EL RIESGO OPERACIONAL, SAE 16 Y AS5: HERRAMIENTAS DE CONTROL Y MEJORA

OPERATIONAL RISK, SAE 16 AND AS5: CONTROL AND IMPROVEMENT TOOLS

Kurt Burneo[1], Luis Berggrun[2], Edmundo R. Lizarzaburu[3]
(1) Banco Interamericano de Desarrollo, 1300 New York Avenue, N.W. Washington, D.C. 20577 - USA
(2) Universidad ICESI, Calle 18 #122-135, Cali - Colombia
(3) School of Business, Esan University, Alonso de Molina 1652, Monterrico Chico, Surco, Lima - Peru
(e-mail: kburneo@iadb.org, lberggru@icesi.edu.co, elizarzaburu@esan.edu.pe)

Recibido: 29/01/2013 - Evaluado: 20/03/2013 - Aceptado: 27/04/2013

RESUMEN

El objetivo del presente documento es desarrollar una revisión de la literatura de los principales conceptos del riesgo operacional en el marco de la evolución de los acuerdos de Basilea I, II y lo propuesto en el marco III y su potencial impacto en las entidades financieras supervisadas. Consideramos que la gestión del riesgo operacional, resultará importante en los próximos años. Asimismo, se presentan normas de auditoría interna y externa que vienen siendo implementadas en economías emergentes y que su aplicación no solo es para el sector financiero, sino para otras industrias. De esta manera, se analizarán temas tales como las fuentes del riesgo operacional, las metodologías para el cálculo del requerimiento de capital por riesgo operacional y una revisión de los estándares de auditoría interna y externa tales como el SAE16 y el AS5. Al final se presentan comentarios y conclusiones finales para posibles líneas de investigación.

ABSTRACT

The main purpose of this paper is to develop a literature review of the concepts of operational risk in the context of the evolution of the Basel Accords I, II and III and, its potential impact in the supervised financial institutions. We believe that, the operational risk management will be important in the following years. Also, the paper shows the characteristics of internal and external auditing process that are being implemented in emerging economies and its application. Thus, the paper will explore topics such as the sources of operational risk, the methodologies for calculating the capital requirement for operational risk and a review of internal audit standards and external such as SAE16 and AS5. At the end, comments and conclusions show potential future researches.

Palabras clave: riesgo operacional; normas de auditoría; SAE 16; AS 5
Keywords: operational risk; audit norms; SAE 16; AS 5

INTRODUCCIÓN

"La administración de riesgos financieros (risk management por sus siglas en inglés) se remonta a comienzos del siglo XX (creo que los financieros fue más o menos en los 70s u 80s), cuando la administración científica de Frederick Taylor fue convertido formalmente para gestionar la incertidumbre y las pérdidas en la producción de Taylor (1911)" (Dean & Bowen, 1994). La administración científica fue el primer intento sistemático para gestionar y mejorar los procesos en las empresas. Este concepto sustituyó a la toma de decisiones basada en la tradición y las reglas generales que pueden ser vistos como un enfoque proactivo para la gestión de los riesgos en las operaciones utilizando los métodos científicos. En la década de 1930, el control de calidad fue introducido por Walter Shewhart, que combina las estadísticas con la Teoría de Lewis de los conocimientos para controlar la variación de los procesos de producción y mejorar la calidad del producto (Shewhart, 1939).

Deming en 1986, señala que el trabajo en equipo es necesario en toda la organización para compensar la fuerza de uno de las debilidades de otros. Puede ser caracterizado como un equipo multi-funcional y la colaboración entre los directivos y no directivos (Dean & Bowen, 1994). Para tener una participación eficaz de los empleados, sugerencias de los empleados deben recibir una seria consideración y tenerse en cuenta siempre que sea relevante en las operaciones. La gestión de riesgos es un paso fundamental del proceso económico, con la incertidumbre como los principales factores de riesgo básico. Se trata de un enfoque riguroso y documentado en todos los niveles de desarrollo de los eventos analizados, lo que requiere información de todas las áreas de interés.

Ward y Chapman proponen un enfoque llamado la incertidumbre de gestión que considera las consecuencias positivas y negativas de la incertidumbre (Chapman & Ward, 2003). Ellos argumentan que la palabra "riesgo" ya tiene una connotación negativa, lo que complica la exploración de oportunidades en la identificación de riesgos y el proceso de análisis. La incertidumbre se centra en la gestión identificación y gestión de todas las fuentes de incertidumbre, la formación de amenazas u oportunidades.

Hay un interés creciente en los mecanismos para la cuantificación y comunicación del riesgo. "El manejo integral de riesgos o Gestión Integral de Riesgos (GIR) ha presentado una gran evolución en los últimos años, como consecuencia de la necesidad de conocer y manejar los niveles de incertidumbre a los que está expuesto durante la ejecución de la estrategia y el cumplimiento de los objetivos, debido en gran parte al proceso de globalización, el cual ha ampliado considerablemente el espectro de oportunidades y también de riesgos a los que se enfrentan las empresas" (Wharton, 1992).

Para Philippe Jorion "el riesgo puede ser definido como la volatilidad de los flujos financieros no esperados, generalmente derivada del valor de los activos o pasivos" (Jorion, 2007, 2010).

El riesgo se caracteriza a menudo por un evento de disparo vinculado a determinadas consecuencias (ISO /IEC, 2009). De hecho, las referencias a los riesgos con frecuencia la asocian con la combinación de la probabilidad y las consecuencias de la ocurrencia de un evento (ISO / IEC, 2009). Desde el campo de la seguridad informática, es posible extrapolar el concepto adicional de una amenaza combinada con una vulnerabilidad que provoca una situación de riesgo (Harris, 2010).

Dentro de este concepto de administración de riesgos, el riesgo operacional (COSO, 2004)[1] ha existido siempre como uno de los principales riesgos en todas las empresas, incluyendo el sector financiero. Si bien no existe consenso por una definición general; el Grupo de Gestión de Riesgo del Comité de Basilea[2] desarrolló recientemente una definición estandarizada de este riesgo y lo define como: *"al riesgo de pérdidas resultantes de la falta de adecuación o deficiencias en procesos internos, actuación del personal, sistemas o bien aquellas que sean producto de eventos externos"* (Servaes *et al.*, 2009).En otras palabras, el riesgo operacional se asocia a

[1] *Coso - Committee of Sponsoring Organizations of the Tread way Commission. (2004). Enterprise Risk Management Integrated Framework.*
[2] *Risk Management Group (RMG).*

errores humanos, fallas en los sistemas y a la existencia de procedimientos y controles inadecuados. Esta definición incluye el riesgo legal pero excluye el riesgo estratégico y reputacional (de Basilea, C.D.S.B - Comité de Basilea, 2003[3]; Coleman & Cruz, 1999).

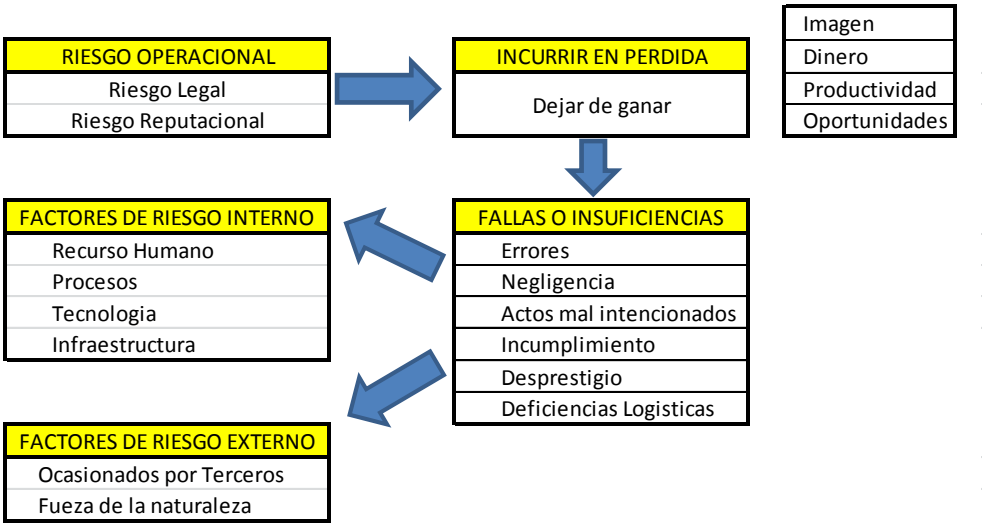

Fig. 1: Riesgo Operacional – Esquema Conceptual (Fuente: Ernst & Young[4])

En relación a la Figura 1, existe una corriente que señala que el riesgo reputacional está excluido del riesgo operacional y es un riesgo que debe medirse por separado (Basel III, 2010), pero se considera que para países emergentes y mientras la metodología se desarrolla es mejor considerando dentro del riesgo operacional para tenerlo claramente identificado.

