UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
CENTRO UNIVERSITARIO DE ORIENTE
CIENCIAS ECONÓMICAS
CONTADURÍA PÚBLICA Y AUDITORÍA

AUDITORÍA DE CONTROL Y GESTIÓN DE RIESGOS BASADO EN EL INFORME COSO II: ADMINISTRACIÓN DEL RIESGO EMPRESARIAL

JORGE EDUARDO VILLATORO BOLAÑOS

CHIQUIMULA, GUATEMALA, OCTUBRE 2010

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
CENTRO UNIVERSITARIO DE ORIENTE
CIENCIAS ECONÓMICAS
CONTADURÍA PÚBLICA Y AUDITORÍA

AUDITORÍA DE CONTROL Y GESTIÓN DE RIESGOS BASADO EN EL INFORME COSO II: ADMINISTRACIÓN DEL RIESGO EMPRESARIAL

TRABAJO DE GRADUACIÓN
(MONOGRAFÍA)

Sometida a consideración del Honorable Consejo Directivo

Por

JORGE EDUARDO VILLATORO BOLAÑOS

Previo a optar al título de:

CONTADOR PÚBLICO Y AUDITOR

En el grado académico de

LICENCIADO

CHIQUIMULA, GUATEMALA, OCTUBRE 2010

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
CENTRO UNIVERSITARIO DE ORIENTE
CIENCIAS ECONÓMICAS
CONTADURÍA PÚBLICA Y AUDITORÍA

RECTOR

Lic. CARLOS ESTUARDO GÁLVEZ BARRIOS

CONSEJO DIRECTIVO

Presidente:	MSc. NERY WALDEMAR GALDÁMEZ CABRERA
Representantes de Profesores:	MSc. GILDARDO GUADALUPE ARRIOLA MAIRÉN
	Dr. BENJAMÍN ALEJANDRO PÉREZ VALDÉS
Representante de Graduados:	Ing. Agr. WALTER ORLANDO FELIPE ESPINOZA
Representantes Estudiantiles:	P. C. EDGAR WILFREDO CHEGUÉN HERRERA
	A.T. GIOVANNA GISELA SOSA LINARES
Secretario:	Lic. TOBÍAS RAFAEL MASTERS CERRITOS

AUTORIDADES ACADÉMICAS

Coordinador Académico:	Ing. Agr. FILIBERTO COY CORDÓN
Coordinador del Programa:	MSc. GILDARDO GUADALUPE ARRIOLA MAIRÉN

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

Contabilidad	M.A. RAÚL AUGUSTO DÍAZ MONROY
Auditoría	Lic. LUIS EDUARDO CASTILLO RAMÍREZ
Finanzas e Impuestos:	MSc. GILDARDO GUADALUPE ARRIOLA MAIRÉN

JURADO QUE PRACTICÓ LA EVALUACIÓN DEL INFORME FINAL DEL TRABAJO DE GRADUACIÓN

Presidente:	Lic. JOSÉ ABELARDO RUANO CASASOLA
Secretario:	Lic. EDY ALFREDO CANO ORELLANA
Vocal:	Lic. LUIS EDUARDO CASTILLO RAMÍREZ

Chiquimula, 12 de octubre de 2010

Maestro
NERY WALDEMAR GALDÁMEZ CABRERA
PRESIDENTE DEL CONSEJO DIRECTIVO
Su Despacho

Señor Presidente:

En virtud del nombramiento emitido por la Coordinatura Adjunta del Programa de Ciencias Económicas de este centro de estudios superiores, procedí a asesorar el trabajo de graduación profesional del Auditor Técnico **JORGE EDUARDO VILLATORO BOLAÑOS**, que consistió en el desarrollo de la monografía que intituló: "**AUDITORÍA DE CONTROL INTERNO Y GESTIÓN DE RIESGOS BASADO EN EL INFORME COSO II: ADMINISTRACIÓN DEL RIESGO EMPRESARIAL**".

Con los cambios habidos a nivel mundial en el mundo de los negocios y el surgimiento de nuevas modalidades en el gerenciamiento de las entidades, se ha podido determinar que los viejos esquemas y técnicas para realizar una auditoría interna ya no responden a las necesidades actuales. En ese orden de ideas, ha surgido un nuevo modelo, que se basa en los informes presentados por el Comité de Organizaciones Patrocinadoras de la Comisión Treadway, integrado por la Asociación Americana de Contadores, el Instituto Americano de Contadores Públicos Autorizados, el Instituto de Ejecutivos Financieros, el Instituto de Auditores Internos, y el Instituto de Contadores Gerenciales, a los cuales se les ha denominado COSO I y COSO II.

Sobre la base de ese modelo el auditor interno está en mejor disposición de cumplir con los objetivos de una auditoría, con su proceso de planificación, ejecución, control y comunicación de los resultados obtenidos en la evaluación del control interno y la gestión de riesgos de una entidad.

La investigación se justifica, por cuanto, aporta elementos que esclarecen la aplicación del modelo y seguramente será de beneficio para los profesionales que se dedican a la prestación de este tipo de servicios, como a estudiantes que actualmente se forman en dicha área.

Por lo expuesto, en mi opinión, el trabajo de graduación profesional del señor Jorge Eduardo Villatoro Bolaños, cumple con los requisitos exigidos por el Normativo de Trabajos de Graduación de la Carrera de Contaduría Pública y Auditoría de este centro de estudios, por lo que por su medio, recomiendo al Consejo Directivo, se acepte como requisito parcial previo a optar al título de **Contador Público y Auditor** y el grado académico de Licenciado.

Atentamente,

"ID Y ENSEÑAD A TODOS"

Prof. Gildardo Guadalupe Arriola Mairén
ASESOR PRINCIPAL

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
CIENCIAS ECONOMICAS
COORDINADOR GENERAL
-CUNORI-

CENTRO UNIVERSITARIO DE ORIENTE
Finca El Zapotillo, Zona 5, Chiquimula
Teléfono 79424679 Extensión 114

CUNORI
CIENCIAS ECONOMICAS

PROVIDENCIA: CCEE-LCPA-004/2010

COORDINATURA GENERAL DEL PROGRAMA DE CIENCIAS ECONÓMICAS DEL CENTRO UNIVERSITARIO DE ORIENTE DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA: Chiquimula, doce de octubre de dos mil diez.- - - - - - - - - - - - - -

ASUNTO: Solicitud de impresión del informe final de trabajo de graduación, intitulado: "**AUDITORÍA DE CONTROL Y GESTIÓN DE RIESGOS BASADO EN EL INFORME COSO II: ADMINISTRACIÓN DEL RIESGO EMPRESARIAL**", que para optar al título de **CONTADOR PUBLICO Y AUDITOR y** el grado académico de **Licenciado**, presenta el estudiante **JORGE EDUARDO VILLATORO BOLAÑOS**.- - - - - - - - - - - - - - - - - - -

Siendo que en opinión de esta Coordinatura, el informe final del trabajo de graduación presentado cumple plenamente con los requisitos establecidos por el normativo específico, atentamente pase a la Dirección, para que se sirva autorizar la impresión del informe de mérito.

"ID Y ENSEÑAD A TODOS"

Prof. Gildardo Guadalupe Arriola Mairén
COORDINADOR GENERAL

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
CIENCIAS ECONOMICAS
COORDINADOR GENERAL
-CUNORI-

NOTA: Únicamente el autor del trabajo de graduación es responsable de la originalidad, autenticidad de los datos aportados, opiniones o doctrinas sustentadas, redacción, ortografía y citas bibliográficas; incluyendo, la apropiación indebida de créditos que no le corresponden por no ser de su autoría, que pudieran ser violatorias de los derechos de autor o de las normas de ética.

c.c. Archivo

DICTAMEN DE LA COORDINATURA: TRABAJO DE GRADUACIÓN
ESTUDIANTE: JORGE EDUARDO VILLATORO BOLAÑOS - 199840147

DIRECCIÓN DEL CENTRO UNIVERSITARIO DE ORIENTE DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA: Chiquimula, dieciséis de octubre de dos mil diez.- -

Con base en el dictamen favorable emitido por el profesor GILDARDO GUADALUPE ARRIOLA MAIRÉN, Asesor y Coordinador General del Programa de Ciencias Económicas, se acepta el informe final del trabajo de graduación intitulado: "**AUDITORÍA DE CONTROL Y GESTIÓN DE RIESGOS BASADO EN EL INFORME COSO II: ADMINISTRACIÓN DEL RIESGO EMPRESARIAL**", que como requisito parcial para optar al título de **CONTADOR PUBLICO Y AUDITOR y** el grado académico de **Licenciado**, presenta el estudiante **JORGE EDUARDO VILLATORO BOLAÑOS**, autorizándose su impresión.- -

"ID Y ENSEÑAD A TODOS"

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA – CENTRO UNIVERSITARIO DE ORIENTE – CHIQUIMULA – DIRECCION

MSc. Nery Waldemar Galdámez Cabrera
DIRECTOR

c.c. Archivo

AGRADECIMIENTOS

A DIOS TODOPODEROSO:

Por haberme dado la sabiduría y el entendimiento para poder llegar al final de mi carrera; por ser mí apoyo, mi luz, mi camino y mi fortaleza en los momentos de debilidad. Te agradezco con todo mi corazón.

A MIS PADRES:

Por su infinito amor, apoyo incondicional, dedicación y empeño en ayudarme a ser una persona mejor cada día; por el esfuerzo y los sacrificios realizados para que alcanzara este triunfo. Gracias por creer en mí y haberme motivado a seguir adelante. Los amo.

A MI HERMANA:

Por su apoyo y por llenar de alegría mi vida; siempre fuiste y serás mi mayor ejemplo. Te quiero y admiro.

A EL MSc. GILDARDO GUADALUPE ARRIOLA MAIREN:

Por compartir desinteresadamente sus amplios conocimientos y experiencia; por el apoyo que me demostró a lo largo de mi carrera; por impulsarme a lograr mi sueño y sobre todo por su invaluable amistad.

A EL LIC. EDY ALFREDO CANO ORELLANA:

Por su valiosa colaboración en la elaboración del presente trabajo.

A MIS COMPAÑEROS(AS) Y AMIGOS(AS):

Miguel Angel Samayoa, Yuri Chang, Rossmary Sagastume, Marvin Monroy, Romelia Roque y Boris Peña; por su incondicional apoyo, desinteresada colaboración, sus preciados consejos y gratos momentos; a todos y cada uno de ustedes gracias por su amistad y cariño.

RESUMEN

Toda organización o entidad constantemente enfrenta riesgos, derivados de las amenazas externas y las debilidades internas, que pueden tener impacto negativo sobre la actividad de la vida de los negocios. Es por ello, que las organizaciones o entidades han adoptado funciones específicas, denominada gestión del riesgo, para identificar eventos potenciales y establecer respuestas, reduciendo los costos o pérdidas asociados con éstos. La administración del riesgo empresarial provee una estructura conceptual para la gestión del riesgo mediante el seguimiento de un proceso básico para identificar, evaluar, medir y reportar amenazas que afectan el logro de los objetivos de la entidad u organización; simultáneamente a este proceso debe ir unido el establecimiento de normas internas que le ayuden a cumplir sus metas, evitando peligros no reconocidos y sorpresas a lo largo del camino.

Entre los objetivo establecidos para la investigación se consideraron: a) Describir la metodología que debe utilizar el auditor interno en la evaluación del control interno y la gestión de riesgos según el informe COSO II sobre la administración del riesgo empresarial; b) Definir el marco teórico referido al control interno así como los componentes que lo integran según el informe COSO I; c) Definir el marco teórico referido a la auditoría interna, su proceso de planeación y ejecución; d) Definir los conceptos y categorías sobre el riesgo y su proceso de administración según el informe COSO II; y e) Desarrollar un modelo sobre el proceso de administración de riesgos.

Para abordar el objeto de estudio, se utilizaron los modelos propuestos por el Committee of Sponsoring Organizations of the Treadway Commission (COSO) denominados Informe COSO I sobre control interno e Informe COSO II sobre la administración del riesgo empresarial. La contribución de la investigación radica principalmente en dar a conocer estos informes y en el empleo de modelos de evaluación y gestión diferentes a los que tradicionalmente aplican los auditores internos.

La investigación comprendió la recopilación de diversas fuentes de información dispersas, las cuales se expusieron en forma sistemática y lógica, de manera que permitiera al investigador tener una guía de ayuda que facilitara la comprensión del sistema de control interno en la planeación y desarrollo de la auditoría y el diseño de procedimientos de

auditoría en la gestión del riesgo. Durante este proceso se tuvo la limitante que en el medio guatemalteco no se cuenta con la literatura especializada.

Entre las principales conclusiones y recomendaciones, se determinó: a) Que el departamento de recursos humanos debe contar con profesionales que se dediquen a investigar a los empleados potenciales; considerando que el recurso humano es el elemento más importante del control interno y de la gestión de riesgos; b) Las personas que ocupen los cargos de auditores internos deben ser profesionales con conocimientos en diversas áreas; c) Las organizaciones o entidades deben contar con instrumentos que permitan identificar los riesgos y sus efectos; y d) Las organizaciones o entidades deben responder ante la administración de riesgos de acuerdo a sus características particulares y actividades en las que participa.

ÍNDICE GENERAL

CAPÍTULO II

LA AUDITORÍA INTERNA

CAPÍTULO III

ADMINISTRACIÓN DEL RIESGO EMPRESARIAL

CAPÍTULO IV
PROCESO DE ADMINISTRACIÓN DE RIESGOS

ÍNDICE DE CUADROS

ÍNDICE DE FIGURAS

LISTA DE ABREVIATURAS

COSO:	Committee Of Sponsoring Organizations (Comité de organizaciones patrocinadoras)
DOFA:	Debilidades, Oportunidades, Fortalezas y Amenazas
ERM:	Enterprise Risk Management (Gestión de riesgo empresarial)
FODA:	Fortalezas, Oportunidades, Debilidades y Amenazas
GESI:	Gubernamentales, Económicos, Sociales e Informáticos
IFAC:	International Federation of Accountants (Federación internacional de contadores)
IIA:	Instituto Internacional de Auditoria Interna
IT:	Tecnología de Información
PCGA:	Principios de Contabilidad Generalmente Aceptados
PEST:	Políticos, Económicos, Sociales y Tecnológicos

INTRODUCCION

El ambiente cambiante y de alto nivel competitivo en el que operan las empresas en general, crea un nivel de riesgo e incertidumbre por lo que resulta necesario establecer un sistema de control interno que promueva la eficiencia, reduzca los riesgos y ayude a asegurar la confiabilidad de los estados financieros y el cumplimiento de las leyes y regulaciones; un sistema de control interno no importando que tan bien ha sido concebido y operado, éste solo puede proveer seguridad razonable y es por ello la auditoría interna desempeña un rol importante dentro de una organización.

Las Normas Internacionales de Auditoría señalan que el auditor deberá obtener una compresión suficiente del sistema de control interno para planear la auditoría y desarrollar un enfoque de auditoría efectivo. Además que debería usar su juicio profesional para evaluar el riesgo de auditoría y diseñar los procedimientos de auditoría para asegurar que el riesgo se mantenga a un nivel aceptablemente bajo. Esta compresión del sistema de control interno y la capacidad del auditor de diseñar procedimientos que reduzcan el riesgo, requieren del conocimiento claro y amplio de los conceptos de: control interno y gestión de riesgos además de las herramientas disponibles para su evaluación.

La presente investigación persigue dar a conocer esos conceptos así como modelos y herramientas que el auditor interno puede utilizar al momento de planear su auditoría; para tal efecto se utilizaron como base los informes presentados por el Comité de Organizaciones Patrocinadoras (COSO) de la Comisión Treadway integrado por la Asociación Americana de Contadores (AAA), el Instituto Americano de Contadores Públicos Autorizados (AICPA), el Instituto de Ejecutivos Financieros (FEI), el Instituto de Auditores Internos (IIA) y el Instituto de Contadores Gerenciales (IMA); denominados Informe COSO I bajo cinco componentes de control interno (ambiente de control, evaluación de riesgos, actividades de control, información y comunicación y monitoreo) el cual estableció nuevas técnicas para la implementación y evaluación del control interno y el informe COSO II para la práctica de la Administración de Riesgos Empresariales ERM bajo ocho componentes (análisis del entorno interno, definición de objetivos, identificación de eventos, valoración de riesgos, respuesta al riesgo, actividades de control, información y comunicación y monitoreo), en el cual se desarrolló una estructura conceptual para la administración del riesgo empresarial. Partiendo de estos informes el auditor puede

obtener la compresión necesaria que le permita cumplir con los objetivos de la auditoría en el proceso de planificación, ejecución, control y comunicación de los resultados de su trabajo en la evaluación del control interno y la gestión de riesgos.

La investigación es de carácter monográfico y se centra principalmente en reunir en un solo documento y en clarificar los conceptos de control interno y gestión de riesgos, los componentes que los integran, las herramientas de evaluación así como el proceso que debe seguir el auditor interno al momento de planear su auditoría basada en riesgos.

El informe se estructura en cuatro capítulos. En el primero se desarrolló el tema del control interno, en el cual se describen las definiciones del control interno su importancia y aplicación, sus elementos así como las partes responsables de su implantación y funcionamiento. En el segundo, la auditoría interna; en este capítulo se exponen temas relacionados con la auditoría interna y su organización, sus objetivos y alcance, la planificación y ejecución y la presentación de informes. En el tercero, la administración del riesgo empresarial; en este capítulo se define el riesgo, y su administración, los beneficios y componentes, las limitaciones y el proceso de la auditoría en la administración de los riesgos. Y en el cuarto capítulo, se describe el proceso de administración del riesgo; en éste se plantean los pasos que sigue la administración de riesgos: definición del contexto, identificación, análisis, valoración y tratamiento de los riesgos, monitoreo, revisión, comunicación y consulta.

CAPÍTULO I
EL CONTROL INTERNO

1.1 Control

El control forma parte ineludible del ambiente de cualquier organización, ayudando a los gerentes a detectar los cambios que afectan a sus organizaciones; Ricardo Vilches define control como: "Cualquier acción que lleva a cabo una persona para aumentar la probabilidad de que se logren las metas y objetivos propuestos. Su propósito final es, preservar la existencia de cualquier organización y apoyar a su desarrollo; su objetivo es contribuir con los resultados esperados.

El control no debe ser aislado, sino un todo, relacionado con los planes estratégicos de la empresa y su gestión organizacional. Está diseñado para proporcionar una razonable seguridad respecto al logro de objetivos, dentro de las categorías eficacia, eficiencia y economía de las operaciones, confiabilidad de la información financiera y cumplimiento con leyes y normas aplicables.

La responsabilidad de organizar, establecer y mantener el sistema de control, el cual debe ser adecuado a la naturaleza, estructura y fines de la organización le corresponde a la máxima autoridad jerárquica de la empresa; sin embargo, todo el personal tiene responsabilidades sobre el control, las cuales deben formar parte, explícita o implícita, de la descripción del trabajo de cada uno. Asumiendo el compromiso de comunicar problemas y violaciones que se observen y que afecten el logro de los objetivos".[1]

1.1.1 Tipos de controles

Entre los tipos de control, están los siguientes:

- **Controles directivos:** son todos aquellos procedimientos, estructuras funcionales, directrices, políticas y normas estratégicas, emanados desde la más alta gerencia

[1] Ricardo Vilches Troncoso. Apuntes del Estudiante de Auditoría [en línea]. Consultado el 20 de agosto de 2009. Disponible en: http://www.ecobachillerato.com/temasecem/auditoria.pdf

de la empresa con el fin de delimitar la gestión estratégica de la organización y que dicha gestión esté sincronizando con los objetivos del negocio;

- **Controles preventivos:** son todos aquellos procedimientos administrativos y/o automatizados orientados a prevenir antes de su ocurrencia o materialización, riesgos que puedan afectar la seguridad física y lógica de las áreas impactando negativamente en la continuidad de las operaciones de negocio;

- **Controles detectivos:** son todos aquellos procedimientos administrativos y/o automatizados orientados a detectar la ocurrencia o materialización, de los riesgos o acciones indeseadas que puedan afectar la seguridad física o lógica de las áreas impactando negativamente en la continuidad de las operaciones del negocio;

- **Controles correctivos:** son todos aquellos procedimientos administrativos y/o automatizados orientados a corregir o restaurar un objeto que haya sufrido la ocurrencia o materialización, de los riesgos o acciones indeseadas que afectaron la seguridad física o lógica de las áreas impactando negativamente en la continuidad de las operaciones del negocio; y

- **Controles de recuperación:** son todos aquellos procedimientos administrativos y/o automatizados orientados a recuperar la capacidad de operación, servicio y gestión de negocio frente a la materialización, de los riesgos o acciones indeseadas que afectaron la seguridad física o lógica de las áreas impactando negativamente en la continuidad de las operaciones del negocio.[2]

1.1.2 Sistema de control interno

Toda organización requiere un sistema que le permita identificar los riesgos a los cuales está expuesta y le provea las actividades de control necesarias para minimizarlos hasta que el riesgo residual sea considerado aceptable; un buen sistema de control interno es lo que permite a cualquier organización tener mayores posibilidades de lograr los objetivos que la misma fija. El sistema de control interno "es un instrumento de gestión que comprende el plan de la empresa, conjuntos y procedimientos adoptados para

[2] Ibid., p. 16.

salvaguardar su patrimonio, verificar la exactitud y veracidad de su información financiera y administrativa, promover la eficiencia en las operaciones, estimular las políticas y comprender el cumplimiento de las metas y objetivos programados.

Algunas de sus herramientas son los organigramas, manuales de funciones, manuales o normas de procedimientos internos, matriz de autorizaciones, etc.

El objetivo del control interno es permitir el logro de las metas y resultados presupuestados por la administración, es decir, se cumplirá a través del logro de los siguientes objetivos intermedios:

- **El logro de la protección de los activos:** la seguridad de los activos supone que los bienes de la organización sean utilizados de forma normal en el cuadro del objetivo social, que sus derechos sean salvaguardados y que la empresa no corra riesgos anómalos. En otras palabras, proteger los activos contra cualquier situación no deseable;

- **La obtención de información adecuada:** el control interno tiene el objetivo de permitir que toda la información, particularmente la contable y de gestión, es veraz, oportuna y no ha sido alterada por errores o negligencias, permitiendo de este modo una adecuada toma de decisiones y preparación de estados financieros de acuerdo con los principios de contabilidad generalmente aceptados o cualquier otro criterio aplicable, a fin de mantener activos y obligaciones debidamente contabilizados;

- **Promover la eficiencia operativa:** esto implica establecer acciones o controles que tiendan a hacer más eficientes los procesos, como por ejemplo, evitar pérdidas de existencias por compras mal planificadas, evitar el mantenimiento de una estructura fija obsoleta, etc.; y

- **Estimular la adhesión a las políticas de la dirección:** esto también puede entenderse como asegurar la aplicación de las instrucciones de la dirección, para ello el sistema de control interno debería asegurarse que el objetivo de las instrucciones está bien definido y que las mismas son claras, apropiadas y

comprensibles, estando dirigidas a las personas adecuadas, asegurándose además que dichas instrucciones sean aplicadas".[3]

1.2 Definición

Existían muchas y diversas definiciones y opiniones sobre el control interno; así es que se desarrollaron algunas estructuras de control que alcanzaron amplia difusión internacional, principalmente por la obligatoriedad que existe en algunos países de que las organizaciones informen a terceros sobre la eficacia de su sistema de control interno. En los últimos años se han elaborado una serie de informes que presentan un enfoque integrador sobre el control interno, siendo el más difundido el Informe COSO, que fuera publicado en 1992 en Estado Unidos, el cual define el control interno como: "…un proceso, ejecutado por el consejo de directores, la administración y otro personal de una entidad, diseñado para proporcionar seguridad razonable con miras a la consecución de objetivos en las siguientes categorías:

- Efectividad y eficiencia de las operaciones;
- Confiabilidad en la información financiera; y
- Cumplimiento de las leyes y regulaciones aplicables.

Esta definición refleja ciertos elementos fundamentales:

1.2.1 Es un proceso

El control interno no es un evento o circunstancia, sino una serie de acciones que penetran las actividades de una entidad. Tales acciones son penetrantes, y son inherentes a la manera como la administración dirige los negocios.

El proceso de los negocios, que es conducido con o a lo largo de las unidades o funciones de la organización, es administrado mediante el proceso básico gerencial de planeación, ejecución y monitoreo. El control interno es parte de ese proceso y está integrado al mismo. Les facilita funcionar y monitorear su conducta y relevancia continuada. Es una herramienta usada por la administración, no un sustituto de la administración.

---

[3] Ibid., p. 16.

Esta conceptualización del control interno es muy diferente de la perspectiva de algunos observadores quienes ven el control interno como un añadido a las actividades de la entidad, o como una carga necesaria, impuesta por los reguladores o por los dictados de burócratas extremadamente celosos. El sistema de control interno está entrelazado con las actividades de operación de una entidad y fundamentalmente existe por razones de negocios. Los controles internos son más efectivos cuando se construyen dentro de la infraestructura de la entidad y son parte de la esencia de la empresa.

1.2.2 Es ejecutado por personas

El control interno es ejecutado por un consejo de directores, la administración y otro personal de una entidad. Es realizado por las personas de una organización quienes establecen los objetivos de la entidad y ubican los mecanismos de control en su sitio.

El personal de la organización incluye al consejo de directores, así como la administración y otras personas. Aunque los directores suelen ser vistos como quienes primariamente proporcionan supervisión, también proporcionan dirección y aprueban ciertas transacciones y políticas. Por lo tanto, son un elemento importante del control interno.

1.2.3 Proporciona seguridad razonable

El control interno, no tanto cómo es diseñado y operado, puede proporcionar solamente seguridad razonable a la administración y al consejo de directores con miras a la consecución de los objetivos de una entidad. La probabilidad de conseguirlos está afectada por las limitaciones inherentes a todos los sistemas de control interno. Ellas incluyen la realidad de que los juicios humanos en la toma de decisiones pueden ser defectuosos, las personas responsables del establecimiento de los controles necesitan considerar sus costos y beneficios relativos, y la desintegración puede ocurrir a causa de fallas humanas tales como errores o equivocaciones. Adicionalmente, los controles pueden circunscribirse a la colusión de dos o más personas. Finalmente, la administración tiene la capacidad de desbordar el sistema de control interno.

1.2.4 Consecución de objetivos

Cada entidad fija su misión, estableciendo los objetivos que espera alcanzar y las estrategias para conseguirlos. Los objetivos pueden ser para la entidad, como un todo, o específicos para las actividades dentro de la entidad. Aunque muchos objetivos pueden ser específicos para una entidad particular, algunos son ampliamente participados. Por ejemplo, los objetivos comunes a casi todas las entidades son la consecución y el mantenimiento de una reputación positiva dentro del comercio y los consumidores, proporcionando estados financieros confiables a los accionistas, y operando en cumplimiento de las leyes y regulaciones.

Los objetivos se pueden ubicar dentro de tres categorías:

- **Operaciones:** relacionados con el uso efectivo y eficiente de los recursos de la entidad;

- **Información financiera:** relacionados con la preparación de estados financieros públicos confiables; y

- **Cumplimiento:** relacionados con el cumplimiento de la entidad con las leyes y regulaciones aplicables.

Esta categorización sitúa el énfasis en aspectos separados del control interno. Tales categorías distintas pero interrelacionadas (un objetivo particular se puede ubicar en más de una categoría) orientan diversidad de necesidades y pueden ser responsabilidad directa de ejecutivos diferentes. Esta categorización también permite distinguir lo que se puede esperar de cada categoría de control interno.

De un sistema de control interno se puede esperar que proporcione una seguridad razonable para la consecución de los objetivos relacionados con la confiabilidad de la información financiera y con el cumplimiento de leyes y regulaciones. El cumplimiento de tales objetivos, en gran parte basados en estándares impuestos por sectores externos, depende de cómo se desempeñen las actividades dentro del control de la entidad.

Sin embargo, la consecución de los objetivos de operación –tales como un retorno particular sobre la inversión, participación en el mercado o ingreso de nuevas líneas de producto- no siempre está bajo el control de la entidad. El control interno no puede prevenir juicios o decisiones incorrectas, o eventos externos que puedan causar una falla en el negocio para la consecución de sus objetivos de operación. Para lograr estos objetivos, el sistema de control interno puede proporcionar seguridad razonable solamente si la administración y, en su papel de supervisión, el consejo están siendo acatados, de manera oportuna, en la orientación dada para la consecución de ellos".[4]

1.3 Objetivos generales

Los objetivos del control interno son diseñados para ayudar a organizar, controlar y mejorar las operaciones en las distintas etapas de su proceso, lo cual se relaciona con:

- Promover la eficiencia de las operaciones en lo relativo a las recaudaciones, distribución y uso de los recursos que generan las actividades empresariales o públicas, dentro del marco correspondiente;

- Promover la utilidad y conveniencia de los sistemas de administración y finanzas, diseñados para el control de las operaciones e información de los resultados alcanzados;

- Ayudar a generar información útil, oportuna, confiable y razonable sobre el manejo, uso y control de los derechos y obligaciones de las empresas o entes públicos;

- Promover la actualización, modernización y sostenibilidad de los sistemas y su tecnología;

- Promover la aplicación de las leyes, reglamentos y los procedimientos diseñados para que toda autoridad, ejecutivo y funcionario, rindan cuenta oportuna de los

---

[4] Samuel Alberto Mantilla B. Control Interno: Informe COSO. (Bogotá: Ecoe Ediciones Ltda, 2007), p.14.

resultados de su gestión en el marco de un proceso transparente y ágil de rendición de cuentas; y

- Motivar la capacidad administrativa para reaccionar frente a los estímulos negativos de su entorno, para que esté en condiciones de identificar, comprobar e impedir, posibles malos manejos de los recursos disponibles, así como administrar los riesgos existentes.[5]

1.4 Importancia

El control interno es un instrumento eficaz para lograr la eficiencia y eficacia en el trabajo de las entidades, "porque ayuda:

- A que los recursos (humanos, materiales y financieros) disponibles, sean utilizados en forma eficiente, bajo criterios técnicos que permitan asegurar su integridad, su custodia y registro oportuno, en los sistemas respectivos;

- A producir la información administrativa y financiera oportuna, correcta y confiable, como apoyo a la administración en el proceso de toma de decisiones y la rendición de cuentas de la gestión de cada responsable de las operaciones;

- A detectar los riesgos de errores e irregularidades como base para identificar sus causas y promover acciones correctivas que permitan manejar y controlar los riesgos y sus efectos; y

- A promover el cumplimiento de las políticas gerenciales, así como de las leyes y reglamentos aplicables, en todos los niveles y procesos de la organización, para la consecución de las metas y objetivos programados en forma efectiva, eficiente y económica".[6]

---

[5] René Fonseca Borja. Auditoría Interna: Un enfoque moderno de planificación, ejecución y control. (Guatemala: Artes Gráficas Acrópolis, 2004), p.114.

[6] Ibid., p.114.

1.5 Aplicación

El control interno es global e integrado, diseñado en forma específica para cada ámbito de operación que tenga la empresa o ente público. Por tanto, abarca toda la estructura organizacional, los sistemas administrativos y financieros, y todas las operaciones que ocurran en todos los niveles de la organización o ente público, independientemente de dónde estas se realicen, y de quienes intervengan en los procesos y conducción de las mismas, es decir que nada queda fuera del mismo; no hay operación que no se controle o que no se informe de su funcionamiento, ni que se deje de medir sus resultados, incluyendo a las personas, quienes son las que hacen buenos o malos los procesos.[7]

1.6 Implantación

Con el fin de que el control interno dentro de una organización, se implante y funcione de la forma más adecuada, es necesario:

- **Darle una concepción sistemática:** el diseño y la implantación de los controles internos se debe hacer en forma sistemática, con base en las necesidades y prioridades institucionales, es decir, tomando como base el campo real de los hechos empresariales o públicos, para evitar el trasplante de controles que funcionan bien en otras organizaciones, pero que, probablemente, podrían no funcionar en la organización que se quiere implantar;

- **Asignar los recursos suficientes:** el diseño y la implantación del control interno, debe estar respaldado con la asignación de la tecnología y los elementos, humanos, materiales y financieros necesarios, para que se pueda dimensionar suficientemente de acuerdo a las necesidades del sector o la organización global y la interrelación con el entorno en el que se desenvuelve; y

- **Definir objetivos concretos:** para el diseño de los controles internos deben diseñarse los objetivos hacia los que se orientan los controles internos específicos a implantar.

---

7 Ibid., p.115.

Es conveniente, antes de implantar controles internos, que se definan los objetivos específicos que se deben alcanzar al implantar tal o cual medida de control, ya que los objetivos serán los que dirigen los pasos de trabajo para alcanzar aquello que originó la implantación de nuevas medidas de control interno, a más de que servirán de parámetros para medir si los objetivos se alcanzan o no, en función de los resultados obtenidos.

En el diseño e implantación de controles internos, es necesario tener presente que el exceso de controles no garantiza necesariamente que los errores e irregularidades se eviten, por lo tanto es muy saludable definir el costo frente al beneficio en el caso de implantar los controles.[8]

1.7 Restricciones

Un sistema de control interno, no importa que tan bien ha sido concebido y operado, puede proveer solamente seguridad razonable – no absoluta – a la administración y a la junta directiva mirando la consecución de los objetivos de una entidad. “El control interno ha sido visto por algunos observadores como el que asegura que una entidad no fallará, esto es, que la entidad siempre conseguirá sus objetivos de operación, financieros y de cumplimiento. En este sentido, el control interno algunas veces es visto como la cura para todos los males reales y potenciales de los negocios. Este punto de vista no es correcto, el control interno no es una panacea.

Considerando las restricciones del control interno, deben reconocerse dos conceptos distintos:

- Primero, el control interno – lo mismo que el control interno efectivo – opera a niveles diferentes con relación a los distintos objetivos. Para los objetivos relacionados con la efectividad y la eficiencia de las operaciones de una entidad – consecución de su misión básica, objetivos de rentabilidad y semejantes – el control interno puede ayudar a asegurar que la administración sea consciente del progreso de la entidad, o no. Pero no puede proporcionar igual seguridad razonable de que los mismos objetivos se conseguirán; y

---

8 Ibid., p.115.

- Segundo, el control interno no puede proporcionar seguridad absoluta con respecto a cualquiera de las tres categorías de objetivos.

La seguridad razonable ciertamente no implica que los sistemas de control interno fallarán frecuentemente. Muchos factores, individual y colectivamente, sirven para fortalecer el concepto de seguridad razonable. El efecto acumulativo de los controles que satisfacen objetivos múltiples y la naturaleza multipropósito de los controles reducen el riesgo de que una entidad no consiga sus objetivos. Además, las operaciones y responsabilidades de operación normales, diarias, de la gente funcionando en diversos niveles de una organización están dirigidas a la consecución de los objetivos de la entidad. En verdad, en medio de una parte de entidades bien controladas, es muy probable que la mayoría estarán regularmente apreciando el movimiento hacia sus objetivos de operaciones, regularmente conseguirá sus objetivos de cumplimiento, y producirá consistentemente – período a período, año a año – estados financieros confiables. Sin embargo, a causa de las restricciones inherentes discutidas atrás, no hay garantía respecto a que, por ejemplo, un evento incontrolable, una equivocación o un reporte de incidentes impropio nunca puedan ocurrir. En otras palabras, incluso un sistema de control interno efectivo puede experimentar una falla. Seguridad razonable no es seguridad absoluta.

1.7.1 Juicios

La efectividad de los controles estará limitada por la realidad de las fallas humanas en la toma de decisiones. Tales decisiones deben tomarse mediante juicios humanos en el tiempo requerido, basados en información disponible, y bajo las presiones del giro de los negocios. Algunas decisiones basadas en juicios humanos pueden después, con la clarividencia de análisis posteriores, ser el fundamento para producir menos que los resultados deseables, y pueden requerir cambios.

1.7.2 Resquebrajamientos

Aunque los controles internos estén bien diseñados, pueden resquebrajarse. El personal puede interpretar mal las instrucciones. Se pueden hacer juicios equivocados, o cometer errores debido a negligencia, distracción o fatiga. Un supervisor del departamento de contabilidad responsable de la investigación de inconsistencias puede simplemente

olvidarse de o fallar en la orientación de la investigación hasta no ser capaz de realizar las correcciones apropiadas. El personal temporal que ejecuta responsabilidades de control durante las vacaciones o personal enfermo puede no desempeñarse correctamente. Los cambios en los sistemas pueden ser implementados antes que el personal haya sido entrenado para reaccionar apropiadamente a los signos de funcionamiento incorrecto.

1.7.3 Desbordamiento de la administración

Un sistema de control interno solamente puede ser tan efectivo como la gente que es responsable de su funcionamiento. De la misma manera que en las entidades efectivamente controladas – aquellas que generalmente tienen altos niveles de integridad y conciencia de control – un administrador puede ser capaz de desbordar el control interno.

El término desbordamiento de la administración se emplea aquí, para significar el violar las políticas o los procedimientos preestablecidos con propósitos ilegítimos con la intención de que el personal obtenga o acreciente la presentación de la condición financiera o del estado de cumplimiento de una entidad. Un administrador de una división o unidad, o un miembro de la alta administración, puede desbordar el sistema de control por muchas razones: para incrementar ingresos reportados para cubrir un decrecimiento no anticipado en la participación en el mercado, o para aumentar los beneficios reportados para cumplir presupuestos irreales, para empujar el valor de mercado de la entidad antecedente a una oferta o venta pública, para cumplir ventas o protección de beneficios para apalancar desembolso de bonos ligados al desempeño, para simular el cubrimiento de violaciones de acuerdos de convenios de deuda, o para ocultar la falta de cumplimiento con requerimientos legales. Las prácticas de desbordamiento incluyen falsificaciones para banqueros, abogados, contadores y vendedores, y la emisión intencional de documentos falsos tales como órdenes de compra y facturas de venta.

El desbordamiento de la administración no debe confundirse con la intervención de la administración, la cual representa las acciones de la administración para salirse de las políticas o procedimientos prescritos con propósitos legítimos. La intervención de la administración es necesaria para relacionarse con transacciones no recurrentes y no estándares que de otra manera pueden manejarse de manera inapropiada por el sistema

de control. La previsión de la intervención de la administración es necesaria en todos los sistemas de control interno puesto que éstos no se pueden diseñar para anticiparse a cada condición. Las acciones de la administración para intervenir son generalmente manifiestas y comúnmente documentadas o, de otra manera, reservadas para el personal apropiado, mientras que las acciones para desbordarse, generalmente no están documentadas o manifiestas, con la intención de sobrepasarlas.

1.7.4 Colusión

Las actividades colusorias de dos o más individuos pueden derivar en fallas de control. Los individuos que actúan colectivamente para perpetrar y encubrir una acción de detección a menudo pueden alterar los datos financieros u otra información administrativa de manera que no pueda ser identificada por el sistema de control. Por ejemplo, puede haber colusión entre un empleado que desempeña una función de control importante y un cliente, proveedor u otro empleado. En un nivel diferente, algunos estratos de ventas o divisiones administrativas pueden coludir para evadir controles de manera tal que los reportes cumplan presupuestos u objetivos de incentivo.

1.7.5 Costos versus beneficios

Los recursos siempre tienen limitaciones, y por lo tanto las entidades deben considerar lo relativo a los costos y beneficios derivados de establecer controles.

Para determinar si se debe establecer un control particular, debe considerarse el riesgo de fallar y el efecto potencial sobre la entidad, junto con los costos relacionados con el establecimiento de un control nuevo. Por ejemplo, puede no ser rentable para una compañía instalar un sofisticado control de inventarios para monitorear los niveles de materia prima si el costo de la materia prima usada en el proceso de producción es bajo, el material no es peredecedero, está propenso a suplir recursos existentes y está disponible el espacio de almacenamiento.

La medición de costos y beneficios para la implementación de controles se hace con diferentes niveles de precisión. Generalmente, es fácil tratar con el lado de costos de la ecuación que, en muchos casos, puede cuantificarse de una manera verdaderamente

precisa. Todos los costos directos asociados con la institucionalización de un control, y los costos indirectos cuando son medibles de manera práctica, usualmente se consideran. Algunas compañías también incluyen los costos de oportunidad asociados con el uso de los recursos".[9]

1.8 Principios de control interno

Los principios de control interno son indicadores fundamentales que sirven de base para el desarrollo de la estructura y procedimientos de control interno en cada área de funcionamiento institucional; estos se dividen en tres grandes grupos, por su aplicación:

1.8.1 Aplicables a la estructura orgánica

La estructura orgánica necesita ser definida con bases firmes, partiendo de una adecuada separación de funciones de carácter incompatible, así como la asignación de responsabilidad y autoridad a cada puesto o persona, para lo cual son aplicables los siguientes principios de control interno:

a) Responsabilidad delimitada

Este principio permite fijar con claridad las funciones por las cuales adquiere responsabilidad una unidad administrativa o una persona en particular; es decir, a nivel de unidad administrativa y dentro de esta, el campo de acción de cada empleado o servidor público; definiéndole además, el nivel de autoridad correspondiente, para que se desenvuelva y cumpla con su responsabilidad en el campo de su competencia.

Con la nueva tecnología, quizá, para cada empleado, ejecutivo o servidor público; su nivel de autoridad podría corresponder a una clave de acceso al sistema para que en este proceda a autorizar transacciones o realizar operaciones, que sólo el uso de esa clave se lo permite el sistema.

---

9 Mantilla B., Op. Cit., p. 95.

La responsabilidad, independientemente de quien se trate, abarca la organización de la unidad administrativa, el control del personal, los resultados de las operaciones que se ejecutan, y los bienes o activos asignados.

b) Separación de funciones de carácter incompatible

Este principio evita que un mismo empleado, ejecutivo o servidor público, ejecute todas las etapas de una operación dentro de un mismo proceso, por lo que se debe separar la autorización, el registro y la custodia dentro de las operaciones administrativas y financieras, según sea el caso, para evitar que se manipulen los datos y se generen riesgos y actos de corrupción.

Tecnológicamente hablando, quizá, la separación de funciones es un poco más sencilla, pero asimismo, más vulnerable, porque la tecnología puede permitir abusos y usos indebidos que perjudiquen a la organización.

La separación de funciones sustenta incluso la organización física de la organización, actividades afines se concentran y se asignan a una unidad administrativa, llámese Gerencia, Dirección, Departamento, Sección, etc., que en el futuro será la única responsable de ejecutar esas operaciones asignadas, controlar e informar de sus resultados.

c) Instrucciones por escrito

Las instrucciones por escrito dictadas por los distintos niveles jerárquicos de la organización que se reflejan en las políticas generales y especificas, así como en los procedimientos para ponerlos en funcionamiento, garantizan que sean entendidas y cumplidas esas instrucciones, por todo empleado, ejecutivo o servidor público, conforme fueron diseñados.

En este campo también, si hablamos de tecnología, de igual manera, la utilización de redes internas de información, hacen que las órdenes por escrito no necesariamente sean impresas, ya que los correos internos permiten ver documentos en pantalla, lo cual deja sin efecto el papel, pero no el concepto de la orden por escrito como tal.

Es decir que independientemente de la tecnología que se utilice, siempre será aplicable este principio y quedará evidencia para comprobarlo.

1.8.2 Aplicables a los procesos y sistemas

Todos los sistemas integrados o no, deben ser diseñados tomando en cuenta que el control es para salvaguardar los recursos que dispone la organización, destinados a la ejecución de sus operaciones; por tanto, son aplicables los siguientes principios de control interno:

a) Aplicación de pruebas continuas de exactitud

La aplicación de pruebas continuas de exactitud, independientemente de que estén incorporadas a los sistemas integrados o no, permite que los errores cometidos por otros funcionarios sean detectados oportunamente, y se tomen medidas para corregirlos y evitarlos.

