INTOSAI GOV 9130

Las Normas Internacionales de las Entidades Fiscalizadoras Superiores (ISSAI) son emitidas por la Organización Internacional de Entidades Fiscalizadoras Superiores (INTOSAI). Para más información visite *www.issai.org*

INTOSAI

Guía para las Normas del Control Interno del Sector Público

Información adicional sobre la Administración de Riesgos de la Entidad

INTOSAI Professional Standards Committee

PSC-Secretariat

Rigsrevisionen • Landgreven 4 • P.O. Box 9009 • 1022 Copenhagen K • Denmark

Tel.:+45 3392 8400 • Fax:+45 3311 0415 • E-mail: info@rigsrevisionen.dk

I N T O S A I

EXPERIENTIA MUTUA

OMNIBUS PRODEST

INTOSAI General Secretariat - RECHNUNGSHOF
(Austrian Court of Audit)
DAMPFSCHIFFSTRASSE 2
A-1033 VIENNA
AUSTRIA
Tel.: ++43 (1) 711 71 • Fax: ++43 (1) 718 09 69

E-MAIL: intosai@rechnungshof.gv.at;
WORLD WIDE WEB: http://www.intosai.org

Sub-Comité de Normas de Control Interno de la INTOSAI

F. VANSTAPEL
Primer Presidente del Tribunal de Cuentas de Bélgica

Regentschapsstraat 2 – Rue de la Régence 2
B-1000 BRUSELAS
BÉLGICA

Tel : + 32 2 551 8111
Fax : + 32 2 551 8629
E-mail: international@ccrek.be

Guía para las Normas del Control Interno del Sector Público – Información adicional sobre la Administración de Riesgos de la Entidad

Prefacio

La *Guía para las Normas de control interno del sector público* de 1992 de la INTOSAI, fue concebida como un documento vital reflejando la visión que las normas pueden ser promovidas para el diseño, implementación y la evaluación del control interno. Esta visión implica un esfuerzo continuo para mantener la guía actualizada.

La 17ma Reunión de la INCOSAI (Seúl, 2001) reconoció una fuerte necesidad de actualizar la Guía de 1992 y acordó la utilización del marco integrado de control interno del Comité de Organizaciones que patrocinan la Comisión de Treadway (COSO). Consultas subsecuentes dieron resultados a una mayor extensión para tratar los valores

éticos y proporcionar mayor información sobre los principios generales de las actividades del control relativos al tratamiento de la información.

La Guía actualizada para las normas de control interno fue emitida en el 2004, y puede ser considerada como un documento trascendental que debería ser desarrollado y perfeccionado continuamente para incorporar el impacto de nuevos avances como la Estructura de Manejo de Riesgo corporativo del COSO[1]. Por consiguiente, estas extensiones a la Guía han sido elaboradas para cubrir las tendencias actuales en la Administración de Manejo de Riesgos, según lo precisado en la estructura ERM del COSO. Siendo este documento dirigido principalmente para el sector público, el término "entidad" es utilizado en lugar de "corporación" que fue asociado particularmente al sector privado.

La información adicional proporcionada es el resultado del esfuerzo común de los miembros del Sub-Comité de Normas de Control Interno de la INTOSAI. Esta actualización fue coordinada mediante las tareas impuestas entre los miembros del sub-comité con representantes de las EFS de Francia, Hungría, Bangladesh, Lituania, Los Países Bajos, Omán, Ucrania, Rumania, Reino Unido, Estados Unidos de América y Bélgica (presidente de la sede).

[1] Administración de Riesgos Corporativos Marco Integrado (COSO – Septiembre 2004)

Franki VANSTAPEL
Primer Presidente del Tribunal de Cuentas de Bélgica
Presidente del Sub-Comité de Normas de Control Interno
de la INTOSAI

Introducción

La premisa subyacente de la *Administración de riesgos corporativos* del COSO es que cada entidad existe para proporcionar valor a sus grupos de interés. En el sector público, las expectativas generales son que los servidores deben satisfacer o servir al interés público siendo justos e imparciales mediante el manejo apropiado de los recursos. Efectivamente los grupos de interés son la sociedad y sus representantes.

Todas las entidades enfrentan incertidumbres y el reto para su administración es el de determinar cuánta incertidumbre se puede aceptar mientras estas se esfuerzan en incrementar el valor para sus grupos de interés. Es importante también observar que la incertidumbre presenta tanto riesgos como oportunidades con el potencial de desgastar o mejorar el valor, en términos del sector público consiste en servir al interés público mejor. El objetivo de la gestión de riesgos de la entidad es el de permitir a la Gerencia el tratamiento efectivo de la incertidumbre y su riesgo - oportunidad asociados, mejorando la capacidad de construir valor proporcionando servicios más efectivos, de mayor eficiencia y más económicos, considerando y tomando en cuenta valores como equidad y justicia.

La *Guía para las Normas de control interno del sector público* de la INTOSAI ve al control interno como un proveedor de un importante marco conceptual a través del cual una entidad puede manejarse para alcanzar sus objetivos. El marco integrado *ERM* del COSO y otros modelos similares, toman a este aspecto como un escenario entero en el que la entidad se pueda dirigir en base a la identificación de futuros riesgos y oportunidades para

mejorar objetivos y diseñar controles internos que minimicen los riesgos y maximicen las oportunidades.

Tanto como extender la definición de funciones cubiertas por el régimen de gobierno corporativo, la gestión de riesgos de la entidad requiere un cambio en la forma en que la organización piensa a cerca de alcanzar sus objetivos.

Esto se da porque la eficacia en la gestión de riesgos de la entidad es un proceso en curso aplicado al establecimiento de la estrategia desplegado a lo largo y afectado por todas unidades de negocio de una entidad y que se encuentra diseñado para identificar los eventos potenciales que puedan afectar a las organizaciones, facilitando una seguridad razonable respecto al logro de los sus objetivos.

Este documento describe un marco de trabajo recomendado para aplicar los principios de gestión de riesgo en las entidades del sector público y proporciona las bases mediante las cuales una entidad puede evaluar su gestión de riesgos. Sin embargo, no intenta remplazar o suplantar la *Guía de control interno para el sector público*, más bien, está diseñado para proporcionar información adicional complementaria para ser usada dentro de las normas en que los estados miembros consideren apropiado. No se intenta limitar o interferir con la correcta autoridad garantizada relacionada al desarrollo de la legislación, reglamentos y otras políticas discrecionales en una organización.