Asimismo, es importante señalar que el riesgo operacional se diferencia de otros tipos de riesgos, debido a que se ocupa de los procesos establecidos en lugar de la gestión de las circunstancias desconocidas (Frame, 2003).Además se puede definir como los riesgos asociados con las pérdidas que pueden derivarse de las ineficiencias o no conformidades de los procesos operativos dentro de una organización, incluyendo la calidad, la salud ambiental y ocupacional y los riesgos de seguridad, sólo para nombrar los más importantes (Cooke 2004; Raz & Hillson, 2005).

Mientras las empresas están empezando a discutir de manera más categórica la importancia del riesgo operativo, el nuevo Acuerdo de Capital publicado en el 2010 (Basel, 2011), requiere expresamente que la industria de servicios financieros gestione ese riesgo y por tanto lo mitigue.

En este sentido, factores como el desarrollo de las tecnologías de información, el incremento de la competitividad de la industria y la desregulación en los mercados han propiciado una mayor preocupación sobre la importancia de este riesgo y su influencia en la configuración de los perfiles de riesgo de las instituciones (Galloppo & Rogora, 2011).Cabe además señalar que los riesgos operacionales por característica propia son difíciles de identificar, medir, vigilar y controlar.

En últimos años, tanto reguladores como las instituciones del sector financiero se han focalizado en desarrollar modelos para medir y controlar el riesgo de crédito. Sin embargo, la mayoría de problemas ocurridos en este

[3]de Basilea, C. D. S. B. (2003). Sound Practices for the Management and Supervision of Operational Risk. *Basilea, Suiza: Banco de Pagos Internacionales. http://www. bis. org/publ/bcbs96. pdf*.
[4] Ernst & Young, Planning for the New Service Organization Reporting Standards, Insights on IT risk, 2010

tiempo se deben a fallas operativas o al riesgo operacional como resultado de por ejemplo malas prácticas contables, fraudes internos, negociación deshonesta, entre otras. Es por ello que podemos denominar como riesgo operacional a todo lo que implica la posibilidad de incurrir en pérdidas derivadas de fallos en personas, procesos o sucesos externos. Siendo funcional a lo anterior un rápido desarrollo de productos nuevos en los mercados financieros y una más lenta evolución de los sistemas de control por parte de los reguladores.

"El Comité de Basilea de Supervisión Bancaria[5] de Basilea define riesgo operativo como el riesgo de pérdida resultante de procesos internos inadecuados o fallidos, personas y sistemas, o de acontecimientos externos" (Chernobai *et al.*, 2011).

En consecuencia, teniendo en cuenta la magnitud de los eventos y su impacto en el sistema financiero resulta indispensable el desarrollo de sistemas de manejo y control adecuado del riesgo operacional. Por ejemplo, Brown *et al.* (2002), señala que entre los casos que a lo largo de la historia han involucrado fallas operacionales y han tenido gran impacto en el mercado son:

- WORLD TRADE CENTER: Daños a los activos físicos y la interrupción de las operaciones del negocio por los ataques del 11/09 significaron $27 mil millones en pérdidas.
- ALLIED IRISH BANKS: Fraude interno y comportamiento criminal en negociaciones deshonestas ocasionaron pérdidas por $690 millones.
- SUMIMOTO CORPORATION: Pérdidas totales de $2,600millones ocasionadas por negociaciones no autorizadas en 1996.
- ORANGE COUNTY: Negociaciones no autorizadas ocasionaron una pérdida de $1,700 millones y su subsecuente quiebra en 1998.
- BARINGS BANK: La falta de supervisión permitió a Nick Lesson incurrir en pérdidas por $1,200 millones que ocasionaron el colapso del Banco.
- DAIWA BANK: Pérdidas operativas de alrededor de $1,000 millones.
- OTROS: Enron, World Com, Parmalat.

En respuesta a esta serie de los hechos que ocasionaron pérdidas como consecuencia de fallas operacionales y en un contexto en el que la gestión del riesgo trasciende como una estrategia de negocio como respuesta al crecimiento exponencial de la incertidumbre, las exigencias de la regulación y la mayor conciencia sobre el riesgo operacional se ha desarrollado un marco de referencia genérico para la Gestión del Riesgo Operacional (Rodriguez & Corbetta, 2007).

Tomando como base algunas experiencias latinoamericanas, se tiene que en el Perú, la Superintendencia de Banca, Seguros y Fondos de Pensiones (SBS)[6] emitió la norma de gestión integral de riesgos – RS 037 -2008, que se encuentra vigente al 2012, en la Figura 2 se muestra los factores de cambio que inciden en el riesgo operacional y que fueron evaluados por los reguladores. Asimismo la SBS (regulador peruano Superintendencia de Banca, Seguros y Fondos de Pensiones) estableció normas específicas para el manejo de los riesgos operativos a nivel de gestión tales como:

- RS 2116-2009 Reglamento de Gestión ROP.
- Circular G-139 -2009– Gestión de Seguridad de Información
- Circular G-140-2009 – Gestión de continuidad de Negocios

[5]En 1974, los gobernadores de los bancos centrales del G10 conformaron el Comité de Supervisión Bancaria de Basilea, el cual está constituido actualmente por representantes de Alemania, Italia, Bélgica, Luxemburgo, Canadá, España, Reino Unido, Estados Unidos, Francia, Suecia, Japón, Países Bajos y Suiza. Dicho comité no posee autoridad de supervisión supranacional (Banco Internacional de Pagos, 2005).

[6] SBS – Superintendencia de Banca Seguros y Fondos de Pensiones- web site: www.sbs.gob.pe

Asimismo a nivel de requerimiento de capital, la SBS estableció la siguiente norma:

- RS 2115-2009 Reglamento para el Requerimiento de Patrimonio Efectivo por Riesgo Operacional

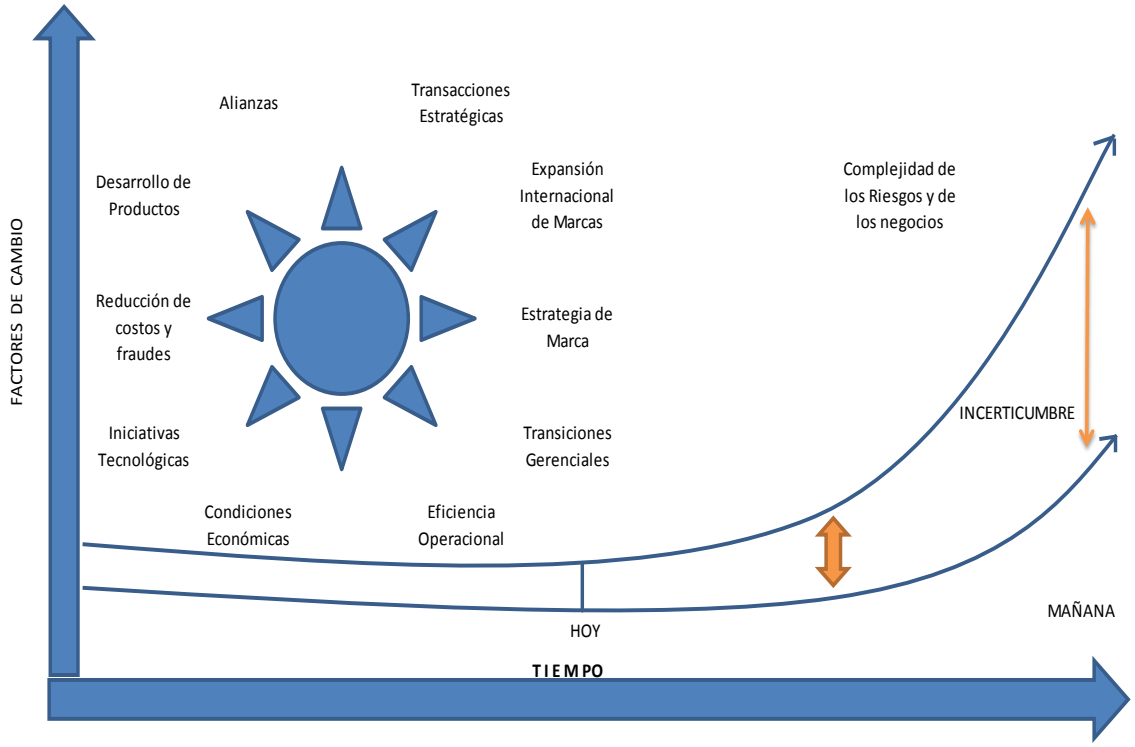

Fig. 2: Riesgo operacional – factores de cambio que inciden en el riesgo operacional
(Fuente: Ernst & Young. Elaboración Propia)