Tecnológicamente, es posible diseñar aplicaciones que, periódicamente, estén informando de errores cometidos o sobre las pruebas aplicadas para verificar la exactitud de los datos ingresados para el proceso o salida de los mismos, lo cual evita que el sistema produzca información errónea, y más bien se tenga la oportunidad de analizar y corregir su contenido.

Existen muchos ejemplos de pruebas de exactitud que el auditor debe estar en condiciones de evaluar, para verificar si las mismas son beneficiosas para el proceso o contribuyen a complicar el mismo; un ejemplo de ellas es que el sistema arroje la suma de un lote de transacciones ingresadas, que los valores ingresado cuadren con un documento de autorización o solicitud de proceso, dependiendo, por supuesto, como está estructurado el control.

b) Uso de numeración en los documentos

El uso de numeración consecutiva, para cada uno de los distintos formatos diseñados para el control y registro de las operaciones, sea o no generados por el propio sistema,

permite el control necesario sobre la emisión y uso de los mismos; además, sirve de respaldo de la operación, así como para el seguimiento de los resultados de lo ejecutado.

La numeración de un documento es fundamental porque permite que se relacione con otros datos que pueden ayudar a descubrir malos manejos o pagos duplicados; por ejemplo: en un sistema integrado donde existen fondos rotativos, cuya forma de reposición exige que cada fondo detalle sus gastos y luego en la unidad financiera consolidan los datos para pedir la reposición, existe la posibilidad de que se paguen las mismas facturas con el fondo rotativo pero también que se paguen en la forma normal, sin que el sistema como tal, detecte el número de factura para indicar que esa factura ya fue pagada.

En otras palabras, el sistema no controla el número de factura, sino el número de documento que genera el sistema para el pago, el cual nunca se va a repetir, pero si se puede pagar la misma factura, con dos distintos documentos de pago, por lo que es conveniente utilizar un sello de goma que diga "PAGADO” para evitar que los documentos se vuelvan a utilizar en nuevos pagos.

c) Uso de dinero en efectivo

Muchas organizaciones aún manejan dinero en efectivo por el uso de fondos de caja chica, lo cual si no existe un buen control, puede convertirse en una fuente de desperdicio constante que a la larga, puede constituirse en una gran estafa.

La alta tecnología actual del mercado aplicable a los sistemas integrados, permite que los pagos se realicen sin el uso de dinero en efectivo ni chequeras, utilizando los servicios bancarios y las redes computacionales que ayudan a ordenar el pago a través de transferencias bancarias, directamente a las cuentas de los beneficiarios, según las necesidades y facilidades del mercado, esto es para empleados y proveedores.

Los únicos pagos en efectivo, para aquellos conceptos considerados de urgencia, se deberán realizar a través de un fondo de caja chica, reglamentando su uso y reposición. Sin embargo, el uso de dinero en efectivo, debe ser lo más restringido posible para evitar incluso asaltos o robos porque los delincuentes saben que se maneja dinero en efectivo;

por esto, la mayoría de empresa pagan los sueldos de los empleados utilizando cuentas bancarias personales, lo cual disminuye el riesgo para las dos partes.

d) Uso de cuentas de control

La apertura de los sistemas integrados de contabilidad, debe ser lo suficientemente amplia para facilitar el control de los distintos momentos de las operaciones, así como de aquellos datos que, por sus características, no formen parte del sistema en si; por ejemplo: control de existencias, control de consumo de gasolina, control de mantenimiento y otras operaciones.

Se deben diseñar los registros auxiliares que sean necesarios para controlar e informar al nivel de detalle que la operación requiera; por esto, el contador público debe hacer un análisis de las necesidades de control para armar los procesos, de tal manera que le permita agrupar datos, integrar y consolidar la información según las necesidades de los ejecutivos y demás personas o instituciones que necesitan de dicha información.

e) Depósitos inmediatos e intactos

Probablemente, es el punto donde mayor esfuerzo se ha dedicado, por lo que se ha escrito mucho al respecto, y es de lo que más se preocupan los auditores internos que pierden su tiempo realizando arqueos del efectivo recibido, sea por la venta de productos, o por el cobro a sus clientes.

Según la tecnología utilizada actualmente, las recaudaciones pueden ser captadas por entes ajenos al ente beneficiario, quienes informan de la gestión realizada, así como de las transferencias que se han realizado a la cuenta principal de la organización.

Se deben crear mecanismos que permitan conocer, a la brevedad posible, el monto de las recaudaciones efectuadas, para evitar que se queden valores en poder de terceros, sin que se registren oportunamente en los sistemas respectivos.

En los casos de recaudaciones directas, esos valores deben ser depositados en forma inmediata e intacta, para evitar que se utilice el efectivo en operaciones ordinarias.

f) Uno mínimo de cuentas bancarias

La aplicación del concepto de cuenta principal, cuenta única o cualquier otra denominación, minimiza el uso de cuentas bancarias ya que, utilizando la tecnología disponible en el mercado, el pago se puede efectuar a través de transferencias bancarias, sin que se cuente con una chequera.

Sin embargo, en los casos necesarios, su uso debe ser limitado a las cuentas exclusivamente necesarias, para facilitar el control del movimiento y disponibilidad de fondos asignados para las operaciones; el concepto de mínimo, no necesariamente se refiere a una o dos cuentas bancarias; por ejemplo: si se trata de un ente público, que maneja o administra proyectos, el mínimo de cuentas bancarias será tantas cuentas como proyectos existan. Por supuesto que lo recomendable es que sea un número razonable que ayude a que el control sobre el movimiento y disponibilidad de recursos, sea fácil y efectivo.

g) Uso de dispositivos de seguridad

En las organizaciones que disponen de equipos informáticos, mecánicos o electrónicos, formando parte de los sistemas de información, deben crearse las medidas de seguridad que garanticen un control adecuado del uso de esos equipos en el proceso de las operaciones, así como para que permitan la posibilidad de comprobación de las operaciones ejecutadas.

Los dispositivos de seguridad dependerán de los sistemas, si son de ultima tecnología, los mismos paquetes traen incorporados dispositivos que ayudan a darle seguridad a los procesos; por ejemplo: Una bitácora que registra las operaciones del día; además puede producir un informe que salga en la pantalla de un supervisor, para que este vea que una clave no autorizada está ingresando a un sector del sistema.

Los dispositivos de seguridad, actualmente, no sólo se refieren a la seguridades físicas o alarmas que se podían colocar en los sistemas; hoy tenemos verdaderas claves de acceso, servidores que tienen la función de verificar que no ingrese información contaminada que puede dañar la información o los sistemas. Es decir que la tecnología ha

cambiado enormemente que hay que pensar en cómo se pone en práctica este principio de control.

h) Uso de indicadores de gestión

El diseño y uso de indicadores de gestión debe formar parte de los sistemas, para que permitan medir el grado de control integral de las operaciones y su avance tanto físico como financiero, de tal manera que se puedan hacer análisis de la gestión en los distintos sectores y proyectar de mejor manera a la organización, ayudando a reorientar las acciones, en los casos específicos.

Los auditores internos pueden ser una gran ayuda en el establecimiento de estos indicadores, ya que ellos son los que más conocen de las operaciones de todos los sectores, bien podrían aportar con la identificación de los sectores o temas donde se pueden diseñar indicadores para controlar y medir la gestión.

De la forma más sencilla, los auditores internos pueden elaborar una hoja de los pasos que sigue un proceso, conjuntamente con el responsable de ejecutar los mismos, para identificar los pasos que agregan valor y aquellos que no; luego pueden asignarles un valor numérico individual, con lo que, posteriormente, se puede evaluar y darle un valor de apreciación, lo cual, si se divide el valor de apreciación producto de la evaluación para el valor que se asignó inicialmente al paso en el proceso, se sacaría un porcentaje de riesgo existente, esto ayudaría al auditor interno a orientar su trabajo, así como al responsable de los pasos, a poner mayor atención a sus funciones.

1.8.3 Aplicables a la administración de personal

La administración de personal requiere de criterios básicos para fijar técnicamente sus responsabilidades, para lo cual se aplicarán los siguientes principios de control interno:

a) Selección de personal hábil y capacitado

La aplicación de este principio permite que cada puesto de trabajo disponga del personal idóneo, seleccionado bajo criterios técnicos que se relacionen con su especialización, el

perfil del puesto y su respectiva jerarquía, así como dentro del marco legal correspondiente.

Las unidades administrativas encargadas de esta actividad, deberán coordinar con las unidades solicitantes, para que el proceso de selección sea el más adecuado a los intereses de la organización, ya que de esto depende la eficiencia que tengan las operaciones. Existen muchos casos, especialmente en el sector público, de personal que está mal ubicado o profesionales que no corresponden a la especialidad que se encuentran trabajando, lo cual disminuye la iniciativa y la producción de la organización.

En las empresas privadas, aunque no ocurre esto, si se dan casos de personal que ingresó con una especialización, pero que en el proceso encontraron otra inclinación y se especializaron, dejando de lado su formación inicial.

b) Capacitación continua

La aplicación de este principio permitirá que una organización o ente público, disponga de los recursos humanos capacitados para responder a las demandas del mercado, para lo cual la organización deberá programar la capacitación de su personal en los distintos campos y sistemas que funcionen en su interior, para fortalecer el conocimiento y garantizar eficiencia en los servicios que brinda.

Aunque las expectativas de un trabajador es capacitarse permanentemente, existen organizaciones que consideran que la capacitación es un gasto y no una inversión como es efectivamente, por lo que no disponen de planes de carrera que permitan capacitar a todo el personal en sus labores.

Las empresas y entes públicos deberán convertirse en administradoras de carreras, con lo cual sabrían a donde quieren llevar a su personal y en función de eso, planificar y ejecutar la capacitación para los distintos niveles en forma permanente; más aún, si tomamos en cuenta que el personal es uno de los activos de riesgo de la organización.

c) Vacaciones y rotación de personal

Desde el punto de vista humano y social, las vacaciones generan la recuperación de las energías perdidas durante el trabajo, por lo que la aplicación de este principio, es importante para que los trabajadores de los distintos niveles de la organización, convivan en armonía.

Las vacaciones y rotación de persona, generan la especialización de otro y motiva el descanso anual de aquellos que hacen uso de este derecho; además permite el descubrimiento de nuevas ideas de trabajo y eventuales malos manejos.

Todas las organizaciones o entes públicos, a través de las unidades administrativas respectivas, deben planificar anualmente el uso de vacaciones de todo su personal, así como el reemplazo temporal de cada uno de ellos, para evitar el entorpecimiento de las operaciones.

Esta práctica es muy beneficiosa para la organización, porque permite oxigenar algunos puestos de trabajo, principalmente aquellos que tienen relaciones con terceras personas que califican la eficiencia de la organización.

d) Cauciones (pólizas de seguro)

La aplicación de este principio, generalmente está en directa relación al riesgo que representa el trabajador para la organización en el sector que ha sido colocado, especialmente en las áreas que tienen que ver con el manejo y custodia de bienes y valores, donde es prudente promover el uso de cauciones o pólizas de seguro contra siniestros, de tal manera que se eviten pérdidas innecesarias, y se asegure la recuperación del bien.

Actualmente, existen muchas posibilidades, ya que las compañías de seguros ofrecen paquetes que hacen más baratas las posibilidades de asegurar los riesgos existentes; por

otro lado, no olvidemos que las organizaciones, al momento, casi no manejan dinero en efectivo, lo cual reduce los riesgo de pérdida o robo en este aspecto.[10]

1.9 Elementos del control interno

1.9.1 El ambiente de control

El entorno de control marca la pauta del funcionamiento de una empresa e influye en la concienciación de sus empleados respecto al control. Es la base de todos los demás componentes del control interno, aportando disciplina y estructura. Los factores del entorno de control incluyen la integridad, los valores éticos y la capacidad de los empleados de la empresa, la filosofía de dirección y el estilo de gestión, la manera en que la dirección asigna autoridad y las responsabilidades y organiza y desarrolla profesionalmente a sus empleados y la atención y orientación que proporciona al consejo de administración.

El núcleo de un negocio es su personal (sus atributos individuales, incluyendo la integridad, los valores éticos y el profesionalismo) y el entorno en que trabaja, los empleados son el motor que impulsa la entidad y los cimientos sobre los que descansa todo.

a) Integridad, ética y capacidad

El entorno de control está en función de la integridad y capacidad del personal de la organización. La eficiencia de los controles internos no puede ser mejor que la ética y los valores de los individuos que los crean, administran y supervisan.

La necesidad de constar con empleados capaces es evidente, especialmente en el entorno de las tecnologías de información. No se puede esperar que un personal con escasa formación o que sencillamente no sabe qué hacer en una crisis, apoye y promueva los controles, ya que estará demasiado ocupado tratando de hacer su trabajo.

---

[10] Fonseca Borja, Op. Cit., p. 122.

La dirección debe especificar el grado de capacidad que se requiere para desempeñar los distintos cargos y procurar los consiguientes conocimientos y habilidades mediante prácticas correctas de contratación, formación continua y otros esfuerzos de perfeccionamiento de los empleados.

b) Factores de evaluación

Los factores a considerar cuando se evalúan la integridad, los valores éticos y la capacidad de los empleados incluyen:

- **La existencia e implementación de códigos de conducta:** es preciso adoptar un código de conducta y otras políticas sobre las prácticas empresariales aceptables, sobre conflictos de intereses y sobre las normas éticas a observar, y comunicarlos a los empleados;

- **La presión para cumplir metas de eficacia poco realistas:** este factor puede crear problemas de control especialmente cuando la presión se relaciona con la obtención de resultados a corto plazo y cuando las retribuciones están basadas en alcanzar tales metas;

- **La descripción oficial de los puestos de trabajo:** u otras maneras de definir las tareas a realizar por quienes ocupan determinados puestos así como la comunicación de tales definiciones a los empleados, por ejemplo, especificando claramente quiénes tienen autoridad para dejar sin efectos determinados controles informáticos;

- **El análisis de los conocimientos y habilidades que se requieren para desempeñar adecuadamente los cargos:** esto tiene particular importancia en vista de la rapidez de los cambios que se producen actualmente en el entorno de las tecnologías de información, donde por ejemplo hay personas que utilizaban las antiguas tecnologías y los sistemas de construcción en COBOL estructurado y pueden no estar preparados para desarrollar una gran aplicación cliente / servidor;

- **Participación de la alta dirección:** el entorno de control también está en función de actuación y filosofía de la alta dirección, así como de la orientación que siguen el consejo de administración y la comisión de auditoría. En último término, el consejo de administración, el consejero delegado, o el propietario si se trata de una pequeña empresa, es el responsable general o titular del sistema de control; y

- **Responsabilidad:** el entorno de control depende en gran medida de que los empleados sepan que deberán responder por sus acciones. Las prácticas en materia de recursos humanos son como mensajes que se envían a los empleados sobre el grado de eficacia y la conducta que se espera de ellos.

Las políticas de formación a través de las cuales se les comunican los papeles y competencias en perspectivas, incluyendo prácticas tales como las clases de formación, seminarios, estudio de casos simulados, y ejercicios de representación de roles, comunican a los empleados cuáles son los niveles e eficacia y de conducta esperados. También se tiende a cada vez más a establecer una línea de comunicación directa u online para que los empleados informen sobre prácticas cuestionables sin sufrir las consecuencias.

Puede decirse que el entorno de control es el elemento más importante del proceso de control. El informe COSO indica que la responsabilidad por el entorno de control se extiende mucho más allá del control que pueden ejercer el director financiero o el auditor interno.

1.9.2 Valoración de riesgos

Las organizaciones, cualquiera sea su tamaño, se enfrentan a diversos riesgos de origen externos e internos que tienen que ser evaluados. Una condición previa a la evaluación del riesgo es la identificación de los objetivos a los distintos niveles, vinculados entre sí e internamente coherentes. La evaluación de los riesgos consiste en la identificación y el análisis de los riesgos relevantes para la consecución de los objetivos, y sirve de base para determinar cómo han de ser gestionados los riesgos. Debido a que las condiciones económicas, industriales, legislativas y operativas continuarán cambiando continuamente,

es necesario disponer de mecanismos para identificar y afrontar los riesgos asociados con el cambio.

La entidad debe conocer y abordar los riesgos con que se enfrenta, estableciendo mecanismos para identificar, analizar y tratar los riesgos correspondientes en las distintas áreas.

Aunque para crecer es necesario asumir riesgos prudentes, la dirección debe identificar y analizar riesgos, cuantificarlos, y prever la probabilidad de que ocurran así como las posibles consecuencias.
En las cambiantes circunstancias actuales hay que prestar especial atención a ciertas condiciones:

- Progresos tecnológicos en el proceso de producción o en los sistemas de información, como consecuencia de los cuales los controles dejan de ser adecuados para reducir los nuevos riesgos que suponen;

- Los cambios que se producen en el entorno operativo y pueden generar un nuevo entorno normativo o económico, aumentando la presión competitiva y creando nuevos riesgos para la empresa. Por ejemplo, las desinversiones y/o adquisiciones que realizan las empresas en el sector de las telecomunicaciones modifican sustancialmente su negocio;

- Nuevas líneas de negocio o nuevos productos, como consecuencia de los cuales los controles existentes dejan de reducir el riesgo de manera efectiva;

- La reestructuración de las empresas mediante el redimensionamiento a los ajustes de plantilla. Es un aspecto delicado ya que en el nuevo entorno existe la posibilidad de eliminar un puesto que desempeña una función clave de control sin instituir otro control en su lugar;

- La expansión o adquisición de explotaciones en el extranjero que implica nuevos riesgos tal vez no del todo conocidos pero que deben tomarse en cuenta. Por

ejemplo, el ambiente de control quizás responda a la cultura y las costumbres de la dirección local;

- Personal nuevo que puede no conocer la cultura de la empresa o puede atender más a los resultados que a las actividades de control. De no estar debidamente formada la gente nueva en una organización puede decidir llevar el negocio a su manera en lugar de hacerlo como lo exige el nuevo entorno en que actúa; y

- Crecimiento rápido cuando se produce una significativa expansión en la actividad, los sistemas existentes se ven sometidos a presiones que pueden producir fallos en los controles.

Debido a la naturaleza dinámica de tales factores, la evaluación del riesgo no es una tarea a cumplir de una vez para siempre. Debe ser un proceso continuo, una actividad básica de la organización, como la evaluación continua de la utilización de los sistemas de información o la mejora continua de los procesos.

Los procesos de evaluación del riesgo deben estar orientados al futuro, permitiendo a la dirección anticipar los nuevos riesgos y adoptar las medidas oportunas. Algunas empresas han creado comités de riesgo para analizar todos los nuevos productos en desarrollo y estudiar los riesgos que suponen para la empresa. Lo importante no es utilizar determinada metodología de evaluación del riesgo sino convertir la evaluación del riesgo en parte natural del proceso de planificación de la empresa.

1.9.3 Actividades de control

Las actividades de control son las políticas y los procedimientos que ayudan a asegurar que se lleven a cabo las instrucciones de la dirección de la empresa. Ayudan a asegurar que se tomen las medidas necesarias para controlar los riesgos relacionados con la consecución de los objetivos de la empresa. Hay actividades de control en toda la organización, a todos los niveles y en todas las funciones.

Deben establecerse y ajustarse políticas y procedimientos que ayuden a conseguir una seguridad razonable de que se llevan a cabo en forma eficaz las acciones consideradas

necesarias para afrontar los riesgos que existen respecto a la consecución de los objetivos de la unidad.

Las actividades de control existen a través de toda la organización y se dan en toda la organización, a todos los niveles y en todas las funciones, e incluyen cosas tales como; aprobaciones, autorizaciones, verificaciones, conciliaciones, análisis de la eficacia operativa, seguridad de los activos, y segregación de funciones.

En algunos entornos, las actividades de control se clasifican en; controles preventivos, controles de detección, controles correctivos, controles manuales o de usuario, controles informáticos o de tecnología de información, y controles de la dirección. Independientemente de la clasificación que se adopte, las actividades de control deben ser adecuadas para los riesgos.

Hay muchas posibilidades diferentes en lo relativo a actividades concretas de control, lo importante es que se combinen para formar una estructura coherente de control global. Los controles físicos garantizan que el equipo informático, inventarios, títulos de valores, dinero en efectivo y otros activos están físicamente protegidos y que periódicamente se rindan cuentas de los mismos y se concilian con los importes que aparecen en los registros de control.

Las actividades de control de alto nivel de la dirección a menudo consisten en el estudio de informes y otras informaciones, y pueden incluir; análisis de gastos reales versus gastos presupuestarios y rastreo de iniciativas importantes tales como el desarrollo de sistemas.

La gestión de actividades se refiere generalmente al estudio por parte de la dirección de informes relativos a la eficacia, tales como; productividad, flujo de caja diario, y cumplimiento con la normativa. Los indicadores de la eficacia se refieren a datos que se utilizan para comunicar información financiera y operativas clave que se analiza con el objeto de identificar áreas en las cuales hay peligro de no alcanzar los objetivos.

Las empresas pueden llegar a padecer un exceso de controles hasta el punto que las actividades de control les impidan operar de manera eficiente, lo que disminuye la calidad

del sistema de control. Por ejemplo, un proceso de aprobación que requiera firmas diferentes puede no ser tan eficaz como un proceso que requiera una o dos formas autorizadas de funcionarios componentes que realmente verifiquen lo que están aprobando antes de estampar su firma. Un gran número de actividades de control o de personas que participan en ellas no asegura necesariamente la calidad del sistema de control.

1.9.4 Información y comunicación

Hay que identificar, recopilar y comunicar información pertinente en forma y plazo que permitan cumplir a cada empleado con sus responsabilidades. Los sistemas informáticos producen informes que contienen información operativa, financiera y datos sobre el cumplimiento de las normas que permite dirigir y controlar el negocio de forma adecuada.

Dichos sistemas no sólo manejan datos generados internamente, sino también información sobre acontecimientos internos, actividades y condiciones relevantes para la toma de decisiones de gestión así como para la presentación de información a terceros. También debe haber una comunicación eficaz en un sentido más amplio, que fluya en todas las direcciones a través de todos los ámbitos de la organización, de arriba hacia abajo y a la inversa.

El mensaje por parte de la alta dirección a todo el personal ha de ser claro; las responsabilidades del control han de tomarse en serio. Los empleados tienen que comprender cual es el papel en el sistema de control interno y como las actividades individuales estén relacionadas con el trabajo de los demás. Por otra parte, han de tener medios para comunicar la información significativa a los niveles superiores. Asimismo, tiene que haber una comunicación eficaz con terceros, como clientes, proveedores, organismos de control y accionistas.

Las mencionadas actividades están rodeadas de sistemas de información y comunicación. Éstos permiten que el personal de la entidad capte e intercambie la información requerida para desarrollar, gestionar y controlar sus operaciones.

a) Sistemas de información

En la actualidad nadie concibe la gestión de una empresa sin sistemas de información. La tecnología de información se ha convertido en algo tan corriente que se da por descontada. En muchas organizaciones los directores se quejan de que los voluminosos informes que reciben les exigen revisar demasiados datos para extraer la información pertinente. En tales casos puede haber comunicación pero la información está presentada de una forma que la gente no la puede utilizar o no utiliza real y efectivamente.

Para ser verdaderamente efectiva la tecnología de información debe estar integrada en las operaciones de manera que soporte estrategias proactivas en lugar de reactivas. Los sistemas de tecnología de información aseguran el control a través de cosas tales como comprobación de edición y otros procedimientos programados que regularmente generan informes sobre excepciones que pueden utilizarse para conocer y evaluar mejor el riesgo. Sin embargo, los sistemas de información no son suficientes para que una organización se comunique bien.

b) Conocimiento de los controles por parte del personal

Todo el personal, especialmente el que cumple importantes funciones operativas o financieras, debe recibir y entender el mensaje de la alta dirección, de que las obligaciones en materia de control deben tomare en serio. Asimismo debe conocer su propio papel en el sistema de control interno, así como la forma en que sus actividades individuales se relacionan con el trabajo de los demás.

Si no se conoce el sistema de control, los cometidos específicos y las obligaciones en el sistema, es probable que surjan problemas. Los empleados también deben conocer cómo sus actividades se relacionan con el trabajo de los demás.

c) Comunicación efectiva

Debe existir una comunicación efectiva a través de toda la organización. El libre flujo de ideas y el intercambio de información son vitales. La comunicación en sentido ascendente

es con frecuencia la más difícil, especialmente en las organizaciones grandes. Sin embargo, es evidente la importancia que tiene.

Los empleados que trabajan en la primera línea cumpliendo delicadas funciones operativas e interactúan directamente con el público y las autoridades, son a menudo los mejor situados para reconocer y comunicar los problemas a medida que surgen.

El fomentar un ambiente adecuado para promover una comunicación abierta y efectiva está fuera del alcance de los manuales de políticas y procedimientos. Depende del ambiente que reina en la organización y del tono que da la alta dirección.

Los empleados deben saber que sus superiores desean enterarse de los problemas, y que no se limitarán a apoyar la idea y después adoptarán medidas contra los empleados que saquen a luz cosas negativas. En empresas o departamentos mal gestionados se busca la correspondiente información pero no se adoptan medidas y la persona que proporciona la información puede sufrir las consecuencias.

d) Comunicación exterior

Además de la comunicación interna debe existir una comunicación efectiva con entidades externas tales como accionistas, autoridades, proveedores y clientes. Ello contribuye a que las entidades correspondientes comprendan lo que ocurre dentro de la organización y se mantengan bien informadas.

Información comunicada por entidades externas; por otra parte, la información comunicada por entidades externas a menudo contiene datos importantes sobre el sistema de control interno.

Los auditores externos y las autoridades tienen una perspectiva más amplia cuando se trata de analizar los controles de una empresa. Pueden proporcionar a la alta dirección, al consejo de administración y a la comisión de auditoría, información importante sobre las deficiencias del sistema de control, y formular recomendaciones para corregirlas.

1.9.5 Supervisión

Los sistemas de control interno requieren supervisión, es decir, un proceso que comprueba que se mantiene el adecuado funcionamiento del sistema a lo largo del tiempo. Esto se consigue mediante actividades de supervisión continuada, evaluaciones periódicas o una combinación de ambas cosas. La supervisión continuada se da en el transcurso de las operaciones. Incluye tanto las actividades normales de dirección y supervisión, como otras actividades llevadas a cabo por el personal en la realización de sus funciones. El alcance y la frecuencia de las evaluaciones periódicas dependerán esencialmente de una evaluación de los riesgos y de la eficacia de los procesos de supervisión continuada. Las deficiencias detectadas en el control interno deberán ser notificadas a niveles superiores, mientras que la alta dirección y el consejo de administración deberán ser informados de los aspectos significativos observados.

Todo el proceso debe ser supervisado, introduciéndose las modificaciones pertinentes cuando se estime necesario. De esta forma el sistema puede reaccionar ágilmente y cambiar de acuerdo a las circunstancias.

Es preciso supervisar continuamente los controles internos para asegurarse de que el proceso funciona según lo previsto. Esto es muy importante porque a medida que cambian los factores internos y externos, controles que una vez resultaron idóneos y efectivos pueden dejar de ser adecuados y de dar a la dirección la razonable seguridad que ofrecían antes.

a) Alcance y frecuencia de las tareas de supervisión

El alcance y frecuencia de las actividades de supervisión dependen de los riesgos a controlar y del grado de confianza que inspira a la dirección el proceso de control. La supervisión de los controles internos puede realizarse mediante actividades continuas incorporadas a los procesos empresariales y mediante evaluaciones separadas por parte de la dirección, de la función de auditoría interna o de personas independientes. Las actividades de supervisión continua destinadas a comprobar la eficacia de los controles internos incluyen las actividades periódicas de dirección y supervisión, comparaciones, conciliaciones, y otras acciones de rutina.

b) Supervisión por personas independientes

Las comunicaciones procedentes de personas independientes también sirven como medios de control. Asimismo, las actividades organizativas y de supervisión permiten supervisar las funciones de control e identificar deficiencias. Los auditores internos y externos, en cierta medida y según la misión que se les ha asignado o los objetivos de la auditoría, examinan la estructura de control y formulan recomendaciones para reforzar los controles.

Estos componentes, vinculados entre sí, generan una sinergia y forman un sistema integrado que responde de una manera dinámica a las circunstancias cambiantes del entorno. El sistema de control interno está entrelazado con las actividades operativas de la entidad y existe por razones empresariales fundamentales. El sistema de control interno es más efectivo cuando los controles se incorporan en la infraestructura de la sociedad y forman parte de la esencia de la empresa.

Mediante los controles incorporados, se fomenta la calidad y las iniciativas de la delegación de poderes, se evitan gastos innecesarios y se permite una respuesta rápida ante las circunstancias cambiantes.[11]

1.10 Roles y responsabilidades

El control interno es ejecutado por un número de partes, cada una con responsabilidades importantes. El consejo directivo (directamente o a través de sus comités), la administración, los auditores internos y otro personal hacen contribuciones importantes para un sistema de control interno efectivo. Otras partes, tales como los auditores externos y los cuerpos reguladores, algunas veces están asociados con el control interno. Existe una distinción entre aquellos que son parte del sistema de control interno de una entidad y aquellos que no lo son, pero cuyas acciones sin embargo pueden afectar el sistema o ayudar a conseguir los objetivos de la entidad.

---

[11] Vilches Troncoso, Op. Cit., p. 22.

1.10.1 Partes responsables

Cada individuo en una entidad desempeña algún papel en la ejecución del control interno. Los roles varían en responsabilidad e involucramiento. Abajo se discuten los papeles y las responsabilidades de la administración, el consejo de directores, los auditores internos y otro personal.

a) Administración

La administración es responsable directa de todas las actividades de una entidad, incluyendo su sistema de control interno. Naturalmente, la administración en los diferentes niveles en una entidad tendrá diferentes responsabilidades de control interno. Tales responsabilidades diferirán, a menudo considerablemente, dependiendo de las características de la entidad.

En cualquier organización, el más fuerte se detiene ante el director ejecutivo. El tiene la responsabilidad última del manejo del control interno. Uno de los aspectos más importantes de su responsabilidad es asegurar la existencia de un ambiente de control positivo. Más que cualquier otro individuo o función, el director ejecutivo da el tono por lo alto que afecta los factores ambientales de control y los otros componentes del control interno.

b) Directivos financieros

Para el monitoreo son de particular importancia los ejecutivos financieros y de control y su personal vinculado, cuyas actividades cubren lo ancho, hacia arriba y hacia abajo, las unidades de operación y las otras en una empresa. Esos ejecutivos financieros a menudo están implicados en el desarrollo de los presupuestos y planes globales de la entidad. Siguen la pista y analizan el desempeño, desde las perspectivas de operaciones y de cumplimiento, lo mismo que desde el punto de vista financiero. Esas actividades usualmente hacen parte de una organización central o corporativa de una entidad, pero comúnmente también tienen una responsabilidad de línea punteada para monitorear las actividades de división, subsidiaria u otra unidad. Por lo tanto, el directivo financiero jefe,

el directivo de contabilidad jefe, el contralor y otros en la función financiera de una entidad son fundamentales para la manera administrativa de ejercer control.

Cuando se miran los componentes del control interno, es claro que el director financiero (de contabilidad) jefe y su personal de planta desempeñan roles críticos. Esa persona debe ser un jugador claro cuando se establecen los objetivos de la entidad y cuando se estudian las estrategias, se analizan los riesgos y se toman decisiones sobre cómo se administrarán los cambios que afectan a la entidad. Proporciona valiosos datos de entrada y dirección, y está posicionado para centrarse en el monitoreo y en el seguimiento de las acciones decididas.

c) Consejo de directores

La administración es responsable ante el consejo directivo o patronato, el cual gobierna, orienta y supervisa. Seleccionando la administración, el consejo tiene un rol principal definiendo que espera en integridad y valores éticos, y puede confirmar sus expectativas mediante sus actividades de supervisión. De manera similar, reservándose autoridad en ciertas decisiones claves, el consejo puede jugar un papel en definir los objetivos de alto nivel y en la planeación estratégica, y con la supervisión que provee, está implicado profundamente en el control interno.

Los miembros de un consejo efectivo son objetivos, capaces e inquisitivos. Tienen un esforzado conocimiento de las actividades y del ambiente de la entidad, y gastan el tiempo necesario para cumplir sus responsabilidades como consejo. Pueden emplear los recursos necesarios para investigar cualquier asunto que consideren importante, y tienen un canal de comunicaciones abierto y sin restricciones con todo el personal de la entidad, incluyendo los auditores internos, con los auditores externos y los asesores legales.

Muchos consejos de directores cumplen sus responsabilidades mediante comités. Su uso y centros de atención varían de una entidad a otra, en general incluyen auditoría, compensación, finanzas, nombramientos y beneficios para los empleados. Cada comité puede dar énfasis específico a ciertos componentes del control interno.

d) Auditores internos

Los auditores internos examinan directamente los controles internos y recomiendan mejoramientos. Los estándares establecidos por el Instituto de Auditores Internos especifican que el alcance de la auditoría interna debe cubrir el examen, la evaluación adecuada y la efectividad del sistema de control interno de la organización y la calidad del desempeño en la realización de las responsabilidades asignadas. Los estándares establecen que los auditores internos deben:

- Revisar la confiabilidad y la integridad de la información financiera y operativa y de los medios empleados para identificar, medir, clasificar, y reportar tal información;

- Revisar los sistemas establecidos para asegurar el cumplimiento de aquellas políticas, planes, procedimientos, leyes y regulaciones que puedan tener un impacto significativo en las operaciones y reportes y deben determinar si la organización los está cumpliendo;

- Revisar los medios de salvaguardia de activos y, cuando sea apropiado, verificar la existencia de tales activos;

- Valuar la economía y la eficiencia con la cual se emplean los recursos; y

- Revisar las operaciones o programas para indagar si los resultados son consistentes con los objetivos y las metas establecidas y si las operaciones o programas se están llevando a cabo como fueron planeados.

Todas las actividades de una organización están potencialmente dentro del alcance de la responsabilidad de los auditores internos. En algunas entidades, la función de auditoría interna está altamente implicada con los controles sobre las operaciones. Por ejemplo, los auditores internos pueden monitorear periódicamente la calidad de la producción, probar la oportunidad de los despachos a clientes o evaluar la eficiencia de la estructura de la planta. En otras entidades, la función de auditoría interna se puede centrar principalmente en el cumplimiento o en las actividades relacionadas con la información financiera.

e) Otro personal de la entidad

El control interno es, en algún grado, responsabilidad de cada persona en una entidad y por consiguiente debe ser parte explícita o implícita de la descripción del trabajo de cada uno. Esto es cierto desde dos perspectivas.

Primero, virtualmente todos los empleados desempeñan algún rol en la labor de control. Pueden producir información usada en el sistema de control interno – por ejemplo, registro de inventario, procesamiento de datos laborales, de ventas o registros de gastos – o realizar otras acciones necesarias para efectuar control. Esas acciones pueden incluir la realización de conciliaciones, seguimiento de reportes de excepciones, desarrollo de inspecciones físicas o investigación de las razones de las variaciones de costos u otros indicadores de desempeño. El cuidado con el que se desempeñan esas actividades afecta directamente la efectividad del sistema de control interno.

Segundo, todo el personal debe ser responsable por la comunicación de los problemas en operaciones a un nivel organizacional más alto, el no cumplimiento del código de conducta, u otras violaciones de políticas o acciones ilegales. El control interno se apoya en verificaciones y balances, incluyendo la segregación de deberes, y en empleados que no miran la otra forma. El personal debe comprender la necesidad de resistir a las presiones de sus superiores para participar en actividades impropias, y deben estar disponibles canales exteriores de información normal para permitir reportar tales circunstancias.

El control interno está en los negocios de cada uno, y deben estar bien definidos y efectivamente comunicados los roles y las responsabilidades de todo el persona.

1.10.2 Partes externas

Diversas partes externas pueden contribuir a la consecución de los objetivos de la entidad, algunas veces mediante acciones paralelas a las que realiza. En otros casos, las partes externas pueden aportar información útil para la entidad en sus actividades de control interno.

a) Auditores externos

Quizás ninguna otra parte externa desempeña un rol tan importante para la consecución de los objetivos de información financiera de la entidad como los contadores públicos certificados independientes. Ellos dan a la administración y al consejo de directores un punto de vista singular independiente y objetivo; contribuyen en una entidad a la consecución de sus objetivos de información financiera, así como a otros objetivos.

En conexión con una auditoría de estados financieros, el auditor expresa una opinión sobre la transparencia de los estados financieros de conformidad con los principios de contabilidad generalmente aceptados, y de esa manera contribuye a los objetivos de información financiera de la entidad. Puesto que el sistema de control interno de una entidad puede proporcionar un grado de seguridad mirando la presentación razonable de los estados financieros, el auditor ofrece la seguridad a un nivel más alto. El auditor, además, proporciona información útil para la administración en la conducción de sus responsabilidades de control.

Un auditor debe obtener conocimiento suficiente del sistema de control interno de una entidad en orden a planear la auditoría. La extensión de la atención dada al control interno varía de auditoría a auditoría. En algunos casos, se presta considerable atención, y en otros, basta una relativa poca atención. Pero en el primer caso, un auditor usualmente no podría estar en posición de identificar todas las debilidades de control interno que puedan existir.

En la mayoría de los casos, los auditores que conducen una auditoría de estados financieros, de hecho, proporcionan información útil para la administración en el desempeño de sus responsabilidades relacionadas con el control interno:

- Comunicando hallazgos de auditoría, información analítica y recomendaciones para uso en la torna de acciones necesarias para conseguir los objetivos establecidos; y

- Comunicando hallazgos mirando las deficiencias en el control interno que demandan su atención, y haciendo recomendaciones para su mejoramiento.

Esta información frecuentemente se relacionará no solamente con la información financiera sino también con las operaciones y las actividades de cumplimiento, y pueden hacer contribuciones importantes para que una entidad consiga sus objetivos en cada una de esas áreas. La información es reportada a la administración y, dependiendo de su significado, al consejo de directores o al comité de auditoría.

b) Legisladores y reguladores

Legisladores y reguladores afectan los sistemas de control interno en muchas entidades, ya mediante los requerimientos para establecer controles internos o ya mediante el examen de entidades particulares. Muchas de las leyes y regulaciones relevantes tratan solamente con controles financieros sobre los informes financieros, si bien algunos, particularmente aquellos que aplican a las organizaciones gubernamentales, pueden relacionarse con objetivos de operaciones y de cumplimiento.

Así, legisladores y reguladores afectan de dos maneras distintas los sistemas de control interno de las entidades. Establecen reglas para que la administración asegure
que los sistemas de control interno reúnen los requerimientos estatutarios y reguladores mínimos. Y, de acuerdo con el examen de una entidad particular, proporcionan información que usa el sistema de control interno de la entidad, y proporcionan recomendaciones y algunas directivas para la administración mirando los mejoramientos que requiere el sistema de control interno.

c) Partes que interactúan con la entidad

Clientes, vendedores y otros que realizan transacciones de negocio con una entidad constituyen una fuente importante de información que se usa para conducir las actividades de control:

Un cliente, por ejemplo, informa a la compañía sobre demoras en los despachos, calidad inferior de los productos o fallas para satisfacer las necesidades de los clientes por productos o servicios. O, un cliente puede ser más proactivo y trabajar con una entidad desarrollando el engrandecimiento de los productos que lo requieran.

Un vendedor proporciona relaciones o información mirando los despachos y la facturación completados o abiertos, los cuales se usan para identificar y corregir discrepancias y balances de conciliación.

Un proveedor potencial notifica a la alta administración sobre la solicitud de un empleado por un retorno.

Esas partes proporcionan información que, en algunos casos, puede ser extremadamente importante para una entidad en la consecución de sus objetivos de operación, información financiera y de cumplimiento. La entidad debe tener mecanismos mediante los cuales recibe tal información y así tomar las acciones adecuadas. Las acciones adecuadas incluirán no solamente la orientación de la situación particular reportada, sino también investigar la fuente subyacente del problema y remediarlo.

Además de los clientes y vendedores, otros agentes, tales como acreedores, pueden proporcionar supervisión mirando la consecución de los objetivos de una entidad. Un banco, por ejemplo, puede requerir informes sobre el cumplimiento de una entidad con relación a ciertos convenios de deuda, y recomendar indicadores de desempeño u otros objetivos o metas deseados.

d) Analistas financieros, agencias de clasificación de obligaciones y medios de comunicación

Los analistas financieros y las agencias de clasificación de obligaciones consideran muchos factores relevantes para la estimación del valor de una entidad para una inversión. Ellos analizan los objetivos y las estrategias de la administración, los estados financieros históricos y la información financiera prospectiva, las acciones que se toman en respuesta a las condiciones en la economía y en el mercado, el éxito potencial en el corto y en el largo plazo, y el desempeño de la industria y la comparación con grupos similares. Los medios de comunicación escritos y hablados, particularmente los periodistas financieros, también pueden realizar al mismo tiempo análisis similares.

Las actividades investigativas y de monitoreo de esas partes pueden proporcionar señales a la administración sobre cómo otras partes perciben el desempeño de la entidad, los

riesgos industriales y económicos que enfrenta la entidad, las estrategias operativas o financieras que pueden mejorar el desempeño, y las tendencias industriales. Esta información algunas veces es proporcionada directamente en reuniones cara a cara entre las partes y la administración, o indirectamente mediante análisis para inversionistas, inversionistas potenciales y el público. En cada caso, la administración debe considerar las observaciones y las señales de los analistas financieros, de las agencias de clasificación de obligaciones y de los medios de comunicación que puedan engrandecer el control interno.[12]

[12] Mantilla B., Op. Cit., p. 101.

CAPÍTULO II
LA AUDITORÍA INTERNA

2.1 Definición

La auditoría interna es como una parte del sistema de control interno que funciona al revisar y evaluar los controles internos establecidos por otros, asesorar y señalar deficiencias y presentar recomendaciones de mejoras; se define como "una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización.

Ayuda a una organización a cumplir sus objetivos apartando un enfoque sistemático y disciplinado para evaluar y mejorar la afectividad de los procesos de gestión, control y dirección.

Es una herramienta gerencia que evalúa los demás controles como ayuda a todos los niveles ejecutivos, para mejorar constantemente la gestión y contribuir a la transparencia de las operaciones, procesos y sistemas de la organización".[13]

2.2 Objetivo y alcance

La auditoría interna surge por la necesidad de mantener un control permanente y más eficaz dentro de la organización; el objetivo principal es "asistir a todos los miembros de la administración en el descargo de sus responsabilidades, suministrándoles análisis, evaluaciones y los comentarios pertinentes con respecto a las actividades bajo revisión, acompañado de recomendaciones positivas, que ayuden a mejorar la gestión de la organización.

La auditoría interna abarca todas las operaciones, procesos y sistemas o cualquier aspecto de las actividades organizacionales donde pueda ser útil a la administración.