En conclusión, debe quedar claramente establecido que este documento incluye directrices adicionales para las normas del gobierno corporativo. La guía no proporciona políticas detalladas, procedimientos y prácticas para implementar la mejor práctica de régimen de gobierno corporativo, tampoco se puede esperar que sea aplicada para todas las

organizaciones. Sin embargo, la adenda enriquece el marco del trabajo dentro de la cual las entidades pueden desarrollar regímenes que las ayuden de mejor manera a maximizar los servicios proveídos para los públicos de interés.

¿Cómo se estructura este documento?

El suplemento se estructura de una manera similar a la *Guía para las Normas de control interno del sector público* de la INTOSAI. En el primer capítulo se define el concepto de la gestión de riesgos de la entidad y se delinea el alcance. En el segundo capítulo se presentan los componentes de la gestión de riesgos de la entidad, resaltándose las extensiones a las normas de control interno.

Capítulo 1: Qué es la Gestión de Riesgos de la Entidad

1.1 Definición

1.1.1 *Administración de Riesgos* del COSO: Marco integrado de trabajo que establece que la gestión de riesgos de la entidad, enfrenta riesgos y oportunidades afectando la creación de valores o la preservación de estos definidos de la siguiente manera:

"Gestión de riesgos de la entidad, es un proceso efectuado por la junta directiva de una entidad, la gerencia y el personal, que aplica en el planteamiento de la estrategia y a lo largo de la Entidad, está diseñado para identificar eventos potenciales que podrían afectar a la entidad y permite administrar el riesgo dentro de los límites aceptados, proveyendo la seguridad razonable para la consecución de objetivos de la entidad" (modelo 2004 de COSO ERM)

1.1.2 En el sector público los términos creación y preservación de valor no tienen una directa relevancia como en el sector privado. Sin embargo, la definición es utilizada ampliamente con el propósito de aplicarse a todos los sectores y tipos de organizaciones que sea posible. En la medida de lo posible al sustituir la creación y preservación de servicio por la creación y preservación de valor esta terminología podrá ser plenamente aplicable en las entidades del sector público.

1.2 Identificando la Misión

1.2.1 El punto de partida para la gestión de riesgos de la entidad es la misión y visión establecida por esta. Dentro del contexto de la misión, la gerencia debería establecer los objetivos estratégicos, seleccionar las estrategias para alcanzar dichos objetivos y proponer objetivos de soporte alineados y desplegados en cascada a través de la organización.

1.3 Fijando Objetivos

1.3.1 La Guía para las Normas de control interno de la INTOSAI indica que los objetivos pueden ser subdivididos en cuatro categorías (aunque la mayoría de los objetivos corresponderán a más de una categoría). Éstos son:

- **Estratégicos** – Metas de alto nivel, alineadas soportando la misión de la entidad.

- **Operacionales** – Orientados a la ejecución ordenada, ética, económica, eficiente y efectivamente de las operaciones; resguardando los recursos en contra de pérdidas, mal uso y daño.

- **Información** – Referido a que la información reportada incluyendo las obligaciones de contabilidad, la cual sea confiable.

- **Cumplimiento** – Cumplimiento de leyes y regulaciones aplicables siendo posible actuar de acuerdo con la política gubernamental.

1.3.2 Los objetivos en las dos primeras categorías no están controlados por el control interno de la entidad, por lo que cualquier sistema de administración puede proporcionar solamente una razonable seguridad de que estos riesgos se manejan satisfactoriamente, pero debería permitir a la gerencia estar enterada del grado de cumplimiento oportuno de estos objetivos en un periodo de tiempo óptimo. Sin embargo, los objetivos referentes a la confiabilidad de los reportes y cumplimi8ento están dentro del control de la entidad, por lo que la gestión efectiva de riesgos usualmente dará la seguridad de que estos objetivos serán alcanzados.

1.4 Identificando Eventos - Riesgos y Oportunidades

1.4.1 Una vez fijados los objetivos de la entidad, la gestión de riesgos requiere organizarse para

identificar eventos que podrían tener impacto en el logro de los objetivos. Los eventos podrían tener impactos negativos o positivos o ambos a la vez. Los eventos con impacto negativo representan riesgos, los cuales podrían dificultar la habilidad de alcanzar los objetivos de una entidad. Estos riesgos pueden surgir debido a factores internos y externos. La Figura 1, presenta muchos de los riesgos que encaran las entidades gubernamentales – también podrían existir otros riesgos relevantes para entidades privadas.

1.4.2 Los eventos con impacto positivo pueden compensar impactos negativos o representar oportunidades. Las oportunidades son la posibilidad de que la ocurrencia de un evento permita a la entidad alcanzar sus objetivos de manera más eficiente así como ver la posibilidad de mitigar los riesgos, la Gestión de riesgos de la entidad, podría permitir formular planes para identificar oportunidades.

1.5 Comunicación y aprendizaje

1.5.1 Determinar si la gestión de riesgos de la entidad, es “efectiva" es una parte fundamental del proceso. La gerencia necesita emitir un juicio acerca de si los componentes de la gestión de riesgos de la entidad, están presentes y operando efectivamente. Con mayor detalle que no existan debilidades materiales y que todos los riesgos hayan sido llevados dentro de los parámetros aceptables de la entidad. Cuando la gestión de riesgos es efectiva la gerencia comprende la extensión, en la cual los objetivos dentro de las

cuatro categorías se han alineado con la misión y están siendo alcanzados. Una comunicación de arriba abajo y de abajo a arriba a través de la entidad es esencial para la facilitación de este proceso.

