ISSN 1813-6494

Documentos Ocasionales

Gestión de riesgos de negocio. Desarrollo e Implementación de Sistemas de Gestión de Riesgos

No. 2009-01

BANCO CENTRAL DE RESERVA DE EL SALVADOR

Banco Central de Reserva de El Salvador

Gestión de riesgos de negocio. Desarrollo e Implementación de Sistemas de Gestión de Riesgos

Luis Ernesto Cañas Pacheco

Documentos Ocasionales No. 2009-01

2009

Departamento de Investigación Económica y Financiera
Banco Central de Reserva de El Salvador
Alameda Juan Pablo II, entre 15 y 17 Avenida Norte
San Salvador, El Salvador, C. A.

El Banco Central al publicar esta serie de Documentos Ocasionales, pretende facilitar la difusión de estudios económicos y financieros que contribuyan al mejor conocimiento de la realidad salvadoreña.

Las interpretaciones, análisis y conclusiones de estos trabajos representan las ideas de los autores y no coinciden necesariamente con el criterio de este Banco Central.

ISSN 1813-6494

RESUMEN

Este trabajo explora el desarrollo, implementación, mantenimiento y monitoreo de los sistemas de gestión de riesgos de negocio, en vista de los beneficios que le confiere a la entidad, independientemente de su naturaleza, tamaño e industria en la que participa.

En esa perspectiva, la gestión de riesgos se convierte en un elemento importante de la estrategia corporativa y del proceso de toma de decisiones de la entidad, y es bajo esta filosofía, que la gestión de riesgos debe ser una tarea a realizar por cualquier entidad, y en torno a la cual se deben estructurar el resto de funciones, puesto que su utilidad e importancia, confiere a la entidad la garantía razonable del cumplimiento de las estrategias y directrices de alto nivel.

La gestión de riesgos debe considerarse una función primordial y uno de los componentes claves a ser tomado en cuenta desde el proceso de planificación estratégica por todos los estamentos de la organización. Se propone el desarrollo e implementación de un Sistema de Gestión de Riesgos, a fin de lograr un menor grado de incertidumbre en el cumplimiento de los objetivos estratégicos de toda empresa.

ABSTRACT

This paper explores the development, implementation, maintenance and monitoring of risk management systems business, given the benefits it confers on the entity, regardless of its nature, size and industry in the participating.

In this perspective, risk management becomes an important element of corporate strategy and of the decision-making process within an entity, and it is under this philosophy that risk management should be a task for any entity, and around which should be structured all other functions, given that its usefulness and importance provides the entity with a reasonable assurance that the guidelines and strategies coming from higher management will be complied with.

Risk management should be considered as a critical activity and one of the key components to be taken into account in the strategic planning process by all levels within the organization. It is proposed that the development and implementation of a Risk Management System, in order to reduce the uncertainty level in meeting the strategic objectives of any enterprise.

CONTENIDO

Introducción

La última década del siglo XX y la primera del XXI, se han caracterizado por cambios vertiginosos en la tecnología; los medios de comunicación y de transporte, están modificando drásticamente la forma de hacer negocios. Cuando se afirma que se ha modificado la forma de hacer negocios, se debe tomar en cuenta que a la par de estas, los riesgos también han evolucionado y modificado su forma de manifestarse. Esto reafirma que el riesgo forma parte integral e inherente de toda actividad, y por lo tanto, la clave está en gestionarlos de forma eficaz y eficiente.

Los riesgos de negocio tienen diferente origen. La misma naturaleza, con terremotos, huracanes, inundaciones; de tecnología asociados a fallos en los sistemas, acceso de intrusos y fallos, deficiencias en los medios de comunicación, disposiciones legales y políticas (riesgo país), en la planificación, financieros y de imagen o reputacional. Este último es quizá, el riesgo más determinante, ya que su ocurrencia incide en la percepción y credibilidad de las personas y organismos internacionales, acerca del funcionamiento de la institucionalidad de un país.

Estándares internacionales como Basilea II que aplica el Sistema Financiero, clasifica los riesgos en tres categorías: de crédito, operativo y de mercado. Esta investigación analiza el riesgo puro desde la perspectiva del negocio, e incluye las categorías antes enunciadas. En ese sentido, se ha hecho una revisión bibliográfica sobre teorías que nos permite comprender, qué es el riesgo, técnicas y herramientas empleadas para su gestión, como la empleada por el FED, por Australia-Nueva Zelanda, entre otros.

El análisis y evaluación de los riesgos, se describe como etapa previa al tratamiento de los riesgos, en esta se identifican los riesgos que pueden afectar e incidir en el cumplimiento de los objetivos y metas estratégicas de la entidad, afectando los resultados previstos. Se detallan las opciones de tratamiento que se adoptan para gestionarlos como son evitar, reducir, compartir y aceptar.

La experiencia ha demostrado que el efecto de los riesgos se puede minimizar y difícilmente eliminar; ese remanente no cubierto se denomina riesgo residual, del cual se deriva el riesgo tolerable el cual está dispuesto a aceptar/asumir la Alta Dirección, y que previamente ha evaluado que la materialización de este evento no afectará la continuidad normal del negocio.

La investigación concluye describiendo los beneficios que se generan de la gestión integral de los riesgos, la cual en esencia agrega valor a la entidad y beneficios futuros. Asimismo, a fines de facilitar la comprensión de la terminología utilizada a lo largo del documento, se incluye un glosario.

I. Riesgos. Su incidencia en los objetivos y metas estratégicas

Cuando se hace referencia al término ***riesgo,*** generalmente se refiere a “aquellos eventos o acontecimientos que adversamente impactan los objetivos y metas estratégicas de toda entidad”. La misión, visión y valores de una entidad, se traducen en metas y objetivos, los cuales, luego de gestionarse a través de un proceso formalmente establecido, se convierten en un producto final: beneficios futuros, de interés particular o común.

¿Es importante para una organización saber a que se enfrenta?, la respuesta es si, ya que no es posible perder de vista que algo puede salir mal o al menos, que el resultado no sea el que se había estimado, o al menos no de forma óptima, en esto la suerte nada tiene que ver. Todo esfuerzo que se hace, destinado a lograr lo que se ha programado, debería prever aquellos posibles eventos que pudiesen impedir o modificar los resultados respecto de lo previsto.

Es bajo esa perspectiva, que para lograr esas metas u objetivos, se deben conocer esos eventos adversos (elementos o factores, internos y externos) que en un momento determinado no permiten dar en el blanco, al cual todos los recursos (personal, económicos-financieros, equipos, etc.) se alinearon.

La identificación y el análisis de los riesgos, requieren del involucramiento de toda la organización, desde el más alto nivel hasta los niveles inferiores, lo que implica conocer lo que se hace, cómo se hace y para que, su comprensión marca la pauta respecto a lo que nos enfrentamos en el día a día.

A. ¿Qué es el riesgo?

Existen muchas definiciones de riesgo, una definición propia y sencilla sería: *"La probabilidad de que, la ocurrencia de un suceso adverso afecte a la entidad e impacte en su habilidad para lograr sus objetivos estratégicos y por ende la capacidad de cumplir su misión y visión".*

Soler et al. (1999), definen el riesgo como ***"la posibilidad de sufrir un daño"***, su libro "Gestión de Riesgos Financieros: un enfoque práctico para países latinoamericanos" se enfoca a riesgos de tipo económicos-financieros, por lo tanto el daño consiste en pérdidas de valor económico.

También el riesgo se concibe como: *"Amenazas que se originan por circunstancias, que pueden afectar adversamente la habilidad de la organización para lograr sus objetivos y ejecutar sus estrategias";* otros lo consideran como una ***"medida de incertidumbre"***, debido a la complejidad de predecir la probabilidad de ocurrencia y la medición del efecto o impacto sobre la entidad.

Los riesgos tienen origen o provienen de fuentes internas y externas. Son de fuente interna aquellos relacionados con el ambiente de control y los procesos operativos, es decir, las personas y el uso adecuado de los recursos (físicos, tecnológicos y económicos-financieros).
Las personas son el componente principal, el capital intelectual apenas medible, que desarrolla e interactúa con el Sistema de Control Interno (SCI), el cual se diseña para responder de forma anticipada a la materialización de los riesgos y otros eventos adversos, previstos y no previstos, con mayor grado de certeza. Son de fuente externa los riesgos relacionados con las operaciones o actividades propias, es decir, aquellos que ocurren durante el desarrollo normal del giro del negocio.

"La valoración de los riesgos es la identificación y análisis de los riesgos relevantes para la consecución de los objetivos, formando una base para la determinación de cómo deben gestionarse los riesgos".[1] Además de identificar y analizar los riesgos, estos se deben clasificar, medir y controlar.

[1] Mantilla B., Samuel A. (2003), Pág. 39.

La Identificación y clasificación de los riesgos, representa una ardua tarea. Su clasificación se puede realizar categorizándolos por su naturaleza y de acuerdo a su relevancia. Se clasifican en Riesgos de Alto Nivel o Macroriesgo, y Factores de Riesgos, estos últimos son aquellas causas específicas derivadas de los primeros. Los Macroriesgos y los Factores de Riesgo, conforman la Matriz de Riesgos de la entidad.

Análisis. Luego de identificar los riesgos se debe hacer análisis de cada uno; esta etapa del proceso es compleja, principalmente por las dificultades que representa la cuantificación de sus efectos, para lo cual se debe investigar, recopilar datos y documentar, aquellas experiencias que previamente ha enfrentado la entidad u otras entidades (que podrían ser de su misma naturaleza o que realicen funciones similares), ello permitirá establecer estimaciones con una mayor precisión.

Medición. Cuando no fuese posible contar con registros o información histórica (en bases de datos o archivos físicos) sobre los efectos adversos que en un momento determinado se materializaron, la medición de los riesgos se hace a partir de la naturaleza de los procesos, es decir el ***riesgo inherente***, por lo tanto, se establecen *Parámetros y Escalas*, para el caso: la **Probabilidad** puede ser Cierta o Acertada, Muy probable, Probable, Posible, Remoto y Poco probable o Escasamente probable; por otro lado el **Impacto** en Severo, Alto, Medio, Bajo y Leve. La combinación de la Probabilidad entre el Impacto nos da como producto la Criticidad, la cual explica que tanto se está expuesto a un riesgo.

Control. Controlar los riesgos no implica únicamente establecer Actividades de Control, significa evaluar el funcionamiento del sistema de control interno, a través de ejercer un monitoreo permanente "ongoing"[2], documentando y registrando esos eventos, los cuales ayudan a establecer las probabilidades de ocurrencia y el impacto de los riesgos.

B. ¿Cómo se manifiestan los riesgos?

Los riesgos se presentan o manifiestan de muchas formas, desde pérdida en la efectividad de los procesos (eficiencia y eficacia), en las operaciones, disminución en la participación en el mercado por pérdida en la preferencia de los clientes o usuarios, deterioro de imagen (mala reputación), deficiencias en las estrategias de las inversiones, sistemas y tecnología de información que no apoyan razonablemente el cumplimiento de los objetivos estratégicos y metas, y la continuidad de las operaciones, todas sin excepción tienen efecto económico-financiero para toda entidad.

Estas manifestaciones, de forma simple, no son más que el efecto e impacto. El efecto se refiere a las consecuencias y el impacto a las pérdidas materiales o cuantías, que no solamente afectan a la entidad misma, también a terceros interesados o usuarios de la entidad.