---

13 Fonseca Borja, Op. Cit., p. 73.

El enfoque de trabajo dentro de este campo de acción requiere que su trabajo vaya más allá de la simple revisión de las transacciones financieras y los registros contables, para tener una compresión global de las operaciones bajo revisión, que se sinterizan en las actividades siguientes:

- Evaluar el contexto institucional, buscando los sectores, sistemas, proceso, operaciones y resultados, donde la auditoría interna identifique que se puede agregar valor;

- Evaluar el ambiente y estructura de control interno, así como la eficacia y aplicación de los controles, financieros y otros de operación, y la implantación de un control efectivo a costo razonable;

- Evaluar la tecnología y su ambiente para verificar si existen las políticas, los procedimientos y mecanismos que aseguren la sostenibilidad de los mismos;

- Evaluar los programas de capacitación para determinar si esto contribuye a los intereses y desarrollo organizacional;

- Evaluar los mecanismos y procedimientos para la administración de riesgos, y las acciones para el control de los mismos;

- Velar por el grado de cumplimiento con las políticas, planes, programas, proyectos, actividades y demás procedimientos que hayan sido establecidos, dentro del marco legal correspondiente;

- Evaluar si los sistemas garantizan que los bienes y derechos de la organización sean contabilizados y protegidos adecuadamente contra pérdidas de cualquier clase;

- Evaluar si los mecanismos y medios de información garantizan la producción de información confiable y oportuna para la toma de decisiones gerenciales;

- Evaluar la calidad, eficiencia y economía en el cumplimiento de las responsabilidades asignadas; y

- Proponer y promover mejoras constantes a la organización, los sistemas, procesos y procedimientos a través de recomendaciones que proyecten una mejor imagen organizacional, así como los resultados esperados".[14]

2.3 Responsabilidad y autoridad

2.3.1 Responsabilidad

Las responsabilidades del auditor interno dentro de la organización son las siguientes:

- Evaluar el contexto de las operaciones y la organización, con el fin de buscar los niveles de riesgos y las posibilidades de agregar valor a la organización;

- Informar y asesorar a la administración y ejercer sus funciones en tal forma que cumpla con las Normas para el Ejercicio Profesional de la Auditoría Interna y las disposiciones del Código de Ética del Instituto de Auditores Internos; y

- Planificar y coordinar sus actividades con aquellas otras personas y unidades administrativas, de tal manera que permita lograr los objetivos de auditoría y los objetivos de la organización.

2.3.2 Autoridad

Ningún auditor interno, dentro de sus funciones, tiene responsabilidad directa ni autoridad sobre las actividades que revisa. Por lo tanto, la evaluación de la auditoría interna no exonera en forma alguna a otras personas dentro de la organización, de sus responsabilidades que les fueron asignadas.[15]

---

14 Ibid., p.73.
15 Ibid., p.74.

2.4 Independencia

Es fundamental que los miembros de la auditoría interna no tengan relaciones con la gerencia de personal, tampoco deberán tener relaciones comerciales con el ente para el cual trabajen y no deben existir lazos directos de familia entre los miembros de la auditoría y el personal a ser auditado. De esta forma se protege la total independencia de criterio y observación, evitando situaciones que tienden a distorsionar la información y proteger a personal del ente. “La independencia es esencial para la efectiva labor de auditoría interna; dicha independencia de acción se encuentra plasmada en su organización, en la objetividad de sus acciones y el respaldo de la gerencia, así como la colaboración del personal auditado:

- El respaldo de la gerencia y la organización operacional de la función de la auditoría interna, son aspectos de importancia que determinan su independencia, alcance de su trabajo, lo cual le permite agregar valor a los sectores evaluados;

- El jefe de la auditoría interna, por lo tanto, es responsable ante el máximo ejecutivo de la organización, cuya autoridad garantiza un alcance amplio de la labor de auditoría, así como la consideración apropiada y efectiva de medidas a tomar sobre los hallazgos y recomendaciones; y

- Para garantizar su independencia y objetividad, el auditor interno no deberá diseñar ni establecer procedimientos, ni preparar registros, ni comprometerse en ninguna otra actividad que normalmente revisaría y evaluaría y que razonablemente constituirá un límite de su libertad. Su objetividad no se verá afectada, sin embargo, por su determinación y recomendación de normas de control que serían aplicadas para la realización de los sistemas y procedimientos bajo su revisión.

La declaración de las responsabilidades del auditor interno, es un instrumentos útil puesto que no solo sirve de guía para determinar que es lo que debe hacer el auditor interno, sino también para evaluar el cumplimiento de sus responsabilidades por aquellos

aspectos que dejó de hacer, asunto que dada la importancia del caso, puede servir como parámetro para medir la eficiencia de la auditoría interna".[16]

2.5 Organización de la auditoría interna

El propósito, autoridad y responsabilidad del departamento de auditoría interna debe definirse en un documento formal por escrito, aprobado por la dirección y aceptado por el consejo; su existencia debe estar establecida "dentro de los estatutos de la entidad o empresa, bajo la denominación de servicios de aseguramiento en funciones y dependencia claramente indicados, en el caso del sector privado. En el sector oficial o público, deberá existir una ley específica que la determine, igualmente bajo funciones específicas y dependencia claramente identificadas, regularmente con dependencia directa al jefe de la dependencia pública.

2.5.1 Nivel jerárquico

La delegación de autoridad debe ser planteada en la escritura organizacional como una dependencia a nivel de staff o asesoría mínimo de la gerencia, idealmente de la junta directiva o consejo de administración con el propósito de que la auditoría interna sea ejercida de una manera totalmente independiente, profesional y que sus resultados sea para la empresa un valor agregado que represente un positivo costo-beneficio.

Los servicios aseguramiento de auditoría interna que sean contratados por el sistema de outsourcing (personal ajeno de la empresa) debe de estar claramente indicado en los estatutos de la entidad.

2.5.2 Profesionales capacitados

Los auditores internos, desde su ejecutivo jefe, deben ser profesionales capacitados y deben tener una aptitud imparcial y objetiva y evitar conflictos de intereses para proveer servicios de aseguramiento en auditoría interna y ejercer un debido cuidado desde la evaluación de riesgos, planeación y ejecución de una auditoría.

---

16 Ibid., p.75.

Si la independencia u objetividad se viese comprometida directa o en apariencia deberá darse a conocer con oportunidad a nivel jerárquico y esperar su pronunciamiento para desarrollar alguna labor comprometida con el impedimento o posible impedimento.

2.5.3 Supervisión y control de calidad

El ejecutivo jefe de auditoría interna debe ejercer una supervisión y asistencia permanente a sus subalternos bajo revisiones periódicas a los trabajos efectuados, desarrollar reuniones primarias de asesoramiento, impulsar cursos de capacitación, de lectura de libros de actualización que ayuden a un buen desarrollo del trabajo no rutinizados y bajo parámetros técnicos actualizados.

2.5.4 Riesgos, controles y fraudes

Dentro de los conocimientos a todo nivel dentro de la auditoría interna, se deben tener conocimientos, sin ser totalmente experto, de los riesgos y controles claves en la informática, pero si en las técnicas de la auditoría, que le permitan desarrollar una labor adecuada de control.

Se deben tener conocimientos en la identificación de fraudes y para ello debe existir una tabla identificadora de riesgos y fraudes, preparado de la experiencia de la empresa o de otras empresas, o bajo un adecuado bermachiting (experiencia de otras empresas).

Se debe estar alerta de los riesgos materiales que pudieren afectar los objetivos de control, las operaciones o los recursos, haciendo salvedad que el auditor interno no es infalible, pudiéndose escapar algunos riesgos o situaciones especiales de errores no intencionales o intencionales, por tanto deben considerarse aquellos que la experiencia le han indicado deben profundizarse en el presente y en el futuro.

2.5.5 Debido cuidado profesional

Los auditores internos deberán cumplir su trabajo con el cuidado y pericia que represente seguridad razonable, desarrollada con prudencia y competencia. Para ello, es importante considerar:

- El alcance necesario para alcanzar los objetivos del trabajo;

- La relativa complejidad, materialidad o significatividad de asuntos a los cuales se les aplica procedimientos de aseguramiento en auditoría interna;

- La adecuación y eficacia de los procesos de administración de riesgos empresariales ERM, controles y gobierno corporativo[17];

- La probabilidad de errores materiales, irregularidades e incumplimiento;

- El costo de aseguramiento de la auditoría en relación con los potenciales beneficios; y

- Las herramientas o apoyo logístico necesarios, como computadores PC o portátiles, impresoras, softwares propios y otras técnicas y bases de datos asistidas electrónicamente.

2.5.6 Planeación del trabajo de auditoría interna

La auditoría interna debe elaborar y registrar un plan para cada trabajo que incluya el alcance, los objetivos, y la asignación de recursos. Al planificar el trabajo la auditoría interna debe considerar:

- Los objetivos definidos en los estatutos o en la Ley para ser alcanzados por la auditoría interna;

- Los medios con los cuales cuenta la auditoría interna para controlar su desempeño;

[17] El gobierno corporativo es un sistema interno dentro de una empresa mediante el cual se establecen las directrices que deben regir su ejercicio, buscando, entre otro, transparencia, objetividad y equidad en el trato a los socios y 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 interno y externos, frente a los grupos de interés como: clientes, proveedores, competidores, empleados, terceros colocadores de recurso y hacia la comunidad en general.

- Los riesgos significativos, su impacto potencial y su evaluación para determinar de que se conservan a un nivel aceptable; y

- Análisis de los sistemas de administración de riesgos empresariales ERM con el propósito que se adecuen a niveles de eficacia comparados con modelos previstos, y también la de lograr mejoras a este sistema.

2.5.7 Objetivos, alcance y programa de trabajo de aseguramiento

Tomados con base en los objetivos generales, para cada trabajo de auditoría interna, ya sea de procesos, riesgos o controles, deberán establecerse objetivos específicos para cada área evaluada.

El alcance del trabajo debe ser suficiente y competente referido a cada objetivo general o específico dentro de los diferentes sistemas de información, registro, personal y propiedades físicas relevantes o cuantitativamente importantes, incluyendo las propiedades en su poder de terceros.

Para lograr los objetivos, se deben tener definidos los recursos físicos, de personal y logístico basado en una evaluación de la naturaleza y complejidad de cada tarea, las restricciones de tiempo y los recursos disponibles.

Para desarrollar e identificar los objetivos y su alcance, la auditoría interna deberá contar con programas en los cuales se establezcan los procedimientos para identificar, analizar, evaluar y registrar información de cada área evaluada dentro del proceso, riesgo y control. Los programas, antes de cada trabajo, deben ser revisados por el Jefe de la Auditoría Interna y adicionado o complementado para que “quede hecho a la medida”, según los parámetros de evaluación en esta clase de documentos en auditoría.

2.5.8 Cumplimiento de los objetivos

Se dijo que la auditoría interna debe identificar, analizar, evaluar y registrar suficiente información para que pueda desempeñar su trabajo adecuadamente y cumplir con sus objetivos determinados.

La información identificada y registrada en sus papeles de trabajo, debe ser suficiente, confiable, relevante y útil para ser analizada y evaluada, derivando conclusiones y así sus resultados sean considerados como beneficios reales de valor agregado para la administración en general.

2.5.9 Supervisión del trabajo en auditoría interna

Todos los trabajos realizados de servicio de aseguramiento en auditoría interna deberán ser supervisados para asegurar el logro de sus objetivos, la calidad del trabajo, y el desarrollo profesional del personal.

La supervisión debe incluir que se cumpla cabalmente con las funciones de evaluación de procesos, riesgos y controles internos, comprobando que ellos están dando seguridad razonable a los terceros interesados y en especial de que la auditoría interna se desempeña con bases en normas de auditoría y de ética de manera eficaz y eficiente, y que su trabajo agrega valor y mejoras a las operaciones de la empresa; incluyendo, entre otros, supervisión apropiada, evaluación interna periódica y monitoreo continuo del aseguramiento de calidad y mejora.

2.5.10 Comunicación de los resultados

Los informes a presentar sobre los resultados de la auditoría interna deben incluir los objetivos y el alcance del trabajo realizado, así como las conclusiones con sus recomendaciones y los planes de acción, ya sea de manera parcial o de manera específica o integral, según el plan y programa diseñado para el cumplimiento de los objetivos.

Los informes deben ser objetivos, precisos, claros, concisos, constructivos, completos y oportunos. Antes de enviar oficialmente un informe, es conveniente se envíe un borrador a los departamentos afectados con el propósito de aclarar suficientemente su contenido y tener base de seguridad, después de lograr su fin, se preparará el informe oficial y se entregará personalmente o en una reunión o foro especial, donde deben participar la alta gerencia y si es posible personal del comité de auditoría o gobierno corporativo.

En caso de errores y omisiones significativas del informe oficial ya presentado deben ser enviadas las correcciones a las mismas personas que recibieron el original. Como reglas fundamentales en la preparación definitiva de los informes, se deben tener en cuenta las siguientes:

- Evaluar el riesgo potencial para la organización;
- Consultar con la alta gerencia o consultor legal, según corresponda; y
- Controlar la difusión, restringiendo la utilización de los resultados.

2.5.11 Monitoreo y seguimiento

Como base fundamental del monitoreo, la auditoría interna en sus programas deberá contemplar la forma de lograr un proceso de seguimiento, para supervisar y asegurar que las acciones de la dirección hayan sido efectivamente implantadas o que la alta gerencia haya aceptado el riesgo de tomar acción de seguimiento, discutiendo aquellos riesgos residuales, dejando en claro la responsabilidad de la alta gerencia y solicitando que ellos sean informados a la junta directiva o consejo de administración.

2.5.12 Naturaleza del servicio de aseguramiento

Los fundamentos principales del aporte que debe dar la auditoría interna en la empresa se basa en la evaluación y contribución a la mejora de los procesos:

- Gestión de riesgos;
- Controles; y
- Gobierno corporativo.

Se deberán utilizar enfoques sistemáticos y disciplinados que sirvan para identificar y evaluar las situaciones significativas de los riesgos, y a la contribución de mejoras de los sistemas de gestión de riesgos, la de control.

Deben servir también, para asistir a la administración en el mantenimiento de controles efectivos, mediante la evaluación de eficacia y eficiencia para proveer mejoras continuas.

El gobierno corporativo, debe evaluar y hacer las recomendaciones apropiadas para mejorar el proceso del gobierno corporativo bajo el cumplimiento de los siguientes objetivos:

- Promover la ética y los valores apropiados dentro de la empresa;
- Asegurar la gestión y las responsabilidades eficaces en el desempeño de la empresa; y
- Comunicar eficazmente las actividades y la información de comunicación entre la junta directiva o consejo de administración de los auditores internos y externos con la alta gerencia.

2.5.13 Evaluaciones internas

Es compromiso de la auditoría interna, con el propósito de lograr programas de calidad, mejoras continuas y aprovechamientos de los resultados obtenidos y plasmados en sus informes, ejercer revisiones continuas y periódicas de su trabajo mediante autoevaluaciones o evaluaciones realizadas por terceros especializados.

Esa metodología debe asegurar que se sigan los procesos adoptados por la actividad de la auditoría interna según el plan anual de auditoría y revisión de procesos, bajo retroalimentación, presupuestos de proyectos, sistemas de control interno, ciclos transaccionales, recuperación de costos y de las diferentes recomendaciones dadas por la misma auditoría interna y de terceros especializados.

Deben establecerse conclusiones respecto de la calidad del desempeño continuo y tomarse acciones de seguimiento a fin de asegurar que se implementen las mejoras apropiadas. Se requieren también, de entrevistas y encuestas con los terceros interesados en la información presentada por la auditoría interna, como el del desempeño y la acción apropiada para lograr mejoras, contribución a la gestión de riesgos, al gobierno corporativo y a los procesos de control de la empresa, el cumplimiento de las leyes, reglamentaciones y normas gubernamentales o de la industria, así como la determinación de eficacia en las operaciones, mejores prácticas y real valor agregado".[18]

[18] Rodrigo Estupiñán Gaitán. Administración de Riesgos E.R.M. y la Auditoría Interna. (Bogotá: ECOE Ediciones, 2008), p. 19.

2.6 Prácticas del ERM en la auditoría interna

La nueva definición de la auditoría interna separada en los dos grandes servicios a prestar como son el de aseguramiento y consulta para agregar valor y mejorar las operaciones para evaluar y mejorar la eficacia de los procesos de la administración o gestión de riesgos, control y gobierno corporativo. Dentro de las normas de auditoría interna internacionales, se encuentran varias normas específicas dirigidas a manejar la metodología de la administración de riesgos dentro de los dos servicios enunciados, las cuales se recomiendan se apliquen por parte de los auditores internos, para cada caso los siguientes:

CUADRO No. 1: NORMAS INTERNACIONALES PARA EL EJERCICIO PROFESIONAL DE LA AUDITORÍA INTERNA

SERVICIO DE ASEGURAMIENTO	SERVICIO DE CONSULTORÍA
Deben tener conocimiento de los riesgos y controles informáticos claves sin ser un experto en riesgos e informática. (1210 A-3)	La aceptación de trabajos de consultoría, debe hacerse basado en el potencial para mejorar la gestión de riesgos, añadir valor y eficacia en las operaciones. (2010 C-1)
Debe tener suficientes conocimientos para identificar los indicadores de fraude sin ser su principal función la detección e investigación. (1210 A-2)	Durante los trabajos de consultoría, deben considerar el riesgo compatible con los objetivos del trabajo y estar alertas a la existencia de otros riesgos significativos. (2110 C-1)
Deben ejercer el debido cuidado profesional al considerar la adecuación y eficacia de los procesos de gestión de riesgos, control y gobierno. (1220 A-1)	Deben aplicar conocimientos de riesgos y controles obtenidos de los trabajos de consultoría en el proceso de identificación y evaluación de riesgos significativos. (2110 y 2120 C-2)
Debe estar alerta en identificar los riesgos materiales que pudieran afectar los objetivos, las operaciones y los recursos. (1220 A-3)	Los objetivos de los trabajos deben considerar los procesos de riesgos, control y gobierno, hasta el grado de extensión acordado con el cliente. (2210 C-1)
El plan de trabajo debe estar basado en una evaluación de riesgos efectuada anualmente (2010 A-1), y, la de efectuar una evaluación preliminar de los riesgos.	Durante los trabajos pueden ser identificados cuestiones referidas a gestión de riesgos, control y gobierno (2440 C-2)
Debe supervisar y evaluar la adecuación y eficacia del Sistema de Administración de Riesgos ERM, como las de gobierno corporativo, controles, operaciones y los sistemas de información. (2110 A-1 y 2 y 2120 A-1)	Cuando sean significativos los riesgos deben ser comunicados oportunamente a la Alta Gerencia o al Consejo de Administración o Junta Directiva. (2440 C-2)
Antes de enviar los resultados a partes externas de la empresa se debe evaluar el riesgo potencial. (2440 A-2)	
Finalmente se debe establecer un proceso de seguimiento para supervisar y asegurar que las acciones de la dirección hayan sido implementadas o la posibilidad de que la Alta Gerencia haya aceptado el riesgo de no tomar acciones. (2550 A-1)	

Fuente: Rodrigo Estupiñán Gaitán, Administración de Riesgos E.R.M. y la Auditoría Interna. (Bogotá: ECOE Ediciones, 2008), p. 198.

2.6.1 Plan de auditoría referidos al riesgo

Dentro de varios consejos para la práctica de auditoría interna formulados por las normas de auditoría interna internacionales relacionados con la Administración de Riesgos (ERM), se presentan a continuación varios que sirven de fundamentos para lograr un adecuado enlace dentro de un plan de auditoría con la Administración del Riesgo (ERM):

- El plan de trabajo de la actividad de auditoría interna debe estar basado en una evaluación de riesgos y exposiciones que puedan afectar el ente económico;

- El universo de auditoría puede incluir componentes del plan estratégico;

- El calendario de trabajo de auditoría debe estar basado, entre otros factores, en las prioridades de una evaluación de riesgos, tales como: materialidad, liquidez de activos, competencia de la gerencia, calidad de los controles internos, grado de cambio o estabilidad, tiempo transcurrido desde la última auditoría, complejidad, relaciones del personal y gubernamentales, etc.;

- Los cambios en la dirección de la gestión, objetivos, énfasis y enfoques, deben reflejarse en las actualizaciones del universo de auditoría y el plan de trabajo relacionado;

- Al llevar a cabo trabajos de auditoría interna, los métodos y técnicas de pruebas y validaciones deben reflejar la materialidad del riesgo y la probabilidad de ocurrencia;

- La información y comunicación a la alta gerencia deben transmitir conclusiones de gestión de riesgos y recomendaciones para reducirlos o contrarrestarlos; y

- El jefe de auditoría interna debe preparar un estado de la adecuación de los controles internos para mitigar los riesgos, al menos una vez al año.

2.6.2 Informe de auditoría interna sobre la administración de riesgos (ERM)

Las observaciones significativas surgidas del trabajo son aquellas situaciones que, a juicio del jefe de auditoría interna pueden afectar adversamente al ente económico, los cuales pueden referirse a irregularidades, actos ilegales, errores, ineficiencias, desperdicios, ineficacias, conflictos de intereses, y debilidades de control, resaltando aquellos ya enunciados y que no han sido corregidos.

Así mismo, incluirse observaciones y recomendaciones significativas, aclarando que es responsabilidad de la administración en general, la de tomar decisiones sobre las medidas apropiadas a adoptar. La alta gerencia puede tomar el riesgo de no corregirse debido a su costo u otras consideraciones, siendo su responsabilidad o la de no asumir medidas de monitoreo para erradicarlas.

La elaboración e informes sobre los procesos de administración o gestión de riesgos es de alta prioridad para la auditoría interna, separándolas con la necesidad de que se utilicen análisis de riesgos para planificar sus auditorías.

2.6.3 El rol del auditor interno en el proceso de la administración de riesgos empresariales (ERM)

La administración del riesgo empresarial ERM es una responsabilidad clave de la junta directiva o consejo de administración como de la alta gerencia, para lo cual deben asegurarse de que existan y funcionen procesos de gestión de riesgos sólidos, apropiados y eficaces. Esta función puede ser ejercida por un comité de auditoría con dirección directa de miembros de la junta directiva o consejo de administración, colaborándose mediante el examen, evaluación, informe y recomendaciones de mejoras sobre la adecuación y eficacia de los procesos del ERM. A su vez, el auditor interno cumpliendo un rol de consultor puede ayudar a la organización a identificar, evaluar e implementar metodologías de administración de riesgos empresariales ERM e implementar controles adecuados.

El auditor interno debe obtener un entendimiento de las expectativas o del “apetito al riesgo” en general de la empresa, coordinando entre los distintos grupos y personas que

tengan un rol en ese proceso, en cuanto a las responsabilidades y actividades relacionadas con el riesgo, las cuales deben estar establecidas en los planes estratégicos o políticas de la empresa.

Si en una organización aún no ha establecido un proceso de administración del riesgo ERM, el auditor interno tiene la obligación de presentar un informe especial para que se establezca dicho proceso, indicando claramente la importancia y beneficios que existen para la empresa. Llegado el caso, de que le soliciten a la auditoría interna su establecimiento dentro de un rol proactivo, es importante aclararle a toda la administración en general, que la junta directiva o consejo de administración es el "propietario de los riesgos" y por ende responsables de identificar, mitigar y vigilar los diferentes riesgos.

2.6.4 Identificación y cuantificación de riesgos

En las organizaciones existen eventos de amenaza, que podrían ocurrir y afectaran de manera adversa la capacidad de la empresa y no se lograran todos sus objetivos y no se ejecutaran sus estrategias, para los cuales necesitaríamos evaluar el posible impacto financiero si sucediera [valor simple de exposición de pérdida] o ¿con que frecuencia podría ocurrir? [frecuencia] o probabilidad que suceda una causa cualesquiera [incertidumbre], así que también que podría hacerse para prevenir, evitar, mitigar y detectar los riesgos, cómo se informaría o notificaría [garantías y controles], cuánto costaría [costos] y cuán eficiente sería [análisis costo beneficio].[19]

2.7 El rol de la auditoría interna en la gestión del riesgo empresarial

El rol de la auditoría interna está cambiando, mientras que tradicionalmente su rol a sido asegurar cumplimiento, hoy en día está mas involucrada a proveer información para la toma de decisiones colaborando en la administración de riesgos y mejorando los sistemas de control de las operaciones relevantes y de mayor valor estratégico en la organización.

El rol fundamental de la auditoría interna respecto al ERM es proveer aseguramiento objetivo a la junta sobre la efectividad de las actividades de ERM en una organización,

---

[19] Ibid., p. 197.

para ayudar a asegurar que los riesgos claves de negocio están siendo gestionados apropiadamente y que el sistema de control interno está siendo operado efectivamente.

“Los servicios que presta la auditoría interna son los siguientes:

2.7.1 Rol de aseguramiento

El rol principal en el ERM es proveer aseguramiento objetivo a la junta directiva o consejo de administración sobre la efectividad de la gestión de riesgo y para proveer valor a la organización, brindando aseguramiento objetivo de si los principales riesgo de negocios están siendo manejados apropiadamente y dando aseguramiento de que la gestión de riesgo y el marco de control interno están operando efectivamente.

La experiencia del auditor interno en consideración de riesgos, en entendimiento de la conexión entre riesgo y gobierno y en facilitación demuestra que está bien calificado para actuar como defensor y hasta como gerente del proyecto de ERM, especialmente en la etapa inicial de su introducción.

Cuando incremente la madurez de riesgo en la organización y la gestión de riesgo se encaja más en las operaciones del negocio, el rol de auditoría interna de defensor del ERM se puede reducir. Similarmente, si la organización emplea los servicios de un especialista o posee función de gestión de riesgo, auditoría interna podría agregar mayor valor a través de concentrarse en su rol de aseguramiento, en vez de realizar mayores actividades de consultoría, no obstante, si auditoría interna no tiene la capacidad real o entrenamiento adecuado no debe comprometerse a liderar etapas de esta naturaleza, siendo si su compromiso de capacitar suficientemente sobre el tema de gestión o administración de riesgo.

2.7.2 Rol de consultoría

La auditoría interna puede también proveer servicios de consultoría para lograr que mejoren los procesos de gobierno corporativo, gestión de riesgos y control en la organización. El alcance de la consultoría de auditoría interna en ERM depende de otros recursos de carácter interno o externo, disponibles para la junta directiva o consejo de

administración y de la madurez del riesgo de la organización y su posibilidad de varias en el tiempo.

En relación con el ERM, mientras más se incluya la auditoría interna en la gestión de riesgos, mayores serán las salvaguardas que deben requerirse par asegurar objetividad e independencia de su parte.

Los roles de consultoría dentro de una auditoría interna que se pueden prestar, podrían:

- Poner a disponibilidad de la gerencia herramientas y técnicas usadas por auditoría interna para analizar riesgos y controles;

- Ser un defensor de la introducción de ERM en la organización, aportando su experiencia en gestión de riesgo y conocimientos de la organización;

- Proveyendo consejo, facilitando talleres, entrenando en la organización sobre riesgos y controles, y promoviendo el desarrollo de un lenguaje, marco y entendimiento común;

- Actuando como coordinador, o de monitoreo;

- Presentando reporte sobre riesgos; y

- Apoyando a la gerencia en su trabajo a través de identificar mejores vías para mitigar un riesgo.

El factor clave en la decisión sobre si los servicios de consultoría son compatibles con el rol de aseguramiento es el de determinar si el auditor interno está asumiendo alguna responsabilidad gerencial. En el caso de ERM, la auditoría interna puede proveer servicios de consultoría mientras no tenga rol actualmente en la gestión de riesgo – esa es una responsabilidad de la gerencia – y mientras la alta dirección endose y apoye el ERM.

Cada vez que auditoría interna actúe apoyando al equipo gerencial en el establecimiento y mejora de los procesos de gestión de riesgo, su plan de trabajo debe incluir una estrategia clara y un tiempo asignado para transferir la responsabilidad de estas actividades a los miembros del equipo gerencial.

2.7.3 Salvaguardas

La auditoría interna puede ampliar su participación en el ERM bajo ciertas condiciones de independencia, aclarando que la responsabilidad de los riesgos es de la gerencia, que debe ser adecuadamente documentada, que la función será la de dar consejos y de motivación, pero eso si la de dar aseguramiento objetivo.

Las principales condiciones podrían ser:

- Debe estar claro que la gerencia mantiene la responsabilidad de la gestión de riesgo;

- La naturaleza de la responsabilidad de auditoría interna debe ser documentada en los estatutos de la auditoría y aprobado por el comité de auditoría;

- Auditoría interna no debe gestionar ningún riesgo a favor de la gerencia;

- Auditoría interna debe proveer consejo, motivar y soportar decisiones realizadas por la dirección, en vez de tomar decisiones de riesgo por ellos mismos;

- Auditoría interna tampoco puede brindar aseguramiento objetivo en ninguna parte del marco de ERM de la cual es responsable. Tal aseguramiento debe ser provisto por otra parte sustancialmente calificada; y

- Cualquier trabajo más allá de las actividades de aseguramiento debe reconocerse como que es una asignación de consultoría y la implementación de normas relativas a tales asignaciones deben seguirse.

2.7.4 Destrezas y cuerpo de conocimientos

Los auditores internos y gerentes de riesgo comparten algunos conocimientos, destrezas y valores. Ambos, por ejemplo, conocen sobre requerimientos de gobierno corporativo, poseen destrezas de manejo de proyectos, analíticas y de facilitación y tienen valores de crear un balance saludable de riesgo en vez de tomar riesgos extremos o comportamiento evasivo, sin embargo, los gerentes de riesgo como solamente brindan servicio a la dirección de la organización y no tiene que proveer aseguramiento independiente y objetivo al comité de auditoría. Tampoco debe el auditor interno que busque ampliar su rol en el ERM, subestimar el conocimiento especializado de los gerentes de riesgo (tales como transferencia de riesgo, calificación de riesgos y técnicas de modelos), las cuales están fuera del cuerpo de conocimientos de la mayoría de auditores internos. Ningún auditor interno que no pueda demostrar las destrezas y conocimientos apropiados debe realizar trabajos en el área de gestión de riesgo. Aún más, la cabeza de auditoría interna no debe proveer servicios de consultoría en esta área si las destrezas conocimientos dentro de la función de auditoría interna no se encuentran disponibles y no se pueden obtener de otra parte".[20]

CUADRO No. 2: ROL DE LA AUDITORÍA INTERNA EN EL ERM

ROLES PRINCIPALES DE LA AUDITORÍA INTERNA RESPECTO AL ERM	ROLES LEGÍTIMOS DE AUDITORÍA INTERNA REALIZADOS CON SALVAGUARDA	ROLES QUE LA AUDITORÍA INTERNA NO DEBE REALIZAR
• Brindar aseguramiento sobre procesos de gestión de riesgo. • Brindar aseguramiento de que los riesgos son correctamente evaluados. • Evaluación de los procesos de gestión de riesgo. • Evaluación de reporte de riesgos claves. • Revisión del manejo de los riesgos claves.	• Facilitación, identificación y evaluación de riesgos. • Entrenamiento a la gerencia sobre respuesta a riesgos. • Coordinación de actividades de • ERM. • Consolidación de reportes sobre riesgos. • Mantenimiento y desarrollo del marco de ERM. • Defender el establecimiento del • ERM. • Desarrollo de estrategias de gestión de riesgo para aprobación de la junta.	• Establecer el apetito de riesgo. • Imponer procesos de gestión de riesgo. • Manejar el aseguramiento sobre los riesgos. • Tomar decisiones en respuesta a los riesgos. • Implementar respuestas a riesgos a favor de administración. • Responsabilidad de la gestión.

Fuente: Rodrigo Estupiñán Gaitán, Administración de Riesgos E.R.M. y la Auditoría Interna. (Bogotá: ECOE Ediciones, 2008), p. 141.

[20] Ibid., p. 140.

2.8 Planificación y supervisión

El proceso de planeación le permite al auditor identificar las áreas criticas y los problemas potenciales del examen, evaluar el nivel de riesgo y programar la obtención de la evidencia necesaria para emitir opinión sobre la suficiencia, la eficacia y la efectividad del sistema de control interno del auditado; “el auditor deberá planear su trabajo de modo que la auditoría sea desarrollada de una manera efectiva. Planeación significa desarrollar una estrategia general y un enfoque detallado para la naturaleza, oportunidad y alcance esperados de la auditoría. El auditor planea desarrollar la auditoría de forma eficiente y oportuna.

2.8.1 Planeación del trabajo

La planeación adecuada del trabajo de auditoría ayuda a asegurar que se presta atención adecuada a áreas importantes de la auditoría, que los problemas potenciales son identificados y que el trabajo es completado en forma expedita. La planeación también ayuda a la apropiada asignación de trabajo a los auxiliares y para la coordinación del trabajo hecho por otros auditores y expertos.

El grado de planeación variará de acuerdo con el tamaño de la entidad, la complejidad de la auditoría y la experiencia del auditor con la entidad y conocimiento de la actividad del cliente.

Adquirir conocimiento de la actividad del cliente es una parte importante de la planeación del trabajo. El conocimiento de la actividad del cliente por el auditor ayuda en la identificación de eventos, transacciones y prácticas que puedan tener un efecto importante sobre los estados financieros u otros aspectos de la auditoría.

El auditor puede desear discutir elementos del plan global de auditoría y algunos procedimientos de auditoría con el comité de auditoría, administración y personal de la entidad, para mejorar la efectividad y eficiencia de la auditoría y para coordinar los procedimientos de la auditoría con el trabajo de los empleados de la entidad. El plan global de auditoría y el programa de auditoría, sin embargo, permanecen como responsabilidad del auditor.

2.8.2 El plan global de auditoría

El auditor debería desarrollar y documentar un plan global de auditoría describiendo el alcance y conducción esperados de la auditoría. Mientras que el registro del plan global de auditoría necesitará estar suficientemente detallado para guiar el desarrollo del programa de auditoría, su forma y contenido precisos variarán de acuerdo con el tamaño de la entidad, a la complejidad de la auditoría y a la metodología y tecnología específicas usadas por el auditor.

Los asuntos que tendrá que considerar el auditor al desarrollar el plan global de auditoría incluyen:

a) Conocimiento de la actividad del cliente

Se debe tomar en cuenta:

- Los factores económicos generales y condiciones de la industria que afectan al negocio de la entidad;

- Las características importantes de la entidad, su negocio, su desempeño financiero y sus requerimientos para informar incluyendo cambios desde la fecha de la anterior auditoría; y

- El nivel general de competencia de la administración.

El auditor puede obtener un conocimiento de la industria y de la entidad de un número de fuentes. Por ejemplo:

- Experiencia previa con la entidad y su industria;

- Discusión con personas de la entidad;

- Discusión con personal de auditoría interna y revisión de informes de auditoría interna;

- Discusión con otros auditores y con asesores legales o de otro tipo que hayan proporcionado servicios a la entidad o dentro de la industria. Discusión con personas enteradas fuera de la entidad (por ejemplo, economistas de la industria, reglamentadores de la industria, clientes, abastecedores, competidores);

- Publicaciones relacionadas con la industria (por ejemplo, estadísticas de gobierno, encuestas, textos, revistas de comercio, reportes preparados por bancos y corredores de valores, periódicos financieros);

- Legislación y reglamentos que afecten en forma importante a la entidad;

- Visitas a los locales de la entidad y a instalaciones de sus plantas; y

- Documentos producidos por la entidad (por ejemplo, minutas de juntas, material enviado a accionistas, o presentado a autoridades reglamentadoras, literatura promocional, informes anuales y financieros de años anteriores, presupuestos, informes internos de la administración, informes financieros provisionales, manual de políticas de la administración, manuales de sistemas de contabilidad y control interno, catálogo de cuentas, descripciones de puestos, planes de mercadotecnia y de ventas).

b) Comprensión de los sistemas de contabilidad y de control interno

Se debe tomar en cuenta:

- Las políticas contables adoptadas por la entidad y los cambios en esas políticas;

- El efecto de pronunciamientos nuevos de contabilidad y auditoría; y

- El conocimiento acumulable del auditor sobre los sistemas de contabilidad y de control interno y el relativo énfasis que se espera se ponga en las pruebas de procedimientos de control y otros procedimientos sustantivos.

c) Riesgo e importancia relativa

Se debe tomar en cuenta:

- Las evaluaciones esperadas de los riesgos inherentes y de control y la identificación de áreas de auditoría importantes;

- El establecimiento de niveles de importancia relativa para propósitos de auditoría;

- La posibilidad de manifestaciones erróneas, incluyendo la experiencia de periodos pasados, o de fraude; y

- La identificación de áreas de contabilidad complejas incluyendo las que implican estimaciones contables.

d) Naturaleza, tiempos, y alcance de los procedimientos

Se debe tomar en cuenta:

- El posible cambio de énfasis sobre áreas específicas de auditoría;

- El efecto de la tecnología de información sobre la auditoría; y

- El trabajo de auditoría interna y el efecto esperado sobre los procedimientos de auditoría externa.

e) Coordinación, dirección, supervisión y, revisión

Se debe tomar en cuenta:

- La inclusión de otros auditores en las auditorías de componentes, por ejemplo, subsidiarias, sucursales y divisiones;

- La inclusión de expertos;

- El número de locales o plantas; y

- Requerimientos de personal.

f) Otros asuntos

Se debe tomar en cuenta:

- La posibilidad de que el principio de negocio en marcha pueda ser puesto en duda;

- Las condiciones que requieren atención especial, como la existencia de partes relacionadas;

- Los términos del trabajo y cualesquiera responsabilidades estatutarias; y

- La naturaleza y oportunidad de los informes u otra comunicación con la entidad que se esperan bajo los términos del trabajo.

2.8.3 El programa de auditoría

El auditor deberá desarrollar y documentar un programa de auditoría que exponga la naturaleza, oportunidad y alcance de los procedimientos de auditoría planeados que se requieren para implementar el plan de auditoría global. El programa de auditoría sirve como un conjunto de instrucciones a los auxiliares involucrados en la auditoría y como un medio para el control y registro de la ejecución apropiada del trabajo. El programa de auditoría puede también contener los objetivos de la auditoría para cada área y un presupuesto de tiempos en el que son estimadas las horas para las diversas áreas o procedimientos de auditoría.

Al preparar el programa de auditoría, el auditor debería considerar las evaluaciones específicas de los riesgos inherentes y de control y el nivel requerido de certeza que tendrán que proporcionar los procedimientos sustantivos. El auditor debería también considerar los tiempos para pruebas de controles y de procedimientos sustantivos, la

coordinación de cualquier ayuda esperada de la entidad, la disponibilidad de los auxiliares y la inclusión de otros auditores o expertos.

2.8.4 Cambios al plan global de auditoría y al programa de auditoría

El plan global de auditoría y el programa de auditoría deberían revisarse según sea necesario durante el curso de la auditoría. La planeación es continua a lo largo del trabajo a causa de cambios en las condiciones o resultados inesperados de los procedimientos de auditoría. Deberán registrarse las razones para cambios importantes.

2.8.5 Supervisión

Los objetivos generales de la supervisión son:

- Proporcionar instrucciones a los ayudantes;
- Mantenerse informado de los problemas que se presenten;
- Vigilar que los trabajos se realicen conforme a las normas;
- Asegurarse de que el personal auditor ha comprendido bien su misión;
- Asegurarse que los papeles de trabajo están siendo confeccionados en la forma conveniente;
- Revisar el trabajo efectuado;
- Variar el programa de trabajo de acuerdo con los resultados que se vayan obteniendo; y
- Resolver las diferencias de opinión entre el personal de auditoría.

Es evidente que el grado de supervisión dependerá del tipo de trabajo a realizar, pero en todo caso su objetivo es el de garantizar la calidad y exactitud de los trabajos realizados, asegurándose de que los objetivos propuestos se consiguen; evidentemente el grado de supervisión dependerá de la mayor o menor preparación técnica del personal empleado.

Los supervisores deben dejar constancia de su actuación en las propias hojas de trabajo”.[21]

---

[21] Rodrigo Estupiñán Gaitán, Aspectos Conceptuales Normativos y Metodológicos de la Auditoría Integral. (Bogotá: El Autor, s.a.), p. 3.

2.9 Evidencia y documentación de la auditoría

Para evaluar la efectividad del sistema de control interno y examinar los resultados de la gestión especialmente en áreas y procesos críticos, se debe recopilar evidencia suficiente, convincente y pertinente, debidamente documentada en los papeles de trabajo del auditor.

2.9.1 Evidencia

El auditor deberá obtener evidencia suficiente y apropiada en la auditoría para poder extraer conclusiones razonables sobre las cuales basar su informe.

a) Evidencia en la auditoría

Significa la información obtenida por el auditor para llegar a las conclusiones sobre las que se basa su informe. La evidencia en la auditoría comprenderá documentos fuente y registros contables subyacentes a los estados financieros, información corroborativa de otras fuentes, procedimientos sobre el manejo de los ciclos e indicadores de gestión.

La evidencia en la auditoría se obtiene de una mezcla apropiada de pruebas de control, de procedimientos sustantivos, análisis de proyecciones y análisis de los indicadores de eficiencia y de eficacia.

b) Pruebas de control

Significa pruebas realizadas para obtener evidencia en la auditoría sobre lo adecuado del diseño y operación efectiva de los sistemas de contabilidad y de control interno; el cumplimiento de las metas y objetivos propuestos y el grado de eficacia, economía y eficiencia y el manejo de la entidad.

c) Procedimientos sustantivos

Significa pruebas realizadas para obtener evidencia en la auditoría para encontrar manifestaciones erróneas de importancia relativa en los estados financieros o en sus operaciones, y son de dos tipos:

- Pruebas de detalles de transacciones y balances; y
- Procedimientos analíticos.

d) Evidencia suficiente y apropiada en la auditoría

La suficiencia y la propiedad están interrelacionadas y se aplican a la evidencia en la auditoría obtenida tanto de las pruebas de control como de los procedimientos sustantivos. La suficiencia es la medida de la cantidad de evidencia en la auditoría; apropiada es la medida de la calidad de evidencia en la auditoría y su relevancia para una particular afirmación y su confiabilidad. Normalmente, el auditor encuentra necesario confiar en evidencia en la auditoría que es persuasiva y no definitiva y a menudo buscará evidencia en la auditoría de diferentes fuentes o de una naturaleza diferente para soportar la misma afirmación.

Para obtener las conclusiones de la auditoría, el auditor normalmente no examina toda la información disponible ya que se puede llegar a conclusiones sobre el saldo de una cuenta, los procesos, operaciones, transacciones o controles, por medio del ejercicio de su juicio o de muestreo estadístico.

El juicio del auditor respecto de qué es evidencia suficiente y apropiada en la auditoría es influenciado por factores como:

- La evaluación del auditor de la naturaleza y nivel del riesgo inherente tanto a nivel de los estados financieros como a nivel del saldo de la cuenta o clase de transacciones u operaciones;

- Naturaleza de los sistemas de contabilidad y de control interno y la evaluación del riesgo de control;

- Importancia relativa de la partida o transacción que se examina;

- Experiencia obtenida en auditorías previas;

- Resultados de procedimientos de auditoría, incluyendo fraude o error que puedan haberse encontrado; y

- Fuente y confiabilidad de información disponible.

e) Fuente de la que es obtenida

La confiabilidad de la evidencia en la auditoría es influenciada por su fuente: interna o externa, y por su naturaleza: visual, de documentos u oral. Si bien la confiabilidad de la evidencia en la auditoría depende de la circunstancia individual, las siguientes generalizaciones ayudarán para evaluar la confiabilidad de la evidencia en la auditoría:

- La evidencia en la auditoría de fuentes externas por ejemplo, confirmación o manifestación recibida de una tercera persona es más confiable que la generada internamente;

- La evidencia en la auditoría generada internamente es más confiable cuando los sistemas de contabilidad y de control interno relacionados son efectivos;

- La evidencia en la auditoría obtenida directamente por el auditor es más confiable que la obtenida de la entidad; y

- La evidencia en la auditoría en forma de documentos y manifestaciones escritas es más confiable que las manifestaciones orales.

