento de los objetivos, lineamientos y políticas para la Administración Integral de Riesgos.
- Resúmenes de los resultados de las auditorías, en lo que hace al cumplimiento de los objetivos, lineamientos y políticas para la AIR, así como sobre las evaluaciones de los sistemas de medición de riesgos.
- Casos en que los límites de exposición al riesgo o los niveles de tolerancia al mismo fueron excedidos, según se trate de riesgos discrecionales o no discrecionales, ya sea que se contara o no con autorización previa.

Finalizando, según el Artículo 88 las Instituciones deberán revelar al público, de manera trimestral, a través de sus notas a los estados financieros la información relativa a las políticas, metodologías, niveles de riesgo asumidos y demás medidas relevantes adoptadas para la administración de cada tipo de riesgo.

En tal sentido deberán exponer por lo menos la siguiente información:

1. Información cualitativa:

- Descripción de los aspectos cualitativos relacionados con el proceso de Administración Integral de Riesgos.
- Los principales elementos de las metodologías empleadas en la administración de los riesgos de mercado, de liquidez, de crédito y operacional.
- Carteras y portafolios a los que se les está aplicando.
- Breve explicación de la forma en que se deben interpretar los resultados de las cifras de riesgo que se den a conocer.

2. Información cuantitativa:

- Valor en riesgo de crédito, de mercado y operacional, incluyendo el tecnológico y legal; este último, sólo cuando la institución esté autorizada para calcular sus requerimientos de capital mediante modelos internos.
- Evaluación de variaciones en los ingresos financieros y en el valor económico.
- Estadística descriptiva del riesgo crediticio.
- Valores promedio de la exposición por tipo de riesgo correspondiente al período de revelación.
- Informe de las consecuencias y pérdidas que sobre el negocio generaría la materialización de los riesgos operacionales identificados, sólo cuando la institución esté autorizada para calcular sus requerimientos de capital mediante modelos internos.



## **Estados Unidos**

La Reserva Federal de Estados Unidos considera que el Nuevo Acuerdo constituye un avance en la medición del riesgo y la determinación del capital regulatorio. Sin embargo, la posición de los supervisores de este país es la de no aplicar Basilea II en la mayoría de los bancos, pues mantienen niveles de capital más altos que los requeridos y consideran que el sistema está sólido, a la vez que estiman que su aplicación elevaría los costes en la banca y no reportaría mayores beneficios.

Siguiendo esta misma línea, en documentos publicados por la Reserva Federal conjuntamente con la OCC y otras agencias de relevancia, se reafirma el hecho de que sólo un mínimo grupo de organizaciones bancarias están obligadas a aplicar las disposiciones previstas en Basilea II, para el establecimiento de su capital regulatorio (aplicando métodos de medición avanzada “AMA”). El resto de los bancos se sigue rigiendo por la normativa general de requerimiento de capital, salvo aquellos que optasen voluntariamente por atenerse a la regulación de Basilea II, quienes pasarían a aplicar la normativa establecida en Basilea IA.

La propuesta de la normativa establecida por Basilea IA, busca mejorar la sensibilidad al riesgo de las ya existentes reglas de capital por riesgos.

Los cambios propuestos por Basilea IA comprenden, entre otros, aumento del número de las categorías de riesgo a considerar (pasan de ser 5 a 8), admisión de uso de calificaciones de crédito externas y otras relativas a la regulación de créditos en general.

Por otra parte, las Agencias (Reserva Federal, OCC, Corporación del Seguro de depósitos federal, “Thrift supervisión Office”), han publicado guías con relación al

proceso de supervisión de la adecuación del capital, para aquellas entidades que se encuentren implementando las aproximaciones avanzadas (AMA). Este proceso de supervisión (descrito en la norma publicada el 7 de diciembre de 2007), destaca los estándares que deben tener las entidades para cumplir con los requerimientos calificativos previstos en la norma definitiva de aproximación avanzada y las agencias supervisarán, dentro de otros aspectos, si cada entidad:

- Satisface los requerimientos establecidos para implementar estos métodos de aproximación avanzada;
- si cuentan con procesos rigurosos para determinar la adecuación del capital en función de su perfil de riesgo y si posee una estrategia razonable para mantener los niveles adecuados de capital;
- si mantiene una administración de riesgo satisfactoria y una estructura de control consistente con su posición de capital y su perfil de riesgo.

Se establece que un banco debería aumentar su reserva de capital en caso de que el aumento en el nivel de riesgos sea material y que no esté siendo mitigado de alguna otra manera, a no ser que el banco mantenga un nivel de capital que exceda al requerido de acuerdo con sus procesos internos y con lo que sus supervisores establecen como adecuado. Por lo tanto, se entiende que un aumento en el perfil de riesgos de una entidad financiera no necesariamente debería repercutir en un aumento de capital.

En forma adicional, se trata de incentivar a los bancos a que continuamente evalúen y mejoren sus técnicas de medición e identificación de riesgos.

Esta guía se hizo efectiva a partir del 2 de setiembre de 2008.



## **España**

Al final del preámbulo de la actual Circular del Banco de España (BOE N° 140) publicada el 10 de junio de 2008, se establece que la información a exigir por parte del Banco de España a las Instituciones, será homogénea a la que presentarán el resto de las instituciones dentro de la Unión Europea.

En el primer capítulo menciona las entidades que estarían obligadas a informar y cumplir con dicha norma, que resumidamente serían las entidades de crédito, pertenecientes o no a grupos que consoliden.

Según el Capítulo 8 de la mencionada norma, los métodos aceptados por el Banco de España para la medición del requerimiento de capital por riesgo operativo, son los siguientes:

1. El método del indicador básico.
2. El modelo estándar y su variante de modelo estándar alternativo.
3. Los métodos avanzados, basados en sistemas de medición interna.

Para que la entidad pueda usar alguno de los dos últimos métodos, será necesario que cuente con autorización previa por parte del banco de España (BE).

Las entidades que apliquen el método estándar, no podrán volver a aplicar el método del indicador básico, salvo en casos justificados y con previa autorización del BE. Lo mismo pasa con las entidades que apliquen por una vez métodos avanzados, respecto de los dos métodos anteriores.

No obstante, con previa autorización del banco de España las entidades podrán aplicar una combinación de los métodos antes mencionados, pero dicha combinación tendrá carácter transitorio.

Calculo del requerimiento de recursos propios para cada método:

1. Método del indicador Básico:

El requerimiento se calculará como el producto de los ingresos relevantes de los últimos tres ejercicios financieros completos (cuando sean positivos), por un porcentaje fijo del 15%. En el caso de que los resultados no fuesen positivos o fuesen nulos, se tomarán las cifras positivas de los resultados y se dividirá por el número de cifras positivas.

Los ingresos relevantes se definen como la suma de los siguientes rubros del estado de resultado:

- Intereses y rendimientos asimilables
- Intereses y cargas asimilables
- Rendimiento de instrumentos de capital
- Comisiones percibidas
- Comisiones pagadas
- Resultado de operaciones financieras (neto)
- Diferencia de cambio (neto)
- Otros productos de exportación

En caso de absorciones o cesiones de negocios significativas, los ingresos relevantes se ajustarán para tomar en cuenta el efecto que esto produce.

## 2. Método estándar:

Las entidades que decidan aplicar este método, deberán comunicar su decisión al BE y mantener a disposición del mismo la documentación que justifique la aplicación del mismo.

Para el cálculo del requerimiento de capital aplicando este método, las entidades deben identificar todas las líneas de negocio que intervienen en la institución (para hacerlo el BE le brinda a las instituciones una lista puntillosa de tareas). De esta manera se llega a una media simple de los tres últimos años, de la agregación para cada año, del valor máximo entre cero y la suma de los ingresos relevantes para cada una de las líneas de negocio, multiplicado por su correspondiente coeficiente de ponderación previsto.

En resumen obtenemos lo siguiente:

$$\left\{ \sum_{\text{años } 1-3} \text{Max} [\sum (IR_{1-g} \times \beta_{1-g}); 0] \right\} / 3$$

Donde:

IR: Ingresos relevantes para cada una de las líneas de negocio.

$\beta$ : Coeficiente de ponderación para cada línea de negocio, según la siguiente lista:

- Financiación empresarial 18%
- Negociación y ventas 18%
- Intermediación minorista 12%
- Banca comercial 15%
- Banca minorista 12%
- Pago y liquidación 18%
- Servicios de agencia 15%
- Gestión de activos 12%

A continuación se exponen algunos de los requisitos a cumplir para poder aplicar el método estándar:

a) Disponer de un sistema de evaluación y gestión de RO bien documentado, con responsabilidades claramente definidas. Deberán identificar su exposición al RO y llevar un registro sobre las pérdidas derivadas de este tipo de riesgos, que superen los umbrales internos establecidos.

Dichos umbrales deberán ser adecuados para el RO asumido por la institución.

b) El sistema de evaluación de RO deberá estar perfectamente integrado en los procesos de gestión de riesgos de la entidad y sus resultados utilizarse activamente, en el proceso de seguimiento y control de su perfil de RO.

c) Disponer de un sistema de elaboración de informes de gestión, que facilite reportes sobre RO a los responsables de las funciones pertinentes. Quienes deberán contar con procedimientos que permitan adoptar las acciones necesarias, a la luz de la información contenida en estos reportes.

d) El sistema de gestión y evaluación de RO deberá ser objeto de una revisión periódica, al menos una vez al año, por parte de la unidad de auditoría interna u otra unidad funcionalmente comparable.

e) Las entidades deberán desarrollar y documentar políticas y criterios específicos, para la asignación de sus actividades y de los componentes de los ingresos relevantes a las respectivas líneas de

negocio. Dichas políticas y criterios deberán ser revisadas y ajustadas, según el caso, a los nuevos riesgos y actividades económicas que pudieran surgir, así como a los cambios resultantes de la evolución de los ya existentes.

#### Método Estándar Alternativo:

En este método para las líneas de negocios, banca minorista y banca comercial, el cálculo de requerimiento de recursos propios podrá realizarse (previa autorización) sustituyendo los ingresos relevantes a los que hicimos referencia en el método anterior, por ingresos relevantes normalizados. Para normalizar los ingresos, se tomarán los saldos contables, para los activos financieros asignados a la correspondiente línea de negocio y se lo multiplica por 0,035.

### 3. Métodos avanzados:

Para obtener la autorización por parte del BE, para aplicar métodos avanzados, es necesario cumplir con algunos requisitos.

#### Requisitos cualitativos:

1. El sistema interno de medición de RO, deberá estar perfectamente integrado en los procesos habituales de gestión de RO. Los resultados de dicho sistema de medición deberán usarse activamente en el proceso de seguimiento y control del perfil de riesgo operacional de la misma.
2. Contar con una unidad de gestión de RO independiente.

