

Riesgo operativo desde una perspectiva de supervisión

FECOOPSE

Comité Interinstitucional de Riesgos (CIR)

San José, Marzo de 2013

Genaro Segura C., FRM

Índice de temas

- 1 Riesgo Operativo (Definición y dimensiones de abordaje supervisor)
- 2 Principios de Sana Gestión del RO (Basilea)
- 3 Principios de Supervisión Efectiva del RO (Basilea)
- 4 Una regulación específica para RO

Riesgo Operativo

Definición – Gestión - Regulación

FECOOPSE

Comité Interinstitucional de Riesgos (CIR)

San José, Marzo de 2013

Genaro Segura C., FRM

Definición de riesgo de RO

Algunas definiciones

SUGEF 2-10:

Es la posibilidad de una pérdida económica debido a fallas o debilidades de Procesos, Personas, Sistemas internos y tecnología, Eventos imprevistos. El riesgo operacional incluye el Riesgo de Tecnologías de Información y el Riesgo Legal.

Basilea (PB25):

El riesgo de sufrir pérdidas debido a la inadecuación o fallos de Procesos, Personas, Sistemas internos, Acontecimientos externos. La definición incluye el riesgo legal pero excluye los riesgos estratégico y de reputación.

Retos de gestión del RO

- Por su naturaleza el RO afecta potencialmente a cada actividad de la entidad financiera
- Su gestión no puede centralizarse completamente; es compartida tanto a nivel de la entidad como un todo y al nivel de cada nivel línea de negocio.
- Dada esta naturaleza, Basilea sugiere que la gestión del RO se aborde desde tres líneas de defensa.

Líneas de defensa

RO

1

Gestión de líneas de negocio:

Primer responsable por identificar y gestionar los riesgos inherentes a los productos, actividades, procesos y sistemas de los cuales es responsable.

2

Función de gestión del RO independiente:

Complemento a las actividades de gestión de las líneas de negocio

3

Revisión independiente mediante AI o AE:

Verificación
Validación

Sobre la tercerización de actividades de AI

- La función de auditoría interna de los bancos (Basilea, Junio 2012)
 - ✓ Principio 15: Independientemente de si las actividades de la AI son tercerizadas, la Junta Directiva mantiene la responsabilidad final por la función de la auditoría interna.
 - ✓ Se tercerizan actividades, pero no la función en sí misma.
 - ✓ Las razones de la tercerización de actividades específicas de AI deben ser bien razonadas.
 - ❑ Alcance limitado y dirigido, de manera que traiga beneficios, como el acceso a experiencia y conocimiento especializado.
 - ❑ Respuesta temporal a restricciones de recursos que pueden afectar la ejecución de un plan de auditoría.

Dimensiones de abordaje regulatorio y supervisor del RO

Gestión

Sanas prácticas de gestión (Expectativa del supervisor)

Capital

Requerimientos de capital

Supervisión

Sanas prácticas de Supervisión

Principios de Gestión del Riesgo Operativo

11 Principios de Basilea sobre gestión del Riesgo Operacional

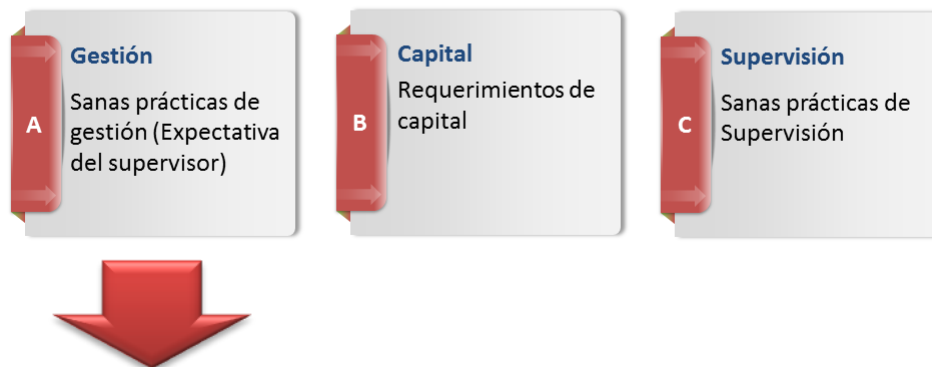
Marco de Capital de Basilea

Método Básico
Estandarizado
Avanzado

Principios Básicos para una Supervisión Efectiva

Principio 25 de Basilea sobre supervisión del Riesgo Operacional

**Dimensiones de abordaje regulatorio
y supervisor del RO**



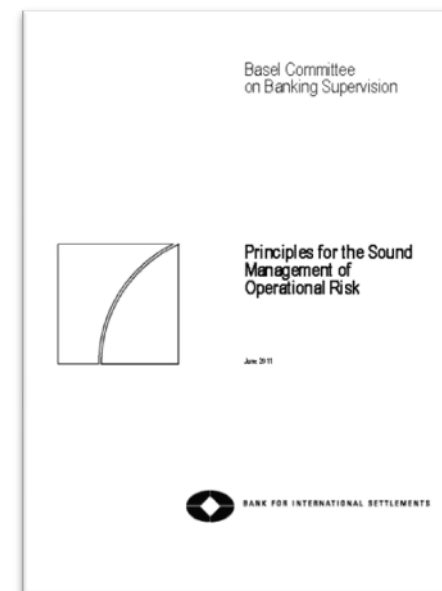
Recomendaciones internacionales

Principios sobre sanas practicas de Gestión del RO

Junio, 2011

FECOOPSE
Comité Interinstitucional de Riesgos (CIR)

