PARTE II: RIESGO OPERATIVO –

Introducción

1. Conceptos básicos

    1.1. Definición de riesgo operativo
    1.2. Fuentes de riesgo operativo
    1.3. Clasificación de eventos de pérdida por riesgo operativo
    1.4. Gestión de riesgo operativo: Identificación, análisis, evaluación, tratamiento y monitoreo

2. Consideraciones previas a la implementación de Basilea II

    2.1. Alcance de la aplicación, disponibilidad de métodos y plazos de implementación
    2.2. Razones para el requerimiento de capital
    2.3. Métodos para el cálculo del requerimiento de capital y áreas de discreción nacional

3. Rol de los Supervisores en el Proceso de Implementación

    3.1. Adaptación de la estructura organizativa del supervisor
    3.2. Divulgación de la información sobre gestión del riesgo operativo
    3.3. Comunicación y coordinación transfronteriza
    3.4. Capacitación del personal

4. Situación actual de la regulación y supervisión del riesgo operativo, en algunos sistemas financieros de la región.

5. Referencias

Abreviaturas

Anexos

PARTE II: RIESGO OPERATIVO –

INTRODUCCIÓN

La presente sección, en muchos aspectos, describe las Sanas Prácticas para la Gestión y Supervisión del Riesgo operativo, las cuáles describen un conjunto de principios que proveen un marco para la gestión y supervisión efectiva del riesgo operativo, así como para el uso de bancos y autoridades de supervisión al evaluar las políticas y prácticas de gestión del riesgo operativo.

El documento reconoce que los países miembros de ASBA, desarrollarán e implementarán un marco de supervisión del riesgo operativo que depende de diversos factores, incluyendo el tamaño, la sofisticación y complejidad de los bancos que operan en sus respectivos países. Dicho esto, la implementación de guías que promuevan un enfoque más disciplinado a la gestión del riesgo operacional, se mantiene como un tema central entre los países contribuyentes, cuyas experiencias se resaltan como referentes principales, en este documento.

Los miembros del Grupo de Trabajo reconocen el menor desarrollo relativo que se observa en la regulación y supervisión del Riesgo Operativo en la Región. Sin embargo, destacan que los esfuerzos están encaminados a la adopción plena de sanas prácticas, en línea con las recomendaciones del Comité de Basilea. En un número importante de países de América Latina, se ha promovido, como paso previo, la adopción de sanas prácticas de gobierno corporativo y de control interno, demandando a los Directorios y Alta Gerencia de las entidades bancarias la adopción de políticas y procedimientos para una mejor gestión integral de riesgos.

Esta percepción no es ajena a la realidad de las propias instituciones bancarias a nivel global que consideran, de acuerdo con los resultados de la 4ta. Encuesta Bianual de Gestión de Riesgo Global 2004[1]. Los principales hallazgos de la encuesta indican que:

- "*un ambiente regulatorio más rígido y un mayor escrutinio sobre las instituciones financieras en el ambiente de negocios post-Enron ha contribuido significativamente a un mayor énfasis en la gestión de riesgo.*
- *el 81 por ciento de las instituciones de servicios financieros han establecido la posición de Gerente de Riesgos, 75 por ciento de los cuales reportan al Gerente Ejecutivo o al Directorio.*
- *se observa un 25 por ciento de incremento en la supervisión directa del Directorio sobre la gestión de riesgo en los últimos 2 años.*
- *la gestión de riesgo operativo (GRO) continúa siendo un campo relativamente Nuevo y en desarrollo, comparado con las disciplinas más establecidas de gestión de riesgo, con una mayoría de entidades todavía en las fases iniciales de implementación. Sin embargo, la encuesta muestra un incremento, respecto de 2002, en el número de entidades que han establecido programas de GRO.*
- *los resultados de la encuesta todavía permiten sostener la noción de que la GRO está siendo vista como un proceso y herramienta para mejorar el control interno.*
- *más del 95 por ciento de los encuestados consideran que sus sistemas actuales de GRO se quedan cortos en las capacidades requeridas.*
- *más del 70 por ciento considera que la razón fundamental para mejorar sus capacidades de GRO, es la respuesta a los requerimientos regulatorios, en especial el Nuevo Acuerdo de Capital de Basilea*."

Evolución del Riesgo Operativo y las Actividades Bancarias

La desregulación y globalización de los servicios financieros, junto con la creciente sofisticación de la tecnología financiera están haciendo las actividades bancarias, y en consecuencia, sus perfiles de riesgo,

[1] 162 instituciones financieras participaron en la encuesta de la firma Deloitte & Touche LLP, incluyendo a 28 en Norte América y 43 en Sudamérica.

cada vez más complejos. Adicionalmente a los riesgos de crédito, de tasa de interés y de mercado, el riesgo operacional puede ser sustantivo y las tendencias de pérdidas parecen indicar que se está incrementando. Como resultado, una sólida gestión del riesgo operativo es cada vez más importante para bancos y supervisores, con riesgos operativos emergiendo en un número de áreas críticas, tales como las siguientes:

- Mayor uso de tecnología automatizada (p.e. riesgos derivados de la automatización de procesos manuales, errores de procesamiento y riesgos de fallas en los sistemas);
- Proliferación de productos nuevos y altamente complejos;
- Crecimiento de transacciones bancarias electrónicas y aplicaciones de negocios relacionadas;
- Adquisiciones de gran escala, fusiones y consolidaciones;
- Aparición de bancos que actúan como proveedores de servicios a gran escala;
- Desarrollo y uso de técnicas de mitigación de riesgos (p.e. garantías, seguros, derivados de crédito, arreglos de neteo y titularizaciones); e,
- Integración global de servicios financieros (p.e. riesgos de transacciones de pago procesadas en múltiples monedas, crecientes transacciones comerciales, etc.).

El rango de prácticas de negocio y áreas afectadas por los riesgos operacionales debe ser ampliamente considerado y tratado en el desarrollo de la gestión del riesgo operativo de las entidades financieras. Debido a que no está confinado a líneas de negocio particulares, tipos de producto o unidades organizacionales y a que los riesgos pueden estar interrelacionadas, el riesgo operativo debería ser administrado de una manera integral y consistente en la entidad financiera. Consecuentemente, la gestión de estos riesgos debe incorporar el rango total de riesgos operativos, así como también las estrategias que ayuden a identificar, medir, monitorear y controlar estos riesgos.

Los conceptos y principios esbozados en este documento proveen una base para el establecimiento de un enfoque más disciplinado para la supervisión de la gestión del riesgo operativo, y en particular de su medición, teniendo en cuenta que el riesgo operativo no es nuevo. El documento está organizado en cuatro cuerpos: el primero se centra en repasar los conceptos y definiciones básicas del riesgo operativo, tal como lo plantea el Comité de Basilea, el segundo trata sobre algunos factores que las instituciones en ciertos países deberían considerar al momento de diseñar e implementar estrategias para la gestión y medición del riesgo operativo, el tercero se concentra en analizar las actividades que los supervisores de la Región vienen encarando en la preparación del proceso de implementación, incluyendo las adaptaciones realizadas en la estructura organizacional de algunas agencias de supervisión así como los requerimientos de información previstos, los esfuerzos de coordinación entre Supervisores y el énfasis que se debe poner en la capacitación permanente de sus cuadros técnicos. Finalmente, el cuarto describe de manera muy resumida la situación actual de la regulación y supervisión del riesgo operativo en la Región, la misma que se encuentra en un proceso dinámico de evolución.

1. Conceptos básicos

1.1. Definición de riesgo operativo

Se entiende por riesgo operativo a la posibilidad de ocurrencia de pérdidas financieras por deficiencias o fallas en los procesos internos, en la tecnología de información, en las personas o por ocurrencia de eventos externos adversos. Esta definición incluye el riesgo legal, pero excluye el riesgo estratégico y el de reputación.

1.2. Fuentes de riesgo operativo

Procesos Internos

Posibilidad de pérdidas financieras relacionadas con el diseño inapropiado de los procesos críticos, o con 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.

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

Personas

Posibilidad de pérdidas financieras asociadas con negligencia, error humano, sabotaje, fraude, robo, paralizaciones, apropiación de información sensible, lavado de dinero, inapropiadas relaciones interpersonales y ambiente laboral desfavorable, falta de especificaciones claras en los términos de contratación del personal, entre otros factores. Se puede también incluir pérdidas asociadas con insuficiencia de personal o personal con destrezas inadecuadas, entrenamiento y capacitación inadecuada y/o prácticas débiles de contratación.

Tecnología de Información

Posibilidad de pérdidas financieras derivadas del uso de inadecuados sistemas de información y tecnologías relacionadas, que pueden afectar el desarrollo de las operaciones y servicios que realiza la institución al atentar contra la confidencialidad, integridad, disponibilidad y oportunidad de la información.

Las instituciones pueden considerar de incluir en ésta área, los riesgos derivados a fallas en la seguridad y continuidad operativa de los sistemas TI, a errores en el desarrollo e implementación de dichos sistemas y su compatibilidad e integración, problemas de calidad de información, inadecuada inversión en tecnología y fallas para alinear la TI con los objetivos de negocio, con entre otros aspectos. Otros riesgos incluyen la falla o interrupción de los sistemas, la recuperación inadecuada de desastres y/o la continuidad de los planes de negocio.

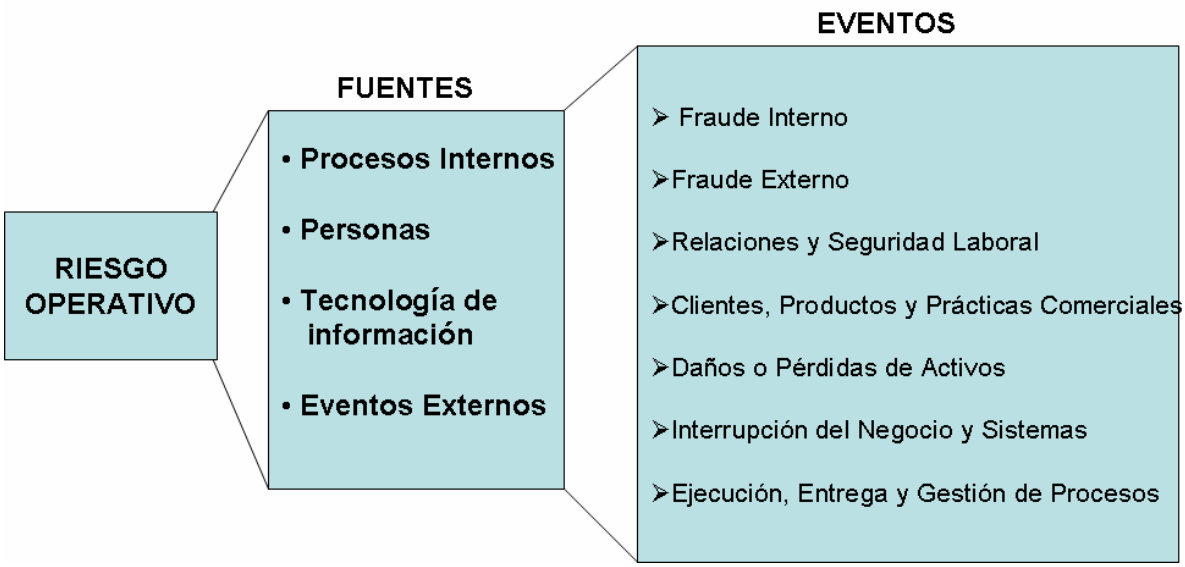
Eventos Externos

Posibilidad de pérdidas derivadas de la ocurrencia de eventos ajenos al control de la empresa que pueden alterar el desarrollo de sus actividades, afectando a los procesos internos, personas y tecnología de información. Entre otros factores, se podrán tomar en consideración los riesgos que implican las contingencias legales, las fallas en los servicios públicos, la ocurrencia de desastres naturales, atentados y actos delictivos, así como las fallas en servicios críticos provistos por terceros. Otros riesgos asociados con eventos externos incluyen: el rápido paso de cambio en las leyes, regulaciones o guías, así como el riesgo político o del país.