3. Informar periódicamente a los distintos responsables designados, incluida la Alta Gerencia, de las exposiciones al RO y del historial de pérdidas. La entidad deberá asimismo disponer de procedimientos para la adopción de medidas correctivas apropiadas.
4. El sistema de gestión de RO deberá estar bien documentado.
5. El sistema de gestión de RO deberá ser objeto de revisión periódica (por lo menos de una vez al año) por parte de la unidad de auditoría interna u otra unidad comparable.
6. Los procesos de validación interna serán llevados a cabo por una unidad que cuente con una adecuada capacitación e independencia.
7. El flujo y proceso de los datos asociados al sistema de medición de riesgo deberá ser transparente y accesible.

Requisitos cuantitativos:

1. Requisitos Generales:

- Las entidades deberán calcular su requerimiento de capital tomando en cuenta, tanto la pérdida esperada como la no esperada. A menos que puedan demostrar que la pérdida esperada está adecuadamente cubierta.
- Para cumplir con el grado de solidez del que habla el párrafo anterior, la entidad deberá tener en cuenta los siguientes elementos: datos internos, datos externos, análisis de escenarios hipotéticos y factores que reflejen el entorno del negocio y el sistema de control interno. Las entidades asimismo deberán disponer de una metodología bien documentada, para ponderar el uso de estos elementos en sus sistemas globales de medición del RO.

- El sistema de medición de este riesgo, recogerá las principales condicionantes que influyan en la forma de las colas de distribución de las estimaciones de pérdidas.
- Deberán identificarse y justificarse adecuadamente las distintas categorías de RO para las que se efectúen cálculos separados de requerimientos de recursos propios, que posteriormente deberán agregarse.
- El sistema de medición del RO deberá tener coherencia interna y evitar la consideración de aspectos cualitativos.

## 2. Requisitos relativos a los datos internos de pérdidas por RO:

- El periodo histórico mínimo de observación será de cinco años.
- Las entidades deberán asignar su historial de datos internos de pérdidas por RO a las líneas de negocio definidas.
- Las pérdidas por este riesgo que estén relacionadas con el riesgo de crédito e históricamente se hayan incluido en la base de datos interna de riesgo de crédito, deberán también incluirse en la base de datos de RO e identificarse por separado. Estas pérdidas no están sujetas a requerimiento de capital por riesgo operacional, siempre que se sigan tratando como pérdidas por riesgo de crédito a la hora de determinar el requerimiento de recursos propios por dicho riesgo.
- Los datos de pérdidas de las entidades deberán ser completos e incluir la totalidad de las actividades y exposiciones importantes de todos los subsistemas y ubicaciones geográficas pertinentes.
- Las entidades deberán recopilar información sobre la fecha del evento, cualquier recuperación respecto del importe bruto de pérdidas, así como información de carácter descriptivo sobre los

factores desencadenantes o las causas del evento que da lugar a la pérdida.

- Deberán contarán con criterios específicos para la asignación de datos pérdidas, procedentes de eventos sucedidos en una unidad centralizada o en una actividad que incluya mas de una línea de negocio, así como los procedentes de eventos relacionados a lo largo del tiempo.
- Asimismo, deberán disponer de procedimientos debidamente documentados para evaluar en todo momento la relevancia de los datos históricos de pérdidas.

### 3. Requisitos relativos a los datos externos de pérdidas por RO:

- El sistema de medición de RO de la entidad deberá utilizar datos externos pertinentes, especialmente cuando existan razones para creer que dichos datos pueden suponer pérdidas potencialmente importantes pero infrecuentes.

### 4. Requisitos relativos al análisis de escenarios hipotéticos:

- Las entidades deberán realizar análisis de escenarios hipotéticos basados en dictámenes de expertos y datos externos, con el objeto de evaluar su exposición a eventos generadores de pérdidas severas.

## 5. Requisitos relativos al entorno del negocio y sistema de control interno:

- La metodología de medición del riesgo, deberá identificar factores básicos de su entorno de negocio y de sus controles internos, que puedan modificar su perfil de RO.
- La elección de cada factor deberá justificarse por su papel de generador significativo de riesgo.
- Deberá razonarse adecuadamente la sensibilidad de las estimaciones de riesgo ante variaciones de los factores, así como la ponderación relativa de cada factor.
- Y por último, los resultados obtenidos de las evaluaciones deberán ser objeto de valuación y reevaluación a lo largo del tiempo, por lo menos anualmente.

### Fuentes consultadas:

- Brasil: Comunicación N° 12746 (9 de diciembre de 2004)  
Comunicación N° 16137 (27 de setiembre de 2007)  
Resolución N° 3380 (29 de junio de 2006)  
Resolución N° 3490 (29 de agosto de 2007)  
Circular N° 3383 (30 de abril del 2008)  
Compilado de consultas frecuentes del BCB, publicado en [www.bcb.gub.br](http://www.bcb.gub.br)
- Chile: “Directrices de la Hoja de Ruta para la transición hacia Basilea II” de la Superintendencia de Bancos e Instituciones Financieras de Chile.  
Ley General de Bancos de Chile.  
Recopilación actualizada de normas de Chile.
- Argentina: “Hoja de Ruta para la implementación de Basilea II” del Banco Central de la República Argentina.  
Comunicación N° 4854 (20 de octubre de 2008)
- México: “Disposiciones de carácter general aplicables a las instituciones de crédito” publicada por la Comisión Instituciones Financieras de Chile.
- EEUU: OCC Basel II – “Regulatory Impact Analysis for Risk-Based Capital Guidelines; Capital Adequacy Guidelines;  
Capital Maintenance: Domestic Capital Modifications; 44620 al 44628 Federal Register /Vol 73, N° 148/  
Thursday, July 31, 2008 / Rules and Regulations  
Web: <http://www.federalreserve.gov/generalinfo/basel2/default.html>  
Boletín Económico de ICE N° 2826 del 29 de noviembre al 12 de diciembre de 2004 “Influencia de Basilea II en la financiación bancaria de los países emergentes” Antonio Partal Ureña, Pilar Gómez Fernández Aguado)
- España: Circular del Banco de España – BOE N° 140 (del 10 de junio del 2008)

# **CAPÍTULO 4**

## **ADMINISTRACIÓN DEL RIESGO OPERACIONAL**

### **EN URUGUAY**



En el presente apartado vamos a tratar de brindarle al lector un panorama general de cómo el ente regulador ha ido incorporando a su normativa, aspectos que pretenden llevar adelante un marco regulatorio alineado con Basilea II.

El Banco Central del Uruguay posee un marco normativo fuerte, que se compone en primer lugar, por una Recopilación de Normas de Regulación y Control del Sistema Financiero (RNRCSF), que trata de resumir toda la normativa emitida por el BCU que se modifica a partir de Circulares. En segundo lugar y por debajo dicha recopilación, se encuentran las Comunicaciones que lo que hacen es reglamentar lo que dice la Recopilación; y por último tenemos los Estándares Mínimos de Gestión (en adelante EMG). Esta herramienta si bien no es una norma, describe los ojos con los que el órgano regulador va a mirar a las entidades, en tal sentido es de entenderse que todas las instituciones han tratado de aplicarlo lo mas puntillosamente posible, dependiendo de su estructura y actividad.

Comenzaremos por comentar los EMG que tienen que ver con el RO, debido a la relevancia que tiene dicha herramienta en nuestro trabajo. Luego de esto, vamos a centrar nuestro interés en la RNRCSF, y comentaremos todos aquellos Artículos que tienen que ver con el RO. Por último, mencionaremos brevemente la Comunicación 2003/179 que refiere específicamente al tema de Gestión de la Tecnología.

- Estándares Mínimos de Gestión

Una de las herramientas más fuertes y nuevas usada por BCU a la hora realizar evaluaciones a las diferentes instituciones bancarias de plaza, son los EMG. Esta herramienta se dio a conocer a las entidades en el año 2007, las mismas tuvieron un plazo para autoevaluarse y de esta manera plantear las inquietudes encontradas.

Tiene el propósito de evaluar la calidad de la gestión de las entidades y en caso de detectar debilidades, evaluar el impacto que las mismas podrían tener sobre la capacidad de la entidad para mantener niveles adecuados de solvencia en todo momento.

Asimismo y con el propósito de contar con un mecanismo que permita resumir los resultados de la evaluación anteriormente mencionada, se ha definido una metodología de Calificación denominada CERT. Este sistema lo que busca es sintetizar la evaluación en los siguientes cuatro componentes:

**C:** Gobierno Corporativo, evalúa el sistema a través del cual las instituciones son dirigidas, monitoreadas y controladas.

**E:** Evaluación Económico Financiera, se evalúa haciendo hincapié en el nivel y calidad del patrimonio de la institución y su capacidad de respaldar los riesgos asumidos y proveer seguridad a los acreedores.

**R :** Riesgos, evalúa la capacidad del ente de identificar, controlar, medir y monitorear los siguientes riesgos de forma integral: Riesgo de Crédito, Riesgo País, Riesgo Tipo de Cambio, Riesgo de Tasa de interés, Riesgo de Liquidez, Riesgo de Cumplimiento, *Riesgo Operacional*, Riesgo Estratégico y Reputacional.

**T:** Tecnología, (en adelante TI) evalúa la confiabilidad y la eficiencia de los sistemas de información como herramientas de gestión, así como la gestión propiamente dicha del riesgo tecnológico.

Cabe destacar, antes de seguir adelante, que el BCU en esta herramienta le brinda un papel preponderante al Riesgo Tecnológico dentro del Operacional, ya que lo separa para ser evaluado especialmente, mientras que Basilea II lo asume como parte del RO. Esta tendencia se percibe a lo largo de toda la normativa local.

La herramienta se compone de 86 estándares y se entiende que el no cumplimiento de uno de ellos constituye una debilidad que debe ser atendida prioritariamente por parte de la institución.

Según se nos informó en la entrevista realizada al Banco Central, los EMG son un documento que les dice a las entidades como van a ser evaluadas por el supervisor. Tal como se nos explicó, la metodología de trabajo se lleva adelante de la siguiente manera:

1. Se realiza una inspección a una determinada entidad.
2. Se evalúa dicha entidad a partir de un procedimiento de supervisión independiente a los EMG.
3. Se obtienen conclusiones de la evaluación realizada.
4. Se extrapolan dichas conclusiones a los EMG y se observa si la entidad esta incumpliendo alguno de ellos.
5. Finalmente, se le envía al banco la Carta de Recomendaciones, donde consta la calificación otorgada según el Sistema de calificación CERT y en su caso, los incumplimientos a los EMG encontrados.

A continuación trataremos de realizar un pequeño resumen de aquellos estándares que tienen relación con el RO a lo largo de todo el documento:

Estándar N° 4.

*“El Directorio debe aprobar los objetivos estratégicos de la institución y supervisar su implementación.”*

En tal sentido, el documento plantea que se debe definir una estrategia y políticas adecuadas para el área de TI y asegurar que la Alta Gerencia implemente los procedimientos que las hagan aplicables.

Estándar N° 5.

*“El Directorio debe aprobar una estrategia de riesgos y políticas asociadas que permitan la identificación y análisis de todos los riesgos que pueden afectar el cumplimiento de los objetivos de la entidad, tanto a nivel individual como en base consolidada”*

Para el cumplimiento de este estándar y en lo que tiene que ver con el RO, la norma plantea que el Directorio debe intervenir activamente en la gestión de riesgos que lleva adelante la entidad, asegurándose de que la Alta Gerencia toma las medidas necesarias para implementar un sistema de gestión integral de riesgos que contemple una visión global de los mismos, involucrando a toda la entidad y generando una cultura de riesgos entre los participantes.