San José, Marzo de 2013



Genaro Segura C., FRM

Principios sobre sanas practicas de Gestión del RO

Junio, 2011

1

Principio fundamental para la gestión del RO

- La junta directiva debe liderar en el establecimiento de una fuerte cultura de gestión de riesgos.
- La junta directiva y la alta gerencia deben establecer una cultura corporativa que se guía por la gestión sólida del riesgo y que apoya y proporciona normas adecuadas e incentivos para el desarrollo profesional y el comportamiento responsable.
- En este sentido, es responsabilidad del consejo de directores asegurar que existe una fuerte cultura de gestión del riesgo operacional a lo largo de toda la organización.

Principios sobre sanas practicas de Gestión del RO

Junio, 2011

2

Principio fundamental para la gestión del RO

- Los bancos deben desarrollar, implementar y mantener un marco para la gestión del riesgo operativo que esté plenamente integrado en los procesos generales de gestión de riesgos del banco.
- El marco para la gestión del riesgo operativo elegido por un banco individual dependerá de una serie de factores, incluyendo la naturaleza, el tamaño, la complejidad y el perfil de riesgo.

Principios sobre sanas practicas de Gestión del RO

Junio, 2011

3

Gobernabilidad – Juntas Directivas

- La junta directiva debe establecer, aprobar y revisar periódicamente el marco para la gestión del RO.
- El Consejo de Administración debe supervisar a la alta dirección, para asegurar que las políticas, procesos y sistemas se aplican eficazmente en todos los niveles de decisión.

Principios sobre sanas practicas de Gestión del RO

Junio, 2011

4

Gobernabilidad – Juntas Directivas

- El Consejo de Administración deberá aprobar y revisar el apetito por el riesgo y la declaración de tolerancia para el RO, en la cual se articula la naturaleza, tipos y niveles de riesgo operativo que el Banco está dispuesto a asumir.

Principios sobre sanas practicas de Gestión del RO

Junio, 2011

5

Gobernabilidad – Administración Superior

- La alta gerencia debe desarrollar, para su aprobación por el consejo de administración, una estructura de gobierno clara, eficaz y robusta, con líneas de responsabilidad bien definidas, transparentes y coherentes.
- La alta dirección es responsable de implementar y mantener constantemente, a través de las políticas de organización, procesos y sistemas para la gestión del riesgo operacional, en todos los productos, actividades, procesos y sistemas significativos, que estén en consonancia con el apetito por el riesgo y la tolerancia.

Principios sobre sanas practicas de Gestión del RO

Junio, 2011

6 Entorno de administración de riesgos - Identificación y Valoración

- La alta gerencia debe asegurar la identificación y evaluación de los riesgos operativos inherentes a todos los productos, actividades, procesos y sistemas significativos, para asegurarse de que los riesgos inherentes e incentivos se conocen bien.

Principios sobre sanas practicas de Gestión del RO

Junio, 2011

7 Entorno de administración de riesgos - Identificación y Valoración

- La alta dirección debe asegurarse de que hay un proceso de aprobación para todos los nuevos productos, actividades, procesos y sistemas que evalúa completamente el riesgo operacional.

Principios sobre sanas practicas de Gestión del RO

Junio, 2011

8

Entorno de administración de riesgos - Monitoreo y reportes

- La alta gerencia debe implementar un proceso para monitorear regularmente los perfiles de riesgo operacional y las exposiciones importantes a pérdidas.
- Deben implementarse mecanismos adecuados de reporte al Directorio, la alta gerencia y los niveles de líneas de negocio que apoyan la gestión proactiva del riesgo operacional.

Principios sobre sanas practicas de Gestión del RO

Junio, 2011

9

Entorno de administración de riesgos - Control y mitigación

- Los bancos deben tener un fuerte ambiente de control que utiliza políticas, procesos y sistemas, adecuados controles internos, y la mitigación del riesgo adecuada y / o estrategias de transferencia.

Principios sobre sanas practicas de Gestión del RO

Junio, 2011

10

Capacidad de recuperación y continuidad de negocios

- Los bancos deben tener flexibilidad empresarial y los planes de continuidad para asegurar la capacidad de operar de forma continua y limitar las pérdidas en caso de incidencias graves en el negocio.