ACUERDOS DE BASILEA

En relación a los acuerdos de Basilea (en el 2010 fue publicado el acuerdo denominado Basilea 3) y el riesgo operacional mencionado en ellos, es importante señalar en que momento aparece este (dentro de las principales preocupaciones para el cálculo de capital de entidades financieras) considerando además que es riesgo operacional puede y debe ser considerado como un riesgo que aparece en diversos sectores. Como paso previo, es importante señalar que Basilea define la "Administración de Riesgos como la cultura o conjunto de procesos, políticas, procedimientos y acciones que se implementan para identificar, medir, monitorear, controlar, informary revelar los distintos tipos de riesgo que se encuentra expuesta une empresa, de tal forma que les permite minimizar pérdidas y maximizar oportunidades"[7].

El primer acuerdo de Basilea I[8], se buscó que el capital regulatorio este alineado frente al riesgo de crédito. Basilea II amplió el ámbito de Basilea I, distinguiendo los diversos riesgos entre el crédito o crediticio, operacional y los riesgos de mercado bajo los auspicios de Pilar I: gestión de riesgos. Asimismo, dos pilares se introdujeron nuevos, revisión supervisora y disciplina de mercado.

[7] *BIS – Sanas Prácticas para la gestión y supervisión del riesgo operativo, febrero 2003.*
[8] *BIS, 2001a. Consultativedocument: operationalrisk. www.bis.org.*
BIS, 2001b. Working paper on the regulatory treatment of operational risk. www.bis.org.

Basilea II estableció una tipología de riesgos operacionales a partir de categorías de eventos de perdidas, así tenemos fraude interno y externo, eventos ligados a relaciones laborales y seguridad en el trabajo, eventos ligados a clientes, productos y prácticas empresariales, daños a activos materiales, interrupción de la actividad y fallas en los sistemas y finalmente eventos ligados a ejecución, entrega y gestión de procesos Price waterhouse coopers (2006). De otro lado este acuerdo, establece las técnicas de gestión de riesgos, de diversa complejidad. El riesgo de crédito se puede medir utilizando el método estándar (SA) o basado en calificaciones internas (IRB). Enfoques IRB consisten en el IRB básico (FIRB) y el IRB avanzado (AIRB) enfoques de Basilea (BIS, 2006).

Los métodos propuestos para medir el riesgo operacional son los criterios básicos, la medición estandarizada e internos. El riesgo de mercado y evaluación de las posiciones de la cartera de negociación puede llevarse a cabo utilizando el método de medición estándar o el método de modelos internos (Masood & Fry, 2012).

El segundo pilar, de supervisión, tiene como objetivo asegurar que los bancos los procedimientos internos de evaluación de riesgos son los recursos suficientes (BIS 2006). El Acuerdo estipula que los bancos deben desarrollar sus propios procedimientos de evaluación y que el cálculo de los objetivos de capital se actualiza continuamente (BIS, 1998, 2001[9]). A los supervisores también se les dio la autoridad para intervenir, mediante la revisión y mejora de los requisitos de capital y otros procedimientos de gestión de riesgos y procesos, según convenga (BIS, 1998, 2001[9]).

El tercer pilar, la disciplina de mercado, busca asegurar la divulgación completa de la suficiencia de capital de los bancos a través de los informes públicos de Basilea (BIS, 2006). Mediante la supervisión de las actividades bancarias, y su capacidad para gestionar el riesgo, los participantes del mercado se puede premiar a los bancos que lo hacen con eficacia, penalizando a los que no lo hacen (Makwiramiti, 2008[10]; Comité de Basilea, 2001[11]).

La crisis financiera del 2008 puso en evidencia varias deficiencias clave en el acuerdo de Basilea II. Estos incluye, entre otros, una falta de distinción entre las posiciones simples y complejas en las exposiciones cartera de negociación, apalancamiento, la estabilidad macro-prudencial (impacto de los bancos en el sistema financiero en su conjunto) y el riesgo sistémico.

Estas fallas han comenzado a ser abordadas en una tercera encarnación - Basilea III (Folpmers, 2010). Las modificaciones realizadas son las reglas prudenciales y de micro-macro-prudenciales más conservadores de capital y los requisitos adicionales de liquidez a los bancos de venta libre se acumulan exceso de apalancamiento.

La mayoría de las investigaciones sobre el riesgo operacional en el pasado se han centrado tanto en la calidad de los métodos de medición cuantitativa de la exposición al riesgo operativo (Makarov, 2006; Degen *et al.*, 2006; Mignola & Ugoccioni, 2006; Neslehova *et al.* 2006; Grody *et al.*, 2005; de Fontnouvelle, 2005; Alexander 2003; Coleman & Cruz, 1999; Cruz, 2002) o los modelos teóricos de los incentivos económicos para la gestión.

Hay tres conceptos principales de medición del riesgo operacional (Jobst, 2007):

- El enfoque basado en el volumen, lo que supone que la exposición al riesgo operacional es una función del tipo y la complejidad de la actividad empresarial, especialmente en los casos en que los márgenes notablemente bajos (como en el procesamiento de transacciones y pagos relacionados con actividades del sistema) magnifican el impacto de pérdidas por riesgo operacional.

[9] *BIS, 2001a. Consultative document: operational risk. www.bis.org.*

[10] *Makwiramiti, A. (2008). The Implementation of the New Capital Accord (Basel II): A Comparative Study of South Africa, Switzerland, Brazil and the United States. Grahamstown: Rhodes University.*

[11] *de Basilea, C. D. S. B. (2001). Operational Risk. Basilea. [Links].*

- La auto-evaluación cualitativa del riesgo operacional, que se basa en juicios subjetivos y prescribe una revisión exhaustiva de los distintos tipos de errores en todos los aspectos de los procesos bancarios con el fin de evaluar la probabilidad y la severidad de las pérdidas financieras de los fallos internos y posibles choques externos.
- Las técnicas cuantitativas, que han sido desarrolladas por los bancos con el propósito principal de asignación de capital económico a exposiciones de riesgo operacional en el cumplimiento de los requisitos de capital regulatorio.

FUENTES RIESGO OPERACIONAL

El Riesgo Operacional (Buchelt & Unteregger, 2003) considera cuatro (Cruz, 2002; Coleman & Cruz, 1999) principales fuentes con sus respectivos eventos (Goenka, 2004), se consideran dos niveles con la finalidad de poder separar el grado de impacto, siendo el nivel 1 de grado medio y el nivel 2 de grado alto, es importante señalar que esta separación no está relacionada al grado de tolerancia que una empresa o entidad tiene respecto al riesgo operativo:

PROCESOS INTERNOS

Las empresas deben gestionar apropiadamente los riesgos asociados a los procesos internos implementados para la realización de sus operaciones y servicios, relacionados al diseño inapropiado de los procesos o a políticas y procedimientos inadecuados o inexistentes que puedan tener como consecuencia el desarrollo deficiente de las operaciones y servicios o la suspensión de los mismos (Tabla 1).

Tabla 1: Fuentes de Riesgo Operacional – Procesos Internos

Categoría	Nivel 1	Nivel 2
Procesos	Control Interno	Falta de controles duales
	Contratación y designación del personal de confianza	Deficiente labor de auditoría Interna Falta de idoneidad del personal de confianza
	Cumplimiento	No observancia de los procedimientos de cumplimiento internos Confiabilidad de la información Deficiencias o incumplimientos en el manejo de información reservada
	Seguridad de Información	Deficiencias en procedimientos para proteger la información
	Supervisión de Empresas	Ingreso en el mercado de participantes no adecuados

Elaboración Propia

Personas

Las empresas deben gestionar apropiadamente los riesgos asociados al personal de la empresa, relacionados a la inadecuada capacitación, negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, entre otros (Tabla 2).