1.3. Categorización de eventos de pérdida por riesgo operativo

En coordinación con el sector financiero, el Comité de Basilea ha identificado los siguientes tipos de eventos que pueden resultar en pérdidas sustanciales por riesgo operativo[2]:

[2] Sanas Prácticas para la Gestión y supervisión del Riesgo Operativo – Comité de Basilea de Supervisión Bancaria – Publicación No. 96 Febrero de 2003



Fraude Interno

Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir regulaciones, leyes o políticas empresariales en las que se encuentra implicada, al menos, una parte interna a la empresa; no se consideran los eventos asociados con discriminación en el trabajo. Esta categoría incluye eventos como: fraudes, robos (con participación de personal de la empresa), sobornos, entre otros.

Fraude Externo

Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o soslayar la legislación, por parte un tercero. Esta categoría incluye eventos como: robos, falsificación, ataques informáticos, entre otros.

Relaciones laborales y seguridad en el puesto de trabajo

Pérdidas derivadas de actuaciones incompatibles con la legislación o acuerdos laborales, sobre higiene o seguridad en el trabajo, sobre el pago de reclamaciones por daños personales, o sobre casos relacionados con discriminación en el trabajo.

Clientes, productos y prácticas empresariales

Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación profesional frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto.

Daños a activos materiales

Pérdidas derivadas de daños o perjuicios a activos físicos como consecuencia de desastres naturales u otros eventos de fuentes externas.

Interrupción del negocio y fallos en los sistemas

Pérdidas derivadas de incidencias o interrupciones en el negocio y de fallas en los sistemas.

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. Esta categoría incluye eventos asociados con: captura de transacciones, ejecución y mantenimiento, monitoreo y reporte, entrada y documentación de clientes, gestión de cuentas de clientes, contrapartes de negocio, vendedores y proveedores.

1.4. Gestión del riesgo operativo: Identificación, Evaluación, Medición, Monitoreo y Control

Como principio general, las entidades financieras deben contar con una estrategia aprobada por el Directorio estableciendo principios para la identificación, medición, control, monitoreo y mitigación del riesgo operativo.

Las estrategias y políticas deberían ser implementadas por la Función de Gestión de Riesgo, responsable de identificar y gestionar todos los riesgos. La Función de Gestión de Riesgo puede incluir sub-unidades especializadas por riesgos específicos.

Las entidades financieras deberían desarrollar su propio enfoque y metodología para la gestión de riesgos, de acuerdo con su objeto social, tamaño, naturaleza y complejidad de operaciones y otras características. La implementación del sistema de gestión de riesgo operativo debería considerar todas las etapas de gestión de riesgo, incluyendo la identificación, evaluación, medición, monitoreo y control.

Identificación

La identificación efectiva del riesgo considera tanto los factores internos como externos que podrían afectar adversamente el logro de los objetivos institucionales.

Evaluación

Para todos los riesgos operativos materiales que han sido identificados, la entidad debería decidir si usa procedimientos apropiados de control y/o mitigación de los riesgos o asumirlos. Para aquellos riesgos que no pueden ser controlados, el banco debería decidir si los acepta, reduce el nivel de actividad del negocio expuesta o se retira de esta actividad completamente.

Todos los riesgos materiales deberían ser evaluados por probabilidad de ocurrencia e impacto a la medición de la vulnerabilidad de la entidad a este riesgo. Los riesgos pueden ser aceptados, mitigados o evitados de una manera consistente con la estrategia y el apetito al riesgo institucional. Cuando sea posible, la entidad debería usar controles internos apropiados u otras estrategias de mitigación, como los seguros.

Medición

Las entidades financieras deberían estimar el riesgo inherente en todas sus actividades, productos, áreas particulares o conjuntos de actividades o portafolios, usando técnicas cualitativas basadas en análisis expertos, técnicas cuantitativas que estiman el potencial de pérdidas operativas a un nivel de confianza dado o una combinación de ambos.

Monitoreo

Un proceso efectivo de monitoreo es esencial para una gestión adecuada del riesgo operativo. Un monitoreo regular de las actividades puede ofrecer la ventaja de detectar rápidamente y corregir deficiencias en las políticas, procesos y procedimientos de gestión del riesgo operativo. El monitoreo regular también fomenta la identificación temprana de cambios materiales en el perfil de riesgo, así como la aparición de nuevos riesgos. El alcance de las actividades de monitoreo incluye todos los aspectos de la gestión del riesgo operativo en un ciclo de vida

consistente con la naturaleza de sus riesgos y el volumen, tamaño y complejidad de las operaciones.

Control

Después de identificar y medir los riesgos a los que está expuesta, la entidad financiera debería concentrarse en la calidad de la estructura de control interno. El control del riesgo operativo puede ser conducido como una parte integral de las operaciones o a través de evaluaciones periódicas separadas, o ambos. Todas las deficiencias o desviaciones deben ser reportadas a la gerencia.

Reporte

Debe existir un reporte regular de la información pertinente a la alta gerencia, al directorio, al personal y a partes externas interesadas, como clientes, proveedores, reguladores y accionistas. El reporte puede incluir información interna y externa, así como información financiera y operativa.

2. Consideraciones previas a la implementación de Basilea II

2.1 Alcance de la aplicación, disponibilidad de métodos y plazos de implementación

Solo un grupo reducido de países en la Región han emitido instrucciones específicas a las instituciones supervisadas, requiriendo la implementación de sanas prácticas de gestión del riesgo operativo, incluyendo el alcance de la aplicación, métodos disponibles y plazos de implementación. A continuación se presenta una breve descripción de la experiencia práctica en Ecuador, Honduras, Perú y Estados Unidos.

Ecuador

En Octubre de 2005, la Superintendencia de Bancos del Ecuador emitió una resolución sobre gestión de riesgo operativo, aplicable a todas las instituciones financiera con la excepción de algunas ciertas cooperativas de ahorro y crédito pequeñas, ubicadas en lugares específicos. Debido a su tamaño, estructura y organización, no fue posible que estas cooperativas cumplan con los requerimientos dispuestos en la resolución.

La resolución establece que antes de determinar cargos de capital por riesgo operativo, las instituciones financieras deberían desarrollar un ambiente apropiado de gestión de riesgo operativo. Esto implica asegurar una gestión efectiva de los procesos institucionales, recursos humanos y tecnología de la información, estableciendo y validando planes de contingencia y de continuidad de negocio. Una vez que estos aspectos cualitativos sean alcanzados, las instituciones tendrían la capacidad para moverse hacia requerimientos cuantitativos de capital, como establece el Nuevo Acuerdo de Capital.

Se requirió a las instituciones supervisadas presentar su evaluación y un plan para poner en práctica las nuevas provisiones de gestión de riesgo operativo a la Superintendencia de Bancos y Seguros, dentro de seis meses después de la fecha de emisión de la resolución. El plan de puesta en práctica, aprobado por la junta directiva de la institución, debería incluir una lista (un programa) detallada de actividades y una lista de la gente responsable de su ejecución.

Para el caso de las cooperativas de ahorro y crédito el plazo para la presentación del diagnóstico y proyecto de implementación es de un año contado a partir de la fecha de emisión.

La implementación de las disposiciones previstas en la norma no debía exceder de los siguientes plazos:

a. Para grupos financieros con subsidiarias operando en otros países: hasta dos años y medio después de la fecha de presentación de su diagnóstico y plan de implementación;

b. Para grupos financieros que no cuenten con subsidiarias en el extranjero; para los bancos o sociedades financieras, las compañías de arrendamiento mercantil, las compañías emisoras y administradoras de tarjetas de crédito, las corporaciones de desarrollo de mercado secundario de hipotecas, las instituciones financieras públicas y el Fondo Solidario, hasta tres años de plazo a partir de la presentación de su diagnóstico y plan de implementación; y,

c. Para las cooperativas de ahorro y crédito que realizan intermediación con el público y las asociaciones mutualistas de ahorro y crédito para la vivienda, hasta cuatro años de plazo a partir de la presentación de su evaluación y plan de implementación.

Honduras

La Comisión Nacional Bancaria y de Seguros de Honduras ha conformado un comité para estudiar el alcance de la aplicación y los métodos disponibles para implementar Basilea II. Inicialmente, el Método del Indicador Básico está siendo considerado, sin embargo, algunos temas regionales deben ser antes resueltos.

Debe mencionar que el Consejo Centroamericano de Superintendentes de Bancos también ha creado un comité técnico para analizar temas de implementación de Basilea II.

Perú

La Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (SBS) ha conformado un Comité Especial para el estudio de la adecuación e implementación del Nuevo Acuerdo de Capital (NAC). El Comité cuenta con varios grupos de trabajo que evalúan aspectos específicos sobre el Nuevo Acuerdo.

Se está trabajando simultáneamente en todos los aspectos del Nuevo Acuerdo de Capital que deben ser considerados, a fin de asegurar consistencia una vez que se den pasos prácticos para la implementación efectiva del nuevo Marco.

