



GESTIÓN INTEGRAL DE RIESGOS

II Congreso Metropolitano de Ciencias Económicas
Ciudad Autónoma de Buenos Aires, 14 al 16 de noviembre de 2007

Área: Actuación Actuarial y Finanzas de la Empresa

Tema: Normas de Actuación Profesional del Actuario en Materia de Riesgos de la Empresa

Autores:

- **Mg. Paula M. Angeleri,**

CV resumido:

- Master in Information Systems - Claremont Graduate University, California, USA (becada por la Comisión Fulbright).
- Licenciada en Sistemas - Universidad de Belgrano, Buenos Aires.
- Auditora Líder de Sistemas de Gestión de la Calidad (IRAM-IRCA), Experta en Seguridad de la Información (DQS-IRAM)
- Docente de grado (Diseño de sistemas, Ing. de software, Métricas de software) en la Univ. de Belgrano. Docente de posgrado (Análisis y Diseño de sistemas) en la Univ. Tecnológica Nacional.
- Coordinadora de los subcomités de Calidad en Tecnología de la Información y de Gestión de Riesgos del IRAM.

- **Cdor. Guillermo H. Bilick**

CV resumido:

- Contador Público – Universidad Nacional de Buenos Aires.
- Auditor Interno Certificado (Internal Certified Auditor – CIA)
- Certificador/Evaluador de Calidad de Auditoría Interna.
- Gerente de Auditoría Interna de NASA – Nucleoeléctrica Argentina S.A., Empresa que administra las Centrales Nucleares Atucha I y Embalse.
- Ha realizado Cursos de Postgrado en “Logística y Solución de Casos” (Facultad de Ingeniería – UBA) y “Dirección Estratégica y Planeamiento Empresario (Facultad de Ciencias Económicas – UBA).

- **Act. Carolina Cristina Castro**

- CV resumido:

- Actuarial, egresada de la Universidad de Buenos Aires
- Directora de I+D+i en X Project S.A., empresa dedicada a la consultoría de procesos y al desarrollo de soluciones informáticas.
- Tareas de soporte de auditoría en la Auditoría General de la Nación, y la Obra Social del Personal del Organismo de Control Externo.
- Miembro de los Subcomités de Gestión de Riesgos, Calidad en Tecnología de la Información y Seguridad en Tecnología de la Información del IRAM.



- **Cdor. Julio Maroño**

CV resumido:

- Contador Público y Licenciado en Administración (Universidad de Buenos Aires)
- Master en Finanzas (UCEMA)
- Consultor especializado en Organización y Métodos para la adecuación de procesos y tecnología en Entidades Financieras.
- Gerente de Servicios a la Industria Financiera BDO-Becher (Argentina) a cargo del Departamento de Consultoría.
- Líder en implementación de la práctica de Administración de Riesgos.

- **Cdor. Carlos F. Rozen**

CV resumido:

- Contador Público (Universidad de Buenos Aires)
- Auditor Líder en Sistemas de Gestión de Calidad (The Georgia Institute of Technology)
- Socio de BDO-Becher (Argentina) a cargo del del Departamento de Auditoría Interna y Mejora de Procesos.
- Líder en la implementación de la Ley Sarbanes Oxley para BDO Latinoamérica.
- Integrante del Comité RAS – Risk Advisory Services – BDO Mundial



GESTIÓN INTEGRAL DE RIESGOS

II Congreso Metropolitano de Ciencias Económicas
Ciudad Autónoma de Buenos Aires, 14 al 16 de noviembre de 2007

Área: Actuación Actuarial y Finanzas de la Empresa

Tema: Normas de Actuación Profesional del Actuario en Materia de Riesgos de la Empresa