[2] Ongoing es un término técnico ampliamente conocido, que significa: estar actualmente en proceso, que se está moviendo continuamente hacia adelante, crecientemente. Es lo que también se denomina en tiempo real: en la medida que ocurren los acontecimientos. Ibíd. 1, Pág. 6.

II. La base del Sistema de Gestión de Riesgos

La gestión de los riesgos implica cambios en la toma de decisiones, en la forma de gerenciar, en la eliminación de ciertos paradigmas y creación de la cultura de gestión de riesgos, en todos los niveles de la entidad, iniciando en la alta dirección alcanzando hasta el último nivel de la entidad. Gestionar los riesgos requiere del establecimiento formal de un proceso que permita de forma clara, técnica y sencilla la evaluación y análisis de los riesgos.

Para establecer el proceso de gestión de riesgos, la alta dirección debe estar plenamente convencida que para el fortalecimiento de los procesos de la entidad que gobiernan, es necesario analizar y evaluar los riesgos. Identificar los riesgos, es una labor que requiere de una comprensión exhaustiva del entorno interno y externo en el cual se realiza el proceso.

Definición. La Gestión de Riesgos Corporativos o ERM (Enterprise Risk Management)[3], consta de ocho componentes relacionados entre sí, los cuales se derivan de la manera en que la alta dirección conduce la empresa y como se integran en el proceso en el proceso de gestión.

A continuación se describen los elementos de control interno, según la estructura presentada en el Informe COSO[4] - ERM, conocido como COSO II:

A. Ambiente interno

"El ambiente de control establece el tono de la organización, para influenciar la conciencia de control de su gente. Es el fundamento de todos los demás componentes del control interno, proporcionando disciplina y estructura. Los factores del ambiente de control incluyen la integridad, los valores éticos y la competencia de la gente de la entidad…" [5]

El ambiente de control es más que la manera de cómo se estructuran los negocios, de cómo se establecen los objetivos y se valoran los riesgos. Es la conducta de las personas, la influencia del pensamiento estratégico sobre las personas, es decir, los valores éticos, la moralidad, la entrega de la gente a las funciones que se le confieren y la convicción del más alto funcionario, la filosofía y el funcionamiento que propicia el control interno para el desarrollo de las actividades.

El control interno se debe definir como el proceso realizado por la máxima autoridad, los administradores y demás personal, diseñado para proporcionar seguridad razonable para el cumplimiento de los objetivos.[6]

[3] Committee of Sponsoring Organizations of the Treadway Commission (COSO), Instituto de Auditores Internos de España – PriceWaterHouseCoopers, septiembre 2004, Pág. 28.

[4] Committe of Sponsoring Organizatios of the Treadway Commission (COSO)

[5] Ibíd. 1, Pág. 26

[6] Ibíd. 1, Pág. 6

B. Los objetivos estratégicos y el riesgo

Los riesgos son inherentes a los negocios y por ende a los procesos que permiten desarrollar. Los objetivos deben de existir antes de que la Alta Dirección pueda identificar potenciales eventos que afecten su consecución. Estos objetivos cuidadosamente seleccionados deben estar alineados con la misión y visión institucional y estar a tono con el riesgo aceptado por la entidad.

Instituciones como los Bancos Centrales, al igual que empresas públicas y privadas, sin importar su tamaño o actividad mercantil, establecen objetivos y metas estratégicas. Los objetivos, se pueden clasificar en tres categorías: de Operaciones, de Información Financiera y de Cumplimiento:

1. **Operaciones.** Estos objetivos se relacionan con la consecución de la misión de la entidad, su razón de ser. Están dirigidos a fortalecer la eficiencia de las operaciones y orientan a la entidad hacia sus metas previstas.

2. **Información financiera.** Se refiere a que los Estados financieros de la entidad, informes internos, datos y aún los registros auxiliares sean confiables. La importancia de este objetivo radica en que esta información es utilizada por diferentes usuarios para distintos propósitos.

3. **Cumplimiento.** Todas las actividades, actuaciones y acciones específicas que realiza una entidad, responden a un marco legal, a leyes y regulaciones aplicables. Estas regulaciones pueden ser de índole interna de un país, propias de la entidad e internacionales por haber sido adoptadas por la entidad y por la naturaleza misma de las operaciones o actividades que realiza.

Los objetivos de una categoría pueden cubrir o soportar objetivos de otras, por lo tanto los riesgos que pudiesen afectar a uno, tienen efecto sobre otro o el resto, lo que puede desencadenar un proceso de tipo “dominó”, puesto que los objetivos estratégicos están vinculados entre sí, y se han establecido para cumplir la misión de la entidad.

C. Identificación de eventos. Determinación del origen de los riesgos

En la identificación del origen de esos eventos (internos y externos) que afectan los objetivos y metas de la entidad, se debe tener el cuidado de identificar y clasificar los riesgos y separar las oportunidades. Estas últimas pueden permitir a la entidad descubrir mayores fortalezas que de otra manera no habría descubierto, modificar sus estrategias y la forma de hacer sus negocios, podrían también implicar cambiar procesos complejos a formas más simples u optimizar otros productos e información que antes no le generaban mayor utilidad.

Respecto a los riesgos, la identificación proporciona un mapa global de los riesgos que pudiesen afectar cada proceso.

D. Evaluación de riesgos

Los riesgos se deben analizar considerando su probabilidad e impacto, que a través de escalas, proporciona una medición preliminar, como base para determinar cómo deben ser gestionados. Los riesgos se evalúan en dos fases, desde la perspectiva inherente y residual, la primera por la naturaleza del riesgo, la segunda considera la intervención o efecto de los controles sobre el riesgo.

El impacto de un riesgo se puede definir como las consecuencias que desencadena la materialización de un riesgo y la probabilidad de ocurrencia; esta última puede medirse con criterios de frecuencia, algunos la miden en períodos de tiempo y en épocas o temporadas del año, cuando su ocurrencia proviene de un comportamiento estacional. De la combinación de estos elementos se obtiene como resultado la Criticidad o nivel de exposición al riesgo de un proceso, operación o actividad.

E. Definición del riesgo aceptable por la administración

Riesgo Inherente. Es aquel existente por la naturaleza de la operación o actividad en ausencia de las acciones de la dirección para modificar su probabilidad e impacto.

Riesgo residual. Se considera que el Sistema de Control Interno (SCI) de una entidad puede juzgarse como efectivo, cuando las actividades de control responden de forma preventiva a los eventos adversos. No obstante lo anterior, independientemente de la efectividad del SCI, no es posible eliminar un riesgo. Los controles permiten reducir el efecto de los riesgos, de manera que la parte que no es cubierta, se denomina Riesgo Residual.

El riesgo residual es el que permanece aún después de la aplicación de los controles, y es la Alta Dirección la que formalmente establece el riesgo que está dispuesta a asumir, es decir, declarar lo que se conoce como “apetito al riesgo” o “riesgo tolerable”, ya que sus incidencias son calculadas y asumidas por la administración y estiman que de ocurrir su efecto no impide la continuidad del negocio.

F. Respuesta al riesgo

Ante los riesgos se pueden tomar diferentes posiciones, se pueden Evitar, Reducir, Compartir y Aceptar.[7]

Evitar. Se evita un riesgo, cuando la alta dirección toma la decisión de no realizar aquellas actividades que generan riesgos, esto podría significar, el cese de una línea de producto, dejar de dar un servicio, frenar la expansión hacia un nuevo mercado geográfico o la venta de una división, en la mayoría de los casos esto no es posible, cuando estas representan el giro o actividad principal de la entidad.

Reducir. Implica llevar a cabo acciones necesarias tendientes a reducir la probabilidad o el impacto del riesgo o ambos conceptos a la vez. Reducir implica llevar los riesgos a niveles tolerables o aceptables por la Máxima Autoridad de la Entidad, es decir, la definición del “apetito del riesgo” a partir del riesgo residual.

Compartir. La probabilidad y el impacto del riesgo se reducen trasladando la gestión del riesgo o compartiendo una parte de este con un tercero. Las técnicas comunes utilizadas para compartir riesgos incluyen, por ejemplo: la contratación de seguros, la realización de operaciones de cobertura o la externalización de una actividad.

---

[7] Committe of Sponsoring Organizations of the Treadway Comisión (COSO)(2004), Gestión de Riesgos Corporativos, Instituto de Auditores Internos de España-PriceWaterHouseCoopers, Pags. 71-72.

Aceptar. No se emprende ninguna acción que afecte a la probabilidad o el impacto. La Máxima Autoridad ha estimado la materialización del riesgo por su consecuencia (probabilidad e impacto), valora que ese evento no afectará de forma importante a la entidad, por lo que decide no emprender ninguna acción relevante para mitigarlo.

G. Actividades de control

Como se ha señalado, el Sistema de Control Interno (SCI), ha sido diseñado con acciones preventivas, correctivas y detectivas, como respuesta ante la materialización de los riesgos. Se identifica y percibe a través de las Actividades de Control (AC), las cuales se definen explicita e implícita en "las políticas y los procedimientos que ayudan a asegurar que se están llevando a cabo las directivas administrativas."[8]

Las AC se realizan a lo largo del desarrollo de cada proceso de negocio y en todos los niveles de la estructura de la organización, en todas las actividades y en todas las funciones. De acuerdo a su propósito pueden ser aprobaciones, autorizaciones, verificaciones, reconciliaciones, revisión del desempeño de operaciones, seguridad de activos y segregación de funciones.

Cualquiera que sea la naturaleza de las Actividades de Control, su objetivo es mitigar los riesgos, ello significa que a través de estas se da un tratamiento a los riesgos, aún cuando la gestión del riesgo es trasladada a un tercero (compartir el riesgo) se debe considerar una AC.

H. Efectividad de los controles

Al igual que la probabilidad e impacto de los riesgos, las actividades de control se pueden medir en probabilidad e impacto en cuanto a su efectividad.

Cuando se determina la Criticidad o nivel de exposición al riesgo, esta se enfrenta con los controles; si los controles cubren la mayor parte del riesgo identificado, estos podrían calificarse como efectivos. En algunos casos los controles se diseñan para cubrir una parte del riesgo, es decir, que por lo menos una etapa o actividad del proceso puede cubrirse efectivamente. No debe perderse de vista, que no es posible eliminar del todo un riesgo, sin embargo, la parte no cubierta podría considerarse sin mayor trascendencia y el proceso del negocio se puede continuar realizando sin mayores dificultades. Esa parte no cubierta de un riesgo debe estar totalmente identificada por la Administración y calificado formalmente como tolerable o aceptable, es decir, fijar el apetito por el riesgo.

El término Efectividad es la calificación ponderada del control y se traduce en eficiencia y eficacia de los controles sobre la criticidad de un riesgo. Esta labor implica la vinculación de cada AC con el riesgo que esta cubre, además, una misma AC puede cubrir más de un riesgo de una misma o diferente categoría.

I. Información y comunicación

La información, se debe de calificar y clasificar, a fin de identificar aquella con carácter relevante, captarla y comunicarla en forma y en el plazo oportuno para permitir al personal afrontar sus responsabilidades.

[8] Ibíd. 3 Pág. 59

La comunicación eficaz por su lado, debe producirse en un sentido amplio, fluyendo en todas las direcciones de la entidad sin sufrir modificaciones que puedan afectar, lo que la Alta Dirección quiere trasladar a todos y cada uno de los niveles de la organización, de igual forma la comunicación para propósitos externos, al igual que la interna debe llegar a través de los canales que se han definido y a los usuarios definidos interesados.

