

Rodrigo Estupiñán Gaitán

Administración de Riesgos E.R.M.* y la Auditoría Interna



- Gobierno corporativo
- Mapa de riesgos
- Comités de auditoría
- Listas y cuestionarios de control
- Normas internacionales de auditoría interna

ECOE EDICIONES

* Enterprise Risk Management



RODRIGO ESTUPIÑÁN GAITÁN

Contador público de la Facultad Nacional de Contaduría y Ciencias Económicas. Contador Veterano, Conferencia Interamericana de Contabilidad. Posgrados en auditoría de sistemas, educación contable y otros. Ha sido presidente del Instituto Nacional de Contadores Públicos de Colombia durante dos períodos. Es y ha sido Revisor Fiscal y Auditor General de empresas importantes del país y socio principal de la firma de auditores Rodrigo Estupiñán y Cía. Auditor de libros, profesor universitario y conferencista nacional e internacional en temas contables, de auditoría y tributarios.

En la celebración del día CONTADOR DE LAS AMÉRICAS, el 16 de mayo de 2003, recibió el PREMIO ARCELIO BLANCO MARTÍNEZ en su calidad a TODA UNA VIDA PROFESIONAL, al cumplir 35 años en ejercicio de la profesión.

Autor de: *Estados de flujo de efectivo y de cambios en la situación financiera; Contabilidad e inflación; Estatuto contable; Pruebas selectivas en auditoría; Control interno y fraudes; Papeles de trabajo en la Auditoría financiera; Análisis financiero y de gestión; Contabilidad de las sociedades;* además de diversos trabajos o ponencias presentados en los simposios y congresos de contadores públicos.

Rodrigo Estupiñán Gaitán

Administración o Gestión de Riesgos E.R.M. y la Auditoría Interna

- Gobierno corporativo
 - Mapa de riesgos
 - Comités de auditoría
- Listas y cuestionarios de control
- Normas internacionales de auditoría interna

CON LA COLABORACIÓN DE:

- Miguel Antonio Cano (q.e.p.d.)
 - Rafael Delgado
 - Nelson Díaz
 - René Castro



Estupiñán Gaitán, Rodrigo

Administración de riesgos E.R.M. y la auditoría interna / Rodrigo Estupiñán Gaitán.-- Bogotá : Ecoe Ediciones, 2006

320 p.; 24 cm. (Área administración)

Incluye bibliografía

ISBN 958-648-434-3

1. Administración de empresas 2. Gobierno corporativo 3. Gestión integral del riesgo 4. Administración de riesgos 5. Administración financiera I. Tít. II Serie

658.1 cd 20 ed.

A1078959

CEP-Banco de la República-Biblioteca Luis Ángel Arango

Colección: Ciencias administrativas

Área: Contabilidad y Finanzas

Primera edición: Bogotá, D.C., agosto de 2006

Reimpresiones: Bogotá, D.C., enero de 2008, noviembre de 2009

Reimpresión: Bogotá, D.C., mayo de 2010

Reimpresión: Bogotá, D.C., 2011

ISBN: 958-648-434-3

© Rodrigo Estupiñán Gaitán
E-mail: roesga42@gmail.com

© Ecoe Ediciones
E-mail: correo@ecoeediciones.com
www.ecoeediciones.com
Carrera 19 No. 63C-32, Pbx. 2481449, fax. 3461741

Coordinación editorial: Alexander Acosta Quintero

Autoedición: Magda Rocío Barrero

Carátula: Patricia Díaz

Impresión: Multiimpresos Ltda.

Calle 75 No. 24-20, Pbx. 2506442 - Bogotá D.C.

Impreso y hecho en Colombia.

Tabla de contenido

Prólogo	XI
La administración o gestión del riesgo y la auditoría interna	
Introducción	XV
CAPÍTULO 1. EL CONTROL INTERNO (MODELO)	1
¿Qué es el Control Interno?	1
La Importancia del Control	2
Definición de Control Interno	2
Los modelos de controles actuales	3
EL MODELO COSO	3
El modelo COSO I	3
Factores del ambiente de control	4
EL MODELO COCO	9
Propósitos del modelo COCO	10
Criterios del modelo COCO	10
Objetivos	11
Compromiso	11
Aptitud	11
Evaluación y aprendizaje	11
Participación del personal	12
Estructura del control interno propuesta por el modelo COCO	13
Confiabledad de los reportes internos y externos	13
Evaluación de riesgos	13
Consideraciones	14
Aplicación en el marco integrado del control interno	14
Preguntas y cuestionamientos	17
CAPÍTULO 2. ORGANIZACIÓN DE LA AUDITORÍA	
INTERNA	19
Normas internacionales para el ejercicio profesional de la auditoría interna	24
Preguntas y cuestionamientos	26

CAPÍTULO 3. ENFOQUE MODERNO DE LA AUDITORÍA INTERNA	29
1. The Institute of Internal Auditors (IIA)	29
2. La profesión de Auditor Interno	31
3. Enfoque moderno de la actuación profesional	32
4. Situación de la Auditoría Interna en Venezuela	34
5. Conclusiones	35
Preguntas y Cuestionamientos	36
CAPÍTULO 4. LOS PARADIGMAS EN EL EJERCICIO DE LA AUDITORÍA INTERNA EN AMÉRICA LATINA	39
Primer y principal paradigma	40
Segundo paradigma	40
Tercer paradigma	42
Cuarto paradigma	42
Quinto paradigma	43
Paradigmas a romper en el ejercicio de la auditoría Interna en América Latina	45
Preguntas y Cuestionamientos	47
CAPÍTULO 5. CÓDIGO DE ÉTICA	49
Introducción	49
Aplicación y cumplimiento	50
Principios	50
Reglas de conducta	50
Preguntas y cuestionamientos	52
CAPÍTULO 6. NORMAS INTERNACIONALES DE AUDITORÍA INTERNA Y CONSEJOS PARA LA PRÁCTICA	53
Preguntas y cuestionamientos	98
CAPÍTULO 7. EL RIESGO EMPRESARIAL	101
Introducción	101
El riesgo en el sector financiero	104
Otras clases de riesgos que afectan la industria financiera.	105
Indicadores de riesgo entidades financieras	107
Ejemplo de revelación para una entidad aseguradora	109
Análisis de Riesgos	109
Ejemplo de revelación de una entidad cooperativa financiera	111
Nota de revelación de riesgos	111
Preguntas y cuestionamientos	113
CAPÍTULO 8. ADMINISTRACIÓN DE RIESGO EMPRESARIAL E.R.M.	117
Presentación de la estructura conceptual del E.R.M.	117
Resumen ejecutivo	118
Eventos – Riesgos y oportunidades	119