La evidencia en la auditoría es más persuasiva cuando las partidas de evidencia de diferentes fuentes o de una diferente naturaleza son consistentes. En estas circunstancias, el auditor puede obtener un grado acumulativo de confianza más alto del que se obtendría de partidas de evidencia en la auditoría cuando se consideran individualmente. Por el contrario, cuando la evidencia en la auditoría obtenida de una

fuente es inconsistente con la obtenida de otra, el auditor determina qué procedimientos adicionales son necesarios para resolver la inconsistencia.

f) Procedimientos para obtener evidencia en la auditoría

El auditor obtiene evidencia en la auditoría por uno o más de los siguientes procedimientos:

i. Inspección

La inspección consiste en examinar registros, documentos, o activos tangibles. La inspección de registros y documentos proporciona evidencia en la auditoría de grados variables de confiabilidad dependiendo de su naturaleza y fuente y de la efectividad de los controles internos sobre su procesamiento. La inspección de activos tangibles proporciona evidencia en la auditoría confiable con respecto a su existencia pero no necesariamente a su propiedad o valor.

ii. Observación

La observación consiste en mirar un proceso o procedimiento que está siendo realizado por otros, por ejemplo, la observación por el auditor del conteo de inventarios por personal de la entidad o el desarrollo de procedimientos de control que no dejan rastro de auditoría.

iii. Interrogatorio

Consiste en buscar la información adecuada, dentro o fuera de la organización del cliente. Los interrogantes podrán variar desde las formales por escrito, dirigidos a terceras personas, hasta consultas informales orales, dirigidas a la dirección o al personal del cliente. Las respuestas a las preguntas podrán proporcionarnos nueva información o corroborar la evidencia. Siempre que se obtengan evidencias orales, se debe documentar cuáles fueron las partes involucradas y la esencia de la conversación en la que estas fueron obtenidas, mediante memorandos.

iv. Confirmación

Consiste en la respuesta a una pregunta o solicitud para corroborar la información obtenida en los registros contables, tal como una circular o una muestra representativa de los deudores, para que confirmen los saldos vigentes que aparecen en los estados financieros. El objetivo fundamental de obtener manifestaciones del cliente consiste en confirmar las declaraciones orales ofrecidas e indicar y documentar la exactitud de tales declaraciones. Las manifestaciones por escrito emanadas de la dirección, bajo la forma de carta de manifestaciones dirigidas al auditor generalmente estarán firmadas por los directores generales y financieros.

v. Cálculo

Consiste en comprobar directamente la exactitud aritmética de los documentos de origen y de los registros contables, o desarrollar cálculos independientes.

vi. Procedimientos analíticos

Los procedimientos analíticos consisten en el análisis de índices, indicadores y tendencias significativas incluyendo la investigación resultante de fluctuaciones y relaciones que son inconsistentes con otra información relevante o que se desvían de los montos pronosticados. El análisis de las tendencias y relaciones financieras implicará la revisión de las situación financiera y la marcha de la entidad, expresados por indicadores; cerciorándose si estos índices tienen o deben tener una relación lógica obteniendo explicaciones razonables sobre los movimientos inusuales y determinando si lo que encontramos reflejan la necesidad de procedimientos de auditoría adicionales.

2.9.2 Documentación

El auditor deberá documentar los asuntos que son importantes para apoyar la opinión o informe de auditoría y dejar evidencia de que la auditoría se llevó a cabo de acuerdo con las normas técnicas de trabajo señaladas por los organismos profesionales.

Documentación significa el material, papeles de trabajo preparados por y para, u obtenidos o retenidos por el auditor en conexión con el desempeño de la auditoría. Los papeles de trabajo pueden ser en la forma de datos almacenados en papel, película, medios electrónicos, u otros medios.

Los papeles de trabajo:

- Auxilian en la planeación y desempeño de la auditoría;
- Auxilian en la supervisión y revisión del trabajo de auditoría; y
- Registran la evidencia en la auditoría resultante del trabajo realizado, para apoyar el informe del auditor.

El auditor deberá preparar papeles de trabajo que sean suficientemente completos y detallados para proporcionar una comprensión global de la auditoría.

El auditor deberá registrar en papeles de trabajo la planeación, la naturaleza, oportunidad y el alcance de los procedimientos de auditoría desarrollados, y por lo tanto los resultados, y las conclusiones extraídas de la evidencia obtenida. Los papeles de trabajo incluirían el razonamiento del auditor sobre todos los asuntos importantes que requieran un ejercicio de juicio, junto con la conclusión del auditor. En áreas que impliquen cuestiones difíciles de principio o juicio, los papeles de trabajo registrarán los hechos relevantes que fueron conocidos por el auditor en el momento de alcanzar las conclusiones.

La extensión de los papeles de trabajo es un caso de juicio profesional ya que no es necesario ni práctico documentar todos los asuntos que el auditor considera. Al evaluar la extensión de los papeles de trabajo que se deberán preparar y ser retenidos, puede ser útil para el auditor considerar qué es lo que sería necesario para proporcionar a otro auditor sin experiencia previa con la auditoría una posibilidad de comprensión del trabajo realizado y la base de las decisiones de principios tomadas pero no los aspectos detallados de la auditoría.

La forma y contenido de los papeles de trabajo son afectadas por asuntos como:

- La naturaleza del trabajo;
- La forma del informe del auditor;
- La naturaleza y complejidad del negocio;
- La naturaleza y condición de los sistemas de contabilidad y control interno de la entidad;
- Las necesidades en las circunstancias particulares, de dirección, supervisión, y revisión del trabajo realizado por los auxiliares; y
- Metodología y tecnología de auditoría específicas usadas en el curso de la auditoría.

Los papeles de trabajo son diseñados y organizados para cumplir con las circunstancias y las necesidades del auditor para cada auditoría en particular. El uso de papeles de trabajo estandarizados (por ejemplo, listas de control, cartas machote, organización estándar de papeles de trabajo) puede mejorar la eficiencia con que son preparados y revisados dichos papeles de trabajo; facilitan la delegación de trabajo a la vez que proporcionan un medio para controlar su calidad.

Para mejorar la eficiencia de la auditoría, el auditor puede utilizar agendas o calendarios, análisis y otros documentos preparados por la entidad. En tales circunstancias, el auditor necesitaría estar satisfecho de que esos materiales han sido apropiadamente preparados. Los papeles de trabajo regularmente incluyen:

- Información referente a la estructura organizacional de la entidad;
- Extractos o copias de documentos legales importantes, convenios, y minutas;
- Resumen de las principales leyes, reglamentos y normas que debe cumplir la entidad;

- Información concerniente a la industria, entorno económico y entorno legislativo dentro de los que opera la entidad;

- Evidencia del proceso de planeación incluyendo programas de auditoría y cualesquier cambios al respecto;

- Evidencia de la comprensión del auditor de los sistemas de contabilidad y de control interno;

- Evidencia de evaluaciones de los riesgos inherentes y de control y cualesquiera revisiones al respecto;

- Evidencia de la consideración del auditor del trabajo de auditoría interna y las conclusiones alcanzadas;

- Análisis de transacciones y balances de prueba;

- Análisis de tendencias, índices importantes e indicadores económicos;

- Un registro de la naturaleza, tiempos, y grado de los procedimientos de auditoría desarrollados y de los resultados de dichos procedimientos;

- Evidencia de que el trabajo realizado por los auxiliares fue supervisado y revisado;

- Una indicación sobre quién desarrolló los procedimientos de auditoría y cuándo fueron desarrollados;

- Copias de comunicaciones con otros auditores, expertos y otras terceras partes;

- Copias de cartas o notas referentes a asuntos de auditoría comunicados a, o discutidos con la entidad, incluyendo los términos del trabajo y las debilidades sustanciales en control interno;

- Cartas de representación recibidas de la entidad;

- Conclusiones alcanzadas por el auditor concernientes a aspectos importantes de la auditoría, incluyendo cómo se resolvieron los asuntos excepcionales o inusuales, si los hay, revelados por los procedimientos del auditor; y

- Copias de los estados financieros, dictamen u otros informes del auditor.

2.9.3 Informes de la auditoría

La culminación de cada una de las fases o segmentos principales de la auditoría es la emisión del informe. Con base en los resultados que se vayan obteniendo en la auditoría, el auditor debe rendir a los administradores u órganos de dirección de la entidad examinado los siguientes informes:

a) Informes eventuales

Emitidos sobre errores, irregularidades, actos ilegales o desviaciones significativas del control interno que se encuentre en el desarrollo del trabajo; así como las recomendaciones que estime pertinentes con relación a las diferentes situaciones observadas a fin de adoptar las medidas a que haya lugar.

b) Informes intermedios

Con periodicidad trimestral (a manera de ejemplo) con indicación del trabajo desarrollado y los resultados obtenidos, indicando los procedimientos de auditoría aplicados en cada una de las áreas auditadas con sus hallazgos y conclusiones.

Los informes intermedios pueden tener su origen en requerimientos gubernamentales de comisiones de valores o de organismos encargados del control y vigilancia de las compañías, en estos casos se exigen al auditor alcances mínimos en el trabajo y elementos básicos en el contenido del informe. Pero también los informes intermedios son fruto del proceso de la auditoría para comunicar la culminación de un trabajo en un área o sección de la compañía, para comunicar deficiencias importantes en los controles internos, incumplimiento de leyes y regulaciones o para proponer sugerencias y recomendaciones.

De lo expuesto en el párrafo anterior se concluye que los informes intermedios de la auditoría son muy variados en su estructura y contenido y dependen de las circunstancias en las que sean elaborados. En el presente trabajo se dieron pautas para los informes de la auditoría de gestión que pueden clasificarse como informes intermedios.

c) Informe final

Un informe final con su dictamen u opinión sobre: los estados financieros básicos; lo adecuado del control interno; el cumplimiento de las normas legales reglamentarias y estatutarias; la gestión de los administradores; y la concordancia entre la información adicional presentada por los administradores.[22]

CUADRO No. 3: INFORME FINAL DE AUDITORÍA

A los Accionistas de Compañía Hipotética S.A.

He auditado el balance general de la Compañía Hipotética S. A., al 31 de diciembre de 20XX, y los correspondientes estados de resultados, de cambios en el patrimonio, de flujos de efectivo por el año terminado en esa fecha y su sistema de control interno. La administración es responsable de la preparación, integridad y presentación razonable de los estados financieros y de mantener un sistema de control interno adecuado para proveer una seguridad razonable en la conducción ordenada y eficiente del negocio de la compañía. Mis obligaciones son las de expresar una opinión, con base en la auditoría practicada, sobre dichos estados financieros y sobre lo adecuado del control interno en relación con la efectividad y eficiencia de las operaciones, confiabilidad de la información financiera y cumplimiento con las leyes y reglamentos aplicables.

Realicé mi auditoría de acuerdo con las normas internacionales de auditoría. Esas normas requieren que una auditoría se planifique y se lleve a cabo de tal manera que se obtenga una seguridad razonable sobre la situación financiera de la entidad, y sobre lo apropiado del control interno para cumplir los objetivos de eficiencia y efectividad de las operaciones, confiabilidad de la información financiera y cumplimiento con las leyes y regulaciones aplicables. Una auditoría incluye el examen, sobre una base selectiva, de la evidencia que respalda las cifras y las notas informativas en los estados financieros. Una auditoría también incluye la evaluación de las normas o principios de contabilidad utilizados y de las principales estimaciones efectuadas por la administración, así como la evaluación de la presentación global de los estados financieros. Considero que mi auditoría proporciona una base razonable para expresar mi opinión.

---

22 Ibid., p. 9.

El sistema de control interno abarca una estructura organizacional documentada y divisiones de responsabilidades, políticas establecidas y procedimientos que incluyen un código de conducta; los auditores internos supervisan el control interno e informan a niveles apropiados los resultados y recomendaciones sobre los que se toman las acciones correctivas para controlar las deficiencias y para mejorar el sistema a medida que se superan las debilidades. Hay limitaciones inherentes en la efectividad de cualquier sistema de control interno, incluyendo la posibilidad de errores humanos, fraudes y encubrimientos de los controles. De esta manera, aún con un sistema de control interno efectivo, éste solo puede proveer una seguridad razonable con respecto a sus objetivos. Adicionalmente, la efectividad de un sistema de control puede cambiar con las circunstancias.

En mi opinión, los estados financieros arriba mencionados presentan razonablemente la situación financiera de la Compañía Hipotética S.A. al 31 de diciembre de 20XX, los cambios en el patrimonio, los resultados de las operaciones y los flujos de efectivo por los años terminados en esa fecha, de conformidad con principios internacionales de contabilidad, aplicados uniformemente.

Además, en mi opinión, la entidad ha observado medidas adecuadas de control interno para proporcionar seguridad razonable en la consecución de los siguientes objetivos: efectividad y eficiencia de las operaciones, confiabilidad de la información financiera y cumplimiento con las leyes, regulaciones aplicables y sus estatutos.

La información suplementaria que se presenta en el informe anual fue objeto de mi autoría y existe concordancia o consistencia, en todos los aspectos importantes, con los estados financieros.

Nombre del Auditor
Firma

Guatemala, 30 de marzo de 20XX

Fuente: Elaboración propia.

CAPÍTULO III
ADMINISTRACIÓN DEL RIESGO EMPRESARIAL

3.1 El riesgo

En la mayoría de las definiciones el riesgo se interpreta como incertidumbre, probabilidades, alternativas, perdidas. En un sentido más amplio el riesgo "es concebido como la probabilidad de que un evento o acción afecte adversamente el cumplimiento de los objetivos de la entidad y el tratamiento del mismo, constituyen el punto determinante para la decisión sobre qué procesos y áreas serán objeto de evaluación en profundidad.

Dicha evaluación sólo podrá llevarse a cabo si el auditor ha comprendido apropiadamente los objetivos de la organización a auditar. Recién entonces, podrá juzgar lo apropiado de los riesgos que pueden impedir a la organización alcanzar los resultados esperados eficientemente.

En función de la información obtenida por el auditor, debe evaluarse el riesgo de auditoría a efectos de establecer los procedimientos a aplicar para asegurar que el mismo se reduce a un nivel aceptablemente bajo".[23]

3.2 Riesgos en auditoría

Cada vez que un auditor ejecute una auditoría, no importando como se llame ésta, sé vera enfrentado a una serie de riesgos los cuales deben ser identificados, evaluados y considerados adecuadamente, para lograr en forma satisfactoria su labor, es decir, con eficiencia y eficacia profesional.

Hoy en día, cuando un auditor se enfrenta al tema de los riesgos en la auditoría, su mayor dificultad no está en el conocimiento y manejo de la teoría que lo sustenta, sino más bien en como evaluarlos para así poder minimizarlos al máximo. El auditor cada vez que se enfrenta a una auditoría debe considerar la posible existencia de riesgos, los que tienen

---

[23] Universidad de Buenos Aires. Manual de Procedimientos de Auditoría Interna. (Buenos Aires: Editorial Universitaria, s.a.), p. 62.

relación con su actividad profesional y los relacionados con el trabajo de la auditoría como proceso.

Si consideramos que riesgo es la contingencia o proximidad de un daño, la posibilidad de que ocurra algo no esperado o de que no ocurra lo esperado, cada vez que el auditor se relaciona con un trabajo de auditoría, debe considerar la posible existencia de riesgos, tanto de aquellos relativos a su actividad profesional, como los relacionados a cada trabajo de auditoría en particular, de lo anterior surge la siguiente clasificación de los riesgos en auditoría a los que puede enfrentarse un profesional del área:

3.2.1 Riesgo profesional

Es el riesgo a que está expuesto el auditor frente a la posibilidad de emitir una opinión errónea o un informe equivocado o que no satisfaga a su cliente. Éste de materializarse puede provocar en el auditor daño en su imagen o prestigio profesional, personal o incluso en su patrimonio.

Es el primer riesgo que debe ser evaluado por el auditor cuando se enfrenta a un nuevo trabajo de auditoría, el cual depende de los siguientes factores:

- Grado de satisfacción de los auditados con relación al trabajo efectuado por el auditor; y

- Características de la organización que será auditada y sus integrantes.

El riesgo profesional, se relaciona al daño que puede sufrir el auditor al no poder satisfacer las expectativas de su cliente si se trata de un auditor externo o de la jefatura e integrantes de la organización si es un auditor interno, este tipo de riesgo por lo general es producto de objetivos de auditorías mal definidos, en donde el auditado espera mucho más de lo que el auditor es capaz de entregar, dado el trabajo realizado, encontrándonos frecuentemente con comentarios como los siguientes:

- ¿Pero como pudo producirse esta situación anormal en el área “XY”, si los auditores nos visitaron el mes pasado?;

- ¿Si la sucursal fue auditada recientemente, significa entonces que, excepto por lo indicado por los auditores en su informe de auditoría, el resto está bien?; y

- ¿Dónde estaban los auditores cuando se produjo esta situación fraudulenta o anormal?.

Dado los comentarios anteriores y muchos otros, el auditor antes de comprometerse a realizar un trabajo de auditoría, deberá definir en forma clara y en conjunto con el auditado los objetivos de su trabajo, evitando así la posible materialización del riesgo profesional.

El riesgo profesional también se relaciona con el daño que puede sufrir el auditor en su imagen profesional, en su persona o en su patrimonio, cuando se relaciona a través de un trabajo de auditoría a empresas o personas cuestionadas. Lo anterior hace necesario que el auditor deba obtener un conocimiento previo de la organización con el cual se vincula, para disminuir de este modo el nivel de riesgo profesional causado por lo antes mencionado.

3.2.2 Riesgo en auditoría (RA)

Es la posibilidad que una vez efectuado el examen de auditoría, de acuerdo a las normas establecidas, permanezcan situaciones relevantes no informadas o errores significativos en el objeto auditado.

La materialización de este riesgo implica la emisión de un informe incorrecto o incompleto. A fin de precaverse del riesgo asociado a su labor profesional, el auditor debe explicitar formalmente los objetivos de la revisión. Además debe efectuarse una adecuada planificación, ejecución y control del trabajo de tal modo de reducir este riesgo a niveles aceptables.

El riesgo de auditoría es la combinación de tres elementos:

- La posibilidad de existencia de errores o irregularidades significativas en el objeto a auditar;

- La posibilidad de - no - detección o neutralización de la materialización de estos errores o irregularidades por el sistema de control interno del ente auditado; y

- La posibilidad de su - no - detección por parte del auditor, mediante la aplicación de sus procedimientos de auditoría.

Los tres elementos componentes del riesgo de auditoría antes citados dan origen a los siguientes riesgos:

a) Riesgo inherente (RI)

Está dado por la posibilidad de la existencia de omisiones, errores o irregularidades significativas en el objeto sometido a examen, ya sean estos estados financieros, procedimientos operativos o administrativos, gestión, etc. Es aquel propio de la naturaleza del objeto auditado y está influido tanto por factores internos y como por externos. Aquél que no se puede eliminar, siempre estará presente en toda empresa.

Las organizaciones conscientes de la existencia de estos riesgos inherentes y con el objetivo de detectarlos o neutralizarlos, diseñan e implementan acciones, procedimientos y sistemas de control interno, los cuales se constituyen en una especie de filtros de los riesgos inherentes, surgiendo de este modo el siguiente componente del riesgo de auditoría el: riesgo de control.

b) Riesgo de control (RC)

Corresponde a la posibilidad que se materialicen los riesgos inherentes y que éstos no se hayan detectado, controlado o evitado por el sistema de control interno diseñado para tales efectos.

Dado que es posible que el sistema de control interno no detecte o neutralice los riesgos inherentes significativos, la organización deberá considerar, mientras sea costo -

beneficio, la participación activa del auditor a través de la realización de sus labores de auditoría, las que tendrán como uno de sus objetivos el detectar aquellos riesgos inherentes que no fueron detectados por el sistema de control interno vigente en la organización, agregándose así el tercer elemento componente del riesgo de auditoría el: riesgo de detección.

c) Riesgo de detección (RD)

Es la posibilidad que los procedimientos de auditoría seleccionados no detecten los errores, o irregularidades existentes en el objeto auditado situaciones que tampoco fueron detectadas o neutralizadas por el sistema de control interno de la organización. Esto puede originarse en el alcance de las pruebas, la oportunidad en que fueron efectuadas y la calidad con que fueron aplicadas.

Los riesgos antes mencionados deberán ser evaluados por el auditor durante la ejecución de su trabajo, apoyando así a la consecución de su objetivo de auditoría en forma eficaz como eficiente. La actividad de evaluación de los riesgos al interior de un trabajo de auditoría se constituye en una de las actividades más complejas del trabajo del auditor dada la gran cantidad de factores que intervienen en cada uno de los riesgos antes mencionados.

3.2.3 Evaluación del riesgo de auditoría

Si consideramos que el riesgo de auditoría es una combinación de tres elementos (RI – RC – RD). Cada uno de estos riesgos se puede expresar en forma cuantitativa, a través del uso de probabilidades, con valores que van desde ceso (0) a uno (1), es decir, desde aquello que es casi imposible a aquello de certeza casi absoluta.

Cuando el riesgo inherente tiende a cero, es decir, cuando su materialización es casi imposible, no se justifica invertir en controles internos, por la alta probabilidad de que dicha inversión no sea beneficiosa, menos hacer grandes inversiones en auditorías para emitir una opinión adecuada al respecto, dado lo poco significativo del riesgo en cuestión.

Cuando el riesgo inherente es significativo pero, existe un buen sistema de control interno asociado a dicho riesgo inherente, difícilmente éste se materializará, obteniéndose con ello un riesgo de control bajo, es decir, que tienda a cero y por consiguiente el riesgo de auditoría también será bajo, indicándonos esto último que no es necesario efectuar grandes inversiones en la auditoría de estos componentes.

Finalmente, cuando el nivel de riesgo inherente y de control es alto, cercanos a la unidad producto de la existencia de riesgos inherentes significativos que el sistema de control interno no logra detectar o neutralizar, pero que el auditor con sus procedimientos de auditoría si los detecta, con lo cual puede opinar correctamente dado que su riesgo de detección tiende a cero.

Lo anterior se puede cuantificar o representar utilizando la siguiente formula:

$$RA = RI * RC * RD$$

También sabemos que el riesgo inherente y el riesgo de control no son atribuibles directamente a la labor del auditor. El riesgo inherente depende de la naturaleza del objeto a auditar y el impacto del entorno en él y el riesgo de control de la existencia, calidad y funcionamiento del control interno de la organización, en cambio el riesgo de detección dependerá exclusivamente de la calidad de trabajo del auditor, de la adecuada planificación y ejecución de sus procedimientos de auditoría, de su naturaleza, oportunidad y alcance, siendo este nivel de riesgo, el riesgo de detección, el que el auditor debe manejar para lograr el nivel de riesgo de auditoría que ha sido previamente determinado por él, dado un nivel de riesgo inherente y de control existente en el objetivo auditado.

Lo anterior se puede ser expresado utilizando la siguiente formula:

$$RD = \frac{RA}{RI * RC}$$

Según la expresión anterior el riesgo de detección depende directamente del riesgo de auditoría e inversamente de los riesgos inherentes y de control, siendo el riesgo de

detección permitido para que dado un cierto nivel de riesgo inherente y de control, el riesgo de auditoría se mantenga dentro de límites aceptables.

La expresión anterior nos indica que para poder determinar en nivel de seguridad que se debe alcanzar con un trabajo de auditoría, será necesario en primer lugar determinar el nivel de riesgo de auditoría aceptable, nivel que dependerá de la importancia relativa del componente auditado en relación con un todo. Por ejemplo; si consideramos que un 5% es un nivel de riesgo de auditoría aceptable para el todo auditado, es decir, para el total del objeto sobre el que debemos emitir nuestra opinión, no necesariamente igual nivel debe ser exigido a cada uno de los componentes del todo auditado, pudiendo exigirse un nivel de riesgo menor al 5% para aquellos componentes de mayor significancia o importancia relativa, en cambio para aquellos de significancia menor, podría ser aceptable un nivel de riesgo mayor al 5%. Si mantenemos constante los niveles de riesgo inherente y de control, podríamos concluir que el nivel de riesgo de detección aceptable para aquellos componentes poco significativos es mayor, y por lo tanto, el trabajo de auditoría es más reducido, siendo el caso inverso para aquellos componentes de mayor significación o importancia relativa.[24]

3.3 El riesgo empresarial

Se produce riesgo cuando hay probabilidad de que algo negativo suceda o que algo positivo no suceda, la ventaja de una empresa es que conozca claramente los riesgos oportunamente y tenga la capacidad para afrontarlos. El riesgo es un concepto que bien podríamos llamar vital, por su vinculo con todo lo que hacemos, casi podríamos decir que no hay actividad de la vida, de los negocios o de cualquier asunto que se nos ocurra, que no incluya la palabra riesgo.

Fue por ello que la humanidad, desde sus inicios, buscó maneras de protegerse contra las contingencias del quehacer diario y desarrolló maneras de esquivar, eliminar, minimizar o enfrentar los riesgos. Entre esas formas de protección está la acción colectiva, cooperada o sindicalizada; la precaución individual o corporativa, las normas comunitarias y en fin tantas otras, entre las cuales se incluye la tecnología como medio de prevención.

---

[24] Vilches Troncoso, Op. Cit., p. 43.

Para ello, las empresas están adoptando profesionalmente funciones especificas manejados por departamentos especializados en la identificación del riesgo no solo de sus activos, sino de sus pasivos, equilibrando la rentabilidad y la de poder asumir los riesgos implícitos en los negocios, denominándolas gerencias de riesgos, logrando así una mayor eficiencia y eficacia de los procesos para una mayor efectividad y seguridad razonable, como también determinando factores de mecanismos de medición, fuentes de información confiables, oportunas, series históricas de valores relevantes y sistemas computarizados de identificación y corrección.

Los riesgos pueden ser originados por las amenazas externas y las debilidades internas, algunos cuantificables y otros no originados específicamente por inadecuada estructura organizacional, la competencia desleal, por la mala calidad de los productos, por exigencias exageradas de los empleados, huelgas, nuevos impuestos, catástrofes, iliquidez, tasas de interés exageradas, aumento de precios de los proveedores, perdida de imagen, por inadecuada auditoría externa e interna o por autocontroles no aplicados, etc.

Se pueden clasificar los diferentes riesgos de gestión en “Riesgos estratégicos y del negocio”, en “Riesgos financieros” y en “Riesgos generales o de apoyo”.

Los riesgos estratégicos y del negocio los podemos clasificar en:

- Riesgo político y de país o macroeconómico o soberano (inflación o devaluación interna o de países vecinos, guerrilla, narcotráfico, terrorismo, recesión, impuestos, etc.);

- Riesgo de crédito (tasas de interés altas, desconfianza en el mercado, regulaciones estrictas, falsificación de documentos y corrupción en general);

- Riesgo de imagen (fusiones, reestructuraciones, manejo del cambio);

- Riesgo competitivo (calidad, precio, distribución, servicio, productos sustitutos, competidores potenciales);

- Riesgo regulatorio (impuestos, aranceles de aduana, restricciones, control de precios);

- Riesgo de operación (proveedores, calidad, liquidez, producción, maquinaria, especialización de la mano de obra, convertibilidad, fraudes, etc.);

- Riesgo de liquidez (financiaciones, exceso de activos improductivos, stock exagerados, poco apoyo financiero de sus dueños, inversiones inoficiosas con disponibilidad a largo plazo, etc.);

- Riesgo de desastres naturales (incendios, terremotos, huracanes, inundaciones, etc.);

- Riesgo fiduciario (inversiones a la baja, patrimonios autónomos inadecuados, comisiones onerosas, poca gestión fiduciaria, etc.);

- Riesgo interbancario (intervención del gobierno, desencajes, colocaciones a largo plazo y captaciones a corto plazo, gestión inescrupulosa, etc.); y

- Riesgo de intervención estatal (por desencajes, colocaciones sin análisis suficientes, corrupción, etc.).

Los riesgos financieros, se clasifican en:

- Riesgo de interés (volatilidad de las tasas de interés); y

- Riesgo cambiario y de convertibilidad (devaluación o revaluación de la moneda nacional con el dólar, otras monedas y ahora con el euro).

Los riesgos generales o de apoyo, se clasifican en:

- Riesgo de organización (estructura poco clara, ausencia de planificación, carencia o fallas en el sistema, mal clima laboral, malos canales de comunicación);

- Riesgo de auditoría (inherente, control y detección);

- Riesgo de información (tecnológico, integridad información, comunicación y disponibilidad de información);

- Riesgo de operaciones ilícitas (lavado de activos, fraudes y delitos financieros); y

- Seguridades físicas y humanas (contratación de personas sin investigación suficiente, problemas graves personales, plan de contingencias inadecuado, etc.).[25]

3.4 Administración del riesgo empresarial (ERM)

Dado que el riesgo queda inevitablemente ligado a la incertidumbre sobre eventos futuros, resulta imposible eliminarlo. Ante esto, la única forma de enfrentarlo es administrándolo. La administración del riesgo empresarial "es un proceso, efectuado por la junta de directores de una entidad, por la administración y por otro personal, aplicado en el establecimiento de la estrategia y a través del emprendimiento, diseñado para identificar eventos potenciales que pueden afectar la entidad, y para administrar los riesgos que se encuentran dentro de su apetito por el riesgo, a fin de proveer seguridad razonable en relación con el logro de los objetivos de la entidad.

La definición refleja ciertos elementos fundamentales, como son:

- Proceso, ongoing[26] y fluyente a través de una entidad;

- Efectuados por gente en cada nivel de la organización;

- Aplicados en el establecimiento de la estrategia;

- Aplicados a través del emprendimiento, en cada nivel y unidad, e incluye tomar un punto de vista del riesgo de portafolio a nivel de la entidad;

---

25 Estupiñán Gaitán, Op. Cit., p. 101.

26 Término técnico que significa estar actualmente en proceso, en continuo movimiento, hacia adelante.

- Diseñado para identificar eventos potenciales que, si ocurren, afectarán la entidad y para administrar los riesgos que caen dentro de su apetito por el riesgo;

- Capaces de proveer seguridad razonable a la administración y a la junta de directores de una entidad; y

- Enfocados al logro de objetivos en una o más categorías separadas pero sobrepuestas.

3.4.1 Un proceso

La administración de riesgos del emprendimiento no es un evento o una circunstancia, sino una serie de acciones que permean las actividades de una entidad. Esas acciones son penetrantes e inherentes en la manera como la administración opera el negocio.

La administración de riesgos del emprendimiento difiere de la perspectiva de algunos observadores que la consideran como algo añadido a las actividades de una entidad, o como una obligación necesaria. Esto no es para decir que la administración efectiva de los riesgos del emprendimiento no requiere un esfuerzo incremental. Por ejemplo, la valoración del riesgo puede requerir esfuerzo incremental para desarrollar los modelos requeridos y para realizar el análisis y los cálculos necesarios. Sin embargo, esos y otros mecanismos de la administración de riesgos del emprendimiento están mutuamente involucrados con las actividades de operación de la entidad y existen por razones de negocio fundamentales. La administración de riesgos del emprendimiento es más efectiva cuando esos mecanismos se construyen en la infraestructura de la entidad y hacen parte de la esencia de la empresa. Mediante su construcción en la administración de riesgos del emprendimiento, una entidad puede afectar directamente su habilidad para implementar su estrategia y lograr su visión o misión.

Comprometerse en la administración de riesgos del emprendimiento también tiene implicaciones importantes para la reducción de costos, especialmente en los mercados altamente competitivos que muchas compañías enfrentan. Agregar procedimientos nuevos separados de los existentes añade costos. Mediante el centrarse en las operaciones existentes y en su contribución a la efectiva administración de riesgos del

emprendimiento, e integrando la administración de riesgos en las actividades de operación básicas, una empresa puede evitar procedimientos y costos innecesarios. Además, una práctica de construir la administración de riesgos del emprendimiento en la fábrica de las operaciones ayuda a identificar oportunidades nuevas para que la administración las sopese en el crecimiento del negocio.

3.4.2 Efectuado por la gente

La administración de riesgos del emprendimiento es realizada por la junta de directores, la administración y por otro personal. Constituye un logro de la gente de una organización, a causa de lo que hacen y dicen. La gente establece la misión/visión, la estrategia y los objetivos de la entidad, y pone en funcionamiento los mecanismos de administración de riesgos del emprendimiento. De manera similar, la administración de riesgos del emprendimiento afecta las acciones de la gente. La administración de riesgos del emprendimiento reconoce que la gente no siempre entiende, comunica, o no se desempeña de manera consistente. Cada individuo le aporta al lugar de trabajo un trasfondo y una habilidad técnica únicos, y tiene diferentes necesidades y prioridades. Esas realidades afectan, y son afectadas por, la administración de riesgos del emprendimiento.

Cada persona tiene un punto de referencia único que influye la manera como identifica, valora y responde frente al riesgo. La administración de riesgos del emprendimiento provee los mecanismos requeridos para ayudar a que la gente entienda el riesgo en el contexto de los objetivos de la entidad. La gente tiene que conocer sus responsabilidades y límites de autoridad. De acuerdo con ello, se requiere que exista un vínculo claro y estrecho entre las obligaciones de la gente y la manera como son llevadas a cabo, así como con la estrategia y los objetivos de la entidad.

La gente de una organización incluye la junta de directores, lo mismo que la administración y otro personal. Si bien los directores principalmente proveen supervisión, también proveen dirección y aprueban la estrategia y ciertas transacciones y políticas. Por lo tanto, las juntas de directores constituyen un elemento importante de la administración de riesgos del emprendimiento.

3.4.3 Aplicado en la definición de la estrategia

Una entidad define su misión o visión y establece objetivos estratégicos, los cuales son las metas de alto nivel que se alinean con y apoyan su visión o misión. Una entidad establece una estrategia para lograr sus objetivos estratégicos. También define los objetivos relacionados que espera lograr, siguiendo a partir de la estrategia, y en forma de cascada, hacia las unidades de negocio, divisiones y procesos. Al definir la estrategia, la administración considera los riesgos relacionados con las estrategias alternativas.

3.4.4 Aplicado a través de la empresa

Para aplicar exitosamente la administración de riesgos del emprendimiento, una entidad tiene que considerar el espectro completo de sus actividades. La administración de riesgos del emprendimiento considera las actividades en todos los niveles de la organización, desde actividades a nivel de la empresa tales como planeación estratégica y asignación de recursos, hasta las actividades de la unidad de negocios tales como mercadeo y recursos humanos, hasta los procesos de negocio tales como producción y revisión del crédito de los clientes nuevos. La administración de riesgos del emprendimiento también aplica a proyectos especiales y a iniciativas nuevas que pueden todavía no tener designado un sitio en la jerarquía o en el organigrama de la entidad.

La administración de riesgos del emprendimiento requiere que una entidad asuma un punto de vista de portafolio en relación con los riesgos. Esto conlleva implicar a cada administrador responsable por una unidad de negocios, función, proceso u otra actividad que desarrolle una valoración del riesgo para la unidad. La valoración puede ser cuantitativa o cualitativa. Con un punto de vista compuesto en cada siguiente nivel de la organización, la administración principal está posicionada para determinar si el perfil general de riesgo de la entidad es proporcional con su apetito por el riesgo.

A partir de una perspectiva de portafolio a nivel-de-la-entidad, la administración considera los riesgos interrelacionados. Estos, requieren ser identificados y que se actúe sobre ellos para conocer completamente el riesgo junto con el apetito que por el riesgo tiene la entidad. Los riesgos que corresponden a las unidades individuales de la entidad pueden encontrarse dentro de la tolerancia al riesgo de las unidades, pero tomados juntos pueden

exceder el apetito que por el riesgo tiene la entidad como un todo. El apetito general que por el riesgo tiene la entidad se refleja en una corriente que fluye desde arriba hacia abajo en la entidad, a través de tolerancias que se establecen para los objetivos específicos.

3.4.5 Apetito por el riesgo

El apetito por el riesgo es la cantidad de riesgo que una entidad está dispuesta a aceptar en la búsqueda de valor. Las entidades a menudo consideran cualitativamente el apetito por el riesgo, en categorías tales como alto, moderado o bajo, o pueden tomar un enfoque cuantitativo, reflejando y balanceando las metas de crecimiento, retorno y riesgo.

El apetito por el riesgo está relacionado directamente con la estrategia de una entidad. Se considera en la definición de la estrategia, en la que el retorno deseado de una estrategia se debe alinear con el apetito que por el riesgo tiene la entidad. Estrategias diferentes expondrán a la entidad a riesgos diferentes. La administración de riesgos del emprendimiento, aplicada en la definición de la estrategia, le ayuda a la administración a seleccionar una estrategia consistente con el apetito que por el riesgo tiene la entidad.

El apetito que por el riesgo tiene una entidad orienta la asignación de recursos. La administración asigna recursos a través de las unidades de negocio teniendo en consideración el apetito que por el riesgo tiene la entidad y las estrategias de las unidades de negocio individuales para generar un retorno deseado sobre los recursos invertidos. La administración considera su apetito por el riesgo en cuanto éste está alineado con su organización, su gente y sus procesos, y diseña la infraestructura necesaria para responder y monitorear efectivamente a los riesgos.

La tolerancia al riesgo es el nivel aceptable de variación relativa con el logro de los objetivos. Al definir tolerancias específicas frente al riesgo, la administración considera la importancia relativa de los objetivos relacionados y alinea la tolerancia al riesgo con su apetito por el riesgo. Operar con esta tolerancia al riesgo provee a la administración con mayor seguridad de que la entidad permanecerá con su apetito por el riesgo y, a su vez, provee un alto grado de comodidad respecto de que la entidad logrará sus objetivos.

3.4.6 Provee seguridad razonable

Una bien diseñada y operada administración de riesgos del emprendimiento puede proveer a la administración y a la junta de directores con seguridad razonable en relación con el logro de los objetivos de una entidad. Como resultado de una administración de riesgos del emprendimiento que se determinó es efectiva, en cada una de las categorías de los objetivos de la entidad, la junta de directores y la administración obtiene seguridad razonable de que:

- Entienden la extensión en la cual se están logrando los objetivos estratégicos de la entidad;
- Entienden la extensión en la cual se están logrando los objetivos de operación;
- La presentación de reportes de la entidad es confiable; y
- Se está cumpliendo con las leyes y regulaciones aplicables.

La seguridad razonable refleja la noción de que la incertidumbre y el riesgo se relacionan con el futuro, el cual uno no puede predecir con certeza. Las limitaciones también se derivan de las realidades de que el juicio humano en la toma de decisiones puede ser imperfecto, las decisiones sobre las respuestas al riesgo y el establecimiento de los controles requieren considerar los costos y los beneficios asociados, pueden ocurrir rupturas a causa de fallas humanas tales como errores o equivocaciones simples, los controles se pueden eludir por acuerdos secretos e ilegales de dos o más personas, y la administración tiene la habilidad para eludir las decisiones de la administración de riesgos del emprendimiento. Esas limitaciones hacen imposible que la administración tenga seguridad absoluta de que se lograrán los objetivos.

3.4.7 Logro de objetivos

De la administración efectiva de riesgos del emprendimiento se puede esperar que provea seguridad razonable del logro de los objetivos relacionados con la confiabilidad de la presentación de reportes y con el cumplimiento con las leyes y regulaciones. El logro de

esas categorías de objetivos está bajo control de la entidad y depende de qué tan bien se están desempeñando las actividades relacionadas de la entidad.

Sin embargo, el logro de los objetivos estratégicos y de operaciones no siempre está bajo control de la entidad. Para esos objetivos, la administración de riesgos del emprendimiento puede proveer seguridad razonable solamente de que la administración, y la junta en su rol de supervisión, son conscientes, de una manera oportuna, de la extensión en la cual la entidad se está moviendo hacia el logro de los objetivos.

Esta definición es poderosamente amplia. Captura conceptos clave que son fundamentales respecto de cómo las compañías y otras organizaciones administran el riesgo, proveyendo una base para la aplicación a través de organizaciones, industria y sectores. Se centra directamente en el logra de los objetivos establecidos por una entidad particular y provee una base para definir la efectividad de la administración de riesgos empresariales".[27]

3.5 Beneficios del ERM

Ninguna entidad opera en un entorno libre de riesgos, y la administración de riesgos del emprendimiento no crea tal entorno. Más aún, la administración de riesgos del emprendimiento le permite a la administración operar más efectivamente en entornos llenos de riesgos.

La administración de riesgos del emprendimiento provee capacidad enriquecida para:

- **Alinear el apetito por el riesgo y la estrategia:** el apetito por el riesgo es el grado de riesgo, en un nivel de base amplia, que una compañía u otra entidad está dispuesta a aceptar en la búsqueda de sus metas. La administración considera el apetito por el riesgo que tiene la entidad evaluando primero las alternativas estratégicas, y luego estableciendo objetivos alineados con la estrategia seleccionada y desarrollando mecanismos para administrar los riesgos relacionados;

---

[27] Committee of Sponsoring Organizations of the Treadway Commission. Estructura Conceptual de la Administración de Riesgos del Emprendimiento -RESUMEN EJECUTIVO- Borrador en exposición para comentarios públicos. (Bogotá: ECOE Ediciones, 2003), p. 6.

- **Vincular crecimiento, riesgo y retorno:** las entidades aceptan el riesgo como parte de la generación y preservación del valor, y esperan retornos que sean proporcionales con el riesgo. La administración de riesgos del emprendimiento provee una habilidad enriquecida para identificar y valorar riesgos, y para establecer niveles aceptables de riesgo relacionados con los objetivos de crecimiento y retorno;

- **Enriquecer las decisiones de respuesta frente al riesgo:** la administración de riesgos del emprendimiento provee el rigor para identificar y seleccionar entre las respuestas alternativas frente al riesgo (evitar, reducir, compartir y aceptar el riesgo). La administración de riesgos del emprendimiento provee metodologías y técnicas para tomar esas decisiones;

- **Minimizar sorpresas y pérdidas operacionales:** las entidades han enriquecido la capacidad para identificar eventos potenciales, valorar el riesgo y establecer respuestas, reduciendo por consiguiente la ocurrencia de sorpresas y de los costos o pérdidas relacionados;

- **Identificar y administrar los riesgos a través del emprendimiento:** muchas entidades enfrentan una miríada de riesgos que afectan las diversas partes de la organización. La administración requiere no solo administrar los riesgos individuales, sino también entender los impactos interrelacionados;

- **Proveer respuestas integradas para los riesgos múltiples:** los procesos de negocio conllevan muchos riesgos inherentes, y la administración de riesgos del emprendimiento permite soluciones integradas para administrar los riesgos;

- **Sopesar oportunidades:** la administración considera los eventos potenciales, más que solamente los riesgos, y mediante el considerar un rango completo de eventos, la administración obtiene un entendimiento de cómo ciertos eventos representan oportunidades; y

- **Racionalizar el capital:** información más robusta sobre el riesgo total de la entidad le permite a la administración evaluar más efectivamente las necesidades de capital y mejorar la asignación de capital.

La administración de riesgos del emprendimiento no es un fin en sí misma, sino más aún, un medio importante. No opera y no puede hacerlo aislada de una entidad, sino que es un facilitador para los procesos de la administración. La administración de riesgos del emprendimiento se interrelaciona con el gobierno corporativo proveyendo información a la junta de directores sobre los riesgos más significantes y sobre cómo están siendo administrados. Y, se interrelaciona con la administración del desempeño proveyendo medidas ajustadas al riesgo, y con el control interno, el cual es parte integral de la administración de riesgos del emprendimiento.

La administración de riesgos del emprendimiento le ayuda a una entidad a lograr sus objetivos, y a prevenir la pérdida de recursos. Ayuda a asegurar una efectiva presentación de reportes. Y, ayuda a asegurar que la entidad cumple con las leyes y regulaciones, evitando daños a su reputación y otras consecuencias. En resumen, le ayuda a una entidad a ir a donde desea y a evitar equivocaciones y sorpresas en el camino.[28]

3.6 Componentes del ERM

El ERM consta de ocho componentes interrelacionados. Estos, se derivan de la manera como la administración opera un riesgo empresarial y están integrados dentro del proceso administrativo. Estos componentes son:

3.6.1 Entorno interno

Es el fundamento de todos los otros componentes del ERM, creando disciplina y organizando adecuadamente la estructura empresarial, determinando las estrategias y los objetivos, como también estructurando las actividades del negocio e identificando, valorando y actuando sobre los riesgos. Además este componente, influye en el diseño y funcionamiento de las actividades de control, de los sistemas de información y comunicación, y del monitoreo de las operaciones.