Tabla 2: Fuentes de Riesgo Operacional – Personas

Categoría	Nivel 1	Nivel 2
Personas	Fraude cometido por empleados	Colusión
		Malversación de fondos
		Robo
	Actividad no autorizada / Operaciones fraudulentas/ Delitos cometidos por empleados	Uso indebido de información confidencial
		Manipulación del mercado
	Pérdida o falta de Personal Clave	Ignorar o pasar por alto deliberadamente los procedimientos
		Falta de empleados idóneos

Elaboración Propia

Sistemas

Las empresas deben gestionar los riesgos asociados a la tecnología de información, relacionados a fallas en la seguridad y continuidad operativa de los sistemas informáticos, los errores en el desarrollo implementación de dichos sistemas y la compatibilidad e integración de los mismos, problemas de calidad de información, la inadecuada inversión en tecnología, entre otros aspectos (Tabla 3).

Tabla 3: Fuentes de Riesgo Operacional – Sistemas

Categoría	Nivel 1	Nivel 2
Sistemas	Capacidad de los Sistemas	Falta de la adecuada capacidad de planeamiento / software inadecuado
	Violación de los Sistemas de Seguridad	Violaciones de la seguridad externa
		Fallas en los controles de seguridad interna

Elaboración Propia

Eventos Externos (Rutledge, 2004)
Las empresas deberán gestionar los riesgos asociados a eventos externos ajenos al control de la empresa, relacionados por ejemplo a fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, entre otros factores. En relación al nivel 1 de los eventos externos, se hace referencia a los grupos de interés que tienen o pueden interactuar con la organización (Tabla 4).

Tabla 4: Fuentes de Riesgo Operacional – Eventos Externos

Categoría	Nivel 1	Nivel 2
Eventos Externos	Riesgo Sistémico en el mercado de valores	Desconfianza del Público
	Inadecuado manejo de la crisis por la autoridades	Medidas por parte de las autoridades Daños a la credibilidad de los organismos supervisores

Elaboración Propia

ASPECTOS DEL RIESGO OPERACIONAL (Buchelt & Unteregger, 2003)

La naturaleza del riesgo operacional es muy compleja; una de sus características es que es frecuentemente incurrido de manera inconsciente. Dentro de una institución es importante identificar activamente los riesgos y desarrollar una cultura de consciencia entre las personas, así como también en todos los niveles de la institución.

El riesgo operacional se presenta frecuentemente en los lugares y situaciones menos esperados porque no se ha desarrollado una cultura de prevención y acción proactiva en relación al riesgo (Alexander, 2003).

Por esta razón, tomar referencia en experiencias pasadas no resulta una opción viable en este contexto. En contraste con otras categorías de riesgo, para las cuales las fuentes de riesgo son comprensibles y bastante claras, el desafío es anticipar la mayor cantidad de aspectos de riesgo operacional posibles dentro una entidad financiera. Por lo tanto, la única manera de prevenir o, al menos, limitar los daños que pueden presentarse es desarrollar procedimientos adecuados.

La gestión del riesgo operacional (Chernobai *et al.*, 2006) es, sin duda, un tipo distinto de gestión de riesgo, ya que no está limitada en su alcance a una división específica de una empresa o una línea de negocio particular y, además, la naturaleza de las diversas fuentes de error - procesos, personas, sistemas o eventos externos - varían ampliamente y requiere de una extensa gama de mecanismos de prevención y control.

Las diferentes formas de riesgo operacional posibles, deben ser identificadas y evaluadas respecto de su impacto potencial y de los procesos necesarios para prevenir y mitigar los riesgos (Mignola & Ugoccioni, 2006). El objetivo es afianzar la forma adecuada de lidiar con el riesgo, es decir, darle un nivel de importancia de acuerdo a la relación que tiene con las operaciones del negocio (Mignola & Ugoccioni, 2006).

El carácter integral de la gestión del riesgo operativo hace necesario el compromiso dentro de todos los niveles de la organización. En este contexto, resulta indispensable la comunicación continua, abierta y directa, no sólo para diagnosticar y evaluar adecuadamente la situación de riesgo, sino también para lograr un conceso en las medidas relacionadas a la adecuación del marco de referencia.

La única manera de reconocer y evitar este riesgo es con la realización consistente de autoevaluaciones de control de la situación de riesgo y el mantenimiento de un sistema eficaz de aseguramiento de calidad durante la ejecución de un marco de referencia de gestión del riesgo operacional.

METODOLOGÍAS DE MEDICIÓN DEL RIESGO OPERACIONAL (Sundmacher, 2007)

El primer paso en la medición del riesgo es contar con una definición del mismo (Jorion, 2007). Como se menciona anteriormente, Basilea II define el riesgo operacional como el riesgo de pérdida resultante de una falta de adecuación o de un fallo de los procesos, el personal o los sistemas internos; o bien como consecuencia de acontecimientos externos. Esta definición incluye el riesgo legal, pero estaría excluyendo el riesgo estratégico y el riesgo reputacional.

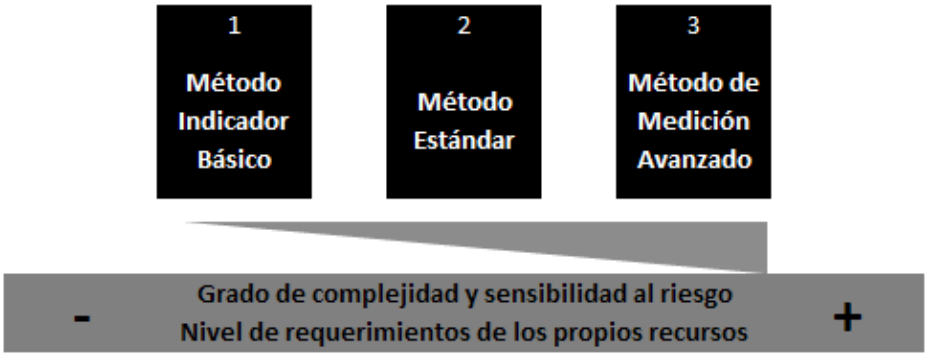

Fig. 3: Riesgo Operacional – Metodologías de Medición (elaboración propia)

Las metodologías propuestas por el Comité de Basilea y que se muestran en la Figura 3 son básicamente tres: el modelo básico, el modelo estándar y los modelos avanzados (Folpmers, 2010). Se trata de modelos cada vez más avanzados (Cruz, 2002) para los cuales se exige cumplir unos requisitos cada vez más complejos en cuanto a la gestión del riesgo operacional por parte de las entidades.

Método Indicador Básico (BIA)

El cálculo se realiza multiplicando un factor α = 15% por promedio de los tres últimos años de los ingresos netos anuales positivos de la institución. Dicho cálculo tendrá un piso de 5% y un techo de 15% del promedio de los últimos 36 meses de los requerimientos de capital por riesgo de crédito y de mercado. Basilea II define ingresos brutos como los ingresos netos por intereses más otros ingresos netos ajenos a intereses.Esta medida debe excluir las provisiones dotadas, los gastos de explotación, 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 indicador ingresos brutos pretende ser una aproximación al tamaño o nivel de actividad de una entidad. Se buscaba una medida que fuese simple y pudiera ser comparable entre distintas jurisdicciones. Obviamente, no es una medida perfecta de riesgo operacional, pero su representatividad es muy superior a la de los otros indicadores que se tuvieron en consideración alternativamente, como cifras de balance (concretamente, inversión crediticia 7) o número de trabajadores.

El BIA es un método muy simple, que no exige ningún otro requisito cualitativo aparte de este sencillo cálculo. Por ello, no se espera que sea utilizado por las entidades internacionalmente activas.
Método Estándar (STDAOp) y Estándar Alternativo (ASA)

Se trata del mismo sistema que el método básico, con la diferencia de que en estos enfoques se exige a las entidades que dividan su actividad en líneas de negocio.

El método de cálculo consiste en multiplicar unos porcentajes fijos (β) por un indicador de la exposición al riesgo operacional en cada una de las 8 líneas de negocio siendo estas:

- Finanzas corporativas
- Negociación y ventas
- Banca minorista
- Banca comercial
- Liquidación y pagos
- Servicios de agencia
- Administración de activos
- Intermediación minorista

STDAOP

Se clasifican los activos en ocho líneas de negocio y se les asigna un factor β que puede ser del 12%, 15% ó 18%. Cada factor se multiplica al promedio de los tres últimos años de los ingresos netos positivos; en caso de que el ingreso neto total sea negativo en algún año, entonces se sustituye el valor de ese año por cero. El método estándar no consiste en un mero cálculo de recursos propios, sino que pretende que las entidades que lo sigan realicen una gestión activa de su riesgo operacional. Por ello, para poder optar por este método se deberán cumplir unos requisitos cualitativos bastante exigentes.