Definición del E.R.M.	119
Logro de objetivos	120
Componentes del E.R.M.	121
Relación entre objetivos y componentes	122
Efectividad	122
Limitaciones	123
Abarca el control interno	123
Roles y responsabilidades	123
¿Quiénes deben usar este reporte?	123
Preguntas y Cuestionamientos	125
CAPÍTULO 9. EL RIESGO EN EL NUEVO ENFOQUE DE AUDITORÍA INTERNA	127
El rol del auditor interno	127
NUEVOS ENFOQUES DE AUDITORÍA INTERNA	129
Nueva definición	131
Visión y misión	132
Preguntas y cuestionamientos	134
CAPÍTULO 10. LA AUDITORÍA INTERNA Y EL (E.R.M.)	137
Introducción	137
Qué es la Gestión o Administración de Riesgo Empresarial (ERM)	138
Responsabilidad por el ERM	139
Beneficios del ERM	139
Actividades incluidas en el ERM	139
Aseguramiento en el ERM por la Auditoría Interna	140
Servicios que presta la auditoría interna	140
Rol de aseguramiento	141
Rol de consultoría	141
Salvaguardas	142
Destrezas y cuerpo de conocimientos	143
Conclusiones principales	143
Preguntas y cuestionamientos	144
CAPÍTULO 11. CONOCIMIENTO DEL CLIENTE PARA LA ADMINISTRACIÓN DEL RIESGO	147
Conocimiento del negocio mediante herramienta Balanced Scorecard	147
Cómo obtener un entendimiento del cliente y su actividad	158
1. Análisis del GESI (Gubernamental, Económico, Social e Informática)	159
2. Análisis del FODA (Fortalezas, Oportunidades, Debilidades y Amenazas)	159
3. Análisis de las 5 fuerzas políticas	161
Características claves para la identificación de riesgos	162
Preguntas y cuestionamientos	166

CAPÍTULO 12. EL AUDITOR INTERNO, EL ADMINISTRADOR EN LA GESTIÓN DE RIESGOS CORPORATIVOS	169
Introducción	169
1. Auditorías basadas en riesgo	170
Planeación	170
Evaluación de Riesgos y controles	171
2. Metodología para la administración integral de los riesgos	173
Prerrequisitos	173
3. Metodología general de la administración del riesgo	176
¿Estamos preparados?	176
4. Proceso de la Administración del Riesgo	178
Definir la escala de costo	183
Cálculo del valor esperado de pérdida	183
Costo de la pérdida	184
Acciones de mitigación	186
Identificando opciones para el tratamiento del riesgo	186
Valorando las opciones para tratamiento del riesgo	187
Preparando planes de tratamiento	189
Implementando planes de tratamiento	189
Auditoría a la implementación de los planes de mejora	190
Preguntas y cuestionamientos	193
CAPÍTULO 13. PRÁCTICAS DE LE.R.M. EN LA AUDITORÍA INTERNA	197
Preguntas y cuestionamientos	203
CAPÍTULO 14. MAPA DE RIESGOS PARA USO EN LA AUDITORÍA INTERNA	205
Riesgos en el área gerencial	206
Área financiera	207
Riesgos en el área de contratación	209
Riesgos en el área de trámites y procedimientos	210
Riesgos en el área de control interno	211
Preguntas y cuestionamientos	213
CAPÍTULO 15. AUDITORÍA DE CUMPLIMIENTO POR PARTE DEL AUDITOR INTERNO	217
Definición	217
Responsabilidad de la administración del cumplimiento con leyes y reglamentos	218
Diseño de la auditoría de cumplimiento	218
Planeación de la auditoría de cumplimiento	219
Incumplimiento de leyes y reglamento	220
Procedimiento en caso de incumplimiento	220
Consultas a asesores jurídicos	221
Evaluación del riesgo	221

Ejercicios de auditoría operacional, cumplimiento y de control interno	224
Caso práctico número 1	224
Eficiencia operacional general	224
Caso práctico número 2	229
Caso práctico número 3 producción	230
Caso práctico número 4	232
Caso práctico número 5	234
Caso práctico número 6	236
CAPÍTULO 16. DETECCIÓN DE OPERACIONES ILÍCITAS POR LA AUDITORÍA INTERNA	239
1. ¿Es verdaderamente independiente el auditor interno para emitir informes, cuando sabemos que depende laboralmente de la empresa que audita?	240
2. ¿La ubicación jerárquica que ocupa el auditor interno en las organizaciones, le permite auditar libremente a la alta directiva de la organización?	244
3. ¿La responsabilidad del auditor interno frente al fraude y a la detección de operaciones ilícitas, solo se limita a evaluar que el control interno implementado por la administración sea adecuado?	245
4. ¿La metodología utilizada por el auditor interno para hacer un trabajo basado en muestras, es suficiente para garantizar la transparencia de la totalidad de las operaciones?	248
5. ¿Aplicar las normas de auditoría interna vigentes son suficiente razón para eximir de las responsabilidades a los auditores internos en el caso de que ocurran operaciones ilícitas?	251
Conclusiones	252
Preguntas y cuestionamientos	253
Guía de discusión	256
CAPÍTULO 17. LISTAS Y CUESTIONARIOS DE CONTROL INTERNO PARA LA AUDITORÍA INTERNA	257
¿Qué es la FLAI?	257
Activos financieros	288
Activos fijos	292
Preguntas y cuestionamientos	253
CAPÍTULO 18. GOBIERNO CORPORATIVO O CORPORATE GOVERNANCE	299
Definición	299
Principios de gobierno corporativo	300
Otros elementos prácticos de un Código de gobierno corporativo	301
Compañías que preparan estados financieros	302
Las Entidades Financieras	303
Gobierno Corporativo	305