Índice

Índice.....	4
Resumen.....	5
Evolución del concepto de <i>gestión de riesgos</i>	6
1. Estándares	6
Gestión de riesgos, Basilea II y COSO	7
1. Gestión de riesgos y Basilea II	7
2. Los nuevos conceptos del control interno y gestión de riesgos (Informes COSO I y II).....	8
El marco COSO (Committee of Sponsoring Organizations of the Treadway Commission) es un esfuerzo voluntario del sector privado para mejorar la calidad de los reportes financiero a través de elementos tales como la ética en los negocios, controles internos efectivos y adecuadas prácticas de gobierno corporativo.....	8
El rol de los organismos de normalización	9
1. ISO (International Organization for Standardization)	9
2. IRAM (Instituto Argentino de Normalización y Certificación)	9
Las normas argentinas: IRAM 17550 y el proyecto de certificación (IRAM 17551).....	10
1. El proceso de gestión de riesgos y la IRAM 17550.....	11
Adopción de la IRAM 17550 por organismos de auditoría del estado nacional	13
1. Identificación del riesgo.....	13
2. Determinación del Impacto	13
3. Determinación de la probabilidad.....	13
4. Elaboración de la Matriz de Exposición	13
Bibliografía	14



Resumen

Esta presentación pretende brindar un panorama de la gestión de riesgos en sus aspectos generales y la situación actual del desarrollo de estándares que sirvan de guía para el diseño de una adecuada gestión para la evaluación y el tratamiento de los riesgos que enfrenta una organización, cualquiera sea su forma jurídica, sector o país en el que ésta desarrolle sus actividades. Considera dentro del análisis los estándares más conocidos a nivel internacional (Basilea II, COSO-ERM, y AS / NZS 4360), así como el estándar vigente actualmente en Argentina (IRAM 17550), y su proyecto de norma certificable (IRAM 17551).



Gestión integral de riesgos

Esta presentación pretende brindar un panorama de la gestión de riesgos en sus aspectos generales y la situación actual del desarrollo de estándares que sirvan de guía para el diseño de una adecuada gestión para la evaluación y el tratamiento de los riesgos que enfrenta una organización, cualquiera sea su forma jurídica, sector o país en el que ésta desarrolle sus actividades.

Evolución del concepto de *gestión de riesgos*

La idea de gestionar sistemáticamente los riesgos a los que está expuesta una organización surgió en la segunda mitad del siglo XX. Tradicionalmente, siempre se han identificado, analizado y tratado de alguna forma los riesgos a los que está expuesta una actividad, pero en los últimos años se han agregado consideraciones adicionales, tales como:

- la **interacción** de los distintos riesgos enfrentados por la **organización en su conjunto**,
- la **responsabilidad de la dirección** de la organización en la gestión de riesgos,
- gestión de **todos** los riesgos enfrentados por la organización,
- la visión del riesgo no sólo como destructor, sino también como posible **creador de valor**,
- la **cuantificación** del riesgo,
- la expansión de la gestión de riesgos a **todo tipo** de organizaciones (financieras, industriales, gubernamentales, ONGs, etc.),
- la creación de estándares para la gestión de riesgos como concepto general y aplicado a distintos sectores.

La gestión de riesgos evolucionó desde la consideración de los riesgos en forma individual hacia el análisis conjunto y coordinado de las oportunidades y peligros a los que se enfrenta la organización. Esto es lo que consideramos la *gestión integrada de riesgos* (o ERM, Enterprise Risk Management).

1. Estándares

Numerosos organismos han emitido estándares relacionados con la gestión de riesgos. Entre los más conocidos se encuentran:

- Basilea II
- COSO
- Estándar de Australia / Nueva Zelanda (AU/NZS 4360)

Pueden mencionarse también otros estándares (Basilea I, estándares emitidos por asociaciones de profesionales de gestión de riesgos, normativa de supervisores de seguros, financieros, etc.), además de estándares en desarrollo (ISO 31000, Solvencia II, etc.).



En general, consideran estos aspectos:

- la definición de “riesgo” para el estándar o norma (puede incluir una clasificación),
- participación de la dirección en el proceso,
- énfasis en el proceso de control interno,
- aspectos relacionados con la cuantificación y el tratamiento de los riesgos,
- requisitos relacionados con la estructura organizacional de la empresa y la documentación del sistema.

