Universidad Nacional Autónoma de México
Facultad de Contaduría y Administración
Sistema Universidad Abierta y Educación a Distancia

Licenciatura en Contaduría

Sistemas de Control Interno

SUAyED

COLABORADORES

DIRECTOR DE LA FCA
Dr. Juan Alberto Adam Siade

SECRETARIO GENERAL
L.C. y E.F. Leonel Sebastián Chavarría

– – – –

COORDINACIÓN GENERAL
Mtra. Gabriela Montero Montiel
Jefe de la División SUAyED-FCA-UNAM

COORDINACIÓN ACADÉMICA
Mtro. Francisco Hernández Mendoza
FCA-UNAM

– – – –

AUTOR
Lic. Rosa Elena Ruíz Aguilar
Mtro. Jorge Escutia Serrano

DISEÑO INSTRUCCIONAL
Lic. Dayanira Granados Pérez

CORRECCIÓN DE ESTILO
Lic. Francisco Vladimir Aceves Gaytán

DISEÑO DE PORTADAS
L.CG. Ricardo Alberto Báez Caballero
Mtra. Marlene Olga Ramírez Chavero
L.DP. Ethel Alejandra Butrón Gutiérrez

DISEÑO EDITORIAL
Mtra. Marlene Olga Ramírez Chavero

OBJETIVO GENERAL

Al concluir el curso el alumno conocerá el marco de control aplicable en México, identificará los objetivos y elementos del control interno en la estructura de una entidad, reconocerá sus aspectos normativos y los aplicará a la evaluación de las entidades.

TEMARIO OFICIAL
(64 horas)

	Horas
1. Aspectos generales del control interno	4
2. Teoría del riesgo y del control y sus aplicaciones	6
3. Modelos de control interno	18
4. Normatividad nacional sobre el estudio y evaluación del control interno y su metodología	24
5. Normas internacionales aplicables al estudio y evaluación del control interno	6
6. Tendencias	6
Total	64

INTRODUCCIÓN

Con el paso del tiempo el concepto de ‘control’ ha ido evolucionando y perfeccionándose con la finalidad de hacer frente a las necesidades actuales de las empresas.

La globalización y el avance tecnológico han originado grandes e importantes cambios no sólo en la emisión de la información financiera sino también en la operación de las entidades. Todas las empresas, independientemente de su tamaño o actividad, requieren de controles que les ayuden a elevar el grado de cumplimiento de sus objetivos.

El control interno ayuda a las organizaciones a detectar con oportunidad cualquier desviación significativa en el cumplimiento de las metas y objetivos establecidos que pudieran afectar sus operaciones y, por lo tanto, las declaraciones contenidas en sus Estados Financieros (EEFF).

En los últimos años, el tema de control interno ha tomado gran relevancia, las crisis financieras y los problemas de fraude, suscitados en Estados Unidos, provocaron la emisión de nuevas formas de implementar, mejorar y perfeccionar el control interno, pero no sólo eso, las autoridades también han emitido nuevas disposiciones de carácter prudencial en materia de control.

En este trabajo se analizará, en seis unidades, los aspectos fundamentales en materia de control interno, desde sus orígenes y aplicación hasta las tendencias que existen hoy en día.

En la unidad 1, se analizará los aspectos generales del control interno, sus orígenes, importancia e implementación, se conocerá en qué consiste la función de auditoría y cuál es su responsabilidad en relación con el control. En la unidad 2, se estudiará el

análisis de riesgos y controles, así como su aplicación dentro de la empresa. En la unidad 3 se verán los nuevos modelos de control interno que se aplican en la actualidad. La unidad 4 incluye una síntesis de las principales disposiciones normativas, aplicables al estudio y evaluación del control interno. La unidad 5 comprende una síntesis de algunas de las disposiciones emitidas en Estados Unidos en materia de control. Por último, en la unidad 6, se apreciarán las tendencias actuales relacionadas con el control interno.

ESTRUCTURA CONCEPTUAL

Unidad 1.
Aspectos generales del control interno

OBJETIVO PARTICULAR

Comprender los fundamentos y aspectos teóricos generales que conforman la teoría del Control Interno, a fin de que el alumno entienda la importancia de su aplicación y operación dentro de las entidades así como las responsabilidades del auditor sobre los mismos.

TEMARIO DETALLADO

(4 horas)

1. Aspectos generales del control interno

1.1. Aspectos Generales del Control Interno
1.2. Estructura del Control Interno
1.3. Objetivos del Control Interno
1.4. Definiciones relacionadas con Control Interno (Sistema, Control, Riesgo, Control Interno y Sistema de Control Interno)
1.5. Responsabilidad del auditor (Interno / Externo)

INTRODUCCIÓN

Todas las entidades, independientemente de su tamaño o actividad, requieren de controles que les ayuden a lograr sus objetivos.

Una entidad es una unidad identificable que realiza actividades económicas, constituida por una combinación de recursos humanos y financieros, coordinados por una autoridad que toma decisiones. Las operaciones que realiza la entidad son registradas contablemente y reportadas como información a través de los estados financieros (EEFF)[1].

Los EEFF son documentos que contienen las declaraciones que los administradores de la entidad hacen sobre su situación financiera y el resultado de sus operaciones.

En términos generales, la importancia del Control Interno radica en que su principal propósito es detectar con oportunidad cualquier desviación significativa en el cumplimiento de las metas, así como objetivos establecidos que pudieran afectar las operaciones de la entidad y, por lo tanto, las declaraciones contenidas en los EEFF.

El Control Interno promueve la eficiencia de las operaciones, ayuda a reducir los riesgos a que pudieran estar expuestos los recursos, aporta mayor confiabilidad a la información financiera y operacional, proporciona mayor seguridad respecto al cumplimiento efectivo de las leyes, normas y políticas aplicables.

En este tema se conocerá qué es el control interno, cuáles sus objetivos y elementos, se identificará su importancia e implementación en las entidades, se verá en qué consiste la función de auditoría y su responsabilidad en relación con el control interno.

[1] Consejo Mexicano para la Investigación y Desarrollo de Normas de Información Financiera [CINIF]. (2006). *Normas de Información Financiera*. México, D.F.

1.1. Aspectos Generales del Control Interno

Sir Adrian Cadbury dijo: “la gobernabilidad corporativa trata del modo en el que se dirige y controla una empresa” (en Pickett, 2007, p. 33). Si el consejo de administración está al mando de su empresa y se cumplen todas las normas adecuadas, los accionistas conseguirán beneficiarse de estos hechos. Pensemos que, cuando todo está bajo control, eso significa que todos los riesgos previsibles para el éxito de la empresa se han anticipado y se han analizado de la forma más eficiente posible. Esto por sí solo no ofrece la garantía de conseguir el éxito, pero significa que existe una posibilidad razonable de que la empresa mantenga o, incluso, supere las expectativas del mercado.

Pickett (2007) en su libro *Manual básico de auditoría interna* señala que para subrayar la necesidad de mantener un control, el informe anual que publican aquellas empresas que cotizan en la bolsa de valores y la mayor parte del sector público o de organismos públicos deberá incluir una exposición sobre el control interno. Esta exposición es un tema de fundamental importancia que viene dado por los sistemas complejos de disposiciones de procesos y de relaciones que se han establecido dentro de la empresa. Si esos controles llevan a la empresa hacia adelante y, al mismo tiempo, afrontan todos los riesgos conocidos que amenazan la trayectoria positiva, entonces se puede decir que existe un buen sistema de control interno.

Por otro lado, debido a la globalización de las organizaciones y de la actividad económica en el mundo, se ha hecho indispensable el desarrollo armónico de sistemas que otorguen certidumbre a los inversionistas y público en general sobre el correcto funcionamiento de las organizaciones; por ello los distintos organismos y agrupaciones de profesionales relacionados con temas financieros y empresariales tanto nacionales como internacionales se han preocupado por armonizar estos temas y hacerlos

entendibles y accesibles para todos los interesados, tal es el caso de los temas relacionados con el Control Interno.

Relacionado con los temas desde el interior de las entidades, el control interno se entiende como el conjunto de planes, políticas y procedimientos que han sido diseñados por la administración de una organización con el fin de prevenir, detectar y corregir cualquier problema o desviación de los objetivos planteados por la misma que le impidan obtener información financiera confiable y oportuna, así como cumplir con las regulaciones; por otro lado, el control interno es de suma importancia, ya que fomenta la eficiencia en la operación y reduce el riesgo en la pérdida de valor de los activos.

Por su parte, desde la óptica de la Auditoría, y, de acuerdo con las Normas de Auditoría, el estudio y evaluación del Control Interno, es efectuado con el objeto de cumplir con la norma de ejecución del trabajo que requiere que el auditor efectúe un estudio y evaluación adecuados del control interno existente que le sirva de base para determinar el grado de confianza que va a depositar en el mismo y que a su vez le permita determinar la naturaleza, alcance y oportunidad de los procedimientos que va a efectuar.

Visto en conjunto, el Control interno adquiere importancia en todos los ámbitos, ya que su adecuada implementación y su correcto funcionamiento dan certeza del adecuado desarrollo y operación de la organización a todos los interesados, y garantiza la adecuada aplicación de los procedimientos de auditoría, dando certeza a la información generada por la organización, así como de las operaciones efectuadas por las entidades.

1.2. Estructura del Control Interno

Elementos del control interno[2]

De acuerdo con el **modelo COSO**, un sistema de control interno consta de **cinco elementos** interrelacionados entre sí. Dichos elementos, provienen de la manera en la cual la Administración de una empresa lleva a cabo sus responsabilidades y están integrados en su proceso de administración.

Los **elementos** que integran un sistema de control interno son:

Elementos del control

Aunque estos elementos se aplican en todas las entidades, las empresas pequeñas y medianas los implementan de manera diferente a las grandes empresas. Sus controles pueden ser menos formales y menos estructurados, aunque una pequeña empresa puede, sin embargo, tener un efectivo control interno.

[2] Véase, The Committee of Sponsoring Organizations. (1992). *Informe COSO*, disponible en línea: www.coso.org

A continuación se explican cada uno de estos elementos:

Ambiente de control

El ambiente de control, (véase SAS o Declaraciones sobre Normas de Auditoría), es el componente básico de la organización, el cimiento de apoyo de los demás componentes del control interno. Aporta disciplina, estructura y refleja la actitud general en la entidad, la conciencia y acciones de la administración y sus propietarios respecto a la importancia de los controles y el peso que ejercen en la determinación de las políticas, sus procesos y estructura organizacional.

El ambiente de control establece el tono de la organización al influir sobre la conciencia de control de su personal, por lo tanto afecta a las probabilidades de información financiera fraudulenta y la sustracción de activos.

El ambiente de control está integrado a su vez por los siguientes factores:

Factores que integran el ambiente de control

A continuación se explica cada uno de los factores que integran el ambiente de control.

Conciencia de control y estilo operativo

La administración es responsable de dirigir y controlar las operaciones, así como de establecer, comunicar, vigilar sus políticas y procedimientos. El ambiente de control está influido principalmente por las acciones y decisiones de la administración.

La **conciencia de control** se refiere a la importancia que la administración le da al control interno. Es un concepto intangible que se puede definir como la actitud que la administración toma para asegurar que funcionen o no los controles.

En términos generales, la conciencia de control se refiere a las **actitudes y acciones que la administración asume**, en relación con:

- La importancia, cumplimiento y respeto de los controles.
- Las debilidades o errores que se le informan.
- La atención que presta a los sistemas de información.
- Las acciones que lleva a cabo ante o en condiciones inusuales.
- La actitud que toma ante presiones de los accionistas para alcanzar determinados resultados.