Principios sobre sanas practicas de Gestión del RO

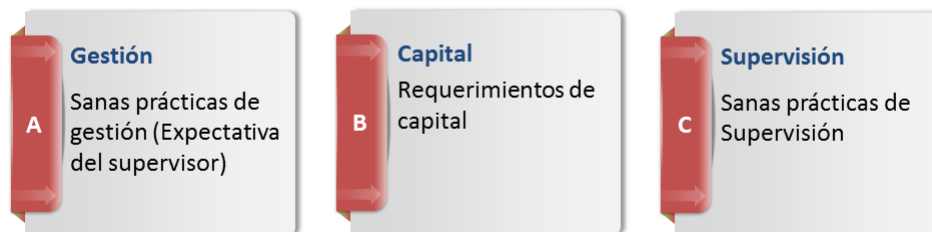
Junio, 2011

11

Divulgación

- La divulgación pública de un banco debe permitir a los interesados evaluar su enfoque de gestión del riesgo operacional.

**Dimensiones de abordaje regulatorio
y supervisor del RO**



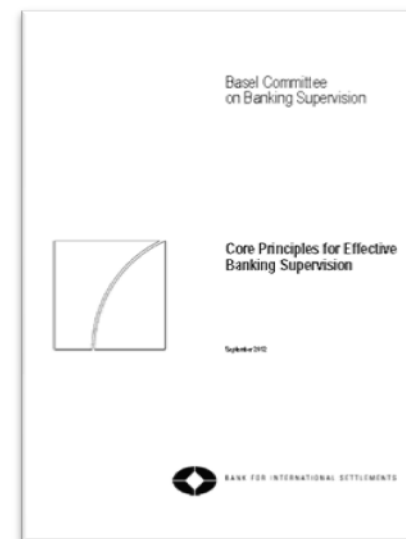
Recomendaciones internacionales

Principios para una Supervisión Bancaria Efectiva

Setiembre, 2012

FECOOPSE
Comité Interinstitucional de Riesgos (CIR)

San José, Marzo de 2013



Genaro Segura C., FRM

Principios Básicos para una Supervisión Efectiva - Basilea

Principio 25. Riesgo Operacional

- El supervisor **determina** que los bancos cuentan con un marco adecuado de gestión del riesgo operacional, que toma en cuenta su apetito por el riesgo, su perfil de riesgo y la situación macroeconómica y de los mercados.
- Esto incluye **políticas** y **procesos** prudentes para identificar, cuantificar, evaluar, vigilar, informar y controlar o mitigar el riesgo operacional en el momento oportuno.

Principios Básicos para una Supervisión Efectiva - Basilea

Principio 25. Riesgo Operacional

Criterio Esencial 1

- La legislación, la regulación o el supervisor **exigen** que el banco disponga de adecuadas **estrategias, políticas y procesos** para la gestión del RO que permitan **identificar, cuantificar, evaluar, vigilar, informar y controlar** o **mitigar** dicho riesgo.
- El supervisor **determina** que la **estrategia, políticas y procesos** del banco están en consonancia con
 - ✓ el perfil de riesgo,
 - ✓ la importancia sistémica,
 - ✓ el apetito por el riesgo y la solidez del capital de la entidad,
- Y toman en cuenta
 - ✓ la situación macroeconómica y de los mercados, y
 - ✓ abarcan todos los aspectos esenciales del RO latente en los negocios realizados por la entidad como un todo (incluidos periodos en los que el RO podría aumentar).

Principios Básicos para una Supervisión Efectiva - Basilea

Principio 25. Riesgo Operacional

Criterio Esencial 2

- El supervisor **exige** que las **estrategias**, **políticas** y **procesos** de los bancos para la gestión del riesgo operacional (incluido su apetito por el riesgo operacional) sean aprobados y revisados periódicamente por el Consejo.
- El supervisor también **exige** que el Consejo vigile a la dirección del banco para asegurarse de que dichas **políticas** y **procesos** se aplican eficazmente.

Principios Básicos para una Supervisión Efectiva - Basilea

Principio 25. Riesgo Operacional

Criterio Esencial 3

- El supervisor **determina** que la dirección del banco aplica en la práctica la **estrategia** aprobada y las pertinentes **políticas** y **procesos** para la gestión del riesgo operacional, quedando éstos plenamente integrados en el proceso global de gestión del riesgo de la entidad.

Principios Básicos para una Supervisión Efectiva - Basilea

Principio 25. Riesgo Operacional

Criterio Esencial 4

- El supervisor **evalúa** la calidad y exhaustividad de los planes de recuperación ante desastres y de continuidad del negocio del banco en escenarios de graves alteraciones de la actividad que plausiblemente pueden afectar a la entidad.
- En este sentido, el supervisor **determina** que el banco es capaz de operar sin interrupciones y con pérdidas mínimas, incluidas las que pueden producirse a raíz de alteraciones en los sistemas de pago y liquidación, en caso de graves alteraciones de la actividad.

Principios Básicos para una Supervisión Efectiva - Basilea

Principio 25. Riesgo Operacional

Criterio Esencial 5

- El supervisor **determina** que los bancos cuentan con adecuadas políticas y procesos en materia de tecnología informática para identificar, evaluar, vigilar y gestionar los riesgos tecnológicos.
- El supervisor también **determina** que los bancos disponen de una sólida y adecuada infraestructura tecnológica para cubrir las necesidades actuales y previstas del negocio (en circunstancias normales y en periodos de tensión), que garantice la integridad, seguridad y disponibilidad de datos y sistemas y facilite una gestión integral y exhaustiva del riesgo.