1.6 Limitaciones

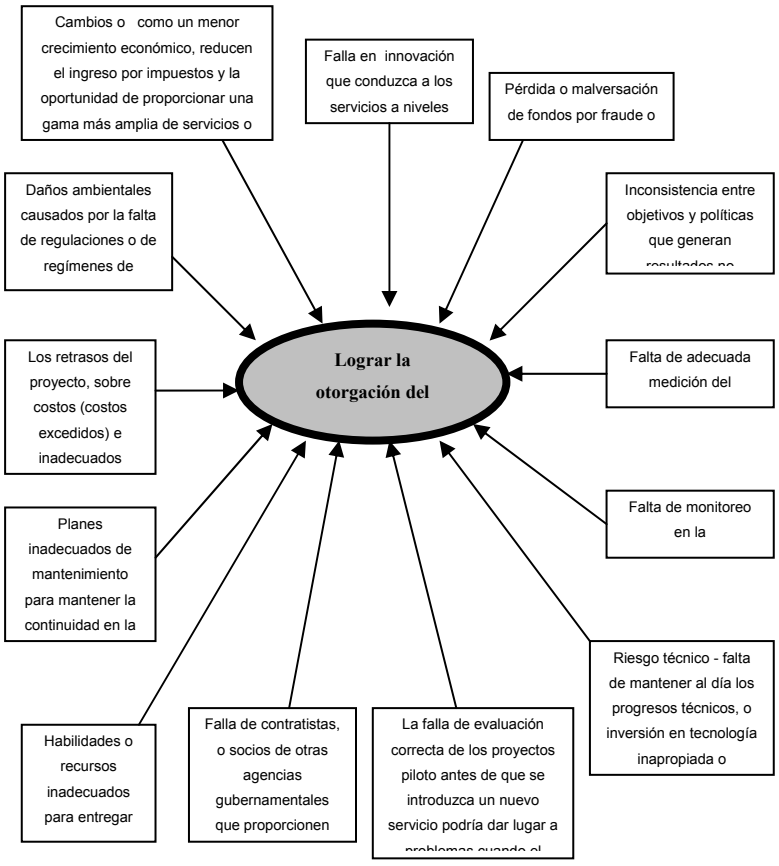
1.6.1 No importa cuan bien se haya diseñado y este operando el sistema, de gestión de riesgos de la entidad, esta no puede proveer a la gerencia seguridad absoluta respecto al logro de los objetivos generales. En lugar de ello, este soporte reconoce que solo puede obtenerse un nivel razonable de seguridad.

1.6.2 La seguridad razonable se compara con un nivel satisfactorio de confianza de que los objetivos podrán ser alcanzados o que la gerencia podrá hacer conocer oportunamente si los objetivos probablemente no serán alcanzados. Determinar cuanta seguridad es requerida para alcanzar un nivel satisfactorio de confianza es tema de criterio. Al ejercitar esta decisión gerencial será necesario considerar los límites de riesgo de la entidad y los eventos que podrían impactar en el logro de los objetivos.

1.6.3 La seguridad razonable refleja la noción de que la incertidumbre y el riesgo se relacionan con el futuro, el cual nadie puede predecir con certeza. Además, los factores fuera del control o de la influencia de una entidad, tal como el factor político, pueden impactar la capacidad de alcanzar estos objetivos. En el sector público, los factores

fuera del control de una entidad pueden incluso cambiar los objetivos centrales en un tiempo muy corto para saberlo. Las limitaciones también resultan de las siguientes realidades: el juicio humano en la toma de decisiones puede ser errado; crisis ocurridas debido a fallas humanas tales como errores simples o equivocaciones; que las decisiones en respuesta a un riesgo y controles establecidos necesitan considerar los costos relevantes y beneficios; y que los controles pueden ser vulnerados por colusión entre dos o más personas y la gerencia puede anular el sistema de control. Estas limitaciones impiden a la gerencia tener una seguridad absoluta de que los objetivos serán alcanzados. El cuadro 1 presenta algunos de los riesgos que se podrían enfrentar típicamente. Intenta ser ilustrativo más que exhaustivo.

Cuadro 1: Algunos riesgos típicos que las entidades del Gobierno enfrentan



1.7 Vínculo entre control interno y la gestión de riesgos de la entidad (GRE)

1.7.1 En muchos aspectos la gestión de riesgos de la entidad, puede ser vista como una evolución natural del modelo de control interno. La mayoría de las organizaciones intentarán aplicar completamente el modelo de control interno antes de implementar los conceptos inherentes a la gestión de riesgos de la entidad, el control interno es una parte integral de la gestión de riesgos. El marco integrado de la gestión de riesgos de la entidad, involucra el control interno, formando una conceptualización y herramienta mas robusta para la toma de decisiones respecto a posibles desvíos de su misión fundamental y objetivos asociados brindando una herramienta para la gerencia que le ayude a determinar cual sería la respuesta correcta a un evento particular. El modelo GRE (ERM en ingles) va más allá de las normas de control interno de la INTOSAI en un número de áreas, específicamente:

- Las categorías de objetivos son más amplias, y también incluyen información más completa, información no financiera, objetivos estratégicos;
- Amplía el componente de evaluación de riesgos e introduce diversos conceptos del riesgo, tales como tendencia al riesgo, tolerancia del riesgo, respuesta al riesgo; y

- Acentúa la importancia de los directores independientes en el directorio y elabora sus roles y responsabilidades.

Capítulo 2:

Componentes de la Gerencia de riesgos de la entidad (GRE)

La Gerencia de riesgos de la entidad, consta de ocho componentes interrelacionados. Éstos fueron derivados de la manera como la administración lleva a cabo un negocio y fueron integrados con el proceso de gestión. Los componentes son:

- Ambiente interno
- Establecimiento de objetivos
- Identificación de eventos
- Evaluación de riesgos
- Respuesta a los riesgos
- Actividades de control
- Información y comunicación
- Monitoreo

En la aplicación de los componentes de la gestión de riesgos, de la entidad, ésta debería considerar todos los alcances de sus actividades en todos los niveles de la organización. La administración debería también considerar nuevas iniciativas y proyectos usando el marco de trabajo de la gestión de riesgos de la entidad (GRE).

Aplicando la gestión de riesgos a toda la entidad

La gerencia requiere adoptar una perspectiva según el portafolio de riesgos. En efecto todos los mandos medios de la gerencia necesitarán considerar los eventos que pueden impactar sus áreas de actividad y alimentar con los mismos a la gerencia superior. Esta evaluación puede ser cualitativa o cuantitativa. La gerencia superior debe utilizar estas evaluaciones a través de todos los niveles y áreas de negocios de la entidad para construir un nivel medio para de evaluación general del portafolio de riesgos de la organización.

Importancia de las personas

La gestión de riesgos de la entidad, es implementada y puesta en marcha efectiva por la gerencia y otro personal lograda por las personas dentro de la organización mediante lo que hacen y dicen; de similar forma, afecta a las acciones de las personas debido a que cada empleado es una persona con diferente forma de entender y competencias. Asimismo, la GRE trata de proporcionar los mecanismos necesarios para permitir a los miembros del directorio a entender el riesgo en el contexto de los objetivos de la entidad.

Los miembros del directorio deben conocer sus responsabilidades y los límites de su autoridad. Por este motivo deberá existir un vínculo claro y conciso entre los deberes de las personas y el modo de realizarlos. La gerencia superior principalmente proporciona un asesoramiento. Sin embargo, ellos también proporcionan directrices, aprueban estrategias y ciertas transacciones y políticas de forma que desempeñen un papel importante en el fortalecimiento de la cultura organizacional.