Gestión de riesgos, Basilea II y COSO

1. Gestión de riesgos y Basilea II

La Industria Bancaria ha impulsado grandes cambios en la gestión de Riesgos a través del nuevo estándar de Basilea II para estimar la suficiencia de Capital. Dicho estándar surge como propuesta del Comité de Basilea, un grupo conformado en 1974 por los presidentes de los Bancos Centrales de los 10 principales países, cuya función es determinar lineamientos de supervisión bancaria, recomendando prácticas óptimas en una amplia gama de temas. Basilea II es un estándar que propone entre otras medidas regulatorias, mecanismos de evaluación de riesgos a adoptar por los regulados para determinar cual es el capital mínimo a mantener. Dichos riesgos se presentan en 3 categorías:

- Riesgo de Crédito
- Riesgo de Mercado
- Riesgo Operativo

El primer riesgo consiste en la posibilidad de no poder recuperar los préstamos otorgados por problemas con la morosidad de los clientes, el segundo consiste en la posibilidad de pérdidas ocasionada por volatilidades en las posiciones mantenidas en los instrumentos financieros, y el tercero obedece a la probabilidad de pérdidas por fallas en los procesos, sistemas y personal, combinado o no con acciones externas.

Si bien para los dos primeros riesgos existe un amplio consenso respecto de su medición y aplicación, no sucede lo mismo respecto al riesgo operativo. Para éste último Basilea II propone mecanismos de medición que van desde una ponderación simple (indicador básico y estándar) hasta la aplicación de modelos cuantitativos y cualitativos supervisados por el Directorio de la Entidad, y autorizados por el Ente Supervisor.

Este último método además ha sido el más controversial respecto a los modelos matemáticos válidos a aplicar, puesto que éstos deben combinar información de eventos de riesgos del pasado con correlaciones estadísticas para proyectar curvas de distribución de cada riesgo a cuantificar. Si bien muchos modelos propuestos son matemáticamente válidos, su complejidad de aplicación dificulta su difusión en el mercado. Por otra parte, si bien los modelos de ponderación cuali-cuantitativa desarrollados (como por ejemplo el estándar australiano) son amigables y de aplicación simplificada, deben ser reforzados para su utilización como indicadores del capital expuesto a riesgo por la organización.



2. Los nuevos conceptos del control interno y gestión de riesgos (Informes COSO I y II)

El marco COSO (Committee of Sponsoring Organizations of the Treadway Commission) es un esfuerzo voluntario del sector privado para mejorar la calidad de los reportes financieros a través de elementos tales como la ética en los negocios, controles internos efectivos y adecuadas prácticas de gobierno corporativo.

El marco COSO fue originalmente desarrollado en 1985 por la “National Commission on Fraudulent Financial Reporting”, un organismo privado e independiente que estudió las principales causas que pueden conducir a presentar reportes financieros fraudulentos y desarrollaron recomendaciones para compañías públicas y sus auditores externos, para la SEC (Securities and Exchange Commission) y para otros organismos reguladores, así como, para instituciones educativas.

En la comisión participaron cinco de las principales asociaciones financieras de los Estados Unidos, la “American Accounting Association”, el “American Institute of Certified Public Accountants”, el “Financial Executives Institute”, el “Institute of Internal Auditors” y la “National Association of Accountants”. La comisión fue totalmente independiente de cada uno de sus organismos y contenía adicionalmente representantes de la industria, contaduría pública, firmas de inversión y el mercado de valores de New York.

La Treadway Commission tenía la visión de un estudio integral completo y una evaluación de controles cuando recomendó que sus compañías públicas ejecutaran los siguientes pasos en sus esfuerzos por prevenir y detectar información financiera fraudulenta:

Identificar y comprender los factores que pueden conducir a reportar información financiera fraudulenta incluyendo factores que son únicos o específicos para cada organización.

Evaluar el riesgo de reportar información financiera fraudulenta creada por estos factores dentro de las organizaciones.