La conciencia de control se refleja en la sustancia de las políticas y procedimientos de la administración, en sus acciones, más que en su forma, porque pueden establecerse controles pero no cumplirse. Por lo tanto, para que la conciencia de control sea un aspecto eficaz del ambiente de control, la administración debe establecer controles apropiados y difundir su convicción sólida sobre la importancia de respetarlos.

Por ejemplo: si la dirección establece un plan para incrementar las ventas, pero ignora las políticas de crédito, no se debe esperar que el personal cumpla con los controles. En este caso la dirección no estableció con sus acciones un ambiente propicio para la ejecución efectiva del control interno.

El **estilo operativo** se refiere al grado de riesgo que asume la administración al establecer los juicios para preparar los EEFF. Está determinado por la integridad, motivación, competencia, habilidades, capacidad y aptitud que posea la administración. También incluye la importancia que la administración le brinda a la capacidad que requiere cada uno de los puestos considerados claves en la entidad. A mayor competencia del director, exigirá mayor conocimiento y experiencia a sus colaboradores.

Integridad y valores éticos

La integridad y los valores éticos son elementos esenciales del ambiente de control pues afectan el diseño, administración y vigilancia de los procesos clave de la entidad. La integridad y los valores son producto tanto de las normas éticas como del comportamiento de la administración, incluyen:

a) Las **acciones adoptadas** por la administración para eliminar o reducir incentivos y tentaciones que pueden invitar al personal a realizar actos deshonestos, ilegales o no éticos, que afecten la confiabilidad de la información financiera.	b) La **comunicación al personal** de los valores de la entidad, sus normas de comportamiento, mediante declaraciones de políticas y códigos de conducta, así como mediante ejemplos de los ejecutivos.

Un ejemplo, en relación con este factor, son los **códigos de conducta**, su existencia no asegura su cumplimiento, sin embargo, indica la importancia que tienen para la administración las normas de conducta.

Participación de la administración y del Comité de auditoría

El ambiente de control y la cultura de la organización están influidos en forma significativa por el Consejo de Administración y el Comité de Auditoría, el grado de independencia del Consejo o del Comité de Auditoría respecto de la administración, la experiencia, la calidad de sus miembros, grado de implicación, vigilancia y el acierto de sus acciones son factores que inciden en la eficacia del control interno.

El Comité de Auditoría es un órgano de vigilancia nombrado por el consejo de administración cuya función principal consiste en apoyar a la administración en la vigilancia de las políticas, procedimientos contables y de información financiera que se aplican en la entidad, además de las funciones de auditoría interna y externa.

Estructura organizacional

La estructura organizacional de una entidad proporciona el marco general dentro del cual se planean, ejecutan, controlan y vigilan sus actividades junto con sus operaciones, para lograr los objetivos de la empresa.

El establecimiento de una estructura organizacional adecuada incluye la consideración de las áreas clave de autoridad y responsabilidad, así como de las líneas apropiadas de información. Cada entidad desarrolla la estructura organizacional idónea para sus necesidades, de acuerdo con su tamaño y la naturaleza de sus actividades.

Elementos que integran la estructura organizacional de una empresa

Asignación de autoridad y responsabilidad

La asignación de autoridad y responsabilidad se refiere a las **políticas así como comunicaciones para asegurar que todo el personal comprende su función dentro de la empresa**, ayudan a que el personal reconozca cómo, de qué y por qué

es responsable; también sirven para identificar la fuente de autorización de las operaciones de la entidad.

Políticas y prácticas de recursos humanos

Las políticas y prácticas respecto a recursos humanos incluyen las actividades de:

Actividades de recursos humanos

La eficacia de las políticas, procedimientos y controles, generalmente depende de las personas que las ejecutan. Por lo tanto, la competencia e integridad del personal son elementos esenciales del ambiente de control.

La habilidad de la compañía para reclutar y retener suficiente personal competente y responsable depende, en gran medida, de sus políticas y prácticas sobre recursos humanos.

Por ejemplo la capacitación impartida por la empresa o por personal externo, comunican al personal funciones así como responsabilidades, muestran los niveles esperados de desempeño y comportamiento.

Evaluación de riesgos

Los **riesgos** son las acciones, eventos o circunstancias, internas o externas a la empresa que afectan su capacidad para lograr sus objetivos.

Los riesgos pueden afectar la existencia de la empresa, sin embargo, no existe una forma que garantice eliminarlos totalmente. Todas las entidades, independientemente de su tamaño, estructura, naturaleza o industria a la que pertenezcan, tienen riesgos en todos los niveles de su organización, la decisión de establecer **una empresa** es un riesgo.

La **administración** es la responsable de determinar el nivel de riesgo que su empresa puede aceptar y determinar acciones para mantenerlo en ese nivel. El nivel de riesgo apropiado para cada empresa varía en función de la naturaleza y circunstancias de cada negocio.

Algunas situaciones que generan riesgo pueden ser

- Cambios en el entorno de la entidad (ejemplo: nuevos reglamentos)
- Obsolescencia tecnológica
- Pérdida de mercado
- Dependencia hacia pocos clientes o proveedores
- Crecimiento o disminución acelerada
- La experiencia y competencia del responsable de una cuenta
- Personal nuevo
- Ubicación geográfica de la empresa o sucursales (incendios, huracanes, etc.)
- La naturaleza y complejidad de sus operaciones (materiales explosivos, químicos, etc.)

Los riesgos aumentan cuando la administración:

- Acepta compromisos sin considerar los riesgos originados.
- Firma contratos que exceden la capacidad de la empresa para cumplirlos.
- Debilita las políticas de crédito para aceptar nuevos clientes.
- Hace inversiones especulativas sin considerar coberturas de riesgos.
- No cumple con requerimientos legales o contractuales.

La **evaluación de riesgos** es un proceso en el cual una vez identificados los factores de riesgo, la administración considera su **importancia**, **la probabilidad de ocurrencia**, manejo o administración, establece a través de planes, programas o acciones, controles que prevengan o detecten:

- Riesgos específicos en la realización de sus actividades normales.
- Cambios importantes originados dentro de la empresa (ejemplo: una huelga).

- Cambios importantes en la normativa contable o legal que pudieran afectar el registro de las operaciones.
- Otros eventos que afectan el entorno operativo de la empresa (ejemplo: una devaluación).

Etapas del proceso de evaluación de riesgo

El propósito de esta evaluación es identificar, analizar y manejar los riesgos que pudieran afectar la capacidad de la empresa para lograr sus objetivos, es decir, aquellas situaciones que pudieran poner en peligro su continuidad de operación (problemas de negocio en marcha).

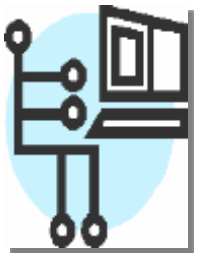
Ejemplo: La empresa *X*, SA, realiza el 100% de sus compras de materia prima en dólares.

Proceso de **evaluación de riesgos**:

1. Identificación del riesgo. Que ocurra una devaluación, lo cual provocaría un alza en el precio del dólar y por lo tanto el incremento de la deuda, lo que podría originar incapacidad de la empresa para cumplir con el pago de la obligación.

2. Probabilidad de ocurrencia: 60%.

3. Establecimiento de controles Adquisición de un instrumento de cobertura que garantice la compra del dólar a un precio previamente establecido.



Información y comunicación

Es el proceso de capturar e intercambiar la información necesaria para conducir, administrar y controlar las operaciones de una entidad. La calidad tanto de la información como la comunicación de una entidad afectan la toma de decisiones oportunas, en el control de sus actividades y en la preparación de información financiera confiable.

Información

Es el conjunto de datos generados por las operaciones y actividades (financieras y no financieras) que realiza una entidad. La información es necesaria en todos los niveles de la organización, para el logro de los objetivos.

a) Sistemas de información

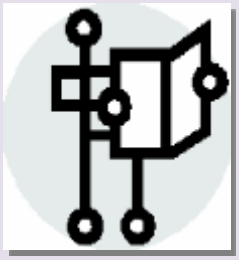
Los sistemas de información identifican, capturan, procesan los datos generados por las actividades y operaciones que realiza una entidad; también incluyen el reporte de los mismos, pueden ser computarizados, manuales o una combinación de ambos.

Al establecer los **sistemas de información en una entidad**, es necesario considerar, entre otros, los siguientes aspectos:

- Deben aportar a la dirección los informes necesarios sobre el desempeño de la empresa.
- Los reportes generados por los sistemas de información deben emitirse con oportunidad y contener el suficiente detalle para que sean de utilidad al personal idóneo.
- Deben existir controles que aseguren y vigilen la participación de los usuarios en el desarrollo, actualización y prueba de los programas de cómputo.
- Deben existir controles que aseguren el acceso a la información sólo a personas autorizadas para ello.
- Debe existir un plan de recuperación de desastres para todos los centros de datos primarios.

b) Sistemas de información financiera

Son los métodos y registros establecidos para contabilizar, procesar, resumir e informar sobre operaciones, eventos, condiciones de la empresa, y para mantener responsabilidad sobre los activos, pasivos e inversión de los accionistas. Un **sistema de información financiera** debe contener tanto métodos como registros que:



- Identifiquen y registren todas las operaciones ocurridas.
- Describan oportunamente las operaciones para su adecuada clasificación.
- Cuantifiquen el valor de las operaciones en términos monetarios apropiadamente en los estados financieros.
- Determinen la fecha en que las operaciones ocurrieron para registrarlas en el periodo contable correspondiente.
- Presenten adecuadamente las operaciones y las revelaciones en los EEFF.

Comunicación

La comunicación es el intercambio de información entre el personal idóneo para que descargue sus responsabilidades en tiempo y forma. La comunicación se realiza en todos los niveles de la organización a través de: manuales de políticas, procedimientos, de información financiera, memorandos, mensajes verbales y acciones de la administración.

Un **sistema efectivo de comunicaciones** debe contener:

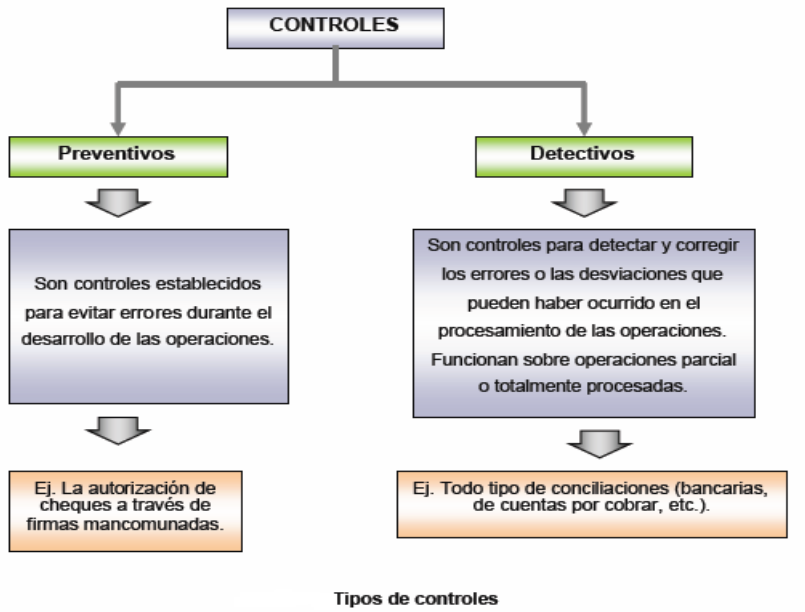
• Controles que aseguren la comunicación al personal de sus deberes y responsabilidades. • Mecanismos y canales de comunicación para que el personal reporte sospechas sobre irregularidades. • Controles para el manejo de situaciones inesperadas. • Controles para dar seguimiento oportuno a comunicaciones que recibe de compradores, proveedores, autoridades y otras entidades externas. • Controles que aseguren la comunicación de las normas éticas y políticas de la empresa tanto al personal como a entidades externas (compradores, proveedores).	