2.1 Ambiente de Riesgo/Contexto

2.1.1 El riesgo ambiente/contexto abarca el tono de una organización, influenciando la conciencia del riesgo a toda su gente y es la base para todos los componentes de la Gerencia de riesgos de la entidad, proporciona disciplina y estructura. Los factores del ambiente interno influyen en la filosofía de la gestión de riesgos de la entidad; su tendencia al riesgo; el descuido del consejo de administración; integridad y valores éticos, competencia del personal; formas de asignar autoridad y responsabilidad, organización y desarrollando al personal.

2.1.2 La filosofía de la gestión de riesgos de una entidad, es el conjunto de creencias y actitudes compartidas que tienen la intención de determinar cómo la entidad considera el riesgo en todo lo que hace, desde la implementación de la estrategia hasta las actividades funcionales cotidianas. Esto influye a la cultura y estilo de funcionamiento, incluyendo cómo se identifican los riesgos, el tipo de riesgos aceptados y cómo son manejados. La filosofía de la gestión de riesgos de una entidad, debe ser evidente en las declaraciones de política, comunicaciones orales y escritas a los beneficiarios, al personal y en la toma de decisiones. Independiente del método de comunicación es de critica importancia que la gerencia superior refuerce la filosofía, no solamente a través de políticas de comunicación, también con las acciones diarias (dar el ejemplo).

2.1.3 La tendencia al riesgo es la suma de riesgos a un nivel amplio, que una entidad está dispuesta a aceptar en la búsqueda de intentar alcanzar sus objetivos. Refleja la filosofía de la gestión de riesgos y conduce la influencia de la cultura y el estilo de funcionamiento de la entidad. El riesgo aceptado puede ser considerado cuantitativa o cualitativamente. Debería ser considerado en la fijación de la estrategia, donde el rendimiento deseado de la estrategia debe estar alineado con la tendencia al riesgo, que es la predisposición de aceptar o tolerar un riesgo.

2.1.4 Además, cuando identifican el ambiente del riesgo y seleccionan un apropiado tendencia al riesgo, las entidades del sector público necesitan considerar la "la entidad en pleno". Las opiniones y expectativas de los patrocinadores y organizaciones patrocinadas, sean ellos de otros Órganos de gobierno o legisladores, y las opiniones de las organizaciones asociadas pueden dar una conducción clara en cuanto a una filosofía apropiada de gestión de riesgos apropiada y tendencia al riesgo.

2.1.5 La gerencia superior de una entidad es parte decisiva del ambiente interno e influye significativamente en sus elementos. Es una verdad que la cultura organizacional puede ser determinada o ser debilitada por el "tono gerencial". La independencia de la gerencia superior, la experiencia de la Gerencia Ejecutiva y jerarquía de sus miembros, el grado de participación e investigación, y la apropiada conveniencia de sus actividades juegan un papel importante. Los miembros de la gerencia ejecutiva

pueden ser parte de la gerencia superior, pero para que el ambiente interno sea efectivo es recomendable que el equipo de gerencia superior tenga algunos miembros exteriores independientes. Esto se da porque la gerencia superior debe estar preparada para mantener una gerencia ejecutiva, que pueda responder por opiniones, actividades de preguntas, escrutinio y estar preparada para presentar visiones alternativas.

2.1.6 La integridad y los valores éticos de la gerencia influyen en la manera de implementar la estrategia y los objetivos. Dado que la buena reputación de una entidad es tan valiosa, las normas de conducta deben ir más allá del mero cumplimiento de la ley. La integridad ética del comportamiento de la gerencia deriva de la cultura corporativa, que abarca normas éticas y de conducta y cómo son comunicadas y reforzadas. La gerencia superior desempeña un papel clave en la determinación de la cultura corporativa. Un énfasis indebido sobre los resultados a corto plazo en particular puede impedir el cumplimiento de la misión general y puede fomentar un ambiente interno inadecuado.

2.1.7 Los códigos formales de conducta son importantes como fundamento para la promoción de un tono ético apropiado. También son importantes los canales de comunicaciones ascendentes (o procedimientos formales) donde los empleados se sienten cómodos aportando con información relevante a la dirección. Sin embargo, un código escrito de conducta no asegura por si mismo que los procedimientos se estén cumpliendo, incluso si los empleados tienen que demostrar atención sobre

el comportamiento esperado. Igualmente importante para su cumplimiento son las sanciones resultantes para los empleados que violan el código. Los mensajes transmitidos por la gerencia superior se incorporan rápidamente a la cultura corporativa, "por ello hacer las cosas correctamente" cuando se enfrentan arduas decisiones de negocios, difunde un mensaje poderoso por toda la entidad.

2.1.8 La competencia refleja los conocimientos y habilidades necesarias para realizar las tareas asignadas. Esta necesita ser fortalecida por los recursos humanos mediante prácticas de reclutamiento y promoción de individuos apropiados, la inducción, el entrenamiento y enfrentar pobres rendimientos. La gerencia establece los niveles de competencia para trabajos concretos y los transforma en conocimientos y habilidades requeridas para los puestos específicos. Es importante reconocer que puede existir una compensación entre la competencia y el costo.

2.1.9 La estructura organizacional de una entidad proporciona el marco para planificar, ejecutar, controlar y monitorear sus actividades. La estructura organizacional adoptada debe ajustarse a sus necesidades. Algunas son centralizadas y otras descentralizadas, algunas están organizadas por la ubicación geográfica y otras por la funciones. Sea cual sea el tipo de estructura, una entidad se debería organizarse para permitir una efectiva gestión de riesgos, y desarrollar sus actividades para alcanzar sus objetivos.

2.1.10 La asignación de autoridad y responsabilidad implica el grado hasta el cual los individuos y equipos están autorizados animados a utilizar su iniciativa para tratar temas y resolver problemas, así como los límites de dicha autoridad. Los desafíos que implican asegurar que todo el personal entiende los objetivos de la entidad y cómo sus acciones contribuyen al logro de esos objetivos y delegar solo la cuantía requerida para alcanzar los objetivos. La responsabilidad es tan importante como la autoridad. El ambiente interno se ve muy influenciado por el grado de responsabilidad reconocido por los individuos. Esto permite al ejecutivo confiar durante todo el proceso.