Principios Básicos para una Supervisión Efectiva - Basilea

Principio 25. Riesgo Operacional

Criterio Esencial 6

- El supervisor **determina** que los bancos cuentan con sistemas de información adecuados y eficaces para:
 - (a) vigilar el riesgo operacional;
 - (b) recopilar y analizar datos sobre el riesgo operacional; y
 - (c) promover la existencia de adecuados mecanismos de notificación al Consejo, la alta dirección y las líneas de negocio del banco para facilitar una gestión proactiva del riesgo operacional.

Principios Básicos para una Supervisión Efectiva - Basilea

Principio 25. Riesgo Operacional

Criterio Esencial 7

- El supervisor **exige** que los bancos dispongan de adecuados mecanismos de notificación que le mantengan al día de cualquier cambio que afecte al riesgo operacional de los bancos de su jurisdicción.

Principios Básicos para una Supervisión Efectiva - Basilea

Principio 25. Riesgo Operacional

Criterio Esencial 8

- El supervisor **determina** que el banco ha establecido políticas y procesos adecuados para evaluar, gestionar y vigilar las actividades subcontratadas.
- El programa para la gestión del riesgo de subcontratación incluye:
 - (a) aplicar la diligencia debida al seleccionar posibles proveedores de servicios;
 - (b) estructurar el procedimiento de subcontratación;
 - (c) gestionar y vigilar los riesgos relacionados con el procedimiento de subcontratación;
 - (d) garantizar un entorno de control eficaz; y
 - (e) establecer planes de contingencia viables.
- Las políticas y procesos de subcontratación exigen que el banco disponga de exhaustivos contratos y/o otros acuerdos de prestación de servicios que delimiten claramente las responsabilidades entre la empresa subcontratada y el banco.

Principios Básicos para una Supervisión Efectiva - Basilea

Principio 25. Riesgo Operacional

Criterio Adicional 1

- El supervisor **identifica** periódicamente factores comunes de exposición al riesgo operacional o de posibles vulnerabilidades (por ejemplo, la subcontratación de operaciones esenciales por parte de numerosas entidades con un mismo proveedor de servicios o una alteración de los servicios prestados por sistemas subcontratados de pago y liquidación).

Regulación específica sobre Riesgo operativo

FECOOPSE

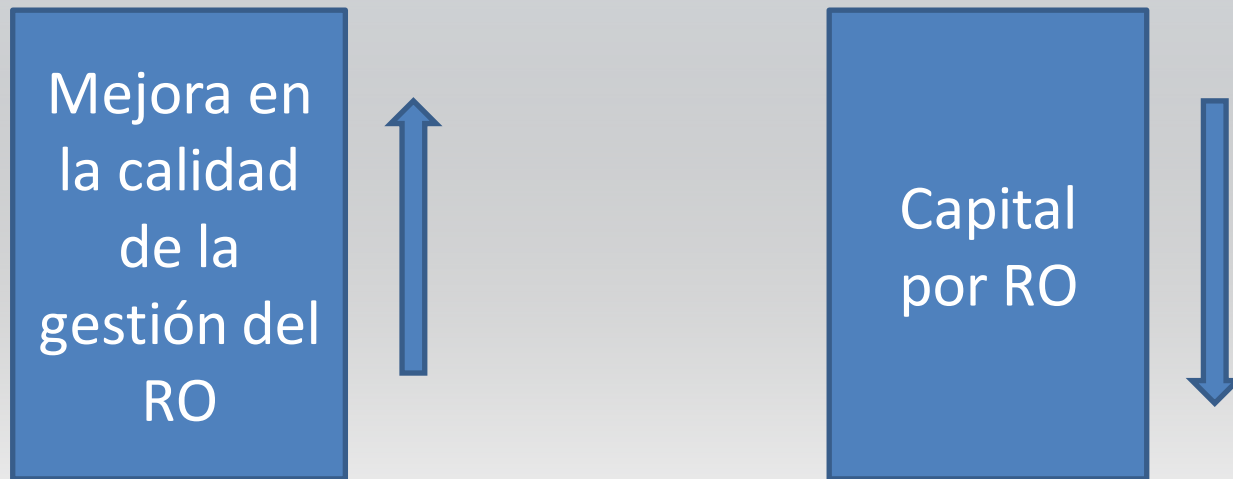
Comité Interinstitucional de Riesgos (CIR)

San José, Marzo de 2013

Genaro Segura C., FRM

Hacia un enfoque de incentivos adecuados

Promover incentivos adecuados para la mejora en la calidad de la gestión de RO



La disyuntiva actual del método básico

Regulación específica sobre gestión del RO

La regulación específica debe enmarcarse y ser complementaria al marco normativo general sobre gobierno y gestión de riesgos

- Gobierno Corporativo (16-09)
 - Administración de Riesgos (2-10, 9-08-Cap.IV)
 - Resolución SUGEF R-008-2010
 - Titularización y fideicomisos (13-10)
 - Tecnología de información (14-09)
-
- Legitimación (12-10)

Regulación específica sobre gestión del RO

La regulación específica debe acogerse a los mismos atributos del proceso de Administración Integral de Riesgos

- Formal
- Continuo
- Integral
- Proporcional

Regulación específica sobre gestión del RO

La regulación específica debe destacar la relevancia del RO

- Inherente a la actividad financiera
- Transversal a las actividades, procesos, productos
- Objeto de gestión en el proceso de administración integral de riesgos
- Asumido con definición propia sobre su alcance para la entidad, y de manera funcional para el proceso de administración de riesgos.