Actualmente, se encuentra en revisión el proyecto de norma sobre el requerimiento patrimonial por riesgo de operación, el mismo que establece como métodos de cálculo, los siguientes:

- Método del indicador básico.
- Método estándar
- Método estándar alternativo
- Métodos de medición avanzados

Estados Unidos

Alcance de la aplicación

Las normas de capital en base a riesgo (Anuncio de Propuesta de Reglamentación (ANPR por sus siglas en inglés), emitido en Septiembre 25 de 2006, identifica tres grupos de bancos (1) bancos grandes o internacionalmente activos que estarían requeridos de adoptar los métodos avanzados de las normas propuestas (bancos básicos); (2) bancos que voluntariamente decidan adoptar los enfoques avanzados (bancos opcionalmente adentro); y, (3) bancos que no adoptarán los métodos avanzados (bancos generales). Cada banco básico y opcionalmente

adentro serían requeridos de alcanzar ciertos requerimientos de calificación mínimos a la satisfacción de su supervisor federal primario, en consulta con otros supervisores relevantes, antes que el banco haga uso de lo enfoques avanzados para propósitos de capital basado en riesgo.

Para poder identificar los bancos básicos, las Agencia propusieron los dos criterios umbral independientes siguientes: (1) activos comerciales totales del banco (o Mutual) de $250 billones o más, según reporte regulatorio de fin de año (con activos bancarios de grupos consolidados agregados a nivel de una compañía bancaria holding americana; o (2) Exposición dentro la hoja de balance de fin de año de $10 billones o más.

Todas las otras instituciones, identificadas como "bancos generales" permanecerían sujetos a Basilea I o la propuesta de enmienda de Basilea I para capital basado en riesgo. La propuesta para enmendar Basilea I (Anuncio de Propuesta de Reglamentación sobre Modificaciones al Marco de Capital Basado en Riesgo (Basilea 1A)) fue hecha pública para comentarios en Diciembre 26, 2006.

Métodos Disponibles

Bajo la ANPR, las Agencias sólo permitirán a las instituciones adoptar la metodología del Método de Medición Avanzado (AMA) para determinar su capital regulatorio por riesgo operativo bajo Basilea II. Sin embargo, las agencias reconocen que, en raras circunstancias, pueda no existir suficiente información disponible para un banco para generar un estimado creíble de su propia exposición al riesgo operativo. En estas raras circunstancias, un banco puede proponer el uso de un sistema de cuantificación de riesgo operativo alternativo que podría ser sujeto de aprobación por parte del supervisor Federal primario, del banco.

Cronograma

Las agencias están proponiendo para hacer al año 2008 el primer año posible para un banco para efectuar sus pruebas en paralelo y 2009 – 2011, como los primeros años posibles para los tres períodos de pisos de transición.

Periodo de Piso para la Transición	Porcentaje del Piso de Transición
Primer Período de Piso	95%
Segundo Período de Piso	90%
Tercer Período de Piso	85%

2.2 Razones para el requerimiento de capital por riesgos de operación

The members of the Working Group underline the importance of a capital requirement for operational risk to increase the soundness of banks and other financial institutions, and as an incentive for implementing a more effective operational risk management system.

Los Miembros del Grupo de Trabajo desean resaltar la importancia del requerimiento de capital por exposición a los riesgos de operación para incrementar la solidez de los bancos y demás empresas del sistema financiero, y a la vez, constituirá un incentivo para la implementación de una mejor gestión del riesgo operativo.

Efforts undertaken by financial institutions to implement improved operational risk management systems should be in line with the size and degree of complexity of their operations. As the larger and more complex financial institutions develop more sophisticated operational risk management systems, they will be authorized to use advanced methods for determining an adequate capital level.

Los esfuerzos de las instituciones financieras por implementar sistemas mejorados de gestión de riesgo operativo deben estar en línea con el tamaño y grado de complejidad de sus operaciones. Conforme los bancos y entidades financieras de mayor tamaño y sofisticación implementen mejores esquemas para la administración del riesgo operacional, podrán ser autorizados a utilizar métodos de cálculo avanzados, lo que les permita asignar un adecuado nivel de capital.

Los Miembros del Grupo de Trabajo no han discutido la validez y relevancia de los métodos propuestos por el Comité de Basilea con el propósito de revisar su utilidad una vez que las instituciones supervisadas hayan ganado experiencia práctica. Solo entonces, podrían proponerse métodos alternativos aplicables a la realidad de los países de la Región, de ser ello necesario.

2.3 Métodos de cálculo y áreas de discreción nacional

La mayoría de los países representados en el Grupo de Trabajo están estudiando la recomendación del Comité de Basilea, relacionada al establecimiento de un requerimiento de capital específico por riesgo operativo. Los Estados Unidos y Perú han determinado los métodos a ser usados para el cálculo de tales requerimientos.

Perú

En Perú se está revisando actualmente una regulación preliminar sobre requerimientos de capital por riesgo operativo. La norma propuesta presenta cuatro metodologías para determinar cargos de capital; el Método de Indicador Básico, el Método Estandarizado, el Método Estandarizado Alternativo y los Métodos de Medición Avanzada. Las instituciones financieras deberán contar con una autorización de la Superintendencia para usar cualquiera de estos métodos, excepto el Método del Indicador Básico.

Las empresas que estén autorizadas a aplicar el Método avanzado podrán reconocer el efecto mitigador de los seguros en el cálculo del requerimiento patrimonial por riesgos de operación, siempre que cumplan con ciertos requisitos asociados a la empresa de seguros y al contenido de la póliza. El reconocimiento del efecto de los seguros estará limitado al 20% del requerimiento patrimonial calculado con el Método avanzado.

Los requisitos mínimos para que las empresas puedan emplear los métodos estándar alternativo o avanzado, son los siguientes:

- La empresa deberá contar con un sistema de gestión de los riesgos de operación que cumpla con las disposiciones del Reglamento para la administración de los riesgos de operación

- En cuanto al método estándar alternativo, las empresas deberán desarrollar políticas específicas y documentar los criterios de asignación de los ingresos brutos a las líneas de negocio del modelo estándar. Las desviaciones con respecto a la asignación estándar de ingresos y gastos por líneas de negocio deberán ser sustentadas y documentadas. Los criterios deberán revisarse y ajustarse, en caso existan cambios en las líneas de negocio de la empresa o se incorporen nuevas actividades de negocio. Esto es aplicable para las líneas de negocio distintas a banca minorista y banca comercial.

  Asimismo, las empresas deberán recopilar sistemáticamente datos sobre los riesgos de operación que enfrentan, incluyendo pérdidas importantes por línea de negocio, e incorporar dicha información en el análisis y evaluación de los riesgos de operación y su reporte a la Alta Dirección. Además, deberán implantar técnicas que establezcan incentivos para la mejora de la gestión de los riesgos de operación, en toda la empresa.

Para que las empresas puedan emplear el método avanzado deberán cumplir con requisitos cualitativos y cuantitativos adicionales. Los principales requisitos cuantitativos se encuentran completamente alineados a lo indicado en el Nuevo Acuerdo, principalmente porque es necesaria la compatibilidad con la situación internacional, dado que bancos locales con matriz en el exterior han anticipado que se están preparando para el método avanzado.

En cuanto a los principales requisitos cualitativos, son los siguientes:

- El sistema de medición de los riesgos de operación de la empresa deberá estar integrado dentro de sus procesos habituales de gestión de riesgos. La información que se obtenga de dicho sistema deberá ser utilizada como parte integral del proceso de monitoreo y control del perfil de riesgos de operación
- Deberá existir un reporte periódico sobre las exposiciones a los riesgos de operación y la experiencia de pérdidas debidas a estos riesgos, dirigido a las gerencias de las unidades de negocio, a la Gerencia General y al Directorio.
- Como parte de la revisión requerida a la Unidad de Auditoria Interna y a la Sociedad de Auditoria Externa, debe incluirse una evaluación del sistema interno de medición de riesgos de operación.

Los principales requisitos cuantitativos son:

- La empresa debe ser capaz de demostrar que el método potencialmente captura los eventos de pérdida de cola severos.
- La empresa debe calcular su requerimiento de capital como la suma de la pérdida esperada (PE) y la pérdida inesperada (PI), a menos que pueda demostrar que está capturando adecuadamente la PE en sus prácticas de negocio internas.
- Las mediciones para estimaciones de riesgo operativo diferentes deben ser agregadas para efectos de calcular el requerimiento de capital regulatorio mínimo. Sin embargo, la empresa puede ser permitida de usar correlaciones determinadas internamente en pérdidas de riesgo operativo, una vez que puede demostrar la solidez de sus sistemas para determinar correlaciones.
- La empresa debe rastrear datos de pérdida internos e incorporar esta información como parte de su sistema interno de medición de riesgo operativo.
- Medidas de riesgo operativo generadas internamente usadas para propósitos de capital regulatorio deben estar basadas en un período de observación mínimo de cinco años de datos de pérdida internos.
- El sistema de medición de riesgo operativo de un banco debe usar datos externos relevantes (ya sean datos públicos y/o datos reunidos por la industria), especialmente cuando hay razón de creer que el banco está expuesto a pérdidas infrecuentes, pero potencialmente severas.
- Un banco debe usar el análisis de escenario de opinión experta en la conjunción con datos externos para evaluar su exposición a acontecimientos de alta severidad. Este acercamiento utiliza el conocimiento de directores comerciales experimentados y los expertos de gestión de riesgo para derivarse evaluaciones razonadas de pérdidas severas plausibles.
- La metodología de evaluación de riesgo, de toda la firma, de un banco debe capturar el ambiente de negocios clave y los factores de control interno que pueden cambiar su perfil de riesgo operativo.

Las áreas sujetas a la discreción de supervisores nacionales han sido identificadas y están actualmente en revisión, para definir la posición final de la Superintendencia. La decisión sobre áreas de discreción nacional deberá ser consistente con la adoptada para riesgos de crédito.

Comentarios adicionales

Los lineamientos emitidos por la SBS han permitido que la gestión de este riesgo haya sido iniciada por los bancos locales en una etapa relativamente temprana, debiendo destacarse que estas mismas normas son vigentes para el sistema bancario, microfinanciero y asegurador, dado que los riesgos de operación se encuentran en todos los sistemas supervisados.

El departamento de riesgos operativos se encuentra representado en los grupos de trabajo del comité especial de Adecuación a Basilea 2 creado en la SBS, y participa en el diseño regulatorio y en la definición del esquema futuro de supervisión, donde coordina también con las áreas de riesgos de crédito y de mercado, liquidez e inversiones.

En ese sentido, la SBS considera que las empresas se encuentran sustancialmente compatibles con los criterios de gestión cualitativos previstos en las recomendaciones internacionales, y cuenta con estructuras y responsabilidades definidas. Debido a la existencia de un plan contable bancario único, los cálculos que se requerirían para la eventual aplicación de los métodos estandarizado alternativo y básico se realizan sobre base rutinaria como parte del monitoreo de los impactos asociados a la aplicación del nuevo acuerdo, y no se estima ninguna dificultad importante en la adecuación hacia el método estándar alternativo. No obstante, las actividades dedicadas hacia la medición cuantitativa en el marco del método avanzado se encuentran aún en sus fases iniciales, mayormente en empresas con matriz fuera del país.