Se requiere la implicación activa de la alta dirección y el consejo de administración; que el sistema de evaluación del riesgo sea sólido y esté 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, se exige que la entidad disponga de un sistema de evaluación y gestión del riesgo operacional que:

- Esté integrado dentro de los procesos de gestión del riesgo de la entidad.
- Asigne responsabilidades a una unidad de riesgo operacional.
- Realice un seguimiento sistemático de las pérdidas relevantes sufridas en cada línea de negocio.
- Cuente con un sistema periódico de información a la dirección de las líneas de negocio, alta dirección y al consejo de administración.
- Esté suficientemente documentado.
- Sea validado interna y externamente por los auditores y/o supervisores.

Los requerimientos totales de capital serán:

$$\boldsymbol{RC_{SA} = \{\Sigma_{años\ 1-3} max[\Sigma(IB_{1-8} \times \beta_{1-8}), 0]\} / 3} \quad (1)$$

Donde:

$RC_{SA} = RequerimientosdeCapitalenelMétodoEstándar.$

$IB_{1-8} = IngresosBrutosdecadaLíneadeNegocio.$

$\beta_{1-8} = Porcentajefijocuyovalor^{9}paracadalíneadenegocio:$

- *Finanzas corporativas: (β1) = 18%*
- *Negociación y ventas: (β2) = 18%*
- *Banca minorista: (β3) =12%*
- *Banca comercial: (β4) = 15%*
- *Liquidación y pagos: (β5) = 18%*
- *Servicios de agencia: (β6) = 15%*
- *Administración de activos: (β7) = 12%*
- *Intermediación minorista: (β8) = 12%*

ASA
Se calcula igual que el STDAOp, a excepción de dos líneas de negocio, la banca comercial y la minorista. En el caso de estas líneas de negocio, los préstamos y los anticipos son multiplicados por un factor fijo m = 0.035, y el resultado sustituye a los ingresos brutos como indicador de riesgo.

En la Tabla 5, se presenta un ejemplo del cálculo de capital requerido por el Método Indicador Básico y el Método Estándar: quizás colocar este ejemplo antes del párrafo anterior que explica el ASA.

Tabla 5: Riesgo Operacional – Cálculo del Requerimiento de Capital

Líneas de Negocio	2005	2006	2007	Promedio	Factor α	Capital Requerido
Ingresos Brutos Anuales Positivos	15,620.0	17,977.0	22,321.0	18,639.0	15%	2,797.0
Total	**15,620.0**	**17,977.0**	**22,321.0**	**183,639.0**		**2,797.0**

RWA =Capital Requerido x 12.5 (*) >>>>>>2,797 x 12.5 = 34,949

STDAOp		Ingreso Anual Bruto (GI)					
N°	Líneas de Negocio	2005	2006	2007	Promedio	Factor p	Capital Requerido
1	Finanzas Corporativas	0	0	30	10	18%	2
2	Negociación y Ventas	565	781	1,846	1,064	18%	192
3	Pagos y Liquidación	755	918	1,062	912	18%	164
4	Banca Comercial	4,532	5,035	6,226	5,264	15%	790
5	Servicios de Agencia	-	-	-	-	15%	-
6	Banca Minorista	9,600	11,096	12,944	11,213	12%	1,348
7	Administración de Activos	169	147	183	166	12%	20
8	Intermediación Minoristas	-	-	-	-	12%	-
	Total	**15,621**	**17,977**	**22,291**	**18,630**	-	**2,516**

RWA =Capital Requerido x 12.5 (*) >>>>>>2,797 x 12.5 = 34,949
(*) 12.5 es la inversa del coeficiente mínimo de capital del 8% (12.5 = 1 / 0.08)
Se consideran además saldo de cartera o de préstamos, con lo que se afina el cálculo.

Ahorro de Capital utilizando el STDAOp = 10.1%

Método de Medición Avanzado (AMA) (McNeil *et al.*, 2005)

Sin duda, una de las mayores novedades de Basilea IIha sido la admisión de los modelos internos de medición del riesgo operacional de las entidades para calcular los requerimientos de capital, previa aprobación del supervisor.

Es un enfoque más avanzado que el utilizado en riesgo de crédito, donde las entidades utilizan sus modelos internos para calcular ciertos parámetros, pero no para obtener el importe final de los requerimientos de capital. La novedad y el atractivo de la utilización de los modelos internos en riesgo operacional radican, precisamente, en que la entidad puede utilizar a efectos regulatorios el resultado de su propio modelo (que ha diseñado según sus necesidades de gestión).

En este sentido, existe una mayor similitud con la regulación actual del riesgo de mercado, si bien la flexibilidad que se otorga en riesgo operacional es aún mayor, pues no se especifica qué método de medición se debe seguir.

En el AMA, los requerimientos de capital son determinados por el sistema de medición de riesgo operacional interno de la Institución. Para poder utilizar este método se requiere de autorización del regulador local, misma que dependerá del cumplimiento de los siguientes requisitos:

- La administración debe estar fuertemente involucrada con el marco de administración de riesgo operacional.
- Se debe contar con un sistema de administración de riesgo operacional íntegro.
- Se debe contar con recursos suficientes en el uso del enfoque en las líneas de negocio más importantes así como en las áreas de control y auditoría.
- Estándares cualitativos y cuantitativos.

El AMA (Helbok & Wagner, 2006) considera los siguientes enfoques:

ENFOQUE DE MEDICIÓN INTERNA
El regulador determina el Índice de Exposición y un múltiplo, en el cual convierte la Pérdida Esperada (EL) en Pérdida no Esperada (UL), en forma análoga para todo el gremio, y cada Entidad obtiene, solamente, estimaciones de la Probabilidad de Fallo y de la Proporción de Pérdida dado el Fallo.

REQUERIMIENTOS NECESARIOS PARA LOS MODELOS INTERNOS: Basilea II sienta unos criterios generales cualitativos y cuantitativos muy rigurosos que deberán cumplir las entidades que sigan el modelo AMA para poder obtener una aprobación del supervisor, a efectos de cómputo de capital.

REQUISITOS GENERALES: En primer lugar, se establecen criterios generales que, de alguna forma, vienen a recoger la filosofía de todos los requisitos necesarios para la admisión los modelos internos a efectos de capital. En síntesis, el Nuevo Acuerdo requiere la implicación activa de la alta dirección y del consejo de administración en la gestión del riesgo operacional, que el modelo interno sea sólido y esté plenamente integrado en los sistemas de medición y gestión de riesgos de la entidad (use test), y que la entidad cuente con recursos suficientes tanto en las líneas de negocio como en las áreas de control y auditoría. Desde el punto de vista del supervisor, el denominado use test es un requisito primordial en la validación de los modelos internos a efectos de capital. Consiste en la comprobación de que el modelo de medición sirve para la gestión activa del riesgo y es utilizado diariamente por la organización. Este requisito implica que en ningún caso sería admisible un modelo cuya única finalidad fuera el cálculo de los requerimientos regulatorios de capital.

REQUISITOS CUALITATIVOS: Todo modelo interno debe servir para su finalidad básica, que es facilitar una gestión activa del riesgo. Dada la gran flexibilidad admitida en el tratamiento del riesgo operacional, 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 (Sundmacher *et al.* 2007):

- 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 información periódica a las direcciones de las líneas de negocio, a la alta dirección y al consejo de administración.
- El sistema debe estar suficientemente documentado.
- Debe ser validado interna y externamente.

REQUISITOS CUANTITATIVOS: Dada la continua evolución de los métodos analíticos en el tratamiento y medición del riesgo operacional, el Comité no especifica el método o los supuestos sobre distribuciones de probabilidad utilizados para medir este riesgo a efectos del capital regulador. Sin embargo, la entidad deberá demostrar que el método utilizado identifica los eventos situados en las colas de la distribución de probabilidad y que generan grandes pérdidas. Con independencia del método empleado, el banco deberá demostrar que su medida del riesgo operacional satisface unos criterios de solidez comparables a los del IRB (Internal rating-based approaches).