Diseñar e implementar controles que proporcionen seguridad razonable que el reportar información financiera fraudulenta será prevenido y detectado

Los controles internos se diseñan e implantan con el fin de detectar, en un plazo deseado, cualquier desviación respecto a los objetivos de rentabilidad establecidos para cada empresa y de prevenir cualquier evento que pueda evitar el logro de los objetivos, la obtención de información confiable y oportuna y el cumplimiento de leyes y reglamentos. Si analizamos lo antedicho, tendremos la definición de “control” en los términos que utiliza la Gestión de Riesgos.

Los controles internos fomentan la eficiencia, reducen el riesgo de pérdida de valor de los activos y ayudan a garantizar la confiabilidad de los estados financieros y el cumplimiento de las leyes y normas vigentes.

En sentido amplio, Control Interno se define como: *un proceso efectuado por el Consejo de Administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos.*



En el 2004 aparece COSO ERM – Enterprise Risk Management (COSO II) que según la opinión de muchos expertos no resulta en un esfuerzo aislado, sino que es un complemento del modelo anterior introduciendo algunos elementos relacionados con Administración de Riesgos, resultando un modelo de Administración de Riesgos que contempla:

3 Objetivos de la Gestión de Riesgos

Objetivos estratégicos

Eficiencia y Eficacia operativa

Confiabilidad en la Información

Cumplimiento Normativo y Regulatorio

8 Componentes o Pilares de la Gestión de Riesgos

Ambiente interno

Establecimiento de objetivos

Identificación de acontecimientos

Evaluación de riesgos

Respuesta a los riesgos

Actividades de control

Información y comunicación

Supervisión

El rol de los organismos de normalización

Los organismos de normalización han emitido o tienen en estudio normas para estandarizar los conceptos relacionados con gestión de riesgos.

En el nivel internacional, podemos mencionar a:

1. ISO (International Organization for Standardization)

ISO se creó en 1946 en una conferencia de organismos nacionales de normalización en Londres, con el objetivo de crear un organismo internacional para coordinar y unificar estándares nacionales.

Los estándares internacionales sirven como marco de referencia o lenguaje común entre proveedores, clientes, gobiernos, consumidores, etc., para evaluar bienes o servicios, en base a criterios de calidad, seguridad, etc., y así facilitar el comercio internacional.

Las normas surgen de comités de trabajo en los que participan los organismos de normalización de cada país miembro.

En la actualidad, está en tratamiento un borrador de norma ISO sobre gestión de riesgos, la futura ISO 31000 *Risk management — Guidelines on principles and implementation of risk management*⁽¹⁾.

Y, a nivel argentino:

2. IRAM (Instituto Argentino de Normalización y Certificación)

(1) Fecha estimada de publicación, 30/06/2009. Ver: http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43170



IRAM, asociación civil sin fines de lucro, nació como el Instituto Argentino de Racionalización de Materiales, en el año 1935. Luego de la creación del Sistema Nacional de Normas, Calidad y Certificación (decreto 1474/1994), fue designado como Organismo Nacional de Normalización por la Secretaría de Industria de la Nación, y cambió su denominación por la actual. Es el representante de la Argentina en la ISO, en la Comisión Panamericana de Normas Técnicas (COPANT), y en la Asociación MERCOSUR de Normalización (AMN).

Tiene entre otros fines, el de elaborar normas técnicas y brindar servicios de certificación para promover el uso racional de recursos y facilitar la producción, el comercio y la transferencia de conocimiento.

En los comités de estudio de normas participan representantes de empresas de distintos sectores, instituciones educativas, gobierno en sus distintos niveles, etc.

Las normas argentinas: IRAM 17550 y el proyecto de certificación (IRAM 17551)

A inicios del 2004, se constituyó el “Subcomité de Gestión de Riesgos”, dentro del IRAM, integrado por un equipo de profesionales en Ciencias Económicas, en Ingeniería, Sistemas, y otras disciplinas, que, además de los conocimientos y experiencias propios de sus profesiones, resultaban ser versados en gestión de riesgos, procesos, calidad, medioambiente, auditoría y consultoría, provenientes de actividades propias tanto del ámbito público – gobierno – como así también privado, y que participan además en diferentes entidades académicas y asociaciones profesionales.