La supervisión y el acompañamiento de los proyectos de adecuación al método avanzado, requerirá del reforzamiento de las habilidades matemáticas y estadísticas del personal encargado de la validación de los modelos avanzados.

Estados Unidos

Las Agencias estadounidenses han propuesto que las instituciones sólo sean capaces de adoptar el Método de Medición Avanzada (AMA) para determinar capital regulatorio por riesgo operativo bajo Basilea II. La ANPR de septiembre de 2006 establece las exigencias de calificación para bancos que usan un Sistema AMA para calcular el componente de riesgo operativo del requerimiento de capital basado en riesgo del banco. Además, las Agencias propusieron lineamientos de supervisión preliminares en agosto de 2003 cubriendo varios aspectos del marco AMA de una institución, incluyendo: gestión del riesgo operativo, datos y evaluación, cuantificación del riesgo operativo, manejo de datos y mantenimiento, verificación y validación. Las normas identificadas en los lineamientos proporcionan una hoja de ruta que un banco debería seguir para poner en práctica y mantener un sistema AMA. Las normas establecen amplias directrices regulatorias, proporcionando a cada banco la capacidad de adaptar el marco, de una manera única, a su estructura de organización y cultura.

Las Agencias propusieron que el requerimiento de capital AMA estuviera basado en una medida de "exposición al riesgo operativo" (ERO) generada por el "sistema de medición de riesgo operativo" interno de una organización bancaria. Al calcular la ERO, una institución calificada como AMA estimaría su pérdida agregada de riesgo operativo que afronta durante un período de un año, como una norma sólida compatible con un nivel de confianza del 99.9 por ciento.

Bajo la propuesta, la institución tendría que usar una combinación de datos de eventos de pérdida internos, datos relevantes de eventos de pérdida externos, el ambiente de negocio y factores de control interno y análisis de escenario en la determinación de su "distribución de pérdida total " y el cálculo de su "exposición a riesgo operativo". Las Agencias propusieron que se pueda permitir a las instituciones, reconocer el efecto de dependencia de riesgo (por ejemplo, la correlación) y, a un grado limitado, el efecto de mitigantes de riesgo, tales como las pólizas de seguro.

La "exposición a riesgo operativo" sería convertida a una cantidad equivalente de "activos ponderados por riesgo" para el cálculo de los ratios de capital basado en riesgo, de una institución. Una institución calificada AMA multiplicaría la ERO generada por su marco analítico, por un factor de 12.5 para convertir la exposición a un "activo ponderado de riesgo" equivalente. La cantidad resultante sería añadida a las cifras correspondientes para riesgo de crédito y riesgo de mercado en el cálculo del denominador de capital basado en riesgo total.

Las definiciones precedentes describen, en realidad, un “marco analítico de riesgo operativo” (o sistema de medición) que combina cuatro “elementos”:

i) datos internos sobre eventos de pérdidas operativas;
ii) datos externos relevantes sobre eventos de pérdidas operativas;
iii) análisis de escenario; y
iv) ambiente de negocio y factores de control interno.

Para operar un sistema de medición, la institución debe reunir cuatro tipos de datos para asegurar lo siguiente:

i) Con respecto a los datos internos de pérdidas operativas:
a) reunir datos internos sobre pérdidas operativas de al menos cinco años, capturados a lo largo de todas las líneas de negocio relevantes, eventos, tipos de producto y regiones geográficas;
b) para cada número de pérdida, reunir también la fecha, cualquier recuperación posterior, así como la información causal relevante;
c) fijar umbrales realistas encima los cuales todas las pérdidas operativas internas serían capturadas;
d) construir un sistema para trazar un mapa de variables de pérdida de la base de datos de uno a siete tipos de eventos, especificados en Basilea II;
d) el reconocimiento que, en general, cualquier pérdida con atributos de riesgo de crédito debería ser atribuida al riesgo de crédito y no parcialmente ser atribuido al riesgo operacional, incluso si se hubiera implicado fraude.

ii) Con respecto a los datos externos de pérdidas operativas:
Establecer y adherirse a políticas y procedimientos que aseguren el empleo de datos externos relevantes de pérdidas en el marco de riesgo operativo (particularmente relevante donde la historia de pérdidas interna de una institución no es suficiente para generar una estimación de grandes pérdidas inesperadas).

iii) Con respecto a los datos de escenarios:
Desarrollar un proceso para incorporar escenarios en el modelo (el análisis de escenarios es un proceso sistemático para obtener opiniones expertas de directores comerciales y expertos de gestión de riesgo para derivar evaluaciones razonables de la probabilidad y el impacto de pérdidas operacionales plausibles).

iv) En lo que concierne a datos del factor de control interno del ambiente de negocio:
Desarrollar un método para incorporar las evaluaciones del ambiente de negocio y factores de control internos (por ejemplo, registros de auditoria, evaluaciones de riesgo y de control, indicadores de riesgo, etc.) en su evaluación de capital AMA.

Empleando los datos reunidos, la institución debe desarrollar un modelo cuantitativo que calcule la exposición de riesgo operativo (ERO), la pérdida operativa esperada (POE) y la pérdida operativa inesperada (POI) correspondientes al riesgo operativo.

El Nuevo Acuerdo de Capital de 2004 proporciona una gama de opciones para determinar las exigencias de capital para riesgo de crédito y riesgo operativo, para permitir a instituciones y

supervisores seleccionar los métodos más apropiados para sus operaciones y la infraestructura del mercado financiero. Las diferencias discrecionales más significativas entre el Nuevo Acuerdo y la propuesta de implementación estadounidense incluyen lo siguiente.

- Un régimen de capital bifurcado. Las Agencias han determinado que sólo las instituciones (principales) más grandes y las instituciones opcionales tienen que poner en práctica el método AMA.
- Como fuera propuesto bajo el ANPR, se permitirá a las instituciones principales y opcionales usar sólo métodos avanzados tanto para riesgo de crédito (A-IRB) como para riesgo operativo (AMA). Así, los métodos de indicador básico y estandarizado no estarán disponibles para las instituciones para el cálculo de su exposición de capital por riesgo operativo.
- Con la aprobación del supervisor, un período de observación más corto que cinco años para datos internos de observaciones de pérdidas, puede ser aceptable para las instituciones de reciente autorización para usar una metodología AMA.
- Los supervisores permitirán a una institución para manejar internamente sus variables de datos de riesgo operativo, mientras pueda trazar un mapa de estas variables a una de las siete categorías estándar de eventos de pérdida prescritas.

3 El Rol de los Supervisores en el Proceso de Implementación

Los Miembros del Grupo de Trabajo han analizado cuáles deberían ser las tareas primordiales que deben enfrentar los supervisores en esta etapa del proceso de implementación y cómo se va a conducir la supervisión de la gestión de riesgo operativo en las entidades financieras.

Las siguientes recomendaciones han sido efectuadas en base a dicho análisis:

- Los supervisores bancarios deben requerir que todos los bancos y entidades financieras cuenten con un sistema efectivo capaz de identificar, evaluar, monitorear, controlar y mitigar los riesgos operativos en todas sus líneas de negocio.

- La Gestión del Riesgo Operativo no debe estar desligada de la gestión de los otros riesgos inherentes a la actividad de intermediación financiera, por el contrario, debe ser parte de un enfoque integral de gestión de riesgos.

- Los supervisores deben evaluar de manera permanente, mediante actividades in-situ y extra-situ, que los bancos cuentan con estrategias, políticas, procedimientos y sanas prácticas escritas y debidamente aprobadas por su Directorio, para gestionar adecuadamente el riesgo Operativo, al que están expuestos.

- Los Supervisores deben asegurarse que las estrategias, políticas y procedimientos de gestión del riesgo operativo consideran el tamaño, complejidad y perfiles de riesgo de las entidades supervisadas.

- Los supervisores deben requerir a los bancos la generación de reportes que permitan tanto al Directorio y Gerencia, así como a los propios supervisores, efectuar el seguimiento y acompañar la implementación y aplicación de las estrategias, políticas y procedimientos.

- Los supervisores deben promover que los bancos divulguen información suficiente que permita a los participantes del mercado entender y evaluar su exposición al riesgo operativo, la calidad de su Gestión y las medidas adoptadas para mitigarlo.

- Los Bancos y entidades financieras deben registrar y acumular información histórica en función de las fuentes de riesgo y los tipos de eventos con el objeto de identificar:

- los riesgos por Unidad de Negocio
- las estimaciones de Pérdidas Esperadas
- las estimaciones de Pérdidas Inesperadas
- la frecuencia de los eventos de pérdida
- la severidad de los eventos de pérdida
- la tendencia de los eventos de pérdida.

- Los datos sobre la experiencia histórica de pérdidas del banco, proporcionarán información importante para evaluar la exposición a Riesgo Operativo del banco", necesaria para el cálculo de los requerimientos de capital.

- Es necesario que los supervisores provean orientación sobre como deben diseñarse los registros para la recolección de datos[3].

Los Miembros del Grupo de trabajo reconocen que muchos de estas recomendaciones son un reflejo de los principios del Comité de Basilea, sobre los que algunos países han venido adoptando posiciones más concretas.

3.1 Adaptación de la estructura organizativa del supervisor

Por la experiencia exitosa en países de la región, los Miembros del Grupo de trabajo consideran que a objeto de asignar los recursos necesarios para una gestión efectiva del riesgo operativo, las Autoridades de Supervisión deberían contar con una Unidad especializada de Riesgo Operativo, llámese Departamento/Dirección/Intendencia, en el Organigrama de la entidad supervisora.

Algunos ejemplos de cambios en las estructuras organizativas de los Organismos de Supervisión son:

Chile

Existe la Unidad de Riesgo Operativo y Tecnológico encargada de supervisar en terreno el cumplimiento de la normativa emitida por la Superintendencia, dándole especial énfasis a la incorporación por parte de las instituciones bancarias de los pilares del riesgo operacional y las buenas prácticas, especialmente en seguridad de la información, continuidad del negocio, calidad de servicio, administración de proveedores (outsourcing), gestión operacional y tecnológica y participación de auditoria interna en la evaluación de estos temas. Además existe en la Dirección de Estudios de esta Superintendencia, una unidad encargada de la Hoja de Ruta y específicamente en el riesgo operacional de centralizar el cálculo de requerimiento de capital efectuado por las entidades financieras en base al enfoque estándar alternativo.