Regulación específica sobre gestión del RO

La regulación específica debe exigir la identificación de líneas de negocio y procesos relevantes

- Catálogo de líneas de negocio (procesos y subprocesos asociados)
- Identificación adecuada de riesgos operacionales
- Discriminación de procesos críticos.
- Referencia a grandes líneas de negocio Basilea

Líneas de Negocio

Nivel 1	Nivel 2	Grupo de actividades
Finanzas corporativas	Finanzas corporativas	Fusiones y adquisiciones, suscripción de emisiones, privatizaciones, titulización, servicio de estudios, deuda (pública, alto rendimiento), acciones, sindicaciones, Ofertas Públicas iniciales, colocaciones privadas en mercados secundarios.
	Finanzas de Administraciones locales/públicas	
	Banca de Inversión	
	Servicios de asesoramiento	
Negociación y ventas	Ventas	Renta fija, renta variable, divisas, productos básicos, crédito, financiación, posiciones propias en valores, préstamo y operaciones con pacto de recompra, intermediación, deuda.
	Creación de Mercado	
	Posiciones propias	
	Tesorería	
Banca minorista	Banca minorista	Préstamos y depósitos de clientes minoristas, servicios bancarios, fideicomisos y testamentarías.
	Banca privada	Préstamos y depósitos de particulares, servicios bancarios, fideicomisos y testamentarías, y asesoramiento de inversión.
	Servicios de tarjetas	Tarjetas de empresa / comerciales, de marca privada y minoristas.
Banca comercial	Banca comercial	Financiación de proyectos, bienes raíces, financiación de exportaciones, financiación comercial, factoring, arrendamiento financiero, préstamo, garantías, letras de cambio.
Pago y liquidación	Clientes Externos	Pagos y recaudaciones, transferencia de fondos, compensación y liquidación.
Servicios de agencia	Custodia	Certificados de depósito, operaciones de sociedades (clientes) para préstamo de valores
	Agencia para empresas	Agentes de emisiones y pagos
	Fideicomisos de empresas	
Administración de activos	Administración discrecional de fondos	Agrupados, segregados, minoristas, institucionales, cerrado, abiertos, participaciones accionariales.
	Administración no discrecional de fondos	Agrupados, segregados, minoristas, institucionales, de capital fijo, de capital variable.
Intermediación minorista	Intermediación minorista	Ejecución y servicio completo

Regulación específica sobre gestión del RO

La regulación específica debe exigir la generación de información estadística (Procesos rigurosos de gestión)

- Proceso de generación y acumulación de información histórica
- Fuentes de riesgo (personas, procesos, sistemas, eventos externos) y los tipos de eventos, con el propósito de identificar:
 - ✓ los riesgos por líneas de negocio
 - ✓ las estimaciones de pérdidas esperadas e inesperadas
 - ✓ la frecuencia de los eventos de pérdida
 - ✓ la severidad de los eventos de pérdida
 - ✓ la tendencia de los eventos de pérdida.