Actividades de control

Tanto las actividades como operaciones de una entidad se realizan conforme a políticas establecidas por la administración. Los controles son las políticas y procedimientos adicionales establecidos por la administración para prevenir y detectar riesgos, con ello proporcionar una seguridad razonable de lograr los objetivos en el desarrollo de las actividades y el registro de las operaciones de la entidad.

Su finalidad es la investigación de resultados inesperados o extraordinarios que permitan a la administración decidir acciones correctivas necesarias.

Los controles pueden ser:



Tipos de controles

Los controles tanto preventivos como de detección **varían** de acuerdo con el tipo de empresa; dependen de la naturaleza de las actividades y de la competencia, preferencias e imaginación de las personas que los diseñan.

La **efectividad** de los controles establecidos en una entidad disminuye el grado de riesgo, de posibles errores o irregularidades que afecten su información financiera.

Los procedimientos de control están dirigidos a cumplir con los siguientes objetivos:

Objetivos de control

a) Procesamiento de la información

Los controles implementados en el procesamiento de la información deben asegurar confiabilidad en la información contable y lograr los siguientes siete objetivos:

1. Que se contabilicen todas las operaciones.
2. Que todas las operaciones contabilizadas sean reales.
3. Que todas las operaciones estén valuadas conforme a las bases contables correspondientes.
4. Que todas las operaciones estén registradas en el periodo contable correspondiente.
5. Que todas las operaciones estén clasificadas correctamente.
6. Que todas las operaciones estén sumarizadas correctamente.
7. Que todas las operaciones estén transferidas al mayor correctamente.

Cabe mencionar que el procesamiento de la información financiera debe cumplir con los postulados básicos establecidos en las Normas de Información Financiera. De

acuerdo con la NIF A-1 “Estructura de las Normas de Información Financiera”.[3] Los postulados son los fundamentos que rigen el ambiente en el cual debe operar el sistema de información contable utilizado para el registro de las operaciones que afectan económicamente a una entidad.

Los postulados básicos son:

CLASIFICACIÓN	POSTULADOS BÁSICOS
a) Postulado que obliga a la captación de la esencia económica en la delimitación y operación del sistema de información contable.	1. Sustancia económica.
b) Postulado que identifica y delimita al ente.	2. Entidad Económica.
c) Postulado que asume la continuidad del negocio.	3. Negocio en marcha.
d) Postulados que establecen las bases para el reconocimiento contable de las operaciones.	4. Devengación contable. 5. Asociación de costos y gastos con ingresos. 6. Valuación. 7. Dualidad económica. 8. Consistencia.

Clasificación de los Postulados Básicos

[3] Las Normas de Información financiera entraron en vigor en enero de 2006 y son el conjunto de pronunciamientos normativos, conceptuales, y particulares, emitidos por el CINIF (Consejo Mexicano para la investigación y desarrollo de las Normas de Información Financiera) o transferidos al CINIF, que regulan la información contenida en los estados financieros y sus notas, en un lugar y fecha determinados, y que son aceptados de manera amplia y generalizada por todos los usuarios de la información financiera.

Con la finalidad de que puedas profundizar en el estudio de los postulados, en el **apéndice A** (ver el **ANEXO**, al final de este documento) se presentan las NIF A-1 “Estructuras de la información Financiera” y la NIF A-2 “Postulados Básicos”.

b) Segregación de funciones

Los controles deben asegurar la existencia de una adecuada división de funciones, con la finalidad de que ningún empleado o grupo de empleados esté en una posición de incurrir en errores o irregularidades, o bien, ocultarlos, en el curso normal de sus labores.

No siempre resulta posible una segregación de funciones, por el número de empleados que se necesitarían, sin embargo, en esos casos deben existir otros controles que compensen la falta de segregación.

Las principales funciones que deben segregarse son:

Funciones que deben de segregarse

c) Autorización

Las autorizaciones se deben otorgar de acuerdo con los criterios establecidos por la administración, por lo tanto, necesitan existir controles que aseguren que sólo aquellas operaciones que reúnan los requisitos establecidos por la administración son reconocidas como tales y procesadas oportunamente.

d) Salvaguarda física y responsabilidad de activos

Deben existir controles que aseguren el acceso a los activos sólo a personas autorizadas de acuerdo con las políticas prescritas por la administración para tales efectos.

e) Verificación

Deben existir controles para verificar y evaluar de manera periódica:

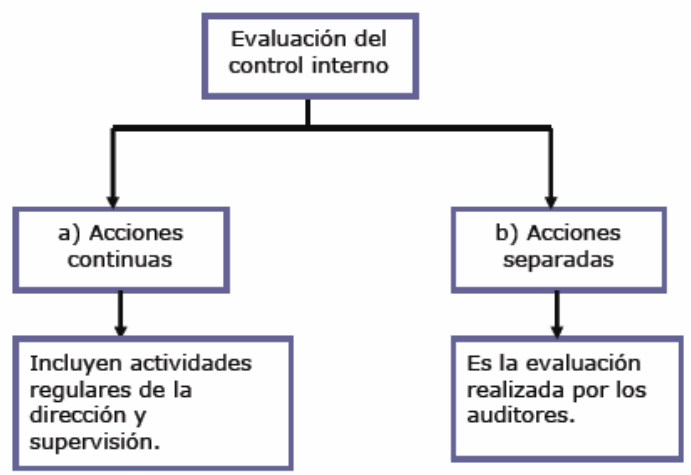
1. Que los datos registrados relativos a los activos sujetos a custodia existan físicamente.
2. Los saldos de los EEFF, informes, bases de datos y archivos.

Vigilancia

Los sistemas de control interno al igual que cualquier empresa evolucionan con el tiempo. Los procedimientos y políticas de una entidad pierden efectividad o bien dejan de aplicarse debido a los cambios constantes que ocurren dentro y fueran de la entidad. La administración es la responsable de establecer acciones que le permitan determinar si el sistema de control interno es efectivo y continúa vigente.

La vigilancia es el proceso en el cual la administración evalúa la calidad de ejecución del Control Interno en el tiempo. Implica evaluar el diseño y la operación de controles en forma oportuna y tomar las acciones correctivas necesarias.

La evaluación se realiza a través de acciones continuas, evaluaciones separadas, o bien, una combinación de ambas.



Evaluación de control interno

a) Acciones continuas de evaluación

La evaluación continua se da en el transcurso de las operaciones, incluye las actividades normales de administración y supervisión, así como otras actividades llevadas a cabo por el personal en la realización de sus funciones.

Las conciliaciones, la toma física de inventarios y las revisiones de desempeño son ejemplos de actividades de evaluación realizadas de manera continua en una entidad y que permiten efectuar un seguimiento de la efectividad del control interno.

b) Acciones separadas de evaluación

La evaluación (separada) del control interno forma parte de las funciones normales de auditoría interna. La Auditoría Interna[4] es una función independiente de evaluación establecida dentro de una organización, para examinar y evaluar sus actividades como un servicio a la misma organización.

[4] *Statements on Internal Auditing Standards* (SIAS)- Declaraciones sobre las Normas para la Práctica de Auditoría Interna, emitidas por el Comité de Normas y responsabilidades profesionales del *Institute of Internal Auditors* –IIA, Estados Unidos, 2004.

Se considera una evaluación separada porque el auditor no participa en la ejecución de las operaciones que realiza la entidad, su función consiste en revisar y evaluar la efectividad con la cual se realizan dichas operaciones.

1.3. Objetivos del Control Interno

Los objetivos del control interno pueden ser clasificados de la siguiente manera:

Básicos

- Provocar y asegurar el pleno respeto, apego, observancia y adherencia a las políticas prescritas o establecidas por la administración de la entidad.
- Promover la eficiencia en la operación.
- Asegurar razonabilidad, confiabilidad, oportunidad e integridad de la información financiera, administrativa y operacional que se genera en la entidad.
- Protección de los activos de la entidad

Los objetivos listados podrían ser clasificados en objetivos administrativos (1 y 2) y controles contables (3 y 4).

Por su parte, Juan Ramón Santillana González comenta que el Sistema de Control Interno contable habrá de ser diseñado en función de los objetivos generales siguientes:

a) **Objetivos del sistema contable**: Para que un sistema contable sea útil y confiable, debe contar con métodos y registros que: (I) identifiquen y registren únicamente las transacciones reales que reúnan los criterios establecidos por la administración; (II) Describan oportunamente todas las transacciones en el detalle

necesario que permita su adecuada clasificación; (III) Cuantifiquen el valor de las transacciones en unidades monetarias; (IV) Registren las transacciones en el periodo correspondiente; (V) Presenten y revelen adecuadamente dichas transacciones en los estados financieros.

b) **Objetivos de autorización**: Todas las operaciones deben realizarse de acuerdo con autorizaciones generales o específicas de la administración: (I) Las autorizaciones se deben dar de acuerdo con criterios establecidos por el nivel apropiado de administración; (II) Las transacciones deben ser válidas para conocerse y someterse a su aceptación con oportunidad; (III) Todas y solamente aquellas transacciones que reúnan los requisitos establecidos por la administración, deben reconocerse como tales y procesarse oportunamente; (IV) Los resultados del procesamiento de transacciones deben informarse en tiempo y forma y estar respaldados por archivos adecuados.

c) **Procesamiento y clasificación de transacciones**: Todas las operaciones deben registrarse para permitir la preparación de estados financieros de conformidad con las normas de información financiera o de cualquier otro criterio aplicable a dichos estados; y para mantener en archivos apropiados datos relativos a los activos sujetos a custodia: (I) Las transacciones deben clasificarse en forma tal que permitan la preparación de estados financieros de conformidad con las Normas de Información Financiera y el criterio de la administración; (II) Las transacciones deben quedar registradas en el mismo periodo contable ciudadano específicamente que lo sean aquellas que afectan más de un ciclo. Cuando existan enlaces entre diferentes ciclos, habrán de identificarse plenamente éstos para verificar que se han hecho “cortes” de operación adecuados.

d) **Salvaguarda Física**: El acceso a los activos sólo debe permitirse de acuerdo con políticas prescritas por la administración; cuidando de manera específica el pleno apego y respeto a las debidas autorizaciones.

e) **Verificación y Evaluación**: Los datos registrados relativos a los activos sujetos a custodia deben compararse, a intervalos razonables, con los activos físicos existentes. Tomar medidas apropiadas y oportunas respecto a las diferencias que se detecten; así mismo deben existir controles relativos a la verificación y evaluación periódica de los saldos que se informan en los estados financieros, este objetivo complementa en forma importante a todos los demás objetivos. El contenido de los informes y de las bases de datos y archivos debe verificarse y evaluarse periódicamente.