---

[28] Ibid., p. 4.

Existen varios elementos importantes que influyen dentro del ambiente interno, los cuales deben seguirse, aplicarse y divulgarse como son los valores éticos de la entidad, la competencia y desarrollo del personal, el estilo de operación de la administración, la manera de asignar autoridad y responsabilidad, la filosofía de la administración del riesgo.

En cuanto a la administración del riesgo empresarial identifica también el apetito que por el riesgo tiene la entidad y la cultura de riesgo, integrándolos con las iniciativas que se plantean en el desarrollo de la aplicación de las prácticas dentro de la administración de riesgos empresariales.

3.6.2 Definición de objetivos

Dentro del contexto de la misión o visión, se establecen objetivos estratégicos, seleccionan estrategias y establecen objetivos relacionados, alineados y vinculados con la estrategia, así como los relacionados con las operaciones que aportan efectividad y eficiencia de las actividades operativas, ayudando a la efectividad en la presentación de reportes o informes internos y externos (financiera y no financiera), como la de cumplir con las leyes y regulaciones aplicables y de sus procedimientos internos determinados.

3.6.3 Identificación de eventos

La alta gerencia reconoce normalmente que existen incertidumbres – que no se puede conocer con certeza cuándo, dónde y cómo ocurrirá un evento, o si ocurrirá su resultado – , existiendo factores internos y externos que afectan la ocurrencia de un evento.

La metodología de identificación de eventos pueden comprender una combinación de técnicas vinculadas con herramientas de apoyo, como la identificación de eventos pasados (cesación de pagos, cambios en los precios, pérdidas por accidentes) y futuros (cambios demográficos, mercados nuevos y acciones de los competidores). Las técnicas que se centran en las planeaciones consideran asuntos como cambios demográficos, mercados nuevos y acciones de los competidores. Potencialmente los eventos tienen un impacto negativo, positivo o de ambos, representando los primeros riesgos inmediatos, mediatos o de largo plazo, los cuales deben ser evaluados dentro del ERM.

Dentro de las metodologías más conocidas para la identificación de eventos, las cuales se han aplicado de parte de varias firmas de auditores y dentro de las metodologías internas de la empresa son las matrices “análisis PETS o GESI”, “análisis FODA o DOFA”, “análisis de las cinco fuerzas” y “matriz de conocimiento del negocio e identificación de riesgos”.

3.6.4 Valoración de riesgos

Le permite a una entidad considerar como los eventos potenciales pueden afectar el logro de los objetivos. La gerencia valora los eventos bajo las perspectivas de probabilidad (la posibilidad de que ocurra un evento) e impacto (su efecto debido a su ocurrencia), con base en datos pasados internos (pueden considerarse de carácter subjetivo) y externos (son más objetivos).

La metodología normalmente comprende una combinación de técnicas cuantitativas y cualitativas. Los hechos que se relacionan directamente con la contabilidad como las captaciones, colocaciones, aportes de capital, donaciones, etc., se les aplican técnicas cuantitativas (riesgo de crédito, competitivo, regulatorio, de operación, liquidez, fiduciario); y cualitativos, cuando los datos no ofrecen precisión (riesgo país, económico, de auditoría, de imagen, de desastres naturales).

3.6.5 Respuesta al riesgo

Identifica y evalúa las posibles respuestas de los riesgos y considera su efecto en la probabilidad y el impacto.

Evalúa las opciones en relación con el apetito del riesgo en la entidad, el costo y su beneficio de la respuesta a los riesgos potenciales, y el grado que más reporta las posibilidades de riesgo. Las respuestas al riesgo caen dentro de las categorías de evitar, reducir, compartir y aceptar el riesgo.

3.6.6 Actividades de control

Son las políticas y los procedimientos que ayudan a asegurar que se están ejecutando de manera apropiada las respuestas al riesgo, hacen parte del proceso mediante el cual una empresa intenta lograr sus objetivos de negocio. Se clasifican en controles generales y de aplicación.

Controles generales representan la infraestructura de la tecnología, seguridad y adquisición de los hardwares; y el desarrollo y mantenimiento de los softwares; y los controles de aplicación aseguran complejidad, exactitud, autorización y validez de la base de datos.

3.6.7 Información y comunicación

Identifica, captura y comunica información de fuentes internas y externas, en una forma y en una franja de tiempo que le permita al personal llevar a cabo sus responsabilidades. La comunicación efectiva también ocurre en un sentido amplio, hacia abajo o a través y hacia arriba en la entidad. En todos los niveles, se requiere información para identificar, valorar y responder a los riesgos, así como para operar y lograr los objetivos.

3.6.8 Monitoreo

Es un proceso que valora tanto la presencia como el funcionamiento de sus componentes y la calidad de su desempeño en el tiempo. Se puede realizar mediante actividades de ongoing o a través de evaluaciones separadas, los dos aseguran que la administración de riesgos continúa aplicándose en todos los niveles y a través. Es una evaluación continua y periódica que hace la gerencia de la eficacia del diseño y operación de la estructura del control interno, para lograr una adecuada identificación del riesgo, de acuerdo a lo planificado, modificando los procedimientos cuando se requiera.

Para un adecuado monitoreo el COSO II estableció las siguientes reglas de monitoreo:

- Obtención de evidencia de que existe una cultura a la identificación del riesgo;
- Si las comunicaciones externas corroboran las internas;

- Si se hacen comparaciones periódicas;
- Si se revisan y se hacen cumplir las recomendaciones de los auditores;
- Si las capacitaciones proporcionan realidad de lograr una cultura del riesgo;
- Si el personal cumple las normas y procedimientos y es cuestionado; y
- Si son confiables y efectivas las actividades de la auditoría interna y externa.

La administración del riesgo empresarial no es estrictamente un proceso serial, donde un componente afecta únicamente al siguiente. Es un proceso multidireccional, interactivo, en el cual prácticamente cualquier componente puede e influye en otro.[29]

3.7 Relación entre objetivos y componentes

Existe una relación directa entre los objetivos, que son lo que una entidad quiere lograr, y los componentes de la administración de riesgos empresariales, que representan lo que se necesita para logarlos. La relación se describe en una matriz tridimensional, en la forma de un cubo.

Las cuatro categorías de objetivos – estrategia, operaciones, presentación de reportes y cumplimiento – se representan mediante columnas verticales, los ocho componentes mediante filas horizontales, y las unidades de una entidad mediante la tercera dimensión. La descripción facilita centrase en la totalidad del ERM de una entidad, o por categoría de objetivos, componentes, unidad de la entidad, o cualquier subconjunto.

---

[29] Estupiñán Gaitán, Op. Cit., p. 121.

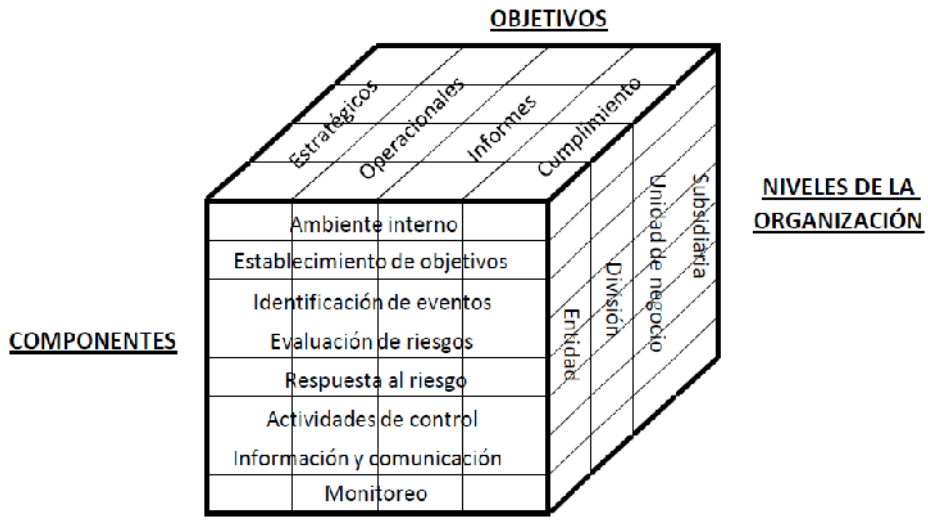


FIGURA No. 1: EL CUBO ERM

Fuente: Rodrigo Estupiñán Gaitán, Administración de Riesgos E.R.M. y la Auditoría Interna. (Bogotá: ECOE Ediciones, 2008).

3.8 Efectividad

Determinar si la administración de riesgos (ERM) de una entidad es "efectiva" constituye un juicio que resulta de una valoración respecto de si los ocho componentes están presentes y funcionan de manera efectiva. Por lo tanto, los componentes también constituyen el criterio para la efectiva administración del ERM. Para que los componentes estén presentes y funcionen de manera apropiada tienen que no existir debilidades materiales, y las necesidades de riesgo tienen que encontrase dentro del apetito que por el riesgo tiene la entidad.

Cuando se determina que la ERM es efectiva en cada una de las cuatro categorías de objetivos, respectivamente, la junta de directores y la administración tiene seguridad razonable de que entienden la extensión en la cual se están logrando los objetivos estratégicos y de operaciones de la entidad, y que la presentación de reportes de la entidad es confiable y se está cumpliendo con las leyes y regulaciones que son aplicables.

Los ocho componentes no funcionarán de manera idéntica en todas las entidades. Por ejemplo, la aplicación en las entidades de tamaño pequeño y mediano puede ser menos

formal y menos estructurada. Sin embargo, aún así las entidades pequeñas pueden tener efectiva administración de riesgo del emprendimiento, en la medida en que los componentes estén presentes y funciones de manera apropiada.

3.9 Limitaciones

Si bien la ERM provee beneficios importantes, existen limitaciones a causa de las realidades de que en la toma de decisiones pueden fallar los juicios humanos, las decisiones sobre como responder al riesgo y como establecer controles requieren considerar los costos y beneficios relacionados, pueden ocurrir interrupciones a causa de fallas humanas tales como errores o equivocaciones simples, los controles pueden ser eludidos por colusión de dos o más personas, y la administración tiene la capacidad de pasar por encima de las decisiones de la ERM. Esas limitaciones imposibilitan que una junta y la administración tengan seguridad absoluta respecto del logro de los objetivos de la entidad.

3.10 Conocimiento del negocio para la detección del riesgo

Con el propósito de implementar una metodología para el conocimiento del negocio y la detección de riesgo, se viene utilizando por parte de auditores externos e internos unas matrices fundamentales establecidas con base en hechos económicos externos o de su entorno e internos, así como de los sistemas de información generales como de control interno y contables.

Se utilizan tres matrices, la del entorno denominada “Análisis GESI o PETS”, “Análisis FODA o DOFA” que identifica factores internos (fortalezas y debilidades) y externos (oportunidades y amenazas), como la filosofía de Michael Porter del “Análisis de las cinco fuerzas”.

3.10.1 Análisis GESI o PETS

Sirve para determinar los riesgos que afectan a una empresa de su entorno, dentro de los ambientes Políticos o Gubernamentales, Económicos, Tecnológicos o Informáticos y Sociales. Para su estudio se identifican los siguientes factores:

CUADRO No. 4: FACTORES DEL ANÁLISIS GESI O PETS

FACTORES GUBERNAMENTALES O POLÍTICOS • Regulaciones de la industria • Legislación social • Aranceles • Impuestos	**FACTORES ECONÓMICOS** • Inflación • Tasas de interés • Desempleo • Tasas de cambio • Gastos del consumidor
FACTORES INFORMÁTICOS O TECNOLÓGICOS • Información / comunicaciones • Sistemas de computación • Producción • Distribución	**FACTORES SOCIALES** • Crecimiento / cambio de la población • Trabajo / tiempo libre / calidad de vida • Salud / educación / bienestar

Fuente: Rodrigo Estupiñán Gaitán, Administración de Riesgos E.R.M. y la Auditoría Interna. (Bogotá: ECOE Ediciones, 2008), p. 159.

3.10.2 Análisis FODA o DOFA

Ayuda a identificar las circunstancias internas o externas dependiendo de la capacidad de la empresa para explotarlas, aprovecharlas o corregirlas como son las de carácter interno las oportunidades y las amenazas, así como las externas que son las debilidades y fortalezas.

Las circunstancias externas pueden presentar oportunidades y amenazas para la empresa dependiendo la capacidad para explotarlas. Las oportunidades deben reconocerse y tomarse medidas para manejarlas, de no hacerse la organización puede sufrir graves consecuencias. Dentro de las oportunidades y amenazas se deben considerar los siguientes factores:

CUADRO No. 5: FACTORES A CONSIDERAR DENTRO DE LAS OPORTUNIDADES Y AMENAZAS

FACTORES A CONSIDERAR		
MERCADO • Crecimiento • Declive • Cambio de moda	**TECNOLOGÍA** • Desarrollo de productos • Sustitución • Nueva tecnología	**ECONOMÍA** • Inflación o deflación • Recesión • Fortaleza de la moneda
LEGISLACIÓN • Contaminación ambiental • Protección consumidores • Responsabilidad sobre productos • Impuestos	**SOCIEDAD** • Prácticas de venta • Prácticas de empleo • Prácticas de sindicatos	**ECOLOGÍA** • Políticas con respecto a energía • Reciclaje • Protección ambiental

Fuente: Rodrigo Estupiñán Gaitán, Administración de Riesgos E.R.M. y la Auditoría Interna. (Bogotá: ECOE Ediciones, 2008), p. 160.

Las circunstancias internas representan debilidades y las fortalezas de una entidad. Es necesario reconocer las fortalezas sobre las cuales resultan los éxitos y determinarse claramente las debilidades para corregirlas oportunamente.

CUADRO No. 6: FACTORES A CONSIDERAR DENTRO DE LAS DEBILIDADES Y FORTALEZAS

FACTORES A CONSIDERAR		
PERSONAL • Habilidades • Entrenamiento • Actitud	**ORGANIZACIÓN** • Estructura • Normatividad interna • Ambiente de control	**PRODUCTOS** • Calidad • Vida útil • Costos
PRODUCCIÓN • Naturaleza • Capacidad • Calidad	**FINANZAS** • Disponibilidad • Credibilidad entidades financieras • Socios comprometidos capital	**PLUSVALÍA** • Reputación • Fama • Percepción de los clientes
	CONOCIMIENTOS • Técnicos • Mercado • Competencia	

Fuente: Rodrigo Estupiñán Gaitán, Administración de Riesgos E.R.M. y la Auditoría Interna. (Bogotá: ECOE Ediciones, 2008), p. 161.

3.10.3 Análisis de las cinco fuerzas

El punto de vista de Porter es que existen cinco fuerzas que determinan las consecuencias de rentabilidad a largo plazo de un mercado o de algún segmento de éste. La idea es que la corporación debe evaluar sus objetivos y recursos frente a éstas cinco fuerzas que rigen la competencia industrial:

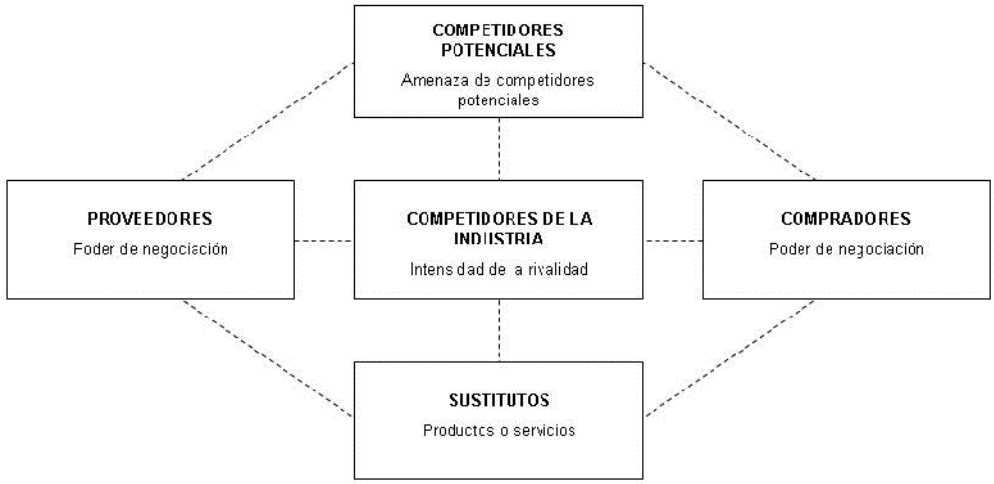


FIGURA No. 2: ANÁLISIS DE LAS CINCO FUERZAS DE PORTER

Fuente: Rodrigo Estupiñán Gaitán, Administración de Riesgos E.R.M. y la Auditoría Interna. (Bogotá: ECOE Ediciones, 2008), p. 161.

a) Amenaza de entrada de nuevos competidores

El mercado o el segmento del mercado, es atractivo o no dependiendo de la complicidad de los productos, por ejemplo fórmulas secretas, calidad del producto, etc., para que nuevos competidores puedan entrar con nuevos recursos y capacidades para apoderarse de una porción del mercado.

b) La rivalidad entre los competidores

Para una empresa le será más difícil competir en un mercado o en uno de sus segmentos, donde los competidores estén muy bien posicionados, sean muy numerosos y los costos fijos sean bajos, pues constantemente estará enfrentada a guerras de precios, campañas publicitarias agresivas, promociones y entrada de nuevos productos.

c) Poder de negociación de los proveedores

Un mercado o segmento del mercado no será atractivo cuando los proveedores estén muy bien organizados monopolíticamente, no exista control de precios por parte del gobierno, tengan fuertes recursos y puedan imponer sus condiciones de precio y tamaño

del pedido. La situación será aún más complicada si los insumos que suministran son claves para la empresa, no tengan sustitutos claros, sean pocos y además de alto costo.

d) Poder de negociación de los compradores

Un mercado o segmento no será atractivo cuando el producto o productos para los clientes, tengan varios o muchos sustitutos, el producto no se diferencie mucho de otros y que sea de bajo costo, lo que permitiría que ellos puedan hacer sustituciones por igual o a muy bajo costo. Otro problema fundamental es cuando sus clientes tienen posibilidad de organizarse para exigir reducción de precios, mayor calidad y servicios, lo que llevaría a una empresa a disminuir sus márgenes de utilidad.

e) Amenaza de ingreso de productos o servicios sustitutos

Un mercado o segmento no es atractivo si existen productos o servicios sustitutos reales o potenciales y más aún cuando los sustitutos están más avanzados tecnológicamente o pueden entrar a precios más bajos reduciendo los márgenes de utilidad de la empresa y de la industria en general.

Para evaluar las incidencias de cada fuerza, se deben considerar los aspectos anteriores y otros, los cuales se presentan ordenados en el siguiente cuadro integral para que el investigador o analista puedan identificarlos de manera más fácil.[30]

CUADRO No. 7: ASPECTOS A CONSIDERAR EN CADA FUERZA

ASPECTOS A CONSIDERAR
COMPETIDORES POTENCIALES • Economías de escala • Identidad de marcas • Requerimientos de capital • Obstáculos de salida • Represalia previsible • Ventajas absolutas de costo • Curva de aprendizaje para los competidores potenciales • Diseños de productos de bajo costo • Acceso a información necesaria • Políticas gubernamentales
PODER DE LOS PROVEEDORES • Diferencias en los suministros • Costos cambiantes de los proveedores y las firmas en la industria

[30] Ibid., p. 147.

• Presencia de los proveedores • Concentración de proveedores • Importancia de los proveedores • Costo relativo al total de las compras en la industria • Efecto de los insumos en el costo o en la diferencia
AMENAZA DE PRODUCTOS / SERVICIOS DE SUSTITUCIÓN
• Precio / calidad relativa del sustituto • Costos de intercambio • Propensión del comprador a sustituir • Velocidad de cambio de productos • Nivel de investigación y desarrollo
PODER DE NEGOCIACIÓN DE LOS COMPRADORES
• Concentración de compradores • Volumen de los compradores • Costos de sustitución de compradores • Capacidad para sustituir productos • precio / total de las compras • Diferencia de los productos • Identidad de las marcas • Efecto de calidad / desempeño • Rentabilidad del comprador / fortaleza financiera • Incentivos de los que toman decisiones
COMPETENCIA
• Crecimiento de la industria • Costos fijos / valor agregado • Sobrecapacidad de producción intermitente • Diferencia de los productos • Identidad de las marcas • Diversidad de los miembros de la competencia • Intereses corporativos • Obstáculos para salir del mercado

Fuente: Rodrigo Estupiñán Gaitán, Administración de Riesgos E.R.M. y la Auditoría Interna. (Bogotá: ECOE Ediciones, 2008), p. 161.

3.11 Cambios de paradigmas en auditoría interna

Específicamente para la auditoría interna, por todo lo expuesto, se ha tenido que cambiar algunos paradigmas sobre los cuales se sustentaba el enfoque y ejecución de la auditoría interna hasta hace unos pocos años, siendo uno de los principales cambios el de modificar el enfoque de la auditoría interna basada en los controles por el enfoque de auditoría basada en el riesgo. Este cambio ha implicado a la vez una modificación de fondo en la actitud mental del auditor y en los requerimientos técnicos y de competencias que debe tener para responder satisfactoriamente a los nuevos retos.

CUADRO No. 8: PARADIGMAS QUE SE HAN MODIFICADO EN LA ACTIVIDAD DE LA AUDITORÍA INTERNA

CARACTERISTICAS	ANTIGUO PARADIGMA	NUEVO PARADIGMA
Enfoque de la AI	Control interno.	Riesgos del negocio.
Respuesta	Reactiva, posterior a los hechos. Observadores de las iniciativas del plan estratégico.	Proactiva, en tiempo real. Monitoreo continuo y participación en el proceso del plan estratégico.
Pruebas de AI	Importancia de los controles	Importancia de los riesgos
Métodos de AI	Énfasis en integridad de la evaluación de controles Detallados.	Énfasis en la importancia de una significativa cobertura de los riesgos del negocio.
Recomendaciones de AI	Controles Internos: -Fortalezas/ debilidades -Costo/beneficio -Eficiencia/ efectividad	Manejo del riesgo: -Evitarlos/diversificados -Repartición/transferencia -Controlarlos/aceptarlos
Informes de AI	Dirigidos hacia la funcionalidad de los controles.	Dirigidos hacia el proceso de riesgos.
Rol de la AI en la organización	Función de evaluación independiente de los controles internos.	Integración en el manejo del riesgo y comunicación constante con la dirección.

Fuente: Rodrigo Estupiñán Gaitán, El Riesgo en el Nuevo Enfoque de la Auditoría Interna. (Bogotá: El Autor), p. 46.

Las implicaciones de los nuevos paradigmas son de gran importancia, se cambió el enfoque de la auditoría hacia el pasado por un enfoque hacia situaciones presentes y futuras, a través del análisis de detalles y hechos del pasado. Con el enfoque sobre riesgos presentes y sobre futuras transacciones, el auditor está trabajando en un nivel que está por encima de los detalles y se proyecta hacia la generación de recomendaciones de alto valor agregado. El nuevo auditor requiere desarrollarse en aspectos relacionados con la visión de los negocios, planeación con base en riesgos y habilidades de comunicación.

En conclusión, el nuevo auditor debe moverse del tradicional enfoque financiero y contable hacia el enfoque de negocios y de sus riesgos asociados, considerando los aspectos financieros y contables como una parte del proceso de revisión y no como una finalidad de su trabajo.[31]

3.12 Marco de la administración de riesgos empresariales

- El gobierno corporativo se requiere para asegurarse de que la junta directiva y la gerencia hayan establecido los procesos organizacionales apropiados y los

[31] Ibid., p. 26.

controles corporativos para medir y para manejar los riesgos a través de la empresa;

- La creación y el mantenimiento de un sistema sólido de control interno se requiere para salvaguardar la inversión del accionista y los activos de la empresa;

- Un recurso específico se debe identificar para implementar los controles internos con suficiente conocimiento y experiencia que genere el máximo beneficio del proceso;

- Se requiere un claro proceso de administración de riesgos que establezca los procesos individuales, sus aportaciones, sus resultados, sus limitantes y sus responsables; y

- El valor de un proceso de administración de riesgos se reduce sin una clara comprensión de los orígenes del riesgo y a cómo deben ser respondidos. El marco separa los orígenes del riesgo en dos elementos clave, denominándolos procesos internos y el entorno donde opera la empresa.

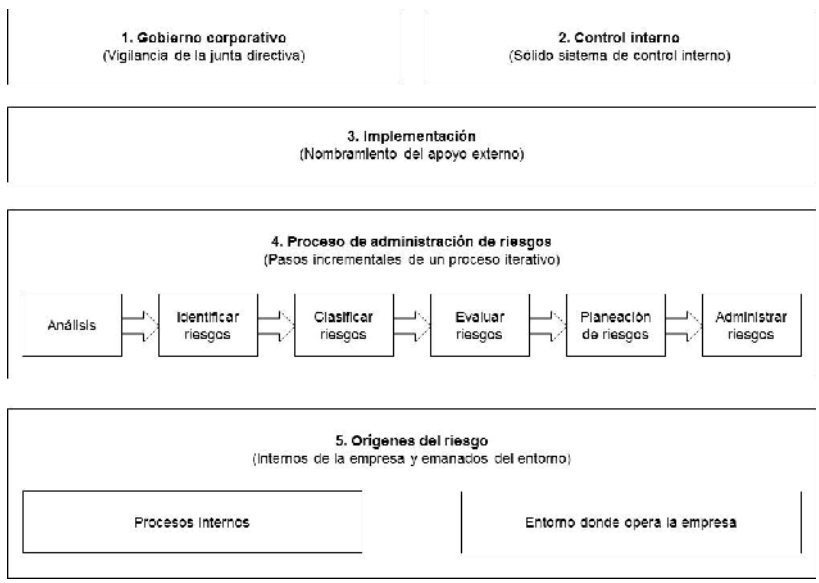


FIGURA No. 3: MARCO DE LA ADMINISTRACIÓN DE RIESGOS EMPRESARIALES

Fuente: Aleida González-Cueto Longres y Manuel Pando Franco. La Administración de Riesgos Empresarial en el contexto actual de Control Interno [en línea]. Consultado el 21 de julio de 2009. Disponible en: http://www.nodo50.org/cubasigloXXI/economia/gcueto_311206.pdf

3.12.1 Gobierno corporativo

Una revisión de las recientes investigaciones sobre el gobierno corporativo, revelan que es un catalizador para la administración de riesgos empresarial y es también en gran medida el contribuyente principal a sus actuales responsabilidades.

Esto explica las expectativas que los accionistas tienen de sus juntas directivas. Revela las posturas que las compañías han adoptado hacia a la administración de riesgos y el gran impulso que ha recibido la práctica de la administración de riesgos. Actualmente el gobierno corporativo se ha convertido un componente esencial de la administración de riesgo empresarial porque proporciona monitoreo integral de la empresa y aplica la administración del riesgo. Además establece la responsabilidad en la junta directiva de asegurar el adecuado funcionamiento de los sistemas y las políticas para la administración de riesgos. La utilización de prácticas transparentes de la junta directiva y un sólido gobierno corporativo son cruciales para una efectiva administración de riesgos empresarial.

3.12.2 Control interno

La evaluación de los controles internos proporciona un entendimiento de qué debe ser controlado y de cómo. Hay más de un punto de vista en los enfoques formales. Los controles internos son un subconjunto de gobierno corporativo y la administración de riesgos es un subconjunto de controles internos. Por lo que la administración de riesgos esta dirigida a: facilitar la efectiva y eficiente operación de un negocio, mejorando los informes internos y externos, favoreciendo el cumplimiento de las leyes y regulaciones. Su objetivo es lograr esto a través de la identificación y la evaluación de los riesgos a los que hace frente al negocio, para removerlos, o reducirlos, o cuando sea necesario transferirlos a terceros, cuando sea económicamente factible hacerlo.

3.12.3 Implementación

La puesta en práctica de la administración de riesgos (que forma la parte de los procesos del control interno de un negocio) puede ser realizados internamente en una empresa o puede ser apoyada por consultores externos. Ambas formas son normalmente

aceptables. Cualquiera de ellas puede ser seleccionada; los parámetros del estudio tienen que ser localizados en un mapa de riesgos, deben ser comunicados y ser aceptados de acuerdo con los tiempos establecidos; los recursos, los costos, las contribuciones y las personas responsables deben ser establecidos.

3.12.4 Proceso de administración de riesgos

Una manera de explorar los mecanismos para implementar un proceso de administración de riesgos es descomponerlo en todas sus partes y examinar que tanto debería contribuir cada parte a todo el conjunto. Aquí se propone que el proceso de administración de riesgos se divida en seis procesos llamados: análisis, identificación, clasificación, evaluación, planeación y administración. Muchas de las actividades siguen un patrón en gran parte secuencial, pero puede ser un proceso altamente iterativo. Al identificar los nuevos riesgos, el anterior proceso de la identificación y su clasificación se revisan, por lo que el proceso secuencial se repite a través de la implementación de las acciones de respuesta al riesgo.

3.12.5 Orígenes del riesgo

Una manera de examinar los orígenes del riesgo del negocio es considerar que emana a partir de dos sectores, de dentro de un negocio (referente a las acciones toma) y del ambiente dentro del que opera, sobre el cual, aparentemente, no tiene ningún control. En la Figura 3, estas fuentes se han denominado “procesos internos” y “entorno donde opera la empresa”. Estos son un desarrollo del análisis tradicional del PEST (por sus siglas en inglés Polítical, Economic, Social y Technological, para las influencias externas).[32]

---

[32] Aleida González-Cueto Longres y Manuel Pando Franco. La Administración de Riesgos Empresarial en el contexto actual de Control Interno [en línea]. Consultado el 21 de julio de 2009. Disponible en: http://www.nodo50.org/cubasigloXXI/economia/gcueto_311206.pdf

CAPÍTULO IV
PROCESO DE ADMINISTRACIÓN DE RIESGOS

4.1 Plan de administración de riesgos

La cantidad de pasos requeridos para implementar una administración eficaz de riesgos dentro de una organización. Dependiendo de la filosofía, cultura y estructura general de administración de riesgos de la organización, podría ser posible combinar algunos pasos. Sin embargo, todos los pasos deberían recibir consideración.

El plan debería procurar satisfacer los propósitos y objetivos del sistema de administración de riesgos y debería procurar lograr los objetivos de la declaración de política de administración de riesgos.

Finalmente, la intención debería ser incorporar el proceso de administración de riesgos en todas las prácticas y procesos de negocio críticos de la organización de tal forma que sea relevante, eficaz y sustentable. El plan de administración de riesgos debería tener a esto como su objetivo primario.

4.1.1 Asegurar el apoyo de la alta gerencia

Desarrollar una filosofía organizacional de administración de riesgos y concientización de riesgos a nivel de alta gerencia. Esto podría verse facilitado mediante entrenamiento, educación y resúmenes para los gerentes senior. Esto incluye:

- Obtener el apoyo activo y vigente de los directores y ejecutivos senior de la organización para la administración de riesgos y para el desarrollo e implementación de un plan;

- Designar un gerente senior o similar ‘campeón’ (o equipo) para liderar y patrocinar las iniciativas;

- Obtener la aprobación y apoyo de todos los gerentes senior para la ejecución de un plan de administración de riesgos; y

- Obtener el apoyo a la política y al plan de administración de riesgos por parte del Directorio y/o su comité delegado.

4.1.2 Desarrollar la política de administración de riesgos

El ejecutivo de la organización debería definir y documentar su política para administrar los riesgos, incluyendo sus objetivos y su compromiso con la administración de riesgos. La política de administración de riesgos debería ser relevante para el contexto estratégico de la organización y para sus metas, objetivos y la naturaleza de su negocio.

La política debería incluir información tal como:

- Los objetivos de la política y los fundamentos para administrar los riesgos;

- Los vínculos entre la política y los planes corporativos y estratégicos de la organización;

- Una expresión del apetito de riesgo en términos del proceso que la organización adoptará al tomar decisiones acerca de la tolerancia a los riesgos;

- La amplitud, o rango de aspectos de los riesgos, a los cuales se aplica la política;

- Los procesos a ser utilizados para administrar los riesgos;

- Los responsables por administrar riesgos particulares;

- El apoyo y la pericia disponibles para asistir a los responsables por administrar los riesgos;

- La declaración sobre cómo se medirá y reportará el desempeño del proceso de administración de riesgos para brindar confianza a los directores y ejecutivos senior;

- Un compromiso por la revisión periódica del sistema de administración de riesgos; y

- Una declaración de compromiso de los directores y ejecutivos senior respecto de la política.

La publicación de una declaración de política de esta naturaleza es también esencial para mostrar el compromiso de los directores y ejecutivos senior con el proceso de planeamiento e implementación.

4.1.3 Comunicar la política

Desarrollar, establecer e implementar una infraestructura y las medidas que aseguren que la administración de riesgos quede incorporada en los procesos de planificación, administración y toma de decisiones y en la cultura general de la organización.

Esto podría incluir:

- Establecer un equipo, incluyendo personal de alta gerencia, como responsables por las comunicaciones internas sobre la política;

- Procurar la toma de conciencia sobre la administración de riesgos y el proceso de administración de riesgos;

- Comunicación y diálogo en toda la empresa acerca de la administración de riesgos y sobre la política de la organización al respecto;

- Desarrollar destrezas sobre administración de riesgos en el personal mediante educación y entrenamiento;

- Asegurar niveles apropiados de reconocimiento, recompensas, aprobación y sanciones; y

- Establecer procesos de medición de desempeño y elaboración de informes.

4.1.4 Establecer responsabilidad y autoridad

Los directores y ejecutivos senior son los máximos responsables de la organización por la administración de riesgos. Dentro de una organización, todo el personal es responsable por administrar riesgos en sus áreas de control.

Deberían definirse y registrarse las responsabilidades, autoridades e interrelaciones del personal por la administración de riesgos. En particular, deberían ser registrados e informados los responsables por la vigilancia de aspectos particulares de los riesgos, por implementar estrategias de tratamiento y por la conducción de acciones de control de riesgos.

4.1.5 Personalizar el proceso de administración de riesgos

El proceso para la administración de riesgos necesitará ser personalizado a las políticas, procedimientos y cultura de cada organización específica. Como parte de este proceso la organización debería especificar el desempeño y los criterios para juzgar el éxito del proceso de administración de riesgos.

4.1.6 Recursos

La organización debería identificar los requerimientos de recursos y proveer recursos adecuados, incluyendo entrenamiento del personal que aplica el proceso de administración de riesgos y de quienes desempeñan un rol de apoyo, monitoreo y verificación. Esto debería involucrar un análisis de las necesidades de capacitación.

Un recurso importante es un proceso para administrar la información de riesgos que permita:

- Registrar y mostrar cualquier cambio en los perfiles de riesgo;
- Registrar medidas y estrategias para tratamiento de los riesgos;
- Rastrear el progreso y el cumplimiento de las acciones de control de riesgos;
- Permitir medir el progreso respecto del plan de administración de riesgos;
- Asignar y rastrear la responsabilidad por los riesgos, las medidas de tratamiento y las acciones de control;
- Iniciar la actividad de monitoreo y aseguramiento; y
- Proveer un medio para la medición y reporte de la actividad de administración de riesgos.

4.1.7 Monitorear y revisar

Los riesgos no son estáticos y las organizaciones deberían adoptar e incorporar procesos dinámicos para administrarlos.

Esto debería incluir el desarrollo de mecanismos para revisar los riesgos y para su evaluación y tratamiento. Debería también monitorear la eficacia del proceso de administración de riesgos en si mismo.

4.2 Modelo de administración del riesgo

La administración de riesgos es un proceso lógico y sistemático que puede ser utilizado cuando se toman decisiones para mejorar la efectividad y eficiencia.

Cuando administramos el riesgo, tratamos de identificar y estar preparados para lo que puede suceder, se trata de tomar acciones destinadas a eludir y reducir la exposición a los costos u otros efectos de aquellos eventos que ocurran, en lugar de reaccionar después de que un evento ya ha ocurrido e incurrir en los costos que implican recuperar una situación.

Para realizar una eficaz administración de riesgos, se desarrollan diferentes métodos, entre los cuales tenemos el Estándar Australiano/Neozelandés el cual fue creado por el Comité OB-007 de la junta de estándares de Australia y Nueva Zelanda sobre administración de riesgos.

De acuerdo con éste método los objetivos son los siguientes:

- Proveer un marco conceptual genérico para es establecimiento del contexto;
- Identificación del riesgo;
- Análisis del riesgo;
- Evaluación del riesgo;
- Tratamiento del riesgo; y
- Monitoreo y comunicación del riesgo.

4.3 Proceso de administración del riesgo

4.3.1 Definición del contexto

Para la formulación y operacionalización de la política de administración del riesgo es fundamental tener claridad de la misión institucional, sus objetivos y tener una visión sistémica de la gestión de manera que no se perciba esta herramienta gerencial como algo aislado del mismo accionar administrativo. Por ende, el diseño se establece a partir de la identificación de los factores internos o externos a la entidad que pueden generar riesgos que afecten el cumplimiento de sus objetivos.

Este contexto estratégico es la base para la identificación de los riesgos en los procesos y actividades, el análisis se realiza a partir del conocimiento de situaciones del entorno de la entidad, tanto de carácter social, económico, cultural, de orden público, político, legal y /o cambios tecnológicos, entre otros; se alimenta también con el análisis de la situación actual de la entidad, basado en los resultados de los componentes de ambiente de control, estructura organizacional, modelo de operación, cumplimiento de los planes y programas, sistemas de información, procesos y procedimientos y los recursos económicos, entre otros.

Se recomienda la aplicación de varias herramientas y técnicas como por ejemplo: entrevistas estructuradas con expertos en el área de interés, reuniones con directivos y con personas de todos los niveles en la entidad, evaluaciones individuales usando cuestionarios, lluvias de ideas con los servidores de la entidad, entrevistas e indagaciones con personas ajenas a la entidad, usar diagramas de flujo, causa y efecto, análisis de

escenarios y hacer revisiones periódicas de factores económicos y tecnológicos que puedan afectar la organización, entre otros.

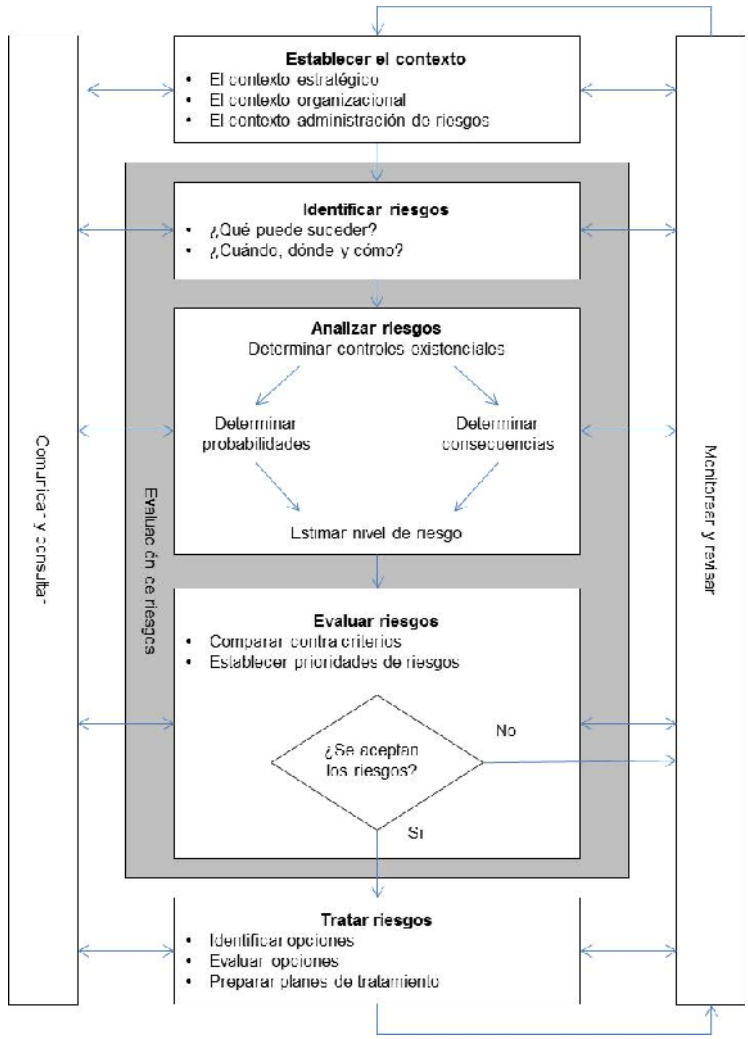


FIGURA No. 4: PROCESO DE ADMINISTRACIÓN DE RIESGOS

Fuente: Comité Conjunto de Estándares Australia/Estándares Nueva Zelanda. Administración de Riesgos, Borrador para Comentario Público [en línea]. Consultado el 13 de septiembre de 2009. Disponible en: http://www.netconsul.com/riesgos/Modificacion4360.pdf

Igualmente pueden utilizarse diferentes fuentes de información de la entidad, tales como registros históricos, experiencias significativas registradas, opiniones de especialistas y expertos, informes de años anteriores, los cuales pueden proporcionar información importante, la técnica utilizada dependerá de las necesidades y naturaleza de la entidad.

Con la realización de esta etapa se busca que la entidad obtenga los siguientes resultados:

- Identificar los factores externos que pueden ocasionar la presencia de riesgos, con base en el análisis de la información externa y los planes y programas de la entidad;

- Identificar los factores internos que pueden ocasionar la presencia de riesgos con base en el análisis de los componentes ambiente de control, direccionamiento estratégico y demás estudios que sobre la cultura organizacional y el clima laboral se hayan adelantado en la entidad; y

- Aportar información que facilite y enriquezca las demás etapas de la administración del riesgo.

4.3.2 Identificación de riesgos

El proceso de la identificación del riesgo debe ser permanente e interactivo basado en el resultado del análisis del contexto estratégico, en el proceso de planeación y debe partir de la claridad de los objetivos estratégicos de la entidad para la obtención de resultados.

Una manera para que todos los servidores de la entidad conozcan y visualicen los riesgos, es a través de la utilización del formato de identificación de riesgos el cual permite hacer un inventario de los mismos, definiendo en primera instancia las causas o factores de riesgo, tanto internos como externos, presentando una descripción de cada uno de estos y finalmente definiendo los posibles efectos. Es importante centrarse en los riesgos más significativos para la entidad relacionados con el desarrollo de los procesos y los objetivos institucionales. Es allí donde, al igual que todos los servidores, la gerencia pública adopta un papel proactivo en el sentido de visualizar en sus contextos estratégicos y misionales los factores o eventos que pueden afectar el curso institucional, dada la especialidad temática que manejan en cada sector o contexto socioeconómico.

Entender la importancia del manejo del riesgo implica conocer con más detalle los siguientes conceptos:

- **Proceso:** nombre del proceso;

- **Objetivo del proceso:** se debe transcribir el objetivo que se ha definido para el proceso al cual se le están identificando los riesgos;

- **Riesgo:** representa la posibilidad de ocurrencia de un evento que pueda entorpecer el normal desarrollo de las funciones de la entidad y afectar el logro de sus objetivos;

- **Causas (factores internos o externos):** son los medios, las circunstancias y agentes generadores de riesgo. Los agentes generadores que se entienden como todos los sujetos u objetos que tienen la capacidad de originar un riesgo; se pueden clasificar en cinco categorías: personas, materiales, comités, instalaciones y entorno;

- **Descripción:** se refiere a las características generales o las formas en que se observa o manifiesta el riesgo identificado; y

- **Efectos (consecuencias):** constituyen las consecuencias de la ocurrencia del riesgo sobre los objetivos de la entidad; generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como: daños físicos, fallecimiento, sanciones, pérdidas económicas, de información, de bienes, de imagen, de credibilidad y de confianza, interrupción del servicio y daño ambiental.