2.2 Establecimiento de Objetivos

2.2.1 Los objetivos se establecen a nivel estratégico, estableciendo con ellos una base para los objetivos operativos, de reporte y de cumplimiento. Cada entidad enfrenta una variedad de riesgos procedentes de fuentes externas e internas y una condición previa para la identificación efectiva de eventos, la evaluación de sus riesgos y la respuesta a ellos es el establecimiento de los objetivos, que tienen que estar alineados con el tendencia al riesgo por la entidad, orientados a su vez a los niveles de tolerancia al riesgo de la entidad.

2.2.2 La gerencia define objetivos estratégicos, formula la estrategia y establece operaciones relacionadas. Los objetivos estratégicos son metas de alto nivel alineadas con y soportando la misión de la entidad. La estrategia implementada para alcanzar

la misión y los objetivos relacionados tienden a ser más dinámicos que la misión y tienen que ser adecuados a las condiciones cambiantes.

2.2.3 A pesar de la diversidad de objetivos entre entidades, existen ciertas categorías amplias que pueden ser aplicadas. Todos los objetivos se clasifican en uno o más de las siguientes categorías:

- *Objetivos operativos* - Estos se refieren a la efectividad y eficiencia de las operaciones de la entidad, incluyendo metas de rendimiento y salvaguarda de recursos frente a perdidas. Cuando este es utilizado conjuntamente con la divulgación pública, una definición ampliada de "salvaguarda de recursos/valores" puede ser utilizada: en la prevención, detección y corrección de malversación de fondos públicos. Los objetivos operativos necesitan reflejar el ambiente particular en el cual la entidad funciona. Los objetivos operativos proporcionan un punto de focalización para orientar la asignación de recursos, si no están bien concebidos, dichos recursos pueden estar mal direccionados.

- *Objetivos de información* - Estos pertenecen a la confiabilidad de la información y pueden implicar ambos datos financieros y no financieros. A pesar que los objetivos de información, también se relacionan con reportes preparados para difusión externa, el objetivo clave de la información confiable es proporcionar a la gerencia información exacta y completa adecuada para la finalidad

pretendida. Sin una información exacta y completa es muy difícil que la gerencia tome buenas decisiones.

- *Objetivos de cumplimiento* - Estos pertenecen al cumplimiento de leyes y regulaciones relevantes. Este requisito puede referirse al mercado, medioambiente, bienestar de los empleados, etc. Algunas entidades también necesitarán cumplir con objetivos de cumplimiento internacionales.

2.2.4 Una gestión de riesgos efectiva provee una razonable seguridad sobre las operaciones de la entidad, reporte y cumplimiento y la consecución de objetivos de la entidad.

2.2.5 El riesgo aceptado es establecido por la gerencia bajo control de junta directiva, es una orientación para establecer la estrategia y para evaluar la importancia relativa de los objetivos. Efectivamente el riesgo aceptado por la entidad es el nivel del riesgo tolerante que una entidad está preparada para aceptar en la entrega de valor (en la forma de servicios públicos) a los grupos de interés. Normalmente se pueden diseñar muchas estrategias diferentes para conseguir la misión, cada una con riesgos diferentes. La gerencia debe seleccionar la estrategia y los objetivos asociados que mejor se ajuste dentro de la tendencia al riesgo.

2.2.6 Las tolerancias del riesgo son los niveles aceptables de desviación relativos a la consecución de objetivos. Pueden ser medidos a través de objetivos de desempeño. Frecuentemente Las metas de rendimiento se miden mejor si es

posible, con las mismas unidades que los objetivos correspondientes. El funcionamiento dentro de la tolerancia del riesgo, proporciona mayor aseguramiento para la gerencia de que la entidad permanezca dentro de su riesgo aceptado y lograr sus objetivos.

2.3 Identificación de eventos

2.3.1 La gerencia identifica los eventos potenciales que, de ocurrir, afectarían la entidad. Los eventos necesitan ser clasificados, si representan oportunidades o al contrario afectarán la capacidad de la entidad para implantar la estrategia y alcanzar los objetivos con éxito (riesgos). Cuando la gerencia identifica los eventos, considera una serie de factores internos y externos que pueden dar lugar a riesgos y oportunidades, en el contexto del alcance pleno de la entidad.

2.3.2 Un evento es un incidente o acontecimiento, derivado de fuentes internas o externas, que afecta a la implantación de la estrategia o la consecución de objetivos. Los eventos pueden tener impactos positivos o negativos o ambos tipos a la vez. Los eventos abarcan desde lo obvio a lo desconocido y los efectos desde lo inconsecuente a lo muy significativo. Sin embargo, para evitar una consideración excesiva de eventos relevantes, procede realizar de forma separada su identificación y la evaluación de su probabilidad de ocurrencia e impacto.

2.3.3 La gerencia necesita entender los tipos de factores clave internos y externos y los eventos que

pueden derivarse de ellos. Los factores externos se pueden incluir pero no limita a los cambios que se presentan en el ambiente político, el ambiente social, tecnológico y los problemas económicos que afectan a la entidad misma o a sus proveedores. Los factores internos se derivan de las elecciones de la gerencia respecto a como funcionan. Esto puede incluir la infraestructura de la entidad, cuántas localizaciones funcionan dentro, las habilidades y competencia del personal y cómo funcionan los sistemas de información del negocio.

2.3.4 Las técnicas de identificación de eventos se aplican tanto al pasado como al futuro. Las técnicas que se centran en eventos pasados pueden considerar temas tales como informes y cuentas anuales, historial de cuentas por pagar e informes internos. Las técnicas que se centran en eventos futuros pueden considerar temas tales como cambios demográficos, nuevas condiciones de mercado y cambios futuros en el ambiente político. Las técnicas varían ampliamente en su nivel de sofisticación y automatización y se centran en una perspectiva ascendente o descendente de eventos.

2.3.5 Frecuentemente los eventos no ocurren de forma aislada. Un acontecimiento puede hacer que se desencadene otro, por lo que pueden ocurrir de forma concurrente. La gerencia debería entender cómo estos se relaciona entre si. Evaluando estas relaciones, se puede determinar donde mejor deberían aplicarse los esfuerzos en la gestión de riesgos

2.3.6 Puede ser útil agrupar los eventos potenciales en categorías. Al agregarlos horizontalmente en toda la entidad y verticalmente dentro de unidades operativas, la gerencia desarrolla un entendimiento de las relaciones entre eventos. Mediante esta agrupación de eventos similares la dirección puede determinar cuales son las mejoras respuestas en costo y efectividad. Aunque cada entidad desarrollará su propio método de agrupación de eventos existen herramientas estándares tales como estudio de mercado PEST[2] que puede servir como base.