Los diferentes criterios y enfoques constituyeron ser una sumatoria con todos los resultados orientados hacia un mismo fin: obtener una base común sobre la cual gestionar riesgos, minimizando sus efectos negativos, y a la vez aprovechando las oportunidades derivadas de los mismos.

Luego de un detallado análisis de los diferentes documentos y estándares referidos a la administración de riesgos, hemos desarrollado sobre la base de los principales conceptos contenidos en los mismos – en especial el estándar de Riesgos Australiano/Neozelandés –, el primer estándar argentino sobre Gestión de Riesgos: la Norma IRAM 17550.

El Subcomité consideró especialmente y llevó a cabo el análisis exhaustivo, entre otras, de las siguientes normas: Risk Management AS/NZS 4360:1999; Risk Management AS/NZS 4360:2004; Integrated Risk Management Framework – Canada 2001; A Risk Management Standard – Published by AIRMIC, ALARM, IRM:2002; ISO/IEC Guide 73:2002; COSO; COSO-ERM Framework.

En nuestra opinión, el estándar logrado Norma IRAM 17550, servirá como herramienta de gestión empresarial “integral”, es decir, abarcadora de una organización –como un todo – y este enfoque debe servir de base para definir el contexto, identificar, analizar, evaluar y tomar adecuadas decisiones frente al riesgo.

El objeto de este trabajo no pretende tratar tipos de riesgos en particular, ni siquiera grupos de riesgos, o actividades puntuales sujetas a riesgos, por el



contrario, se trata de un enfoque metodológico global y abarcador, y por sobre todas las cosas orientado a la Gestión.

A su vez, como producto de la continuidad mantenida en el presente proyecto estamos logrando poner a discusión pública en los próximos días un estándar certificable.

Como conclusión queremos puntualizar que, a nuestro criterio, la Norma IRAM 17551 estándar certificable, permitirá mediante su correcta aplicación, que cualquier tipo de organización – sin importar el tamaño o volumen de sus operaciones, sea pública a privada –, logre identificar y gestionar sus riesgos, de manera tal que pueda asegurar en forma razonable alcanzar los objetivos propuestos; y asimismo, pueda no sólo lograrlo sino acreditarlo, mostrando a las partes interesadas que pudo certificar públicamente su adecuada Gestión de Riesgos.

1. El proceso de gestión de riesgos y la IRAM 17550

La gestión de riesgos es una parte integrante del proceso de gestión. La gestión de riesgos es un proceso multifacético, por lo que las tareas involucradas son a menudo llevadas a cabo por un equipo multidisciplinario. Es un proceso iterativo de mejora continua, cuya incorporación en las prácticas o procesos de negocio existentes resulta beneficiosa.

1.1. Elementos principales

Establecer el contexto: Establecer los contextos estratégico, organizacional y de gestión de riesgos en los cuales tendrá lugar el resto de los procesos. Deberán establecerse los criterios contra los cuales se evaluarán los riesgos y definirse la estructura del análisis.

Identificar riesgos: Identificar qué, por qué, dónde, cuándo y cómo los eventos podrían impedir, degradar, demorar o mejorar el logro de los objetivos estratégicos y de negocio de la organización.

Analizar riesgos: Determinar los controles existentes y analizar los riesgos en términos de consecuencia y probabilidad en el contexto de tales controles. El análisis debería considerar el rango de consecuencias potenciales y cuán probable es que esas consecuencias puedan ocurrir. Consecuencia y probabilidad deberían ser combinadas para producir un nivel estimado de riesgo.

Evaluar riesgos: Comparar los niveles estimados de riesgo contra los criterios preestablecidos y considerar el balance entre beneficios potenciales y resultados adversos. Esto posibilita que los riesgos sean ordenados como para identificar las prioridades de gestión. Si los niveles de riesgo establecidos son bajos podría caer en una categoría aceptable y no se requeriría tratamiento.

Tratar riesgos: Si los niveles de riesgo establecidos son bajos y son tolerables entonces no se requiere tratamiento. Para otros riesgos desarrollar e



implementar estrategias y planes de acción específicos costo-beneficios para aumentar los beneficios potenciales y reducir los costos potenciales.