Para una mejor comprensión observar el siguiente cuadro.

CUADRO No. 9: FORMATO DE IDENTIFICACIÓN DE RIESGOS

PROCESO:			
OBJETIVO DEL PROCESO:			
CAUSAS	**RIESGO**	**DESCRIPCIÓN**	**EFECTOS**

Fuente: Universidad Nacional de Colombia. Guía Básica de Administración de Riesgos. (Bogotá: Editorial Universitaria, s.a.), p. 8.

Durante el proceso de identificación del riesgo se recomienda tener en cuenta la clasificación de los mismos según los tipos de riesgos.

Con la realización de esta etapa se busca que la entidad obtenga los siguientes resultados:

- Determinar las causas (factores internos o externos) de las situaciones identificadas como riesgos para la entidad;
- Describir los riesgos identificados con sus características; y
- Precisar los efectos que los riesgos puedan ocasionar a la entidad.

4.3.3 Análisis del riesgo

El análisis del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y evaluándolos con el fin de obtener información para establecer el nivel de riesgo y las acciones que se van a implementar. El análisis del riesgo dependerá de la información obtenida en el formato de identificación de riesgos y la disponibilidad de datos históricos y aportes de los servidores de la entidad.

Se han establecido dos aspectos a tener en cuenta en el análisis de los riesgos identificados, probabilidad e impacto. La probabilidad puede ser medida con criterios de frecuencia, si se ha materializado (por ejemplo: número de veces en un tiempo determinado), o de factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado. Por impacto se entiende el grado en que las consecuencias o efectos puede perjudicar a la organización si se materialización del riesgo.

Para adelantar el análisis del riesgo se deben considerar los siguientes aspectos:

a) La calificación del riesgo

Se logra a través de la estimación de la probabilidad de su ocurrencia y el impacto que puede causar la materialización del riesgo. La primera representa el número de veces que el riesgo se ha presentado en un determinado tiempo o puede presentarse, y la segunda

se refiere a la magnitud de sus efectos. Los criterios para la calificación son subjetivos, podemos utilizar unas tablas como en el Cuadro No. 10.

CUADRO No. 10: CRITERIO PARA CALIFICACIÓN DE PROBABILIDAD E IMPACTO

VALOR DE PROBABILIDAD	NIVEL DE PROBABILIDAD	DESCRIPCIÓN
1	Bajo (raro)	Puede ocurrir solo en circunstancias excepcionales (una vez entre 10 y 20 años)
2	Medio (posible)	Es posible que ocurra algunas veces (1 vez entre 1 y 3 años)
3	Alto (casi cierto)	Se espera que ocurra en la mayoría de las circunstancias (mas de 10 casos al año)

VALOR DE IMPACTO	NIVEL DE IMPACTO	DESCRIPCIÓN
5	Leve	Perdidas insignificantes, menor grado de incumplimiento en metas y objetivos
10	Moderado	Perdidas considerables, posibilidad de un alto grado de incumplimiento en metas y objetivos
20	Catastrófico	Perdidas enormes, daño en la imagen de la entidad, alto grado de incumplimiento en metas y objetivos

Fuente: Universidad Nacional de Colombia. Guía Básica de Administración de Riesgos. (Bogotá: Editorial Universitaria, s.a.), p. 9.

b) La evaluación del riesgo

Permite comparar los resultados de su calificación, con los criterios definidos para establecer el grado de exposición de la entidad al riesgo; de esta forma es posible distinguir entre los riesgos aceptables, tolerables, moderados, importantes o inaceptables y fijar las prioridades de las acciones requeridas para su tratamiento. Con el fin de facilitar la calificación y evaluación a los riesgos, a continuación se presenta una matriz que contempla un análisis cualitativo, que hace referencia a la utilización de formas descriptivas para presentar la magnitud de las consecuencias potenciales (impacto) y la posibilidad de ocurrencia (probabilidad). Tomando las siguientes categorías: leve, moderada y catastrófica en relación con el impacto y alta, media y baja respecto a la probabilidad.

Así mismo, presenta un análisis cuantitativo, que contempla valores numéricos que contribuyen a la calidad en la exactitud de la calificación y evaluación de los riesgos.

Tanto para el impacto como para la probabilidad se han determinado valores múltiplos de 5. La forma en la cual la probabilidad y el impacto son expresados y combinados en la matriz provee la evaluación del riesgo (Ver Cuadro 11).

CUADRO No. 11: MATRIZ DE CALIFICACIÓN, EVALUACIÓN Y RESPUESTA A LOS RIESGOS

Probabilidad	Valor			
Alta	3	15 *Zona de riesgo Moderado* Evitar el riesgo	*30* *Zona de riesgo Importante* Reducir el riesgo Evitar el riesgo Compartir o transferir	60 *Zona de riesgo Inaceptable* Evitar el riesgo Reducir el riesgo Compartir o transferir
Media	2	10 *Zona de riesgo Tolerable* Asumir el riesgo Reducir el riesgo	20 *Zona de riesgo Moderado* Reducir el riesgo Evitar el riesgo Compartir o transferir	*40* *Zona de riesgo Importante* Reducir el riesgo Evitar el riesgo Compartir o transferir
Baja	1	5 *Zona de riesgo Aceptable* Asumir el riesgo	10 *Zona de riesgo Tolerable* Asumir el riesgo Reducir el riesgo	20 *Zona de riesgo Moderado* Reducir el riesgo Compartir o transferir
	Impacto	Leve	Moderado	Catastrófica
	Valor	5	10	20

Fuente: Universidad Nacional de Colombia. Guía Básica de Administración de Riesgos. (Bogotá: Editorial Universitaria, s.a.), p. 10.

Para realizar la evaluación del riesgo se debe tener en cuenta la posición del riesgo en la matriz, según la celda que ocupa, aplicando los siguientes criterios:

Si el riesgo se ubica en la zona de riesgo aceptable (calificación 5), significa que su probabilidad es baja y su impacto es leve, lo cual permite a la Entidad asumirlo, es decir, el riesgo se encuentra en un nivel que puede aceptarlo sin necesidad de tomar otras medidas de control diferentes a las que se poseen.

Si el riesgo se ubica en la zona de riesgo inaceptable (calificación 60), su probabilidad es alta y su impacto catastrófico, por tanto es aconsejable eliminar la causa que genera el riesgo en la medida que sea posible, de lo contrario se deben implementar controles de prevención para evitar la probabilidad del riesgo, de protección para disminuir el impacto o compartir o transferir el riesgo si es posible a través de pólizas de seguros u otras opciones que estén disponibles.

Si el riesgo se sitúa en cualquiera de las otras zonas (riesgo tolerable, moderado o importante) se deben tomar medidas para llevar los riesgos a la zona aceptable o tolerable, en lo posible. Las medidas dependen de la celda en la cual se ubica el riesgo, así: los riesgos de impacto leve y probabilidad alta se previenen; los riesgos con impacto moderado y probabilidad leve, se reduce o se comparte el riesgo, si es posible; también es viable combinar estas medidas con evitar el riesgo cuando éste presente una probabilidad alta y media, y el impacto sea moderado o catastrófico.

Cuando la probabilidad del riesgo sea media y su impacto leve, se debe realizar un análisis del costo beneficio con el que se pueda decidir entre reducir el riesgo, asumirlo o compartirlo.

Cuando el riesgo tenga una probabilidad baja e impacto catastrófico se debe tratar de compartir el riesgo y evitar la entidad en caso de que éste se presente.

Siempre que el riesgo sea calificado con impacto catastrófico la entidad debe diseñar planes de contingencia, para protegerse en caso de su ocurrencia. Con la realización de esta etapa se busca que la entidad obtenga los siguientes resultados:

- Establecer la probabilidad de ocurrencia de los riesgos, que pueden disminuir la capacidad institucional de la entidad, para cumplir su propósito;

- Medir el impacto las consecuencias del riesgo sobre las personas, los recursos o la coordinación de las acciones necesarias para llevar el logro de los objetivos institucionales o el desarrollo de los procesos; y

- Establecer criterios de calificación y evaluación de los riesgos que permiten tomar decisiones pertinentes sobre su tratamiento.

4.3.4 Valoración del riesgo

La valoración del riesgo es el producto de confrontar los resultados de la evaluación del riesgo con los controles identificados en el elemento de control, denominado “Controles”, del subsistema de control de gestión, con el objetivo de establecer prioridades para su

manejo y fijación de políticas. Para adelantar esta etapa se hace necesario tener claridad sobre los puntos de control existentes en los diferentes procesos, los cuales permiten obtener información para efectos de tomar decisiones.

Para realizar la valoración de los controles existentes es necesario recordar que éstos se clasifican en:

- **Preventivos:** aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización; y

- **Correctivos:** aquellos que permiten el restablecimiento de la actividad después de ser detectado un evento no deseable; también permiten la modificación de las acciones que propiciaron su ocurrencia.

El procedimiento para la valoración del riesgo es el siguiente:

Para adelantar la evaluación de los controles existentes es necesario describirlos estableciendo si son preventivos o correctivos y responder a las siguientes preguntas:

- ¿Los controles están documentados?;
- ¿Se esta aplicando en la actualidad?; y
- ¿Es efectivo para minimizar el riesgo?.

Una vez ha respondido todas las preguntas proceda a realizar la valoración, así:

- Calificados y evaluados los riesgos analícelos frente a los controles existentes en cada riesgo;
- Pondérelos según la tabla establecida, teniendo en cuenta las respuestas a las preguntas anteriormente formuladas (los controles se encuentran documentados, se aplican y son efectivos); y
- Ubique en la matriz de calificación, evaluación y respuesta a los riesgos, el estado final de riesgo, de acuerdo a los resultados obtenidos en la valoración del mismo.

CUADRO No. 12: TABLA DE VALORACIÓN DE CONTROLES

CRITERIOS	VALORACION DE RIESGO
No existen controles	Se mantiene el resultado de la evaluación antes de controles
Los controles existentes no son efectivos	Se mantiene el resultado de la evaluación antes de controles
Los controles existentes son efectivos pero no están documentados	Cambia el resultado a una casilla inferior de la matriz de evaluación antes de controles (el desplazamiento depende de si el control afecta el impacto o la probabilidad)
Los controles existentes son efectivos y están documentados	Pasa a escala inferior, es decir el riesgo pasa a estar en una menor zona de riesgo (el desplazamiento depende de si el control afecta el impacto o la probabilidad)

Fuente: Universidad Nacional de Colombia. Guía Básica de Administración de Riesgos. (Bogotá: Editorial Universitaria, s.a.), p. 13.

Un ejemplo de la determinación del nivel del riesgo y del grado de exposición al mismo:

- **Riesgo:** pérdida de información debido a la entrada de un virus en la red de información de la entidad;

- **Probabilidad:** alta - 3, porque todos los computadores de la entidad están conectados a la red de Internet e Intranet;

- **Impacto:** alto - 20, porque la pérdida de información conllevaría consecuencias graves para el quehacer de la entidad;

- **Evaluación del Riesgo:** de acuerdo a la matriz de calificación y evaluación sería de 60 y se encontraría en la zona de riesgo inaceptable; y

- **Descripción de los controles existentes:**
  - Se hace backup o copias de seguridad, semanalmente. Control preventivo
  - Se vacunan todos los programas y equipos, diariamente. Control preventivo
  - Se guarda la información más relevante fuera de la red en un centro de información. Control preventivo
  - ¿Los controles están documentados? SI
  - ¿Se esta aplicando en la actualidad? SI
  - ¿Es efectivo para minimizar el riesgo? SI

De acuerdo a la tabla se entiende que la valoración del riesgo es: Media y se ubica en la zona moderada 10 debido a la efectividad de los controles existentes, ya que los dos primeros controles apuntan a la disminuir la probabilidad y el último a disminuir el impacto, por lo tanto las acciones que se implementen entrarán a reforzar los controles establecidos y a valorar la efectividad de los mismos.

Con la realización de esta etapa se busca que la entidad obtenga los siguientes resultados:

- Identificación de los controles existentes para los riesgos identificados y analizados;

- Priorización de los riesgos de acuerdo con los resultados obtenidos de confrontar la evaluación del riesgo con los controles existentes, a fin de establecer aquellos que pueden causar mayor impacto a la entidad en caso de materializarse; y

- Elaborar el mapa de riesgos para cada proceso.

4.3.5 Tratamiento de los riesgos

El tratamiento de los riesgos involucra identificar las opciones para tratar los riesgos, evaluar esas opciones (costo-beneficio, viabilidad jurídica, etc.), preparar planes para tratamiento de los riesgos e implementarlos.

Las políticas identifican las opciones para tratar y manejar los riesgos basadas en la valoración de riesgos, permiten tomar decisiones adecuadas y fijar los lineamientos de la administración del riesgo, a su vez transmite la posición de la dirección y establecen las guías de acción necesarias a todos los servidores de la entidad.

Se debe tener en cuenta alguna de las siguientes opciones, las cuales pueden considerarse cada una de ellas independientemente, interrelacionadas o en conjunto:

- **Evitar el riesgo:** tomar las medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a considerar, se logra cuando al interior de los

procesos se generan cambios sustanciales por mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas. Un ejemplo de esto puede ser el control de calidad, manejo de los insumos, mantenimiento preventivo de los equipos, desarrollo tecnológico, etc.;

- **Reducir el riesgo:** implica tomar medidas encaminadas a disminuir tanto la probabilidad (medidas de prevención), como el impacto (medidas de protección). La reducción del riesgo es probablemente el método más sencillo y económico para superar las debilidades antes de aplicar medidas más costosas y difíciles. Se consigue mediante la optimización de los procedimientos y la implementación de controles;

- **Compartir o transferir el riesgo:** reduce su efecto a través del traspaso de las pérdidas a otras organizaciones, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra entidad, como en los contratos a riesgo compartido. Es así como por ejemplo, la información de gran importancia se puede duplicar y almacenar en un lugar distante y de ubicación segura, en vez de dejarla concentrada en un solo lugar; y

- **Asumir un riesgo:** luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene, en este caso el gerente del proceso simplemente acepta la pérdida residual probable y elabora planes de contingencia para su manejo.

Para el manejo de los riesgos se deben analizar las posibles acciones a emprender, las cuales deben ser factibles y efectivas, tales como: la implementación de las políticas, definición de estándares, optimización de procesos y procedimientos y cambios físicos entre otros. La selección de las acciones más conveniente debe considerar la viabilidad jurídica, técnica, institucional, financiera y económica y se puede realizar con base en los siguientes criterios:

- La valoración del riesgo; y

- El balance entre el costo de la implementación de cada acción contra el beneficio de la misma. Para la ejecución de las acciones, se deben identificar las áreas o dependencias responsables de llevarlas a cabo, definir un cronograma y unos indicadores que permitan verificar el cumplimiento para tomar medidas correctivas cuando sea necesario.

Con la realización de esta etapa se busca encauzar el accionar de la entidad hacia el uso eficiente de los recursos, la continuidad en la prestación de los servicios, la protección de los bienes utilizados para servir a la comunidad. Igualmente, se busca que la entidad tenga claridad sobre las políticas de administración del riesgo, las acciones de manejo de riesgo y el compromiso de la Dirección y de los servidores de la entidad.

a) Elaboración del mapa de riesgos

El mapa de riesgos contiene a nivel estratégico los mayores riesgos a los cuales está expuesta la entidad, permitiendo conocer las políticas inmediatas de respuesta ante ellos tendientes a evitar, reducir, dispersar o transferir el riesgo; o asumir el riesgo residual, y la aplicación de acciones (a las cuales se evaluará su efectividad) así como los responsables, el cronograma y los indicadores. Nos obstante se considera recomendable, elaborar un mapa de riesgos por cada proceso para facilitar la administración del riesgo, el cual debe elaborarse al finalizar la etapa de valoración del riesgo.

CUADRO No. 13: FORMATO MAPA DE RIESGOS

RIESGO	IMPACTO	PROBABILIDAD	EVALUACION DEL RIESGO	CONTROLES EXISTENTES	VALORACION DEL RIESGOS	OPCIONES DE MANEJO	ACCIONES	RESPONSABLES	CRONOGRAMA	INDICADOR

Fuente: Universidad Nacional de Colombia. Guía Básica de Administración de Riesgos. (Bogotá; Editorial Universitaria, s.a.), p. 15.

La descripción del mapa de riesgos es la siguiente:

- **Riesgo:** posibilidad de ocurrencia de un evento que pueda entorpecer el normal desarrollo de las funciones de la entidad y le impidan el logro de sus objetivos;

- **Impacto:** consecuencias que puede ocasionar a la organización la materialización del riesgo;

- **Probabilidad:** entendida como la posibilidad de ocurrencia del riesgo; ésta puede ser medida con criterios de frecuencia, si se ha materializado (por ejemplo: No. de veces en un tiempo determinado), o de factibilidad teniendo en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque éste no se haya materializado;

- **Evaluación del riesgo:** resultado obtenido en la matriz de calificación, evaluación y respuesta a los riesgos;

- **Controles existentes:** especificar cuál es el control que la entidad tiene implementado para combatir, minimizar o prevenir el riesgo;

- **Valoración del riesgo:** es el resultado de determinar la vulnerabilidad de la entidad al riesgo, luego de confrontar la evaluación del riesgo con los controles existentes;

- **Opciones de manejo:** opciones de respuesta ante los riesgos tendientes a evitar, reducir, dispersar o transferir el riesgo; o asumir el riesgo residual;

- **Acciones:** es la aplicación concreta de las opciones de manejo del riesgo que entrarán a prevenir o a reducir el riesgo y harán parte del plan de manejo del riesgo;

- **Responsables:** son las dependencias o áreas encargadas de adelantar las acciones propuestas;

- **Cronograma:** son las fechas establecidas para implementar las acciones por parte del grupo de trabajo; y

- **Indicadores:** se consignan los indicadores diseñados para evaluar el desarrollo y eficacia de las acciones implementadas.

b) Clasificación del riesgo

Los riesgos se clasifican en:

i. Riesgos estratégicos

Entre los tipos de riesgos estratégicos, están los siguientes:

- Forma de administrar la entidad;
- Cumplimiento de la misión, visión y objetivos generales; y
- Definición de políticas, diseño y conceptualización por parte de la gerencia.

ii. Riesgos operativos

Entre los tipos de riesgos operativos, están los siguientes:

- Aspectos operativos y técnicos de la presentación del servicio;
- Deficiencias en sistemas de información;
- Inadecuada definición de procesos;
- Estructura interna de la entidad;
- Oportunidades de corrupción; y
- Incumplimiento de compromisos organizacionales y contractuales.

iii. Riesgos financieros

Entre los tipos de riesgos financieros, están los siguientes:

- Inadecuado manejo de los recursos de la entidad;
- Inadecuado manejo presupuestal;
- Elaboración inadecuada de los estados financieros;
- Pagos, tesorería, cartera; y
- Y todos aquellos que puedan llevar al fracaso e inestabilidad de la entidad.

iv. Riesgos de cumplimiento

Entre los tipos de riesgos de cumplimiento, están los siguientes:

- Incumplimiento de requisitos legales;
- Contractuales;
- Ética pública; y
- Compromiso ante la comunidad.

v. Riesgos de tecnología

Entre los tipos de riesgos de tecnología, están los siguientes:

- La tecnología disponible no satisfaga las necesidades de la entidad;
- Equipos Inadecuados;
- Afectación en el cumplimiento actual y futuro de la entidad; y
- No permitan el cumplimiento de la misión de la entidad.

4.3.6 Monitoreo y revisión

Es necesario monitorear los riesgos, la efectividad del plan de tratamiento de los riesgos, las estrategias y el sistema de administración que se establece para controlar la implementación. Los riesgos y la efectividad de las medidas de control necesitan ser monitoreadas para asegurar que las circunstancias cambiantes no alteren las prioridades de los riesgos. Pocos riesgos permanecen estáticos.

Es esencial una revisión sobre la marcha para asegurar que el plan de administración se mantiene relevante. Pueden cambiar los factores que podrían afectar las probabilidades y consecuencias de un resultado, como también los factores que afectan la conveniencia o costos de las distintas opciones de tratamiento. En consecuencia, es necesario repetir regularmente el ciclo de administración de riesgos. La revisión es una parte integral del plan de tratamiento de la administración de riesgos.

4.3.7 Comunicación y consulta

La comunicación y consulta son una consideración importante en cada paso del proceso de administración de riesgos. Es importante desarrollar un plan de comunicación para los interesados internos y externos en la etapa más temprana del proceso. Este plan debería encarar aspectos relativos al riesgo en si mismo y al proceso para administrarlo.

La comunicación y consulta involucra un diálogo en ambas direcciones entre los interesados, con el esfuerzo focalizado en la consulta más que un flujo de información en un sólo sentido del tomador de decisión hacia los interesados.

Es importante la comunicación efectiva interna y externa para asegurar que aquellos responsables por implementar la administración de riesgos, y aquellos con intereses creados comprenden la base sobre la cual se toman las decisiones y por qué se requieren ciertas acciones en particular.

Las percepciones de los riesgos pueden variar debido a diferencias en los supuestos, conceptos, las necesidades, aspectos y preocupaciones de los interesados, según se relacionen con el riesgo o los aspectos bajo discusión. Los interesados probablemente harán juicios de aceptabilidad de los riesgos basados en su percepción de los mismos.

Dado que los interesados pueden tener un impacto significativo en las decisiones tomadas, es importante que sus percepciones de los riesgos, así como, sus percepciones de los beneficios, sean identificadas y documentadas y las razones subyacentes para las mismas comprendidas y tenidas en cuenta.

4.4 El auditor interno, el administrador en la gestión del riesgo empresarial

Administrar los riesgos de manera integral implica una proyección de dos vías: una, la empresa como una corporación que se dedica a satisfacer necesidades de los clientes y aumentar sus valores agregados y por otro lado el auditor quien desea hacer más trabajo con menos recursos.

Esto sucede no solo porque la empresa se ve amenazada por la competencia sino que ellas también exige a todos su integrantes una mayor productividad, de esta exigencia no se escapan los auditores por lo tanto ellos también deben priorizar las áreas de riesgo para realizar trabajos con una mejor oportunidad.

La integridad deber ser la percepción de toda la organización no sólo hacia su entorno sino también sobre aquellos aspectos internos que deben funcionar como la maquinaria de un reloj para que el negocio de a sus clientes los productos y servicios en los momentos en que estos sean requeridos por ellos, pero estos objetivos se ven amenazados en su cumplimiento por diferentes tipos de riesgos, categorizados como: estratégicos, operativos, financieros, del recurso humano, o de la categoría que el negocio considere.

Pero lastimosamente los objetivos del negocio no se están logrando fácilmente, pues las empresas u organizaciones no aplican herramientas ni metodologías para eliminar las causas de esas actividades negativas que afectan sus logros.

Para poder hablar de riesgos corporativos o riesgos del negocio o riesgos integrales, es importante contar con algunos aspectos importantes:

- Un buen sistema de control interno, ejemplo COSO;
- Objetivos claramente definidos al nivel de las estrategias, el mercadeo, la tecnología, el recurso humano, los procesos;
- Auditorías basadas en riesgo;
- Auditores líderes;
- Metodologías para auditar los riesgos;
- Metodologías corporativas de gestión de riesgos;
- Experiencia empresarial o corporativa con el manejo de los riesgos, ya sea que se hayan trabajado por procesos o corporativos; y
- Responsables sobre la gestión de los riesgos.

Administrar o gestionar los riesgos del negocio o los riesgos corporativos será una ventaja competitiva única que las empresas no deben dejar pasar por alto, pero son los auditores internos los responsables directos para que la administración basada en riesgos funcione

y de un valor agregado para el cumplimiento de los objetivos organizacionales, y son ellos porque poseen el conocimiento y la experiencia para poderlo realizar, como lo veremos a continuación.

4.4.1 Auditorías basadas en riesgo

Para que se puedan generar metodologías para administración integral de los riesgos, el auditor debe haberlas asimilado con anterioridad, es decir, trabajar el riesgo desde sus diferentes ópticas como el quehacer cotidiano porque forma parte del proceso metodológico; es importante aclarar que este proceso no es individualizado sino compartido con los auditados en otras palabras el enriquecimiento del proceso lo da el compartir los análisis y conclusiones con los dueños o responsables de los procesos auditados así:

a) Planeación

Todos los trabajos que proyecte el auditor se deben establecer con planes basados en los riesgos, a fin de determinar las prioridades de la actividad de la auditoría interna, dichos planes deberán ser consistentes con las metas de la organización, y estarán basados en una evaluación de riesgos, realizada al menos anualmente. En este proceso deben tenerse en cuenta los comentarios de la alta dirección y del consejo.

Una de las principales ventajas de trabajar la planeación con base en los riesgos es que las auditorías se priorizan con base en las situaciones de riesgo del negocio y sirven posteriormente en la construcción de los mapas de riesgo con los auditados.

b) Evaluación de riesgos y controles

En esta fase donde el auditor y auditado aprovechan la sinergia al máximo al unir los conocimientos técnicos del auditor con la experiencia y conocimiento de los auditados al nivel de los riesgo de los proceso del negocio, las causas que los originan, los efectos o riesgos resultantes y los controles existentes para mitigarlos o en su defecto la propuesta de nuevos controles que eviten o mitiguen los efectos negativos de los riesgos.

Con esta metodología no se trabaja el riesgo de auditoría porque se considera que compete más al auditor encargado de emitir un dictamen, y lo estaríamos restringiendo a un campo meramente financiero.

La metodología se complementa con la elaboración de tres matrices: actividades de proceso versus sus causas de riesgo, el objetivo es priorizar cuales riesgos impactan más sobre el proceso y cuales actividades se ven en mayor grado afectadas por los riesgos.

La naturaleza del trabajo del auditor interno está en evaluar y contribuir a la mejora de los sistemas de gestión de riesgo, control y gobierno, asistiendo a la organización en la identificación y evaluación de las exposiciones significativas a los riesgos, y la contribución a la mejora de los sistemas de gestión de riesgos y control debe supervisar y evaluar la eficacia del sistema de gestión de riesgos de la organización. Las exposiciones al riesgo referidas a gobierno, operaciones y sistemas de información con relación a lo siguiente:

- Confiabilidad e integridad de la información financiera y operativa;
- Eficacia y eficiencia de las operaciones;
- Protección de activos; y
- Cumplimiento de leyes, regulaciones y contratos.

Los anteriores puntos los evalúa el auditor con los auditados en la segunda matriz de riesgos versus las causas que originan los riesgos, el objetivo es determinar que situaciones son las que pueden materializar más la ocurrencia del riesgo, con el objetivo de concentrarnos solo en las causas raizales, dado que el proceso para todas sería muy dispendioso y no justificaría realizarlo para todas las causas de los riesgos.

Determinadas las causas que más influyen en la generación de los riesgos auditado y auditor proceden a validar con la tercera matriz de causas de riesgo versus controles existentes, como se pueden mitigar o eliminar las causas, si los controles existentes son suficientes o si hay necesidad de proponer nuevos controles.

Es importante recordar que toda esta metodología de auditoría se trabaja con el acompañamiento del auditado.

4.4.2 Metodología para la administración integral de los riesgos

La administración del riesgo es un término aplicado a un método lógico y sistemático que establece el contexto, identificación, análisis, evaluación, tratamiento, monitoreo y comunicación sobre los riesgos asociados con una determinada actividad, función o proceso, con el fin de capacitar a las organizaciones para minimizar sus pérdidas y maximizar sus oportunidades. La administración del riesgo está orientada a identificar y aprovechar las oportunidades y/o reducir las pérdidas.

Antes de entrar en la metodología ERM, es importante tener en cuenta los siguientes aspectos para evitar que por su inexistencia o incumplimiento el manejo integral del riesgo falle en la corporación.

a) Apoyo de la administración

Sin lugar a dudas cualquier proyecto o acción que se desee ejecutar corporativamente debe contar con el apoyo total e incondicionado de la alta dirección esto con el fin de evitar la creación de islas independientes o de ideas de que esto no me aplica.

b) Objetivos claros

Las modas administrativas o proyectos de tecnología generan euforias inusitadas que no dejan ver claramente los objetivos y beneficios de los proyectos, es por eso importante que se especifiquen las responsabilidades de cada integrante en relación con la administración de riesgos, para evitar suspicacias o errores de interpretación.

c) Cronogramas

Los mejores métodos de supervisión y seguimiento por parte del auditor al manejo de la administración de riesgos en cuanto a las fases, responsabilidades, tiempos, entregables, verificaciones, compromisos e indicadores se puede apoyar el auditor con cronogramas elaborados en un manejador del proyectos.

d) Recursos

No solo el tiempo del desarrollo de los talleres es importante para obtener buenos resultados, pues hay que disponer de los recursos financieros, físicos y tecnológicos para el desarrollo de los talleres y la consolidación de la información.

e) Formación de equipos

Para que la metodología de administración de riesgos funcione ésta debe ser respaldada por equipos integrados por los dueños o responsables de los procesos, facilitados u orientados por los auditores internos, quienes se acompañarán de herramientas y metodologías que faciliten el desarrollo y análisis de los riesgos.

f) Metodologías

Son las que permiten afinar los procesos de trabajo, evitan que cada unidad de negocio vaya por su lado, estandarizan y normalizan las actividades que se deben ir ejecutando y documentando. Las metodologías son la esencia de cualquier cambio porque marcan los pasos a seguir, estas deben estar documentadas (papel o mejor en medio magnético, intranet) y actualizadas.

g) Herramientas

Corresponde a todos aquellos archivos en medios electrónicos estructurados en la hoja electrónica Excel que permiten a unos bajos costos y amigabilidad en su ejecución, poder desarrollar las metodologías:

- Matrices de auditoría basada en el riesgo;
- Mapas de riesgo;
- Documentación del proceso de priorización y tratamiento del riesgo; y
- Glosario de términos con ejemplos de su significado.

h) Bases de datos

Son los archivos a donde estaremos dejando toda la información sobre los riesgos, sus categorías, planes de acción, de mitigación y control, responsables, mapas de riesgo y cronogramas que facilitan el análisis y supervisión del auditor en el cumplimiento de la metodología.

Como apoyo no solo a la gestión de los riesgo se tiene la base del conocimiento de la auditoría la cual no solo es para lo auditores sino permite por la intranet de la empresa también el acceso a los responsables de los negocios que se deben enterar sobre informes emitidos, mapas de riesgo, estándares de control y método de auto evaluación del control COSO.

i) Política de administración del riesgo

La organización o entidad debe definir y documentar las políticas de administración del riesgo, incluyendo sus objetivos y su compromiso para ello. La política de administración del riesgo debe ser relevante dentro del contexto estratégico de la empresa, sus objetivos y metas, y la naturaleza del negocio. La alta gerencia debe asegurarse que esta política es entendida, implantada y mantenida por todos los niveles de la organización. Debe tener entre otro aspecto los siguientes:

- La organización y el contexto de la administración del riesgo;
- Los riesgos identificados por la organización;
- El análisis y evaluación de estos riesgos;
- Las estrategias para su tratamiento;
- Los mecanismos para revisar el programa; y
- Las estrategias para obtener la conciencia, adquirir habilidades, entrenamiento y educación.[33]

[33] Estupiñán Gaitán, Op. Cit., p. 169.

CONCLUSIONES

1. Para que se pueda generar una metodología para la administración integral de los riesgos, es necesario contar con un buen sistema de control interno y objetivos claramente definidos; el auditor debe desarrollar la metodología compartiendo los análisis y conclusiones con los responsables de los procesos auditados, estableciendo planes basados en los riesgos a fin de determinar las prioridades de la actividad de la auditoría interna, dichos planes deberán ser consistentes con las metas de la organización y posteriormente éstos, servirán en la construcción de los mapas de riesgos con los auditados.

2. El control interno es 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 de las leyes y normas aplicables. Comprende el plan de organización, los métodos y medidas coordinadas adoptadas por una organización o entidad 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. El control interno lo integran cinco componentes interrelacionados: (1) El ambiente de control; (2) Evaluación de riesgos; (3) Actividades de control; (4) Información y comunicación; y (5) Supervisión, seguimiento o monitoreo.

3. La auditoría interna es una actividad independiente y objetiva de aseguramiento y consulta, concebida para agregar valor y mejorar las operaciones de una organización; juega un papel importante en la evaluación de riesgos, su rol principal es proveer aseguramiento a la dirección y la junta sobre la efectividad de la gestión de riesgo. Su trabajo debe ir enfocado hacia la identificación de riesgos para recomendar previamente a la alta dirección, controles en los procesos que minimicen la ocurrencia de los riesgos. Además ayuda a que la organización cumpla con sus objetivos mediante la aplicación de un enfoque sistemático y disciplinado para evaluar y mejorar la efectividad de los procesos de manejo de riesgos, control y dirección.

4. La gestión o administración del riesgo empresarial es un proceso estructurado, consistente y continuo, efectuado por la junta de directores, la administración superior y otros miembros de la organización, es aplicado desde la definición estratégica hasta las actividades del día a día, diseñado para identificar, evaluar, medir y reportar eventos potenciales que pueden afectar a la organización y administrar los riesgos dentro de su apetito, a objeto de proveer una seguridad razonable respecto del logro de los objetivos de la organización.

5. La administración de riesgos es un proceso iterativo que consiste en pasos que, cuando se siguen en secuencia, facilitan una mejora continua en el desempeño y en la toma de decisiones. Involucra establecer una infraestructura y cultura apropiada y aplicar un método lógico y sistemático para establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con cualquier actividad, función o proceso de forma tal que permita a las organizaciones minimizar pérdidas y maximizar beneficios.

RECOMENDACIONES

1) Considerando que el recurso humano es el elemento más importante del control interno y de la gestión de riesgos, los procesos de contratación deben ser minuciosos y selectivos y de ser posible el departamento de recursos humanos debe contar con profesionales que se dediquen a investigar a los empleados potenciales; además de realizar evaluaciones periódicas y capacitación constante en todos los niveles de la organización que permitan implementar los procedimientos adecuados.

2) Las personas que ocupen los cargos de auditores internos deben ser profesionales con conocimientos en las siguientes áreas: razonamiento, ética, auditoría, comunicación, organización, informática, sociología, fraude, contabilidad financiera, recolección de datos, marketing, contabilidad de gestión, estadística, finanzas, economía, métodos cuantitativos, internacionales, gubernamentales y fiscales.

3) Para minimizar los riesgos empresariales, las organizaciones o entidades deben contar con instrumentos que permitan identificar tales riesgos y sus efectos debiendo evaluarlos con los siguientes componentes: entorno interno; definición de objetivos; identificación de eventos; valoración de riesgos; respuesta al riesgo; actividades de control; información y comunicación; y monitoreo, que permitan construir mapas de riesgos.

4) Las organizaciones o entidades deben responder ante la administración de riesgos de acuerdo a sus características particulares y actividades en las que participa, sin embargo deben considerar como parte del proceso de administración de riesgos los siguientes elementos: definición del contexto; identificación de riesgos; análisis del riesgo; valoración del riesgo; tratamiento de los riesgos; monitoreo y revisión; y comunicación y consulta.

LITERATURA CITADA Y CONSULTADA

Chet Cifuentes, Edwin Estuardo. **Evaluación del Control Interno en una Institución con una Administración Estratégica bajo el Sistema COSO**. Tesis de Licenciatura, Facultad de Ciencias Económicas: Universidad de San Carlos de Guatemala, 2006.

Coopers & Lybrand. **Los Nuevos Conceptos de Control Interno (Informe COSO).** Madrid: Ediciones Díaz de Santos, S.A., 1997.

Comité Conjunto de Estándares Australia/Estándares Nueva Zelanda. **Administración de Riesgos, Borrador para Comentario Público** [en línea]. Consultado el 13 de septiembre de 2009. Disponible en: http://www.netconsul.com/riesgos/Modificacion4360.pdf

Committee of Sponsoring Organizations of the Treadway Commission. **Estructura Conceptual de la Administración de Riesgos del Emprendimiento -RESUMEN EJECUTIVO- Borrador en exposición para comentarios públicos.** Bogotá: ECOE Ediciones, 2003.

Consejo de Auditoría Interna General de Gobierno. **Programación en Auditoría en Base a Riesgos** [en línea]. Consultado el 3 de diciembre de 2009. Disponible en: http://www.auditoriainternadegobierno.cl/index.php/menu/show/id/25

Ernst & Young LLP. **Evaluación del Control Interno: Consideraciones para Evaluar el Control Inerno a Nivel de Empresa** [en línea]. Consultado el 14 de abril de 2009. Disponible en: http://www.pericia.cl/Doc/control_interno.pdf

Estupiñán Gaitán, Rodrigo. **Administración de Riesgos E.R.M. y la Auditoría Interna.** Bogotá: ECOE Ediciones, 2008.

Estupiñán Gaitán, Rodrigo. **Aspectos Conceptuales Normativos y Metodológicos de la Auditoría Integral.** Bogotá: El Autor, s.a.

Fonseca Borja, René. **Auditoría Interna. Un enfoque moderno de planificación, ejecución y control**. Guatemala: Artes Gráficas Acrópolis, 2004.

González-Cueto Longres, Aleida y Manuel Pando Franco. **La Administración de Riesgos Empresarial en el contexto actual de Control Interno** [en línea]. Consultado el 21 de julio de 2009. Disponible en: http://www.nodo50.org/cubasigloXXI/economia/gcueto_311206.pdf

Lam Alvarez, Elsa María. **Evaluación del Control Interno Basado en el Modelo COSO**. Tesis de Licenciatura, Facultad de Ciencias Económicas: Universidad Francisco Marroquin, Guatemala, 2002.

Mantilla B., Samuel Alberto. **Control Interno: Informe COSO.** Bogotá: Ecoe Ediciones Ltda., 2007.

Mantilla B., Samuel Alberto y Sandra Yolita Cante S. **Auditoría del Control Interno**. Bogotá: ECOE Ediciones, 2005.

Universidad de Buenos Aires. **Manual de Procedimientos de Auditoría Interna.** Buenos Aires: Editorial Universitaria, s.a.

Universidad Nacional de Colombia. **Guía Básica de Administración de Riesgos.** Bogotá: Editorial Universitaria, s.a.

Vilches Troncoso, Ricardo. **Apuntes del Estudiante de Auditoría** [en línea]. Consultado el 20 de agosto de 2009. Disponible en: http://www.ecobachillerato.com/temasecem/auditoria.pdf

ANEXOS

ANEXO No. 1: CUESTIONARIO DE EVALUACIÓN DEL CONTROL INTERNO[34]

Entorno de control

El entorno de control refleja la pauta fijada por la alta gerencia y la actitud general, la conciencia y las acciones de la junta directiva, la gerencia, los dueños y otros, con respecto a la importancia del control interno y el énfasis puesto sobre el control en las políticas, procedimientos, métodos y estructura organizacional de la compañía. Esto es el fundamento para todos los otros componentes del control interno, que proveen disciplina y estructura.

Puntos a considerar	*Si*	*No*	*Respuestas / Comentarios*
Integridad, valores éticos, y comportamiento de los ejecutivos clave			
• ¿Muestra la junta directiva interés por la integridad y los valores éticos? ¿Hay un código de conducta y/o una política de ética, y estos han sido comunicados adecuadamente?			
• ¿Se ha comunicado eficazmente el compromiso de la gerencia a la integridad y el comportamiento ético a toda la compañía, tanto en palabras como en hechos? ¿La gerencia lidera dando el ejemplo?			
• ¿Se le pide al personal de la alta gerencia que ha sido contratado fuera de la compañía que se familiarice con la importancia de altos valores éticos y controles?			
• ¿Trata la gerencia de eliminar o reducir los incentivos o tentaciones que pueden propiciar que el personal se involucre en actos fraudulentos, ilegales o no éticos?			
• ¿Otorga la gerencia recompensas, tales como bonos o acciones de la compañía, fomentando un tono ético apropiado (p. ej., estas no se otorgan a quienes cumplen objetivos, sino, en el proceso, evaden las políticas, procedimientos o controles establecidos)?			
• ¿Toma la gerencia acción disciplinaria apropiada en respuesta a las desviaciones de políticas y procedimientos aprobados o violaciones del código de conducta?			

[34] Ernst & Young LLP. Evaluación del Control Interno: Consideraciones para Evaluar el Control Inerno a Nivel de Empresa [en línea]. Consultado el 14 de abril de 2009. Disponible en: http://www.pericia.cl/Doc/control_interno.pdf

Puntos a considerar	*Si*	*No*	*Respuestas / Comentarios*
Conciencia de control de la gerencia y estilo operativo			
• ¿Es apropiada la estructura de la gerencia (p. ej., no es dominada por uno o unos pocos individuos) y existe una supervisión eficaz por parte de la junta directiva y/o el comité de auditoría?			
• ¿Tiende a ser conservadora la filosofía de la gerencia sobre reportar información financiera, incluyendo su actitud hacia el desarrollo de estimaciones? ¿Se reducen al mínimo las influencias que puedan afectar estimaciones contables significativas y minimizar otros juicios?			
• ¿Existe un mecanismo establecido para educar y comunicar regularmente a la gerencia y a los empleados la importancia de los controles internos, y elevar el nivel de entendimiento de los controles?			
• ¿Presta la gerencia la apropiada atención al control interno, incluyendo los efectos del procesamiento de sistemas de información?			
• ¿Corrige la gerencia oportunamente las deficiencias identificadas en el control interno?			
• ¿Están equilibrados los incentivos a la gerencia (p. ej., la parte de la compensación de la gerencia derivada de bonos, opciones de compra de acciones, u otros incentivos no promueve un excesivo nivel de interés en mantener o aumentar el precio de las acciones o las ganancias de la empresa)?			
• ¿Establece la gerencia objetivos financieros y expectativas reales (p. ej., no excesivamente agresivos) para el personal operativo?			
Compromiso de la gerencia a ser competente			
• ¿Parece el personal tener la capacidad y el entrenamiento necesarios para su nivel de responsabilidad asignado o la naturaleza y complejidad del negocio?			
• ¿Posee la gerencia una amplia experiencia funcional (la gerencia viene de varias áreas funcionales en vez de sólo unas pocas, tales como producción y ventas)?			

Puntos a considerar	***Si***	***No***	***Respuestas / Comentarios***
• ¿Es apropiado el personal departamental, (particularmente con respecto al conocimiento y experiencia de la gerencia y los niveles supervisores dentro de las áreas de contabilidad, sistemas de información y reporte de información financiera)?			
• ¿Muestra la gerencia una voluntad de consultar con los auditores y tratar asuntos significativos que se relacionan con el control interno y asuntos de contabilidad?			
• ¿Demuestra la gerencia un compromiso para proveer suficiente personal de contabilidad y financiero para mantener el ritmo de crecimiento y/o complejidad del negocio?			
Participación de la junta directiva y/o el comité de auditoría en el gobierno y la vigilancia			
• ¿Es apropiada la estructura de la junta directiva, incluyendo el número de directores, sus antecedentes y experiencia, dada la naturaleza de la compañía? ¿La independencia de los miembros externos de la junta directiva ha sido revisada adecuadamente, incluyendo afiliaciones, relaciones y transacciones con la compañía?			
• ¿Son independientes de la gerencia, la junta directiva y el comité de auditoría, tanto así que con frecuencia indagan y plantean preguntas según sea necesario?			
• ¿Consideran adecuadamente la junta directiva y/o el comité de auditoría la importancia del entendimiento de los procesos que la gerencia emplea para monitorear los riesgos de negocios que afectan a la organización?			
• ¿Representa el comité de auditoría un supervisor informado, vigilante y eficaz del proceso de reporte de información financiera y del control interno de la compañía, incluyendo el procesamiento de sistemas de información y los controles computarizados relacionados?			
• ¿Incluye el comité de auditoría al menos a un “experto financiero”?			
• ¿Mantiene el comité de auditoría una línea directa de comunicación con los auditores externos e internos de la empresa?			