Ecuador

Con miras a fortalecer y dar continuidad al nuevo modelo de supervisión enfocado a riesgos implementado a partir del año 2001, la Superintendencia de Bancos y Seguros introdujo un nuevo modelo de gestión por procesos, apoyado en una estructura matricial, que permite consolidar una nueva cultura organizacional encaminada hacia una supervisión con enfoque a riesgo.

---

[3] Un ejemplo de dicha orientación se presenta en el Anexo No. 1, provisto a las entidades financieras por la Superintendencia del Ecuador.

Considerando que una adecuada supervisión de los riesgos a los que se encuentran expuestas las instituciones que conforman el sistema financiero ecuatoriano supone la adecuación de la estructura organizativa del órgano de control para fomentar su mejora continua en la capacidad para evaluar riesgos, se creó la Dirección Nacional de Riesgos, que tiene entre otras funciones, la responsabilidad de generar políticas de supervisión bajo un enfoque basado en riesgos.

Adicionalmente, para la realización de sus actividades, la Dirección Nacional de Riesgos tiene la siguiente estructura:

- Subdirección de Riesgos Financieros
- Subdirección de Riesgos Operativos
- Subdirección de Riesgos Legales

Los procesos de la Dirección Nacional de Riesgos son la "Evaluación del Riesgo Financiero, Operativo y Legal de los sistemas: Financiero, de Seguro Privado y de Seguridad Social".

La Subdirección de Riesgos Operativos tiene entre sus funciones, la elaboración de metodologías para evaluación de riesgos operativos; elaboración de proyectos de norma; y, participación en los procesos de supervisión de los riesgos de operación en coordinación con las áreas encargadas de la supervisión.

Perú

La SBS cuenta con un Departamento especializado en temas de gestión de riesgo operativo, desde el año 2000, encargado del diseño de la regulación y de la supervisión extra-situ e in-situ de este riesgo, en coordinación con las áreas de supervisión integral.

El departamento forma parte de la Superintendencia Adjunta de Riesgos (SAR), que a su vez cuenta con los Departamentos de Evaluación de Riesgos de Mercado y Liquidez, de Riesgos de Crédito, y de Riesgos de Supervisión. La SAR trabaja en un esquema matricial con todas las unidades de supervisión directa de los sectores: bancario, microfinanciero, de seguros y de fondos privados de pensiones.

Estados Unidos

Bajo el actual marco regulatorio de capital, las instituciones no calculan un cargo explícito de capital por riesgo operativo, tal como lo harán bajo Basilea II.

Tanto las instituciones como los supervisores vienen enfrentando grandes desafíos para alcanzar la fecha efectiva propuesta para la implementación de Basilea II, Enero de 2009. Para asistir en la implementación de la norma propuesta de capital basado en riesgo, las Agencias emitieron un Lineamiento de Supervisión en Agosto de 2003, el cual provee una Hoja de Ruta que los bancos deberían seguir para implementar y mantener un sistemas AMA. Las Agencias también han dedicado sus equipos de inspección y expertos en la materia como responsables de la supervisión permanente en las instituciones afectadas. Estos supervisores están activamente envueltos en la revisión de planes preliminares y modelos recientemente adoptados.

Como parte de las normas propuestas de capital basado en riesgo, las Agencias han diseñado un proceso de calificación que requiere a las instituciones el desarrollo de un Plan de Implementación y un cronograma propuesto para la adopción de los métodos avanzados. El Plan debe ser sometido al supervisor Federal primario de cada institución con al menos 18 meses de antelación a una fecha esperada de adopción. Adicionalmente, el Plan debe ser amplio tomando en cuenta los requerimientos de implementación para todas las entidades

legales relevantes de la institución, tanto doméstica como extranjera, toda vez que el Plan debe ser adoptado a lo largo y ancho de todas las líneas de negocio y regiones geográficas.

El Plan debe estar aprobado por el directorio de la institución. Además, el Directorio y la Alta Gerencia deben comprender totalmente el perfil de riesgo diseñado en el plan institucional y establecer planes para asegurar que el perfil es alcanzado.

Cada institución debe desarrollar un Plan de Implementación detallado. El Plan debe incluir:

- Una auto-evaluación de la situación actual de la institución
- Un análisis de brechas, describiendo las áreas en las cuales la institución necesita trabajo adicional
- Planes de remedio
- Metas objetivas y fechas de cumplimiento
- Demostración de los recursos asignados y su adecuación
- Evidencia de la aprobación por el Directorio
- Un cronograma de discusión regular del Plan y su implementación con la Agencia de supervisión.

El supervisor Federal primario de la institución examinará las metodologías y resultados contemplados en el Plan como una parte normal del proceso de supervisión, confiando en expertos cuantitativos cuando sea necesario y otorgando o denegando la aprobación de los varios elementos.

Después de la evaluación del Plan por el Supervisor Federal primario, la institución debe todavía ejecutar el Plan satisfactoriamente, a objeto de obtener una calificación total. Las Agencias están considerando requerir a las instituciones efectuar Corridas Paralelas de sus sistemas AMA en una manera aceptable al Supervisor Federal primario durante al menos un año antes de usar sus sistemas para la determinación de los requerimientos de capital regulatorio mínimo. Las instituciones deben reportar sus resultados trimestralmente a la Agencia de Supervisión. Los requerimientos de capital durante el período de Corrida Paralela serán derivados de las normas de Basilea I y su enmienda de Riesgo de Mercado. La Corrida Paralela permitirá a la Agencia de Supervisión observar la actual corrida de los modelos y examinar las disparidades entre el capital requerido bajo el viejo y el nuevo sistema.

The Parallel Run will allow the supervising Agency to observe the actual running of the models and examine disparities between capital required under the old and new systems. En última instancia, la revisión del supervisor de la Corrida Paralela proporcionaría la base para las decisiones de calificación del supervisor Federal primario.

3.2 Requerimientos de divulgación de la información sobre gestión del riesgo operativo.

Si bien a la fecha de elaboración del presente reporte, no se ha identificado ejemplos concretos de cómo el Supervisor está encarando el tema de transparencia en la gestión y supervisión del riesgo operativo, los Miembros del Grupo de Trabajo recomiendan que los esfuerzos en esta materia estén orientados por los siguientes principios:

- Que las entidades financieras, en las publicaciones que efectúan sobre su situación financiera, incluyan en un apartado especial, la descripción resumida de sus políticas y procedimientos para gestionar el riesgo operativo, así como los enfoques empleados por la Gerencia y el Directorio para cuantificarlo y las medidas adoptadas para mitigarlo.

- Que los supervisores incluyan en sus manuales y procedimientos formales de supervisión “in-situ” y “extra-situ” la descripción de tareas de supervisión del riesgo operativo.
- Que los supervisores incluyan reportes escritos periódicos sobre los avances que vienen observando en la aplicación de sanas prácticas de gestión de riesgo operativo en las entidades bajo su control, identificando las fortalezas y las debilidades. Dichos reportes deberían incluirse en la Memorias Anuales y publicarse en las páginas web de los organismos de supervisión.

Para fortalecer el nivel de transparencia del supervisor, es necesario contar con un marco legal apropiado que no solo respalde las iniciativas de brindar información al público, sino también que las promueva.

En este sentido, a manera de ejemplo se cita las disposiciones generales de la LSF de Guatemala, que establece entre las funciones de la SB, publicar información suficiente, veraz y oportuna sobre la situación financiera de las entidades sujetas a su vigilancia e inspección, en forma individual o consolidada.

En el Perú, el Reglamento emitido por la SBS no señala requerimientos de divulgación de información sobre gestión del riesgo operativo; sin embargo, algunas empresas del sistema financiero, por propia iniciativa, publican en sus Memorias Anuales, las acciones que han desarrollado para administrar sus riesgos de operación, así como en otras acciones de difusión. Asimismo, como parte del proceso de implementación del NAC, se viene considerando este tema, a fin de incrementar el nivel de transparencia del supervisor, en cuanto a las metodologías y criterios utilizados para evaluar a las empresas del sistema financiero.

En Chile, en la Hoja de Ruta (Punto C-2) se señala la información que los bancos deben publicar y su frecuencia. En el caso del riesgo operativo se señala que se deben publicar riesgos y requisitos de capital al menos tres veces al año.

En los Estados Unidos, la sección VII del ANPR de septiembre de 2006 sobre las normas de capital basado en el riesgo: Marco Avanzado de Adecuación de Capital y Riesgo de Mercado, describe el grado de divulgación al público en materia de riesgos de crédito, mercado y operativo que deberán observar las instituciones y los supervisores. En particular, las Agencias señalan que “los requerimientos de revelación pública proveen importante información a los participantes del mercado sobre la estructura de capital, exposición al riesgo, procesos de evaluación de riesgos y, por tanto, la adecuación de capital del banco.”

Los requisitos de divulgación serían de aplicación solo a la institución depositaria o la sociedad bancaria de inversión, que representa el máximo nivel de consolidación del grupo bancario, sujeto a los métodos avanzados. Adicionalmente, las normas propuestas establecen requerimientos de revelación para instituciones subsidiarias de depósito dentro del grupo bancario a través de lo procesos de reporte regulatorios.

Como medida preliminar, las Agencias proponen que la divulgación se realice en los informes financieros trimestrales. Sin embargo, revelaciones cualitativas que proporcionan un resumen general de los objetivos, políticas, sistemas de reporte y definiciones de la gestión de riesgos del banco, podría publicarse anualmente, siempre que se publique cualquier cambio significativo entre los informes anuales. La revelación debe estar disponible en informes financieros públicos (como los informes 10-Q y 10-K presentados al SEC).

Las divulgaciones clave bajo el marco de riesgo operativo deberían incluir:

- Los requerimientos generales de revelación cualitativa para riesgo operativo.

- La descripción del AMA, incluyendo una explicación de los factores internos y externos relevantes considerados en el método de medición de la organización.
- Una descripción del uso de los seguros para el propósito de mitigar el riesgo operativo.

3.3 Comunicación y coordinación transfronteriza.

Para una exitosa implementación de la gestión de riesgos operativos en las entidades bancarias de mayor tamaño y que son parte de un grupo o conglomerado financiero cuyas actividades se realizan en diversas jurisdicciones, los Miembros del Grupo de Trabajo consideran fundamental la fluida comunicación entre supervisores. Asimismo, es necesaria una amplia coordinación de esfuerzos entre supervisores en la supervisión consolidada continua de las entidades que conforman un conglomerado.

Algunas iniciativas de coordinación entre Supervisores de la Región, como por ejemplo, el Acuerdo AC-02-1998 del Consejo Centroamericano de Superintendentes de Bancos, de Seguros y de Otras Instituciones Financieras, que estableció un esquema de cooperación multilateral entre los países miembros, con el propósito de lograr una adecuada y eficaz supervisión de los sistemas financieros sujetos a su control, especialmente lo relativo a grupos financieros, el cual incluye el intercambio de información significativa en su poder relacionada con las entidades matrices, sus agencias, sucursales y filiales y particularmente de los grupos financieros de los que forman parte. Cabe mencionar que este esquema está sujeto a lo que dispongan las leyes internas de cada país miembro.