En sus dos últimos puntos, la norma se refiere por segunda vez a la correcta gestión de TI, diciendo que debe existir un sistema de Evaluación de Riesgos que garantice el logro de los objetivos y que permita a la institución enfrentar adecuadamente las amenazas que pueden afectar los servicios tecnológicos. Finalmente agrega que los servicios de TI deben ser monitoreados y auditados por personal independiente.

Estándar N° 19.

*“La Alta Gerencia debe implementar un proceso íntegro de gestión de la Tecnología de Información (TI) consistente con la estrategia”*

Una vez más, la norma hace referencia a la gestión del riesgo tecnológico haciendo hincapié en la importancia de que los procedimientos y controles del área de TI estén claramente definidos y alineados con la estrategia del negocio.

Los estándares que se exponen a continuación, hacen referencia específicamente al tratamiento del *Riesgo Operacional*.

En el preámbulo del mismo la norma plantea que cada entidad puede tener su propia definición de RO, pero que la misma debe ser difundida y entendida a lo largo y ancho de toda la organización. Sin embargo, a partir de nuestro trabajo de campo, llegamos a la conclusión de que la mayoría de los bancos de plaza manejan la definición de RO brindada por Basilea II.

Estándar N° 59.

*“El Directorio debe aprobar y revisar periódicamente los principios generales para el manejo del riesgo operacional y las políticas significativas de la institución para este riesgo. Debe asegurar que la Alta Gerencia implementa los procesos necesarios para que los riesgos asumidos sean consistentes con las estrategias y políticas aprobadas.”*

En este punto, la norma replantea la importancia de la participación del Directorio en la gestión del RO, aprobando las políticas relacionadas a dicho riesgo; promoviendo una cultura de control adecuada en la organización; asegurando

que la gestión de RO se lleva a cabo en forma continua y que sea revisada periódicamente.

Estándar N° 60.

“La Alta Gerencia debe implementar las políticas aprobadas por el Directorio en relación al riesgo operacional, asegurar que las mismas se cumplen y reportar al Directorio sobre su efectivo cumplimiento. Estas políticas y procedimientos deben considerar el riesgo operacional en todas las actividades de la institución.”

Para cumplir con este estándar la Alta Gerencia debe asegurar una estructura organizacional adecuada, con responsabilidades claramente definidas.

Estándar N° 61.

“La Gerencia responsable del manejo del riesgo operacional debe implementar procedimientos de identificación y evaluación de las fuentes de riesgo operacional y definir los mecanismos para mitigar o eliminar dichos riesgos.”

La norma en este punto nos recomienda los siguientes mecanismos conocidos para identificar y evaluar las diferentes fuentes de RO:

- Mapeo de los diferentes procesos, que debe ser sujeto a revisión periódica.
- Mecanismos de auto-evaluación.
-

- Llevar un registro de eventos de pérdidas por RO, así como un registro de incidencias en la atención al cliente.
- Sistema de indicadores de alerta.

Este punto termina haciendo referencia a que en el proceso de creación de nuevos productos debe ser considerado el RO en forma específica.

Estándar N° 62.

“La Gerencia responsable debe implementar procedimientos de control de riesgo operacional”

Según la norma para lograr lo anterior, la gerencia debe mantener un estrecho contacto con las estructuras de control establecidas, tanto para los procesos internos como para aquellos que se encuentran tercerizados.

Estándar N° 63.

*“La Gerencia responsable del área de TI debe proporcionar los servicios en un ambiente seguro, que incluya no solamente las condiciones operativas del área de TI sino también factores tales como confiabilidad, confidencialidad e integridad. Incluye además el soporte y la capacitación a los usuarios del servicio y la habilidad para manejar problemas e incidentes, operaciones, desempeño del sistema, planificación de la capacidad de los datos e instalaciones.”*

Nuevamente la norma nos habla de la importancia de la gestión del área de TI, haciendo hincapié en que se deben promover operaciones de TI efectivas,

seguras y sólidas, que aseguren la continuidad de las operaciones y la confiabilidad y disponibilidad de la información.

Estándar N° 64.

“La entidad debe contar con un plan de contingencia y de continuidad de los negocios que permita operar ante la ocurrencia de eventos externos severos”

Para ello la norma nos dice que se deben establecer planes corporativos que ante distintos escenarios de desastre, aseguren la continuidad del negocio siendo los mismos revisados periódicamente. Además de lo anterior, la norma nos remarca la importancia de contar con planes de respaldo de información que aseguren su recuperabilidad.

El siguiente estándar se encuentra separado del resto y trata específicamente sobre la gestión del área de TI.

Estándar N° 86.

*“La gerencia de TI debe tener la habilidad para identificar las necesidades y para desarrollar, adquirir, instalar y mantener soluciones de TI apropiadas de acuerdo a las necesidades de la entidad”*

En este último punto, se enfatiza la importancia de mantener políticas y procedimientos adecuados y claramente establecidos para gestionar el riesgo tecnológico. Dichas políticas y procedimientos deben considerar específicamente los riesgos asociados a proveedores externos.

- Recopilación de Normas de Regulación y Control del Sistema Financiero

Dentro de la RNRCSF en su libro 5º, nos encontramos con varios Artículos que tratan de guiar a las entidades hacia una correcta administración del RO. Los Artículos que a continuación se van a mencionar fueron reglamentados en primer lugar por la Circular N° 1.878 del 2 de marzo del 2003 y luego por la Circular N° 1.985 del 1º de abril de 2008.

Por un lado, el Art. 307.1 hace referencia a que las entidades deberán mantener procedimientos de resguardo de datos y software que permitan a la organización recuperar toda la información relevante del negocio. Dentro de esta información la norma destaca los reportes que la institución debe presentar al BCU, así como toda la información contable que permite generar dichos reportes. Más adelante, el mismo Artículo plantea que se deben realizar dos resguardos diarios y uno de ellos debe ser almacenado fuera de la institución. Finaliza diciendo que por lo menos una vez al año se deben hacer pruebas debidamente documentadas de levantamiento de un respaldo.

El Art. 307.2 plantea que los máximos niveles directivos y gerenciales son responsables por la ejecución de los procedimientos de resguardo de información, añadiendo que la institución deberá informar al Banco Central el nombre y cargo de la persona mencionada anteriormente.

En este Artículo, vemos claramente la importancia que le da el ente regulador a la participación activa de los altos directivos en la administración del RO (Gobierno Corporativo).

Luego, en el Art. 307.3 la norma plantea que tanto los procedimientos de resguardo así como cualquier recurso que interviene en el proceso de TI,

deberán satisfacer los siguientes requerimientos: disponibilidad, integridad, confidencialidad, autenticidad y confiabilidad.

El Art. 307.5 retoma el tema de que las instituciones deberán contar con un plan debidamente documentado de continuidad operacional, que asegure que las mismas podrán seguir operando en caso de ocurrir cualquier evento que afecte las instalaciones, equipos, datos, etc.

Por último, el Art. 307.6 plantea que las entidades deberán solicitar autorización al Banco Central cada vez que necesiten procesar su información a través de un agente externo (sea éste parcial o total, local o del exterior).

Además de lo anterior, deberán contar con políticas y procedimientos establecidos por escrito, así como con una organización funcional adecuada, para asegurar una efectiva identificación, medición, control y monitoreo de los riesgos (tanto presentes como futuros) asociados a los acuerdos de tercerización relativos al procesamiento externo de la información, ya sea en el país o en el exterior.

Termina el Artículo diciendo que la persona dentro de la organización encargada del área de RO y tecnológico, deberá presentar un informe anual al BCU donde conste un análisis de todos los riesgos asociados a actividades tercerizadas, y una relación de todos aquellos eventos que afectaron la continuidad del negocio y las medidas implementadas para mitigarlos o eliminarlos.

- Comunicación 2003/179

El 12 de septiembre de 2003, el Banco Central publicó la Comunicación N° 2003/179, la cual plantea que para administrar el área de TI deberán adoptar un sistema de gestión que contemple las mejores prácticas de administración en esta materia. En tal sentido, las instituciones deberán guiarse por el marco de referencia C.O.B.I.T (Control Objectives for Information and Related Technology)

emitido por la ISACF (Information Systems Audit and Control Foundation de los Estados Unidos de América). La norma plantea que el BCU va a evaluar el sistema de gestión en las instituciones, considerando los cuatro dominios descriptos en el C.O.B.I.T, la planificación y organización, la adquisición e implementación, la entrega y soporte y el monitoreo.

Según la entrevista realizada al ente regulador, todas las instituciones de plaza se encuentran aplicando C.O.B.I.T para la gestión de su área de TI.

- Conclusión

Podemos ver que la normativa emitida al respecto por el ente regulador local es bastante acotada y su principal hincapié lo realiza alrededor del área de gestión del riesgo tecnológico.

Quedan todavía bastantes aspectos a regularizar, entre ellos la posibilidad de requerir una reserva de capital por riesgo operativo, tal como se tiene previsto en la “Hoja de Ruta hacia Basilea II” (publicado en la pagina web del BCU). Según lo dialogado con el BCU, vienen atrasados con la implementación del cronograma, pero esperan que para el año 2010 ya puedan estar emitiendo nueva normativa al respecto.

Fuentes consultadas:

- Recopilación de Normas de Regulación y Control del Sistema Financiero Web: [www.bcu.gub.uy](http://www.bcu.gub.uy)
- Estándares Mínimos de Gestión Web: [www.bcu.gub.uy](http://www.bcu.gub.uy)
- Comunicación N° 2003/179
- “Hoja de Ruta hacia Basilea II”

## **CAPÍTULO 5**

# **CRÍTICAS A LA ADMINISTRACIÓN DEL RIESGO OPERATIVO**

En el presente capítulo vamos a tratar de acercar al lector a una perspectiva crítica en cuanto a las diferentes formas de administrar el riesgo operativo. Hay quienes entienden que este enfoque no se está llevando por el camino adecuado, ya que consideran que lo verdaderamente importante para administrar este riesgo no pasa por cuantificarlo, si no por gestionarlo de la mejor manera posible.

En tal sentido, a continuación haremos referencia a diferentes críticas sobre el tema<sup>14</sup>:

Doug Hoffman (presidente de Operational Risk Advisors), afirma que el objetivo de la gestión de los riesgos operativos es mejorarla gracias a la identificación anticipada y posterior prevención de malas prácticas empresariales.

Destaca 6 principios fundamentales en la gestión de este riesgo, mencionando la importancia de la aplicación de los mismos por parte de las empresas para mejorar su gestión:

1. Compromiso y cultura en toda la empresa;
2. gobernabilidad en temas de gestión de RO;
3. posibles respuestas ante los RO;
4. identificación, estimación y respuestas ante los riesgos dinámicos;
5. el papel de la legislación;
6. y los cambios tecnológicos que mejoran la capacidad de la empresa para estimar y gestionar el riesgo operativo.