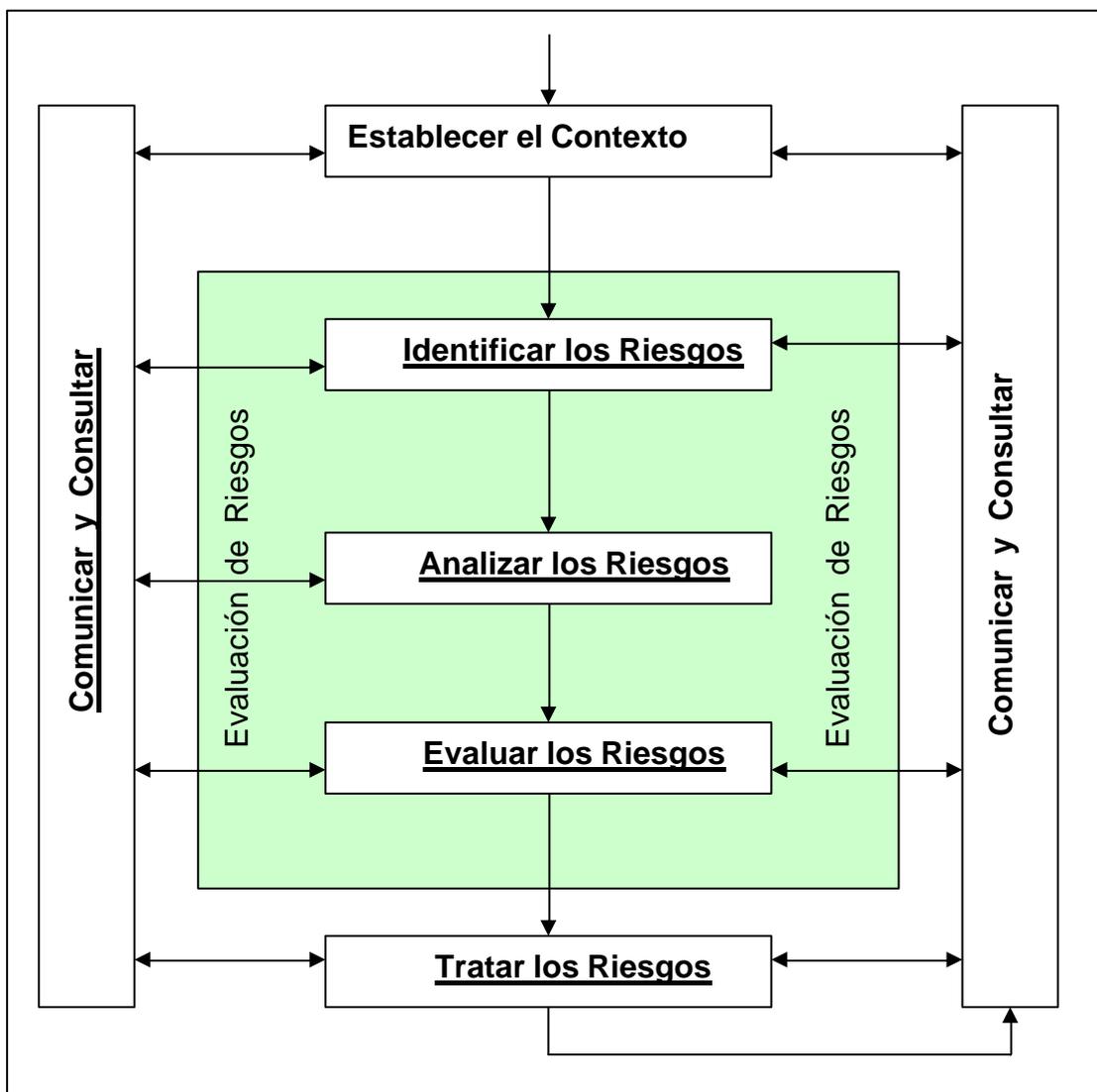
Monitorear y revisar: Monitorear y revisar el desempeño del sistema de gestión de riesgos y procurar detectar cambios que pudieran afectar la adecuación o beneficio de costo de los controles.