1.4. Definiciones relacionadas con Control Interno (Sistema, Control, Riesgo, Control Interno y Sistema de Control Interno)

Para entender qué es el Control Interno y un Sistema de Control Interno es necesario conocer algunas definiciones relacionadas con el Control Interno, siendo por supuesto la más importante la referida a Control interno; a continuación se listan las definiciones de *Sistema, Control, Riesgo, Control Interno y Sistema de Control Interno*, poniendo énfasis en la referida a *Control Interno.*

Sistema

De acuerdo con la segunda acepción de la RAE, es “Conjunto de cosas que relacionadas entre sí ordenadamente contribuyen a determinado objeto”

Por su parte Juan Ramón Santillana (2002) lo define como: “Conjunto Organizado de las partes que integran una estructura, regularmente interactuantes e interdependientes, que se concatenan para la consecución de un propósito u objetivo determinado”

Control

De acuerdo con el diccionario de la RAE es la “Comprobación, inspección, fiscalización, intervención” || Dominio, mando, preponderancia. || Regulación, manual o automática, sobre un sistema”.

Por su parte Juan Ramón Santillana (2002) lo define como:

> Fase del proceso administrativo que tiene como propósito coadyuvar al logro de los objetivos de las cuatro fases que lo componen: planeación, organización, captación de recursos y administración; éstas se armonizan de tal manera que todas participan en el logro de la misión y objetivos de la entidad.

Para J. Stoner, el control es el proceso por medio del cual los gerentes se aseguran de que las actividades efectivas están de acuerdo con lo que se ha planeado.

Para R. Buchele, es el proceso de medir los actuales resultados en relación con los planes, diagnosticando la razón de las desviaciones y tomando las medidas correctivas necesarias.

F. Kast lo define como la función administrativa que mantiene la actividad organizacional dentro de límites tolerables, al compararlos con las expectativas.

Riesgo

De acuerdo con el diccionario de la RAE es: “Contingencia o proximidad de un daño”

Por otro lado, y en relación con el tema tratado, podemos decir, que es el conjunto de factores que podrían afectar la consecución de los objetivos así como la forma en que éstos deben ser administrados y controlados.

Control Interno

De acuerdo con el modelo COSO[5], el Control Interno es un proceso realizado por la dirección, la gerencia y demás personal, diseñado para aportar seguridad razonable sobre el logro de los objetivos específicos de la entidad, a través de la implementación y ejecución de métodos, políticas y procedimientos coordinados e interrelacionados para lograr:

- Seguridad en la información financiera.
- Efectividad y eficiencia de las operaciones.
- El cumplimiento de las leyes aplicables a la entidad.

La definición anterior contempla varios conceptos fundamentales que a continuación se analizan, siguiendo al Banco de México en la V Reunión de Auditores Internos de Banca Central, recuperado por el Centro de Estudios Monetarios Latinoamericanos (CEMLA, 2000):

- El control interno es un proceso, es un medio utilizado para la consecución de un fin, no un fin en sí.
- El control interno lo llevan a cabo las personas, no se trata solamente de manuales de políticas e impresos, sino de personas en cada nivel de la organización.
- El control interno solo puede aportar un grado de seguridad razonable, no la seguridad total, a la dirección y al consejo de administración de la entidad, ya que sin importar qué tan bien diseñado y operado, su

5 “Declaraciones sobre normas de auditoría”, SAS No. 78 Consideraciones sobre control interno, p.97.

efectividad está sujeta a limitaciones inherentes a él, tales como: malos entendidos, errores de juicio, descuido o fatiga personal, colusión entre personas de dentro y fuera de la entidad, cultura, costumbres, entre otros.
• El control interno no puede hacer que un mal gerente se convierta en un buen gerente. Asimismo, los cambios en la política o en los programas gubernamentales, las acciones que tomen los competidores o las condiciones económicas pueden estar fuera de control de la administración.
• El control interno está diseñado para facilitar la consecución de objetivos propios de cada entidad, por lo tanto su diseño estará en función de las necesidades de cada entidad y de la creatividad de las personas que lo diseñen.
• La seguridad en la información financiera se refiere a la preparación de estados financieros confiables y a la prevención de la falsificación de la información financiera.
• La eficacia y eficiencia de las operaciones de la entidad, incluye los objetivos de rendimiento, rentabilidad así como la salvaguarda de los recursos contra posibles pérdidas.
• El objetivo de cumplimiento se refiere al acatamiento de las leyes y normas a las que está sujeta la entidad. Depende de factores externos (como por ejemplo: la reglamentación en materia de medio ambiente), tienden a ser parecidos en todas las entidades, en algunos casos, o en todo un sector, en otros.

Sistema de Control Interno

Por su parte Juan Ramón Santillana (2002) lo define como: “Conjunto ordenado, concatenado e interactuante de los objetivos que persigue el control interno para el logro de la misión y objetivos de la entidad”.

1.5. Responsabilidad del auditor (Interno / Externo)

Responsabilidad del auditor

Como se ha visto el diseño, operación y vigilancia del control interno son responsabilidad de la administración de la compañía. Sin embargo, para llevar a cabo la vigilancia de la funcionalidad y operación del control interno la administración realiza acciones de evaluación separada a través del área de **auditoría**.

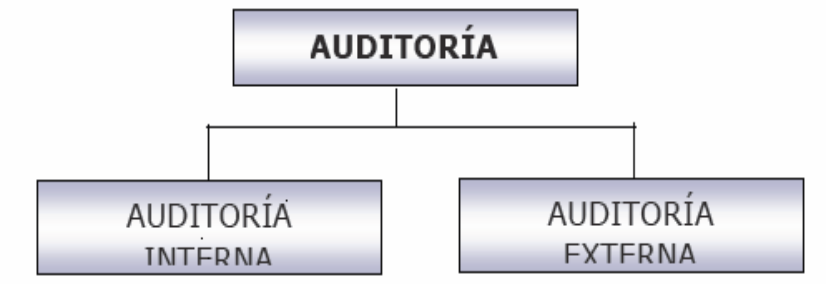
Para delimitar cuál es la responsabilidad del auditor en relación con el control interno, es necesario analizar brevemente en qué consiste esta función.

Concepto de auditoría

En términos generales, la palabra “auditoría” puede aplicarse como “sinónimo de revisión” (Santillana, 2002, p. 6). Desde el punto de vista de la contaduría, la auditoría es una actividad profesional, realizada por un contador público o licenciado en contaduría para verificar los EEFF (Estados Financieros) de una entidad, sus operaciones, o bien, su proceso administrativo, con la finalidad de emitir un informe.

Clasificación

Por su **ámbito de aplicación**, la auditoría, se clasifica en:



Auditoría Interna

a) Concepto

La auditoría interna es una función independiente de evaluación establecida dentro de una organización, para examinar y evaluar sus actividades como un servicio a la organización. (Véase, IIA, SIAS)

Es una herramienta de prevención de riesgos y fortalecimiento de operaciones, ya que participa activamente en el cumplimiento de los objetivos de la empresa.

Su objetivo es apoyar a los miembros de la empresa en el desempeño de sus actividades, proporcionándoles análisis, evaluaciones, recomendaciones, asesoría e información

b) Funciones

La auditoría interna examina y revisa los procesos de planeación, organización y administración, sus evaluaciones incluyen todos los sistemas, procesos, operaciones, programas, funciones y actividades dentro de la entidad (véase, IIA, Standards & Guidance).

Las evaluaciones de auditoría interna asisten a la organización en el mantenimiento de controles efectivos mediante la **evaluación** de la eficacia y eficiencia de los mismos y promoviendo la **mejora continua**.

Las evaluaciones de auditoría interna deberán enfocarse a evaluar:

- La confiabilidad e integridad de la información financiera y operativa.
- La eficacia y eficiencia de las operaciones.
- La protección de activos.
- El cumplimiento de leyes, regulaciones y contratos.

c) El auditor interno

Es el contador público o licenciado en contaduría que forma parte de la organización, su función consiste en revisar todas las operaciones que realiza la empresa, con la finalidad de emitir un informe sobre la racionabilidad de la efectividad con la cual se ejecutan dichas operaciones.

Por la naturaleza de sus actividades, el trabajo del auditor interno, implica la aceptación de una responsabilidad, ya que es considerado como profesional que aporta confianza, los resultados de su auditoría, sirven de base para la toma de decisiones de los niveles jerárquicos más importantes en la organización.

d) Ubicación del departamento de auditoría interna

La posición organizacional de la auditoría interna debe ser relevante para asegurar un amplio margen de cobertura y para asegurar acciones efectivas sobre los hallazgos y recomendaciones de auditoría.

De acuerdo con el tamaño y la estructura organizacional de la entidad, el departamento de auditoría interna debe estar ubicado dentro de los primeros niveles jerárquicos de la organización, con la finalidad de tener la suficiente autoridad y respeto hacia las áreas que va a revisar así como una línea directa de comunicación con los niveles de toma de decisiones.

e) Responsabilidad del auditor interno en relación con el Control Interno

La función de auditoría interna forma parte de la estructura del control interno de una organización, es la encargada de realizar las acciones de vigilancia del diseño, ejecución, funcionalidad y mejora continua de los controles establecidos por la administración.

El alcance y la naturaleza de sus revisiones dependen de las peticiones que realice el consejo de administración, la administración o el comité de auditoría, así como del

grado de efectividad del control y de los cambios ocurridos en la propia organización o en el entorno de la misma.

Auditoría Externa

(Véase, IMCP, Normas y procedimientos de auditoría)

Concepto

Para los propietarios, acreedores y terceros interesados en una empresa, resulta de primordial importancia, contar con información útil y confiable para la toma de decisiones adecuadas. Los EEFF son el instrumento utilizado por la administración de una empresa para dar a conocer información de carácter económico sobre la misma. La información contenida en los EEFF sirve de base para la toma de decisiones no sólo para la propia entidad sino para un gran número de usuarios, (accionistas, empleados, autoridades, inversionistas, acreedores), por ello surge la necesidad de que un profesional independiente a la entidad revise el contenido de los EEFF, a través de una auditoría que le permita determinar el grado de confiabilidad de dichos EEFF.

La auditoría **externa** representa el examen de los EEFF de una entidad, que realiza un contador público o licenciado en contaduría **independiente**, con la finalidad de emitir una opinión respecto a si dichos estados presentan **razonablemente** la situación financiera, los resultados de las operaciones, las variaciones en el capital contable y los cambios en la situación financiera de la empresa, de acuerdo con las bases contables correspondientes.

El término “razonablemente” significa medianamente y se utiliza debido a que el auditor efectúa su revisión con base en pruebas selectivas, es decir, no revisa la totalidad de las operaciones y por lo tanto no puede aseverar que todo está correcto.

El auditor externo

Es el contador público o licenciado en contaduría independiente que, con base en su examen, emite una opinión sobre la información financiera que revisó de una entidad.

El auditor es llamado como un técnico independiente y de confianza para emitir una opinión, sobre la razonabilidad de la información que revisó. Su opinión, por ser independiente a la de la administración de la empresa, permite incorporar credibilidad al contenido de los EEFF examinados, por lo que los resultados de su auditoría sirven de base para la toma de decisiones no sólo de quien contrata al auditor, sino del público en general.

Responsabilidad del auditor externo en relación con el Control Interno

La preparación, el contenido de los EEFF así como el diseño, ejecución y vigilancia del control interno, son **responsabilidad de la administración de la entidad**.

La responsabilidad del auditor consiste en expresar una opinión profesional independiente, respecto a si los EEFF examinados presentan razonablemente la situación financiera de una empresa, de acuerdo con las bases contables correspondientes.