2.4 Evaluación de riesgos

2.4.1 La evaluación de riesgos permite a una entidad considerar el grado de amplitud con que eventos potenciales impactaran en el logro de objetivos. La gerencia debe evaluar estos acontecimientos a partir de dos perspectivas – probabilidad e impacto – usando una combinación de técnicas cuantitativas y cualitativas. Los impactos positivos y negativos de los eventos potenciales deben ser

[2] El análisis del PEST es una herramienta útil para entender y determinar el impacto de factores externos para el logro de los objetivos de la entidad. El PEST es la sigla de la determinación de factores políticos, económicos, sociales y tecnológicos.

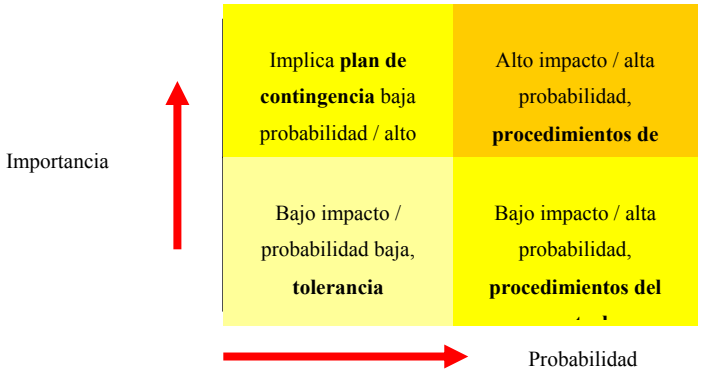
evaluados individualmente o por categoría sean su impacto a través de la entidad. Los riesgos se evalúan sobre una base inherente y residual.

2.4.2 Aunque el término "evaluación de riesgo" se aplica a veces en relación con una actividad puntual, en el contexto de la gestión de riesgos de la entidad, su componente con esa misma denominación constituye una continua e iterativa interacción de acciones que ocurren en toda la entidad. El objetivo de la Evaluación de riesgos es identificar eventos suficientemente importantes y significativos que concentren la atención de la gerencia.

2.4.3 La incertidumbre de los eventos potenciales necesitan ser evaluadas desde dos perspectivas - probabilidad e impacto. La probabilidad representa la posibilidad de que un evento determinado ocurra en un período de tiempo dado, mientras que el impacto representa el tamaño y efecto que tendría en la capacidad de la entidad para alcanzar sus objetivos. El período de tiempo usado para evaluar la probabilidad debe ser consistente con el horizonte del tiempo de la estrategia y de los objetivos relacionados. Los riesgos más importantes son aquellos con una alta probabilidad de ocurrencia y de alto impacto. Inversamente los riesgos menos importantes son aquellos con una baja probabilidad de ocurrencia y bajo impacto. La atención de la gerencia debe estar enfocada en los riesgos de alta probabilidad y alto impacto (véase el cuadro 2 en la página siguiente). El resultado final del proceso será el de asignar a cada riesgo una categoría de probabilidad e impacto. Algunas entidades utilizan

un tipo alto-bajo, otros el "sistema de semaforización" rojo, amarillo y verde, otros la medida cuantitativa de acuerdo a porcentajes.

Cuadro 2: Matriz simple de evaluación y respuesta a riesgos



2.4.4 La metodología de evaluación de riesgo puede ser cuantitativa o cualitativa. Puede estar basada en métodos objetivos o subjetivos. Una entidad no necesita emplear técnicas comunes de evaluación a través de todas sus unidades de negocio. Sin embargo, la gerencia necesita estar enterada de las necesidades humanas al determinar riesgos y necesita asegurarse de que todos los miembros relevantes del personal tengan una comprensión común de lo que significa la terminología de la clasificación para determinar el riesgo. Si no se hace esto será difícil que la gerencia superior determine la importancia relevante de lo diversos riesgos.

2.4.5 Una vez que se hayan evaluado los riesgos, emergerán los riesgos prioritarios que la entidad. Si la exposición del riesgo es inaceptable de acuerdo al nivel del riesgo aceptado por la entidad, debe ser clasificado como un riesgo de alta prioridad o "riesgo clave". Los riesgos dominantes merecen una atención continua en el nivel más alto de la entidad. Las prioridades específicas del riesgo cambiarán en un cierto plazo cuando los objetivos de la entidad cambien, el ambiente del riesgo cambia y se tratan los riesgos clave.

2.4.6 La evaluación del riesgo según lo descrito anteriormente pertenece al riesgo inherente. El riesgo inherente es aquel al que se enfrenta a una entidad en ausencia de acciones de la gerencia para modificar su probabilidad o impacto. El riesgo residual es el que permanece después de la que la gerencia desarrolle sus actividades de respuesta al riesgo, que se resume en el siguiente párrafo. La ventaja de este método es que permite a las entidades identificar los riesgos que consumen el tiempo de la gerencia, tiempo que utilizarse mejor en otro tema (e.g. porque el riesgo inherente tiene una probabilidad baja de ocurrir).

2.5 Respuesta a los Riesgos

2.5.1 Evaluados los riesgos relevantes, la gerencia determina cómo responder a ellos. Las respuestas a los riesgos incluyen la transferencia, tratamiento, interrupción de la actividad y tolerancia del riesgo. Al considerar su respuesta, la gerencia evalúa su efecto sobre la probabilidad e impacto del riesgo, así como los costos y beneficios, de seleccionar

aquella que situé el riesgo residual dentro de la tolerancia al riesgo deseado. La gerencia debería identificar también cualquier oportunidad de ampliación que pueda existir y asumir una perspectiva amplia de riesgo de la entidad o bien un portafolio de riesgos.

2.5.2 Las Respuestas al riesgo se encuentran dentro de las siguientes categorías:

- *Compartiendo/Transferencia de riesgos* – Reducir la probabilidad de impacto del riesgo transfiriendo o de otra forma compartiendo una parte del riesgo. Esto se puede realizar incluyendo la contratación de seguros, la realización de operación de cobertura y la terciarización de una actividad. Esta opción es particularmente útil para mitigar los riesgos financieros, riesgos de los activos y para las actividades subcontratadas. Sin embargo, la mayoría de los riesgos no siempre son transferidos completamente. En detalle, generalmente no es posible transferir el riesgo de reputación aunque podría contratarse externamente la entrega de un servicio.