Cooperativa multiactiva financiera	310
Preguntas y cuestionamientos	315
CAPÍTULO 19. LOS COMITÉS DE AUDITORÍA Y EL GOBIERNO CORPORATIVO	319
Apéndice 1. El comité de auditoría o CI, según el comité de Basilea II	322
Apéndice 2. Dos Comités de auditoría según el Instituto Mexicano de contadores Públicos	323
Preguntas y cuestionamientos	327
Glosario	329
Bibliografía	335
Apéndice. Enterprise Risk Management – Integrated Framework Marco integrado de Administración de Riesgos Empresariales	337
Preguntas y cuestionamientos	350

Prólogo

The Committee of Sponsoring Organizations of the Treadway Commission de los Estados Unidos de Norteamérica, a través del documento denominado “Control Interno – Marco Integrado”, conocido como el modelo de control COSO, estableció nuevas técnicas para la implementación y evaluación del control interno, a través de las cuales se orientaron los controles en las organizaciones; así mismo, la auditoría interna empezó a mejorar la efectividad de su función y con ello a ofrecer servicios más eficientes y con un valor agregado importante, metodología recibida y ampliada por otras asociaciones de varios países y puestas en práctica en la mayoría de las organizaciones públicas, financieras, manufactureras, comerciales, de servicios y demás, con resultados inicialmente acertados.

No obstante, después se vieron afectados con problemas de errores intencionales y no intencionales, algunos convertidos en fraudes insalvables como los sucedidos a partir de 1998 con la grandes bancarrotas de empresas reconocidas de los EEUU y de Europa (Worldcom, Enron, Parmalat y muchas más), lo que impuso la necesidad primaria de evaluar los riesgos de las empresas antes de realizar las planeaciones estratégicas, representando para los gobiernos y para las asociaciones de contadores de todo el mundo el reto de establecer parámetros obligatorios de saber administrar los riesgos para determinar correctivos o poder soportarlos a menores costos.

El mismo Comité interdisciplinario del llamado COSO I, encomendó a la Price Waterhouse Coopers & Co., la profundización y estudio de los problemas suscitados en el mundo empresarial y achacados a bajas auditorías o complacencia de las mismas, determinándose que en las empresas se encierran riesgos incalculables de carácter interno y externo que requieren ser clasificados y orientados al entendimiento de los mismos y por ende se hace necesario, en principio, estudiar con

detenimiento los posibles riesgos que las rodean para tratar de mitigarlos o corregirlos, concluyendo la necesidad de establecer en las organizaciones “Gerencias de Riesgos”, las cuales antes de cualquier toma de decisión asesoren a la alta gerencia en cómo administrar los riesgos.

Del anterior estudio se estableció un documento denominado Enterprise Risk Management – ERM – Integrated Framework¹, conocido por todos nosotros como el COSO II, en el cual se desarrolló una estructura conceptual para la administración del riesgo empresarial y se planteó la formulación y seguimiento de un proceso básico para identificar, evaluar, medir y reportar amenazas, debilidades, fortalezas y oportunidades que afectan el logro de las metas y objetivos de una empresa.

Simultáneamente con la administración del riesgo, debe ir unido el establecimiento de normas internas de uso adecuado de gobiernos corporativos, con las cuales se organiza un sistema interno dentro de una empresa y se establecen las directrices que deben regir su ejercicio, buscando transparencia, objetividad y equidad en el trato a los socios o accionistas de una entidad, como también identificando la gestión de su junta directiva o consejo de administración y la responsabilidad social de sus organismos de control internos y externos frente a los grupos de interés como clientes, proveedores, competidores, empleados, terceros colocadores de recursos y hacia la comunidad en general.

La auditoría interna con el apoyo del IIA², de la FLAI³ y la CLAI⁴ está logrando adaptarse a las metodologías tecnológicas asimétricas requeridas en el gran desarrollo de las organizaciones empresariales de toda índole y está a la vanguardia de apoyo inmediato a la Alta Gerencia y su Junta Directiva o Consejo de Administración, de cuyas orientaciones en este libro retoma las más reconocidas y las presenta debidamente coordinadas con el tema de la Administración o Gestión de Riesgos.

Los temas tratados en el libro de *Administración o Gestión de Riesgos - ERM y la Auditoría Interna* los considero oportunos, de fácil entendimiento y con recomendaciones fundamentales necesarias para una adecuada Administración del Riesgo, los cuales no solamente son útiles para la profesión del Contador Público

1 Marco Integrado de Administración de Riesgos Corporativos

2 The Institute of Internal Auditors

3 Federación Latinoamericana de Auditores Internos

4 Congreso Latinoamericano de Auditores Internos

sino para las demás profesiones y sobretodo para los Miembros de Juntas Directivas, Comités de Auditoría, Consejos de Administración, Presidencias y Gerencias en general de toda clase de organizaciones empresariales.

La organización que se hace en este libro de la gestión del riesgo con la auditoría interna, apoyados en las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna, los Consejos para la Práctica y el Código de Ética del IIA, así como las listas y cuestionarios de control interno para la Auditoría Interna de la FLAI, ayudarán a los auditores internos y externos para evaluar los controles internos, el gobierno corporativo y los riesgos que afectan a las empresas donde presten sus servicios profesionales.