Así también, para efectos de supervisión consolidada, muchos organismos supervisores de la Región han suscrito Memorandos de Entendimientos (MOU). Es el caso de la SB de Guatemala, que ha suscrito 14 MOU, entre memorandos de entendimiento, acuerdos y cartas de cooperación con otras entidades supervisoras extranjeras, con los cuales persigue, entre otros aspectos, lo siguiente: i) facilitar la supervisión consolidada, bajo los principios de reciprocidad, pertinencia, trato nacional y confidencialidad; ii) el intercambio de información sobre el sistema de regulación y procedimientos de supervisión aplicables en las respectivas jurisdicciones, tanto a entidades bancarias nacionales como extranjeras; iii) el suministro de información relevante a la otra parte con relación a progresos materiales o cuestiones de supervisión con respecto a las operaciones de un establecimiento transfronterizo; iv) informar sobre sanciones impuestas o sobre cualquier otra medida correctiva adoptada con respecto al establecimiento transfronterizo; y, v) facilitar la transmisión de información que pueda ser requerida para apoyar al proceso de supervisión.

Los MOU también incluyen el compromiso de los supervisores para conceder asistencia técnica recíproca en la ejecución de inspecciones in-situ de los establecimientos transfronterizos en la jurisdicción anfitriona por funcionarios del supervisor de origen. Por otro lado, también incluye las condiciones de cooperación en la prevención del blanqueo de capitales (lavado de activos).

3.4 Capacitación al personal.

La capacitación permanente del personal involucrado en la supervisión del Riesgo Operativo debe ser prioridad, tanto en las entidades financieras, como en los Organismos de Supervisión.

En los últimos años, la supervisión basada en riesgos ha sido una constante en las iniciativas de capacitación a nivel regional. En algunos casos, los supervisores brindan capacitación a las entidades controladas, en especial, a aquellas entidades no bancarias, menos sofisticadas y de menor tamaño. Esta última práctica ayuda a difundir sanas prácticas de gestión de riesgos y

debería ser apoyada por los organismos de supervisión, en la medida en que la propia utilización óptima de sus recursos lo permita.

Bolivia

En el marco de los lineamientos institucionales de la Superintendencia, de reorientación a principios de supervisión basada en riesgos, se cuenta con programas de capacitación permanente de los supervisores.

Chile

La capacitación es focalizada en algunas personas, y se realiza localmente.

Ecuador

La Dirección Nacional de Riesgos ha realizado eventos de capacitación en coordinación con las diferentes áreas encargadas de la supervisión dentro de la institución. La temática ha estado concentrada en la difusión de bases conceptuales, mejores prácticas internacionales, disposiciones normativas y cuestionarios para la supervisión de la administración de riesgos llevada a cabo por las entidades controladas. De la misma manera, se han realizado eventos de capacitación, en la modalidad de talleres prácticos y exposiciones a la administración y a los responsables de las áreas de riesgo de algunas entidades financieras, fundamentalmente de cooperativas.

Guatemala

En cuanto a la capacitación sobre tópicos relacionados al tema de Basilea II, se ha facilitado la participación de personal en diversas actividades de capacitación especializada y orientada a la Supervisión de Riesgos.

Honduras

Existe un grupo de estudio del tema de Basilea II que han estado dando charlas y capacitación al personal sobre el mismo.

Perú

Se viene capacitando al personal de la Superintendencia en los temas del NAC, según los niveles requeridos. Un primer nivel, dirigido a la mayoría de los funcionarios a cargo de labores de supervisión, consiste en difundir los alcances, contenido y consecuencias del NAC. Un segundo nivel, dirigido a grupos de trabajo específicos, consiste en profundizar aspectos puntuales del NAC, a fin de realizar estudios cuantitativos, desarrollar regulación y evaluar su impacto en la supervisión bancaria.

4 Estado actual de la regulación y supervisión del Riesgo Operativo en algunos sistemas financieros de la Región

En línea con su mandato, el Grupo de Trabajo ha revisado el estado actual de implementación en la Región, de sanas prácticas de gestión de riesgo operativo. A continuación, se presenta la información proporcionada por 10 países:

Bolivia

La Superintendencia de Bancos y Entidades Financieras (SBEF) no ha emitido normas específicas para el riesgo operativo, tampoco se han establecido cargos de capital regulatorio para el mismo. Sin embargo, como primera medida para favorecer una estructura que permita gestionar de mejor manera el riego operativo, la SBEF ha regulado las estructuras y sistemas de control interno (Síndicos, Comité de Auditoría y Unidad de Auditoría Interna) sobre la base de las recomendaciones emitidas por el Comité de Basilea sobre Gobierno Corporativo. Asimismo, ha establecido requisitos mínimos de seguridad informática para la administración de sistemas de información y tecnologías relacionadas.

El Reglamento de Funciones y Responsabilidades del Síndico tiene como objeto coadyuvar al fortalecimiento del gobierno corporativo. Establece las responsabilidades de los órganos de fiscalización interna de las entidades de intermediación financiera, en cuanto a velar por el cumplimiento de las leyes, reglamentos y normas internas, gestión diligente y adopción de medidas correctivas oportunas.

El Reglamento de Control Interno tiene como objeto establecer pautas para los aspectos técnicos y metodológicos para el adecuado funcionamiento del sistema de control interno. Este sistema funciona con cinco componentes relacionados entre sí:

a. Ambiente de control
b. Evaluación de los riesgos
c. Actividades de control y segregación de funciones.
d. Información y comunicación.
e. Actividades de monitoreo y corrección de deficiencias.

Según el Reglamento, en el sistema de control interno están involucrados todos los miembros: directivos, gerentes y personal de las entidades financieras. Adicionalmente, en los casos que contraten empresas para tercerizar servicios, las entidades financieras deben asegurarse que éstas sean competentes, financieramente sanas, con apropiados conocimientos y experiencia y que dispongan de un adecuado sistema de control interno.

Asimismo, el Reglamento regula el ámbito de acción del Comité de Auditoría y la Unidad de Auditoría Interna, el primero conformado por tres directores que tienen la función de coordinar las tareas de control y del adecuado funcionamiento del sistema de control interno. La Unidad de Auditoria Interna debe ser organizacional y funcionalmente independiente de las áreas de negocios y operativas, y depender orgánicamente del Directorio a través del Comité de Auditoria. Dicha unidad debe estar a cargo de un profesional idóneo y libre de cualquier impedimento para realizar su trabajo con independencia y contar con estabilidad laboral, pudiendo ser destituido únicamente de manera justificada por el Directorio.

El Reglamento sobre requisitos mínimos de seguridad informática para la administración de sistemas de información y tecnologías relacionadas, tiene por objeto establecer los requisitos mínimos que las entidades financieras deben cumplir para administrar los sistemas de información y la tecnología que los soporta y que son utilizados en las operaciones de intermediación financiera, transferencia electrónica de datos, transacciones electrónicas de datos, banca electrónica y cajeros automáticos.

Brasil

El Banco Central do Brasil está planificando emitir una regulación cualitativa sobre riesgo operacional en los próximos meses. No obstante, el riesgo operativo ha sido evaluado por la supervisión como un riesgo relevante que debe ser considerado por el directorio y la alta gerencia, de acuerdo a lo requerido por la regulación de control interno y las guías de supervisión.

Dicha regulación establece que todos los riesgos inherentes a las actividades de una institución financiera deben ser identificados, incluyendo: riesgo de crédito, riesgos de mercado (incluyendo riesgos de tasa de interés, tipo de cambio y precios), riesgo de liquidez, riesgos operativos, legales y reputacionales.

Los riesgos operativos, legales y reputacionales no son fáciles de adaptar a técnicas cuantitativas de gestión de riesgo. Sin embargo, es responsabilidad de la alta gerencia la identificación y entendimiento de estos riesgos, así como el establecimiento de políticas de control interno y procedimientos para mitigar su potencial impacto negativo en la fortaleza y viabilidad económico-financiera.

Colombia

En la actualidad no se tiene ninguna normativa al respecto y no se han identificado los eventos a incluir en la evaluación del mismo. Los temas revisados por el Grupo de Trabajo, relacionado al riesgo operativo no son aplicables a la situación en Colombia a la fecha.

Chile

El riesgo operacional es una de las áreas temáticas de la evaluación de gestión a las instituciones financieras, basada en las mejores prácticas.

El capítulo 1-13 de la Recopilación Actualizada de Normas disponible en www.sbif.cl, indica en términos generales la utilización de buenas prácticas en la gestión del riesgo operativo, destacándose entre otras la seguridad de la información, la continuidad del negocio y la calidad de la información, productos y servicios, materias que son evaluadas en función de estándares internacionales.

En enero del 2005, la Superintendencia de Bancos e Instituciones Financieras emitió la “Hoja de Ruta” para la transición de la banca chilena a Basilea II, en la cual se señala el método de cuantificación de los riesgos operativos, considerando que para su medición se utilizará el método estándar alternativo.

Ecuador

El sistema financiero ecuatoriano no ha sido ajeno a las pérdidas que genera la falta o la inadecuada administración del riesgo de operación; esta situación se puede apreciar en los eventos de riesgo operativo que se presentaron en la crisis financiera que vivió el Ecuador hace cinco años y que fueron ocasionados por fallas e insuficiencias en los procesos, en las personas y en la tecnología de información.

Es así que la Superintendencia de Bancos y Seguros del Ecuador emitió la norma sobre “La Gestión del Riesgo Operativo” que contiene disposiciones encaminadas a promover en las instituciones financieras controladas la aplicación de los principios y prácticas recomendadas por el Comité de Basilea, para la gestión del riesgo operativo, como un paso necesario y previo para ascender, en el futuro, hacia requerimientos cuantitativos de capital, contemplados en el Nuevo Acuerdo de Capital de Basilea.

La participación activa y la responsabilidad que asuman los máximos organismos de administración de las entidades son cruciales para el éxito del proceso, es por eso que la norma, en el marco de la administración integral de riesgos, define responsabilidades específicas sobre el riesgo operativo para el Directorio, el Comité de Riesgos y la Unidad de Riesgos.

Considerando la realidad del sistema financiero ecuatoriano, las disposiciones del organismo de control se orientan a exigir de las entidades requisitos mínimos para la administración de cada uno de

los factores del riesgo de operación: procesos, personas, tecnología de información y eventos externos.