Comunicar y consultar: Comunicar y consultar con interesados internos y externos según resulte apropiado en cada etapa del proceso de administración de riesgos e interpretando al proceso como un todo.

La gestión de riesgos es un proceso iterativo que puede contribuir a la mejora organizacional. Puede ser aplicada a todos los niveles en una organización: a nivel estratégico y a niveles tácticos y operacionales. También puede ser aplicada a proyectos específicos, para sustentar decisiones específicas o para administrar áreas específicas de riesgo reconocidas. Para cada etapa del proceso deberían mantenerse registros adecuados, suficientes como para satisfacer a una auditoría independiente.

1. 2. Proceso de Gestión de Riesgos

Vista General





Adopción de la IRAM 17550 por organismos de auditoría del estado nacional

La Sindicatura General de la Nación – SiGeN – ha definido para la elaboración de los Planes Anuales de Auditoría, para todas las Unidades de Auditoría Interna que le dependen, en cuanto a la metodología de análisis de riesgos aplicada, que deben tenerse en cuenta entre los principales antecedentes normativos a la Norma IRAM 17550: Sistema de gestión de riesgos. Directivas Generales.

El proceso comprende las etapas de identificación del riesgo, y de determinación del impacto y la probabilidad a los efectos de elaborar la Matriz.

1. Identificación del riesgo

Se propone encarar la tarea considerando como riesgo principal aquel relativo al incumplimiento de los objetivos, ya sean globales o específicos de la misión del organismo u organización.

Complementariamente, sobre la base de información disponible relativa a la eficacia del sistema de control interno, se deben considerar los riesgos o vulnerabilidades en cuanto a:

- Empleo de criterios de eficiencia y economía.
- Cumplimiento de normativa vigente, incluyendo las políticas y procedimientos propios de la empresa.

2. Determinación del Impacto

En relación con los objetivos de las políticas de gobierno se consideran dos aspectos: **prioridad y criticidad**. Se asigna mayor ponderación a la **prioridad** que a la **criticidad** para la determinación del nivel de impacto.

La **prioridad** se evalúa estableciendo la precedencia de los objetivos asociados a cada función respecto de los objetivos asignados a las otras.

La **criticidad** refleja la medida en que la gestión de una función condiciona el desempeño de funciones asociadas a otros objetivos y el grado de urgencia percibido.

3. Determinación de la probabilidad

El criterio a adoptar es considerar que la probabilidad de los riesgos se verá directamente afectada por la calidad del control interno.

En ese sentido, para determinar la probabilidad se elabora una matriz en la cual se consideraron diversos factores que permitieran reflejar la eficacia del control interno.

4. Elaboración de la Matriz de Exposición



Con los valores determinados para probabilidad e impacto se agrupan en una determinada cantidad de intervalos. La relación probabilidad/impacto define la Matriz de Exposición.

Bibliografía

- Norma IRAM 17550: Sistema de gestión de riesgos. Directivas generales. Instituto Argentino de Normalización y Certificación (IRAM), 2005.
- Proyecto de norma IRAM 17551: Sistema de gestión de riesgos. Requisitos. Subcomité de Gestión de Riesgos, Instituto Argentino de Normalización y Certificación (IRAM), 2007.
- “Enterprise Risk Management – Integrated Framework”. 2004, Committee of Sponsoring Organizations of the Treadway Commission (COSO), 2004.
- “Internal Control – Integrated Framework”. Committee of Sponsoring Organizations of the Treadway Commission (COSO), 1992.
- “Core Principles for Effective Banking Supervision”. Basel Committee on Banking Supervision, 2006.
- “Core Principles Methodology”. Basel Committee on Banking Supervision, 2006.
- “Buenas prácticas para la administración del riesgos operacional en entidades Financieras”, Enero 2007, Miguel Delfiner, Ana Mangialavori y Cristina Pahilé, Gerencia de Investigación y Planificación Normativa, Banco Central de la República Argentina.