---

<sup>14</sup> Estas críticas fueron tomadas del siguiente documento que resume la conferencia del año 2003 organizada por Finanzas e Inversión de Wharton: “El riesgo operativo plantea nuevos retos a las instituciones financieras y a los legisladores” Publicación en la página Finanzas e Inversión de Wharton, publicado el 23/01/03, [www.wharton.universia.net](http://www.wharton.universia.net))

Andy Kuritzkes (vicepresidente de Oliver Wyman), clasifica los riesgos entre financieros y no-financieros y dentro de esta última categoría se encuentra el riesgo operativo el cual a su vez, se divide en 3 categorías:

1. Riesgo de acontecimientos internos (ejemplo: Caso Barings)
2. Riesgo de sucesos externos: pérdidas procedentes de sucesos externos imposibles de controlar (ej. Atentado del 11 de setiembre)
3. Riesgo de acontecimientos en el ámbito de los negocios: incluye riesgos de todo tipo, como aquellos relacionados con las guerras de precios, bajos niveles de actividad, retroceso en los mercados de valores entre otros. (Ejemplo: caída de Wall Street)

Plantea que: *“las categorías de riesgos no son rígidas y lo que comienza como un riesgo externo puede rápidamente convertirse en un riesgo relacionado con los negocios”. “Y los riesgos relacionados con los negocios sí que tienen importancia. Un cálculo por lo alto nos muestra que, a grandes rasgos, estos riesgos suponen el 60% de los riesgos totales no-financieros. Sin embargo el Bank for International Settlements (BIS) sigue ignorándolos”.*

Alexander Muermann, profesor de Gestión de seguros y riesgos de Wharton, también sugirió que tal vez no fuera necesario tener capital regulador. Y agrega: *“¿Podría la asignación de capital haber evitado los principales hechos ocurridos relacionados con el riesgo, como por ejemplo el colapso de Barings?”*

En 1999, el BIS estableció que el riesgo operativo debía ser respaldado con capital, a lo que Kuritzkes responde: *“en mi opinión, no creo que el BIS ni ninguna otra autoridad legislativa pueda establecer normas sobre cuánto capital deberían inmovilizar los bancos para luchar contra los riesgos operativos. La forma primordial de defensa para este tipo de riesgos, son los controles internos.”*

También critica la metodología utilizada por el BIS para cuantificar el riesgo operativo, el Advanced Management Approach, AMA (Enfoque de gestión avanzada): *“El AMA intenta especificar un enfoque basado en reglas que además sea muy estructurado y sofisticado y que en mi opinión, amplía los límites para los que en un principio se pensó la estimación de los riesgos operativos. No parece merecer la pena. Sería más productivo para el BIS concentrarse en otro tipo de riesgos, como por ejemplo el riesgo crediticio.”*

Richard A. Koss, vicepresidente senior y jefe de gestión de ingresos de Brown Brothers Harriman (BBH), opina acerca de las condiciones del mercado de recompra o repos luego del 11 de setiembre. Anteriormente, en el mercado de recompra no existían riesgos de precios ni de crédito por ser un mercado a corto plazo. Sin embargo, luego del 11 de setiembre, este mercado se vio fuertemente amenazado por riesgos operativos originados por la alta concentración en el mercado de bancos de compensación. Pocas empresas manejaban la tenencia del 50% de repos, por lo que cuando tras el 11 de setiembre una de ellas se hundió durante un tiempo, causó una reacción en cadena en la totalidad del mercado. El mercado de bonos se vio afectado porque habitualmente son utilizados en esas transacciones. El mercado funcionaba pero la liquidez era limitada.

Koss, agrega que el riesgo operativo y el de mercado están relacionados y que para poder tomar mejores decisiones tanto de inversión como de política pública, sería deseable que los agentes de ese mercado y legisladores comprendiesen mejor dichas interrelaciones.

Stefan Walters, vicepresidente y director de mercados y liquidez del Banco de la Reserva Federal de Nueva York y miembro del Comité de Basilea, admitió que en un mundo ideal el capital regulador podría ser innecesario bajo un enfoque que incluya procesos internos de evaluación sobre la idoneidad del capital y de los perfiles de riesgo, así como la revisión y supervisión de la legislación.

El tema fundamental en la gestión de los riesgos operativos, es la recopilación y el análisis de la información pérdida. Walters al contrario de lo que opina Kuritzkes, afirma que el AMA intenta ofrecer cierto equilibrio entre la flexibilidad y la estructura para que el sector bancario desarrolle técnicas de cuantificación pertenecientes a la gestión de riesgos operativos.

Por otra parte, Karen Shaw Petrou, directora ejecutiva del Financial Guardian Group, señala que no existe ninguna manera de cuantificar los riesgos operativos con la que todos estén de acuerdo y que haya sido aceptada internacionalmente. Además, menciona que las propuestas de Basilea hacen muy poco por el reconocimiento del valor de la gestión de los riesgos operativos y su mitigación. Plantea que los sistemas bancarios de Estados Unidos, Europa y Japón son muy distintos y mientras que en Europa y Japón el capital puede proporcionar soluciones efectivas, en Estados Unidos los controles internos y una mejora de la cuantificación de los riesgos operativos serían una mejor solución.

Por último, Frank Loverso del Banco Nacional de Canadá, opina que sería más eficaz desarrollar para el sector bancario un sistema efectivo de detección temprana de señales de peligro, que obligar a las instituciones a asignar un capital regulador para protegerse contra el riesgo.

Fuentes consultadas:

“El riesgo operativo plantea nuevos retos a las instituciones financieras y a los legisladores” Publicación en la página Finanzas e Inversión de Wharton, publicado el 23/01/03, Web: [www.wharton.universia.net](http://www.wharton.universia.net)

## **CAPÍTULO 6**

### **TRABAJO DE CAMPO EN LA PLAZA URUGUAYA**

En el presente capítulo intentaremos acercar al lector a la percepción y tratamiento del riesgo operacional en la plaza financiera uruguaya, considerando la normativa establecida en el Nuevo Acuerdo de Capitales de Basilea.

Según información publicada en la página web del Banco Central del Uruguay ([www.bcu.gub.uy](http://www.bcu.gub.uy)), actualmente la plaza uruguaya está conformada por 14 bancos, siendo 2 oficiales y 12 privados.

Para nuestro trabajo de campo obtuvimos una muestra de los 5 bancos más preponderantes de plaza (públicos y privados) y del ente regulador local (BCU), a los que entrevistamos a partir de los cuestionarios que adjuntamos en los ANEXOS IV y V.

### **6.1. Estudio realizado en Bancos Privados y Públicos**

En particular, para el estudio de los bancos, nuestra atención se centró en los siguientes aspectos:

- A. Definición del RO considerando la gestión y las herramientas utilizadas.*
- B. Medición y cuantificación del RO.*
- C. Gobierno Corporativo y aspecto cultural.*
- D. Consorcio de datos en Latinoamérica y la región.*

#### ***A. Definición del RO considerando la gestión y las herramientas utilizadas.***

Con este punto buscamos exponer resumidamente, la definición y bases de gestión del RO que se manejan en plaza, centrandó nuestra atención en las diferentes herramientas utilizadas a estos efectos.

A partir de las entrevistas realizadas, logramos observar que el 100% de las instituciones encuestadas manejan la misma definición de RO brindada por Basilea II. Por lo que no fue difícil llegar a un entendimiento en el tema.

A modo de resumen, a continuación expondremos un cuadro acerca de las distintas herramientas de gestión que están siendo utilizadas por las instituciones estudiadas.

Banco	Herramientas Propias (P) o de Casa Matriz (CM)	Nombre	Tipo de Herramienta		Periodicidad	Forma de obtención del input	¿Qué se busca con esta herramienta?
			Estática	Dinámica			
1	CM	CIRO (Informe de Pérdidas)		<input checked="" type="checkbox"/>	Mensual	Contabilidad	Informar a CM de las pérdidas ≥ a 3.000 euros
		EBRO (Foto de la situación por área de negocio)	<input checked="" type="checkbox"/>		Anual	Entrevista a los responsables	Obtener un mapeo por clase de riesgos para c/área.
		TRANBAR (22 Indicadores - Valorados entre 0-5)		<input checked="" type="checkbox"/>	Trimestral	A través de los responsables y de los sistemas informáticos	Encontrar las causas que fueron determinantes en un evento de RO
2	P	Mapas de Riesgos	<input checked="" type="checkbox"/>		A definir	Automáticamente, a partir de un software específico	Visualizar todos los riesgos que atentan contra el logro de los objetivos operacionales
		Matrices de Riesgo		<input checked="" type="checkbox"/>			

3	P	Mapeo de Indicadores de Riesgo	<input checked="" type="checkbox"/>		Sin Información	Sin Información	Visualizar todos los riesgos que atentan contra el logro de los objetivos operacionales
		Base de Datos Histórica		<input checked="" type="checkbox"/>	Diaria	Sin Información	
4	CM	Matrices de Riesgo		<input checked="" type="checkbox"/>	Depende del tipo de control	Auto evaluaciones	Para identificar aquellos procesos, riesgos y controles mas críticos
5	CM	Base de Datos Histórica		<input checked="" type="checkbox"/>	Diaria	Por la propia gente o por la contabilidad	Para identificar las características de los eventos de RO así como la cuantificación de los mismos
		Cuestionarios de Auto evaluación	<input checked="" type="checkbox"/>		Depende del área	Cuestionarios específicos por áreas y generales	Evidenciar cuál es la visión de la gente acerca de los riesgos a los que están expuestos
		Indicadores de Riesgo (cerca de 50)		<input checked="" type="checkbox"/>	Depende del Indicador (mensuales, trimestrales y anuales)	Algunos en forma automática y otros recolectando información por todos lados.	Ver su evolución en el tiempo e identificar cambios en su comportamiento

Tal como podemos observar...

El *Banco 1*, posee herramientas novedosas que fueron aportadas por su Casa Matriz y están siendo utilizadas en Uruguay desde el año 2002.

Por un lado tenemos el *EBRO*, que es una herramienta que permite obtener un mapeo por clase de riesgo para cada área (según la clasificación aportada por Basilea), identificándose factores de riesgo y asignándoseles un valor.

Dicho valor es asignado automáticamente en función a una escala que trae la herramienta. Posteriormente, se ordenan de mayor a menor en función de su valor y así se clasifican en riesgos de seriedad alta, de seriedad media y seriedad baja. Los de seriedad alta, son los que acumulan el 80% del riesgo total, los de seriedad media son los que acumulan un 15% restante y los de seriedad baja son los que acumulan el 5% final.

Por otro lado, el *CIRO* es una herramienta que tiene por objetivo recoger los datos de todas aquellas pérdidas que superen los 3.000 euros para ser reportadas a su Casa Matriz.

Por último, el *TRANSBAR* es una herramienta distinta, se compone de 22 indicadores que apuntan a descubrir las causas que fueron determinantes en un evento de RO.

Cada indicador va a ser ponderado, obteniéndose de esta forma un número entre 0 y 10 que representará el nivel de riesgo al que se está expuesto.