El Comité examinará antes de la implantación del Nuevo Acuerdo los progresos de la industria bancaria en el ámbito de la medición del riesgo operacional, los datos acumulados de pérdidas y los requerimientos de capital estimados por los modelos AMA, y refinará las propuestas si lo estima oportuno.

EL ENFOQUE DE TARJETAS DE PUNTAJE
Se calcula un nivel de riesgo tomando como base toda la estadística de eventos de pérdida disponible para la Entidad (habida cuenta de que es estadísticamente significante), y se redistribuye por Línea de Negocio, en función de una tarjeta de puntaje diseñada exprofeso y que contiene el seguimiento de ciertas medidas de control.

El capital regulatorio del AMA está dado por la suma de la Perdida Esperada (EL) y la no esperada (UL). En caso que la Institución pueda demostrar que se está registrando apropiadamente la Perdida Esperada (EL), entonces podrá disminuir este monto a únicamente la Perdida no Esperada (UL).

Todos los modelos AMA deberán utilizar los cuatro elementos básicos de un sistema de medición de riesgo operacional, a saber: datos internos, datos externos, escenarios, y factores de control y entorno de negocio.

SAS 70 Y SU CAMBIO AL SSAE16

SAS 70 (Statementon Auditing Standard N° 70) (Nickell & Denyer, 2007) es un estándar de auditoria reconocido internacionalmente desarrollado por el American Institute of Certified Public Accountants (AICPA) en 1992 y que viene siendo empleado como herramienta para mitigar el riesgo operativo.

Existen diversas razones por las cuales se exige que las empresas de servicios sigan los lineamientos de SAS 70. Las leyes "Probability and Accountability" de 1996 (HIPAA), Gramm-Leach-Biley de 1999 pero sobre todo la Ley Sarbanes-Oxley de 2002 (Secciones 302 y 404) (Nickell & Denyer, 2007)

En conjunto estas tres leyes respaldan la protección de la privacidad, responsabilidad corporativa y el establecimiento de controles internos en las organizaciones. Por lo tanto, se creó la necesidad dentro de las organizaciones de realizar un duedilligence que puede agregar muchos de los principios que se encuentran dentro de estas tres leyes y ofrecer a las empresas un alto nivel de seguridad y confianza cuando se utilizan empresas de outsourcing de funciones críticas del negocio. Además, el crecimiento global de la tecnología y su penetración en todos los niveles de la organización ha facilitado el crecimiento de las auditorías de SAS 70.

Centros de TI (definir sigla) como por ejemplo de los proveedores de Internet, los data wharehouses, junto con los seguros y otras organizaciones relacionadas con el procesamiento de quejas han crecido de manera exponencial en los últimos años. Por tanto, resultaba necesario un proceso de auditoría que asegurará la integridad de la información y todas las operaciones.

Además, existe dentro de la cultura empresarial la idea que los datos y todas las transacciones relacionadas con TI deben ser seguros y protegidos en todo momento. La fuerte dependencia en los sistemas informáticos ha producido la necesidad de brindar seguridad para proteger datos, procesos y procedimientos relacionados con controles diseñados para hacerlo de manera efectiva.

En consecuencia, las auditorías de SAS 70 han llegado a ser conocidas como "documento de duedilligence de facto" con respecto a la presentación de informes sobre los controles internos de una organización con la capacidad de impactar en la presentación de reportes financieros. Dado que el alcance de las auditorías SAS 70 ha crecido enormemente en los últimos años, organizaciones de servicio en casi todas las industrias son candidatos idóneos para este tipo de auditorías. Existen numerosas ventajas para empresas de servicios al certificarse como SAS 70 y para los usuarios de informes de SAS 70.

El resultado de una auditoria SAS 70 reflejaría un análisis de una organización en términos de la efectividad de sus controles. Un informe SAS 70 tipo I emitiría un diagnostico desde un punto específico en el tiempo, mientras que un informe SAS 70 tipo II revelaría la situación dentro de un periodo de tiempo específico.

Un beneficio adicional para las organizaciones de servicio es la posibilidad de aprovechar la certificación SAS 70 como un elemento diferenciador en el mercado y establecer una ventaja competitiva frente a otras empresas del mismo rubro. Cumplir con SAS 70 permite disminuir la cantidad de eventualidades que interrumpen de las actividades del negocio eliminando de manera efectiva la posibilidad de auditorías esporádicas que tengan el único propósito de satisfacer los requerimientos establecidos por las organizaciones usuarios.

En última instancia, las organizaciones usuarias son capaces de obtener una mayor comprensión y garantía de los controles internos existentes en las organizaciones de servicios. La certificación SAS 70 significa que las organizaciones de servicios han tomado medidas proactivas en el desarrollo e implementación de controles a lo largo de la plataforma utilizan para procesar las transacciones de las organizaciones usuarias. Además, los informes SAS 70 Tipo I y Tipo II ayudan a los auditores externos de las organizaciones de usuarias al reducir el tiempo y los costos de tener que informarse sobre los controles en las organizaciones de servicios.

La naturaleza única de las auditorías SAS 70 está en lo que está permitido incluir en su informe, los auditores han implementado una lista de políticas procedimientos y controles relacionados que deben ser examinados para este trabajo. Por lo tanto, lo que hace que este tipo de auditoría sea más exhaustiva o distinta a cualquier tipo de revisión de control interno es, sencillamente, su alcance y la gran cantidad de información que se incluye en el informe final del auditor. Mientras que los consultores de seguridad de IT se centran principalmente en los controles generales y de aplicación cuando realizan sus evaluaciones, los auditores de SAS ponen énfasis en estos aspectos, otros como recursos humanos y operativos, junto con las directrices de seguridad física y los planes de continuidad de negocio. Es decir, cuanto mayor sea el alcance, más significativo y útil será el documento. Esto es lo que hace que SAS 70 sea superior a cualquier otro procedimiento de revisión de control. Sólo un contador público certificado o empresa contable puede firmar y emitir un informe SAS 70 Tipo I o Tipo II.

Aunque hay muchos profesionales de TI que participan en el trabajo de auditoría SAS 70, no se encuentran autorizados para la emisión de esta clase de informes y por lo tanto, nunca deben ser considerados como una fuente primaria para la realización de este tipo de auditoría. Además, su escaso dominio de habilidades contables y de auditoría resulta en una desventaja al momento de entender los componentes principales de las auditorías de SAS 70. Sólo un contador con experiencia, tanto en auditoría de estados financieros como habilidades de TI, debe ser considerado como la fuente principal de los trabajos de SAS 70.

Un informe tipo I se emite para una fecha determinada. Por ejemplo, se realiza una revisión de los controles de procesamiento de transacciones de una organización para un punto específico en el tiempo.

Un informe de tipo II se emite después de que un periodo de prueba mínimo de seis meses se ha completado. Por ejemplo, se realiza un análisis de los controles que existen en la organización en periodo de tiempo específico. El informe se realiza sobre los controles aplicados y se realizan pruebas de su efectividad en ese periodo.

En concreto, a diferencia de un informe Tipo I, que consiste en emitir un diagnóstico sobre la revisión y observación de los controles, un tipo II incluye las pruebas de efectividad de dichos controles (Tabla 6).

Debido a la naturaleza especializada de las auditorías SAS 70, la organización completa no pasa a través de esta auditoría. En cambio, las plataformas que están siendo utilizadas para mantener actividades tercerizadas relacionadas con las organizaciones usuarias será lo auditado, junto con otras áreas consideradas por el auditor. Por ejemplo, si una organización de servicios lleva a cabo actividades relacionadas con el procesamiento de reclamos, todos los procedimientos y operaciones relacionadas con esa plataforma específica estarán bajo el alcance de la auditoría de SAS 70.

Tabla 6: SAS 70 – Lista de Contenidos de los informes SAS 70 Tipo I y Tipo II.

Información	Tipo I	Tipo II
Reporte de Auditoría SAS 70	Requerido	Requerido
Descripción de los Controles	Requerido	Requerido
Información proporcionada por el auditor: Lista detallada de los controles y pruebas de la eficacia operativa	Opcional	Requerido
Información proporcionada por la organización de servicios	Opcional	Opcional
Consideraciones de Control de la organización usuarios: Controles que las organizaciones usuarios tienen	Opcional	Opcional

Fuente: Nickelly Denye (2007)

En general, una auditoria SAS 70 analiza los controles que implementa una organización de servicios que implementa controles a lo largo de varios niveles dentro del negocio y no solamente la plataforma identificada como objetivo de la auditoría.