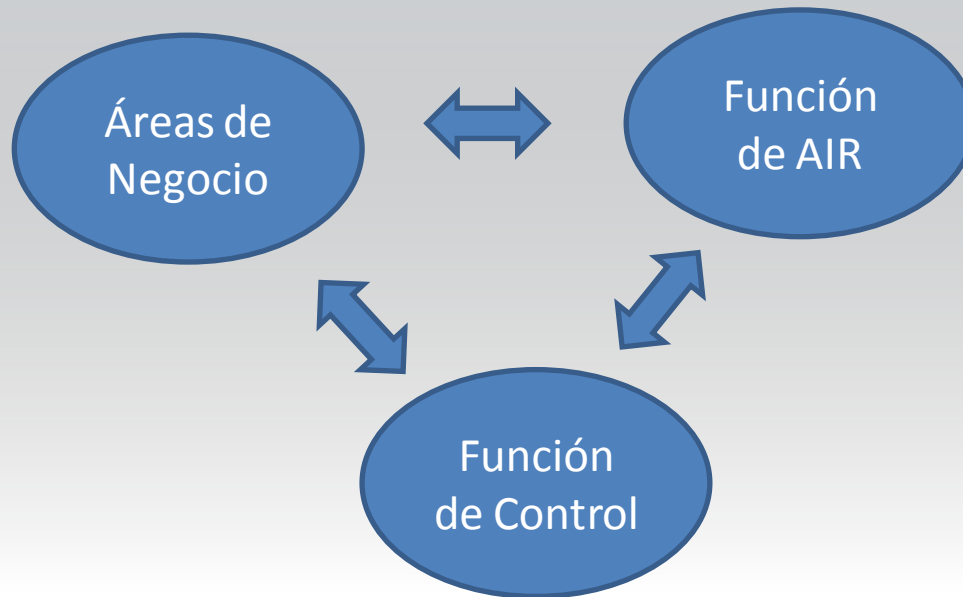
Eventos de Pérdida

1	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 implicado, al menos, un miembro de la empresa, y que tiene como fin obtener un beneficio ilícito.
2	Fraude externo.- Pérdidas derivadas de algún tipo de actuación encaminada a defraudar, apropiarse de bienes indebidamente o incumplir la legislación, por parte de un tercero, con el fin de obtener un beneficio ilícito.
3	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 reclamos por daños personales, o sobre casos relacionados con la diversidad o discriminación.
4	Clientes, productos y prácticas empresariales.- Pérdidas derivadas del incumplimiento involuntario o negligente de una obligación empresarial frente a clientes concretos (incluidos requisitos fiduciarios y de adecuación), o de la naturaleza o diseño de un producto.
5	Daños a activos materiales.- Pérdidas derivadas de daños o perjuicios a activos materiales como consecuencia de desastres naturales u otros acontecimientos.
6	Interrupción del negocio y fallos en los sistemas.- Pérdidas derivadas de interrupciones en el negocio y de fallos en los sistemas.
7	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

Regulación específica sobre gestión del RO

La regulación específica debe exigir un proceso formal y permanente de identificación y evaluación del RO

- Apoyado en una fuerte cultura de gestión del RO
- Actividades, procesos, productos existentes y nuevos



Regulación específica sobre gestión del RO

La regulación específica debe fomentar el desarrollo de bases de datos

- Consideraciones de tamaño, modelo de negocio, volumen o complejidad de operaciones
- Algunos aspectos a incluir :
 - ✓ Código interno de identificación del evento (secuencial).
 - ✓ Línea de negocio /proceso o subproceso asociado
 - ✓ Tipo de evento de pérdida
 - ✓ Descripción del evento.
 - ✓ Fecha de ocurrencia (o de inicio del evento).
 - ✓ Fecha de conclusión del evento.
 - ✓ Fecha de descubrimiento del evento.
 - ✓ Fecha de registro contable del evento.
 - ✓ Monto bruto de la pérdida, moneda y tipo de cambio.
 - ✓ Monto recuperado mediante coberturas existentes de forma previa al evento, moneda, tipo de cambio y tipo de cobertura aplicada.
 - ✓ Monto neto de la pérdida, moneda y tipo de cambio.
 - ✓ Cuenta(s) contable(s) asociadas.

Regulación específica sobre gestión del RO

La regulación específica debe contextualizar la exigencia de una función especializada de gestión del RO

- La función de riesgos es la llamada a abordar el análisis del riesgo operacional
- Mayor grado de especialización para RO según tamaño y complejidad de operaciones
- Labor de la función de riesgos y el Comité: velar la integración de la gestión del RO al proceso de AIR

Regulación específica sobre gestión del RO

La regulación específica debe demarcar la gestión de la continuidad de negocio

- Garantizar, de manera razonable, la capacidad para continuar operando en caso de interrupciones significativas.
- En consonancia con tamaño, complejidad y volumen de las negocio de la entidad.
- Algunos aspectos a considerar:
 - ✓ Alcance a procesos críticos, incluyendo de terceros.
 - ✓ Impacto al negocio.
 - ✓ Plan de contingencia para la continuidad.
 - ✓ Pruebas periódicas de efectividad.
 - ✓ Divulgación y entrenamiento.

Riesgo operativo desde una perspectiva de supervisión

FECOOPSE

Comité Interinstitucional de Riesgos (CIR)

San José, Marzo de 2013

Genaro Segura C., FRM

Principios de Gestión del RO (64 Principios)

SUGEF 24-00 (R-008-2010)

FECOOPSE
Comité Interinstitucional de Riesgos (CIR)

San José, Marzo de 2013

Genaro Segura C., FRM

Marco de regulación vigente – LG-24-00 (R-008-2010)

Tópicos de RO sujetos a supervisión

Principio 34.

- La Junta Directiva ha establecido una definición propia de riesgo operacional que es funcional a la naturaleza de su estrategia de negocios.

Marco de regulación vigente – LG-24-00 (R-008-2010)

Tópicos de RO sujetos a supervisión

Principio 35.

- La Junta Directiva ha identificado los principales riesgos operacionales a que está expuesta.

Marco de regulación vigente – LG-24-00 (R-008-2010)

Tópicos de RO sujetos a supervisión

Principio 36.

- La Junta Directiva ha definido políticas y procedimientos para evitar o mitigar los riesgos operacionales que considera más relevantes.
- Además, las medidas adoptadas para evitar su ocurrencia son proporcionales a la magnitud de ellos.

Marco de regulación vigente – LG-24-00 (R-008-2010)

Tópicos de RO sujetos a supervisión

Principio 37.