A partir de esta herramienta se puede: observar la evolución de los indicadores y arribar a un nivel de riesgo global para cada área de negocio, así como ver cuál indicador está teniendo problemas (niveles de riesgo superiores a 5) y realizar una gestión para mejorarlo.

Las tres herramientas se manejan a nivel de todo el grupo, no existiendo libertad por parte de la sucursal de Uruguay para modificarlas, pero de todos modos las tratan de adaptar lo mejor posible a la realidad de la plaza local.

Por su parte el *Banco 5*, si bien utiliza las clásicas herramientas de gestión (la base de datos histórica y los indicadores de riesgos) utiliza también una tercer herramienta, que son los cuestionarios de auto-evaluación. Son éstos muy interesantes porque muestran la percepción sobre la exposición a los RO, que tiene el personal que está directamente vinculado al área.

Asimismo, la institución tiene por objeto anexar a nivel local nuevas herramientas para gestionar el RO, siendo una de éstas muy parecida a la anterior: entrevistas de auto-evaluaciones grupales. Esta nueva herramienta ampliará el caudal informativo, ya que la gente podrá mostrar su percepción real sobre el RO y seguramente de la discusión van a surgir mayor cantidad de elementos que de un cuestionario.

La segunda herramienta en la que ya se encuentran trabajando, es un Mapa de Riesgo de la entidad, con la que van a evaluar tres aspectos:

- el *impacto financiero* que puede tener un eventual RO en cada una de las áreas, según la pérdida potencial que se pueda generar;
- el *impacto reputacional*, que si bien no es de RO puede tener una gran influencia;
- y por último, *el impacto frente a entes reguladores* quienes pueden ser la DGI, el BCU, etc, pudiendo pasar de una simple multa a que se instale el BCU en la institución.

Es en base a cada uno de estos elementos que se le va a pedir a cada área que se auto-evalúe, para luego ser revisadas por un comité de RO donde se tomarán las decisiones convenientes. De esta manera, van a ir midiendo cuales son las áreas que van a requerir mayor control, en definitiva identificar las áreas de mayor riesgo potencial.

Lo último a destacar respecto al Banco 5, es el fluido relacionamiento con la CM. Ellos envían la información relevada localmente, para ser considerada a nivel consolidado y una vez procesada, les envían lo siguiente:

- un *informe con 7 relojes*, donde cada uno de ellos representa el peso que tiene para el *Banco 5* cada categoría de RO mencionada en Basilea II;
- una *gráfica de barras* que les muestra la posición en que se encuentra cada país, mostrando a su vez la media del sector. Con esto el banco puede ver cuáles son sus debilidades frente a los demás países que componen el grupo y de esta manera ver dónde va a tener que centrar su atención.

Por último, es importante destacar que los bancos públicos del Uruguay están obligados a reportar al Tribunal de cuentas cada fraude interno que se evidencie, ya que se estaría afectando la caja patrimonial del Estado. En tal sentido, se entiende que desde hace ya muchos años, los bancos públicos han desarrollado una gestión del RO en este aspecto en particular incluso desde antes de la publicación de Basilea II.

### ***B. Medición y cuantificación del RO.***

Para analizar este aspecto, intentamos relevar dentro de la muestra analizada, si los bancos locales se encuentran aplicando técnicas de medición y cuantificación del RO y en caso afirmativo, cuáles son las herramientas y modelos que están siendo utilizados a estos efectos.

Así es que encontramos lo siguiente:

1. Ninguno de los bancos entrevistados se encuentra actualmente aplicando modelos o herramientas para cuantificar el capital que se debería reservar para hacer frente a potenciales eventos de RO a nivel local.

2. Dos de estos bancos (Bancos 1 y 5), son considerados por sus Casas Matrices a la hora de realizar su cálculo de requerimiento de capital por RO, es decir que, indirectamente estos bancos locales están teniendo una reserva de capital por este riesgo. Ambas Casas Matrices realizan su cálculo considerando el RO de todas sus sucursales. Sin embargo, podemos diferenciar los dos bancos mencionados en función de los modelos que están utilizando sus Casas Matrices para realizar esta cuantificación:

- *Banco 1*: Lo interesante de este banco, es que su Casa Matriz utiliza dos modelos diferentes, dependiendo de un perímetro que han definido en función de los activos totales de cada sucursal y el margen, entre otros. Es así, que para sucursales como por ejemplo, las de Uruguay, Paraguay y Panamá, que no alcanzan cierto umbral, se van a regir por el modelo Estándar. En cambio los bancos de España y México, se encontraban a fines del 2008 realizando todos los trámites para certificarse por el Modelo Interno Avanzado y ya estarían aplicándolo durante este año (2009). Este grupo, se encontraba trabajando en el modelo avanzado desde hace ya varios años, elaborando el modelo matemático-estadístico con cálculos de distribuciones, etc, porque reconocieron el importante ahorro de capital que este método les permitiría obtener. Es un modelo mucho más completo y complejo y requiere contar con una base de datos de pérdidas de 5 años por lo menos. Para su elaboración, también se tuvieron en cuenta datos provenientes de bases externas para así evaluar distintos escenarios (desde escenarios más benévolos a otros más críticos), y visualizar qué nivel de capital se debería reservar en cada situación (“pruebas de stress”).

-

- *Banco 5*: En este caso, el ente regulador de su Casa Matriz exige que para poder aplicar el modelo Avanzado, se cumplan con los requisitos establecidos para la utilización de este modelo en el 95% del grupo. Por lo anterior, dado que este grupo no cumple con los requisitos mencionados en el 95% de sus sucursales, actualmente se encuentran aplicando el modelo Estándar.
3. El *Banco 4*, si bien no cuantifica un capital por RO, utiliza parámetros elaborados en función de estadísticas que definen rangos para medir las pérdidas operativas materiales que están sufriendo en determinado producto, tarjetas de crédito. Este es el único caso en donde se establecen directrices de medición de pérdidas por RO.
  4. Por su parte, el *Banco 3* se encuentra en la espera de que su Casa Matriz le de los lineamientos y bases para cuantificar el capital a reservar por RO.
  5. Por último, el *Banco 2* no tiene definido un modelo o método a adoptar para realizar este cálculo. Sin embargo, sus sucursales establecidas en países de la región, le han solicitado apoyo en este sentido ya que los entes reguladores de esos países se los están exigiendo. A pesar de ello, este banco se encuentra muy lejos de adoptar un modelo para cuantificar su RO a nivel local.

### **C. Gobierno Corporativo y aspecto cultural.**

Para abordar este punto, indagamos acerca del grado de involucramiento que demuestran los altos directivos de cada entidad en la administración del RO; cómo está estructurada la Unidad de riesgos (en caso de existir); y de qué

manera influye una adecuada cultura organizacional en esta administración o gestión.

De esta forma, destacamos lo siguiente:

- *Banco 5*: mencionaron la novedad que representa la administración del RO dentro de la organización, tanto a nivel local como internacional. La Alta Dirección muestra resistencia frente a la incorporación de una gestión por RO, no tienen conciencia de la verdadera importancia e utilidad de esta área. Los responsables de la misma mantienen informada a la Gerencia mediante reuniones trimestrales en el Comité de RO, donde participan, además el área de Auditoría y de Operaciones. En estas instancias, las áreas involucradas comparten información y discuten las mediciones que se fueron dando así como las medidas que se tomaron.

Sin embargo, la cultura organizacional sigue funcionando como un obstáculo para la correcta administración de RO, evidenciándose cuando se realizan las auto-evaluaciones (herramienta que usan como input) y la gente demuestra falta de entendimiento e interés en el tema. Esto se ve potenciado por el hecho de que no se la considere como un “área prioritaria” dentro de la organización.

Este banco, a nivel mundial está recién avanzando en el tema, encontrándose por el momento más preocupados por cumplir con su CM que por gestionar el riesgo.

La cultura es básica para gestionar el RO, la gente tiene que entender que los gestores de los riesgos son ellos y no hay nadie más que pueda entender mejor los riesgos a los que se exponen y cómo se mitigan.

- *Banco 1*: Localmente, existe una Unidad de Riesgos que está conformada por dos “Guías de Riesgos”, quienes reportan al Director de Riesgos y se

subdivide en: Contaduría, Análisis de Banca Minorista, Análisis de Empresas y la parte de Riesgo Operativo, Control Interno y Riesgo de Mercado. Los reportes que se elaboran son enviados a Casa Matriz, a la Unidad Central de Riesgo Operacional, obteniendo un feedback continuo.

En sucursales de otros países, hay personas responsables del RO que se les denomina “Gestor de RO” y gran parte de su trabajo radica en reportar y actualizar todos los procesos a medida que van surgiendo fallas. Sin embargo, esto es inviable en Uruguay porque la sucursal local es muy pequeña como para tener un encargado de RO en cada área.

Esta Unidad de Riesgos, participa y promueve los *Comités de RO*, donde también participan el Gerente o Responsable del área bajo análisis y eventualmente se puede citar a personas de otras áreas, por ejemplo, alguien de Legales, de Sistemas o de Organización según corresponda al tema a tratar. Estos Comités tienen periodicidad mínima trimestral y constituyen el cierre de las herramientas de gestión de RO, donde los involucrados se comprometen a realizar un seguimiento estricto y de dar o no, la posibilidad de mitigación a las fallas encontradas. La mitigación en sí, le corresponde generalmente al área afectada.

Por otra parte, existen también los llamados *Comités de Dirección* que se encuentran por encima de los *Comités de RO*, y éstos consisten en presentaciones semestrales más genéricas, donde no se analiza cada área puntual sino que se evalúa cómo va el nivel de RO en la Unidad.

Los entrevistados en este banco entienden que la Dirección debe y debería estar involucrada directamente en todo lo relacionado al RO. Manifestaron que en cierta manera, la Dirección está participando de estos temas pero de forma superficial. Consideran que esta es una debilidad que es necesario reforzar a nivel de todo el grupo, pero entienden que la “intangibilidad” de este riesgo representa un obstáculo para involucrar a la Alta Dirección. Opinan que la

*cultura* es todo un tema y la deben imponer ellos mismos con las herramientas que manejan y en la medida de las posibilidades. Para lograrlo, se debe de transmitir y estar presentes capacitando al personal, ya que siempre va a existir gente más receptiva que otra.

- *Banco 4*: En éste no existe un encargado de riesgos que cubra todos los riesgos, sino que cada familia de riesgos está bajo la responsabilidad de diferentes encargados. Es así, que existe un *Gerente de Operaciones* que se encarga de controlar el RO, otro que se encarga del Riesgo de Crédito, etc. Como su estructura es de forma “piramidal hacia fuera”, cada una de estas personas reporta a jefes de Casa Matriz, independientemente de que también emiten reportes a la Gerencia interna. De manera de cumplir con los requerimientos del BCU, existe un Comité de Riesgos que se reúne para analizar todos estos riesgos y se labran Actas con lo que se resolvió.

En definitiva, todo es manejado desde la Casa Matriz y a nivel de grupo se maneja todo un sistema de seguimiento de pérdidas donde cada falla que surge en cada una de las sucursales, es acumulada a nivel global.