En enero de 2010, el American Institute of Certified Public Accountants (AICPA) y el Auditing Standards Board (ASB) emitieron el Statement on Standards for Attestation Engagements (SSAE) Nº16. El SSAE N°16 reemplaza al Statementon Auditing Standards N°70 (SAS 70), para organizaciones de servicio como la guía autorizada para la realización de auditorías en organizaciones de servicio. Este nuevo estándar fue publicado en abril 2010 y es efectivo a partir del 15 de junio de 2011.

SSAE 16[12] que incluye el SOC (Service Organization Control) se redactó con la intención y el propósito de actualizar la norma para los informes de auditoría para las organizaciones de servicio de los EE.UU. de tal manera que refleje y cumpla con la nueva norma internacional de informes de auditoría para organizaciones de servicio ISAE 3402.

ESTÁNDAR: AUDITING N° 5 (Doogar *et al.*, 2010)

En junio de 2007, el PCAOB emitió el Auditing Standard No. 5 (AS5) (PCAOB, 2004), que sustituye al Auditing Standard No. 2 (AS2). AS5 cambiado de manera significativa las normas relativas a las auditorías de control interno sobre los informes financieros.

El artículo 404 de la Ley Sarbanes-Oxley de 2002 (en adelante SOX 404) exige a las empresas que cotizan en bolsa incluir en los informes de gestión y del auditor la efectividad de su control interno en su Formulario 10-K presentados.

En relación con las auditorías de los estados financieros se establecieron en el Auditing Standard No. 2 (AS2), una auditoría del control interno sobre la información financiera realizado en conjunto con una auditoría de estados financieros, que entró en vigencia en noviembre de 2004.

En respuesta, el PCAOB emitió una nueva norma, el Auditing Standard N º 5 (AS5), una auditoría del control interno sobre la información financiera que se integra con una auditoría de estados financieros, efectivo para los años fiscales que terminan el 15 de noviembre 2007, destinados a abordar los problemas derivados de AS2 (PCAOB, 2007).

[12] *Statement on Standards for Attestation Engagements (SSAE) No. 16 including the Service Organization Control (SOC) reporting framework (SOC 1, 2, 3).-http://ssae16.com/ - American Institute of Certified Public Accountants (AICPA).*

La mayor parte de la discusión en torno a AS5 se ha centrado en el impacto esperado en la eficacia de la auditoría. AS5 prescribe una de arriba hacia abajo, basado en el riesgo de auditoría, que cree que el PCAOB se traducirá en importantes ahorros de costes pulgadas a través de todas las empresas. Además, AS5 pretende facilitar una mejor escalabilidad de las auditorías entre empresas de diferente tamaño y complejidad, permitiendo el ahorro de costes a ser relativamente mayor para las entidades más pequeñas y menos complejo (Krishnan, 2011).

El AS5 contempla diversas secciones tales como: *Introducción, planeamiento de la auditoría* (rol de determinar los riesgos, escala de auditoría, determinación de los riesgos por fraude, uso del trabajo de otras áreas y la materialidad), *método de la aproximación de arriba hacia abajo* (que considerada identificar los niveles de control, uso de los recursos, selección de los controles para el testeo de los mismos), *testeo de controles, evaluación e identificación de deficiencias, pre informe y finalmente la elaboración del reporte final.*

Asimismo, el AS5 estable el alcance de aplicación y determina los aspectos de control interno sobre el reporte financiero, aspectos claves en el manejo de los riesgos operativos. Un aspecto que se vuelve crítico es el proceso de identificación de la evidencia que, debe ser tan representativa que permita al auditor realizar conclusiones para toda la organización. Este proceso de identificación debe ser evidenciado en un plan o proceso de auditoría y revisión que considerada aspectos internos y externos (normas legales aplicables por ejemplo). Este plan podría contemplar realizar revisiones denominadas de "arriba – hacia abajo" o "Top-down" (en inglés), que permiten revisar la secuencia de auditoría e identificación de los riesgos en diferente orden y no en el orden en el que son encontrados.

CONCLUSIONES

El manejo del riesgo operacional y los mecanismos de control y mitigación son bastante extensos e importantes debido no solo a las crisis que han acontecido en los mercados financieros e internacionales desde 1997, pasando por el 2001 y la última del 2008, sino además, porque el crecimiento de un país está en función no solo a los recursos que tienen, el grado de inversión privada o gasto público en infraestructura, sino también, de la cultura y educación y conocimiento de los riesgos en las organizaciones y este aspecto el conocimiento de riesgo operativo se vuelve importante para la continuidad de los negocios. En esta línea el riesgo operacional se vuelve un elemento a gestionar constantemente.

Los riesgos operativos, en particular para las instituciones financieras, pueden ser más difícil de definir y gestionar que otros riesgos financieros tradicionales. El riesgo de crédito y riesgo de mercado por ejemplo se conocen bien, y se han construido modelos para entender y mitigar las pérdidas en estas áreas durante años.

El riesgo operativo u operacional puede incluir una amplia gama de amenazas internas o externas, como la perturbación a causa de desastres naturales, el fraude de los empleados, y las transacciones fallidas. Este último elemento - el riesgo transaccional - está ganando importancia de para los próximos años, principalmente debido a su naturaleza generalizada (por ejemplo en los mercados financieros over the counter).

Un óptimo funcionamiento de las gerencias de negocios, riesgos y operaciones incidirán en una adecuada gestión de los riesgos operacionales, gestión que puede integrarse con acciones de mejora y estabilidad en los ingresos de las firmas así como en la reducción de costos en ellas definiendo mejores perspectivas de estabilidad en el largo plazo.

Los auditores en general han tenido durante mucho tiempo para gestionar los riesgos como parte de sus funciones. Se espera que los auditores internos, en particular de los bancos y compañías de seguros, exigen más análisis de riesgos: de forma continua y en revisiones anuales formales. Los informes deberán ser independientes, a pesar de que exista reporte directo del auditor al gerente general de la empresa.

Los tipos de riesgos que enfrentan los auditores serán variados y van desde Sabanes-Oxley (relacionado con la tendencia de riesgo el cumplimiento de 2011 ya se ha señalado) a fraudes de los empleados en caso de incumplimiento de las TI, el AS5 y lo señalado en las normas o circulares de cada país. Nuevas regulaciones en el mercado americano tendrán un impacto en otros países y los diversos operadores. Un aspecto a considerar es entender el correcto uso de las herramientas de control y manejo de riesgo operacional, no solo quedando estas en papel, sino efectivizándose.

Además los eventos recientes tales como como la crisis financiera, la desaceleración de Gran Bretaña, el colapso de MF Global, y los problemas de la zona euro (Grecia, España, Portugal e Italia, entre otras islas) han provocado un renovado enfoque en la gestión de riesgos financieros entre los reguladores y ejecutivos de servicios financieros, siendo el aspecto operacional un factor que marcará la agenda global de los próximos años.

Se considera que el riesgo operacional es un lugar generado por la intersección de diversos factores, tales como fraudes, error al procesar, la discontinuidad de los negocios, gestión adecuada de recursos humanos, responsabilidad legal, así como preocupaciones sobre el riesgo de reputación y de gestión estratégica, siendo este último una línea importante de investigación futura.

La gestión del riesgo operacional contempla un adecuado control de la información que se procese, por lo que el manejo de bases de datos, resulta un aspecto importante a considerar.

Este documento permite abrir para los mercados emergentes, otras investigaciones y aplicadas al impacto de los riesgos operativos en:

• Implicancias en las finanzas a nivel general, es decir establecer mecanismos de control que aseguren la continuidad de las empresas. Así como la recuperación de inversiones en plazos pertinentes y no cortos.

• Desarrollo de los mercados derivados, supervisión y control de los mismos, alineado a su impacto en la economía de un país, considerando importaciones, exportaciones, inflación, etc. Las transacciones denominadas over the counter serán un aspecto a monitorear.

• Entre otras, áreas de estudio que presentan en la actualidad una creciente relevancia en los países emergentes, no solo por la mayor integración del sector financiero con el sector real en cada uno de estos, sino también porque en contextos de crecimiento económico, con mayores niveles de descentralización territorial y sectorial implican mayores demandas por financiamiento siendo el estadio inicial de estas ubicable en el segmento microfinanciero.