"Los sistemas de información, deben diseñarse tal que puedan producir información de utilidad para la entidad, estos documentos contienen información de tipo operacional, financiera, de cumplimiento y del mismo funcionamiento de los sistemas y tecnología de información, con la cual se opera y controla el negocio; representan sucesos, actividades y condiciones externas necesarias para la toma de decisiones y la información externa de negocios..."[9]

J. Supervisión (monitoreo)

El funcionamiento del Sistema de Control Interno y de Gestión de los riesgos se debe supervisar permanentemente, realizando las modificaciones oportunas cuando se perciba sea necesario. Esta supervisión se debe realizar mediante actividades permanentes definidas por la Alta Dirección y ejecutadas por los dueños de los procesos, asimismo, se deben realizar evaluaciones independientes (auditorías) o ambas actuaciones a la vez.

La Supervisión debe efectuarse en el curso de las operaciones, en tiempo real, reacciona de modo dinámico a las condiciones cambiantes y está integrada a la entidad. El alcance y la frecuencia de las evaluaciones dependerá primariamente de la valoración de los riesgos y de la efectividad de los procedimientos de monitoreo.

III. Técnicas y Metodologías para la gestión de los riesgos

Las metodologías para la gestión de los riesgos usadas a nivel mundial, coinciden en que el empleo de estas de forma planificada a través de un proceso formal, fortalecen las operaciones y procesos de las entidades, independientemente del tamaño o actividad empresarial.

Como consecuencia del empleo de herramientas para la gestión de los riesgos, se provoca un fortalecimiento del sistema de control interno. En orden lógico se deben identificar y analizar los riesgos, luego se diseñan y establecen formalmente las actividades de control necesarias para responder ante los riesgos. La característica que debe poseer toda actividad de control es que su beneficio sea superior a su costo o gasto de implementación.

A. Metodologías de gestión de riesgos

La implantación de sistemas de gestión de riesgos, comenzó a tomar relevancia desde la década de los noventas, período en que fue necesario reconvertir y replantear la forma de hacer negocios, como consecuencia de la ocurrencia de fraudes a importantes entidades, defraudando la confianza del público en general; su impacto a nivel mundial desencadenó una serie de medidas que conlleva a mejores prácticas, tendientes a evitar fraudes de cualquier naturaleza; se emitieron sendos documentos técnicos y en algunos países, consideraron emitir leyes. Ejemplo de ello, los informes de COSO y Ley Sarbanes-Oxley, entre otras.

[9] Ibíd. 1 Pág. 71

Como parte del esfuerzo de la implementación de Sistemas de Gestión de Riesgos, en algunos países ha sido necesario el involucramiento de los Órganos del Estado, emitiéndose Leyes sobre Control Interno y Administración de Riesgos, generalmente para ser aplicados en Instituciones Públicas, pero por su naturaleza, estos Instrumentos Normativos pueden ser aplicados y tomados como punto de referencia por empresas privadas.

Entre las entidades que realizan importantes esfuerzos para la gestión de los riesgos, están los bancos centrales, por su naturaleza, rol y responsabilidades que cumplen en los países son llamados a ser eficientes y eficaces en el manejo de los recursos, tanto propios como del público, y principalmente por este último, se hace necesario mantener una imagen y reputación muy alta de confianza y prestigio que gozan. Para estas entidades gestionar los riesgos suele ser una práctica diaria, la observancia y control de los riesgos inherentes de sus procesos les otorga una garantía razonable del cumplimiento de sus objetivos y metas.

A fin de ejemplificar metodologías para Gestión de Riesgos, se han tomado de referencia las siguientes:

1. AS/NZS 4360:1999, Estándar Australiano para la Administración de Riesgos.
2. Metodología de Riesgos U.S. Federal Reserve Banks. (1994 revisión más reciente)
3. Gestión de Riesgos Corporativos – Marco Integrado, COSO-ERM
4. Basilea II: Nuevo enfoque basado en tres pilares.

Descripción de las metodologías:

1. AS/NZS 4360:1999, Estándar Australiano para la Administración de Riesgos

Este modelo parte de la necesidad de desarrollar una política organizacional de administración de riesgos y de un mecanismo de soporte, con el objeto de proveer una estructura para llevar a cabo un programa de administración de riesgos más detallado a nivel sub-organizacional o de proyecto.

Para el establecimiento de dicha política es necesario que el ejecutivo de la organización defina y documente su política de administración de riesgos, incluyendo objetivos para, y su compromiso con, la Administración de Riesgos. Esta política debe ser relevante para el contexto estratégico de la organización, sus metas, objetivos y naturaleza de negocio, asegurándose que es comprendida, implementada y mantenida en todos los niveles de la organización.

La metodología requiere establecer el compromiso gerencial, los niveles de responsabilidad y autoridad, recursos necesarios, programa de implementación y la correspondiente revisión gerencial.

Los elementos principales del proceso de administración de riesgos, se describen a continuación:

I) Establecer el contexto. Implica establecer el contexto estratégico, organizacional y de administración de riesgos en el cual tendrá lugar el resto del proceso. Deberán en este punto establecerse los criterios contra los cuales se evalúan los riesgos y la definición de la estructura del análisis.

II) Identificar riesgos. Identificar qué, por qué y cómo pueden surgir las cosas, como base para el análisis posterior.

III) Analizar riesgos. Determinar los controles existentes y analizar riesgos en términos de consecuencias y probabilidades en el contexto de esos controles. El análisis debería considerar el rango de esas consecuencias potenciales y cuán probable es que ocurran. La combinación de consecuencias y probabilidades pueden producir un nivel estimado de riesgo.

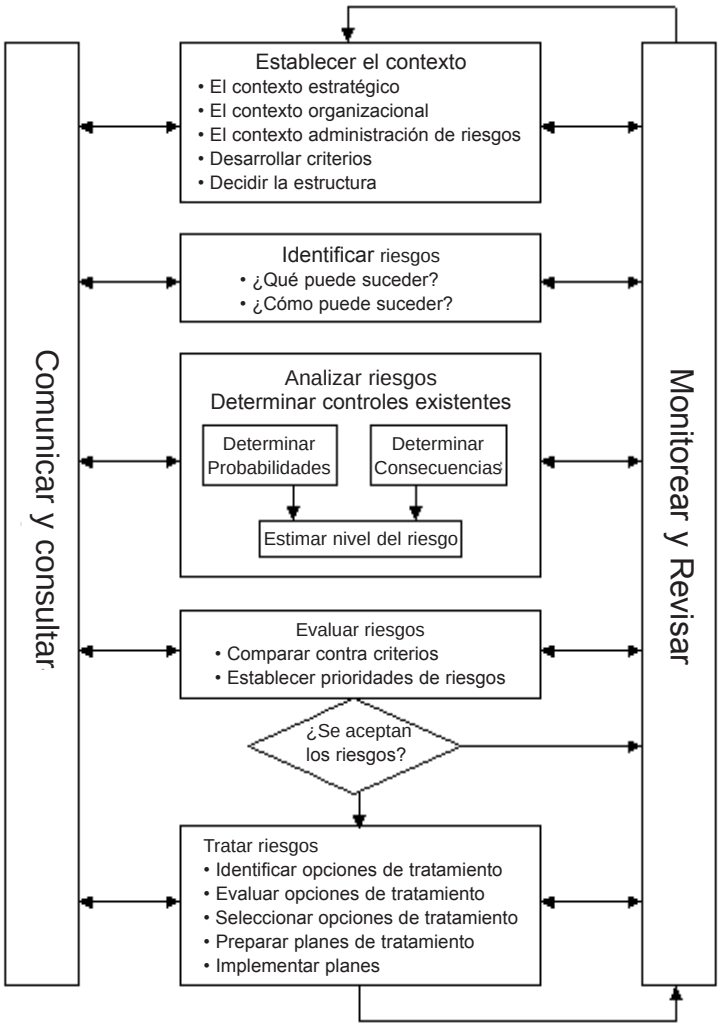
IV) Evaluar riesgos. Comparar niveles estimados de riesgos contra los criterios preestablecidos. Esto posibilita que los riesgos sean ordenados como para identificar las prioridades de administración. Si los niveles de riesgo establecido son bajos, los riesgos podrían caer en una categoría aceptable y no se requerirá un tratamiento.

V) Tratar los riesgos. Aceptar y monitorear los riesgos de baja prioridad. Para otros riesgos, desarrollar e implementar un plan de administración específico que incluya consideraciones de fondeo.

VI) Monitorear y revisar. Se hace necesario el monitoreo y la revisión permanente del desempeño del sistema de administración de riesgos y los cambios que podrían afectarlo.

VII) Comunicar y consultar. Es necesario comunicar y consultar a los interesados internos y externos, según corresponda, en cada etapa del proceso de administración de riesgos. La administración de riesgos se puede aplicar en una organización a muchos niveles, los niveles estratégicos y operativos, proyectos específicos. Llevar registros adecuados concernientes a la administración de riesgos, suficientes como para satisfacer a las evaluaciones independientes.

En la siguiente figura se resume el proceso de administración de riesgos que propone el Estándar Australiano/Nueva Zelanda:



2. Metodología de Riesgos U.S. Federal Reserve Banks. (1994 versión disponible)

La metodología de riesgos del FRB parte de un nuevo paradigma, señalando que:

- La evaluación de riesgo es continua.
- La evaluación de riesgos anticipa y previene.
- La evaluación de riesgos se enfoca en la identificación, medición y control de riesgos, velando que la organización logre los objetivos con un menor impacto de riesgos posible.
- La evaluación de riesgos está integrada en todas las operaciones y líneas de negocios.
- La política de evaluación de riesgos es formal y claramente entendida.

El proceso general de evaluación de riesgos se describe a continuación:

1. Definir las actividades de auditoría en el universo de proceso
2. Desarrollar los perfiles del negocio
3. Identificar los riesgos y asignar puntajes según la escala definida
4. Clasificar las actividades de auditoría de acuerdo al riesgo
5. Programar la cobertura de auditoría basado en la evaluación de riesgo

A continuación se presenta la estructura del proceso de evaluación de riesgo de la US Federal Reserve Bank:

PROCESO DE LA EVALUACIÓN DEL RIESGO

1. Define actividades en el universo de auditoría

Actividades intervenibles

Empresa	**Distrito**
Aplicaciones de central	Aplicaciones únicas de distrito
Proyectos de sistemas	Servicios de Central Bank
	Servicios Financieros

2. Para Desarrollar Perfiles de Negocio

Riesgo de Operaciones	Riesgo Financiero	Riesgo de información de Tecnología	Información para el riesgo de Toma de Decisiones	Riesgo de Recursos Humanos
Cambio Complejidad y lo crítico Cumplimiento y controles	Ingresos y gastos Características Monetarios de contabilidad	Ambiente de automatización Confiabilidad	Reporte Financiero Control Confiabilidad	Estructura de la Organización Política y Procedimiento

3. Puntaje de Riesgo

Matriz de Puntaje

Puntajes asignados a cada factor

4. Clasificación de Riesgo

Clasificación Absoluta

Puntajes totales clasificados en orden de magnitud

5. Para programar la cobertura de auditoría

Programa de Auditoría

Basado en las actividades intervenibles clasificadas

Una síntesis de los factores y elementos del riesgo definidos por el FRB, se presenta en el siguiente cuadro:

RESUMEN DE LOS FACTORES Y ELEMENTOS DEL RIESGO

Factor de riesgo	Elementos	
Riesgos de Operaciones	▪ Cambios ▪ Administración del cambio ▪ Tendencias en el desempeño ▪ Crítico de operaciones ▪ Eficiencia ▪ Presupuesto y planificación ▪ Lo adecuado y eficacia del ambiente de control interno	▪ Reasunción de negocios ▪ Complejidad/ interdependencia de las operaciones ▪ Incidentes, errores y omisiones desusados ▪ Planificación estrategia/ compromiso con metas y objetivos
Riesgos Financieros	▪ Liquidez ▪ Ingresos ▪ Gastos ▪ Costos de proyectos	▪ Contabilidad total ▪ Valor por transacción ▪ Valor total diario de las transacciones
Riesgos de tecnología de la información	▪ Cambios en la tecnología ▪ Tendencias en el desempeño ▪ Administración del ambiente automatizado ▪ Confiabilidad del software / hardware	▪ Administración del cambio ▪ Lo adecuado de la planificación de contingencia ▪ Adherencia a la metodología de desarrollo del sistema de Bank ▪ Conexión externa
Riesgo de información para la toma de decisiones	▪ Control de desempeño ▪ Capturar la información apropiada	▪ Precisión e integridad de la información financiera y no financiera ▪ Comunicación
Riesgo de recursos humanos	▪ Estructura de la organización ▪ Niveles de personal ▪ Moral y rotación / cambio en el personal clave	▪ Aptitud, entrenamiento y desarrollo ▪ Liderazgo y clima ético ▪ Políticas / procedimientos para el rendimiento y compensación
Riesgo de ambiente	▪ Política y reguladores ▪ Exposición legal o publicidad adversa	▪ Cambios en el mercado, industria o condiciones económicas

La siguiente imagen presenta matriz de puntuación de evaluación de riesgos:

	FACTOR DE RIESGO	PESO	NIVEL DE RIESGO	PUNTAJE (Peso x Nivel)
1.	Operaciones	27		0
2.	Financiero	25		0
3.	Tecnología de Información	23		0
4.	Información para la toma de decisiones	10		0
5.	Recursos Humanos	10		0
6.	Ambiente	5		0
	Total	100		0

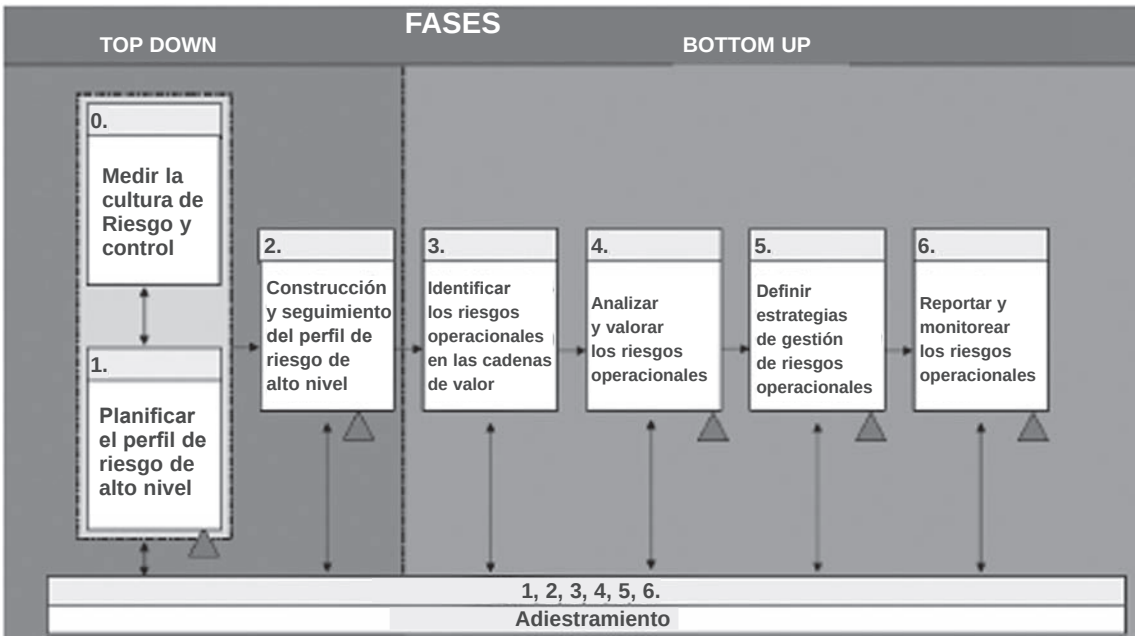
NIVEL DE RIESGO		
CLASIFICACIÓN	PUNTAJE	
	Mínimo	Máximo
Alto	301	400
Moderadamente alto	251	300
Moderado	176	250
Bajo	100	175

El proceso de evaluación de riesgos prevé el siguiente valor agregado:

- La identificación de los factores relevantes de riesgo y una evaluación de su significado relativo
- El proceso de evaluación de riesgos proporciona un medio para la organización e integración de juicios profesionales para el desarrollo del programa de auditoría.
- El proceso de evaluación de riesgos debe conducirse anualmente
- El proceso de evaluación de riesgos puede revisarse y actualizarse durante el año.

3. Metodología de Gestión de Riesgos Operacional desarrollado recientemente (2007) por PriceWaterHouseCoopers, denominada Top Down + Botttom Up.

Esta metodología propone las siguientes fases y etapas:



El detalle de cada una de las etapas es el siguiente:

Fase Top Down (Arriba hacia abajo)

1. Esta metodología inicia con la Medición de la cultura de riesgo y control del personal en las diferentes áreas de la organización, a un momento determinado.

2. La planificación del perfil de riesgo de alto nivel, permite analizar la viabilidad de la planificación estratégica en las organizaciones, a través de la visión global de los riesgos que pueden oponerse al logro de dicha planificación.
3. La construcción y seguimiento del perfil de riesgo de alto nivel, para el desarrollo de esta fase se sigue la metodología de Gestión Integral de Riesgos COSO II-ERM, es decir, el establecimiento de objetivos (entender el negocio y clasificar los objetivos), la identificación de eventos/riesgos (identificar riesgos por cada objetivo del negocio), la evaluación de riesgos (Valorar los riesgos/Determinar el apetito de riesgo) y respuesta al riesgo (Considerar respuestas al riesgo/tratamiento de los riesgos).

Fase Bottom Up (de abajo hacia arriba)

1. Identificar los riesgos operacionales en las cadenas de valor. Determinar los riesgos operacionales a los cuales se encuentra expuesta la organización, considerando tanto factores internos como externos que puedan afectar adversamente la implantación de estrategias y el logro de objetivos del negocio.
2. Analizar y valorar los riesgos operacionales. Consiste en hacer un análisis y valoración de los riesgos operacionales que permite comprender el perfil de riesgo y dirigir de manera más efectiva los recursos para la gestión de riesgos identificados.
3. Definir la estrategia de gestión de riesgos operacionales. En esta etapa se determina la estrategia de gestión de riesgos operacionales identificados y evaluados, para lo cual se deberán definir, evaluar y seleccionar las acciones para reducir el riesgo a niveles aceptables.
4. Reportar y monitorear los riesgos operacionales. Consiste en desarrollar una estructura y proceso de información y comunicación del estado de gestión de los riesgos operacionales que permita comunicar a la máxima autoridad y niveles gerenciales, y que cada una de las áreas de negocio realicen el monitoreo del estatus de los riesgos operacionales.

4. Basilea II: hacia un nuevo esquema de medición de riesgos

Por su parte, el nuevo Acuerdo de Basilea, mejor conocido como Basilea II, se orienta a la aplicación de modelos mas sofisticados de medición del riesgo, pasando de un enfoque de tipo contable a uno que propicia el manejo más dinámico de los riesgos, proponiéndose el tratamiento explicito de otros tipo de riesgos presentes en toda actividad financiera, incluyéndose el riesgo operativo.

El Comité de Basilea explica que: “el objetivo que persigue el marco de suficiencia de capital es poner más énfasis en la gestión de riesgo y fomentar mejoras continuas en la capacidad de los bancos para evaluar riesgos”. “Dicho objetivo se traslada a las prácticas supervisoras y a la disciplina del mercado mediante la mejora en la divulgación de la información referida al riesgo y al capital”.

La propuesta se basa en tres pilares:

- Pilar I: Requerimiento mínimo de capital
- Pilar II: Proceso de supervisión bancaria y
- Pilar III: Disciplina del mercado

El pilar I, requerimiento mínimo de capital considera los tres tipos de riesgos: de crédito, mercado y operativo. El pilar II el proceso de Supervisión Bancaria y finalmente la disciplina del mercado. Este último establece los requerimientos de divulgación de la información con el objeto de permitir a los participantes del mercado evaluar el perfil de riesgo del banco. Los nuevos métodos de estimación de riesgo que se introducen dependen en mayor medida de las estimaciones de las propias entidades.

¿A quien aplica este nuevo Acuerdo de Basilea? Este se aplica en forma consolidado a bancos internacionales activos. La consolidación tiene por objeto preservar la integridad del capital de los bancos con sus filiales, eliminando el doble apalancamiento de capital. Su ámbito de aplicación alcanzará en forma consolidada al holding que sea matriz de un grupo bancario, asegurando de esta manera incluir todos los riesgos de la industria.

Basilea II esta orientada a la banca por lo que vincula los riesgos al requerimiento de capital.

Determinación del ratio del capital mínimo

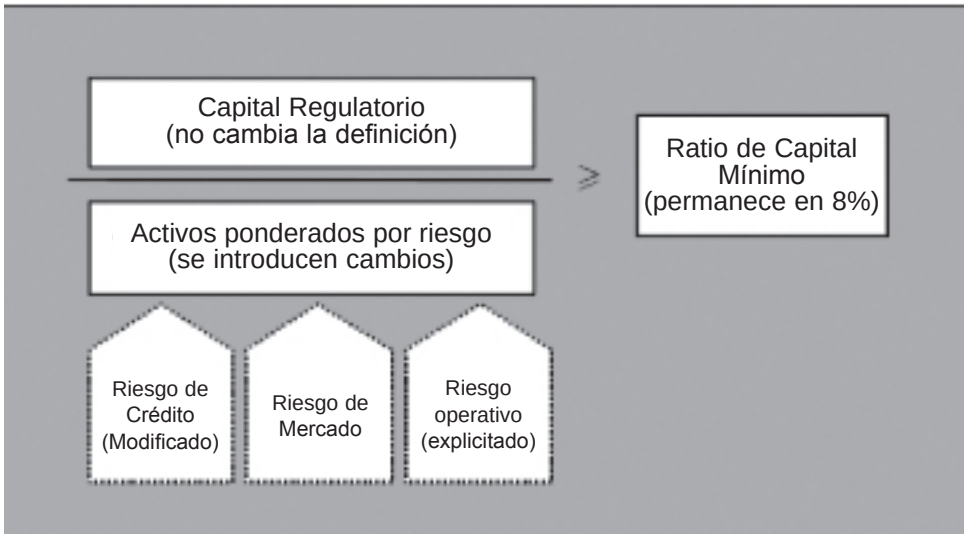


Figura tomada del extracto Basilea II, Superintendencia de Entidades Financieras y Cambiarias de Análisis del Sistema, Diciembre 2003.

El acuerdo previo, Basilea I, hacía énfasis en dos tipos de riesgos: de Crédito y de Mercado, entendiéndose que los otros tipos de riesgos se encuentran comprendidos en estos conceptos. Basilea II ha propuesto cambiar la medición de los activos sujetos a la medición de riesgo basándose en dos elementos: (a) Modificaciones sustanciales en el tratamiento del riesgo de crédito y (b) el Tratamiento explicito del riesgo operativo.