Para que el auditor pueda obtener una base razonable para sustentar su opinión, deberá realizar su auditoría de acuerdo con las **Normas de Auditoría Generalmente Aceptadas**[6], las cuales requieren que se cubran todos los aspectos de importancia de los EEFF examinados, mediante la aplicación de procedimientos de auditoría.

Las normas de auditoría señalan que como parte de su trabajo, el auditor debe **realizar un estudio y evaluación del control interno**[7], establecido en la empresa sujeta a

[6] Son los requisitos mínimos de calidad relativos a la personalidad del auditor, al trabajo que desempeña y a la información que rinde como resultado de ese trabajo, emitidas por el IMCP a través de su Comisión de Normas y Procedimientos de Auditoría.

[7] Para llevar a cabo esta evaluación el auditor deberá aplicar la metodología establecida en el boletín 5030 “Metodología para el estudio y evaluación del control interno” de las Normas de auditoría generalmente aceptadas, el estudio de dicho boletín será tratado en la unidad 3.

revisión, con la finalidad de verificar si los controles establecidos por la empresa aseguran el procesamiento confiable de la información contable y por tanto, permiten el cumplimiento de cada una de las aseveraciones efectuadas por la administración en los EEFF.

Los resultados del estudio y evaluación del control interno le ayudan al auditor a determinar la naturaleza, el alcance, así como la oportunidad de sus procedimientos de auditoría: Son las pruebas que aplica el auditor para llevar a cabo su revisión.

RESUMEN

El control interno es la parte medular de toda organización, independientemente de su tamaño o de la actividad que realice, el control interno aporta seguridad razonable sobre el logro de sus objetivos específicos, ya que, disminuye los riesgos a los que está expuesta cualquier entidad.

A través de la implementación y ejecución de los cinco elementos que integran el Control interno, permite que la entidad obtenga:

- Seguridad en su información financiera,
- efectividad y eficiencia de sus operaciones, y
- el cumplimiento de las leyes aplicables a la misma.

En la actualidad y como consecuencia de numerosos escándalos financieros ocurridos en Estados Unidos a importantes compañías, el control interno ha tomado gran relevancia no sólo para las empresas sino también para las autoridades correspondientes y los estudiosos en la materia, que se han visto en la necesidad de buscar nuevas formas (modelos) de control que ayuden a las empresas a alcanzar sus objetivos.

Ahora si bien es cierto que el Control interno es fundamental para una empresa, sin embargo, para que el control sea de utilidad, es necesaria la función de auditoría, ya que realiza la vigilancia de la funcionalidad y de la efectividad de los sistemas de control interno, a través del tiempo.

BIBLIOGRAFÍA

SUGERIDA

Autor	Capítulo	Páginas
IMCP-Normas de Auditoría	3-3050	1-21

Instituto Mexicano de Contadores Públicos. (2006). *Normas y procedimientos de auditoría y normas para atestiguar*. (26ª ed.) México: IMCP. [En 2010 la versión las llama Normas Internacionales de Auditoría, ISA, del inglés. De cualquier manera, **siempre consultar las vigentes**.]

Unidad 2.

Teoría del riesgo y del control y sus aplicaciones

OBJETIVO PARTICULAR

Analizar los conceptos inherentes al riesgo y control, el diseño y ejecución de controles, su relación con el establecimiento y funcionamiento del Sistema de Control Interno, y su administración y evaluación.

TEMARIO DETALLADO

(6 horas)

2. Teoría del riesgo y del control y sus aplicaciones

2.1. Relación del riesgo con objetivos de la organización
2.2. Tolerancia al riesgo, riesgo residual y exposición
2.3. Evaluación de los riesgos y su impacto
2.4. Técnicas de Administración de riesgos/Análisis de costo/Beneficio
2.5. Definición de controles
2.6. Tipos y características de controles
2.7. Relación entre control, riesgo y objetivo
2.8. Técnicas para evaluar la efectividad
2.9. Técnicas de documentación

INTRODUCCIÓN

La alta gerencia tiene la carga de supervisar el establecimiento, administración y evaluación de los procesos de administración de riesgo y control. Las responsabilidades de los gerentes operativos incluyen la evaluación de los riesgos y controles en sus unidades. Los auditores internos y externos proveen varios grados de aseguramiento, respecto del estado de efectividad de la administración de riesgos y procesos de control de la organización. Tanto gerentes como auditores tienen un interés en usar técnicas y herramientas que tracen el foco y expandan los esfuerzos para evaluar la administración de riesgo y procesos de control que están vigentes e identificar maneras de mejorar su efectividad.

La gerencia y los empleados deben establecer y mantener un ambiente a través del cual la organización fije una actividad positiva y de apoyo hacia el control interno y una administración consistente y basada en la ética. La gerencia tiene la responsabilidad del ambiente de control.

Los sistemas de gobierno corporativo han evolucionado a lo largo del tiempo, frecuentemente en respuestas a fallas ocurridas en los negocios o la ejecución de fraudes, esto ha sido así desde los problemas financieros en los Estados Unidos en los años 80 hasta los recientes escándalos corporativos (Enron y Word Com) en la primera década del 2000. Aunque lamentables, tales fallas y pérdidas, brindaron enseñanzas respecto de por qué y cómo ocurrieron, y llevaron a nuevos conceptos sobre controles y ambientes de control que resultaron en mejoras para el sistema de gobierno corporativo.

En respuesta a los escándalos recientes la SEC (*Security and Exchange Commission*) de los Estados Unidos implementó nuevos requerimientos estrictos para la gerencia y juntas de directores a través de la Ley Sarbanes Oxley de los Estados Unidos en 2002.

Esta nueva regulación claramente delinea las responsabilidades de la gerencia y provee definiciones específicas de tal responsabilidad. Bajo estos lineamientos la gerencia recibe la confianza de una tarea y debe proveer aseguramiento de que se ha entendido y cumplido con tales responsabilidades.

Por lo anterior, a lo largo de este capítulo, el alumno analizará la importancia de la administración de riesgos y establecimiento de controles así como su importancia para el adecuado funcionamiento de las organizaciones y la responsabilidad de la administración respecto al correcto funcionamiento de los mismos.

2.1. Relación del Riesgo con objetivos de la Organización

El riesgo es inherente en todas las actividades de negocios y una de las mejores formas de ilustrar la relación entre riesgo y recompensa es la filosofía básica de inversión, la cual promueve la relación positiva entre riesgo y recompensa. A medida que el potencial de recompensa se incrementa, lo mismo hace la posibilidad de pérdidas (riesgo). Desde una perspectiva de inversión, los inversionistas necesitan evaluar sus objetivos y su tolerancia al riesgo (apetito).

Pese a que la relación entre riesgo y recompensa varía según la actividad de negocios, hay algunos elementos de riesgo presentes en todas las actividades de negocios. Es de incumbencia de la gerencia incorporar alguna forma de evaluación de riesgos dentro de las actividades de planeación estratégica.

La planeación estratégica es el proceso de adoptar una visión de largo plazo de la organización. Cuanto más larga la visión, mayor incertidumbre existe respecto de los riesgos y las oportunidades. Como los riesgos y las oportunidades cambian a lo largo del tiempo, la gerencia debe estar preparada para adaptar sus planes y proceso. Un proceso efectivo de administración de riesgo provee un mecanismo para evaluar continuamente los riesgos y su relación con las oportunidades.

De acuerdo con David McNamee, en su publicación *Bussiness Risk Assessment*, “la evaluación de riesgos de negocio se refiere a la evaluación de riesgos y oportunidades que afectan el logro de las metas y objetivos organizacionales”. El riesgo se evalúa en tres niveles:

1. **Estratégico**: Se usa para guiar a la organización a lo largo de un periodo de tiempo de entre cinco y diez años. Por lo común, la alta gerencia lo practica.
2. **Procedimental [**o **Proceso]**: Se usa para desarrollar y administrar el periodo actual de la actividad organizacional. El gerente de “proceso” es normalmente responsable de la evaluación inicial. Él o ella deberá también ser responsable de monitorear el riesgo del proyecto.
3. **Operacional**: Se usa en las operaciones de todos los días, es mayormente un asunto de salud y seguridad. Esta evaluación se desarrolla normalmente en un nivel de supervisión o por individuos o equipos de trabajo encargados de una asignación en particular.

Las evaluaciones estratégicas de riesgos usualmente están limitadas a la evaluación. La evaluación de los riesgos operacionales usualmente se enfoca en la administración de riesgos. La administración de riesgos de proyectos es una mezcla de ambos: evaluación de riesgos en la fase de planeación y administración de riesgos en la fase de implementación.

La evaluación de riesgos de negocios a estos tres niveles es esencial para identificar las amenazas, oportunidades y alternativas para lograr las metas y objetivos de la organización.

2.2. Tolerancia al riesgo, riesgo residual y exposición

La administración de riesgos incluye la evaluación de estos riesgos y el proceso de actuar sobre dicha desviación. El uso de la evaluación de riesgo en las etapas de planeación asume que la administración prudente tomará las medidas necesarias para administrar el riesgo una vez que lo ha evaluado. La evaluación de riesgo incluye un proceso de tres pasos:

1. Identificación de riesgo: Entender los riesgos y cuáles pueden sus consecuencias.
2. Medición de los riesgos: Medir las consecuencias probables y su severidad.
3. Priorización de riesgo: Priorizar los resultados para colocar mayor esfuerzo gerencial en los riesgos más altos.

La administración de riesgos cierra entonces el círculo cuando toma decisiones sobre cómo administrar el riesgo evaluado:

- Evaluar el riesgo: diseñar el proceso para eliminar riesgos particulares, minimizar los riesgos o cambiar la naturaleza de los riesgos que serán enfrentados.
- Controlar el riesgo: establecer las consecuencias y la severidad de la ocurrencia de los riesgos. Esto incluye aceptar algún riesgo.
- Compartir el riesgo: A través de arreglos contractuales con proveedores, clientes, integrantes o terceras partes (tales como aseguradores), se distribuye alguna porción del riesgo o actividades de riesgos sobre otros aceptando el remanente.

Siempre hay un monto de riesgo residual que permanece luego de todos los esfuerzos que se han hecho para evitar, controlar o compartir el riesgo. Si el riesgo residual es

demasiado alto, entonces la tarea no debe llevarse a cabo. Si el riesgo residual no es demasiado alto, la gerencia puede optar por aceptar tal cantidad de riesgo para lograr los objetivos.

Adicionalmente a los riesgos residuales, que permanecen pese a los esfuerzos de administración de riesgos, hay riesgos inherentes en el proceso de administración, conocidos como riesgos de control, o aquellos riesgos asociados con confiar en cierto procedimiento de control, etcétera, que fallan en el cumplimiento de su tarea. Tanto el riesgo residual como el riesgo de control necesitan ser explícitamente tratados por la administración.

Después de una detallada evaluación de riesgos, la organización debe tener definida su tolerancia al riesgo, haber identificado el riesgo residual y determinar si éste excede su umbral y finalmente haber aceptado algún grado tolerable de riesgo (exposición).