Para el entendimiento de este libro y como ejercicio didáctico, esta recopilación y ampliación de los temas enunciados, en mi concepto van a hacer fundamentales para la orientación de los administradores y para el apoyo que deben dar los auditores tanto internos como externos en la formulación de recomendaciones para lograr una adecuada administración del riesgo, un eficiente control interno y un buen gobierno corporativo.

Para la orientación y estudio de estos temas es importante revisar los títulos, los cuales estoy seguro lograrán despertar gran interés y facilitarán su análisis y aplicación de los mismos en nuestro ejercicio profesional como auditores, asesores, consultores o a nivel de dirección empresarial:

- El Control Interno (modelos)
- Organización de la Auditoría Interna
- Enfoque Moderno de la Auditoría Interna
- Los Paradigmas en el Ejercicio de la Auditoría Interna en América Latina
- Código de Ética para el Ejercicio de la Auditoría Interna
- Normas Internacionales de Auditoría Interna
- Riesgo
- Administración del Riesgo Empresarial - ERM
- El Riesgo, en el Nuevo Enfoque de Auditoría Interna
- La Auditoría Interna y la Administración de Riesgo
- Conocimiento del Cliente para la Administración del Riesgo
- El Auditor Interno, el Administrador en la Gestión de Riesgos Corporativos
- Práctica Administración del Riesgo en la Auditoría Interna
- Mapa de Riesgos para Uso de la Auditoría Interna
- Auditoría de Cumplimiento por parte del Auditor Interno
- El Enfoque de Trabajo del Auditor Interno en Detección de Operaciones Ilícitas
- Listas y Cuestionarios de Control Interno para la Auditoría Interna
- Gobierno Corporativo (Corporate Governance)
- Los Comités de Auditoría y el Gobierno Corporativo

Con un saludo muy especial para el colega Rodrigo Estupiñán Gaitán, gran impulsador de obras técnicas de contabilidad y auditoría y de la iniciativa de impulsar el tema del riesgo y el gobierno corporativo conjuntamente con otros grandes colegas, que hacen de nuestra profesión un ejemplo a seguir.

EDGAR W. AMARILLO R.⁵

⁵ Auditor Externo por varios años de la firma KPMG y actual Auditor Interno de FOGAFIN

La administración o gestión del riesgo y la auditoría interna

INTRODUCCIÓN

La Auditoría Independiente, interna o la Revisoría Fiscal deberá enfocar el análisis de operaciones, procedimientos, resultados de información y asesoría a la administración, utilizando para ello el nuevo concepto, apoyado por las Federaciones Internacionales de AUDITORÍA INTEGRAL¹ enmarcado en 4 grandes segmentos denominados:

- Auditoría de control interno
- Auditoría de cumplimiento
- Auditoría de gestión
- Auditoría financiera

Precisamente sobre la Auditoría de Control Interno² se ha modificado el enfoque, esquematizando su evaluación y conclusiones más en el *Riesgo de control*, sabiendo como obtener un conocimiento de la estructura de control interno en la organización, su proceso de diseño y realización de pruebas de controles que sirva de base para análisis o estudios posteriores.

“...es un proceso, ejecutado por la Junta Directiva o Consejo de Administración de una entidad por su grupo directivo (gerencia) y por el resto de personal, diseñado para proporcionarles seguridad razonable de conseguir en la Empresa las tres siguientes categorías de objetivos: (1) Efectividad y eficiencia en las operaciones;

(1) En el libro *Normas y Procedimientos de la Auditoría Integral* del Dr. Yanel Blanco Luna, Ecoe Ediciones, Bogotá 2ª ed, 2003.

(2) Committee Of Sponsoring Organizations Of The Treadway Commission (COSO) quien emitió el documento “Internal Control - Integrated Framework”.

(2) Suficiencia y confiabilidad de la información financiera; y (3) Cumplimiento de las leyes y regulaciones aplicables...”

Convierte los antiguos elementos de Control Interno en 5 componentes interrelacionados, que se derivan de la forma como la administración maneja el ente económico, y están integrados a los procesos administrativos, como son:

1. El ambiente de control
2. Evaluación de riesgos
3. Actividades de control
4. Información y comunicación; y
5. Supervisión, seguimiento o monitoreo

Esta nueva metodología asegura al auditor una mayor seguridad razonable dentro del proceso de la auditoría porque antiguamente el control interno no tenía en cuenta los avances de la tecnología, especialmente de la década de los 90's, cuya revolución informática ha sido demasiado rápida, así como el marco no dedicado solamente a la eficiencia de las personas sino también a la eficiencia de las operaciones y si la empresa y el auditor no están atentos a los cambios, pueden aparecer hechos irregulares no detectados oportunamente o por el contrario se puede dedicar tiempo precioso a situaciones relativamente no importantes, mientras que aspectos relevantes no son detectados porque su enfoque era el de detectar fraudes solamente sin medir la relación costo-beneficio, que en el diseño es fundamental.

Otro de los cambios que se notan en las investigaciones sobre el control interno es el de apoyo administrativo dentro de los informes de deficiencias, inconsistencias y fallas administrativas que quedaban sin soluciones, las cuales en nuevas visitas eran detectadas sin dar la importancia, de parte de la administración, siendo así el costo de la auditoría, gasto sin reposición.

Con el enfoque formulado por el COSO como herramientas fundamentales de establecimiento, control y seguimiento se han manejado en mejor forma y más económicamente las organizaciones de control interno en las empresas privadas y públicas, utilizando componentes más organizados y claves como son:

1) En el Ambiente de Control por:

- Compromiso para la competencia
- Comité de auditoría
- Filosofía de la administración y estilo de operación
- Estructura organizacional
- Asignación de autoridad y responsabilidad
- Políticas y prácticas de recursos humanos

2) **En la Valoración de riesgos, enfocando los siguientes puntos:**

- Objetivos globales de la entidad
- Objetivos a nivel de actividad
- Identificación, valoración y consecuencia de riesgos
- Manejo del cambio

3) **Actividades de Control para asegurar la :**

- Existencia de las políticas apropiadas y los procedimientos necesarios con respecto a cada una de las actividades del ente económico.
- Identificación de las actividades de Control para que sean usadas apropiadamente.