El Riesgo Operacional en Basilea II [10]

Con relación al Riesgo Operacional (RO), Basilea define que “Es el riesgo de incurrir en pérdidas directas o indirectas como resultado de fallas en los procesos internos, fallas del personal o del sistema, o eventos externos”. Esta definición incluye el riesgo legal, pero excluye el estratégico y el reputacional.

[10] Superintendencia de Banca, Seguros y AFP, IV Programa Internacional de Especialización en Finanzas y Administración de Riesgos, Colombia (Autor desconocido).

El acuerdo propone tres métodos para su medición:

- Método del Indicador Básico (función de ingresos netos)
- Método Estándar (en función de líneas de negocio)
- Método de Medidas Avanzadas (cálculos probabilísticos)

A continuación se presenta un resumen de los tres métodos:

Método del Indicador Básico

Es equivalente a un porcentaje fijo (alpha) de los ingresos brutos anuales medios de los tres últimos años.

$$K_{BIA} = GI \times \alpha$$

Donde:
K_{BIA} = Requerimiento de capital en el Método del Indicador Básico
GI = Ingresos brutos anuales medios de los tres últimos años
α = 15%, fijado por el Comité de Basilea

Método Estandarizado

En este enfoque, las actividades de la entidad se dividen en 8 líneas de negocio. Dentro de cada línea, el ingreso bruto es indicador para aproximar la magnitud del negocio operacional y, por lo tanto del riesgo de operaciones. Su uso se recomienda para bancos que no son internacionalmente activos.

$$K_{TSA} = S(GI_{1-8} \times b_{1-8})$$

Donde:
K_{TSA} = Requerimiento de capital en el Método Estandarizado
GI_{1-8} = Ingresos brutos anuales medios de los tres últimos años para cada línea de negocio
b_{1-8} = porcentaje fijado por el Comité de Basilea

Para poder adoptar este método se requiere:

- Una participación activa de la alta dirección y la gerencia.
- Un sistema de evaluación de riesgo sólido y plenamente integrado a la gestión de la entidad.
- La entidad debe contar con recursos suficientes tanto en las líneas de negocio como en las áreas de control y auditoría.

Aproximaciones de Medición Avanzada (AMA)

- Bajo esta aproximación, el requerimiento de capital será igual a la medida de riesgo generada por el sistema de medición del riesgo operacional que la institución ha implementado.
- A diferencia del enfoque IRB para el riesgo de crédito, el rol del sistema de riesgo implementado por la institución no solo se enfoca en la determinación de parámetros sino que define (siempre que haya sido aprobado) el nivel de carga de capital por riesgo operacional.

- Es posible combinar el uso del enfoque AMA en algunas líneas de negocio con los dos previamente definidos siempre que el supervisor lo autorice.
- La carga de capital será igual a la pérdida esperada y la no esperada, a menos que el banco pueda demostrar al supervisor que ya ha tomado en cuenta la pérdida esperada.

Estándares cualitativos necesarios para la implementación de AMA

- El banco debe poseer una gestión del riesgo operacional responsable del diseño, implementación y documentación del marco global de análisis, control y gestión del riesgo operacional de la institución.
- El sistema de gestión de riesgo operacional debe estar integrado en los procesos de gestión de riesgo que a diario se llevan a cabo en el banco.
- Debe existir un reporte periódico a la gerencia general y a los directores, de las exposiciones y la experiencia de pérdidas en riesgo operacional.
- Se deben realizar revisiones periódicas por parte de auditores internos y externos a los procesos y sistemas de gestión del RO.

Estándares cuantitativos necesarios para la implementación de AMA

- El Comité de Basilea no especifica metodologías específicas que puedan ser empleadas en la modelación del riesgo operacional. Sin embargo, un banco AMA debería:
  - Ser capaz de demostrar que su aproximación captura eventos de pérdida que se ubicarían en la cola de la distribución de probabilidad.
  - Emplear un periodo de referencia de 1 año
  - Emplear un nivel de confianza de 99.9%
  - Agregar los estimados de riesgo operacional para calcular el requerimiento de capital, pero puede considerar algún tipo de análisis de correlaciones que refleje los efectos de portafolio.
- Los reguladores tienen discreción para la exigencia de requisitos adicionales.

Elementos clave en la AMA

1. Uso de data interna

El registro de datos de eventos de pérdida es una condición indispensable para el desarrollo de modelos AMA.

- Los datos representan los riesgos propios de la institución según su historia y sus propias políticas de gestión.
- Se requieren al menos 5 años de registro para la implementación del modelo, pero para su primera revisión se permitirá solo 3 años.
- Se debe realizar un mapeo de los datos internos según las categorías definidas
- Se debe definir un umbral mínimo de recolección de información.
- Las pérdidas por R.O que derivan en pérdidas por Riesgo de Crédito no serán tomadas en cuenta en la base de datos, mientras que las de Riesgo de Mercado sí lo serán.

2. Datos externos relevantes:

- Un banco debe emplear datos externos relevantes (públicos o capturados a partir de iniciativas de pool). Especialmente, esto es necesario cuando el banco está expuesto a eventos de pérdida infrecuentes pero de alto valor.
- Si bien no existe un criterio estadístico sólido para su combinación con los datos internos, se establece que deben ser combinados.
- Los datos públicos no propios deben ser tomados con cuidado en tanto su ocurrencia también es condicional al tipo de políticas del banco reportante, las que no necesariamente son las mismas en el banco que adopta la data.

3. Análisis de escenarios.

- Debe ser realizado mediante la combinación de la experiencia propia, la opinión de expertos y los datos externos.
- Tiene un carácter prospectivo. Los escenarios se pueden simular puntualmente o sobre la base de las distribuciones de pérdida calculadas empíricamente (modificándolas o estresándolas).
- Es útil en tanto los datos pasados no siempre son la mejor forma de predecir el futuro, sobre todo cuando los datos de baja frecuencia y alta severidad son raramente observados.

4. Factores básicos del entorno del negocio y control interno

El banco debe capturar los factores de riesgo del entorno y de control interno que pueden cambiar su perfil de riesgo operacional. Estos factores permitirán que las evaluaciones de riesgo del banco tengan un carácter más prospectivo y reflejen de manera más exacta el entorno operativo y de control de la institución.

Indistintamente de los requerimientos de capital (que no aplica para los bancos centrales), para toda organización se hace necesario contar con una metodología de gestión de riesgos que le permita prevenir impactos en el cumplimiento de objetivos.

B. El rol del Auditor Interno

El auditor por su carácter multidisciplinario, y su actitud independiente respecto de los responsables de la ejecución de los procesos, juega un papel importante, como apoyo a la Dirección, tanto en la actividad de aseguramiento, como de consultoría.

Los principales factores que debe considerar el auditor interno es si al momento de asesorar a la entidad en algún proceso o actividad, esto no amenaza su independencia mental, y que no pierde en ningún momento su alto grado de objetividad, esto es establecido por Normas de Auditoría, además, no puede ni debe ejercer en ningún momento responsabilidades en el proceso de administración de riesgo de la entidad.[11]

[11] The Institute Internal Auditors (IIA) (2004).

Respecto a los roles fundamentales del Auditor ante la gestión de los riesgos, el auditor puede:[12]

- Brindar aseguramiento sobre los procesos de gestión de riesgos
- Brindar aseguramiento de que los riesgos son correctamente evaluados
- Evaluar los procesos de gestión de riesgos
- Evaluar la documentación soporte y reportes de la gestión de los riesgos por parte de la administración
- Revisar el manejo de los riesgos claves

Algunos roles legítimos que debe realizar el auditor interno con una salvaguarda, son los siguientes:[13]

- Facilitar la identificación y evaluación de los riesgos
- Coordinar actividades de gestión de riesgos
- Consolidar reportes sobre riesgos
- Defender el establecimiento de mecanismos y herramientas para la gestión de los riesgos

A continuación se describen los roles que el auditor interno no debe realizar:[14]

- Establecer el apetito o riesgo tolerable por la administración
- Imponer procesos de gestión de riesgos
- Manejar el aseguramiento sobre los riesgos
- Tomar decisiones de respuesta a los riesgos
- Implementar respuesta a los riesgos a favor de la administración
- Tener responsabilidades en la gestión de los riesgos

C. El funcionamiento efectivo del sistema de control interno en el tiempo

Pensar que un Sistema de Control Interno (SIC) permanece vigente en el tiempo, es errado. Tanto a nivel doméstico como en los mercados internacionales, la forma de hacer negocios cambia vertiginosamente, de un día para otro y esto no se puede impedir, su dinamismo es importante para el desarrollo de la humanidad, de manera que, si la forma de hacer negocios cambia, el comportamiento o las manifestaciones de los riesgos también cambia y si estos cambian los controles se deben actualizar y modificar necesariamente.

Con los cambios en el entorno, las entidades están obligadas a incorporar mejoras a sus operaciones, por lo tanto, se afirma que un sistema de control interno funciona a un momento determinado, por lo que es necesaria su actualización en el tiempo. Esta actualización se puede realizar si se ejerce un monitoreo o seguimiento permanente de las operaciones que realiza la entidad.

El monitoreo del SIC ocurre en el curso de las operaciones, mediante evaluaciones separadas o una combinación de ambas. Su alcance y frecuencia dependerá primordialmente de la valoración de los riesgos. Es claro entonces, que analizar y evaluar requiere de una labor permanente y exhaustiva, por lo que los dueños y ejecutores de los procesos deben establecer la periodicidad en la que realizará la valoración de los riesgos, asimismo, documentarán apropiadamente el cumplimiento de las actividades de control.

[12] Ibíd. 7
[13] Ibíd. 7
[14] Ibíd. 5

El funcionamiento del SIC debe comunicarse a la Alta Dirección de la entidad periódicamente, no sólo por el interés de evaluar su gestión, si no porque son los responsables de su funcionamiento y de la continuidad del negocio.

D. La cultura de riesgos

Desarrollar una cultura proactiva para responder a los riesgos, es un proceso de enseñanza y aprendizaje continuo, debido al dinamismo y los cambios en los negocios. La participación de los miembros de la organización en todos los niveles permite crear ese alto grado de conciencia necesaria para que el personal se identifique con las funciones y responsabilidades que la entidad le ha conferido.

Asimismo, es importante que, para el establecimiento de los objetivos y metas se considere que si la tecnología y sistemas de información, y demás recursos físicos responden a esos objetivos, es decir, si están alineados y si responderán eficientemente a la misión y visión de la entidad.

La orquestación de los pilares fundamentales de la entidad, es decir, las personas y los recursos tecnológicos y físicos, permitirán el cumplimiento razonable de los objetivos.

E. Banco de información

Para contar con datos históricos sobre la ocurrencia de los riesgos, las entidades deben establecer un banco de información que permita su utilización en el futuro. Disponer de esta información documental facilita la realización de análisis y evaluaciones de riesgos, esta información debe compartirse a los niveles autorizados por la alta dirección.

En las diferentes metodologías de gestión de riesgos se observan muchas coincidencias, entre otras, todas requieren monitorear, revisar, comunicar y consultar; documentar cada etapa del proceso de administración de riesgo, lo que permite obtener el escenario completo de los acontecimientos durante la ejecución de las operaciones. La documentación debería incluir los supuestos, los métodos, las fuentes de datos, los resultados, la utilidad y destino final de la misma.

