Ing. Carlos Ormella Meyer y Asoc.
Gestión y Auditoría de Riesgos y Seguridad de la Información
Tel: +54-11-4371-4638 – Cel: +54-911-6513-2751
E-mail: ciprio@ingcomyasoc.com.ar

NORMA ISO 31000 DE RIESGOS CORPORATIVOS

La norma **ISO 31000** establece principios y guías para el diseño, implementación y mantenimiento de la gestión de riesgos en forma sistemática y transparente de toda forma de riesgo en cualquier contexto.

Esta norma responde a una internacionalización de la norma **AS/NZS 4360** que, desde hace años se viene aplicando especialmente en Australia y Nueva Zelanda, pero también en otros países, habiendo sido incluso traducida en varios países como Argentina (**IRAM 17550**).

.

La **ISO 31000** se publicó en noviembre de 2009, al mismo tiempo que una nueva versión de la **Guide 73**, también de la ISO, que ofrece una lista de más de 50 términos referidos a la gestión de riesgos con sus correspondientes definiciones (ver recuadro **ISO Guide 73**).

Un punto trascendente de dicha Guía, y que se incorpora a la **ISO 31000**, es el nuevo concepto de riesgo.

Efectivamente, hasta ahora el riesgo se ha venido tratando como la posibilidad que algo ocurra que tenga un **impacto en los objetivos**.

Pero a partir de la **ISO 31000**, el riesgo se define (con ajuste a la **Guide 73**) en términos del efecto de la **incertidumbre en los objetivos**.

La nueva definición implica que la palabra **"riesgo"** se refiere tanto a las situaciones negativas tradicionales de riesgo (***downside risk***) que provocan **pérdidas**, como a las situaciones positivas de riesgo (***upside risk***), que constituyen **oportunidades**.

El nuevo concepto de riesgo y el concepto de ***oportunidades*** ha sido incorporado en la **ISO 27001** (1).

La norma ISO 31000 se puede aplicar a cualquier tipo de riesgo, por ejemplo financieros, de infraestructura, de operación, de mercado, de imagen/reputación corporativa, etc., además por supuesto de la seguridad de la información

Este concepto también se ha incorporado a la **ISO 27001** en el tema de **Valuación de Riesgos** (1).

La generalización de los tipos de riesgos implica que la norma no está pensada para un sistema de gestión en particular ni tampoco para un grupo particular de empresas, sino más bien para proveer una estructura de mejores prácticas y guía para todas las operaciones relacionadas con la gestión de riesgos.

ISO Guide 73

Una de las definiciones más trascendentes de esta Guía, por el cambio que implica respecto a definiciones anteriores, dice que: **"el riesgo es el efecto de la incertidumbre en los objetivos".**

Esta conexión entre riesgos y objetivos implica que una organización debe definir y expresar en forma total y exhaustiva sus objetivos.

Varias **Notas** complementan la nueva definición. Entre ellos se destacan dos.

Una de ellas establece que la desviación de lo esperado en los objetivos puede ser ***positiva* y/o *negativa***.

Otra de las **Notas**, define que los objetivos pueden responder a diferentes aspectos, tales como metas financieras, de salud y seguridad, y ambiental, y que pueden aplicarse a diferentes niveles tales como estratégico, de proyecto, producto y proceso, o incluso de toda la organización.

Esta aproximación en la formalización de las prácticas de gestión de riesgos facilita una mayor adopción por empresas que requieren una norma de gestión de riesgos empresariales que permita incluir múltiples sistemas de gestión.

De esta manera, el **alcance** de la norma a la gestión de riesgos consiste en habilitar todas las tareas estratégicas, de gestión y operacionales de una organización por medio de proyectos, funciones y procesos alineados a un conjunto común de objetivos de gestión de riesgos.

De la misma manera que el nuevo concepto de riesgo con las oportunidades y la valuación de riesgos, el proceso de tratamiento de riesgos también se ha alineado en la **ISO 27001** (1) con los principios y guías de la norma **ISO 31000**.

La **ISO 31000** está estructurada en tres elementos claves para una gestión de riesgos efectiva, transparente, sistemática y creíble. Dichos elementos son:

1) **Principios** de la gestión de riesgos.
2) **Marco de trabajo** (framework) para la gestión de riesgos.
3) **Proceso** de gestión de riesgos.

Principios de la ISO 31000

En primer término, una efectiva gestión de riesgos debiera satisfacer una serie de **Principios** según el listado que sigue.

1) Crear y proteger el valor
2) Estar Integrada a todos los procesos de la organización
3) Ser parte de la toma de decisiones
4) Tratar explícitamente la incertidumbre
5) Ser sistemática, estructurada y oportuna.
6) Basarse en la mejor información disponible
7) Alinearse al contexto y al perfil de riesgos de la organización
8) Tener en cuenta los factores humanos y culturales
9) Ser transparente e inclusiva.
10) Ser dinámica, iterativa y sensible al cambio
11) Facilitar la mejora continua

Marco de Trabajo de la ISO 31000

El segundo elemento clave es el **Marco de Trabajo** o **Marco de Referencia**, o estructura de soporte, cuyo objetivo es integrar el proceso de gestión de riesgos al **gobierno corporativo**.