4) **Información Interna y Externa :** que debe ser obtenida, identificada, capturada, procesada y reportada por el sistema de información basados en planes estratégicos enlazados a las estrategias generales de la empresa y logrando el apoyo de la dirección en el desarrollo de los sistemas de información.

5) **Comunicación**, en cuanto a su efectividad, canales confiables, receptividad en las sugerencias, información precisa y suficiente, franqueza y efectividad en la forma de tratar a la administración, establecer planes adecuados para que se analicen y entiendan los estándares éticos de la entidad y seguimiento oportuno y apropiado de parte de los directivos y en corto plazo, en una nueva evaluación exclusiva a las fallas, inconsistencias o deficiencias informadas dentro del concepto denominado Monitoreo.

6) **Monitoreo o Seguimiento**, ocurre en el curso normal de las operaciones, e incluye actividades de supervisión y dirección o administración permanente y otras actividades que son tomadas para llevar a cabo obligaciones de cada empleado y obtener el mejor sistema de Control Interno, especialmente a :

- Evidencia de si el sistema de control interno continúa funcionando por parte del ente.
- Corroboración en comunicaciones externas, la información generada internamente.
- Comparación periódica de las cantidades registradas por el sistema de información contable.
- La sensibilidad frente a las recomendaciones de auditores externos o internos para fortalecerlos.
- Asegurar retroalimentación a la administración de los seminarios de entrenamiento, las sesiones de planeación y otras reuniones para asegurar que los controles operen efectivamente.

- Si el personal es cuestionado periódicamente para establecer si ellos entienden y cumplen con el código de conducta de la Entidad y desempeñan regularmente actividades críticas de control.
- Efectividad en las actividades de la Auditoría Interna.

Administración de Riesgo³ como apoyo al Control Interno y a la Auditoría Interna.

El COSO II ha desarrollado una estructura conceptual para la administración del riesgo empresarial denominada E.R.M.⁴ (sigla del inglés) para el entendimiento de la formulación y seguimiento de un proceso básico en la administración del riesgo como apoyo al buen gobierno corporativo y mejores medidas de control en una organización.

La gestión o administración de riesgo empresarial ERM es un proceso estructurado, consistente y continuo a través de toda la organización para identificar, evaluar, medir y reportar amenazas y oportunidades que afectan el poder alcanzar el logro de sus objetivos, cuya definición formulada por el COSO II fue de:

“Es un proceso, efectuado por la Junta Directiva o el Consejo de Administración, la Alta Gerencia y otro personal de un ente económico, mediante la determinación de una estrategia diseñada para identificar los eventos potenciales que la pueden afectar y para administrar los riesgos que se encuentran dentro de la cantidad de riesgo que un ente económico esté dispuesto a aceptar en la búsqueda de valor, para así proveer seguridad razonable en relación con el logro de sus objetivos”.

La definición captura los conceptos fundamentales que son claves sobre la manera como las compañías y otras organizaciones administran el riesgo, proveyendo una base para la aplicación a través de diferentes tipos de organizaciones y sectoriales. Se centra directamente en el logro de los objetivos de la entidad y ésta provee una base para definir la efectividad de la administración del riesgo empresarial.

Las empresas con ánimo o sin ánimo de lucro deben propender por crear valor a sus protectores, dueños o accionistas, así como la de enfrentar y superar las incertidumbres⁵, desafiándolas con preparación suficiente, para poder proveer una

3 En capítulos separados se tratará el tema del ERM.

4 Enterprise Risk Management

5 Incertidumbres: afectados por los factores del entorno como son la globalización, la tecnología, regulaciones, reestructuraciones, mercados cambiantes y competencia, los cuales generan incertidumbres. Emanan incapacidad para determinar la probabilidad de que ocurrirán eventos potenciales y sus resultados asociados.

estructura conceptual, así la gerencia trate de manera efectiva la incertidumbre que representan los riesgos y oportunidades, y así enriquecer su capacidad para generar valor⁶.

El riesgo es la posibilidad de que un evento ocurra y afecte adversamente el cumplimiento de los objetivos, en los procesos, en el personal y en los sistemas internos generando pérdidas. Los riesgos se clasifican en cuatro grandes tipos, el riesgo de reputación, el riesgo de mercado, el riesgo de crédito y el riesgo operacional en todas sus divisiones; como formalidad de prevención, detección y mitigación a dichos riesgos, el E.R.M. determinó 8 componentes interrelacionados, los cuales muestran cómo la Alta Gerencia opera un negocio, y cómo están integrados dentro del proceso administrativo en general, ellos son:

Entorno Interno: filosofía de administración de riesgo – Cultura de riesgo – Responsabilidad de la Junta Directiva o Consejo de Administración – Integridad y valores éticos – Compromiso para con la competencia.

Definición de los objetivos: objetivos estratégicos – Objetivos relacionados – Objetivos seleccionados – Apetitos del riesgo – Tolerancia al riesgo.

Identificación de eventos: eventos o factores que influyen en la estrategia y en los objetivos- Metodologías y técnicas – Interdependencia entre los eventos – Categoría de eventos – Riesgos y oportunidades.

Valoración del riesgo: riesgo inherente y residual- Probabilidad e impacto – Metodologías y técnicas de correlación.

Respuesta al Riesgo: identificación de las respuestas al riesgo – Evaluación de las posibles respuestas al riesgo – Selección de respuestas – Punto de vista de mapeo o portafolio.