La ocurrencia de los riesgos puede documentarse a través de registros en sistemas de información y medios electrónicos (desde medios simples como correos electrónicos, microfilmaciones, en bitácoras de aplicaciones software, etc.), archivos físicos, video grabaciones y otros.

Lo anterior no significa que únicamente se documente la ocurrencia de los riesgos, se debe tener evidencia del cumplimiento de las actividades de control; herramientas como las autoevaluaciones de control, permiten que los dueños de los procesos evalúen su gestión.

Las razones para documentar son las siguientes:[15]

- Demostrar que el proceso es conducido apropiadamente.
- Proveer una evidencia de un enfoque sistemático de identificación y análisis de riesgo.
- Proveer un registro de los riesgos y desarrollar la base de datos de conocimientos de la organización.

[15] AS/NZS 4360: (1999), Pág. 20.

- Proveer a los tomadores de decisión relevantes, un plan de administración de riesgos para aprobación y subsiguiente implementación.
- Proveer un mecanismo y herramienta de responsabilidad.
- Facilitar el continuo monitoreo y revisión.
- Proveer una pista de auditoría, y
- Compartir y comunicar información.

F. Beneficios de la gestión de riesgos

La gestión integral de los riesgos se traduce en beneficios presentes y futuros para toda entidad, independientemente de la naturaleza de sus funciones. A continuación se enuncian algunos beneficios:

- Ayuda a asegurar el cumplimiento de los tres objetivos fundamentales: fortalecimiento de los procesos institucionales, generar información financiera confiable y cumplir con leyes y reglamentos aplicables.
- Agrega valor a la entidad.
- Se toma ventaja de las oportunidades que presenta la entidad.
- Crea cultura institucional la cual permite responder proactivamente al riesgo.
- Evita improvisaciones ante la ocurrencia o activación de eventos adversos a los intereses de la entidad.
- Se prevén los factores y las actividades que permitan asegurar que razonablemente se cumplan los objetivos y metas institucionales.
- Se identifican aquellos efectos adversos específicos vinculados a cada proceso, lo que permite el desarrollo de medidas efectivas para su tratamiento.
- Se fortalece el Sistema de Control Interno de la entidad.

IV. Sistema de Gestión de Riesgos

A. Estructura, organización y funciones de la gestión de riesgos

José A. Soler et al. (1999), Gestión de Riesgos Financieros, así como las metodologías citadas proponen que desde el punto vista de la gestión de riesgos, el esquema organizativo de la entidad sea segmentado en dos grandes estructuras de responsabilidad:

- Estructura estratégica
- Estructura operativa

La estructura estratégica debe comunicar al resto de la organización, de forma clara y explicita, la estrategia y las políticas que han definido; igualmente debe crear y transmitir una cultura corporativa de gestión de riesgos, que ayude a concienciar y convencer a todos los estamentos de la entidad sobre la conveniencia de dicho estilo de gestión.

La estructura operativa debe informar a la alta dirección de la entidad sobre todos los aspectos relevantes en relación a la ejecución de la estrategia de gestión de riesgos y la implantación de las políticas, de forma que el proceso pueda realimentarse y adaptarse a las necesidades de la entidad y del mercado en cada momento.

Las diferentes metodologías coinciden en que las funciones que deben cumplir estructuralmente, el Consejo o Junta Directiva, Comité Ejecutivo, Comité de Riesgos y Unidad de Riesgos, son las siguientes:

Consejo o Junta Directiva. Como máximo responsable de la creación de valor, así como de sancionar la estrategia y las políticas de la entidad. En el ámbito de la gestión de riesgos sus funciones son:

- Conocer y comprender los riesgos que asume la entidad.
- Garantizar la existencia del capital necesario para soportar el riesgo global de la entidad.
- Salvaguardar el valor de la entidad de pérdidas potenciales.
- Sancionar la estrategia de gestión de riesgos, que debe incluir criterios de aceptación de riesgos.
- Marcar las líneas maestras de la gestión de riesgos.
- Aprobar las políticas, procedimientos, metodologías (cualitativas-cuantitativas) y los límites de riesgos.
- Conocer periódicamente los resultados obtenidos y el nivel de riesgos asumidos.
- Garantizar la existencia de los recursos necesarios para que la gestión de riesgos sea eficiente.
- Potenciar la cultura de gestión de riesgos dentro de la entidad.
- Monitorear el funcionamiento continuo de los procesos de gestión de riesgo reportados por el Comité de Riesgos.

Comité Ejecutivo. Es el máximo órgano directivo de la organización y, como tal tiene la responsabilidad de la gestión de riesgos asumidos por la entidad, por lo que debe tener las siguientes funciones:

- Garantizar el correcto cumplimiento de las decisiones del Consejo.
- Analizar los resultados obtenidos por las unidades de negocio en función de los presupuestos, identificando las desviaciones y planteando medidas para corregirlas.
- Informar regularmente al Consejo sobre los aspectos relacionados a la gestión de riesgos.
- Proveer dirección y retroalimentación en las respuestas a los principales riesgos.
- Diseñar y aprobar la estrategia de gestión de riesgos de la entidad y liderar su ejecución.
- Conocer y comprender la probabilidad e impacto de los riesgos.
- Tomar decisiones de gestión que puedan tener un impacto importante en el valor de la entidad.
- Monitorear el perfil de riesgo y las respuestas de mitigación, como parte de la revisión de desempeño del negocio.
- Potenciar el ambiente de control y gestión de riesgos dentro de la entidad.
- Definir la estructura organizativa y una política de incentivos adecuada con la filosofía de gestión de riesgos.
- Aprobar la asignación de los recursos necesarios para la gestión de riesgos.
- Asegurar la existencia y utilización de políticas, procedimientos, metodologías y sistemas que permitan medir y gestionar los riesgos cuantificables y controlar los no cuantificables.

Comité de Riesgos. Es el órgano en el cual el Consejo y Comité Ejecutivo han delegado la responsabilidad de definir las políticas y procedimientos y de controlar que las áreas de negocio están ejecutando correctamente la estrategia de gestión de riesgos aprobadas en la entidad, por lo que debe tener las siguientes funciones:

- Promover el compromiso de la Alta gerencia con la estrategia de gestión de riesgos
- Proveer lineamientos y herramientas para la identificación, evaluación, mitigación y monitoreo de los riesgos de forma continua.
- Revisar los reportes elaborados por la Unidad de Riesgos que consolidan los avances de implantación de la estrategia de gestión de riesgos.
- Monitorear la efectividad de la implantación de los planes de acción por parte de las unidades de negocio y apoyo a que se ejecuten en el tiempo establecido.
- Monitorear los cambios en el negocio y en el sector del mercado en donde opera la organización, a fin de evaluar su impacto en el manejo de los riesgos.
- Revisar los indicadores claves de riesgo.
- Asegurar la correcta ejecución de la estrategia de gestión de riesgos e informar al Comité Ejecutivo sobre el desarrollo de la misma.
- Definir y asegurar la correcta implantación de políticas, metodologías y procedimientos, acordes a los riesgos aprobados, que permitan medir y controlar los riesgos cuantificables y los difíciles de cuantificar.
- Proponer límites de control de riesgos al Comité Ejecutivo para su aprobación.
- Conocer en detalle las posiciones y los riesgos asumidos en relación a los límites.
- Aprobar los excesos temporales de límites cuando sea pertinente.
- Informar al Consejo de los resultados obtenidos por las diferentes unidades de negocio en relación a los riesgos asumidos.
- Aprobar el presupuesto de la Unidad de Riesgos y monitorear su desempeño.

Unidad de Riesgos. Las funciones que debe cumplir la Unidad de Riesgos son las siguientes:

- Coordinar y realizar seguimientos periódicos al esquema de control de riesgos.
- Fomentar la cultura de riesgo en todos los niveles de cargo de la organización.
- Proveer políticas y metodologías (cualitativas - cuantitativas) para la identificación, evaluación y medición de los riesgos, a fin de asegurar el cumplimiento de los objetivos de negocio.
- Determinar las herramientas y sistemas de información necesarios para la adecuada administración de los riesgos.
- Proponer al comité de riesgos los límites de exposición al riesgo.
- Velar que todos los proyectos que se llevan a cabo en la organización, así como el diseño de nuevos productos y servicios, cumplan con las premisas básicas de mitigación de riesgos.
- Definir los requerimientos para la recolección de información de pérdidas por riesgos.
- Desarrollar procesos de respuesta al riesgo para asistir en la identificación de los tipos y niveles de respuestas requeridos y evaluar lo adecuado de esas respuestas.
- Capacitar a los delegados de riesgo en los procesos de administración de riesgos en las unidades de negocio.
- Reportar al Comité de Riesgo Operacional los avances de la gestión realizada sobre el proceso de gestión de riesgo y aportar las recomendaciones prácticas para el mejoramiento.

Delegados de riesgo. Debido a lo amplio y complejo de la gestión de riesgos, se hace necesario la existencia de Comités y Delegados de riesgos en las diferentes áreas de negocio de la entidad, por ejemplo: se debe formalizar en las áreas de negocio la gestión de activos y pasivos, operaciones y servicios de tesorería, monitoreo y gestión del riesgo financiero relacionado al portafolio de inversiones (riesgo de liquidez, mercado y crédito), constituyendo Comités de Activos y Pasivos; asimismo, los procesos de gestión de estadísticas, de seguridad física de personas, bienes y valores, de tecnología y sistemas, de asesoramiento jurídico-legal y fiscal, de recursos humanos y formación, así como administradores de imagen y reputación de la entidad. Las funciones que deben cumplir, son las siguientes:

- Apoyar a su unidad funcional en el proceso de identificación de riesgos operacionales y evaluación de su impacto y frecuencia de ocurrencia.
- Revisar los planes de acción para gestionar los riesgos de su unidad funcional.
- Elaborar propuestas de acciones para mitigar los riesgos identificados.
- Definir y proponer indicadores de riesgo, así como la fijación de los límites de tolerancia.
- Monitorear la implantación de los planes de acción e indicadores de riesgos.
- Reportar incidentes o eventos de pérdidas a la Unidad de Riesgos
- Apoyar a la Unidad de Riesgos en los procesos de recolección de eventos de pérdidas, asegurando el seguimiento de dichos eventos en términos de causa, efecto y medida de mitigación.

Perfil de los Delegados de Riesgos. Los Delegados deben tener entre otras las siguientes cualidades:

- Conocimiento en materia de riesgo y control.
- Experiencia en el manejo de procesos, productos y servicios donde se desempeña.
- Debe formar parte de las áreas de negocio y apoyo en las cuales desarrolla su actividad.
- Línea de reporte directa al Gerente o encargado del área de negocio o apoyo (responsable de la Unidad)
- Funcionalmente, debe reportar a la Unidad de Riesgo.
- Dedicación a tiempo parcial o total a esta función, según el tamaño y complejidad del proceso del área de negocio al que representa.
- Capacidad de análisis y comunicación

Unidades de negocio y apoyo. Las Unidades de negocio y apoyo deben cumplir los siguientes roles y responsabilidades:

- Coordinar y realizar seguimiento periódico al esquema de control de riesgo.
- Participar activamente en la identificación y evaluación de riesgos de su área.
- Realizar seguimiento de los indicadores de riesgos de los procesos bajo su responsabilidad.
- Seguir y reportar incidentes y pérdidas por materialización de los riegos a la Unidad de Riesgo.
- Participar en la definición e implantación de las acciones correctivas de los riesgos.
- Designar al personal responsable que desempeñará el rol como Delegado de Riesgo en cada Unidad.
- Implementar las acciones de mitigación de riesgo definidas para cada uno de los riesgos identificados, de acuerdo con las prioridades establecidas.
- Conducir la evaluación periódica del cumplimiento de la política de la organización, los procedimientos y las prácticas relacionadas con los riesgos.
- Asegurar la eficacia del control interno en relación con el manejo de los riesgos de su Unidad.