En el aspecto cultural, están bastante avanzados ya que, mediante la metodología de auto-evaluación de cada área, se llega a que cada uno sea responsable de la gestión y que no sólo tenga incorporado el proceso sino que también lo cumpla correctamente. En caso que ocurra una falla, el responsable es el encargado de esa área en cuestión.

- *Banco 3*: Este banco mantiene una Unidad de Riesgos separada del resto de las Unidades del negocio. Se reúnen en Comités, todos los integrantes de esta Unidad además del Gerente General, los Directores y también está invitada Auditoría aunque no lo integre. En dichos Comités, se siguen todos los “control issues” o “puntos de auditoría” y se resuelven los planes de acción de cada uno de estos puntos con fechas y responsables. Los planes de acción

se toman localmente, por parte de la dirección y con la aceptación del responsable de riesgos.

El Director de Riesgos tiene a su cargo las siguientes áreas:

- Riesgo de Crédito
- Riesgo de Mercado
- Banca Mayorista
- Riesgo de Crédito Retail
- Compliance
- Riesgo Financiero

En cuanto a la cultura, podemos decir que se destaca su alto compromiso por parte del personal de la entidad al momento de generar los datos que son el input para las herramientas de gestión de RO. Siempre que se solicita la información, ésta es entregada en tiempo y forma.

- *Banco 2:* Como el tema de Gestión y Administración del RO en este banco es todavía un proyecto que recién está comenzando a implementarse, sólo podemos mencionar cómo quedará estructurada la Unidad de Riesgos en el futuro.

Estará dividida en las siguientes áreas:

- Riesgo de Crédito
- Riesgo de Mercado
- Riesgo de Cumplimiento (cumplimiento de normativa)
- Riesgo Operacional

En cuanto al compromiso de la Alta Dirección respecto a la administración del RO, el entrevistado enfatizó que se encuentra fuertemente involucrada evidenciándose en la implementación de un Sistema Integrado de Gestión de Riesgos, y a través del Gobierno Corporativo.

Sin embargo, la cultura debe ser reforzada e impulsada junto con la implementación de este nuevo sistema.

#### ***D. Consorcio de datos en Latinoamérica y la región.***

Aquí lo que buscamos fue ver cuál es la predisposición que demostraban las entidades encuestadas a participar en un Consorcio de Datos de RO.

Las respuestas en este sentido fueron muy similares. Todos los bancos hicieron hincapié en el recelo existente en la plaza para compartir su información. El común denominador fue la creencia de que, de formarse un Consorcio, la información que los bancos compartirían sería de baja utilidad, ya que la verdaderamente útil como ser por ejemplo, un fraude interno y las causas que lo motivaron, quedaría en reserva dentro de cada institución.

Sin perjuicio de esto, alguno de los bancos encuestados mencionaron que sus Casas Matrices sí participaban en Consorcios de Datos en el Exterior. En particular, el Banco 5 nos mostró algunos reportes de datos que su CM les había enviado.

A modo de resumen, es importante mencionar que si bien todos los bancos nos mostraron su visión negativa respecto de la factibilidad de la formación de dicho Consorcio, todos coincidieron en que sería importante su implementación, siempre y cuando la plaza adquiriera una cultura de RO, que facilite la colaboración entre los mismos.

## **6.2. Estudio realizado al Ente Regulador (BCU)**

Para estudiar al ente regulador local, interrogamos al Jefe de la Unidad de Riesgo Operativo, acerca de los siguientes aspectos:

- A. Coordinación, comunicación y presiones internacionales.*
- B. Medidas regulatorias del RO y proyecciones a futuro.*
- C. Dificultades evidenciadas por las entidades para gestionar el RO.*
- D. Consorcio de datos en Latinoamérica y la región.*

### ***A. Coordinación, comunicación y presiones internacionales.***

En primer lugar, indagamos acerca de la existencia de alguna presión internacional respecto de la aplicación de Basilea II. La respuesta que obtuvimos fue que por el momento, no existe ninguna obligación explícita pero que al considerarlas las “mejores prácticas”, es necesario tratar de aplicarlas de la mejor manera posible.

Por otro lado, enfatizó que existe una tendencia internacional a la aplicación del marco regulatorio establecido en “Basilea II”, de la que Uruguay no debe quedar afuera. En tal sentido, el BCU está trabajando a través del ASBA (Asociación de Supervisores de Bancos de las Américas, coordinada por México), en un documento que trata de reutilizar el conocimiento de cada país buscando un común denominador, con el propósito de que todos manejen las mismas directrices.

### ***B. Medidas regulatorias del RO y proyecciones a futuro.***

Tal como se comentó en el Capítulo 4, la regulación local sobre este tema es la siguiente:

- Artículos 307. 1, 307.2, 307.3, 307.5 y 307.6 de la Recopilación de Normas de Regulación y control de Sistema Financiero (RNRCSF).
- Comunicación 2003/179 referente al C.O.B.I.T.
- Los estándares 4, 5, 19, 59, 60, 61, 62, 63, 64 y 86 de los Estándares Mínimos de Gestión (EMG)

No existe por el momento mucha normativa al respecto, lo más reciente y novedoso son los EMG que si bien no son obligatorios por el momento, dejan en evidencia la tendencia de la supervisión. El entrevistado remarcó lo siguiente:

*“Los Estándares Mínimos de Gestión son, como lo dice la frase, unos estándares de cómo los bancos deberían de gestionar sus negocios, son lineamientos, si los bancos quieren alinearse a lo que nosotros estamos supervisando deberían mirar los estándares mínimos y tratar de cumplirlos. No es una norma, es un documento que dice como los supervisores vamos a evaluarlos y con qué ojos vamos a mirar el banco.”*

En cuanto al requerimiento de capital por RO, actualmente no existe ninguna exigencia, pero según lo consultado, se espera que ya para finales de 2010 se comience a exigir un capital regulatorio en función del método del Indicador Básico, tal como está estipulado en la “Hoja de Ruta para Basilea II”.

### ***C. Dificultades evidenciadas por las entidades para gestionar el RO.***

Antes de publicarse los EMG, se estableció una instancia consultiva, donde las entidades podían realizar sus descargas y comentarios. Según se nos comentó, las entidades más pequeñas tenían algunos problemas, ya que no les era tan fácil cumplir con todos los puntos y quizás el punto más problemático era el de Gestión Integral de Riesgos.

Puntualmente respecto del RO, el entrevistado hizo énfasis en el hecho de que es un riesgo nuevo y que no todas las entidades lo tienen desarrollado. En la actualidad existen dos grandes bancos de plaza que deberían atenderlo con mayor prioridad y aunque los mismos ya han presentado planes de acción, vienen atrasados. Un banco pequeño de repente no les preocupa tanto ya que por ejemplo, no poseen mesa de dinero.

Por último, según el BCU ya nadie discute sobre la importancia que tiene el RO, pero lo que hace falta es que los EMG tengan más peso normativo.

### ***D. Consorcio de datos en Latinoamérica y la región.***

Con respecto a este tema, nos respondieron que existe una idea a nivel de ASBA de crear algo, pero todavía hay nada concreto. De todos modos, se hizo hincapié en que para Uruguay se visualiza como algo muy lejano, ya que por el momento hay muchos bancos que todavía no han desarrollado datos internos y no existe suficiente regulación al respecto. En primer lugar, las entidades deberían lograr el manejo de sus datos internos para luego poder usar datos externos.

## **CAPÍTULO 7**

### **CONCLUSIONES DEL TRABAJO REALIZADO**

En el presente capítulo, nos enfocaremos en realizar conclusiones acerca de los puntos estudiados durante nuestro trabajo de campo sobre el tratamiento del riesgo operacional en la plaza financiera uruguaya, comenzando por comparar los marcos regulatorios locales con los de los distintos países analizados.

Podemos concluir que en la totalidad de los países bajo análisis, se han contemplado en mayor o menor medida, los lineamientos y directrices establecidas para una adecuada administración del RO, en el Nuevo Acuerdo de Capitales “Basilea II”.

Sin embargo a diferencia de lo que uno podría pensar, no hemos encontrado concordancia entre el desarrollo interno de un país y su plaza financiera, con la consideración de una exigencia de capital por RO dentro de su marco normativo. En este sentido, podemos referirnos al caso particular de EEUU, país perteneciente al “Primer Mundo” con una plaza financiera sumamente desarrollada, que a diferencia de otros países “tercermundistas” (ej: Brasil) no considera dentro de su normativa obligatoria general, lo establecido en el Pilar I para el RO. Únicamente un mínimo grupo de organizaciones bancarias están obligadas a aplicar estas disposiciones para el establecimiento de su capital regulatorio.

Si comparamos los marcos regulatorios de Uruguay frente a los del resto de la región (Argentina, Brasil, Chile), encontramos que en este sentido estamos posicionados a un nivel más bajo. Esto se debe, a que el regulador local ha enfocado su atención en el control del riesgo tecnológico, descuidando otros aspectos del RO que también deberían ser monitoreados.

A pesar de lo anterior, no se puede obviar el hecho de que el BCU ha desarrollado una “Hoja de Ruta hacia Basilea II” proyectándose hacia la convergencia internacional en la materia.

En lo que respecta a la administración local del RO, podemos concluir que si bien el 100% de los bancos encuestados manejan herramientas de gestión, sería importante que se establezcan obligaciones que refuercen y respalden la implementación de las mismas, a los efectos de lograr un mayor grado de involucramiento de la Alta Gerencia en el tema.

Es menester expresar nuestra opinión acerca de la exigencia de un requerimiento de capital por RO. Para ello deberíamos prestar atención a los siguientes aspectos:

- El reducido tamaño que representa nuestra plaza financiera;
- la fuerte presencia de bancos extranjeros (de los 14 bancos existentes, 12 son bancos privados del exterior);
- el peso poco significativo que representan las sucursales locales a nivel de grupo;
- el bajo nivel de pérdidas operativas que se han evidenciado en la plaza.

En función de ellos, entendemos que no sería imprescindible el mantenimiento de una reserva de capital para cubrir pérdidas por eventos operativos. En tal sentido, a la hora de establecer una normativa preceptiva al respecto, sería recomendable considerar la siguiente subdivisión:

- los Bancos Públicos que representan alrededor del 50% de la plaza;
- los Bancos Privados cuyas Casas Matrices no están obligadas a mantener una reserva de capital para sus sucursales en el exterior;
- y los Bancos Privados cuyas Casas Matrices están obligadas a mantener una reserva de capital para sus sucursales en el exterior.

Para los primeros, teniendo en cuenta que el único respaldo que poseen es el Estado, la regulación debería ser más fuerte ya que en caso de la ocurrencia de un evento de RO que de lugar a pérdidas significativas, se estarían afectando las arcas patrimoniales del Estado. Por lo tanto, en este caso sería recomendable exigir una reserva de capital por este concepto utilizando para ello un modelo estandarizado, para demostrar una mayor solidez. Aquí remarcamos el hecho de la utilización de un modelo Estándar y no Básico, como está estipulado en la “Hoja de Ruta Hacia Basilea II”, ya que consideramos que el modelo estandarizado es mucho más adecuado que el Básico y no tiene mayor complejidad.