2.3. Evaluación de los riesgos y su Impacto

Una de las tareas de la junta directiva es establecer y mantener el proceso de gobierno corporativo de la entidad y obtener aseguramiento concerniente a la efectividad de la administración de riesgos y sus correspondientes procesos de control. El rol de la alta gerencia es una supervisión general sobre el establecimiento, administración y evaluación de tal sistema de administración de riesgo y procesos de control. El propósito de tal sistema multifacético de procesos de control es respaldar a la gente de la organización den la administración de riesgos y el logro de los objetivos de la empresa. Específicamente se espera que tales procesos de control aseguren, entre otras cosas, que las siguientes condiciones existan:

- La información financiera y operacional es confiable y posee integridad.
- Las operaciones son desarrolladas eficientemente y obtienen resultados efectivos.
- Los activos son salvaguardados.
- Las acciones y decisiones de la organización están en cumplimiento con las leyes, regulaciones y contratos.

La administración de riesgos es una responsabilidad clave de la gerencia. Para lograr sus objetivos de negocios, la gerencia debe asegurarse de que los procesos de administración de riesgos están vigentes y funcionando adecuadamente.

Las juntas directivas y los comités de auditoría tienen un papel de supervisión general para determinar si tales procesos apropiados por la administración están implementados y que tales procesos son adecuados y efectivos. Los auditores internos deben asistir tanto a la gerencia como a la junta directiva al evaluar, reportar y recomendar mejoras sobre la efectividad y lo adecuado de los procesos de

administración de riesgo. La gerencia y el consejo directivo son responsables por los proceso de administración de riesgo y control de su organización. Sin embargo, los auditores internos actuando en un papel de consultores pueden asistir a la organización al identificar, evaluar e implementar metodologías de administración de riesgo y controles para abordar tales riesgos.

Los cinco objetivos clave de los procesos de administración de riesgos son:

1. Los riesgos surgidos de las estrategias de negocios y actividades son identificados y priorizados.
2. La gerencia y el consejo directivo han determinado el nivel de riesgo aceptable para la organización, incluyendo la aceptación de riesgos diseñado para cumplir con los planes estratégicos de la organización.
3. Las actividades de reducción de riesgos son diseñadas e implementadas para reducir o administrar los riesgos en niveles que fueron determinados como aceptables por la gerencia y la junta directiva.
4. Actividades de monitoreo continuo son conducidas para reevaluar periódicamente el riesgo y la efectividad de los controles que administran el riesgo.
5. El consejo y la gerencia reciben informes periódicos sobre el resultado de los procesos de administración de riesgos.

2.4. Técnicas de administración de riesgos/análisis de costo/Beneficio

1.- **Transferir, administrar o aceptar**: La gerencia debe obtener suficiente conocimiento acerca de cómo aborda los riesgos la organización. Debe elegir entre tres grandes categorías de cursos de acción para abordar un riesgo específico:

- Transferir el riesgo – El riesgo puede ser transferido por medio de la compra de pólizas de seguro para cubrir pérdidas de diversos tipos tales como el efectivo, activos o instalaciones. Otra técnica es asociarse con otra organización que desee asumir una porción del riesgo a cambio de alguna retribución.
- Administrar (controlar) el riesgo – El riesgo puede ser controlado por varias medidas preventivas tales como, agregar personal a una función, instalar alarmas contra robo, incrementar la frecuencia y nivel de las revisiones gerenciales o implementar normas más exigentes.
- Aceptar el riesgo – Es en realidad bastante difícil de controlar o transferir todo el riesgo asociado con un área de operación. En consecuencia, las organizaciones frecuentemente deben decidir el nivel de pérdidas que están dispuestas aceptar. Por ejemplo, una organización podría decidir que el riesgo de incendio es alto y entonces decidir pagar una prima de alta de su póliza de seguro contra incendio para transferir el mayor riesgo posible; sin embargo, la organización aún tendrá que pagar el importe deducible de la póliza, si un incendio ocurre.

La administración de riesgos es una disciplina técnica con metas para proteger los activos e ingresos de una organización, por medio de eliminar, reducir, o transferir pérdidas potenciales antes de que éstas ocurran.

Las organizaciones y empleados están expuestos a riesgos de pérdidas originadas por eventos, tales como la desaparición, daño o destrucción de su propiedad y de la de otros, daños a los empleados, y deshonestidad, así como contingencias imprevistas impuestas por la ley o asumidas contractualmente.

Las organizaciones necesitan minimizar los riesgos en la mayor medida posible y aceptar y administrar el riesgo remanente dentro de lineamientos establecidos. La protección contra las pérdidas imprevisibles es necesaria por medio del uso de seguros disponibles y/o fondeo de la propiedad, cuando hay una posibilidad significativa de pérdida en exceso del monto establecido como razonable.

Para lograr estos objetivos de administración de riesgos, un programa fuerte de seguridad y prevención de pérdidas debería ser acompañado por una conciencia de seguridad y también un conocimiento de los controles de parte del personal de todos los niveles.

Una declaración de política que ayudaría a determinar si el riesgo ha sido transferido, administrado o aceptado sería:

- Aplicar principios de administración de riesgos a todo nivel gerencial con el propósito de :
  - Identificar y evaluar riesgos.
  - Evitarlos o eliminarlos cuando resultara práctico
  - Minimizarlos, controlarlos o transferirlos contractualmente a otros hasta donde sea posible.
- Retener aquellos riesgos que pueden ser auto-asumidos con fondos actuales sin afectar seriamente la condición financiera de la organización, si esta es la

manera más práctica en términos económicos de cumplir con tales obligaciones.

- Comprar cobertura de seguros cuando:
  - El riesgo es catastrófico por su naturaleza o más allá de la capacidad de la organización para absorberlo con sus fondos corrientes y cuando la compra de un seguro es permitida por la ley o por una agencia estatal correspondiente.
  - El gasto en tal prima se justifica por servicios accesorios al contrato de seguros, u otros beneficios esperados.
  - Requerido por la ley o contrato.

La adquisición de seguros estará necesariamente limitada a la disponibilidad de cobertura a un costo razonable y será sujeta a la viabilidad de adoptar programas de auto–aseguramiento, o auto–pago, en todo o en parte, consistente con la probable frecuencia, severidad e impacto de las pérdidas sobre la estabilidad financiera de la organización.

La declaración de política anterior delinea un proceso en el cual los riesgos son evaluados y luego categorizados para tomar la decisión final sobre transferir, administrar o aceptar un riesgo.

Como se ha indicado, estas decisiones son contingentes en relación con el evento de una administración de riesgos que ha incluido, tanto factores internos como externos y que variará significativamente en cada organización.

2.- Impacto / Análisis de Costo – beneficio

Un método para abordar el impacto es a través de la actividad de auditoría interna. El Consejo para la práctica de auditoría interna 2010-2: Vinculando el Plan de Auditoría con Riesgos y exposición delinea las relaciones entre la estrategia de riesgos y la auditoría interna.

La estrategia de riesgos de la organización deberá estar reflejada en el diseño del plan de la actividad de auditoría interna. Un enfoque coordinado debe ser aplicado a las sinergias de apalancamiento entre la administración de riesgos de la organización y los procesos de auditoría interna.

- El plan de la actividad de auditoría interna debe ser diseñado con base en una evaluación de riesgos y exposiciones que puedan afectar a la organización. Finalmente, el objetivo de la auditoría: Es proveer a la gerencia de información para mitigar las consecuencias negativas asociadas con el cumplimiento de los objetivos de la organización. El grado de la materialidad de la exposición puede ser visto como un riesgo mitigado por el establecimiento de actividades de control. El universo de auditoría puede incluir componentes del plan estratégico de la organización. Por medio de la incorporación de tales componentes, el universo de auditoría considerará y reflejará los objetivos generales del plan de negocios. Los planes estratégicos reflejarán también probablemente la actitud de la organización hacia el riesgo y el grado de dificultad para el logro de los objetivos planeados. Es aconsejable evaluar el universo de auditoría al menos una vez al año, para reflejar las estrategias más actuales y la dirección de la organización. El universo de auditoría puede ser influido por los resultados del proceso de administración de riesgos. Al momento de desarrollar planes de auditoría los eventos del proceso de administración de riesgos deben ser considerados.
- Los calendarios de trabajo de auditoría debería estar basados, entre otros factores, en una evaluación de prioridades de riesgos y exposiciones. La priorización es necesaria para tomar decisiones, para aplicar recursos relativos basados en la importancia de riesgo y la exposición. Una variedad de modelos de riesgo existen para asistir al director ejecutivo de auditoría para priorizar temas potenciales de auditoría. La mayoría de estos modelos de riesgos utilizan factores de riesgo para establecer la prioridad de los compromisos tales como:

materialidad monetaria, liquidez de activos, competencia de la gerencia, calidad de los controles internos, grado de inestabilidad, tiempo del último compromiso realizado de auditoría, complejidad, relaciones con los empleados y con el gobierno, etc.

- Cambios en la dirección de la gerencia, objetivos, énfasis y enfoque deben reflejarse en las actualizaciones del universo de auditoría y su plan de auditoría relacionado.
- En la conducción de compromisos de auditoría, los métodos y técnicas para probar y validar las exposiciones deben estar bien analizados con la materialidad del riesgo y su probabilidad de ocurrencia.
- La información en reportes gerenciales deben comunicar las conclusiones de administración de riesgos y las recomendaciones para reducir las exposiciones para que la gerencia entienda completamente el grado de exposición, es crítico que el reporte de auditoría identifique la “criticidad” y consecuencia de la actividad de riesgo respecto del logro de objetivos.
- El director ejecutivo de auditoría debe, al menos anualmente, preparar un informe sobre lo adecuado del sistema de control interno para mitigar los riesgos; tal declaración debe también comentar sobre la materialidad de los riesgos no mitigados y la aceptación gerencial de tales riesgos.

Otro método es determinar el costo – beneficio por medio de un enfoque de medición de riesgos, tal como se esboza en el siguiente texto de evaluación de riesgo de negocio.

Una vez que se han identificado los riesgos y sus consecuencias el próximo paso es medirlos. Medir riesgo es difícil por su naturaleza intangible. Los matemáticos (y muchos auditores internos) prefieren pensar sobre riesgos en términos cualitativos en lugar de cuantitativos. Para muchos gerentes definir los riesgo en una escala de tres riesgos (Alto, Medio y Bajo) es suficiente para sus necesidades.

Medir riesgos no es una ciencia precisa ni lo necesita ser. La evaluación de riesgos apoya la planeación en cuanto que ayuda a identificar las partes del plan que podrían necesitar mayor atención que otras debido a que son más importantes o menos protegidas por controles. El proceso de evaluación de riesgos provee al gerente de importantes partes del proceso de toma de decisión, pero el gerente necesita hacer ajustes a las decisiones con base en las condiciones reales encontradas.

Los riesgos son eventos con alguna probabilidad de ocurrencia. Las consecuencias son los resultados de los riesgos que actúan en nuestros procesos de negocios y nuestras metas y objetivos. Tanto los riesgos como consecuencias se miden en tres dimensiones:

La ocurrencia de riesgo es la probabilidad de que el riesgo cree una consecuencia que podría afectar materialmente nuestra capacidad para lograr nuestras metas de negocio. Ejemplo: Un banco tiene una caja con un grupo de títulos valores registrados con una tasa de interés fija como garantía contra un préstamo otorgado, el banco está en riesgo si las tasas de interés aumentan por encima de cierto importe (la garantía ya no cubrirá el valor del préstamo). Dados razonables registros contables, el banco no está en riesgo si los títulos resultan físicamente dañados aun cuando ese es un riesgo real con una razonable probabilidad de ocurrencia. La razón es que el daño no afecta los procesos de negocios del banco en una forma material (los títulos valores están registrados, entonces pueden remplazarse si se dañan o pierden), independientemente de la probabilidad de ocurrencia.