Por cierto esta relación con el **corporate governance** (2) refuerza la importancia de las decisiones estratégicas de alto nivel con referencia a la seguridad de la información.

La **ISO 31000** recomienda desarrollar, implementar y mejorar en forma continua un marco de referencia, cuyo propósito es integrar el proceso de la gestión de riesgos en el gobierno, estrategia y planificación, gestión, informes de los procesos, políticas, valores y cultura de toda la organización.

El **Marco de Trabajo**, que puede verse gráficamente en la Figura 1, sigue básicamente los lineamientos del ciclo de vida **PDCA** luego de una etapa previa de **Mandato y Compromiso**.

Para el caso, la norma establece una serie de **mandatos** a cumplir por parte de la gerencia para asegurar la ***efectividad*** de la gestión de riesgos, lo que requiere un **compromiso** fuerte y sostenido por parte de la gerencia, así como una planificación estratégica y rigurosa.

Dichos **mandatos** conforman los puntos que siguen:

Figura 1

a) Articular y avalar la ***política*** de gestión de riesgos.
b) Determinar de los ***indicadores de desempeño*** alineados con los de la organización.
c) Asegurar el ***alineamiento de los objetivos*** de la gestión de riesgos con los objetivos y estrategias de la organización.
d) Asegurar las ***conformidades*** legales y regulatorias.
e) Asignar ***rendición de cuentas y responsabilidades*** conforme los diferentes niveles de la organización.
f) Asegurar que se dispongan los ***recursos*** necesarios para la gestión de riesgos.
g) Comunicar los ***beneficios*** de la gestión de riesgos a todas las partes interesadas.
h) Asegurar que se mantenga el ***marco de trabajo apropiado*** para la gestión.

Por su parte, las cuatro fases propias del ciclo **PDCA** se refieren a:

1) El **diseño** del marco de referencia para la gestión del riesgo, que incluye los siguientes puntos:
   a) ***Comprensión*** de la organización y su contexto, tanto interno como externo, a partir de las definiciones correspondientes de la **Guide 73**.
   b) ***Política*** de gestión de riesgos.
   c) ***Integración*** con los procesos de la organización.
   d) ***Rendición de cuentas***.
   e) ***Recursos***.
   f) Establecimiento de las ***comunicaciones internas*** y los mecanismos de informes.
   g) Establecimiento de las ***comunicaciones externas*** y los mecanismos de informes.
2) La **implementación** del marco de referencia de riesgos, en dos aspectos:
   a) Implementación del marco de trabajo para la gestión de riesgos
   b) Implementación del proceso de gestión de riesgos.
3) El **monitoreo y revisión** de la efectividad del marco de trabajo. Establecimiento de las medidas de desempeño, revisión periódica del avance y desviaciones, informes, y revisión de la efectividad del marco de trabajo.
4) La **mejora continua** del marco de trabajo. Decisiones para mejorar la gestión de riesgo y la cultura correspondiente.

Proceso de la ISO 31000

El tercer elemento clave de la norma es el **Proceso** de riesgos que se muestra en la Figura 2

Básicamente el Proceso de gestión de riesgos tiene tres etapas: **Establecimiento del contexto, Valuación de riesgos y Tratamiento** de los mismos.

A su vez, la **Valuación** (***assessment***) de los riesgos está constituida en forma progresiva por la **Identificación, Análisis, y Evaluación (*evaluation*) de riesgos.**

Un verdadero pilar de la norma es establecer el **contexto** en el que opera la organización.

Concretamente se trata de establecer tanto el contexto interno como externo, es decir, los entornos correspondientes en los que la organización busca alcanzar sus objetivos, así como también establecer el proceso para la gestión de riesgos, y la definición de los criterios de evaluación de los mismos.

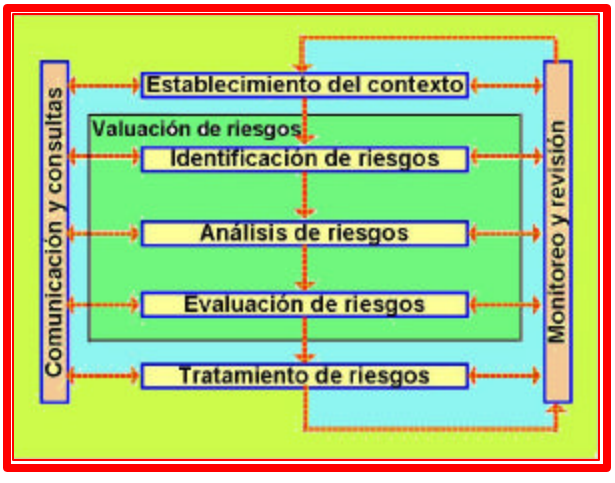

Figura 2

Algunos de estos parámetros son similares a los que se consideran en la fase de Diseño del Marco de Trabajo, pero en esta etapa hay que considerarlas en mayor detalle en referencia al Proceso de gestión de riesgos.