Puntos a considerar	*Si*	*No*	*Respuestas / Comentarios*
• ¿Tiene el comité de auditoría un documento que defina sus deberes y responsabilidades? ¿Tiene el comité de auditoría los recursos adecuados y la autoridad para ejercer sus responsabilidades?			
Estructura organizacional y asignación de autoridad y responsabilidades			
• ¿Es la estructura organizacional adecuada para el tamaño, actividades operacionales, y ubicación de la compañía?			
• ¿Es apropiada la estructura organizacional general (es decir, no demasiado compleja, ni abarca numerosas empresas jurídicas o poco usuales, líneas administrativas de autoridad, o convenios contractuales sin propósito aparente de negocios)?			
• ¿Existe una estructura apropiada para asignar la propiedad de la información, incluso quiénes están autorizados para iniciar y/o modificar transacciones? Se asigna la propiedad para cada aplicación y base de datos dentro de la infraestructura de tecnología de información?			
• ¿Hay políticas apropiadas para aquellos asuntos como aceptación de nuevos negocios, conflictos de interés, y prácticas de seguridad? Son ellas comunicadas adecuadamente a toda la organización?			
• ¿Hay políticas y procedimientos apropiados para la autorización y aprobación de transacciones al nivel adecuado?			
• ¿Es clara la asignación de responsabilidades, incluyendo responsabilidades del procesamiento de sistemas de información y desarrollo de programas?			
• ¿Revisa y modifica la gerencia la estructura organizacional de la compañía de acuerdo a los cambios de condiciones?			
• ¿Hay una adecuada supervisión y monitoreo de las operaciones descentralizadas (incluyendo personal de contabilidad y sistemas de información)?			
• ¿Hay una apropiada segregación de actividades incompatibles (es decir, la separación entre la contabilización y el acceso a activos)?			

Políticas y prácticas de recursos humanos			
Puntos a considerar	***Si***	***No***	***Respuestas / Comentarios***
• ¿Existen normas y procedimientos para la contratación, adiestramiento, motivación, evaluación, promoción, remuneración, traslados y terminación de personal que sean aplicables a todas las áreas funcionales (p.ej., contabilidad, mercadeo, sistemas de información)?			
• ¿Existen procedimientos de investigación para la selección de solicitantes de empleo, particularmente para personal con acceso a activos susceptibles a sustracción?			
• ¿Son claras las políticas y procedimientos y se emiten, actualizan y modifican oportunamente? Se comunican eficazmente al personal en localidades descentralizadas y/o extranjeras?			
• ¿Hay descripciones de funciones, manuales de referencia u otras formas de comunicación que informen al personal sobre sus obligaciones?			
• ¿El desempeño del trabajo es evaluado y revisado periódicamente con cada empleado?			

Evaluación del entorno interno: Eficaz Ineficaz

Resuma las razones que soportan su evaluación, a menos que sean obvias:

_____

_____

_____

_____

_____

_____

Evaluación de riesgos

La evaluación de riesgos es la identificación y análisis de riesgos relevantes (tanto internos como externos) al logro de los objetivos, formando una base para determinar cómo los riesgos deben ser administrados.

Puntos a considerar	*Si*	*No*	*Respuestas / Comentarios*
Se han establecido y comunicado objetivos a nivel de empresa, incluyendo cómo están apoyados por planes estratégicos y complementados a nivel de proceso / aplicación. Se ha establecido un proceso de evaluación de riesgo, incluyendo la estimación de la importancia de los riesgos, la evaluación de la probabilidad de su ocurrencia, y la determinación de las acciones necesarias a seguir.			
• ¿Son establecidos, comunicados y monitoreados los objetivos de negocios? ¿Son comunicados a toda la empresa los elementos clave del plan estratégico de la empresa, de manera que los empleados tengan un entendimiento básico de la estrategia general de la compañía? ¿El plan estratégico de la empresa y los objetivos de negocio se complementan entre si?			
• ¿Existe un proceso que periódicamente revise y actualice los planes estratégicos de toda la empresa? ¿El plan estratégico es revisado y aprobado por la junta directiva?			
• ¿El plan estratégico de toda la empresa incluye la tecnología de información o existe un plan estratégico separado de tecnología de información que trate las necesidades tecnológicas de la empresa para cumplir con su plan estratégico eficaz y eficientemente?			

• ¿Existe un mecanismo adecuado que identifique riesgos de negocios, incluyendo aquellos que resulten de:
  • Entrada a nuevos mercados o líneas de negocios?
  • Ofrecimiento de nuevos productos y servicios?
  • Cumplimiento de requerimientos de privacidad y protección de información?
  • Otros cambios en el negocio, la economía y el entorno regulador?			

Puntos a considerar	*Si*	*No*	*Respuestas / Comentarios*
• ¿Realiza la auditoría interna (u otro grupo dentro de la compañía) evaluaciones periódicas de riesgos (al menos anualmente)? ¿Si la respuesta es si, revisa la alta gerencia las evaluaciones de riesgos y considera acciones para mitigar los riesgos significativos identificados?			
• ¿La gerencia considera cuánto riesgo está dispuesto a aceptar cuando fija la dirección estratégica o la entrada a nuevos mercados, y se esfuerza por mantener los riesgos dentro de esos niveles?			
• ¿Supervisan y monitorean la junta directiva y/o el comité de auditoría el proceso de evaluación de riesgo y toman acciones para tratar los riegos significativos identificados?			
Existen mecanismos para anticipar, identificar y reaccionar a los cambios que pudieran tener un efecto dramático y dominante en la empresa (p. ej., el comité de administración de activos/pasivos en una institución financiera, el grupo de administración de riesgos de comercialización en una empresa manufacturera) o que pudiera afectar el logro de objetivos de la empresa o de niveles de procesos/aplicaciones.			
• ¿Están bien controladas las adquisiciones y ventas disposiciones de negocios significativas y los activos (p. ej., finalizados después de completar los procedimientos de “due diligence”, revisados por un nivel apropiado de la gerencia)?			
• ¿Existen grupos o individuos que son responsables de anticipar e identificar cambios que pudieran tener un efecto significativo sobre la empresa? ¿Existen procesos para informar a niveles apropiados de la gerencia acerca de cambios con posibles efectos significativos en la empresa?			
• ¿Son actualizados durante al año los presupuestos/ proyecciones para reflejar condiciones cambiantes?			

Puntos a considerar	*Si*	*No*	*Respuestas / Comentarios*
• ¿Se hacen revisiones periódicas o existen otros procedimientos para que, entre otras cosas, se anticipen e identifiquen eventos o actividades rutinarios que puedan afectar la capacidad de la empresa de cumplir con sus objetivos y tratarlos?			
• ¿La gerencia reporta a la junta directiva y/o el comité de auditoría acerca de cambios que pudieran tener un efecto significativo en la empresa?			
El departamento de contabilidad tiene procesos establecidos para: (1) identificar cambios en los principios de contabilidad generalmente aceptados promulgados por los organismos con autoridad relevantes, (2) notificar al departamento de contabilidad de cambios en las prácticas de negocios de la compañía que puedan afectar el método o los procesos para registrar transacciones, y (3) identificar cambios significativos en el control interno o el entorno operativo, incluyendo cambios que resulten de nuevas regulaciones o cambios en éstas.			
• ¿Tiene el departamento de contabilidad un proceso para identificar y tratar cambios en principios de contabilidad, así como también para la aprobación de modificaciones en la contabilidad para tratar dichos cambios?			
• ¿Trabaja la gerencia con los auditores externos u otras terceras personas expertas para determinar si están tratando los cambios complejos de los principios de contabilidad apropiadamente?			
• ¿Revisan la junta directiva y/o el comité de auditoría los cambios significativos en las prácticas contables de la empresa y los aprueban?			
• ¿Existen procesos para asegurar que el departamento de contabilidad conozca los cambios en el entorno operativo, para que luego pueda revisar tales cambios y determinar los efectos, si es que existe alguno, que los cambios puedan tener sobre las prácticas contables de la empresa?			

Puntos a considerar	*Si*	*No*	*Respuestas / Comentarios*
• ¿Existen canales de comunicación entre el departamento de contabilidad y/o individuos a cargo de monitorear las regulaciones, para que el departamento de contabilidad conozca los cambios en las regulaciones que podrían afectar las prácticas contables de la empresa?			
• ¿Existen procesos para asegurar que el departamento de contabilidad (y la junta directiva y/o el comité de auditoría) conozcan las transacciones significativas con partes relacionadas, para que luego puedan determinar si tales transacciones son apropiadamente contabilizadas y reveladas?			

Evaluación de la evaluación de riesgos: Eficaz Ineficaz

Resuma las razones que soportan su evaluación, a menos que sean obvias:

Información y comunicación

Los sistemas de información y comunicación apoyan la identificación, captura e intercambio de información en una forma y oportunidad que permiten a la gerencia y a otro personal apropiado cumplir con sus responsabilidades.

Puntos a considerar	*Si*	*No*	*Respuestas / Comentarios*
Información ***Los sistemas de información proveen a la gerencia los reportes necesarios sobre el desempeño de la empresa en relación a los objetivos establecidos, incluyendo información interna y externa relevante, y proporcionan la información a la gente apropiada con el detalle necesario y a tiempo, para permitirles cumplir con sus responsabilidades eficaz y eficientemente.***			
• ¿Es la empresa capaz de preparar informes financieros exactos y oportunos, incluyendo informes interinos?			
• ¿Reciben la junta directiva y la gerencia suficiente información oportuna que les permita cumplir con sus responsabilidades?			
• ¿Son definidos y medibles los objetivos de la gerencia en términos de presupuestos, ganancias, y otros objetivos financieros y operativos? ¿Son los resultados reales medidos en relación a esos objetivos?			
• ¿Hay un alto nivel de satisfacción de los usuarios con el procesamiento de los sistemas de información, incluyendo aspectos como confiabilidad y oportunidad de los informes?			
• ¿Hay un nivel suficiente de coordinación entre las funciones/departamentos de contabilidad y procesamiento de sistemas de información?			
Los sistemas de información son desarrollados o revisados en base al plan estratégico que está interrelacionado con los sistemas de información generales de la empresa, y responden al logro de los objetivos a nivel de empresa y a nivel de procesos/aplicaciones.			

Puntos a considerar	*Si*	*No*	*Respuestas / Comentarios*
• ¿Existen políticas apropiadas para desarrollar y modificar los sistemas de contabilidad y control (incluyendo cambios y uso de programas de computación y/o archivos de computación)?			
• ¿Son los esfuerzos de la gerencia para desarrollar o revisar los sistemas de información (incluyendo sistemas de contabilidad) congruentes con sus planes estratégicos?			
• ¿Existen aplicaciones o transacciones importantes que sean ejecutadas/ procesadas por organizaciones que prestan servicios? Si la respuesta es sí, ¿tiene la gerencia documentados los controles relevantes asociados a la organización de servicios, la compañía o ambos que mitiguen el riesgo de error? ¿Hay políticas para la supervisión periódica de los controles de la organización de servicios o la compañía y se toman acciones apropiadas para mitigar el potencial de nuevos riesgos?			
La gerencia destina los recursos humanos y financieros apropiados para desarrollar los sistemas de información necesarios, y asegura y supervisa a los usuarios que participan en el desarrollo (incluyendo revisiones) y prueba de los programas.			
• ¿Participa la junta directiva y/o el comité de auditoría en los proyectos de monitoreo de los sistemas de información y prioridad de los recursos?			
• ¿Refleja claramente el diagrama de organización de tecnología de información las áreas de responsabilidad y las líneas de reporte y comunicación?			
• ¿Existen responsabilidades definidas para los responsables de implantar, documentar, probar y aprobar cambios en los programas de computación que son comprados o desarrollados por el personal de sistemas de información o los usuarios?			
• ¿Son bien controladas las conversiones de los sistemas (p. ej., completadas de acuerdo a procedimientos o planes escritos)?			
• ¿Asegura y monitorea la gerencia financiera a los usuarios involucrados en el desarrollo de programas, incluyendo el diseño de pruebas del control interno y balances?			

Puntos a considerar	***Si***	***No***	***Respuestas / Comentarios***
• ¿Hay un alto grado de cooperación e interacción entre usuarios y el departamento de tecnología de información (p. ej., procedimientos para asegurar el monitoreo continuo por parte del departamento de tecnología de información de la satisfacción de los usuarios con el procesamiento y políticas de tecnología de información para el desarrollo, modificación y uso de los programas y los archivos de datos)?			
La gerencia ha establecido un plan de continuidad del negocio/ recuperación de desastres para todos los centros primarios de información.			
• ¿Son replicados (backed up) regularmente los programas de aplicación y los archivos?			
• ¿Existe un plan actual de recuperación de desastres para componentes importantes de la infraestructura de tecnología de información?			
• ¿Hay un plan de continuidad de negocios que incorpore el plan de recuperación de desastres y las necesidades de los departamentos usuarios para recuperar oportunamente las funciones críticas, los sistemas, procesos e información del negocio?			
• ¿Son los planes de recuperación de desastres y continuidad de negocios probados periódicamente (al menos una vez al año)?			
• ¿Son los planes de recuperación de desastres y continuidad de negocios actualizados de acuerdo a cambios en las condiciones?			
Comunicación ***La gerencia comunica los deberes y responsabilidades de control de los empleados en una manera eficaz, y ha establecido canales de comunicación para que la gente reporte situaciones que se sospeche son impropias***			
• ¿Son claramente definidas y comunicadas las líneas de autoridad y responsabilidad (incluyendo líneas de reportes) dentro de la compañía?			
• ¿Existen descripciones de funciones por escrito y manuales de referencia que describan las responsabilidades del personal?			

Puntos a considerar	*Si*	*No*	*Respuestas / Comentarios*
• ¿Son las políticas y procedimientos establecidos y comunicados al personal en las localidades descentralizadas (incluyendo operaciones extranjeras)?			
• ¿Hay adiestramiento/orientación para los nuevos empleados, o empleados que comienzan en una nueva posición, para discutir la naturaleza y alcance de sus deberes y responsabilidades? ¿El adiestramiento/orientación incluye una discusión de controles internos específicos de los cuales son responsables?			
• ¿Hay un proceso para que los empleados comuniquen situaciones impropias? Es el proceso bien comunicado a toda la empresa? ¿El proceso permite guardar la identidad de quienes reportan posibles situaciones impropias? ¿Existe un proceso para reportar situaciones impropias, y acciones tomadas para tratarlas, a la alta gerencia, la junta directiva y/o el comité de auditoría?			
• ¿Son revisadas, investigadas y resueltas oportunamente todas las posibles situaciones impropias reportadas?			
Existe una adecuada comunicación a través de la organización que permita a la gente cumplir con su responsabilidad eficazmente, y la gerencia toma acciones de seguimiento oportuna y apropiadamente sobre las comunicaciones recibidas de clientes, proveedores, reguladores u otras partes externas.			
• ¿Creen los empleados que tienen información adecuada para cumplir con las responsabilidades de su trabajo?			
• ¿Hay un proceso que comunique rápidamente la información crítica a toda la compañía cuando sea necesario?			
• ¿Hay un proceso para recopilar la información de los clientes, proveedores, reguladores y otras partes externas?			
• ¿Se asigna responsabilidad a un miembro de la gerencia para ayudar a asegurarse que la empresa responda apropiada, oportuna y correctamente a las comunicaciones de los clientes, proveedores, reguladores y otras partes externas?			

Evaluación de información y comunicación: Eficaz Ineficaz

Resuma las razones que soportan su evaluación, a menos que sean obvias:

Actividades de control

Las actividades de control son las políticas y procedimientos que ayudan a asegurar que las directrices de la gerencia sean cumplidas.

Puntos a considerar	*Si*	*No*	*Respuestas / Comentarios*
Existen políticas y procedimientos necesarios con respecto a que cada una de las actividades de la empresa y los controles señalados por la política están siendo aplicados.			
• ¿Se siguen las prácticas contables y de cierre consistentemente en fechas interinas (p. ej., trimestral, mensualmente) durante el año? ¿Está la gerencia apropiadamente involucrada en la revisión de las estimaciones contables significativas y apoyo para las transacciones no usuales significativas y asientos de diario no estándar?			
• ¿Hay documentación oportuna y apropiada para las transacciones?			
• ¿Revisa la empresa sus políticas y procedimientos periódicamente para determinar si continúan siendo apropiados para las actividades de la compañía?			
• ¿Tienen los miembros de la gerencia responsabilidad sobre las políticas y los procedimientos? ¿La responsabilidad incluye asegurarse que las políticas y los procedimientos sean apropiadas para las actividades de la compañía?			
La gerencia tiene objetivos claros en términos de presupuesto, utilidades y otras metas financieras y de operación, y estos objetivos están claramente escritos, y son comunicados a toda la empresa y activamente monitoreados. Han sido implantados sistemas de planificación y de reporte para identificar variaciones en el rendimiento planificado y comunicar estas variaciones al nivel apropiado de la gerencia. El nivel de la gerencia apropiado investiga las variaciones y toma acciones correctivas apropiadas y oportunas.			
• ¿Existe un sistema de presupuesto?			

Puntos a considerar	*Si*	*No*	*Respuestas / Comentarios*
• ¿Revisa la gerencia los indicadores clave de rendimiento (p. ej., presupuestos, utilidades, metas financieras, metas operativas) regularmente (p. ej., mensual, trimestralmente) e identifica variaciones significativas? ¿La gerencia luego investiga las variaciones significativas y se toman las acciones correctivas apropiadas?			
• ¿Son comunicadas y discutidas con la junta directiva y/o el comité de auditoría las variaciones en el rendimiento planificado por lo menos trimestralmente?			
• ¿Son entregados los estados financieros a la gerencia operativa? ¿Están acompañados de comentarios analíticos?			
Los deberes son lógicamente divididos o segregados (manualmente o a través de la implementación de aplicaciones de tecnología de información (IT) apropiadas) entre diferentes personas para reducir el riesgo de fraude o de acciones impropias.			
• ¿Hay una apropiada segregación de actividades incompatibles (p. ej., separación entre contabilización de activos y acceso a los mismos; la función de operaciones de tecnología de información separada de los sistemas y de la programación; la función de administración de la base de datos separada de la programación de aplicaciones y de la programación de sistemas)? ¿Son revisados los organigramas para asegurar que existe una segregación apropiada de deberes?			
• ¿Se requieren aprobaciones apropiadas de parte de la gerencia antes de permitir acceso a un individuo a aplicaciones y bases de datos específicas?			
• ¿Existe prohibición para que el personal de tecnología de información tenga responsabilidades o deberes incompatibles en departamentos usuarios?			
• ¿Hay procesos para revisar periódicamente (p. ej. trimestral, semestralmente) los privilegios del sistema y controles de acceso a las diferentes aplicaciones y bases de datos dentro de la infraestructura de tecnología de información para determinar si los privilegios del sistema y accesos de control son apropiados?			

Puntos a considerar	*Si*	*No*	*Respuestas / Comentarios*
Se realizan comparaciones periódicas de montos registrados en el sistema de contabilidad con activos físicos. Existen adecuados resguardos para prevenir acceso no autorizado o la destrucción de documentos, registros y activos.			
• ¿Ha establecido la gerencia procedimientos para conciliar periódicamente activos físicos (p. ej., efectivo, cuentas por cobrar, inventarios, activo fijo) con los registros contables relacionados?			
• ¿Se toman inventarios físicos /conteos cíclicos en forma periódica y se ajusta de acuerdo el sistema perpetuo de inventario? ¿Son investigados los ajustes significativos o recurrentes para determinar la razón del ajuste y se toman las acciones apropiadas para tratar las razones de los ajustes?			
• ¿Ha establecido la gerencia procedimientos para prevenir acceso no autorizado a, o la destrucción de, documentos, registros (incluyendo programas de computación y archivos de datos), y activos?			
• ¿Está restringido el acceso de procesamiento de datos a los activos que no son de procesamiento de datos (p. ej., cheques en blanco)?			
Se han establecido políticas para controlar el acceso a programas y archivos de datos. Se usa software de seguridad de acceso, software de sistema operativo, y/o software de aplicaciones para controlar el acceso a programas de datos. Existe una función de seguridad de información y es responsable de monitorear el cumplimiento de las políticas y procedimientos de seguridad de información.			

• ¿Son usados el software de seguridad de acceso, software de sistemas operativos, y software de aplicaciones para controlar ambos accesos centralizados y descentralizados a:
  • Información y-datos?
  • Capacidad funcional de programas (p. ej., ejecutar, actualizar, modificar parámetros, solamente leer)?			

Puntos a considerar	*Si*	*No*	*Respuestas / Comentarios*
• ¿Es razonable la seguridad física sobre los activos de tecnología de información (tanto el departamento de tecnología de información y usuarios), dada la naturaleza del negocio de la compañía?			
• ¿La información electrónica crítica es respaldada diariamente y guardada fuera de las instalaciones?			
• ¿Existen controles para acceso por teléfono a los recursos de computación de la compañía (p. ej., firewalls; directorios centralizados para guardar y manejar identidades de usuarios y privilegios de recursos; solicitud, aprobación y proceso de cumplimiento para acceso a la empresa automatizado y basado en la política)?			
• ¿Hay una función dedicada de ejecutivo de seguridad que monitorea las actividades de procesamiento de tecnología de información y existen informes periódicos para la junta directiva y/o el comité de auditoría sobre el estado actual de la seguridad de tecnología de información en la compañía?			
• ¿Existen sistemas para monitorear y responder a interrupciones potenciales del negocio debido a incidentes de intrusión maliciosa, y para actualizar los protocolos de seguridad para prevenirlos? ¿Son las violaciones de seguridad y otros incidentes automáticamente registrados y revisados?			
• ¿Realiza la compañía revisiones /auditorías periódicas de la seguridad de tecnología de información? ¿Si la respuesta es afirmativa, son los resultados de esta revisión /auditoría reportados a la junta directiva y/o al comité de auditoría?			

Evaluación de actividades de control: Eficaz Ineficaz

Resuma las razones que soportan su evaluación, a menos que sean obvias:

_____

_____

_____

Monitoreo

Monitoreo es un proceso que evalúa la calidad de desempeño del control interno a través del tiempo.

Puntos a considerar	*Si*	*No*	*Respuestas / Comentarios*
Se realizan evaluaciones periódicas del control interno y el personal, mientras realiza sus deberes regulares, obtiene evidencia de que el sistema de control interno sigue funcionando.			
• ¿Requieren los procedimientos que la gerencia revise los procesos de control para asegurarse que los controles están siendo aplicados tal como se esperaba?			
• ¿Existen procedimientos para monitorear cuándo los controles son omitidos y para determinar si la omisión fue apropiada?			
• ¿Existen políticas / procedimientos para asegurar que se toman acciones correctivas de forma oportuna cuando ocurren excepciones en los controles?			
La gerencia: (1) implementa las recomendaciones de control interno de los auditores internos e independientes, (2) corrige las deficiencias conocidas en forma oportuna, y (3) responde apropiadamente a los informes y las recomendaciones de los reguladores.			
• ¿Toma la gerencia acciones adecuadas y oportunas para corregir deficiencias reportadas por la función de auditoría interna?			
• ¿Responde la gerencia en forma oportuna y apropiada a las observaciones de los auditores independientes y a sus recomendaciones en relación al control interno y a las políticas y procedimientos de la Compañía?			
• ¿Recibe la compañía hallazgos y recomendaciones de los reguladores? Si la respuesta es afirmativa, trata los hallazgos adecuada y oportunamente?			

Puntos a considerar	*Si*	*No*	*Respuestas / Comentarios*
• ¿Existen otras funciones de semi-auditoría (p. ej., revisión de crédito en una institución financiera o administración de riesgos en una compañía de seguros) que reportan a la gerencia y afectan el entorno de control general?			
Hay una función de auditoría interna que la gerencia utiliza para asistirle en sus actividades de monitoreo.			
• ¿Es adecuado el nivel de personal, adiestramiento, y habilidades especializadas dado el entorno (p. ej., el uso de auditores de sistemas con experiencia y capacitación en ambientes altamente automatizados y complejos)?			
• ¿Es independiente la función de auditoría interna (en términos de autoridad y relaciones de reporte) de las actividades que auditan?			
• ¿Se prohíbe a los auditores internos tener responsabilidades operativas que tengan conflictos con su función de monitorear?			
• ¿Tienen acceso directo los auditores internos a la junta directiva y/o al comité de auditoría?			
• ¿Se adhiere la función de auditoría interna a las normas profesionales, tales como las normas emitidas por el Instituto de Auditoría Interna?			
• ¿Ha habido una reciente revisión de calidad en la función de auditoría interna por terceros tales como los auditores independientes de la compañía?			
• ¿Es apropiado el alcance de las actividades de auditoría interna (p. ej., balance entre las auditorías financieras y operacionales, cobertura y rotación de operaciones descentralizadas) dada la naturaleza, el tamaño y la estructura de la compañía?			

• ¿El alcance de las actividades planificadas de auditoría interna es revisado en forma anticipada con:
  • La alta gerencia?
  • La junta directiva y/o el comité de auditoría?
  • Los auditores independientes?			

• ¿Desarrolla el departamento de auditoría interna un plan anual que considera el riesgo en la determinación de la asignación de recursos?			

Puntos a considerar	*Si*	*No*	*Respuestas / Comentarios*
• ¿Tienen los auditores internos autoridad para examinar cualquier aspecto de las operaciones de la empresa?			
• ¿Son reportados los resultados de las actividades de la auditoría interna a: • La alta gerencia? • La junta directiva y/o el comité de auditoría? • Los auditores independientes?			

Evaluación de control de monitoreo: Eficaz
Ineficaz
Resuma las razones que soportan su evaluación, a menos que sean obvias:

Evaluación general del control interno a nivel de empresa: Eficaz Ineficaz

Basado en factores documentados en las secciones previas y en cualquier factor adicional (documentado a continuación o en un memorando separado) concluya sobre la eficacia general del control interno a nivel de empresa (proveer una base para la conclusión de la gerencia, si no es obvia).

ANEXO No. 2: PROGRAMACIÓN EN AUDITORÍA EN BASE A RIESGOS[35]

I. Elementos básicos del programa de auditoría

1. Metodología para definir puntos críticos, objetivos específicos de auditoría y determinar los procedimientos de auditoría a aplicar (en base a riesgos)

Los siguientes corresponden a los pasos a considerar en la etapa de programación, para determinar los elementos que corresponden a esta sección. En esta descripción de pasos propuestos se incluye desde el levantamiento de información relativa a riesgos, controles y objetivos operativos realizado a través de matrices, los criterios para la evaluación y determinación de puntos críticos en el proceso a auditar, hasta la determinación de los objetivos específicos de auditoría y los respectivos procedimientos y pruebas de auditoría que se deben aplicar para satisfacerlos.

a. Análisis del proceso, subproceso o etapa a auditar

Parte fundamental de la programación, corresponde al conocimiento que el auditor tiene de todos los elementos estratégicos (internos y externos) que afectan el proceso que se va a auditar. Entre estos elementos deben considerarse los sistemas de información, la estructura organizacional, subprocesos, los planes y políticas, el sistema de control interno, los controles operativos existentes, las normas internas, las leyes y regulaciones y todos los elementos que sean necesarios para asegurar un conocimiento acabado. Una forma de interiorizarse de la estructura y aspectos relevantes del proceso o subproceso, es la revisión de los flujogramas de los mismos, o cuando no existan, y cuando sea posible, la confección de ellos por parte del auditor.

En base al estudio del proceso a auditar, se debe construir como primer paso (en forma previa a la formación de objetivos de auditoría específicos y pruebas de auditoría) una "Matriz preliminar de riesgo operativo". Un ejemplo del formato y la estructura y, escalas de valorización sugeridas, se presentan en el punto II Esquema de Análisis Propuesto y en el Anexo No. 5, respectivamente.

---

[35] Consejo de Auditoría Interna General de Gobierno. Programación en Auditoría en Base a Riesgos [en línea]. Consultado el 3 de diciembre de 2009. Disponible en: http://www.auditoriainternadegobierno.cl/index.php/menu/show/id/25

Esta “Matriz preliminar de riesgo operativo” servirá especialmente como guía para determinar los puntos críticos del proceso, cuyos controles mitigantes asociados a los riesgos serán evaluados a través de procedimientos o pruebas de cumplimiento y sustantivas.

El nivel de desagregación de la “Matriz preliminar de riesgo operativo” dependerá del nivel de desagregación con que se desarrolló la matriz de riesgos estratégica. Esto es, si se determinó a nivel de proceso el área crítica contenida en el plan anual, entonces se deberá realizar la desagregación comenzando desde el nivel de proceso. Si la matriz se desarrolló a nivel de subproceso, entonces el análisis se debe realizar comenzando desde ese nivel y así sucesivamente si el plan anual está configurado con áreas criticas a nivel de etapas.

En este documento técnico, el nivel de desagregación de los procesos se realiza bajo el supuesto que la matriz de riesgo estratégico se desarrolló sólo a nivel de proceso, por lo que en los ejemplos se analizará cada subproceso y las etapas correspondientes en cada uno de éstos.

b. Reconocimiento de objetivos operativos

Una vez determinadas dentro del proceso o subprocesos a auditar, las etapas relevantes que los componen, deben identificarse cuáles son los objetivos que se espera lograr en la gestión de cada una de esos subprocesos o etapas. Este objetivo debería ser formal y obtenerse de la documentación escrita que existe en los servicios (reglamentos, términos de referencia, bases administrativas y técnicas, etc.) y también en base a entrevistas con los ejecutivos y encargados de los procesos o subprocesos. (Esta información debe ser utilizada en la formulación de la “Matriz preliminar de riesgo operativo”).

Es necesario aclarar que en este punto no se está haciendo referencia a los objetivos específicos de auditoría, que se detallan más adelante en este documento.

c. Identificación de riesgos operativos relevantes

Conocidos los objetivos operativos por subproceso o etapa a analizar, de ellos se derivarán los riesgos relevantes que el auditor debe determinar, esto es, identificar los hechos o acontecimientos no deseados que provoquen incumplimiento del objetivo operativo; también los hechos que provoquen que no ocurra un acontecimiento deseado, afectando el cumplimiento de los objetivos y metas especificas del subproceso o etapa que se está evaluando. (Esta información debe ser utilizada en la formación de la "Matriz preliminar de riesgos operativo").

d. Identificación del nivel de severidad del riesgo

Identificados los riesgos operativos relevantes, es necesario identificar el nivel de severidad que presenta dicho riesgo, en términos de probabilidad de impacto.

La probabilidad puede ser medida con criterios de frecuencia o teniendo en cuenta la presencia de factores internos y externos que puedan propiciar el riesgo, aunque éste no se haya presentado nunca.

El impacto se refiere a las consecuencias que puede ocasionar en el proceso y a la organización la materialización del riesgo, y en general puede ser medido en base a criterios cualitativos. (Escalas de medición sugeridas para probabilidad e impacto se presentan en Anexo 5)

e. Identificación y clasificación de la eficiencia de controles claves (detalles y antecedentes se presentan en Anexo 5 – punto 2 y Anexo 6)

Realizada la identificación de los riesgos operativos relevantes en el proceso, deben identificarse los controles existentes, cuyo propósito es mitigar la materialización de esos riesgos en el proceso. También es posible que producto de este análisis se determine inexistencia de controles asociados a los riesgos.

La evaluación de la eficiencia de esos controles, debe considerar el nivel de cumplimiento con normas específicas, lo que sirve para determinar su robustez y en forma

complementaria, debe considerarse aspectos de calidad en su diseño, en relación con la prevención de la ocurrencia de riesgos, tales como, oportunidad, periodicidad y grado de automatización en la aplicación de los controles. (Esta información debe ser utilizada en la formulación de la “Matriz preliminar de riesgo operativo”)

En este punto, es importante señalar que cuando un riesgo tenga más de un control asociado, será necesario concluir del análisis de auditoría realizado, cuáles controles son claves para mitigar el riesgo y cuáles deben eliminarse o fortalecerse de acuerdo a su relación costo beneficio.

f. Determinación preliminar del nivel de exposición del riesgo

El nivel de exposición preliminar se determinará ya sea por la diferencia aritmética o cuociente aritmético (éste último será utilizado en este documento) entre el nivel de severidad del riesgo y el nivel de eficiencia del control. Este análisis entregará una pauta para determinar en cuales puntos críticos los controles deben ser probados mediante procedimientos de auditoría, con la finalidad de determinar si cubren adecuadamente el nivel de severidad del riesgo. (Esta información debe ser utilizada en la formulación de la “Matriz preliminar de riesgo operativo”)

Todo el análisis realizado hasta este punto, es decir, la desagregación de los procesos, el análisis de objetivos operativos, el análisis de riesgos, controles mitigantes y exposición al riesgo, podría haber sido efectuado en la etapa de planificación, al construir la matriz de riesgo estratégica, en base a un modelo que considerara en forma rigurosa las variables antes señaladas para cada proceso crítico. En ese caso, sólo se debe actualizar dicha matriz en lo referente al proceso en análisis y determinar cuáles son los puntos críticos a evaluar, considerando para este efecto, los criterios definidos en el punto siguiente. (Particularmente en este caso, la matriz de riesgo estratégica actualizada en el proceso a auditar, corresponderá a la matriz preliminar de riesgo operativo del proceso)

g. Determinación de los puntos críticos a auditar

De la “Matriz preliminar de riesgo operativo” deben derivarse los puntos críticos a auditar. Para determinarlos es posible utilizar diversos criterios, pudiendo optar por los riesgos con

mayores niveles de severidad (probabilidad x impacto) o los riesgos con mayores niveles de exposición (severidad del riesgo v/s eficiencia del control). También puede considerarse riesgos que presenten una alta probabilidad (por ejemplo; casi certeza), independiente del nivel de impacto del riesgo que tengan o riesgos que presenten un grado de impacto muy relevante (por ejemplo; catastróficas), independientemente del nivel de probabilidad de ocurrencia determinado.

En todo caso, el criterio adoptado finalmente debe ser debidamente justificado por el auditor, señalando en forma expresa en el programa de auditoría, cual fue el criterio utilizado para la elección de los puntos críticos y su fundamento.

Sin perjuicio de lo anteriormente señalado, en los casos en los cuales no se tenga información acerca de la eficiencia de los controles claves (por ejemplo, informes de auditorías anteriores, informes de control operativo, entre otros.), se sugiere utilizar para la determinación de puntos críticos, un criterio distinto al de la exposición al riesgo, ya que ésta pudiese estar distorsionada debido a que su cálculo y clasificación se realiza en base a controles teóricos que no han sido validados y de los cuales no se tiene información confiable.

Por otra parte, cuando se trate de niveles de exposición al riesgo relevantes (por ejemplo, No aceptable o Mayor), y se cuente con información confiable de que los controles mitigantes de esos riesgos son claramente insuficientes, es recomendable informar en forma inmediata a la jefatura del servicio, para que se tomen las medidas preventivas o correctivas necesarias para bajar el nivel de exposición determinado. Procedimiento que debe efectuarse antes de realizar la auditoría, y en el transcurso de ésta, cuando sea posible, analizar y monitorear el estado de implementación de las medidas comprometidas por la organización.

h. Definición de objetivos específicos de auditoría en el programa

Una vez identificados los puntos críticos, con sus respectivos riesgos relevantes que podrían impedir el logro de las objetivos definidos por el servicio para cada etapa relevante e identificados los controles asociados a cada riesgo y el respectivo nivel de

exposición en la “Matriz preliminar de riesgo operativo”, es oportuno y necesario definir los objetivos específicos de auditoría que se incorporarán en el programa.

Los objetivos específicos de auditoría corresponden a la finalidad del trabajo del auditor, fijada en relación a los objetivos generales de auditoría y al nivel y tipo de riesgo detectado. Permiten orientar el trabajo para evaluar y determinar cuál es el nivel del riesgo residual efectivo que presenta un riesgo específico o el proceso completo.

En definitiva, los objetivos específicos deben guardar estrecha relación con los objetivos generales definidos en el programa, debiéndose procurar que el resultado de la auditoría permita cumplirlos adecuadamente. Deben ser coherentes con la descripción de los riesgos operativos identificados, puesto que al cumplir un objetivo de auditoría específico exitosamente, debe concluirse sobre el nivel de exposición al terminar la auditoría.

i. Formulación de procedimientos para alcanzar los objetivos específicos de auditoría

Para satisfacer o alcanzar los objetivos específicos de auditoría determinados, se deben diseñar procedimientos o pruebas de auditoría (de cumplimiento o sustantivos) para determinar el nivel de eficiencia y calidad de los controles mitigantes asociados al riesgo identificado.

Es necesario tener presente que en el diseño de estos procedimientos o pruebas, ya sean de cumplimiento o sustantivos, se debe considerar el tiempo estimado que se requiere para su aplicación. Este elemento debe ser coherente con los objetivos generales de la auditoría, el alcance de la auditoría, los métodos para determinar las muestras de auditoría y la oportunidad y periodo. Estos elementos del programa se sugieren presentar y listar por escrito, en un formato similar al ejemplo dispuesto en Anexo No. 4.

Una variable relevante en la definición de la naturaleza y extensión de las pruebas de cumplimiento y sustantivas a aplicar, es el nivel de riesgo de auditoría que determine el auditor previamente.

Una vez que se han definido completamente las pruebas o procedimientos de auditoría, tanto en su naturaleza, extensión y oportunidad, se ha concluido la formulación del programa de auditoría, que será el documento guía que utilizará el auditor para efectuar su revisión y obtener evidencia adecuada en cantidad y calidad de los hallazgos y debilidades de control que se informarán posteriormente al jefe de servicio.

Finalmente, la aplicación del programa de auditoría debe ser supervisada rigurosamente durante su aplicación y al final de la auditoría, con la finalidad de alcanzar exitosamente los objetivos generales y específicos de auditoría dispuestos en el programa. Producto de estas supervisiones, es probable que dicho programa pueda ser ajustado en el transcurso de la auditoría, con la finalidad de adecuarlo a nuevas necesidades.

j. Construcción de la matriz final de riesgos del proceso, a la fecha de la auditoría

Cuando la auditoría esté terminada, es decir, después de aplicado el programa en la etapa de ejecución y obtenido el resultado y conclusión final de la auditoría, se deberá ajustar y actualizar la “Matriz preliminar de riesgo operativo” del proceso, en base a los niveles de eficiencia del control analizado y por consiguiente del nivel de exposición al riesgo. Generándose después de esta actualización, la “Matriz final de riesgo del proceso”, a la fecha de la auditoría.

Este mecanismo permitirá reflejar finalmente el nivel y clasificación de los controles mitigantes, el nivel y clasificación de la exposición por riesgo específico, por etapa, por subproceso o por proceso según corresponda, en forma coincidente con la oportunidad de envío del informe remitido a la dirección.

El formato y estructura de la “Matriz final de riesgos del proceso”, obviamente es el mismo que se utiliza para la “Matriz preliminar de riesgos operativo”. Ver ejemplo en el punto II. Esquema de análisis propuesto.

II. Resumen esquema de análisis propuesto

De acuerdo a lo detallado en el presente documento, los pasos a seguir para definir puntos críticos, objetivos específicos de auditoría y los procedimientos a aplicar en base a riesgos, se pueden resumir en los siguientes:

- Una vez determinados los procesos críticos a auditar en el plan anual de auditoría (en base a la matriz de riesgo estratégico construida en la etapa de planificación), se deben definir los objetivos generales de cada auditoría;

- Dependiendo de la profundidad del análisis realizado previamente en la matriz de riesgo estratégico en la etapa de planificación, se debe desagregar en un nivel adecuado el proceso a auditar, de acuerdo con sus características y estructura organizacional:

    - Identificar en el nivel de desagregación que corresponda, los objetivos operativos formales;

    - Identificar los riesgos operativos relevantes que afectarían a los objetivos operativos identificados; y

    - Construir una “Matriz preliminar de riesgo operativo” que considere objetivos operativos, riesgos, controles y niveles de exposición para el proceso. (La matriz de riesgo estratégico construida por la organización en la etapa de planificación podría considerar todas estas variables, por lo que se puede actualizar y utilizar cuando corresponda);

- Determinar en base a la “Matriz preliminar de riesgo operativo” los puntos críticos del proceso, subproceso o etapa a evaluar en la auditoría;

- Determinar los objetivos específicos de auditoría que se perseguirán en el desarrollo de la labor y que permitirán orientar la evaluación del nivel de riesgo residual operativo, por cada punto crítico en el proceso, subproceso o etapa;

- Formular los procedimientos o pruebas de cumplimiento o sustantivos para evaluar la eficiencia de los controles mitigantes existentes. Estos procedimientos deben formularse con la finalidad de satisfacer los objetivos de auditoría específicos definidos en el programa; y

- Finalmente, se deben presentar y listar por escrito en el programa de auditoría; los puntos críticos, los objetivos específicos y las actividades y procedimientos a aplicar (se sugiere un formato similar al ejemplo dispuesto en Anexo No. 4).

En páginas siguientes, se presenta un ejemplo del esquema sugerido para determinar los procedimientos de auditoría en base a la metodología explicada en este documento, la que incluye la “Matriz preliminar de riesgo operativo”.

En el desarrollo de este ejemplo, se considera el supuesto que de acuerdo a los recursos existentes para ejecutar el programa de auditoría y al análisis de variables estratégicas, tales como: horas hombre, viáticos, tareas en desarrollo, confiabilidad del sistema de control interno del proceso, etc., la cantidad de riesgos y etapas consideradas a auditar están debidamente sustentadas.

Complementariamente a lo anterior, se considera como supuesto que se tiene poca información acerca de la existencia y nivel de operación de los controles, de modo que se ha considerado como criterio para determinar los puntos críticos, los riesgos que presentan los dos mayores niveles de Severidad (la de calificación Extrema y el mayor valor de las calificadas como Alto) determinados en la “Matriz preliminar de riesgo operativo” para las etapas analizadas de este proceso. El nivel de severidad del riesgo y el nivel de exposición por riesgo específico provienen de esa matriz.

Para la elaboración de dicha matriz (Página No 179), se utilizó las siguientes escalas y procedimientos de cálculo y clasificación consideradas en el esquema No. 1:

ESQUEMA No. 1: ESCALAS UTILIZADAS PARA LA MATRIZ DE RIESGOS

CONCEPTO	PÁGINAS – ESCALAS	PROCEDIMIENTOS DE CLASIFICACIÓN O CÁLCULO
Probabilidad de ocurrencia	Página No 184	Categoría y valor de acuerdo a nivel de escala.
Impacto de ocurrencia	Página No 184	Categoría y valor de acuerdo a nivel de escala.
Severidad del riesgo	Página No 184	Categoría y valor de acuerdo a nivel en escala y análisis de normas de control
Nivel eficiencia del control	Páginas Nos 186 a la 188 Páginas Nos 190 a la 200	Categoría y valor de acuerdo a nivel en escala y análisis de normas de control
Nivel exposición al riesgo de procesos y subprocesos	Página No 188 a la 189	Cuociente entre el nivel de severidad del riesgo y el nivel de eficiencia del control

JEMPLO: ESQUEMA DE ANALISIS PROPUESTO Y MATRIZ PRELIMINAR DE RIESGO OPERATIVO

bjetivo general de auditoría: Evaluar los niveles de eficiencia obtenidos en el ciclo de adquisición de productos, en términos de calidad, cantidad y portunidad, en base a requerimientos organizaciones.