Actividades de control: integración con la respuesta al riesgo – Tipos de actividades de Control – Controles generales – Controles de aplicación – Controles específicos de la actividad.

Información y comunicación: información – Sistemas estratégicos e integrados – Comunicación.

Monitoreo: evaluaciones separadas – Evaluaciones Ongoing.

6 Generación de Valor. Decisiones de la administración generan valor o se debilitan por la definición de las estrategias hasta la operación diaria. El reconocimiento del riesgo y de la oportunidad por la información interna y externa, despliega recursos preciosos, para enderezar las actividades de riesgo frente a las circunstancias cambiantes.
Generación de valor para los stakeholders con o sin ánimo lucro, entidades gubernamentales, la gerencia.

Gobierno Corporativo: por la falta de transparencia y de fluidez de la información contable hacia terceros (principalmente hacia sus dueños), por la inadecuada administración de riesgos y deficientes controles internos, se han promulgado disposiciones y recomendaciones hacia el cambio en las organizaciones en cuanto a la responsabilidad y debido cuidado de su administración en general desde su junta directiva o consejo de administración para que exista directrices que busquen transparencia, objetividad y equidad en el trato a los socios y hacia los clientes, proveedores, competidores, empleados, terceros colocadores de recursos y hacia la comunidad en general.

Este sistema de responsabilidad compartida se denomina “gobierno corporativo” en el cual determina una adecuada distribución de derechos y responsabilidades entre todos los miembros de la administración iniciando en su junta o consejo y alta gerencia conjuntamente, estableciendo para ello reglas y procedimientos para la toma de decisiones sobre asuntos importantes en la empresa, determinando una estructura mediante la cual se establecen sus objetivos y controles para lograr monitorear su desempeño.

Los gobiernos corporativos se rigen bajo principios que ayudan a la gobernabilidad de factores externos, internos e individuales, los cuales ayudan a la organización para a) garantizar que las cosas se hagan bien, aunque a veces existan costos importantes; b) garantizar que la información de la empresa hacia fuera sea oportuna y transparente; y c) crear confianza hacia la empresa de su entorno.

Una de las formas de ejercer gobiernos corporativos es por medio del establecimiento de **Comités de Auditoría** formado por personal de la junta directiva o consejo de administración, bajo reglamento especial, que lleve a analizar la información financiera, los riesgos, los problemas, las inconsistencias, los errores financieros y económicos y sobretodo ayude a cumplir una adecuada labor de los entes de dirección y de control en general. En resumen, debe vigilar la información financiera (políticas contables, examen estados financieros, auditoría externa); gobierno corporativo (políticas, litigios, fraudes, conflictos de intereses, quejas y reclamos, recomendaciones de control); y, control corporativo (modelo de negocio con relación a las estrategias, objetivos y políticas, opinión sobre los controles internos, auditoría interna, monitoreo y administración de riesgos).

El E.R.M. y el gobierno corporativo van entrelazados y enfocados hacia el control operativo, legal, financiero, logístico y de medio ambiente independientes de parte de la Junta Directiva o Consejo de Administración, desligándolos de los controles administrativos y contables utilizados dentro de la organización a nivel interno.

Auditoría Interna: esta área no ha sido esquivada a los cambios de administración de riesgo, controles internos y gobierno corporativo, al contrario, es la organi-

zación de estos entes quienes ayudarán a que se cambien o se adecuen las organizaciones empresariales a los nuevos enfoques requeridos y comentados.

La auditoría interna revisa la confiabilidad e integridad de la información, el cumplimiento de políticas y reglamentos, la salvaguarda de los activos, el uso económico y eficiente de los recursos, las metas y objetivos operativos establecidos. Los trabajos de auditoría interna abarcan todas las actividades financieras y de operaciones incluyendo sistemas, producción, ingeniería, comercialización y recursos humanos.

Dos enfoques han determinado las nuevas normas de auditoría interna, el más común con dependencia directa dentro de la administración son los llamados “servicios de aseguramiento” y los “servicios de consultoría”. Los primeros, comprenden una evaluación objetiva de las evidencias para proporcionar opiniones o conclusiones independientes sobre un proceso, sistema u otro asunto, organizadas en tres partes: a) el dueño del proceso; b) el auditor interno, quien realiza la evaluación; y, c) quien o quienes utilizan la evaluación (el usuario). Los segundos, son por naturaleza consejos o recomendaciones objetivas solicitados por un cliente sin que se vayan a asumir responsabilidades de gestión.

En los conceptos de auditoría interna que se presentan son basados en las normas internacionales de auditoría interna del IIA⁵, su código de ética y en los Consejos para la Práctica emitidos por tan prestante Institución Internacional de reciente publicación y aplicación en la gestión de una adecuada Auditoría Interna.

La gestión de riesgos es uno de los temas en los que más profundizan las normas mencionadas y por ello en varios capítulos del libro se indican aplicaciones y formas de estudio general y consideraciones de apoyo para un adecuada Administración del Riesgo Empresarial E.R.M.⁶ de parte de la empresa en la que presta los servicios de aseguramiento o consultoría, entre esas aplicaciones, la de formalizar mapas de riesgo como forma de detección o mitigación de los riesgos principales.

La Federación Latinoamericana de Auditores Internos (FLAI) recientemente emitió varias listas y cuestionarios de control interno para la evaluación por parte de la auditoría interna, los cuales se presentan en este compendio, y ayudarán a los profesionales y estudiantes de Auditoría Interna a lograr adecuadas evaluaciones internas dentro de sus servicios de aseguramiento o consultoría, organizados de tal

5 Institute of Internal Auditors (IIA)

6 Enterprise Risk Management

forma que no habrá aspectos que no se vayan a tener en cuenta en un servicio de auditoría interna en cuanto a su estructura organizacional, recursos humanos, seguridad física y áreas fundamentales de los ciclos de operación y tecnológicos.