- *Reducción/Tratamiento del Riesgo* – Un gran número de riesgos serán tratados bajo esta forma: Se llevarán a cabo acciones para reducir la probabilidad o el impacto del riesgo o ambos a la vez. Esto implica típicamente alguna de las miles de decisiones empresariales cotidianas incluyendo los procedimientos del control discutidos más detalladamente en la sección 2.6 y en los

controles internos – marco de trabajo integrado.

- *Evitando/interrumpiendo la actividad* – Salir de las actividades que generan riesgos. En las entidades del sector público es raramente probable poder evitar el cese de una línea de un producto central, sin embargo puede ser una respuesta útil frenando la expansión a un nuevo mercado apropiado o considerar continuar con un proyecto específico.

- *Aceptar/Tolerancia* - No se toma ninguna acción que afecte a la probabilidad o el impacto del riesgo. Esta respuesta sugiere que no se identificará ninguna opción de respuesta costo efectiva que sugiera el impacto y probabilidad hasta un nivel aceptable, o que el riesgo inherente está ya dentro de las tolerancias del riesgo. La tolerancia al riesgo se puede complementar por supuesto con la planificación de contingencia para manejar los impactos que se presentarán si se manifiesta el riesgo.

2.5.3 El modelo ERM (GRE) enfatiza la anticipación en el manejo de riesgos, pero también, dentro del mismo un acercamiento, identificando oportunidades. En cualquier situación la gerencia debe observar para identificar oportunidades o acontecimientos con un impacto positivo no solamente, tomando en cuenta el riesgo o eventos con impacto negativo. Existen dos aspectos en esto: en primer lugar atenúa al mismo tiempo las amenazas, las oportunidades que se presenta para

aprovechar un impacto positivo; en segundo lugar, considera si las circunstancias que se presentan, mientras no generan amenazas, ofrece oportunidades positivas

2.5.4 La gerencia debe evaluar los efectos de varios métodos para tratar el riesgo, posteriormente decide cómo manejar lo mejor posible el riesgo, seleccionando una respuesta o una combinación de las respuestas diseñadas para controlar probabilidades e impacto del riesgo dentro de tolerancias del mismo. La respuesta hallada no necesariamente resulta en disminución del riesgo residual, sin embargo cuando una respuesta a los riesgos pudiera terminar en un riesgo residual que superare la tolerancia establecida, la gerencia revisará y/o reconsiderara su respuesta o tolerancias del riesgo.

2.5.5 Evaluar las respuestas alternativas a los riesgos inherentes, requiere tener en cuenta los riesgos adicionales que pueden derivarse de cada respuesta, lo que puede iniciar un proceso iterativo. Aquí es provechoso que la gerencia superior antes de tomar una decisión considere un portafolio de perspectivas que les proporcionen una visión general del perfil de la respuesta permitiendo considerar los tipos y la naturaleza del riesgo residual y si encajan con la tendencia al riesgo derivada de la misión.

2.5.6 Una vez que la gerencia seleccione una respuesta preferente, necesita desarrollar un plan de implantación para ejecutarla. Una parte crítica de dicho plan es el establecimiento de las actividades

del control para asegurarse que el tratamiento del riesgo se realizada con efectividad.

2.6 Actividades de control

2.6.1 Las actividades del control son las políticas y los procedimientos que ayudan a asegurar que se llevan a cabo las respuestas de la gerencia ante los riesgos. Las actividades del control tienen lugar a través de la organización, a todos los niveles en todas las funciones. Las Guías para las normas de control interno para entidades públicas incluyen información detallada sobre controles efectivos, esta adición no intenta nada más que incorporar los controles internos en el contexto de la gestión de riesgos de la entidad.

2.6.2 La Gerencia de riesgo de la entidad observa a las actividades del control como parte importante del proceso con el que una entidad se esfuerza para alcanzar los objetivos de negocio. Las actividades del control no son realizadas simplemente por que si o por que "parezca la actividad correcta o adecuada de hacer", pero sirven bastante como mecanismos para gestionar la consecución de los objetivos de la entidad.

2.6.3 Aunque las actividades del control generalmente son establecidas generalmente para asegurar que las respuestas a los riesgos se lleven a cabo de modo adecuado, con respecto a ciertos objetivos también constituyen por si mismas una respuesta a los riesgos. La selección o revisión de las actividades debería incluir la consideración sobre

su relevancia y adecuación de respuesta al riesgo y a los objetivos relacionados.

2.6.4 Debido a que cada entidad tiene su propio conjunto de objetivos y enfoques de implantaron, existirán diferencias en las respuestas al riesgo y actividades de control relacionadas. Incluso cuando dos entidades tuvieran objetivos idénticos y tomasen decisiones similares respecto a como alcanzarlos las actividades del control probablemente serian distintas. Esto ocurre porque los diferentes equipos de la gerencia tendrán diferentes riesgos aceptados y tolerancias.

2.6.5 Sin embargo, en el contexto de la gestión de riesgos todos los procedimientos quedan en cuatro categorías generales:

- **Controles preventivos** están diseñados para limitar la posibilidad de materialización de un riesgo y de un evento indeseable observado. Cuanto mayor es el impacto del riesgo en la capacidad de alcanzar los objetivos de la entidad, es más importante la implementación de controles preventivos apropiados.

- Los **controles directivos** están diseñados para asegurar que un resultado particular está siendo alcanzado, son importantes particularmente cuando un evento es crítico (como brecha de seguridad) generalmente se utiliza para apoyar el logro de los objetivos de la confiabilidad.

- Los **controles detectivos** se diseñan para identificar si resultados indeseables han ocurrido "después de un acontecimiento". Sin embargo, la presencia de controles detectivos apropiados puede también atenuar el riesgo de los resultados indeseables que ocurren creando un efecto disuasivo.

- Los **controles correctivos** se diseñan para corregir los resultados indeseables que se han observado. Podrían también significar una eventualidad para el logro de recuperación de fondos o de la utilidad contra pérdida o daño.

2.7 Información y comunicación

2.7.1 Existe poca diferencia entre los requisitos de calidad de los datos usados para apoyar objetivos de control interno y los requisitos de calidad de los datos usados para apoyar a la gestión de riesgo de la entidad. Pues las Guías para las normas de control interno para el sector público contienen la información detallada sobre requisitos de la información y de la comunicación, esta adición no propone otra cosa más que aplicar estos requisitos en el contexto de la gerencia de riesgo de la entidad.