- Respecto a los procesos se espera que las entidades establezcan procesos estructurados y organizados en función de su misión, visión y objetivos estratégicos, en armonía para maximizar la efectividad organizacional; que identifiquen sus procesos críticos, es decir, aquellos que en caso de una interrupción, pondrían en peligro la continuidad de las operaciones; por lo cual, se justifica plenamente contar con planes de contingencia.

- Con relación a las personas, la norma demanda a las instituciones administrar adecuadamente el recurso humano, ya que éste constituye el capital más valioso con el que cuenta una organización, para ello, es necesario que las entidades establezcan políticas y procesos para la incorporación, permanencia y desvinculación de su personal.

- En cuanto a la tecnología, la expectativa es que las instituciones cuenten con una tecnología de información que soporte adecuadamente las operaciones y procesos de las entidades. Para esto, es necesario que las entidades planifiquen ordenadamente sus requerimientos actuales y futuros de tecnología; que establezcan toda una serie de requisitos y condiciones de seguridad y de continuidad del negocio, de manera que, puedan contar en todo momento con información que cumpla con las características de integridad, disponibilidad y confidencialidad; además de asegurar que la tecnología no afecte al normal desenvolvimiento de sus operaciones.

- La gestión del riesgo operativo requiere que las instituciones financieras identifiquen cualquier evento externo (no derivado de asuntos políticos o económicos) que pudiera afectar sus actividades y tomen las acciones necesarias para controlarlos, a través del establecimiento de planes de contingencias.

Las entidades también deberán establecer un proceso para identificar, medir, controlar y monitorear el riesgo operativo. Es así que, deberán identificar los eventos (aquellos establecidos por el Comité de Basilea) y las fallas o insuficiencias que los generan; preparar y acumular bases de datos; establecer un sistema de control interno y sistema de reportes periódicos que permitan hacer un seguimiento de las exposiciones del riesgo operativo.

La identificación de los eventos de riesgo operativo deberá efectuarse por línea de negocio, agrupados por tipo de evento:

1. Fraude interno;
2. Fraude externo;
3. Prácticas laborales y seguridad del ambiente de trabajo;
4. Prácticas relacionadas con los clientes, los productos y el negocio;
5. Daños a los activos físicos;
6. Interrupción del negocio por fallas en la tecnología de información; y,
7. Deficiencias en la ejecución de procesos, en el procesamiento de operaciones y en las relaciones con proveedores y terceros.

Los eventos de riesgo operativo y las fallas o insuficiencias serán identificados en relación con los factores de este riesgo a través de una metodología formal, debidamente documentada y aprobada. Dicha metodología podrá incorporar la utilización de las herramientas que más se ajusten a las necesidades de la institución, entre las cuales podrían estar: autoevaluación, mapas de riesgos, indicadores, tablas de control (scorecards), bases de datos u otras.

Para una correcta identificación y cuantificación del riesgo operativo, la norma ecuatoriana, de manera muy ilustrativa, ha dispuesto la inclusión de un Anexo No. 2 que incluye los eventos de

riesgo operativo, agrupados por tipo de evento, fallas o insuficiencias que podrían presentarse en las instituciones controladas y su relación con los factores de riesgo operativo.

El Salvador

Entre las principales prácticas para la gestión del riesgo operativo están las siguientes:

a) El Art. 63 de la Ley de Bancos (LB) establece que los bancos deben de elaborar e implantar sistemas de control interno que permitan manejar adecuadamente los riesgos financieros y operativos.
b) En el Art. 226 de la LB se definen las obligaciones y funciones de los auditores externos de los bancos, entre las que está: opinar sobre la suficiencia y efectividad de los sistemas de control interno contable de la institución, opinar sobre el cumplimiento de las disposiciones legales y reglamentarias, especialmente las relativas al fondo patrimonial, límites de créditos, créditos y contratos con personas relacionadas y la suficiencia de las reservas de saneamiento y opinar sobre el cumplimiento de las políticas internas a las que se refiere el Art. 63 de LB.
c) El Art. 227 dispone la conformación de un comité de auditoria que deberá estar integrado al menos por el auditor interno, el director ejecutivo o un gerente de igual categoría y dos miembros de la Junta Directiva que no ostentan cargos ejecutivos. Entre sus funciones están: dar seguimiento a los informes del auditor interno, del auditor externo y de la Superintendencia para corregir las observaciones que formulen y colaborar en el diseño y aplicación del control interno proponiendo las medidas correctivas pertinentes.
d) La Superintendencia ha emitido el Reglamento para la Unidad de Auditoria Interna de los Bancos y Sociedades de Seguros y las Normas para las Auditorias Externas de Bancos y Sociedades de Seguros, que regulan la actuación del auditor interno y externo en cuanto a la evaluación del control interno de los bancos.

Como parte de las prácticas de supervisión la Superintendencia revisa el trabajo desarrollado por los auditores internos y externos de los bancos y cuenta con facultades legales para sancionarlos administrativamente en caso no estén cumpliendo debidamente con sus obligaciones.

Guatemala

Los artículos 55 y 56 de la Ley de Bancos y Grupos Financieros (LBGF) contemplan que los bancos y los grupos financieros deberán contar con procesos integrales para la administración del riesgo operativo que incluyan sistemas de información y un comité de gestión de riesgos. Todo ello con el propósito de identificar, medir, monitorear, controlar y prevenir los riesgos, además de contar con políticas escritas actualizadas, para una adecuada administración de los diversos riesgos a que están expuestas.

Por su parte, el oficio No. 1216-2003 de la Superintendencia de Bancos (SB), en materia de riesgo operativo incluyó como requerimientos mínimos a los bancos del sistema, lo siguiente: a) sistema de control interno que incluya políticas y procedimientos para identificar, monitorear, controlar y mitigar las exposiciones al riesgo operativo en todos los productos, procesos y sistemas existentes o en proyecto; b) Identificación de procesos críticos de las operaciones, incluyendo aquellos donde exista dependencia de proveedores externos; c) planes de sustitución o relevo cuando se identifique personas clave dentro de la organización; y, d) planes de contingencia y continuidad de negocios.

Proceso de Supervisión

El avance tecnológico en las transacciones bancarias, el reemplazo de los registros físicos por digitales, y la mayor automatización de las operaciones financieras, han generado un nuevo concepto de exposición al riesgo operativo. Por tal razón, actualmente se realizan evaluaciones a las políticas, procedimientos y prácticas de un banco respecto de los riesgos operativos con énfasis en riesgos

tecnológicos de información, dichas revisiones se llevan a cabo con base en la metodología COBIT adaptada a la realidad de Guatemala; en dicha metodología, se consideran los siguientes dominios:

a) Planeación y Organización: Este dominio tiene como propósito determinar la existencia de un plan estratégico de tecnología de información que permita a la entidad financiera un desarrollo tecnológico organizado, y soporte las operaciones del negocio de manera oportuna, eficiente y confiable.

b) Adquisición e Implementación: El objetivo de verificar este dominio es determinar la existencia de políticas y procedimientos establecidos institucionalmente para la adquisición e implementación de sistemas de información con altos estándares de calidad y seguridad que apoyen la adecuada toma de decisiones.

c) Entrega y Soporte: En este dominio incluyen las actividades involucradas en brindar el soporte tecnológico que necesita la organización. Cubre aspectos de seguridad física y lógica, procesamiento de datos, planes de contingencia y continuidad del negocio, entre otros

d) Monitoreo: El propósito de este dominio es determinar si los auditores internos y/o externos están llevando a cabo un programa efectivo de auditoria de riesgos tecnológicos y de sistemas de información.

e) Sistemas de Información: Se evalúan las aplicaciones críticas de la entidad, tales como: inversiones, cartera, tarjeta de crédito, depósitos, obligaciones financieras, Swift y banca electrónica, con el fin de verificar la integridad de las bases de datos, razonabilidad de la información contable como la registrada en las bases de datos y confiabilidad de la información enviada por las entidades financieras a la SB.

Cada dominio tiene una ponderación y posteriormente se obtiene una calificación general para la institución, determinando la situación o condición de la entidad con respecto al riesgo tecnológico.

Cabe comentar que actualmente, la SB se encuentra trabajando en las normas de general aplicación y requisitos mínimos que los bancos deben de cumplir con relación a los diversos riesgos que asumen, incluyendo el riesgo operativo.

Guatemala experimenta dificultades al introducir prácticas internacionales, debido a que el país está todavía en proceso de implementar prácticas de gestión de riesgo y de obtener datos e información que posibilitará evaluar este tipo de riesgo. Es por ello que todavía no ha determinado el método más acorde ni ha establecido un cronograma de implementación de requerimientos de capital para riesgo operativo, en función de los lineamientos de Basilea II.

Honduras

El Artículo 30, Sección 4 de la LSF obliga al Directorio de las Entidades Financieras a asegurar que se implementen y mantengan apropiados sistemas de gestión y control de riesgos. Esto también es requerido por la regulación de gobierno corporativo. Las normas para auditores internos requieren el examen de la efectividad de los controles internos en la mitigación del riesgo operativo.

Perú

La Superintendencia de Banca, Seguros y Administradoras Privadas de Fondos de Pensiones (SBS) ha emitido normas para la administración del riesgo operacional en enero de 2002, las cuales están alineadas con los principios señalados en el documento de “Prácticas adecuadas para la gestión y supervisión del riesgo operacional” publicado por el Comité de Basilea; asimismo, ha emitido otros requerimientos que tratan sobre el riesgo tecnológico, la continuidad operativa y la tercerización. Desde el año 2000, se cuenta con un departamento especializado en la supervisión de los riesgos

operacionales, el cual actualmente desarrolla sus funciones en el sistema bancario, de seguros y de fondos de pensiones.

A través de la regulación y supervisión realizada por la SBS, se busca que las empresas cumplan con las siguientes buenas prácticas señaladas por el Comité de Basilea:

- Participación del Directorio en el monitoreo y aprobación de la metodología utilizada por la empresa para la administración de los riesgos operativos.
- Revisión de Auditoria Interna a la aplicación de dicha metodología.
- Participación de la Alta Gerencia en la implementación de la metodología.
- Identificación de riesgos operativos en los productos, actividades, procesos y sistemas más importantes.
- Monitoreo de los perfiles de riesgo operativo y de las exposiciones importantes a pérdidas.
- Establecer políticas, procesos y procedimientos para controlar y/o mitigar los riesgos operativos importantes.
- Contar con planes de contingencia y planes de continuidad de negocio.