Preguntas y cuestionamientos

1. ¿Qué segmentos comprenden el concepto de Auditoría Integral?
2. ¿Hay un segmento especial del cual se ha modificado el enfoque del mismo?
3. ¿Cuál es la nueva definición de control interno?
4. ¿Qué traduce el COSO y qué relación tiene este documento con el nuevo enfoque de control interno?
5. ¿Cuáles son los componentes de control interno?
6. ¿Qué le representa para el auditor la nueva metodología de control interno?
7. ¿Qué aspectos fundamentales representa el componente de control interno denominado *ambiente de control*?
8. ¿Qué aspectos fundamentales representa el componente de control interno denominado *valoración de riesgos*?
9. ¿Qué aspectos fundamentales representa el componente de control interno denominado *información*?
10. ¿Qué aspectos fundamentales representa el componente de control interno denominado *comunicación*?
11. ¿Qué aspectos fundamentales representa el componente de control interno denominado *actividades de control*?
12. ¿Qué aspectos fundamentales representa el componente de control interno denominado *monitoreo o seguimiento*?
13. ¿Qué es el COSO II y que aspectos desarrolló este documento?
14. ¿Qué se entiende por gestión o administración de riesgos E.R.M.?
15. ¿Qué significan las iniciales de *E.R.M.*?
16. ¿Indique la definición formulada por el COSO II sobre la administración de riesgo empresarial o E.R.M.?
17. ¿Qué aspectos fundamentales captura la definición del E.R.M.?
18. ¿Para enfrentar y superar las incertidumbres, que deben propender las empresas con o sin ánimo de lucro?
19. ¿Qué se entiende por riesgo?
20. ¿En cuántos tipos de riesgos se clasifican?
21. ¿Cuáles son los componentes que estableció el COSO II con relación al *E.R.M.*?
22. ¿Qué aspectos identifican el componente de administración de riesgo denominado *entorno interno*?
23. ¿Qué aspectos identifican el componente de administración de riesgo denominado *definición de los objetivos*?

24. ¿Qué aspectos identifican el componente de administración de riesgo denominado *identificación de eventos*?
25. ¿Qué aspectos identifican el componente de administración de riesgo denominado *valoración del riesgo*?
26. ¿Qué aspectos identifican el componente de administración de riesgo denominado *respuesta al riesgo*?
27. ¿Qué aspectos identifican el componente de administración de riesgo denominado *actividades de control*?
28. ¿Qué aspectos identifican el componente de administración de riesgo denominado *información y comunicación*?
29. ¿Qué aspectos identifican el componente de administración de riesgo denominado *monitoreo*?
30. ¿Cuáles fueron las principales causas para promulgar de parte de las organizaciones gremiales y de los gobiernos, el denominado *gobierno corporativo*?
31. ¿Qué sistema de responsabilidad determina un *gobierno corporativo*?
32. ¿Bajo qué principios se rige un *gobierno corporativo*?
33. ¿Cómo se forma y para qué un Comité de Auditoría?
34. ¿El E.R.M. y el gobierno corporativo van separados o deben ir entrelazados?
35. ¿Qué relación tiene una auditoría interna con los nuevos enfoques del E.R.M., el gobierno corporativo y de los controles internos en general?
36. ¿Qué labores principales debe efectuar una organización de auditoría interna?
37. ¿Qué son servicios de aseguramiento de una Auditoría Interna?
38. ¿Qué son servicios de consultoría de auditoría interna y cómo se deben prestar?
39. ¿Qué Institución a nivel internacional es la que ha perfeccionado y modernizado a las organizaciones de auditoría interna por medio del código de ética, normas y consejos para la práctica?
40. ¿Cómo se trata dentro del libro, la gestión o administración de riesgos, por parte de la auditoría interna?
41. ¿Qué aspectos de evaluación presenta la FLAI a los servicios de aseguramiento y consultoría de una auditoría interna?

1

El control interno (modelos)

*CP Miguel Antonio Cano (q.e.p.d.)
CP Rodrigo Estupiñán Gaitán*

¿Qué es el Control Interno?

“Las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para proporcionar razonable confianza en que los objetivos de los negocios serán alcanzados y que los eventos indeseados serán prevenidos o detectados y corregidos”.

El control interno es definido en forma amplia como un proceso, efectuado por el Consejo de Administración, la Dirección y el resto del personal de una Entidad, diseñado para proporcionar una razonable seguridad con miras a la realización de objetivos en las siguientes categorías:

- Efectividad y eficiencia de las operaciones
- Confiabilidad de la información financiera
- Acatamiento de las leyes y regulaciones aplicables

La primera categoría apunta a los objetivos básicos de la empresa, incluyendo metas de desempeño rentabilidad y salvaguarda de recursos.

La segunda está relacionada con la preparación y publicación de estados financieros dignos de confianza, incluyendo estados financieros intermedios y resumidos e información financiera derivada de dichos estados tales como ganancias por distribuir, reportadas públicamente.

La tercera se ocupa del cumplimiento de las leyes y regulaciones a que la empresa está sujeta.

El control interno comprende el plan de organización y todos los métodos y medidas coordinadas adoptadas dentro de una empresa para salvaguardar sus bienes, comprobar la exactitud y veracidad de los datos contables, promover la eficiencia operante y estimular la adhesión a los métodos prescritos por la gerencia.

“Control Interno en sentido amplio, se define como un proceso efectuado por el Consejo de Administración, la Dirección y el resto del personal de una Entidad, diseñado para proporcionar una razonable seguridad respecto al logro de objetivos, dentro de las siguientes categorías: eficacia y eficiencia de las operaciones, confiabilidad de la Información financiera y cumplimiento con las leyes y normas aplicables”.