La severidad de las consecuencias es otra dimensión de la medición de riesgos. La severidad de las consecuencias es frecuentemente dependiente de la operación de los controles internos. Algunos controles reducen las consecuencias a eventos inmateriales. Las consecuencias deben tener un efecto material sobre la capacidad de lograr objetivos. Los riesgos con consecuencias inmateriales que no afectan nuestra capacidad de lograr nuestras metas son eliminados de consideración. Tales controles internos que reducen las consecuencias a la inmaterialidad son probados en el programa de auditoría. Por ejemplo: Usando el mismo ejemplo del banco antes mencionado en riesgo de pérdida o daño, dado un adecuado registro contable (el control) no vale la pena ser considerado dado que el costo de reemplazo (la consecuencia) no es material. No diseñaríamos un programa de auditoría para cubrir todos los

aspectos de controles de custodia referida a riesgo de daño físico o pérdida, verificaríamos que tenemos buenos registros contables de estas tenencias a través de una prueba de arqueo a la caja.

El espacio de tiempo del riesgo y la duración de sus consecuencias es la tercera dimensión de la medición de los riesgos. Lo riegos pueden tener consecuencias que varían en severidad dependiendo de en qué momento del proceso de negocios se producen y por cuánto tiempo duran sus consecuencias. Por ejemplo: La oportunidad se torna un tema importante en las operaciones de la computadora. El riesgo de interrupción del procesamiento de una computadora del Banco es mayor durante ciertos momentos del día (conexión l sistema eléctrico), algunos momentos del año (mal clima), y aun en ciertas secuencias de procesamiento (operaciones altamente complejas que requieren una gran intervención de operador). Las probabilidades de interrupción debido a un número de causas crecen o disminuyen dependiendo de tales factores.

Análogamente, la duración de las consecuencias puede afectar la magnitud del riesgo. El procesamiento de la computadora del banco es usualmente conducido por ciclos. La interrupción de tales ciclos por una hora es un nivel de riesgo; la interrupción por un día es otro nivel de riesgo (mayor) y la interrupción por una semana probablemente deje al banco fuera de interrupciones.

Finalmente, los beneficios devengados de las actividades de auditoría, revisión y evaluación de riesgo deben exceder el costo de asignar recursos escasos a tales actividades. Adicionalmente la implementación de controles para mitigar cualquier riesgo identificado debe ser menor que sus pérdidas potenciales.

2.5. Definición de Controles

El control se define como el proceso efectuado por la gerencia de una organización y otro personal, diseñado para proveer seguridad razonable en relación con el logro de los objetivos. Un sistema de control puede definirse como las actividades que ayudan a asegurar que las estrategias y directivas de la organización sean llevadas a cabo. Las actividades de control deben ser efectivas y eficientes para el logro de los objetivos gerenciales de control.

Algunos objetivos de control incluyen:

- Efectividad y eficiencia de las operaciones.
- Confiabilidad del reporte financiero.
- Cumplimiento de las leyes y regulaciones.

Algunas actividades típicas de control incluyen:

- Control físico sobre los activos.
- Establecimiento y revisión de medidas de desempeño e indicadores.
- Segregación de funciones.
- Revisiones de la gerencia ejecutiva sobre el desempeño real.
- Controles sobre el procesamiento de información.
- Ejecución y documentación adecuad de transacciones y eventos.
- Restricciones físicas y lógicas de acceso y deber de rendición de cuentas sobre recursos y registros.
- Apropiada documentación de transacciones y control interno.

Otras dos clasificaciones comunes de controles incluyen:

- Controles contables – procedimientos e información relacionados con la salvaguarda de activos y la confiabilidad de los registros contables – los ejemplos incluyen segregación de funciones, monitoreo y conciliaciones.
- Controles administrativos – los procedimientos e información relacionada con el logro de objetivos organizacionales y la eficiencia operacional y la efectividad de la organización.

2.6. Tipos y características de controles

Los controles se clasifican frecuentemente como preventivos, de detección o correctivos.

- Los controles preventivos intentan evitar la ocurrencia de eventos no deseados.
- Los controles de detección intentan identificar los eventos no deseados una vez que éstos han ocurrido.
- Los controles correctivos remedian las circunstancias que permitieron la actividad no autorizada o retornan las condiciones a lo que eran antes de la deficiencia del control.

Los controles preventivos, de detección (algunas veces aparece erróneamente como “detectivos”) y correctivos son adaptados a cada caso en la evaluación de la seguridad informática.

Controles Formales e Informales

Los controles formales también llamados controles duros son las herramientas de control documentadas y tangibles usadas por una organización, tales como políticas y procedimientos; algunos ejemplos de controles formales incluyen:

- Estructura Organizacional – La estructura intencional de roles asignados a la gente para promover la eficiencia y efectividad. Por ejemplo, gráficos que delinean la responsabilidad asignada. Mientras que al mismo tiempo la segregación de funciones para realizar tareas sensibles está dividida.
- Políticas – Instrucciones formales que requieren, guían o restringen acciones.
- Procedimientos – Medios empleados para asegurar que las actividades se desarrollan de acuerdo con lo prescrito por las políticas. Los procedimientos pueden incluir una revisión automática independiente de las transacciones sensibles.
- Personal – Reclutamiento y retención del personal calificado para las funciones.
- Reporte – Oportunos, adecuados y comprensibles informes provistos para respaldar a la gerencia en sus decisiones.
- Revisión Interna – Periódica revisión independiente sobre las operaciones.

Los controles formales son los controles convencionales con los cuales todos los auditores están familiarizados. Los controles informales son más difíciles de asir porque ellos abordan intangibles tales como la competencia, valores, apertura, liderazgo y expectativas. Sin embargo, tienen un impacto significativo sobre la efectividad de la estructura del control interno. A diferencia de los controles formales, los controles informales son frecuentemente difíciles de identificar o medir. Es relativamente fácil de revisar una política de ética para determinar si contiene los elementos necesarios. Sin embargo, como se evidencia por los escándalos corporativos, la promoción y finalmente la implementación de las políticas prescritas es el elemento clave.

Los controles informales relacionados con las políticas de negocios podrían incluir:

- Cultura organizacional
- Conocimiento
- Estructura de recompensas

Es mucho más difícil determinar la existencia de controles informales que de controles formales.

Los controles discrecionales están sujetos a la elección o juicio humano. Los controles no discrecionales son provistos automáticamente por el sistema y no pueden ser eludidos, ignorados o pasados por alto basados en juicio humano. Por ejemplo la revisión por un supervisor de firmas no autorizadas es un control discrecional (el supervisor tiene la opción de ejecutar el control). El requerimiento de que se ingrese un número de identificación validado antes de que un cajero automático acepte una transacción es un control no discrecional.

La clasificación de controles discrecionales y no discrecionales es importante porque los controles no discrecionales apropiadamente diseñados tienden a ser más confiables que los controles discrecionales y son probados de modo diferente. Algunos controles automatizados no pueden ser clasificados como no discrecionales, porque ellos pueden ser pasados por alto o ignorados. Un ejemplo de un control discrecional es un archivo de suspenso que contiene transacciones suspendidas, por ser procesadas, mientras se espera la intervención humana. El proceso de corrección puede no requerir la corrección de cada objeto, puede no proveer la antigüedad de transacciones o puede no someter la corrección de los registros a la apropiada edición o validación. En tal caso, un control que, en la superficie aparece como no discrecional puede, en realidad ser altamente discrecional y puede debilitar el sistema general de control interno.

Los controles formales son más fáciles de monitorear por que la gerencia, auditores o evaluadores del personal pueden obtener y revisar una política, procedimiento, informe, fecha, etc.

Controles Manuales

Por muchos años solo existieron controles manuales en las organizaciones. La introducción de tecnología, particularmente tecnología de computadoras, cambio dramáticamente esto. Los controles manuales fueron vistos como caros e ineficientes porque eran desarrollados por empleados y representaba un riesgo mayor al depender de la competencia y actitud de los individuos que los estaba practicando. Los controles manuales todavía forman parte del sistema de control interno pero no hay duda de que su papel fue declinado conforme más actividades de negocios se volvieron automatizadas. En su lugar, muchos controles fueron reemplazados por controles de alto nivel, esto es, la revisión humana del procesamiento extensivo de computadora y el enfoque solamente en las excepciones.

Los controles manuales también trabajan frecuentemente en conjunción con controles automatizados. Por ejemplo, un sistema de nóminas puede identificar (vía un control de edición) un incremento inusual en la tasa de pagos basado en parámetros programados. La porción manual de control sería una revisión manual de un informe de excepciones para identificar y subsecuentemente evaluar la integridad de la transacción.

Controles automatizados

Los controles automatizados son procedimientos programados diseñados para evitar, detectar y corregir errores o irregularidades que podrían impactar adversamente las actividades de negocios de la organización. Tales controles abordan los aspectos esenciales del procesamiento de transacciones e información, desde la iniciación de la actividad de informe. Los controles automatizados y sus funciones relacionadas de procesamiento computarizado respaldan directamente el sistema de negocios

subyacente y ayudan a asegurar la consistencia y veracidad de los procesos automatizados. Por ejemplo, la edición automatizada de información ingresada para asegurar que se evite correcta y completamente el ingreso de información errónea dentro del sistema.

Los controles automatizados son preferidos debido a su economía velocidad, confiablidad y veracidad. Sin embargo solo son tan efectivos como los controles de alto nivel que los administra. Por ejemplo, un sistema puede producir un informe adecuado sobre transacciones de cuentas por pagar que exceden un límite establecido, sin embargo si no hay revisión efectiva o investigación de tales excepciones por un individuo apropiado, el valor del control es nulo. Los controles automatizados suplementan y aumentan la efectividad de la revisión de empleados y gerentes pero no la reemplazan.

Dos métodos comunes para evaluar controles internos son las pruebas de cumplimiento y sustantivas.

Las pruebas de cumplimiento son procedimientos diseñados para verificar si los controles están siendo aplicados en la manera descrita en flujogramas, cuestionarios, etc. Si, de las pruebas el auditor cree que los controles están operando efectivamente, se puede confiar en tales sistemas de control. El control manual puede ser verificado en su cumplimiento por medio de la revisión de documentación tal como pruebas de auditoría. Donde existen pruebas de auditoría (documentación para respaldar el control, firmas por ejemplo) una revisión de la muestra de documentación es suficiente. Sin embargo, cuando no existe documentación (segregación de funciones) se pueden requerir la observación o entrevistas para verificar el cumplimiento con el sistema de control interno. Los controles automatizados pueden también dejar una pista de auditoría (registros de log, registro de transacciones) que pueden revisarse para asegurar cumplimiento.

Las pruebas sustantivas son procedimientos diseñados para probar los errores en el sistema de control interno (errores monetarios por ejemplo). En tales casos, la información se compara y concilia para asegurar que está adecuadamente representada a través del ciclo de la transacción. Tales pruebas pueden ejecutarse manualmente, sin embargo, las revisiones automatizadas se están volviendo más comunes. La información puede correr a través de un sistema para verificar la integridad del sistema y suplementarse con una revisión de la información producida para asegurar su veracidad.

2.7. Relación entre control, riesgo y objetivo

Evaluación de riesgo – el control interno debería proveer para una evaluación de los riesgos que la organización enfrenta tanto desde fuentes internas como externas.