- La Junta Directiva, en sus decisiones de sistemas de equipamiento y de software ha evaluado las alternativas tecnológicas concordantes con el modelo de negocios que desarrolla y las tendencias del mercado local e internacional en materia de hardware, software y sistemas de comunicaciones.

Marco de regulación vigente – LG-24-00 (R-008-2010)

Tópicos de RO sujetos a supervisión

Principio 38.

- La Junta Directiva dispone de información actualizada acerca de los incidentes de seguridad sobre riesgos operacionales.

Marco de regulación vigente – LG-24-00 (R-008-2010)

Tópicos de RO sujetos a supervisión

Principio 39.

- La Junta Directiva ha definido políticas y procedimientos para el respaldo de todos sus sistemas de registro de transacciones.
- Los respaldos de los sistemas de registro no están expuestos a los mismos eventos de contingencias de daños que los equipos de producción de la entidad.

Marco de regulación vigente – LG-24-00 (R-008-2010)

Tópicos de RO sujetos a supervisión

Principio 40.

- La Junta Directiva ha definido políticas y procedimientos para la contratación de servicios con terceros concordantes con las normas de seguridad de la entidad

Marco de regulación vigente – LG-24-00 (R-008-2010)

Tópicos de RO sujetos a supervisión

Principio 41.

- La Junta Directiva conoce las contingencias que pueden afectar la continuidad operacional y ha definido políticas y procedimientos para enfrentar contingencias que afectan la continuidad operacional.

Marco de regulación vigente – LG-24-00 (R-008-2010)

Tópicos de RO sujetos a supervisión

Principio 42.

- La unidad de auditoría interna realiza pruebas de eficacia de los procedimientos para enfrentar contingencias de interrupción de la continuidad operacional.

Marco de regulación vigente – LG-24-00 (R-008-2010)

Tópicos de RO sujetos a supervisión

Principio 43.

- La Junta Directiva ha definido políticas de seguridad de información, las que incluyen normas sobre archivo, modificaciones y respaldo de los registros contables y de información de la entidad.

Marco de regulación vigente – LG-24-00 (R-008-2010)

Tópicos de RO sujetos a supervisión

Principio 44.

- La Auditoría Interna de la entidad realiza ejercicios de simulación o pruebas de eficacia de las normas de seguridad

Marco de regulación vigente – LG-24-00 (R-008-2010)

Tópicos de RO sujetos a supervisión

Principio 45.

- La Auditoría Interna de la entidad realiza controles sistemáticos sobre control del riesgo operacional y sus resultados los informa a la Junta Directiva.

Marco de regulación vigente – LG-24-00 (R-008-2010)

Tópicos de RO sujetos a supervisión

Principio 46.

- La entidad ha identificado y conoce los riesgos tecnológicos informáticos a que está expuesta la institución.

Marco de regulación vigente – LG-24-00 (R-008-2010)

Tópicos de RO sujetos a supervisión

Principio 47.

- La entidad dispone de una Estrategia Tecnológica, la que comprende políticas sobre adquisición de Hardware y de Software.

Marco de regulación vigente – LG-24-00 (R-008-2010)

Tópicos de RO sujetos a supervisión

Principio 48.

- El control del cumplimiento de las políticas informáticas es efectuado por una unidad especializada de contraloría interna.

Principios Básicos para una Supervisión Efectiva - Basilea

Principio 26. Control y auditoría internos

FECOOPSE

Comité Interinstitucional de Riesgos (CIR)

San José, Marzo de 2013

Genaro Segura C., FRM

Principios Básicos para una Supervisión Efectiva - Basilea

Principio 26. Control y auditoría internos

- El supervisor **determina** que los bancos cuentan con marcos adecuados de control interno para establecer y mantener un entorno operativo correctamente controlado que facilite la gestión de su negocio, teniendo en cuenta su perfil de riesgo.
- Dichos controles incluyen procedimientos claros sobre delegación de autoridad y atribuciones; separación de las funciones que implican compromisos del banco, desembolso de sus fondos y contabilidad de sus activos y pasivos; conciliación de estos procesos; protección de los activos del banco; y funciones independientes de auditoría interna y de cumplimiento para comprobar la observancia de estos controles, así como de la legislación y regulación aplicables.

Principios Básicos para una Supervisión Efectiva - Basilea

Principio 26. Control y auditoría internos

- Al evaluar la independencia, los supervisores tienen debidamente en cuenta los sistemas de control diseñados para evitar conflictos de intereses al evaluar el desempeño del personal asignado a las funciones de cumplimiento, control y auditoría interna.
- Por ejemplo, las retribuciones de dicho personal deberán determinarse con independencia de las líneas de negocio que supervisen.

Principios Básicos para una Supervisión Efectiva - Basilea

Principio 26. Control y auditoría internos

- La expresión «función de cumplimiento» no necesariamente hace referencia a una unidad organizativa.
- El personal encargado del cumplimiento puede formar parte de unidades de negocio operativas o de filiales locales y puede estar bajo la autoridad de los gestores de una línea de negocio operativa o de una entidad local, siempre y cuando también responda ante el responsable de cumplimiento del banco, el cual deberá ser independiente de las líneas de negocio.