Auditoría Interna. La Auditoría Interna entre sus roles y responsabilidades, debe realizar las siguientes:

- Incluir en su plan anual la revisión de las áreas o procesos prioritarios según los resultados de las evaluaciones de riesgo efectuadas.
- Elaborar o adaptar los programas para incluir dentro de las evaluaciones los aspectos relacionados con la gestión de riesgos.
- Revisar el cumplimiento de las políticas y procedimientos de gestión de riesgos por parte de las Unidades de Negocio y Apoyo.
- Examinar y valorar regularmente, de forma independiente, la idoneidad y efectividad global de la estructura de gestión y control de riesgo de la entidad.
- Revisar los procesos de administración de riesgo, tanto su diseño como sus funciones.
- Realizar pruebas de efectividad de los controles asociados a los riegos identificados por las Unidades de Negocio y Apoyo.
- Proveer una opinión independiente a la máxima autoridad y comité ejecutivo, sobre la efectividad de la gestión de riesgo y funcionamiento del Sistema de Control Interno.
- Establecer programas de seguimiento para la determinación del cumplimiento de los planes de acción por parte de las áreas auditadas.
- Presentar como mínimo, semestralmente, un informe de gestión de riesgos a los ejecutivos y a la máxima autoridad, el cual debe contener el resultado de las evaluaciones y observaciones determinadas, de las acciones llevadas a cabo en las Unidades de Negocio y Apoyo en el ámbito de la gestión de riesgo.

Si estructuralmente no existe la Unidad de Riesgos en la organización, y considerando que debido a la formación profesional, Auditoría Interna es conocedora del tema, esta puede impulsar y asesorar a la organización en su implementación.

B. Etapas del Sistema de Gestión de Riesgos

El Sistema de Gestión de Riesgos comprende al menos las siguientes etapas:

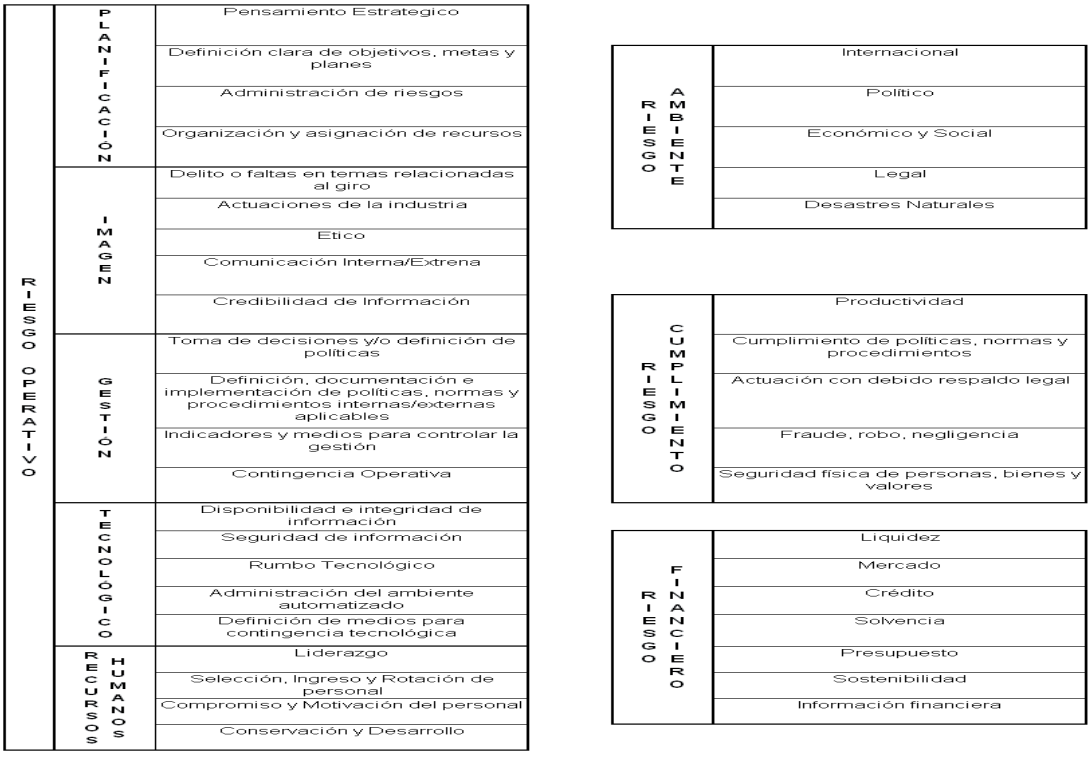
Primera Etapa

Identificación de los procesos globales, intermedios y proyectos de la entidad, los cuales orientan los objetivos y metas institucionales.

En la planeación estratégica de la organización, se debe realizar un esfuerzo importante para identificar los procesos de primer nivel, subprocesos y proyecto de la entidad.

Segunda Etapa

Se deben identificar los Riesgos de Alto Nivel, Riesgos y Factores de Riesgo. Con la identificación de los procesos claves de la organización, se debe hacer el ejercicio de identificación de los riesgos inherentes a estos a fin de obtener un mapa de riesgos, como el que se muestra a continuación:



Tercera Etapa

Asociar los Riesgos a los Procesos globales, procesos intermedios y proyectos de la entidad. Esta etapa implica el juicio y experiencia de los dueños y ejecutores de los procesos.

Esta etapa requiere analizar cada fase, etapa y actividad de cada proceso, identificándose el riesgo inherente. Esta identificación implica evaluar la incidencia o impacto de cada riesgo en tres dimensiones: Patrimonial, Reputacional y Sistémico.

Patrimonial: de ocurrir o materializarse el evento adverso, cual es la incidencia o impacto monetario que éste le imputaría al proceso y por ende a la entidad.

Reputacional: qué impacto tendría en los usuarios o interesados la materialización de un riesgo.

Sistémico: si el evento adverso se materializa en una fase, etapa o actividad del proceso, el servicio se podría ver interrumpido o la calidad del servicio no cumpliría las expectativas y requerimientos válidos del cliente.

Nota: es posible asignar a estas dimensiones del impacto, una escala para efectos de medición.

Cuarta Etapa

Análisis cualitativo y cuantitativo de los riesgos. Cada factor de riesgo se califica por su Probabilidad e Impacto, el resultado o producto de ello, representa el escenario de la exposición o criticidad al riesgo. En esta etapa no se consideran los controles, ya que se está evaluando el riesgo inherente, es decir, el riesgo por la naturaleza del proceso.

Ejemplo de escalas probabilidad e impacto de riesgos para los objetivos estratégicos

Escala de medición para la probabilidad

Escala de probabilidad			
Grado	**Descripción**	**Probabilidad (%)**	
		Mínimo	**Máximo**
1	Poco probable	0	5
2	Remoto	6	10
3	Posible	11	30
4	Probable	31	50
5	Muy probable	51	70
6	Cierto	71	100

Escala de impacto	
Grado	**Estratégico**
1	Impacto mínimo
2	Afecta a la consecución de los objetivos de la unidad organizativa.
3	Impide la consecución de los objetivos de la unidad organizativa.
4	Afecta el cumplimiento de los objetivos de varias unidades organizativas, y por tanto, del negocio.
5	Necesidad de modificar la estrategia corporativa.
6	Modifica sustancialmente el posicionamiento estratégico.

Este impacto se puede asociar con las 3 dimensiones explicadas anteriormente asignándole puntuación en cada grado.

Escalas de probabilidad e impacto para riesgo de reportes financieros

Escala de probabilidad			
Grado	**Descripción**	**Probabilidad (%)**	
		Mínimo	**Máximo**
1	Poco probable	0	5
2	Remoto	6	10
3	Posible	11	30
4	Probable	31	50
5	Muy probable	51	70
6	Cierto	71	100

Escala de impacto	
Grado	**Reporte**
1	Impacto mínimo. (se puede ponderar por reputación, patrimonial y sistémico)
2	Impacto interno y reducido, puede ser rectificado a tiempo.
3	Errores advertidos internamente y que pueden conllevar un impacto relevante.
4	Errores advertidos externamente y que pueden originar opiniones de análisis.
5	Desconfianza en los mercados. Desconfianza por parte de los usuarios.
6	Impacto en los estados financieros y al valor de la acción (reputación, imagen) en el mercado. Deterioro de la imagen.

Escalas de probabilidad e impacto para riesgo de cumplimiento

Escala de probabilidad			
Grado	**Descripción**	**Probabilidad (%)**	
		Mínimo	**Máximo**
1	Poco probable	0	5
2	Remoto	6	10
3	Posible	11	30
4	Probable	31	50
5	Muy probable	51	70
6	Cierto	71	100

Escala de impacto	
Grado	**Cumplimiento**
1	Impacto mínimo.
2	Información relevante para autoridad competente que no deriva en expediente.
3	Apertura de expediente sin sanción económica.
4	Apertura de expediente con sanción económica.
5	Sanción calificada como muy grave, con repercusiones penales.
6	Resolución judicial que obliga a restringir o deshacer posiciones en los negocios.

La combinación entre las probabilidades y el impacto de los riesgos, se expresan cuantitativamente con la siguiente fórmula:

Riesgo Inherente

$$RI = \sum_{i=1}^{n} (Pr_i \, x \, Ir_i) x \, wr_i$$

Descripción
RI : Riesgo Inherente
Pr_i : Probabilidad
Ir_i : Impacto (se puede ampliar la fórmula ponderando 3 dimensiones)
wr_i : peso de los riesgos específicos contenidos en cada macroriesgo

Quinta Etapa

Define el Tratamiento que se dará a los riesgos, sea esto: Evitar, Reducir, Compartir, Aceptar.

Evitar. Se evita un riesgo, cuando la alta dirección toma la decisión de no realizar aquellas actividades que generan riesgos.

Reducir. Implica llevar a cabo las acciones necesarias orientadas a reducir la probabilidad o el impacto del riesgo o ambos conceptos a la vez.

Compartir. La probabilidad y el impacto del riesgo se reduce trasladando o, de otro modo, compartiendo una parte del riesgo.

Aceptar. No se emprende ninguna acción que afecte a la probabilidad o el impacto.

Sexta Etapa

Identificación de las Actividades de Control. Implica extraer u obtener el detalle de todas aquellas acciones diseñadas para controlar las etapas y actividades de los procesos, las cuales están de forma explicita e implícita la normativa interna de la entidad (políticas internas, instructivos, procedimientos, etc).

Séptimo etapa

Evaluar la efectividad de las Actividades de Control. Cuanto más efectivo sea el Sistema de Control Interno Institucional, menor es la criticidad de los riesgos sobre los procesos de la entidad.

El control puede tener las siguientes connotaciones y efecto sobre los riesgos: Muy adecuado, Adecuado, Normal, Deficiente, Muy deficiente, Nulo.

Efectividad	Peso %	Descripción
Muy adecuado	81-100	El control se ha definido formalmente y ocurre de forma eficaz.
Adecuado	61-80	El control existe, aunque requiere ser monitoreado frecuentemente, aunque se sigue de forma eficaz.
Normal	51-60	El control se ha definido y puesto en práctica; pero presentan ciertas debilidades.
Deficiente	31-50	El control se ha definido y puesto en práctica con irregularidades.
Muy deficiente	11-30	Los procesos no se han definido explícitamente y no se realizan.
Nulo	1-10	El control no está definido.