Para los segundos, quizás no sería imprescindible una exigencia de capital por RO, pero sí establecer un seguimiento más estricto acerca de su gestión y administración, a los efectos de brindarle mayor tranquilidad a los depositantes.

Por último, para los terceros, opinamos que no sería necesaria la exigencia de una reserva de capital por RO, ya que en caso de la ocurrencia de un evento de estas características, se encontraría respaldado por su Casa Matriz.

Para finalizar con el presente capítulo, nos gustaría detenernos en el ya mencionado Consorcio de Datos. A nuestro entender, esta herramienta les brindaría a las entidades un interesante material consultivo, que por el momento no consideramos que sea viable, ya que las entidades se manejan con extremo recelo a la hora de compartir datos internos, sin mencionar que todavía existen entidades que aún no mantienen bases de datos históricas.

A pesar de lo mencionado anteriormente, consideramos que se debería comenzar a pensar de qué manera y bajo qué condiciones los bancos estarían dispuestos a pertenecer a un Consorcio. A través del mismo, se lograría mayor difusión acerca de los modelos y herramientas utilizados para administrar el RO

en las distintas entidades, contribuyendo a lograr una efectiva Gestión Integral de Riesgos.

A modo informativo, a continuación brindamos al lector una tabla que expone los diferentes Consorcios de Datos que se han formado alrededor de este tema:

<b>BASE DE DATOS</b>	<b>GESTOR Y OBSERVACIONES.</b>
<i>ORX (Operational Riskdata eXchange Association)</i>	<i>PriceWaterhuose. Principales bancos internacionales.</i>
<i>CERO (Consortio Español de Riesgo Operacional)</i>	<i>Grupo de bancos españoles dentro de ORX.</i>
<i>GOLD (Global Operational Loss Database)</i>	<i>Bancos británicos.</i>
<i>MORE (Multinational Operational Risk Exchange)</i>	<i>Gestionada por Netrisk.</i>
<i>DIPO (The Database Italiano Perdite Operative)</i>	<i>Banco de Italia. Sólo bancos italianos.</i>
<i>Algo OpVantage FIRST</i>	<i>Fitch Ratings. Sólo eventos públicos.</i>

15

---

<sup>15</sup> Cuadro obtenido del documento: "El modelo de distribución de pérdidas agregadas (LDA): una aplicación al riesgo operacional." – José Manuel Fera Domínguez, Enrique José Jiménez Rodríguez y José Luis Martín Marín – web: [www.uibcongres.org/imgdb/archivo\\_dpo3639.pdf](http://www.uibcongres.org/imgdb/archivo_dpo3639.pdf)

## Bibliografía

- Documento “Productos derivados y bancos a la deriva: El caso “BARINGS” – Autor: Dr. Gerard Verna – Director de la Cátedra de Ética en los Negocios, Instituto de Empresa, Madrid, Profesor de gestión internacional de empresas, Universidad Laval, Québec.
- El escándalo de la BCCI fue el objeto de numerosos estudios y publicaciones. Nosotros nos referimos principalmente a "The BM Affair", informe del Sen. Joseph Kerry (D-Mass.) y Sen. Hank Brown (R-Colo.) para el Comité del Senado para Relaciones Extranjeras (The Senate Committee on Foreign Relations, Subcommittee on Terrorism, Narcotics and International Operations 30 septembre 1992.) Texto completo y consultable en: <http://www.fas.org/irp/congress/>
- “Las causas de las crisis bancarias y su manejo” Autor: Tony Latter 63, Primera Edición, 1998 México, D.F. (Publicado en inglés por el Centro de Estudios de Banca Central, Banco de Inglaterra, Londres EC2R 8AH, julio de 1997).
- MPRA – “Sound practices for the management of operational risk in financial institutions” in spanish. Pailhé, Cristina, Delfiner, Miguel and Mangialavori, Ana Central Bank of Argentina. January 2007. Web: <http://mpr.ub.uni-muenchen.de/1803/> MPRA Paper No. 1803, posted 07. November 2007 / 02:00)
- “La valoración de las empresas a la luz de Basilea 2” Prof. Jorge Soley – Ahmad Rahnema Madrid 11 de Marzo de 2004
- Presentación Power Point: “Como prepararse para la implementación de Basilea 2 en el ámbito bancario” Montevideo 15 de Octubre de 2004 – Dr. Daniel Jorge Biau - Banco de la Nación Argentina) (Segundo doc consultivo dic 2000)
- Circular Externa 041 de Junio de 2007 – Superintendencia Financiera de Colombia – Cap. XXIII Reglas relativas a la administración del Riesgo Operativo. [http://www.superfinanciera.gov.co/Normativa/NormasyReglamentaciones/cir100/cap23\\_riesgo\\_-\\_opera.doc](http://www.superfinanciera.gov.co/Normativa/NormasyReglamentaciones/cir100/cap23_riesgo_-_opera.doc)

- Carta Informativa Semanal 6 de Agosto de 2006– Año 16 N° 904 -Superintendencia de Bancos y Entidades Financieras de Bolivia — Web: [http://www.sbef.gov.bo/archivos/carta\\_informativa06082006.pdf](http://www.sbef.gov.bo/archivos/carta_informativa06082006.pdf)
- “Gestión estratégica de riesgos – Cómo gestionar la incertidumbre”  
Web:<http://turan.uc3m.es/uc3m/inst/FC/posgrado/documents/GestionestrategicadeRiesgos-EF2003-FT.pdf>
- Boletín de Asesoría Gerencial N° 8 – 2008, “Riesgo Legal desde la perspectiva del Riesgo Operacional”, Espiñeira, Seldom y Asociados firma miembro de PricewaterhouseCoopers.
- “El tratamiento del riesgo operacional en Basilea II”, María Ángeles Nieto Giménez-Montesinos.
- Riesgo operativo de Angel Vilariño, Guatemala, septiembre 2005, Presentación Power Point  
Web: [www.sib.gov.gt/es/presentaciones\\_y\\_conferencias/X/1.ppt](http://www.sib.gov.gt/es/presentaciones_y_conferencias/X/1.ppt)
- “El Nuevo Acuerdo de -Capital Basilea II- y su transposición europea: El proceso y la implementación” Fernando Vargas, Cristina Iglesias Sarria –  
Web: <http://www.bde.es/webbde/es/secciones/informes/be/estfin/numero7/ef0700.pdf>
- Boletín Informativo KPMG “Mito o Realidad” 2008  
Web: <http://www.kpmg.cl/documentos/Boletin%20Informativo%202.PDF>
- Artículo Félix Campoverde Velez : “Administración de Riesgos – Gobierno Corporativo” - 16 Noviembre, 2007  
Web: <http://www.zonaeconomica.com/gobierno-corporativo>
- Documento de la web: <http://redalyc.uaemex.mx/redalyc/pdf/391/391111110.pdf> “La relación entre la estructura financiera y la estrategia competitiva de la empresa desde el punto de vista del control del riesgo. Una mención especial a la estrategia de diferenciación.” Revista Galega de Economía, Junio, año/vol.11 N°001 – 2002

- Documento: “¿Resuelve la Integración Financiera el Problema de Agencia?: El caso de los Grupos Económicos Chilenos.” Autores: Ricardo Paredes M. y Ana María Caller - Publicación del Departamento de Economía de la facultad de Ciencias Económicas y Administrativas de la Universidad de Chile, vol.19, N°2, Diciembre de 1992.
- MPRA – “Sound practices for the management of operational risk in financial institutions” in spanish. Pailhé, Cristina, Delfiner, Miguel and Mangialavori, Ana Central Bank of Argentina. January 2007.  
Web: <http://mpa.ub.uni-muenchen.de/1803/> MPRA Paper No. 1803, posted 07. November 2007 / 02:00)
- Revista McKinsey Quarterly - Artículo “Better operational-risk management for banks.” Web: [http://www.mckinseyquarterly.com/Financial\\_Services/Banking/Better\\_operationalrisk\\_management\\_for\\_banks\\_1835](http://www.mckinseyquarterly.com/Financial_Services/Banking/Better_operationalrisk_management_for_banks_1835)
- Brasil: Comunicación N° 12746 (9 de diciembre de 2004)  
Comunicación N° 16137 (27 de setiembre de 2007)  
Resolución N° 3380 (29 de junio de 2006)  
Resolución N° 3490 (29 de agosto de 2007)  
Circular N° 3383 (30 de abril del 2008)  
Compilado de consultas frecuentes del BCB, publicado en [www.bcb.gub.br](http://www.bcb.gub.br)
- Chile: “Directrices de la Hoja de Ruta para la transición hacia Basilea II” de la Superintendencia de Bancos e Instituciones Financieras de Chile.  
Ley General de Bancos de Chile.  
Recopilación actualizada de normas de Chile.
- Argentina: “Hoja de Ruta para la implementación de Basilea II” del Banco Central de la República Argentina  
Comunicación N° 4854 (20 de octubre de 2008)
- México: “Disposiciones de carácter general aplicables a las instituciones de crédito” publicada por la Comisión Instituciones Financieras de Chile.

- EEUU: OCC Basel II – “Regulatory Impact Análisis for Risk-Based Capital Guidelines; Capital Adequacy Guidelines;  
Capital Maintenance: Domestic Capital Modifications; 44620 al 44628 Federal Register /Vol 73, N° 148/ Thursday, July 31, 2008 / Rules and Regulations  
Web: <http://www.federalreserve.gov/generalinfo/basel2/default.html>  
Boletín Económico de ICE N° 2826 del 29 de noviembre al 12 de diciembre de 2004  
“Influencia de Basilea II en la financiación bancaria de los países emergentes”  
Antonio Partal Ureña, Pilar Gómez Fernández Aguado)
- España: Circular del Banco de España – BOE N° 140 (del 10 de junio del 2008)
- Uruguay:  
Recopilación de Normas de Regulación y Control del Sistema Financiero  
Web: [www.bcu.gub.uy](http://www.bcu.gub.uy)  
Estándares Mínimos de Gestión Web: [www.bcu.gub.uy](http://www.bcu.gub.uy)  
Comunicación N° 2003/179  
“Hoja de Ruta hacia Basilea II”
- “El riesgo operativo plantea nuevos retos a las instituciones financieras y a los legisladores”  
Publicación en la página Finanzas e Inversión de Wharton, publicado el 23/01/03,  
Web: [www.wharton.universia.net](http://www.wharton.universia.net)
- Cuadro obtenido del documento: “El modelo de distribución de pérdidas agregadas (LDA): una aplicación al riesgo operacional.” – José Manuel Fera Domínguez, Enrique José Jiménez Rodríguez y José Luis Martín Marín – Web: [www.uibcongres.org/imgdb//archivo\\_dpo3639.pdf](http://www.uibcongres.org/imgdb//archivo_dpo3639.pdf)
- Convergencia Internacional de Medidas y Normas de Capital - Comité de Supervisión Bancaria de Basilea, revisado en Junio de 2006.
- Documento consultivo – Nuevo Acuerdo de Capital de Basilea - Enero 2001
- Principios Básicos para una Supervisión Bancaria Efectiva – Comité de Basilea de Supervisión Bancaria - Octubre 2006

## ANEXO I

*Buenas Prácticas para la gestión y supervisión del RO según el documento de BCBS 2003 (versión en Español).*

### **Desarrollo de un marco adecuado para la gestión del riesgo**

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

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

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

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

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

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

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

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

**El rol de los supervisores**

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

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

**El rol de la divulgación de información**

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

## ANEXO II

### Principio Básico Nro. 15 – Riesgo Operacional

#### Principio básico para una supervisión efectiva del Riesgo Operacional

*“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 proporcionados a las dimensiones y complejidad del banco en cuestión.”*

#### Criterios Esenciales

1. El supervisor exige que los bancos cuenten con políticas y procesos de gestión de riesgos para identificar, evaluar, vigilar y mitigar el riesgo operacional. 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.
2. El supervisor exige que las estrategias, políticas y procesos de los bancos para la gestión del riesgo operacional 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.
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 riesgo operacional.
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).
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.
6. El supervisor exige que haya mecanismos de notificación adecuados que le mantengan al día de cualquier cambio que afecte al riesgo operacional de los bancos de su jurisdicción.
7. El supervisor confirma que el riesgo legal se tiene en cuenta en los procesos del banco para la gestión del riesgo operativo.
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:
  - aplicar la debida diligencia al seleccionar posibles proveedores de servicios;
  - estructurar el mecanismo de subcontratación;
  - gestionar y vigilar los riesgos relacionados con los mecanismos de subcontratación;
  - asegurar un entorno eficaz de control y;
  - establecer planes de contingencia viables.