Principios Básicos para una Supervisión Efectiva - Basilea

Principio 26. Control y auditoría internos

- La expresión «función de auditoría interna» no necesariamente hace referencia a una unidad organizativa.
- Algunos países ofrecen a pequeños bancos la opción de aplicar a los controles internos esenciales un sistema de exámenes independientes, por ejemplo realizados por expertos externos.

Principios Básicos para una Supervisión Efectiva - Basilea

Principio 26. Control y auditoría internos

Criterio Esencial 1

- La legislación, la regulación o el supervisor **exigen** que los bancos dispongan de marcos adecuados de control interno con el fin de crear un entorno operativo correctamente controlado para la gestión del negocio, teniendo en cuenta su perfil de riesgo.
- Estos controles, cuya responsabilidad recae en el Consejo y/o la alta dirección, se aplican a la estructura organizativa, las políticas y procesos contables, los sistemas de pesos y contrapesos y la salvaguardia de activos e inversiones (incluidas medidas para la prevención, detección temprana y notificación de abusos como fraude, malversación, operaciones no autorizadas e intrusiones informáticas).

Principios Básicos para una Supervisión Efectiva - Basilea

Principio 26. Control y auditoría internos

Criterio Esencial 1

- En concreto, los controles se aplican a:
 - (a) la **estructura organizativa**: definición de deberes y obligaciones, con una clara delegación de la autoridad (por ejemplo, límites inequívocos a la aprobación de préstamos), políticas y procesos para la toma de decisiones, segregación de funciones críticas (por ejemplo, originación de operaciones, pagos, conciliación, gestión del riesgo, contabilidad, auditoría y cumplimiento);
 - (b) **políticas y procesos contables**: conciliación de cuentas, listados de control, información para la gerencia;
 - (c) **sistemas de pesos y contrapesos** (el «principio de los cuatro ojos»): segregación de tareas, cotejo, doble control de activos, firmas dobles; y
 - (d) **salvaguardia de activos e inversiones**: incluido el control físico y el acceso a sistemas informáticos.

Principios Básicos para una Supervisión Efectiva - Basilea

Principio 26. Control y auditoría internos

Criterio Esencial 2

- El supervisor **determina** que existe un adecuado equilibrio entre las competencias y recursos del back-office, funciones de control y gestión operativa con relación a las de las unidades donde se originan las operaciones.
- El supervisor también **determina** que el personal de las funciones de registro operativo y control tiene capacitación y autoridad suficiente dentro de la organización (y, cuando corresponda, en el caso de las funciones de control, suficiente acceso al Consejo del banco) para constituir un efectivo contrapeso de las unidades donde se originan.

Principios Básicos para una Supervisión Efectiva - Basilea

Principio 26. Control y auditoría internos

Criterio Esencial 3

- El supervisor **determina** que el banco cuenta con una función de cumplimiento permanente, independiente y dotada del personal adecuado que auxilia a la alta dirección en la gestión eficaz de los riesgos de cumplimiento a los que se enfrenta el banco.
- El supervisor **determina** que el personal de la función de cumplimiento cuenta con la formación adecuada, tiene experiencia relevante y dispone de autoridad suficiente dentro de la entidad para desempeñar eficazmente sus funciones.
- El supervisor **determina** que el Consejo realiza un seguimiento de la gestión de la función de cumplimiento.

Principios Básicos para una Supervisión Efectiva - Basilea

Principio 26. Control y auditoría internos

Criterio Esencial 4

- El supervisor **determina** que los bancos cuentan con una función de auditoría interna independiente, permanente y eficaz, encargada de:
 - (a) evaluar si las políticas, procesos y controles internos existentes (incluidos los procesos de gestión del riesgo, cumplimiento y gobierno corporativo) son eficaces, adecuados y continúan siendo suficientes para la actividad del banco; y
 - (b) garantizar el cumplimiento de las políticas y procesos.

Principios Básicos para una Supervisión Efectiva - Basilea

Principio 26. Control y auditoría internos

Criterio Esencial 5

- El supervisor **determina** que la función de auditoría interna:
 - (a) tiene recursos suficientes y personal capacitado y con adecuada experiencia para comprender y evaluar la actividad que está auditando;
 - (b) goza de adecuada independencia, con líneas de comunicación con el Consejo del banco o con un comité de auditoría del Consejo, y suficiente estatus dentro del banco para garantizar que la alta dirección reacciona ante sus recomendaciones y actúa en consecuencia;
 - (c) se mantiene puntualmente informada de cualquier cambio significativo en las estrategias, políticas o procesos para la gestión del riesgo del banco;
 - (d) tiene pleno acceso y comunicación con todos los miembros del personal, así como acceso a los archivos, ficheros o datos del banco y sus compañías afiliadas, siempre que sea relevante para el desempeño de sus tareas;
 - (e) aplica una metodología que identifica los riesgos significativos a los que se enfrenta el banco;
 - (f) prepara un plan de auditoría, periódicamente revisado, basado en su propia evaluación de riesgos y asigna sus recursos en consecuencia; y
 - (g) está autorizada a evaluar cualquier función subcontractada.