La Importancia del Control

A partir de la publicación del informe COSO (Control Interno- Estructura Integrada) en septiembre de 1992 y en cuyo desarrollo participaron representantes de organizaciones profesionales de contadores, de ejecutivos de finanzas y de Auditores Internos, ha resurgido en forma impresionante la atención hacia el mejoramiento del control interno y un mejor gobierno corporativo, lo, cual fue derivado de la presión pública para un mejor manejo de los recursos públicos o privados en cualquier tipo de organización, esto ante los numerosos escándalos, crisis financieras o fraudes, durante los últimos decenios. Al respecto, es importante resaltar el concepto de la “responsabilidad” (accountability), como uno de los factores claves para el gobierno o dirección corporativa de las organizaciones: en este sentido, conviene recordar que un eficiente sistema de control puede proporcionar un importante factor de tranquilidad, en relación con la responsabilidad de los directivos, los propietarios, los accionistas y los terceros interesados.

El Modelo COSO, tanto con la definición de Control que propone, como con la estructura de Control que describe, impulsa una nueva cultura administrativa en todo tipo de organizaciones, y ha servido de plataforma para diversas definiciones y modelos de Control a nivel internacional. En esencia, todos los modelos hasta ahora conocidos, persiguen los mismos propósitos y las diferentes definiciones, aunque no son idénticas, muestran mucha similitud.

Definición de Control Interno

Por ser el modelo mayoritariamente adoptado a la fecha, como referencia tomamos la definición que establece el informe COSO, la cual señala¹:

1 El control interno comprende el plan de la organización y todos los métodos y medidas coordinados que se adoptan en un negocio para salvaguardar sus activos, verificar la exactitud y la confiabilidad de sus datos contables, promover la eficiencia operacional y fomentar la adherencia a las políticas prescritas. MANTILLA, Samuel. CANTE, Sandra, (2005). *Auditoría del Control Interno*, Ecoe ediciones, 1ª ed. p.11

Los modelos de controles actuales

A partir de la divulgación del informe COSO se han publicado diversos modelos de Control, así como numerosos lineamientos para un mejor gobierno corporativo; los más conocidos, además del COSO (USA), son los siguientes: COCO (Canadá), Cadbury (Reino Unido), Vienot (Francia), Peters (Holanda) y King (Sudáfrica). Los modelos COSO y COCO en nuestro continente son los de mayor aplicación; por ello a continuación se hace como referencia una muy breve descripción del enfoque y estructura que cada uno plantea.

EL MODELO COSO

El modelo COSO I

Los tópicos que se comentan a continuación se refieren a la práctica de nuevas técnicas para evaluar el control interno a través de las cuales, la función de auditoría interna pretende mejorar la efectividad de su función y con ello ofrecer servicios más eficientes y con un valor agregado.

La actual *definición del control* interno emitida por **The Committee of Sponsoring Organizations of the Treadway Commission** de los Estados Unidos de Norteamérica, a través del documento denominado “Control Interno-Marco Integrado” mejor conocido como el Modelo de Control COSO, amplía el concepto de la siguiente manera:

“...un proceso efectuado por la Junta Directiva de la entidad, por la Administración y por otro personal diseñado para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos...”

En este sentido se entiende que el control interno se encuentra sobre las personas y, en consecuencia, en cualquier parte de los sistemas, procesos, funciones o actividades y no en forma separada como teóricamente se pudiera interpretar de los enunciados del proceso administrativo, que declara que la administración organiza, planea, dirige y controla.

El señalamiento de propósito del Control en cuanto a asegurar razonablemente el cumplimiento de objetivos de tipo operacional, financiero y normativo, se comprende mejor cuando se analizan los cinco componentes del modelo COSO y sus 17 factores que en conjunto forman una estructura integrada de control, ya que existe una relación directa entre los objetivos que la organización persigue y los citados componentes, puesto que estos representan lo necesario para la consecución de tales objetivos.

Los componentes y factores se presentan en mayor o menor grado en cualquier área, proceso o división de toda organización y se reconoce que los compo-

entes con mayor influencia e importancia son los dos primeros: el Ambiente de Control y la Evaluación de Riesgos.

Estructura del control interno propuesta por el modelo COSO. Identifica cinco componentes interrelacionados:

- | | |
|---------------------------|-------------------------------|
| 1. Ambiente de Control | 4. Información y comunicación |
| 2. Evaluación de riesgos | 5. Monitoreo |
| 3. Actividades de control | |

1. **Ambiente de Control** es el elemento que proporciona disciplina y estructura. El ambiente de control se determina en función de la integridad y competencia del personal de una organización; los valores éticos son un elemento esencial que afecta a otros componentes del control. Entre sus factores se incluye la filosofía de la administración, la atención y guía proporcionados por el consejo de administración, el estilo operativo, así como la manera en que la gerencia confiere autoridad y asigna responsabilidades, organiza y desarrolla a su personal.

Establece el tono de una organización, influenciando en la gente la conciencia o conocimiento sentido del control. Esta es la fundamentación para todos los otros componentes del control interno, suministrando disciplina y estructura. El ambiente de control incluye factores de integridad, valores éticos y competencia del personal de la entidad.

Factores del ambiente de control

Un evaluador debe considerar cada factor del ambiente de control para determinar cuando existe un ambiente de control positivo. Se presentan a continuación varios aspectos a tener en cuenta, la lista no es completa, no todos los ítems se aplican pero sirve como punto de partida.

AMBIENTE DE CONTROL

Integridad y valores éticos	Descripción y comentarios
<p>Existencia e implementación de códigos de conducta y otras políticas mirando las prácticas de negocios aceptables, los conflictos de interés, o los estándares esperados de comportamiento ético y moral.</p> <p>Relaciones con los empleados, proveedores, clientes, inversionistas, acreedores, aseguradores, competidores y auditores, etc. (por ejemplo, si los administradores orientan el negocio sobre un plano de alta ética, e insisten que otros lo hagan, o presten poca atención a los asuntos éticos).</p>	