Información

2.7.2 La gestión de riesgo de la entidad requiere específicamente que una entidad capture una amplia gama de información para alcanzar los objetivos de control interno, por ejemplo, la focalización en los objetivos estratégicos requiere

como resultado amplia información de salida. Además la utilización que se le da estos datos es levemente diferente. Los datos históricos permiten que la entidad mantenga su funcionamiento actual acorde con sus objetivos, planes y expectativas, que faciliten una alerta temprana de eventos potenciales que merecen la atención de la Gerencia. Los datos actuales permiten determinar si se mantiene una perspectiva en tiempo real de lo riesgos existentes en un proceso, función o unidad, e identificar variaciones frente a las expectativas. Esto puede permitir a la entidad determinar si se mantiene operando dentro de la tolerancia del riesgo establecida.

2.7.3 La información pertinente se identifica, captura y comunica de una forma y un margen de tiempo que permiten a las personas llevar a cabo sus responsabilidades. La comunicación efectiva también existe, que fluye hacia abajo, arriba y a través de la entidad. Todo el personal debe recibir un mensaje claro de la alta gerencia el mismo debe considerar seriamente las responsabilidades en la gestión de riesgos de la entidad. Ellos necesitan entender su rol en el proceso de la gestión de riesgo de la entidad y como las actividades individuales se relacionan con el trabajo de otros. Asimismo el personal debe tener medios de comunicar hacia arriba la información significativa. También debe haber una comunicación efectiva con los públicos de interés.

2.7.4 Tener la gente adecuada con la información correcta, en el tiempo y lugar correcto, es esencial para efectuar la gestión de riesgo de la entidad.

Comunicación

2.7.5 La comunicación es inherente a los sistemas de información. Como ya se ha comentado antes estos sistemas deben proporcionar información al personal adecuado, para que puedan llevar a cabo sus responsabilidades, de reporte y de cumplimiento, la comunicación también debe tener lugar en un sentido más amplio, diseminando la cultura corporativa, ocupándose de expectativas, cubriendo las responsabilidades de los individuos y grupos, así como otras materias relevantes.

2.7.6 La gerencia proporciona comunicaciones específicas y orientadas que se dirigen a las expectativas de comportamiento y las responsabilidades del personal. Esto incluye una exposición clara de la filosofía y enfoque de la gerencia de riesgos de la entidad. La comunicación sobre procesos y procedimientos debe alinearse con la cultura deseada y reforzarla. La comunicación debe expresar efectivamente:

- La importancia y relevancia de la gestión de riesgos de la entidad.
- Los objetivos de la entidad.
- El riesgo aceptado y las tolerancias al riesgo de la entidad.
- Un lenguaje común para identificar y determinar riesgos.

- Los roles y responsabilidades del personal en desarrollar y apoyar los componentes de la gestión de riesgos.

2.7.7 También se necesita de métodos para que los empleados comuniquen la información basada en riesgos a su gerencia de línea, a través de la organización. Los empleados de línea que tratan los temas operativos críticos cada día son a menudo los mejor situados para reconocer los problemas cuando surgen. Para que tal información sea reportada, debe haber canales abiertos de comunicación y una clara disposición de atención. Si la cultura corporativa es una de "matar al mensajero", el personal no comunicará los problemas a los superiores y los riesgos no serán identificados oportunamente.

2.7.8 En la mayoría de los casos las líneas normales de reporte de una organización son los canales ascendentes de comunicación. Sin embargo, en algunas circunstancias es necesario líneas de comunicación alternativas (como cierta forma de chisme). Debido a su importancia, una gestión efectiva de riesgos requiere la existencia de un canal alternativo de comunicaciones directo a la gerencia superior y disponible para que todo el personal utilice sin el miedo de la repercusión.

2.7.9 Existe la necesidad de una comunicación adecuada no solo dentro de la entidad, si no también con el mundo exterior. Es importante que los canales de comunicación sean externos y abiertos a los beneficiarios que pueden proporcionar entradas muy significativas sobre la manera en la cual la entidad está manejando riesgo para darle

seguridad sobre la manera en que se satisfagan sus necesidades. Esto es particularmente importante en lo referente a los riesgos que afectan al público y donde el público depende de su gobierno para que maneje el riesgo, por ello la seriedad en la comunicación con las partes externa se toman en base a la honradez de la comunicación también envía mensajes importantes a través de la entidad y puede tener un impacto significativo en la cultura de organizacional.

2.8 Monitoreo

2.8.1 La gestión de riesgo de la entidad se monitorea cuando el funcionamiento de sus componentes cada cierto tiempo, lo que se puede llevar a cabo con actividades de monitoreo, evaluaciones independientes o combinación de ambas técnicas. Las deficiencias en la gestión de riesgo de la entidad necesitan ser divulgadas a un nivel apropiado reportando los temas más importantes a la gerencia superior y gerencias para que la entidad mejore sus procesos.

2.8.2 Los objetivos de una entidad pueden cambiar en un cierto tiempo, el portafolio de riesgos encarados y su importancia relativa también cambiará en el tiempo, las respuestas efectivas a los riesgos de antaño, pueden llegar a ser irrelevantes o imposibles de poner en ejecución; las actividades del control puede resultar menos efectivas o inexistentes. La gerencia necesita determinar si el funcionamiento de su sistema de gestión de riesgos continua siendo efectivo, para determinar si sigue siendo apropiado y efectivo.

2.8.3 Las evaluaciones de la efectividad de la gestión de riesgos variarán en alcance y frecuencia, dependiendo de la significación de los grupos de riesgos y de la importancia de las respuestas del riesgo y de controles relacionados en el manejo de estos. Cuando la gerencia toma la decisión de realizar una evaluación integral de la gestión de riesgos de la entidad, hay que dirigir la atención hacia su aplicación en el establecimiento de la estrategia, así como la relación con las actividades significativas. Sin embargo, las actividades regulares de la gerencia tales como la actualización de los registros del riesgo y de los "cheques de salud de la organización o funcionales", también son parte del monitoreo de la gestión de riesgos.

Bibliografía

Australian Standard® for risk management (Standards Australia, 2004)

Entity Risk Management - Integrated Framework (COSO, 2004)

Integrated Risk Management Framework (Treasury Board of Canada Secretariat, 2001)

Internal Control - Integrated Framework (COSO, 1992)

Risk Management Standard (ARMIC, IRM & ALARM, 2002)

The Orange Book: Management of Risk - Principles and Concepts (HM Treasury, 2004)