Por su parte, en el paso de selección de opciones de tratamiento de los riesgos, la norma da una lista de opciones aplicables en forma individual o concurrente en dicho tratamiento, que se muestran a continuación.

1) Evitar el riesgo decidiendo no comenzar o continuar con la actividad que da lugar al riesgo en cuestión.
2) Aceptar o incrementar el riesgo con el objeto de concretar una *oportunidad*.
3) Remover la fuente de riesgo.
4) Cambiar la probabilidad.
5) Cambiar las consecuencias (impactos).
6) Compartir el riesgo con terceros (incluyendo contratos y financiamiento del riesgo).
7) Retener el riesgo por decisión propia.

El Proceso de Gestión de Riesgos finalmente se cierra con la interconexión de todas las etapas mencionadas con la **Comunicación y Consultas** por un lado, y el **Monitoreo y Revisión** por el otro.

Como puede observarse, hay gran similitud con los procesos de la **ISO 27005**, desde que esta norma en su última versión se adaptó precisamente a la **ISO 31000**.

Anexo de la ISO 31000

La meta de una organización debe procurar un nivel adecuado de **desempeño** del marco de trabajo, conforme la criticidad de las decisiones correspondientes.

La norma responde a esto con un **Anexo** referido a los **atributos** que caracterizan una gestión avanzada de riesgos, a partir de **metas** explícitas de **desempeño**.

Estos **atributos** son los que siguen:

1) Mejora continua
2) Rendición de cuentas
3) Aplicación de la gestión de riesgos en la toma de decisiones
4) Comunicación permanente
5) Integración con el gobierno corporativo de la organización

Adicionalmente, el Anexo proporciona algunos **indicadores** para medir el desempeño de cada uno de dichos atributos.

Con dichos **indicadores** y **metas** se puede incluso trabajar con el **Balanced ScoreCard (BSC)** definiendo los **objetivos** e **iniciativas** correspondientes para lograr cumplir las respectivas metas (3).

Norma ISO 31010

Un complemento muy útil de la norma **ISO 31000** es la **ISO 31010** de ***Técnicas de Valuación de Riesgos***.

La **ISO 31010** primero revisa el proceso de **Valuación de Riesgos** y luego los diferentes criterios para la selección de las técnicas correspondientes.

Dos extensos **Anexos** completan esta norma.

Un **Anexo** de la **ISO 31010** ofrece una tabla de 31 técnicas diferentes y su aplicación a las diferentes etapas del proceso de valuación de riesgos, así como la respectiva relevancia respecto de recursos, incertidumbre, complejidad y posibilidad de resultados cuantitativos.

El otro **Anexo** de esta norma analiza las diferentes técnicas en cuando a su uso, requerimientos de entrada, proceso, resultados, y fortalezas y limitaciones.

Ing. Carlos Ormella Meyer y Asoc.
Gestión y Auditoría de Riesgos y Seguridad de la Información
Tel: +54-11-4371-4638 – Cel: +54-911-6513-2751
E-mail: ciprio@ingcomyasoc.com.ar

ISO 31000 y COSO ERM

En los últimos dos años la **ISO 31000** ha sido extensamente comparada con **COSO ERM**, es decir la ***Gestión de Riesgos Empresariales de COSO***.

COSO ERM tiene su origen en la primera versión de **COSO** de 1992, y cuyo núcleo principal ha estado, *y sigue estando*, centrado en los ***controles internos*** especialmente de carácter financiero.

En 2004 apareció lo que suele denominarse **COSO II**, donde al **COSO** original se incorpora la **gestión de riesgos**.

El uso del **ERM** de **COSO** se ha difundido mucho especialmente en Estados Unidos entre contadores y auditores. Incluso la ley americana Sarbanes-Oxley hace referencia a su uso en la Sección 404.

Contrastando en general con **ERM COSO**, la **ISO 31000** es una norma de sólo 20 páginas, nada compleja, fácil de comprender, clara y práctica, escrita por especialistas en riesgos.

La **ISO 31000** se viene expandiendo rápidamente ya que, si bien es bastante reciente, se valora la experiencia acumulada de la **AS/NZS 4360** originada hace casi 20 años y que fuera revisada posteriormente en 2004.

De hecho, la influencia de la **ISO 31000** se puede llegar a reflejar en las próximas versiones de **COSO** y otros estándares de gestión de riesgo como **FERMA, IRM, M_o_R, y Solvency II**, entre otros.

Referencias

(1) www.angelfire.com/la2/revistalanandwan/nuevas_versiones_ISO_27001_e_ISO_27002.pdf
(2) www.criptored.upm.es/descarga/normas_segu_info_marzo_2014.pdf
(3) www.criptored.upm.es/descarga/MetricasSeguInfoBSC.zip