ROCESOS	SUBPROCESOS	ETAPAS – PUNTOS CRÍTICOS	OBJETIVOS OPERATIVOS DE LA ETAPA	RIESGOS OPERATIVOS (Nivel de exposición o nivel de severidad)	OBJETIVOS ESPECIFICOS DE AUDITORÍA	PROCEDIMIE NTOS DE AUDITORÍA (CUMPLIMIENTO Y SUSTANTIVOS) PARA DETERMINAR LA EFICIENCIA DE LOS CONTROLES EXISTENTES EN BASE A LA POBLACIÓN O MUESTRAS
astecimiento el exposición Media (3,0)	Planificación Nivel exposición = Media (3,4)	Definición de necesidades compra por producto (cantidades) Nivel exposición = Media (3,5)	Asegurar que se adquieran las cantidades necesarias por producto, para abastecer las necesidades de la institución. Otros...	Deficiencia y errores en la definición de cantidades de compra de productos, en relación a las necesidades de la organización. Nivel exposición = Mayor (4) Nivel de severidad = Extremo (16) Otros...	Examinar si las adquisiciones por producto efectuadas por el Depto. De Adquisiciones, se ajustan a las necesidades de la organización. Otros...	Pruebas de cumplimiento: (Determinar) - Existencia de sistemas de información que entreguen información oportuna, completa y veraz, sobre niveles de existencia disponibles por productos. - Existencia de procedimientos que consideren aprobaciones de adquisiciones por producto antes de la orden de compre. Otros... Pruebas sustantivas: - Evaluar y analizar la información de compra establecida en el Plan de Compras por producto, en relación con las necesidades de la institución. - Comparar cantidades de compra por producto contempladas en planes de compra originales con los correspondientes ajustes solicitados y realizados, durante el periodo por las unidades operativas. Otros...
		Otros...	Otros...	Otros...	Otros...	Otros...
		Definición de especificaciones técnicas (Características y calidades) Nivel exposición = Menor (2,8)	Asegurar que las especificaciones técnicas de los bienes que se adquieren, satisfacen las necesidades de la institución. Otros...	Deficiencias y errores en la definición de requisitos técnicos para compra de productos, en relación a las necesidades de la organización. Nivel de exposición = Menor (2,4) Nivel de severidad = Alto (12) Otros...	Calificar la calidad y pertinencia de los mecanismos y técnicas utilizadas para definir especificaciones técnicas por las unidades operativas. Otros...	Pruebas de cumplimiento: (Determinar) - Existencia de instancias de control formales para evaluar las especificaciones técnicas respecto de los productos insertos en el Plan de Compras. - Existencia de aprobaciones previas a la entrega de requerimientos técnicos. - Existencia de sistemas de información que permitan controlar las características del producto recepcionado en relación con los requerimientos técnicos. Otros... Pruebas sustantivas: - Examinar y evaluar las especificaciones existentes, mediante el concurso de personal técnica especialista. - Examinar origen, periodo y frecuencia de problemas de producción, relacionados con deficiencias en especificaciones técnicas de productos adquiridos. Otros...
		Otros...	Otros...	Otros...	Otros...	Otros...

Análisis y niveles de severidad y/o exposición al riesgo obtenidos de la "Matriz preliminar de riesgo operativo"

Definición realizada por el auditor en base a los análisis de riesgo realizados en el proceso.

EJEMPLO: "MATRIZ PRELIMINAR DE RIESGO OPERATIVO" DISEÑADA EN FORMA PREVIA A LA IDENTIFICACION DE PUNTOS CRITICOS, FORMULACION DE OBJETIVOS ESPECIFICOS DE AUDITORIA Y PROCEDIMIENTOS O PRUEBAS DE AUDITORIA.

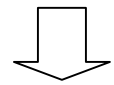
PROCESO	SUBPROCESO	ETAPAS (PUNTOS CRITICOS)	OBJETIVO OPERATIVO DE LA ETAPA	RIESGOS OPERATIVOS IDENTIFICADOS						CONTROLES CLAVES EXISTENTES					CLASIFICACIÓN DE EXPOSICIÓN AL RIESGO	
				DESCRIPCION DEL RIESGO	PORBABILIDAD		IMPACTO		SEVERIDAD DEL RIESGO	VALOR	DESCRIPCION DEL CONTROL	NIVEL EFICIENCIA			VALOR	NIVEL	VALOR
					CLASIFC	VALOR	CLASIFIC	VALOR				PD	O	A			
Abastecimiento Nivel exposición promedio = Media (3,0)	Planificación Nivel exposición promedio = Media (3,4)	Definición de necesidades de compra por producto (cantidades) Nivel exposición promedio = Media (3,5)	Asegurar que se adquieren las cantidades por producto necesarias para abastecer las necesidades de la institución.	Deficiencias y errores en la definición de cantidades de compra de productos, en relación a las necesidades de la organización.	Probable	4	Mayores	4	Extremo	16	Existe un sistema de información informático que entrega información histórica y proyectada, cada 4 meses, la que se utiliza como base para la programación de compras para productos.	Pd	Pv	At	4	4	Mayor
				Sistemas de información no entregan información actualizada y oportuna sobre niveles de stock.	Improb.	2	Moderado	3	Moderado	6	Existe contrato con una empresa externa para mantención y protección de los sistemas. En el ámbito físico y lógico. El jefe de finanzas monitorea este contrato.	Oc	Pv	Sa	2	3	Media
		Otros...	Otros...	Otros...	x	X	x	x	x	X	Otros...	x	x	x	x	x	X
		Definición de especificaciones técnicas (características y calidades) Nivel exposición promedio = Menor (2,8)	Asegurar que las especificaciones técnicas de los bienes que se adquieren, satisfacen las necesidades de la institución.	Faltan capacidades técnicas del personal para definir especificaciones	Moderado	3	Moderado	3	Alto	9	La empresa realiza capacitaciones al personal encargado cada 6 meses en materias técnicas.	Pd	Dt	Ma	3	3	Media
				Deficiencias y errores en la definición de requisitos técnicos para compra de productos, en relación a las necesidades de la organización.	Probable	4	Moderado	3	Alto	12	Existe Comité técnico que una vez al año analiza los productos y los avances tecnológicos con el fin de adecuar y actualizar los requerimientos técnicos que se solicitan. Para cada adquisición, se reúne una Comisión que analiza la compra y especifica a la luz de los criterios del Comité.	Pe	Pv	Ma	5	2,4	Menor
				No se encuentran Proveedores de bienes en el mercado de acuerdo a las especificaciones técnicas.	Moderado	3	Moderado	3	Alto	9	Cada 6 meses se hace un estudio de los proveedores que existen en el mercado y que productos y condiciones técnicas ofrecen.	Pd	Dt	Ma	3	3	Media

ANEXO No. 3: EJEMPLO DE RELACIONES BÁSICAS EN LA ETAPA DE PROGRAMACIÓN EN AUDITORÍA[36]

A objeto de describir una relación global entre riesgos y objetivos generales y específicos, procedimientos generales, medios para obtener evidencia y elementos a considerar en la obtención de evidencia, a continuación se presenta el siguiente esquema:

ESQUEMA No. 2: RELACIONES ENTRE OBJETIVOS GENERALES Y ESPECÍFICOS

OBJETIVO GENERAL DE AUDITORÍA PARA EL PROCESO CRÍTICO INCLUIDO EN EL PLAN ANUAL								
Conocer	Comprender	Explicar	Sintetizar	Interpretar	Deducir	Analizar	Evaluar	Otros…



OBJETIVOS OPERATIVOS DEL PROCESO O SUBPROCESO O ETAPA	IDENTIFICACIÓN DE RIESGOS OPERATIVOS, ASOCIADOS A LOS OBJETIVOS OPERATIVOS	OBJETIVOS ESPECÍFICOS DE AUDITORÍA ASOCIADOS AL RIESGO OPERATIVO Y AL OBJETIVO GENERAL	PROCEDIMIENTOS GENERALES PARA SATISFACER LOS OBJETIVOS DE AUDITORÍA	MEDIOS PARA OBTENER EVIDENCIA DE AUDITORÍA EN BASE A MUESTRAS O POBLACIÓN	ELEMENTOS A CONSIDERAR EN LA OBTENCIÓN DE LA EVIDENCIA DE AUDITORÍA
Categorizar… Clasificar…	Deficiencias o errores en la… Falta de transparencia …	Examinar… Conocer…		• Examen físico • Confirmación • Cálculo • Documentación • Observación • Procedimientos analíticos • Otros…	• Naturaleza y Fuente • Integridad • Disponibilidad y accesibilidad • Autorizaciones • Formatos • Completitud • Firmas • Almacenamiento • Otros…
Transferir… Vincular…	Transferencia incompleta… Falta de autorización…	Deducir… Medir…			
Establecer… Estructurar…	Falta de coherencia de… Falta de claridad en los…	Interrelacionar … Vincular…			
Identificar… Ordenar…	Omisión de… Desconocimiento de…	Relacionar… Inferir…			
Originar… Pronosticar…	Inexistencia de… Falta de oportunidad del…	Analizar… Comparar…			
Resolver… Sintetizar…	Incumplimiento de… Procesamiento incompleto…	Distinguir… Validar… Relacionar…			
Desarrollar…	Seguridad	Identificar…			

[36] Ibid., p. 18.

Diseñar… 	insuficiente… Falta de recursos…	Evaluar… Medir…			
Organizar… Realizar…	Falta de claridad en la comunicación … Calidad insuficiente…	Distinguir… Comparar…			
Reconocer… Sintetizar…	Inexistencia de información… Déficit en competencias …	Calificar… Evaluar…			
Obtener… Adquirir…	Seguimiento inadecuado… Cláusulas deficientes…	Analizar… Determinar…			
Producir… Procesar…	Deficiencia en el control… Ineficiencias en producción…	Revisar… Chequear…			
Otros…	Otros…	Otros…			

ANEXO No. 4: EJEMPLO FORMATO BÁSICO PARA PRESENTAR Y LISTAR EN EL PROGRAMA DE AUDITORÍA: PUNTOS CRÍTICOS, OBJETIVOS ESPECÍFICOS DE AUDITORÍA Y ACTIVIDADES Y PROCEDIMIENTOS A APLICAR[37]

	Nombre del documento: Procedimiento de auditoría para…	Número: … Código: …
		Versión:…
		Página: … de….

1. Tipo de objetivo de control
2. Proceso, subproceso o etapa a auditar y materia de auditoría
3. Equipo de auditores y responsable del equipo
4. Objetivos generales de auditoría
5. Alcance de la auditoría
6. Oportunidad y periodo
7. Horas de auditoría
8. Cronograma especifico para realizar la auditoría
9. Fuentes de información operacional y legal
10. Criterio utilizado para definir los puntos críticos a auditar (severidad, impacto, exposición al riesgo, etc.)

11. Definición de puntos críticos, objetivos específicos de auditoría y procedimientos de auditoría a aplicar (de cumplimiento y sustantivos)

PUNTOS CRÍTICOS	OBJETIVOS ESPECÍFICOS DE AUDITORÍA	DETALLE ACTIVIDADES Y PROCEDIMIENTOS AUDITORÍA	REF. P/T	TIEMPO (HRS.) ESTIMADO APLICACIÓN DE PROCEDIMIENTO

REF. P/T = Referencia a papeles de trabajo

CONTROL DE AUDITORES PARTICIPANTES EN EL PROGRAMA		
AUDITOR (S) QUE ELABORÓ	**AUDITOR(S) QUE REVISÓ**	**AUDITOR(S) QUE AUTORIZÓ**
Nombre:	Nombre:	Nombre:
Firma:	Firma:	Firma:
Fecha:	Fecha:	Fecha:

[37] Ibid., p. 19.

ANEXO No. 5: ESCALAS DE VALORACIÓN SUGERIDA PARA CONSTRUIR LA MATRIZ DE RIESGOS[38]

1. Severidad del riesgo

1.1. ESQUEMA No. 3: CATEGORÍAS DE PROBABILIDAD

CATEGORÍA	VALOR	DESCRIPCIÓN
Casi certeza	5	Riesgo cuya probabilidad de ocurrencia es muy alta, es decir, se tiene un alto grado de seguridad que éste se presente. (90% a 100%)
Probable	4	Riesgo cuya probabilidad de ocurrencia es alta, es decir, se tiene entre 66% a 89% de seguridad que éste se presente.
Moderado	3	Riesgo cuya probabilidad de ocurrencia es media, es decir, se tiene entre 31% a 65% de seguridad que éste se presente.
Improbable	2	Riesgo cuya probabilidad de ocurrencia es baja, es decir, se tiene entre 11% a 30% de seguridad que éste se presente.
Muy improbable	1	Riesgo cuya probabilidad de ocurrencia es muy baja, es decir, se tiene entre 1% a 10% de seguridad que éste se presente.

1.2. ESQUEMA No. 4: CATEGORÍAS DE IMPACTO

CATEGORÍA	VALOR	DESCRIPCIÓN
Catastróficas	5	Riesgo cuya materialización influye gravemente en el desarrollo del proceso y en el cumplimiento de sus objetivos, impidiendo finalmente que éste se desarrolle.
Mayores	4	Riesgo cuya materialización dañaría significativamente el desarrollo del proceso y el cumplimientos de sus objetivos, impidiendo que éste se desarrolló en forma normal.
Moderados	3	Riesgo cuya materialización causaría un deterioro en el desarrollo del proceso dificultando o retrasando el cumplimiento de sus objetivos, impidiendo que éste se desarrolle en forma adecuada.
Menores	2	Riesgo que causa un daño menor en el desarrollo del proceso y que no afecta mayormente el cumplimiento de sus objetivos estratégicos.
Insignificantes	1	Riesgo que puede tener un pequeño o nulo efecto en el desarrollo del proceso y que no afecta el cumplimiento de sus objetivos estratégicos.

1.3. ESQUEMA No. 5: NIVEL DE SEVERIDAD DEL RIESGO

NIVEL PROBABILIDAD (P)	NIVEL IMPACTO (I)	SEVERIDAD DEL RIESGO S = (P x I)
Casi Certeza (5)	Catastróficas (5)	Extremo (25)
Casi Certeza (5)	Mayores (4)	Extremo (20)
Casi Certeza (5)	Moderadas (3)	Extremo (15)
Casi Certeza (5)	Menores (2)	Alto (10)
Casi Certeza (5)	Insignificantes (1)	Alto (5)

[38] Ibid., p. 20.

Probable (4)	Catastróficas (5)	Extremo (20)
Probable (4)	Mayores (4)	Extremo (16)
Probable (4)	Moderadas (3)	Alto (12)
Probable (4)	Menores (2)	Alto (8)
Probable (4)	Insignificantes (1)	Moderado (4)
Moderado (3)	Catastróficas (5)	Extremo (15)
Moderado (3)	Mayores (4)	Extremo (12)
Moderado (3)	Moderadas (3)	Alto (9)
Moderado (3)	Menores (2)	Moderado (6)
Moderado (3)	Insignificantes (1)	Bajo (3)
Improbable (2)	Catastróficas (5)	Extremo (10)
Improbable (2)	Mayores (4)	Alto (8)
Improbable (2)	Moderadas (3)	Moderado (6)
Improbable (2)	Menores (2)	Bajo (4)
Improbable (2)	Insignificantes (1)	Bajo (2)
Muy improbable (1)	Catastróficas (5)	Alto (5)
Muy improbable (1)	Mayores (4)	Alto (4)
Muy improbable (1)	Moderadas (3)	Moderado (3)
Muy improbable (1)	Menores (2)	BAJO (2)
Muy improbable (1)	Insignificantes (1)	BAJO (1)

En el esquema se muestra el resultado de la combinación entre las categorías del nivel de impacto del riesgo y las categorías del nivel de probabilidad de ocurrencia del riesgo, es decir, el nivel de severidad.

De este esquema se puede observar que las categoría de impacto tienen una mayor incidencia en el nivel de severidad asignado, puesto que aunque la probabilidad de ocurrencia sea menor al tratarse de riesgos con impactos altos, cualquier materialización del riesgo (aunque sea en sólo una oportunidad) tendrá una consecuencia significativa en el cumplimiento de los objetivos del proceso examinado.

Esto explica los casos en que a igual valor, la severidad del riesgo de distinta. A modo de ejemplo se presentan las siguientes relaciones:

NIVEL PROBABILIDAD (P)	NIVEL IMPACTO (I)	SEVERIDAD DEL RIESGO S = (P x I)
Muy improbable (1)	Mayores (4)	Alto (4)
Probable (4)	Insignificantes (1)	Moderado (4)
Probable (4)	Moderadas (3)	Alto (12)
Moderado (3)	Mayores (4)	Extremo (12)

2. Clasificación del control clave

2.1. Diseño del control

ESQUEMA No. 6: OPORTUNIDAD DE ACCIÓN DEL CONTROL (O)

CLASIFICACIÓN	DESCRIPCIÓN
Preventivo (Pv)	Controles claves que actúan antes o al inicio de un proceso.
Correctivo (Cr)	Controles claves que actúan durante el proceso y que permiten corregir las deficiencias.
Detectivo (Dt)	Controles claves que sólo actúan una vez que el proceso ha terminado.

ESQUEMA No. 7: PERIODICIDAD EN LA ACCIÓN DEL CONTROL (PD)

CLASIFICACIÓN	DESCRIPCIÓN
Permanente (Pe)	Controles claves aplicados durante todo el proceso, es decir, en cada operación.
Periódico (Pd)	Controles claves aplicados en forma constante sólo cuando ha transcurrido un periodo especifico de tiempo.
Ocasional (Oc)	Controles claves que se aplican sólo en forma ocasional en un proceso.

ESQUEMA No. 8: AUTOMATIZACIÓN EN LA APLICACIÓN DEL CONTROL (A)

CLASIFICACIÓN	DESCRIPCIÓN
100% automatizado (At)	Controles claves incorporados en el proceso, cuya aplicación es completamente informatizada. Están incorporados en los sistemas informatizados.
Semi – automatizado (Sa)	Controles claves incorporados en el proceso, cuya aplicación es parcialmente desarrollada mediante sistemas informatizados.
Manual (Ma)	Controles claves incorporados en el proceso, cuya aplicación no considera uso de sistemas informatizados.

ESQUEMA No. 9: ESCALA DE CLASIFICACIÓN DE LA EFICIENCIA DE LOS CONTROLES

REQUISITO EN CUMPLIMIENTO CON NORMA DE CONTROL	CARACTERÍSTICAS DISEÑO CONTROL CLAVE/FUNDAMENTAL			CLASIFICACIÓN	VALOR DEL DISEÑO DEL CONTROL
	PERIODICIDAD (PD)	OPORTUNIDAD (O)	AUTOMATIZACIÓN (A)		
Cumplimiento adecuado	Permanente Permanente Permanente	Preventivo Preventivo Preventivo	Informatizado Semi informat Manual	Óptimo	5
Cumplimiento adecuado	Permanente Permanente Permanente	Correctivo Correctivo Correctivo	Informatizado Semi informat Manual		
Cumplimiento adecuado	Permanente Permanente Permanente	Detectivo Detectivo Detectivo	Informatizado Semi informat Manual	Bueno	4
Cumplimiento adecuado	Periódico Periódico Periódico	Preventivo Preventivo Preventivo	Informatizado Semi informat Manual		
Cumplimiento adecuado	Periódico Periódico Periódico	Correctivo Correctivo Correctivo	Informatizado Semi informat Manual	Más que regular	3
Cumplimiento adecuado	Periódico Periódico Periódico	Detectivo Detectivo Detectivo	Informatizado Semi informat Manual		
Cumplimiento adecuado	Ocasional Ocasional Ocasional	Preventivo Preventivo Preventivo	Informatizado Semi informat Manual	Regular	2
Cumplimiento adecuado	Ocasional Ocasional Ocasional	Correctivo Correctivo Correctivo	Informatizado Semi informat Manual		
Cumplimiento adecuado	Ocasional Ocasional Ocasional	Detectivo Detectivo Detectivo	Informatizado Semi informat Manual	Deficiente	1
Insuficiente	No determinado	No determinado	No determinado	Inexistente	1

En el esquema anterior, se señala que en primer lugar se debe evaluar si el control mitigante asociado a un riesgo, tiene un nivel de cumplimiento adecuado respecto de las normas de control. Esto implica realizar un análisis integral de las referidas normas (segregación, autorización formalización, etc.) y determinar si las normas que se requieren de acuerdo con la naturaleza del control examinado en particular se cumplen.

Producto de este análisis, se puede dar que las normas se cumplan satisfactoriamente, es decir, que el control está sustentado en una estructura básica sólida. Posteriormente, se debe seguir con el análisis del diseño del control, este aspecto es relevante, ya que los

riesgos son por naturaleza dinámicos y requieren que los controles tengan una estructura que se oriente a la prevención de la materialización del efecto de los riesgos.

Finalmente, se debe clasificar el nivel de eficiencia del control examinado, de acuerdo con el esquema presenta, asignándole el valor respectivo según la escala.

En caso que esto no ocurra, es decir, las normas no presentan un cumplimiento suficiente en el control examinado, debe entenderse que su nivel de cumplimiento es insuficiente y corresponde clasificarlo como si se tratara de un control inexistente, con valoración de 1, sin que ya sea necesario evaluar la eficiencia en el diseño del control respecto de la ocurrencia del riesgo.

En caso que no exista control, obviamente no será necesario probarlo mediante procedimientos y pruebas de auditoría, ni verificar si su diseño está orientado a mitigar el riesgo. Por consiguiente debe clasificarse como inexistente con nivel de eficiencia del control examinado de 1, de acuerdo con la escala contenida en el esquema presentado.

Posteriormente, en la etapa de formación del informe, debe describirse la situación de inexistencia de control y los efectos reales o potenciales para la organización. Debiendo adicionalmente el auditor, aportar a la disminución del nivel de exposición determinado mediante propuestas de medidas correctivas y preventivas, que contribuyan a un adecuado control y administración del riesgo (por ejemplo mediante sugerencias de diseño e implementación de controles con características apropiadas de periodicidad, oportunidad y automatización en relación al riesgo asociado).

Ante inconsistencias entre la medición y la opinión profesional del auditor prevalece esta última, debidamente fundada.

3. Niveles de clasificación del nivel de exposición al riesgo

La exposición al riesgo está determinada por la severidad del riesgo dividida por eficiencia del control asociado a ese riesgo. Estos elementos se obtienen de las relaciones detalladas anteriormente en los apartados: nivel de severidad del riesgo y nivel de eficiencia del control.

A continuación se presenta la escala de nivel de exposición al riesgo que los califica:

ESQUEMA No. 10: ESCALA DEL NIVEL DE EXPOSICIÓN AL RIESGO

INDICADOR DE EXPOSICIÓN AL RIESGO	VALOR	NIVEL DE EXPOSICIÓN AL RIESGO
Nivel severidad del riesgo Nivel eficiencia del control	8,0 – 25,0	No aceptable (Na)
	4,0 – 7,99	Mayor (Ma)
	3,0 – 3,99	Media (Md)
	0,2 – 2,99	Menor (Me)

Tal como se señaló, la escala previamente presentada, ha sido construida en base a la relación entre el nivel de severidad del riesgo (Bajo, Moderado, Alto, Extremo) y el nivel de eficiencia del control asociado a ese riesgo (Deficiente, Regular, Más que regular, Bueno, Óptimo). Dicha relación se presenta en el esquema No. 11.

Un primer análisis de dicha escala observaría que los niveles de exposición al riesgo Mayor y No Aceptable, pudiesen tener un rango muy extenso de valores; 4,0 a 7,99 y 8,0 a 25 puntos respectivamente, pero al realizar un análisis más riguroso, se debería observar que en realidad los niveles de exposición al riesgo con valores más altos, corresponden en general a las combinaciones entre los niveles de riesgo más severos y los niveles de eficiencia del control más bajos, o a las combinaciones entre los riesgos con severidad más altas y con controles que tienen un nivel de eficiencia sólo de regular.

Por otra parte, los niveles de exposición al riesgo más bajos están conformados en general por las combinaciones entre los niveles de riesgos menos severas y los niveles de eficiencia del control más altos, o por las combinaciones entre riesgos con severidades bajas y controles con niveles de eficiencia deficiente o regular, o por las combinaciones entre riesgos con severidad altas, pero con controles con nivel de eficiencia óptimo o bueno.

Por ejemplo, en el esquema No. 11 se observa que el nivel de exposición al riesgo E1 = 10, (Nivel de exposición al riesgo No Aceptable) está conformado por un nivel de severidad del riesgo, Extremo = 20 y un nivel de eficiencia de control, Regular = 2.

En el caso del nivel de exposición E2 = 4 (Nivel de exposición al riesgo Mayor), está conformado por un nivel de severidad del riesgo, Alto = 12 y un nivel de eficiencia de control, Más que Regular = 3.

Finalmente, el nivel de exposición E3 = 1 (Nivel de exposición al riesgo Menor), está conformado por un nivel de severidad del riesgo, Alto = 5 y un nivel de eficiencia de control, Óptimo = 5.

ESQUEMA No. 11: RELACIONES ENTRE SEVERIDAD DEL RIESGO Y EFICIENCIA DEL CONTROL QUE DETERMINAN LA ESCALA DEL NIVEL DE EXPOSICIÓN AL RIESGO

			NIVEL DE CONTROL				
			ÓPTIMO	BUENO	MAS QUE REGULAR	REGULAR	DEFICIENTE
			5	4	3	2	1
NIVEL DEL RIESGO	EXTREMO	25	**5**	**6,25**	**8,33**	**12,5**	**25**
		20	4	5	6,67	10	20
		16	3,2	4	5,33	8	16
		15	3	3,75	5	7,5	15
	ALTO	12	2,4	3	4	6	12
		10	2	2,5	3,33	5	10
		9	1,8	2,25	3	4,5	9
	MODERADO	8	1,6	2	2,67	4	8
		6	1,2	1,5	2	3	6
		5	1	1,25	1,67	2,5	5
		4	0,8	1	1,33	2	4
	BAJO	3	0,6	0,75	1	1,5	3
		2	0,4	0,5	0,67	1	2
		1	0,2	0,25	0,33	0,5	1

ANEXO No. 6: CONCEPTOS GENERALES SOBRE NORMAS DE CONTROL[39]

1. Definición de control

El Control es la función administrativa que consiste en medir el desempeño individual y organizacional para asegurar que las actividades se ajusten a los planes y mitiguen adecuadamente los riesgos.

2. Normas básicas de control

Las normas básicas son los mecanismos o procedimientos que permiten alcanzar los objetivos de control. Estas normas comprenden las políticas específicas, los procedimientos, los planes de la organización (incluida la división de las tareas) y los dispositivos físicos y lógicos (tales como cerraduras o alarmas contra incendio y controles en las aplicaciones computacionales), si bien no se limitan exclusivamente a estos aspectos. Los controles deben proporcionar una seguridad razonable de que se logren continuamente los objetivos del control interno. Para ello, deben ser eficaces y estar diseñados de forma que operen como un sistema integrado y no individualmente.

Los controles, para que sean eficaces, deben cumplir con el propósito previsto en la aplicación real. Es posible que los controles diseñados para funcionar en un ambiente manual no sean eficaces en uno automatizado. Por consiguiente, los controles seleccionados deben cumplir el propósito previsto y funcionar siempre que el caso lo requiera. En cuanto a su eficiencia, los controles deben estar diseñados para poder obtener el máximo beneficio con un esfuerzo adecuado. Los controles que se examinen para verificar su eficacia y suficiencia deben ser los que se utilizan en la práctica y deben ser evaluados periódicamente para asegurar su aplicación constante en la prevención de riesgos.

Los controles que se presentan a continuación son los que se utilizan generalmente en una estructura de control interno ordenada y eficaz. Los métodos y procedimientos específicos que se describen en relación a cada uno de ellos, no pretenden ser exhaustivos sino que deben ser considerados como ejemplos. Entre otros se cuentan: la documentación, el registro oportuno y adecuado de las transacciones y hechos, autorización y ejecución de las

---

[39] Ibid., p. 26.

transacciones y hechos, división de las tareas, supervisión y acceso a los recursos y registros y responsabilidad ante los mismos.

a) Documentación en papel y medios electrónicos

Deben documentarse las estructuras de control interno y todas las transacciones y hechos internos, incluyendo sus objetivos y procedimientos de control, y todos los aspectos pertinentes de las transacciones y hechos significativos. Asimismo, la documentación en papel y electrónica debe estar disponible y ser fácilmente accesible para su verificación por el personal apropiado y los auditores.

La documentación relativa a las estructuras de control interno debe incluir aspectos sobre la estructura y políticas de una institución, sobre sus categorías operativas, objetivos y procedimientos de control. Esta información debe figurar en documentos tales como planes o guías, las políticas administrativas y los manuales de operación y de contabilidad.

La documentación sobre transacciones y hechos significativos debe ser completa y exacta y facilitar el seguimiento de la transacción o hecho, antes, durante y después de su realización.

La documentación de las estructuras de control interno, de las transacciones y de hechos importantes debe tener un propósito claro, ser apropiada para alcanzar los objetivos de la institución y servir a los directivos para controlar sus operaciones y a los auditores para analizar dichas operaciones.

En los casos en que existen sistemas informáticos integrados en la institución, que generen como soporte respaldatorio de las operaciones, documentos electrónicos con existencia legal, se deberá obtener evidencia electrónica respecto del origen, firmas, integridad, completitud, archivo o registro, accesibilidad y disponibilidad y no-repudio de la información.

b) Registro oportuno y adecuado de las transacciones y hechos

Las transacciones y hechos importantes deben registrarse inmediatamente y debidamente clasificados.

Las transacciones deben registrarse en el mismo momento en que ocurren a fin de que la información siga siendo relevante y útil para los directivos que controlan las operaciones y

adoptan las decisiones pertinentes. Ello es válido para todo el proceso o ciclo de vida de una transacción; abarcando el inicio y la autorización, todos los aspectos de la transacción mientras se realiza y su anotación final en los registros. También conviene actualizar rápidamente toda la documentación con objeto de mantener su validez.

Se requiere, asimismo, una clasificación pertinente de las transacciones y hechos a fin de garantizar que la dirección disponga continuamente de una información fiable. Una clasificación pertinente significa organizar y procesar la información a partir de la cual se elaboran los informes, los planes y los estados financieros y presupuestarios.

El registro inmediato y pertinente de la información es un factor esencial para asegurar la oportunidad y fiabilidad de toda la información que la institución maneja en sus operaciones y en la adopción de decisiones.

En los casos en que existen sistemas informáticos integrados en la institución, que generan como soporte respaldatorio de las operaciones, documentos electrónicos con existencia legal, se deberá obtener evidencia electrónica respecto de la firma, integridad, completitud y archivo o registro.

c) Autorización y ejecución de las transacciones y hechos

Las transacciones y hechos relevantes solo podrán ser autorizados en papel o electrónicamente y ejecutados por aquellas personas que actúen dentro del ámbito de sus competencias.

La dirección es quien decide el canje, la transferencia, la utilización o la asignación de fondos para atender metas específicas en condiciones particulares. La autorización es la principal forma de asegurar que sólo se efectúen transacciones y hechos válidos de conformidad con lo previsto por la dirección. La autorización debe estar documentada física o electrónicamente y ser comunicada explícitamente a los directivos y a los empleados, incluyendo los términos y condiciones específicos conforme a los cuales se concede una autorización. La conformidad con los términos de una autorización significa que los empleados ejecutan las tareas que les han sido asignadas de acuerdo con las directrices y dentro del ámbito de competencias establecido por la dirección o la legislación.

En los casos en que existen sistemas informáticos integrados en la institución, que generan como soporte respaldatorio de las operaciones, documentos electrónicos con existencia legal, se deberá obtener evidencia electrónica respecto del origen, firmas e integridad de la información.

d) División o segregación de las tareas

Las tareas y responsabilidades principales ligadas a la autorización, tratamiento, registro y revisión de las transacciones y hechos deben ser asignadas a personas diferentes.

Con el fin de reducir el riesgo de errores, despilfarros o actos ilícitos, o la probabilidad de que no se detecten este tipo de problemas, es preciso evitar que todos los aspectos fundamentales de una transacción u operación se concentren en manos de una sola persona o sección. Las funciones y responsabilidades deben asignarse sistemáticamente a varias personas para asegurar un equilibrio eficaz entre los poderes. Entre las funciones claves figuran la autorización y el registro de las transacciones, la emisión y el recibo de los haberes, los pagos y la revisión o fiscalización de las transacciones. Sin embargo, la colusión puede reducir o eliminar la eficacia de esta técnica de control interno.

Una pequeña organización puede que no tenga suficientes empleados para aplicar esta técnica plenamente. En tal caso, la dirección debe ser consciente del riesgo que ello implica y compensar el defecto con otros controles. La rotación del personal contribuye a que los aspectos centrales de las transacciones o hechos contables no se concentren en una sola persona por un espacio de tiempo prolongado. Debe promoverse e incluso exigirse también el uso del período vacacional anual para ayudar a reducir estos riesgos.

e) Supervisión

Debe existir una supervisión para garantizar el logro de los objetivos de control interno. Los supervisores deben examinar y aprobar cuando proceda, el trabajo encomendado a sus subordinados. Asimismo, deben proporcionar al personal las directrices y la capacitación necesarias para minimizar los errores, el despilfarro y los actos ilícitos y asegurar la comprensión y cumplimiento de las directrices específicas de la dirección.

La asignación, revisión y aprobación del trabajo del personal exige:

- Indicar claramente las funciones y responsabilidades del trabajo del empleado;
- Examinar sistemáticamente el trabajo de cada empleado, en la medida que sea necesario; y
- Aprobar el trabajo en puntos críticos del desarrollo para asegurarse de que avanza según lo previsto.

La asignación, revisión y aprobación del trabajo del personal debe tener como resultado el control apropiado de sus actividades. Ello incluye: la observancia de los procedimientos y requisitos aprobados, la constatación y eliminación de los errores, los malentendidos y las prácticas inadecuadas, la reducción de las probabilidades de que ocurran o se repitan actos ilícitos y el examen de la eficiencia y eficacia de las operaciones. La delegación del trabajo de los supervisores no exime a estos de la obligación de rendir cuentas de sus responsabilidades y tareas.

f) Acceso a los recursos y registros y responsabilidades ante los mismos

El acceso a los recursos y registros debe limitarse a las personas autorizadas para ello, quienes están obligadas a rendir cuentas de la custodia o utilización de los mismos. Para garantizar dicha responsabilidad, se debe cotejar periódicamente los recursos con los registros y verificar si coinciden. La frecuencia de estas comparaciones depende de la vulnerabilidad y relevancia de los activos.

La restricción del acceso físico y lógico a los recursos permite reducir el riesgo de una utilización no autorizada o de pérdida y contribuir al cumplimiento de las directrices de la dirección. El grado de limitación depende de la vulnerabilidad de los recursos y del riesgo potencial de pérdida. Ambos deben evaluarse periódicamente. Por ejemplo, el acceso a los documentos sumamente vulnerables y la responsabilidad ante los mismos, tales como cheques en blanco, puede restringirse:

- Manteniéndolos en una caja fuerte;
- Asignando a cada documento un número de serie;
- Encargando su custodia a personas responsables; y
- Al determinarse la vulnerabilidad de un activo, debe considerarse también su costo, la facilidad de transporte y el riesgo de pérdida o de utilización indebida.

En los casos en que existen sistemas informáticos integrados en la institución, que generan como soporte respaldatorio de las operaciones, documentos electrónicos con existencia legal, se deberá obtener evidencia electrónica respecto del origen, firmas, integridad y accesibilidad y disponibilidad. Además de deberá evaluar los niveles de seguridad de los accesos lógicos a las base de datos de la organización.

3. Principales normas específicas de control en marco integrado de control interno, Modelo C.O.S.O.

Estas normas se presentan a modo de sugerencia, puesto que su existencia y características dependen del tipo de control y de la estructura del proceso, entre otras variables.

- Normas relativas al ambiente de control:

    - Ambiente propicio para el control;
    - Actitud de apoyo superior al control interno;
    - Valores de integridad y ética;
    - Administración eficaz del potencial humano;
    - Estructura organizativa formal y conocida;
    - Delegación formal y adecuada;
    - Coordinación de acciones organizacionales;
    - Participación del personal en el control interno; y
    - Adhesión a las políticas institucionales.

- Normas relativas a la evaluación de riesgos:

    - Identificación y evaluación de riesgos;
    - Planificación formal;
    - Indicadores de desempeño mensurables;
    - Divulgación de los planes;
    - Definición y comunicación de políticas de apoyo a los objetivos;
    - Revisión de los objetivos; y
    - Cuestionamiento periódico de los supuestos de planificación.

- Normas relativas a las actividades de control:

    - Prácticas y medidas de control formales;
    - Control integrado;
    - Análisis de costo/beneficio;
    - Responsabilidad delimitada;
    - Instrucciones por escrito;
    - Separación de funciones incompatibles;
    - Autorización y aprobación de transacciones y operaciones;
    - Documentación de procesos y transacciones;
    - Supervisión constante;
    - Registro oportuno;
    - Sistema contable y presupuestario;
    - Acceso a activos y registros;
    - Revisiones de control permanentes;
    - Conciliación periódica de registros;
    - Inventarios periódicos;
    - Arqueos independientes;
    - Formularios uniformes;
    - Rotación de labores;
    - Toma oportuna de vacaciones;
    - Garantías a favor de la institución; y
    - Dispositivos de control y seguridad lógicos y físicos.

- Normas relativas a información y comunicación:

    - Obtención y comunicación de información efectivas;
    - Calidad y suficiencia de la información;
    - Sistemas de información;
    - Controles sobre sistemas de información;
    - Canales de comunicación abiertos; y
    - Archivo institucional formal.

- Normas relativas al monitoreo:

    - Monitoreo constante del control interno en operación;

- Monitoreo de las actividades;
- Monitoreo constante del ambiente de control;
- Evaluación del desempeño institucional;
- Informes de seguimiento a responsables;
- Rendición de cuentas;
- Reporte de deficiencias;
- Toma de acciones correctivas; y
- Asesoría externa para monitoreo del control interno.

4. Identificación y análisis de controles claves

Identificados los riesgos, es necesario identificar y analizar los controles claves existentes en la institución, los que teóricamente mitigan los riesgos, esto es, todas las medidas que ha tomado la administración con la finalidad de evitar la ocurrencia de un riesgo potencial. Estos controles deben ser evaluados en el nivel de cumplimiento de normas de control y calificados de acuerdo a su diseño, es decir, su oportunidad (en que momento del proceso se aplican; preventivos, correctivos, detectivos), periodicidad (si son permanentes, periódicos u ocasionales), grado de automatización (manual, semi automatizado, 100% automatizado) y evaluados en términos del cumplimiento de normas específicas de control.

Una vez determinada claramente la existencia de todos los controles asociados a los riesgos relevantes que operan en el proceso en estudio, será necesario en primer lugar, definir si existe uno o más controles asociados a cada riesgo específico identificado.

Cuando exista más de un control por riesgo específico, será necesario identificar si se trata de controles cuya presencia es clave o fundamental para mitigar la ocurrencia del riesgo, o si alguno de los controles no tienen esa característica y sólo se trata de controles que no contribuyen significativamente a mitigar el riesgo. En general para este último tipo de controles, es recomendable informar a la Dirección, para su eliminación o fortalecimiento, si corresponde (relación costo/beneficio).

Cuando se identifique que un riesgo específico tiene varios controles asociados y éstos tienen distinto nivel de eficiencia medida en forma individual, el auditor debe sólo evaluar

el nivel de eficiencia que se genera al actuar en conjunto los distintos controles clasificados como claves, desechando para efectos de este análisis a los controles no fundamentales (ver ejemplo en páginas siguientes).

El segundo paso corresponde a determinar (identificar, analizar y cuantificar) el nivel de eficiencia de los controles en base al diseño del control y cumplimiento de normas específicas de control. Nivel definida por los atributos periodicidad, oportunidad y nivel de automatización del control en base al esquema que se presenta en la página siguiente.

El siguiente paso corresponde a analizar para cada uno de los controles claves identificados con los riesgos, el grado de cumplimiento de normas específicas de control.

En resumen, lo que se persigue con este procedimiento, no es sólo verificar la existencia y el grado de cumplimiento de normas específicas para todos los controles, sino que evaluar si existen controles claves o fundamentales asociados a un riesgo en particular y si éstos además de cumplir con normas específicas están diseñados con la finalidad de mitigar los efectos que se puedan producir ante la materialización del riesgo.

A continuación se presenta un procedimiento que permite dejar evidencia del análisis realizado al auditor. Para este efecto, se sugiere utilizar el siguiente esquema:

ESQUEMA No. 12: ANÁLISIS DE CONTROLES CLAVES

ETAPA	RIESGO RELEVANTE	DESCRIPCIÓN DEL CONTROL IDENTIFICADO EN EL PROCESO (ASOCIADO A UN RIESGO DETERMINADO)	IMPORTANCIA DEL CONTROL PRESENTE PARA MITIGAR LOS RIESGOS AL INTERIOR DEL PROCESO	
			CLAVE/ FUNDAMENTAL	NO ES FUNDAMENTAL

Ejemplo de determinación de una evaluación de la eficiencia de los controles claves:

ESQUEMA No. 13: IDENTIFICACIÓN DE CONTROLES CLAVES EN ETAPA DE CÁLCULO DE HORAS EXTRAORDINARIAS

ETAPA	RIESGO RELEVANTE	DESCRIPCIÓN DEL CONTROL IDENTIFICADO EN EL PROCESO (ASOCIADO A UN RIESGO DETERMINADO)	IMPORTANCIA DEL CONTROL PRESENTE PARA MITIGAR LOS RIESGOS AL INTERIOR DEL PROCESO	
			CLAVE/ FUNDAMENTAL	NO ES FUNDAMENTAL
Cálculo de horas extraordinarias	Errores o irregularidades en el cálculo de las horas extraordinarias	El sistema de control biométrico registra las horas trabajadas y calcula aquellas que exceden de las 44 horas ordinarias.	**X**	
		El jefe de la Unidad de remuneraciones revisa y aprueba el cálculo de horas para su pago.	**X**	
		El encargado de remuneraciones lleva un archivador con el detalle de las horas extras por funcionario.		**X**

ESQUEMA No. 14: ANÁLISIS DEL CUMPLIMIENTO DE NORMAS DE CONTROL EN EL CONTROL MITIGANTE EXAMINADO

RIESGO RELEVANTE	NIVEL DE CUMPLIMIENTO DE NORMAS DEL CONTROL ASOCIADO NIVELES DE CUMPLIMIENTO DE NORMAS: ADECUADO, REGULAR, INSUFICIENTE					
	DOCUMENTA-CIÓN	REGISTRO	AUTORIZA-CIÓN	DIVISIÓN O SEGREGA-CIÓN	SUSPENSIÓN	ACCESO
Errores o irregularidades en el cálculo de las horas extraordinarias	Nivel adecuado	Nivel adecuado	Nivel adecuado	Nivel adecuado	Nivel adecuado	Nivel regular
Conclusión del nivel de cumplimiento de las normas: **Adecuado**						

ESQUEMA No. 15: DETERMINACIÓN DE LA EFICIENCIA DE LOS CONTROLES CLAVES

CONTROLES CLAVES/FUNDAMENTA-LES	NIVEL DE CUMPLIMIEN-TO DE NORMAS ESPECÍFI-CAS DE CONTROL	CARACTERÍSTICAS EN EL DISEÑO DEL CONTROL CLAVE/FUNDAMENTAL				
		OPORTUNI-DAD	PERIODICI-DAD	AUTOMATIZA-CIÓN	CLASIFICA-CIÓN	VALOR
El sistema biométrico de control horario, contiene un algoritmo que calcula las horas trabajadas, indicando en forma precisa aquellas que exceden de las 44 semanales. El jefe de remuneraciones revisa el reporte del sistema y aprueba el cálculo para su pago.	Adecuado respecto de las normas de control	Preventivo (previene errores y se encuentra al principio del proceso)	Periódico (a la fecha de corte mensual para pago)	Automatizado y Manual	Óptimo	5