AGRADECIMIENTOS

E. Lizarzaburu, agradece a Omar Briceño Cruzado por los comentarios al documento, a la Superintendencia de Banca Seguros y AFP del Perú, a E&Y del Perú, GFI y Thomson Reuters.

REFERENCIAS

1. Alexander, C. (Ed.) (2003). Operational Risk: Regulation, Analysis and Management, Financial Times Prentice-Hall, New York, NY.

2. Basel Committee on Banking Supervision (1998). Operational Risk Management. Nº42, Basilea, Septiembre.

3. BIS 2006 - Basel Committee on Banking Supervision. (2006). Observed range of practice in key elements of Advanced Measurement Approaches (AMA). Basilea: Bank of International Settlements.

4. Banco Internacional de Pagos. (2005). El BIS y la búsqueda de la estabilidad financiera mundial. http://www.bis.org/about/global_financial_stability.htm (09 oct. 2007)

5. Basel III, Basel 2019 (2010). Black Book - Southern European Banks: Initiating Coverage & Introducing the Success Ratio, 165-169.

6. Basel Committee on Banking Supervision (2011). Revisions to the Basel II Market Risk Framework. Bank for International Settlements.

7. Brown, M., Jordan, J.S. & Rosengren, E. (2002). Quantification of operational risk. In*Federal Reserve Bank of Chicago Proceedings* (No. May, pp. 239-248).

8. Buchelt, R. & Unteregger, S. (2003). Cultural Risk and Risk Culture: Operational Risk after Basel II, Financial Stability Report 6, Oesterreichische National BanK.

9. Chapman, C. & Ward, S. (2003). Project risk management: processes, techniques and insights. Wiley & Sons.

10. Chernobai, A., Rachev, S. & Fabozzi, F. (2006). Operational Risk: A Guide to Basel II Capital Requirements, Models and Analysis. John Wiley & Sons, preprint.

11. Chernobai, A, Jorion, P. & Yu, F. (2011).The determinants of operational risk in U.S. financial institutions. *Journal of Financial and Quantitative Analysis*, *46* (6) 1683-1725.

12. Coleman, R. & Cruz, M. (1999). Operational Risk Measurement and Pricing. *Derivatives Week*, *8* (30) (26 July), 5f.

13. Cooke, D.L. (2004). The dynamics and control of operational risk. The University of Calgary, Alberta.

14. Cruz, M.G. (2002). Modelling, Measuring and Hedging Operational Risk, Wiley& Sons, Chichester, UK.

15. Dean, J.W. & Bowen, D.E. (1994). Management theory and total quality: Improving research and practice through theory development. *Academy of Management Review, 19* (3), 392-418.

16. de Fontnouvelle, P. (2005). The 2004 loss data collection exercise. Paper presented at the Implementing an AMA for Operational Risk Conference of the Federal Reserve Bank of Boston, May 19, available at: www.bos.frb.org/bankinfo/conevent/oprisk2005/defontnouvelle.pdf

17. Degen, M., Embrechts, P. & Lambrigger, D.D. (2006). The quantitative modeling of operational risk: between g-and-h and EVT, working paper, ETH Preprint, Zurich, December 19.

18. Doogar, R., Sivadasan, P. & Solomon, I. (2010). The Regulation of Public Company Auditing: Evidence from the Transition to AS5. *Journal of Accounting Research, 48* (4), 795-814. doi:10.1111/j.1475-679X.2010.00380.x

19. Folpmers, M. (2010). Decoding Basel III: Buffers, Benefits and Bonuses Breaking down Basel III's complex new capital and liquidity rules for banks, and exploring their short term and long term macroeconomic impact. *Risk Professional*, 30-34.

20. Frame, J.D. (2003). Managing risk in organizations: A guide for managers. Jossey-Bass, San Francisco.

21. Galloppo, G. & Rogora, A. (2011). What has worked in operational risk? *Global journal of Business Research*, *5* (3), 1-17.

22. Goenka, A. (2004). ERM in Financial service industry. Bajado en Diciembre de 2010 desde http://www.indiainfoline.com/bisc/ente.html

23. Grody, A.D., Harmantzis, F.C. & Kaple, G.J. (2005). Operational risk and reference data: exploring costs, capital requirements and risk mitigation, working paper, November, Stevens Institute of Technology, Hoboken, NJ.

24. Harris, J.M. (2010). The Macroeconomics of Development without Through put Growth. Tufts University Global Development and Environment Institute Working Paper 10-05.

25. Helbok, G. & Wagner, C. (2006). Determinants of operational risk reporting in the banking industry. *Journal of Risk, 9* (1), 49-74.

26. ISO / IEC, Comunidad, I. S. O. (2009). 25000, Calidad el producto de software y la norma ISO/IEC 25000, Comunidad ISO-25000.

27. Jobst, A.A. (2007). It's all in the data - consistent operational risk measurement and regulation. *Journal of Financial Regulation and Compliance*, *15* (4), 423-449.

28. Jorion, P. (2007). Value at Risk: The New Benchmark for Managing Financial Risk, McGraw-Hill, 3rd Edition.

29. Jorion, P. (2010). Risk Management. *Annual Review of Financial Economics 2*, 347-365.

30. Krishnan, J. (2011).The Effect of Auditing Standard No. 5 on Audit Fees. *Auditing, 30*(4), 1-27

31. McNeil, A.J., Frey, R. & Embrechts P. (2005). Quantitative Risk Management. Princeton University Press, Princeton.

32. Makarov, M. (2006). Extreme value theory and high quantile convergence. *Journal of Operational Risk, 1* (2), 51-57.

33. Masood, O. & Fry, J. (2012). Risk management and Basel-Accord-implementation in Pakistan. *Journal of Financial Regulation and Compliance*, 20 (3), 293-306.

34. Mignola, G. & Ugoccioni, R. (2006). Sources of uncertainty in modeling operational risk losses. *Journal of Operational Risk*, *1* (2), 33-50.

35. Neslehova, J., Embrechts, P. & Chavez-Demoulin, V. (2006). Infinite-mean models and the LDA for operational risk. *J. Operational Risk, 1* (1), 3-25.

36. Nickell, C. & Denyer, C. (2007). An Introduction to SAS 70 Audits. *Benefits Law Journal*, *20* (1), 58-68.

37. PCAOB, Public Company Accounting Oversight Board (2004). An Audit of Internal Control over Financial Reporting Performed in Conjunction with an Audit of Financial Statements. Auditing Standard No. 2 (AS2). Available at: http://pcaobus.org/Standards/Auditing/Pages/Auditing_ Standard_2.aspx

38. PCAOB, Public Company Accounting Oversight Board, (2007). An Audit of Internal Control Over Reporting That Is Integrated with Audit of Financial Statements and Related Independence Rule and Conforming Amendments. Auditing Standard No. 5 (AS5). Available at: http://pcaobus.org/Standards/Auditing/Pages/ Auditing_Standard_5.aspx

39. Price Waterhouse coopers. (2006). "Operational risk management Embedding operational risk management: The real use test". http://www.pwc.com/extweb/pwcpublications.nsf/ (11 mar 2008)

40. Raz, T. & Hillson, D. (2005). A comparative Review of Risk Management Standards. *Risk Management: An International Journal, 7*(4), 53-66.

41. Rodriguez, N. & Corbetta, C. (2007). La administración del Riesgo Operacional. Más allá del requerimiento regulatorio. Topics, *3* (3), 10-25.

42. Rutledge, W.L. (2004). Federal Reserve Bank of New York, Financial Operations Conference. Bajado en Enero de 2011, desde: ttp://www.ny.frb.org/newsevents/speeches/2004/rut040322.html

43. Servaes, H., Tamayo, A. & Tufano, P. (2009). The Theory and Practice of Corporate Risk Management. *Journal of Applied Corporate Finance, 21* (4), 60-78.

44. Shewhart, W.A. (1939). Statistical Method from the Viewpoint of Quality Control. Graduate School of the Department of Agriculture, Washington, D.C. (Republished in 1986 by Dover Publications, Inc., Mineola, NY.)

45. Sundmacher, M. (2007). Basic Indicator approach and the Standardized approach to Operational Risk: An Example-and Case Study-Based Analysis, National Australia Bank.

46. Taylor, F.W. (1911). The principles of scientific management. Reprint, 1967, Norton Company.

47. Wharton, F. (1992). Risk management: basic concepts and general principles, in Ansell, J. and Wharton, F. (Eds), Risk: Analysis, Assessment and Management, John Wiley & Sons Chichester.