La combinación entre las probabilidades y el impacto de los controles, se expresan cuantitativamente con la siguiente fórmula:

Efectividad de los controles

$$CI = \sum_{i=1}^{n} (Pc_i x Ic_i) x wci$$

Descripción

CI: Efectividad de los controles
Pc_i: Probabilidad de la efectividad del control
Ic_i: Impacto de la efectividad del control
wc_i: peso de la actividad de control

Del resultado de confrontar la efectividad de los controles con los riesgos asociados a los procesos y actividades del negocio, se obtiene el riesgo residual.

Riesgo Residual

$$RR = \left[\sum_{i=1}^{n} (Pr_i \, x \, Ir_i) \, x wr_i \right] - \left[\sum_{i=1}^{n} (Pc_i \, x \, Ic_i) \, x wc_i \right]$$

Descripción
RR: Riesgo residual
Pr_i : Probabilidad
Ir_i : Impacto
wr_i: peso de los riesgos
Pc_i: Probabilidad de la efectividad del control
Ic_i: Impacto de la efectividad del control
$wc_{i:}$ peso de la actividad de control
n: número de riesgos y controles seleccionados

C. Implantación del Sistema de Gestión de Riesgos (SGR)

Culturización. Previo a la implantación de un Sistema de Gestión de Riesgos (SGR), es necesario que en el entorno interno se perciba con suma facilidad la intención de gestionar los riesgos a todos los niveles de la organización, que la máxima autoridad denote como parte de su filosofía e intención, la gestión de los riesgos de la entidad. A lo anterior se debe agregar incentivos como capacitaciones, formación de equipos de trabajo, liderazgo, llamamiento a personal clave en la participación de todos los niveles de la entidad, utilización de medios de comunicación físicos, gráficos, electrónicos y de cualquier otra índole, facilita el sentimiento de identificación de los miembros de la entidad a incorporarse en el esfuerzo del establecimiento del SGR. Es necesario realizar talleres orientados a facilitar su implementación.

La gestión de los riesgos es partir de la planificación estratégica, puesto que en ese momento se debe identificar y definir por su origen, las causas de los riesgos y eventos adversos que pudiesen afectar las estrategias y objetivos de la entidad. Esta etapa del proceso, se requiere de un ejercicio exhaustivo y crítico que involucra al personal clave, ejecutor de los procesos, puesto que son estos los que interactúan con los riesgos y toman como propio el Sistema de Control Interno de la entidad. Sólo los responsables y ejecutores directos de los procesos, comprenden mejor las tareas, actividades y productos, por lo tanto se hace necesaria su participación.

Definición de metodología y de estructura de la gestión de riesgos. La Metodología de gestión de riesgos propone un proceso ordenado y lógico, diseñado para responder de forma efectiva a diferentes eventos (adversos, principalmente), cuya ocurrencia podría afectar los objetivos estratégicos de la entidad.

La metodología de gestión de riesgos describe fases, etapas y actividades a realizar, necesarias para su implementación, contiene los roles y responsabilidades de los participantes, definiciones de sus componentes, escalas y valores tendientes a medir su impacto y probabilidad de ocurrencia, a partir de resultados cualitativos y cuantitativos que permiten efectuar análisis y escenarios a fin de lograr un menor grado de incertidumbre del efecto de los riesgos globales de la entidad, y realizar una mitigación efectiva de los riesgos.

Los elementos de la metodología de riesgos se estructuran de forma tal que en cada una de las etapas de la cadena de valor, los resultados permitan hacer análisis parciales que facilitan la comprensión del proceso en evaluación, garantizándose el cumplimiento de su aplicación a través de la aprobación de normas por la máxima autoridad y operativamente por la máxima autoridad o comité ejecutivo, como dueños y ejecutores de los procesos de negocio y de apoyo.

Los SGR son diseñados de forma clara y sencilla, de fácil aplicación y resultados comprensibles a todo nivel de la organización; para ello existen diversas herramientas automatizadas en las que las organizaciones se pueden apoyar, logrando una mayor interactividad de los usuarios. Estas ofertas se ajustan a las necesidades de las organizaciones.

Monitoreo, revisión y reporte. La identificación, monitoreo y actualización del mapa de riesgos de la organización es un ejercicio permanente que debe efectuarse en tiempo real, puesto que la forma de hacer negocios es vertiginosamente dinámica.

El SGR requiere de un seguimiento por todos y cada uno de los estamentos de la entidad, de la estructura estratégica y operativa, por quienes se defina que formalmente deberán realizar metodológicamente la gestión de los riesgos, como por todos y cada uno de los miembros de la organización, por lo que, se hace necesario establecer los mecanismos de control y documentación de esos eventos adversos; se definen roles y responsabilidades para el registro de la ocurrencia de los eventos adversos, pérdidas patrimoniales, deficiencias en los sistemas de información, por deterioro reputacional (imagen pública). Toda esta información es de importancia en la retroalimentación del sistema de registro, la cual es utilizada para fortalecer la actualización del tratamiento de los riesgos, así como, la actualización de la definición del apetito del riesgo o riesgo máximo aceptado por la máxima autoridad de la entidad.

Finalmente, en la gestión de riesgos, cada unidad de negocios debe gestionar los recursos asignados de la manera más eficiente en función de los límites definidos, su conocimiento respecto de su negocio y las expectativas sobre la evolución de los factores de riesgo en los que actúan. Como es lógico, cada unidad mantendrá la libertad de actuación en cuanto a los riesgos que se desean asumir, siempre que estos sean compatibles con los seleccionados previamente y no contribuyan al riesgo de la entidad por encima de los límites establecidos por esta y aceptados por la máxima autoridad.

V. Conclusiones

Los riesgos son inherentes a todo proceso, operación y actividad que se realiza, por lo que su gestión constituye una valiosa herramienta que apoya el crecimiento y desarrollo de las entidades públicas y privadas.

La valoración de los riesgos es un proceso formal que requiere principalmente el establecimiento de aprendizaje del personal, ello facilita la creación de la cultura de riesgos institucional.

Analizar y evaluar los riesgos es una actividad permanente, exigida por el entorno cambiante en la forma de hacer negocios.

Ante los riesgos se pueden tomar dos posiciones, ignorarlos y tratarlos. El tratamiento implica desarrollar acciones dirigidas a evitar, reducir, compartir y aceptar.

El funcionamiento efectivo del sistema de control interno requiere evaluaciones periódicas orientadas a detectar debilidades y oportunidades de mejora para su actualización constante.

La vinculación de las actividades de control con los riesgos permite conocer la cobertura sobre esos efectos adversos, la parte del riesgo no cubierto es el riesgo residual el cual representa el apetito o riesgo tolerable que la Alta Dirección está dispuesta a asumir.

La gestión de riesgos presenta como ventajas: facilitar el logro de los objetivos, permite a la entidad estar preparados ante cambios adversos, reduciendo las posibles pérdidas, crea y fortalece la cultura del riesgo y de la imagen de la entidad, y finalmente proporciona medios que permiten la evaluación del desempeño.

VI. Glosario

Gestión de Riesgos. Es un proceso sistemático de identificar, analizar y responder y dar seguimiento a los riesgos de una organización; este proceso incluye:

- Maximizar la probabilidad y consecuencias de eventos positivos.
- Minimizar la probabilidad y consecuencias de eventos adversos a los objetivos de la compañía.

Riesgos empresariales. Lo conforman eventos o condiciones que si ocurrieran tienen un efecto adverso respecto de los objetivos de la compañía.

Riesgo inherente. Riesgo que existe por la naturaleza de los objetivos que se quieren lograr, antes de considerar los controles internos

Valoración de Riesgos. "Conlleva la existencia de un sistema de detección y valoración de los riesgos derivados del ambiente, entendidos como los factores o situaciones que podrían afectar el logro de los objetivos Institucionales".

Política de Riesgos. Conjunto de disposiciones que son emanadas por el nivel superior estratégico de una empresa, con el fin de establecer los objetivos, instrumentos, métodos y compromiso que se deberá observar para la Administración de los Riesgos.

Apetito de Riesgo. Tolerancia de la compañía por riesgo.

Capacidad de Riesgo. Máxima cantidad de riesgo que la compañía no está preparada a exceder.

Riesgo total. Es el riesgo inherente a un proceso, actividad ó una industria.

Riesgo residual. Es el riesgo que permanece después de la aplicación de controles por parte de la Administración.

Causas o factores de riesgos. También se les denomina "Amenazas". Estos son los elementos, medios, circunstancias, y agentes que generan los riesgos.

Respuesta al riesgo. Respuesta de la Alta Dirección ante la materialización de los riesgos. La mitigación de los riesgos implica acciones para reducir la probabilidad o consecuencias de un riesgo. Los costos de mitigar el riesgo deben ser apropiados y deben considerar que se espera:

- Implementar un nuevo curso de acción que reduzca el problema
- Adoptar procesos menos complejos
- Modificar las condiciones de forma que la posibilidad de ocurrencia disminuya.

Aceptar el riesgo: Es cuando se decide no modificar el plan para tratar el riesgo. Una aceptación del riesgo es establecer un plan de contingencias para accionar cuando el riesgo ocurra (aceptación activa), o no realizar actividad alguna y tratar el riesgo cuando este ocurra (aceptación pasiva).

Evitar el riesgo. Se evita un riesgo, cuando la alta dirección toma la decisión de no realizar aquellas actividades que generan riesgos.

Reducir el riesgo. Implica llevar a cabo acciones necesarias tendientes a reducir la probabilidad o el impacto del riesgo o ambos conceptos a la vez.

Compartir el riesgo. La probabilidad y el impacto del riesgo se reduce trasladando o, de otro modo, compartiendo una parte del riesgo.

Bibliografía

AS/NZS 4360:1999, Estándar Australiano de Administración de Riesgos.

Banco Central de Reserva de El Salvador (2006), Instructivo de Gestión de Riesgos y Metodología de Gestión de Riesgos del BCR, Enero.

Banco Interamericano de Desarrollo y Grupo Santander (1999), Gestión de Riesgos Financieros: Un enfoque práctico para países latinoamericanos, enero.

Banco de Pagos Internacionales (2004), Aplicación Basilea II: Aspectos Prácticos, Julio.

Instituto de Auditores Internos de España/PriceWaterHouseCoopers (2004), Marco de Referencia de Gestión de Riesgos COSO: Resumen Ejecutivo, Septiembre.

Marasca, Rubén et al (2003), Basilea II: Hacia un nuevo esquema de medición de riesgos, Diciembre.

PriceWaterHouseCoopers (2008), Seminario Taller – Workshop Top Down – Bottom Up: Una respuesta exitosa ante el reto del Riesgo Operacional, Marzo.

Samuel A. Mantilla B. (2003), Control Interno Informe COSO: Estructura conceptual integrada, ECOE Ediciones, Octubre.

The Institute Internal Auditors (IIA) (2004), El Rol de la Auditoría Interna en la Gestión de Riesgo Empresarial, www.theiia.org, Septiembre.

V. Mckee, Kenneth (1998), Metodología de Evaluación de Riesgo U.S. Federal Reserve Banks.

Banco Central de Reserva de El Salvador

http://www.bcr.gob.sv
E-mail: info@bcr.gob.sv