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.

#### Criterios Adicionales

1. El supervisor determina que las políticas y procesos de gestión de riesgos cubren los principales aspectos del riesgo operacional, incluyendo un marco adecuado al respecto que se aplica en todo el grupo. Estas políticas y procesos han de incluir entre 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.

## ANEXO III

### *Caída de las Torres Gemelas*

Durante los últimos años ha aparecido un nuevo riesgo (aparte del de crédito y de mercado), que tiene inquietos a más de un ejecutivo financiero. Estamos hablando del riesgo operativo: *“la posibilidad que existe de que una institución pueda paralizarse por culpa de un fallo interno del sistema – como por ejemplo por carecer de protección contra determinadas prácticas comerciales por parte de sus propios empleados que rocen la ilegalidad-, o bien debido a un acontecimiento externo”.*

En el año 2003, la gestión y evaluación de los riesgos operativos constituyó uno de los temas primordiales que fueron tratados en la mesa redonda anual sobre riesgos organizada por Wharton Financial Institutions Center. Básicamente, comentaron acerca de las lecciones que se han aprendido como consecuencia de las pérdidas de explotación, los métodos utilizados para estimar riesgos operativos y los pasos necesarios para gestionarlos.

Como factores desencadenantes del riesgo operativo se nombraron, entre otros:

- Utilización de tecnología automatizada
- Fusiones y adquisiciones a gran escala
- Bancos proveedores de gran variedad de servicios
- Creciente contratación en el exterior
- Mayor utilización de técnicas de financiación, las cuales reducen los riesgos de crédito y de mercado pero incrementan el riesgo operativo.

John Drizk, presidente de Oliver, Wyman & Company, definió el punto sobre el cuál debe girar el debate sobre los riesgos operativos:

- La inconsistencia al definir el riesgo operativo
- La escasez de datos y de técnicas de estimación
- Las limitaciones de acumular capital para hacer frente a este tipo de riesgo
- La importancia de los controles internos y la disciplina del mercado para poder gestionar los riesgos operativos.

*“Aunque se ha progresado mucho para ser capaces de cuantificar los riesgos operativos, se le ha prestado demasiada importancia cuando de hecho no se trata de la solución.”*

*“El riesgo operativo tiene más que ver con la mejora de las prácticas de gestión que con la propia gestión.”*

#### *Consecuencias de los atentados del 11 de Setiembre*

Durante la primera parte de la conferencia se trató especialmente el impacto que tuvo **la caída del 11 de setiembre** sobre los mercados financieros, enfocándose en 3 temas relevantes:

- Las dotaciones para desempleo en la planificación de las empresas y de los sectores
- El peligro que entraña el ciber-terrorismo para el sistema financiero
- La gestión de la necesidad de liquidez de los mercados durante la semana posterior al 11 de setiembre.

Las grandes pérdidas tanto humanas como financieras que ocasionó el desastre, dejó en evidencia las graves fallas en los controles internos y organizacionales que éstas presentaban, razón por la cual un importante número de empresas de gran envergadura se han re-planteado su organización interna.

A continuación nombramos algunas de las medidas que han sido llevadas a cabo con este propósito:

- Establecimiento de múltiples centros de datos, en distintas localidades evitando así la concentración masiva de datos en un solo centro.
- Realojamiento de un significativo número de personal técnico y operativo entre las distintas sedes de la empresa. Antes del 11 de setiembre, era usual que el personal no considerado clave se localizara en lugares seguros mientras que la ubicación de los grandes directivos era centralizada. A raíz de lo ocurrido, hay un mínimo de 2 altos ejecutivos por cada zona.

Sandra C. Krieger (vice-presidente senior y director de gestión de reservas domésticas y descuentos de la Reserva Federal de Nueva York) señala que este nuevo modelo de gestión empresarial puede tener un enorme impacto en los costes, y por este motivo, plantea la necesidad de hacerse un cuestionamiento previo a tomar la decisión de adoptar este modelo para evaluar la relación costo-beneficio.

### Tecnología

El 11 de setiembre mostró la existencia de grandes vacíos entre la redundancia de capacidades de la red de comunicaciones. Internet resultó ser más seguro, por lo que las empresas se están encargando de hacer más seguras estas redes para poder utilizarlas como principal medio de comunicación en caso de crisis y ya han agilizado la recuperación de operaciones de los centros de datos en una hora cuando antes tardaban no menos de 3 horas.

Los participantes del congreso coincidieron en que el ciber-terrorismo es la peor amenaza para los mercados financieros y que las organizaciones deben constantemente protegerse contra potenciales amenazas internas.

### Liquidez

Krieger también habló acerca de la manera que la Reserva Federal hizo frente a las necesidades de liquidez del sistema a raíz del atentado. El 11 de setiembre la Reserva Federal de Nueva York mantuvo sus sistemas de pagos, Fedwire y CHIPS, funcionando sin interrupción.

Sin embargo, para lograr esto, la Reserva Federal se vio obligada a inyectar decenas de billones de dólares en el sistema financiero, y lo hizo a través de préstamos con descuentos y operaciones de mercado abierto. Asimismo, tuvo que dar apoyo a las instituciones financieras del exterior que veían amenazada su situación de liquidez en dólares, mediante acuerdos de intercambios temporales de divisas (con el Banco Central Europeo y el Banco de Inglaterra), e incrementar los acuerdos existentes con el Banco de Canadá.

Por último, señaló la importancia del apoyo gubernamental y de otras instituciones financieras, para determinar el momento de reapertura de la Bolsa ya que cuando esto ocurrió (4 días después), los valores circularon correctamente para acomodarse al mayor volumen de intercambios en un solo día en la historia de la Bolsa de Nueva York. Alrededor de 2 billones de acciones cambiaron de manos ese día sin ninguna dificultad.

## **ANEXO IV**

### **CUESTIONARIO REALIZADO A LOS BANCOS PÚBLICOS Y PRIVADOS**

1. ¿Qué entiende por Riesgo Operativo?
2. ¿Se encuentra actualmente realizando alguna gestión para controlar y monitorear eventuales pérdidas por Riesgo Operativo?
3. ¿Qué herramientas o metodología utiliza la entidad para gestionar el riesgo operacional?
4. ¿Se encuentra actualmente realizado dichos controles por iniciativa propia o por requerimiento de su casa matriz?
5. ¿Por que motivo la entidad se ha interesado en la gestión del riesgo operacional? ¿Piensa que esta gestión le puede aportar ventajas competitivas frente a otras entidades del sector?
6. ¿Participa la alta dirección en la gestión del riesgo operacional? ¿De que forma?
7. ¿Se encuentran actualmente aplicando alguna técnica de las recomendadas por Basilea II para cuantificar el riesgo operativo? ¿Cuáles?
8. ¿Considera que los resultados obtenidos de la aplicación de dicha técnica concuerdan fielmente con la realidad de la institución?
9. ¿Considera el aspecto cultural como un tema de importancia para lograr una correcta gestión del riesgo operacional? ¿En qué medida?
10. ¿Cuál es a su criterio la factibilidad de que se conforme un consorcio de datos en el Uruguay y/o Latinoamérica que puedan ser utilizados para avanzar en la cuantificación del capital por riesgo operacional?
11. Teniendo en cuenta que Basilea II, complementa la definición de riesgo operacional, con una clasificación detallada de pérdidas directamente asociadas a esta categoría de riesgo, ¿Se encuentra actualmente la institución realizando algún procedimiento para cubrirse de alguna de las mencionadas a continuación? ¿De que manera?
  - ✓ Fraude Interno
  - ✓ Políticas de empleo y seguridad laboral
  - ✓ Ejecución, entrega y gestión de procesos
  - ✓ Clientes productos y practicas comerciales
  - ✓ Interrupción de operaciones o fallos del sistema
  - ✓ Daños o pérdidas de activo fijo
  - ✓ Fraude externo

## **ANEXO V**

### ***CUESTIONARIO REALIZADO AL BANCO CENTRAL DEL URUGUAY***

1. ¿Existen exigencias de Organismos Internacionales para que la normativa del BCU se adapte a las disposiciones establecidas en el documento Consultivo de Basilea II?
2. ¿Qué tipos de mecanismos de coordinación y comunicación se han utilizado con otros países?
3. ¿Cuál es a su criterio la factibilidad de que se conforme un consorcio de datos en el Uruguay y/o Latinoamérica que puedan ser utilizados para avanzar en la cuantificación del capital por riesgo operacional?
4. ¿Qué medidas regulatorias ha tomado el Banco Central para supervisar la gestión que realizan las instituciones para administrar su Riesgo Operacional?
5. ¿Qué avances se han hecho a los efectos de establecer un requerimiento mínimo para el capital operativo?
6. ¿Se prevén disposiciones que establezcan la aplicabilidad de métodos de medición interna (IRB) por parte de las Instituciones Financieras (IF) a la hora de evaluar sus riesgos operativos?
7. Con respecto a la Tecnología de la Información (TI) ¿Qué medidas regulatorias ha tomado el BCU al respecto? ¿han sido bien aceptadas por las entidades de plaza?
8. ¿Con qué dificultades se encontraron a la hora de implementar los Estándares Mínimos de Gestión?
9. ¿Cuáles considera usted que son las limitaciones más significativas a las que se enfrentan las entidades financieras para realizar una administración efectiva del RO?
10. Según figura en la Hoja de Ruta para la implementación de Basilea II, publicada en la web, entre el 2009 y 2010 se estaría comenzando a exigir una reserva de capital para cubrir pérdidas operacionales utilizando método del Indicador Básico ¿Estiman cumplir con estos plazos?