Estados Unidos

Las agencias de supervisión poseen una gran cantidad de orientación sobre gobierno corporativo, controles internos y seguimiento e información en sus respectivos procedimientos y políticas de inspección. Todas las agencias tienen normas para operaciones sanas y seguras y para la protección de la información sobre los clientes. Además, existen varias normativas interinstitucionales que cubren temas relacionados con la estructura de control interno. Entre ellas cabe mencionar, por ejemplo, el manual sobre la planificación de la continuidad de la actividad de mayo de 2003 (Federal Financial Institutions Examination Council's (FFIEC's) Business Continuity Planning Booklet), el manual sobre la seguridad de la información, de enero de 2003 (FFIEC's Information Security Booklet), las declaraciones de política interinstitucionales sobre la tercerización del tratamiento de la información y de las transacciones (Outsourcing of Information and Transaction Processing) de febrero de 2000 y la orientación sobre la gestión de riesgos de la tecnología tercerizada (Guidance on the Risk Management of Outsourced Technology) de noviembre de 2000.

La política de inspecciones y procedimientos pueden ser encontrados en los sitios web siguientes:

- www.ffiec.gov
- www.fdic.gov
- www.frb.gov

Referencias

- Comité de Basilea de Supervisión Bancaria: Sanas Prácticas para la Gestión y supervisión del Riesgo Operativo, febrero 2003, Banco de Pagos Internacionales
- Comité de Basilea de Supervisión Bancaria Convergencia Internacional de Medición de Capital y Estándares de Capital Un marco revisado, junio 2004, Banco de Pagos Internacionales.
- Statutory Protection for Banking Supervisors, by Ross S Delston, 2000, disponible en http://www1.worldbank.org/finance/html/statutory_protection.html
- Ley de Bancos y Grupos Financieros - Guatemala, Junio 2002
- Ley de Supervisión Financiera – Guatemala, May 2002
- Ley del Sistema Financiero - Honduras
- Ley General del Sistema Financiero y del Sistema de Seguros y Orgánica de la Superintendencia de Banca y Seguros, Ley 26702. (Texto Concordado)- Perú, Febrero 2004
- Ley de Bancos y Entidades Financieras (Texto ordenado) – Bolivia, Agosto 2004
- Federal Deposit Insurance Act (12 U.S.C. 1831)
- Federal Tort Claims Act, 28 U.S.C
- Risk-Based Capital Guidelines; Capital Adequacy Guidelines; Capital Maintenance: Domestic Capital Modifications - Joint advance notice of proposed rulemaking (ANPR). published in the *Federal Register* on October 20, 2005
- Codificación de Resoluciones de la Junta Bancaria y de la Superintendencia de Bancos y Seguros del Ecuador, Título VII, Subtítulo VI, Capítulo V “De la Gestión del Riesgo Operativo” (Resolución No. JB-2005-834)

Abreviaturas

AMA:	Métodos de Medición Avanzada / Advanced Measurement Approaches
ANPR:	Anuncio de Propuesta de Reglamentación / Advance Notice of Proposed Rulemaking
ERO:	Exposición al Riesgo Operativo / EOR – Exposure to Operacional Risk
FDIC:	Federal Deposit Insurance Corporation (EE.UU.)
FFIEC:	Federal Financial Institutions Examination Council (EE.UU.)
FRB:	Junta de la Reserva Federal / Federal Reserve Board (EE.UU)
GAAP:	Principios de Contabilidad Generalmente Aceptados
GRO:	Gestión de Riesgo Operativo
IF:	Institución Financiera / Financial Institution
IFs:	Instituciones Financieras / Financial Institutions
IRB:	Basado en Clasificación Interna / Internal Rating Based
LB:	Ley de Bancos (El Salvador)
LBEF:	Ley de Bancos y Entidades Financieras (Bolivia)
LBGF:	Ley de Bancos y Grupos Financieros (Guatemala)
LSF:	Ley de Supervisión Financiera (Guatemala)
LSF:	Ley del Sistema Financiero (Honduras)
MOU:	Memorando de Entendimiento / (Memorandum of Understanding)
NAC:	Nuevo Acuerdo de Capital (Basilea II)
OCC:	Office of the Comptroller of the Currency (EE.UU.)
OTS:	Office of Thrift Supervision (EE.UU.)
PE:	Pérdida Esperada / (EL – Expected Loss)
POE:	Pérdida Operativa Esperada / (EOL - Expected Operational Loss)
POI:	Pérdida Operativa Inesperada / (UOL – Unexpected Operational Loss)
QIS:	Estudio de Impacto Cuantitativo / Quantitative Impact Study
SB:	Superintendencia de Bancos (Guatemala)
SBEF:	Superintendencia de Bancos y Entidades Financieras (Bolivia)
SBS:	Superintendencia de Banca y Seguros (Perú)
SEC:	Securities and Exchange Commission (EE.UU.)

Anexo No. 1 – Miembros del Grupo de Trabajo

Asociación de Supervisores Bancarios de las Américas (ASBA)

Grupo de Trabajo en Riesgo de Crédito y Operativo

Presidente:

Alejandro Medina,
Superintendencia de Banca, Seguros y AFPs (Perú)

Miembros:

País	Institución	Representante
Bolivia	Superintendencia de Bancos y E.F.	Carla Ritha Solares Pareja
Brazil	Banco Central do Brasil	Wagner Soares de Almeida
Chile	Superintendencia de Bancos e I. F.	Myriam Uribe Valenzuela
Colombia	Superintendencia Bancaria de Colombia	Fabio Andrés Villalba Ricaurte
Ecuador	Superintendencia de Bancos y Seguros	Rodrigo Mora Guzmán
El Salvador	Superintendencia del Sistema Financiero	Sigfredo Gómez
Estados Unidos	Federal Reserve System	David Wright
Estados Unidos	Federal Deposit Insurance Corporation	John Di Clemente
Guatemala	Superintendencia de Bancos	César Enrique Marroquín Fernández
Honduras	Comisión Nacional de Bancos y Seguros	Jorge Antonio Flores Padilla
Paraguay	Superintendencia de Bancos	Fernando Herrero Portillo
Perú	Superintendencia de Banca y Seguros	Alejandro Medina Moreno
Rep. Dominicana	Superintendencia de Bancos	Luis Andrés Montes de Oca

Secretario Técnico del Grupo de Trabajo:
Guillermo Romano Rivero – ASBA

Anexo No. 2 *Anexo No. 1 de la Resolución No. JB-2005-834 aprobada por la Junta Bancaria del Ecuador (Octubre 2005)*

ANEXO No.1

IDENTIFICACIÓN DE EVENTOS, FALLAS O INSUFICIENCIAS Y FACTORES DEL RIESGO OPERATIVO

LINEAS DE NEGOCIO:

TIPOS DE EVENTOS	FALLAS O INSUFICIENCIAS	FACTORES DE RIESGO DE OPERATIVO	NUMERO DE VECES (FRECUENCIA)	EFECTO CUANTITATIVO PERDIDA PRODUCIDA
FRAUDE INTERNO				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Operaciones no reveladas adecuadamente	Mal diseño de proceso	Procesos		
Operaciones no registradas intencionalmente	Inadecuada selección de personal	Personas		
Inadecuada utilización de información confidencial	Ausencia de control en los perfiles de usuario	Tecnología de Información		
Apropiación indebida de activos	Inadecuada segregación de funciones	Personas		
Falsificación	Inexistencia de controles	Procesos		
Destrucción maliciosa de activos	Inadecuadas medidas de seguridad	Procesos		
Evasión de impuestos	Falta de ética	Personas		
Robo	Inadecuada segregación de funciones	Personas		
FRAUDE EXTERNO				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Robo	Falta de seguridades físicas	Procesos		
Emisión de cheques sin fondos	Inadecuada capacitación del Personal	Personas		
Perjuicios por intrusión o ataque de terceros	Falta de seguridades en la teconología de información para prevenir ataques de terceros	Tecnología de Información		
Falsificación	Falta de seguridades de la tecnología de información	Tecnología de Información		
PRACTICAS DE EMPLEO Y SEGURIDAD DEL AMBIENTE DE TRABAJO				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Reclamos por compensación e indemnización al personal	Inadecuada contratación del personal	Procesos		
Violación de las normas de salud o seguridad	Falta de difusión y comunicación de políticas	Personas		
Todo tipo de discriminación	Inadecuada política de administración de personal	Personas		
PRACTICAS RELACIONADAS CON CLIENTES, LOS PRODUCTOS Y EL NEGOCIO				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Mal manejo de la información confidencial de clientes	Falta de defininición de políticas y procedimientos	Procesos		
Prácticas contrarias a la competencia, prácticas inadecuadas de negociación	Falta de defininición de políticas	Personas		
Actividades no autorizadas	Incursión en nuevas actividades sin considerar riesgos	Procesos		
Abuso de información privilegiada a favor de la institución	Falta de ética	Personas		
DAÑOS A LOS ACTIVOS FÍSICOS PROVOCADOS POR				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Terrorismo	Faltes de planes de contingencia (debidamente probados)	Eventos externos		
Vandalismo	Faltes de planes de contingencia (debidamente probados)	Eventos externos		
Pérdidas por desastres naturales	Faltes de planes de contingencia (debidamente probados)	Eventos externos		
INTERRUPCIÓN DEL NEGOCIO Y FALLAS EN LOS SISTEMAS				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Fallas en el software	Deficiencia en el proceso de desarrollo y/o implantación	Tecnología de Información		
Fallas en el hadware	Falta de previsión de la capacidad de los recursos para el volumen de operaciones. Falta de mantenimiento preventivo de los servidores centrales	Tecnología de Información		
Problemas de telecomunicación	Caída en los enlaces de telecomunicaciones	Tecnología de Información		
Cortes en los servicios públicos	Falta de planes de contingencia	Eventos externos		
DEFICIENCIAS EN LA EJECUCIÓN DE PROCESOS, EN EL PROCESAMIENTO DE OPERACIONES Y EN LAS RELACIONES CON PROVEEDORES Y OTROS EXTERNOS				
Por Ejemplo:	**Por Ejemplo:**	**Por Ejemplo:**		
Errores en el ingreso de los datos	Falta de controles de ingreso de datos en las aplicaciones	Tecnología de Información		
Falla en la administración de colaterales	Inadecuada segregación de funciones	Procesos		
Documentación legal incompleta	Falta de verificación del área legal	Procesos		
Acceso no aprobado a las cuentas de clientes	Proceso no definido	Procesos		
Disputa con los proveedores	Deficiencias en la contratación	Procesos		
Incumplimiento en la entrega de la información hacia terceros	Falta de controles en el proceso de envio de información	Procesos		

NOTAS:

1.- En el presente Anexo constan ejemplos de eventos agrupados por tipo, los cuales consideran los lineamientos establecidos por el Comité de Basilea

2.- Los eventos que se produjeren que no esté alineados a los tipos de eventos especificados en este Anexo, deberán constar bajo la denominación "información no alineada, concepto bajo el cual constarán únicamente por excepción.

3.- Frecuencia, se refiere al número de veces que se repite cada evento