Un prerrequisito para la evaluación de riesgo es el establecimiento de objetivos claros y consistentes. La evaluación de riesgo es la identificación y análisis de los riesgos asociados con el logro de objetivos y forma una base para determinar cómo deberían administrarse y controlarse los riesgos.

La gerencia necesita identificar ampliamente los riesgos y debería considerar las interacciones significativas entre la entidad y otras partes tanto como los factores internos, y a nivel corporativo como al de actividad. Los métodos de identificación de riesgos pueden incluir calificaciones cuantitativas de las actividades, conferencias gerenciales, presupuesto y planeación estratégica y la consideración de hallazgos de los auditores así como otras evaluaciones.

Una vez que los riesgos han sido identificados deben ser analizados respecto de su posible efecto. El análisis de riesgos generalmente incluye la estimación del alcance de los riesgos, ponderación de la probabilidad de su ocurrencia y decisión respecto de cómo administrar el riesgo y qué acciones deben tomarse. La metodología específica de análisis de riesgo usada puede variar según la organización, debido a la diferencia en su misión y la dificultad de asignar niveles cuantitativos y cualitativos a los riesgos. Debido a que las condiciones políticas, económicas, industriales, regulatoria y operacionales cambian continuamente, debería proveerse los mecanismos para identificar y tratar con cualquier riesgo especial surgido de tales cambios.

El sistema de control de una organización tiene una función clave en la administración de riesgos, ya que es significativa para el cumplimiento de sus objetivos de negocio. El sistema de control interno debe:

- Responder a los riesgos cambiantes tanto dentro como fuera de la organización.
- Ser integrado con las operaciones y no tratado como un ejercicio separado.

Las organizaciones deben identificar evaluar y manejar sus riesgos significativos, así como evaluar la efectividad de su sistema relacionado de control interno.

La misión primaria de cada organización es el logro de las metas y objetivos definidos; el logro de los objetivos establece la base para la dirección estratégica de la organización. Los riesgos y oportunidades están presentes en todas las actividades organizacionales y pueden impedir o mejorar el logro de las metas. Los controles son desarrollados para mitigar los riesgos y permitir a la organización lograr sus objetivos en una forma eficiente y efectiva.

2.8. Técnicas para evaluar la efectividad

Cuando se evalúan controles, los revisores deberían enfocarse en la adecuación del ambiente de control de la organización por medio de la evaluación de las siguientes áreas:

- Estructura Organizacional.
- Actitud gerencial hacia el control, la integridad y la ética.
- Actitudes de los empleados hacia el control, la integridad y la ética.
- Efectividad de las políticas y procedimientos de control.
- Compromiso organizacional con la calidad.
- Cultura organizacional.
- Actitudes y moral del personal.
- Efectividad de la junta directiva y comité de auditoría.
- Políticas y procedimientos de recursos humanos.

La gente es quien hace funcionar el control interno; se puede diseñar el mejor control interno posible, sin embargo, si la persona que ejecuta el control no le interesa, o deliberadamente interfiere con el control (fraude), entonces el control ha fallado, por lo tanto mientras la responsabilidad para una buena estructura de control descansa en la gerencia, todo los empleados comparten responsabilidad por la calidad y efectividad de tales controles. La gerencia establece los objetivos, pone en vigencia los mecanismos y actividades de control, monitorea y evalúa el control. Sin embargo, todo el personal de la organización está involucrado para que esto suceda.

La auto-evaluación de control es un método para evaluar los controles, pues provee una comprensión del proceso completo de control, incluyendo la implementación de controles formales y aspectos del control determinados por la cultura organizacional u otros controles informales.

Las técnicas tradicionales de auditorías están basadas en la revisión de controles formales. La auditoría interna tradicional tiene dificultad para medir y controlar los controles débiles y los efectos de la gente sobre el proceso de control.

Una de las técnicas usualmente empleada para evaluar controles es el uso de procedimientos analíticos de auditoría que pueden proveer a los auditores de medios efectivos y eficientes para evaluar y valuar la información.

Los procedimientos analíticos son útiles para identificar, entre otras cosas:

- Diferencias que no se esperaban.
- La ausencia de diferencias cuando éstas se esperaban.
- Errores potenciales.
- Potenciales irregularidades o actos ilegales.
- Otras transacciones inusuales o eventos no recurrentes.

Los procedimientos analíticos de auditoría pueden incluir:

- Comparación del periodo actual con información similar de periodos anteriores.
- Comparación del periodo actual con presupuestos y pronósticos.
- Estudio de relaciones de la información financiera con la información no financiera apropiada.
- Estudio de relaciones entre elementos de información.
- Comparación de información con información similar para otras unidades organizacionales.

- Comparación de la información con información similar para la industria en la cual opera la organización.

Los procedimientos analíticos de auditoría deberían también usarse durante la asignación para examinar y evaluar información para respaldar los resultados de la asignación. Los auditores internos deberían considerar los factores listados seguidamente para determinar la medida en la que deberían usarse los procedimientos analíticos de auditoría.

- La materialidad del área examinada.
- La evaluación de riesgo y efectividad de la administración de riesgos en el área examinada.
- La adecuación del sistema de control interno.
- La disponibilidad y confiabilidad de la información financiera y no financiera.
- La precisión con la cual se pueden predecir los resultados de las pruebas analíticas de auditoría.
- La disponibilidad y comparabilidad de información respecto de la industria en la que opera la organización.
- La medida hasta la que otros procedimientos de auditoría pueden proveer respaldo a los resultados de la asignación.

Cuando se revelan resultados o relaciones inesperadas de resultados en los procedimientos analíticos de auditoría, los auditores internos deberían examinar tales resultados o relaciones. Los resultados o relaciones que no resultan suficientemente explicados deberían ser comunicados a un nivel apropiado de la gerencia. Los auditores internos pueden recomendar apropiados cursos de acciones, dependiendo las circunstancias.

2.9. Técnicas de documentación

Hay una cantidad de técnicas que puede usarse para documentar controles. Cada método tiene sus fortalezas y puede usarse tanto individual como conjuntamente, según lo indique la situación. Recuérdese que el propósito primario de las técnicas es entender y compartir tal entendimiento sobre los controles y los cambios que deben hacerse. Cuanto más extensa y detallada la documentación, más difícil es comunicar y entender la situación óptima.

Flujogramas

Un flujograma es una representación visual de cómo trabaja un proceso. Símbolos interrelacionados son usados para diagramar el flujo de eventos o información a través del sistema. Los flujogramas pueden proveer una buena visión inicial del sistema entero.

Reglas generales para el uso de flujogramas:

- Los flujogramas generalmente fluyen de arriba hacia abajo y de izquierda a derecha.
- Todos los símbolos del flujograma deberían estar conectados por líneas o flechas.
- Los símbolos del flujograma deberían tener un único punto de entrada en la parte superior del símbolo.
- El primer punto de salida para todo los símbolos del flujograma deberían estar en la parte inferior, excepto para el símbolo de decisión. El símbolo de decisión debería tener dos puntos de salida, los cuales deberían estar hacia ambos lados o en la parte inferior y uno de los lados.
- Los conectores deberían usarse para conectar líneas del flujograma.

- Todos los flujogramas deberían comenzar con un conector o símbolo predefinido.
- Todos los flujogramas deberían terminar con un conector o rizo continuo.

Mapeo de procesos

El mapeo de procesos de negocio se usa para crear una comprensión común de los procesos de negocio centrales para presentar estrategias, sistemas e ideas en un proceso visual y fácil de entender. El mapeo de procesos está diseñado para permitir a cualquiera de la organización entender y responder a los temas de economía vital, competitividad, productividad y calidad de los clientes.

Cualquier organización es un conjunto de procesos. Tales procesos son las actividades naturales de negocios que producen valor, sirven a los clientes y generan los ingresos. Administrar tales procesos es la clave para el éxito de una organización. Desafortunadamente muchas organizaciones no están establecidas para administrar procesos – en su lugar, administran tareas. Como resultado, la gente tiende a enfocar asuntos locales, en lugar de las necesidades globales de la organización. Por ejemplo los subprocesos pueden evolucionar dentro de los departamentos sin consideración de otras áreas funcionales. Líneas de comunicación y gerencia son creadas para asegurar los eventos deseados, agregando consecuentemente costos y extendiendo el ciclo y los tiempos de respuesta al cliente.

Muchas organizaciones están también estructuradas alrededor de funciones, en lugar de alrededor del negocio de la organización. Esto crea mucho de la mentalidad de silo donde un área funcional solo mira su porción de negocio y tiende de alguna manera a desconectarse de las otras áreas de la organización. En consecuencia, cuando una actividad importante del negocio cruza a través de un número de áreas funcionales, frecuentemente se cortan las líneas de comunicación y puede, en algunas instancias, resultar en estas áreas competir contra otros en lugar de mirarse a sí mismos como socios colaborando al proceso general de negocios.

El mapeo de procesos de negocio en un método poderoso para mirar más allá de las actividades funcionales y redescubrir los procesos centrales de la organización. Los mapas de procesos proveen la capacidad de trascender la complejidad de la estructura organizacional y enfocarse en los procesos que son realmente el ‘corazón’ del negocio.

Una concienzuda comprensión de los insumos, productos, e interrelaciones de cada proceso permitirá a la organización:

- Entender cómo interactúan los procesos en un sistema.
- Identificar y entender los procesos centrales de la organización.
- Localizar las fallas en el diseño de procesos que están creando problemas sistémicos.
- Evaluar cuáles son las actividades que agregan valor al cliente.
- Movilizar a los equipos para encarrilar y mejorar los procesos.
- Identificar los procesos que necesitan ser rediseñados.
- Eliminar las fallas del sistema que resultan de calidad pobre.
- Distinguir entre procesos técnicos y sociales.

Adecuadamente utilizados, los mapas de proceso pueden cambiar el abordaje total de mejora de procesos y administración del negocio y potencialmente reducir el costo de operaciones por medio de la eliminación de pasaos innecesarios en los procesos de negocio.

Diagramas de Control

Es una herramienta y abordaje técnicamente sofisticado que estudia la variación de un proceso con el propósito de mejorar la efectividad económica de los procesos.

El método se basa en el monitoreo continuo de la variación del proceso. El método provee una descripción gráfica del proceso y áreas de potenciales problemas. Un gráfico de control es un dispositivo para descubrir de una forma precisa el impacto estadístico de un proceso o control del proceso. Los gráficos de control son usados para:

- Mejorar la productividad.
- Revisar o evitar los defectos de manufactura.
- Evitar ajustes innecesarios del proceso.
- Proveer información de diagnostico.
- Proveer información acerca de la capacidad del proceso.

Los diagramas de control se usan primariamente para monitorear una variable del proceso y para la medición de los límites aplicables sobre la variable, determinando si el proceso está fuera de control. La combinación de gráficos para incrementar la detección de un proceso que está fuera de control y/o provee más información para ayudar a determinar las causas de la variación del proceso. Esta información puede usarse para desarrollar métodos para controlar mejor el proceso.

Cuestionarios de Control

Son el marco de trabajo que la gerencia establece para asegurar que éste se ajuste a sus responsabilidades en una variedad de áreas. Las auditorías de controles internos están diseñadas para determinar la existencia y efectividad de un sistema de control interno. Los cuestionarios de control se usan para generar un entendimiento general (superficial) del ambiente de control.

Los cuestionarios de control interno se utilizan para catalogar controles específicos para usar en el proceso. Los auditores usan cuestionarios de control interno para documentar las áreas por cubrir durante la asignación y para indicar las deficiencias

de control. Un cuestionario de control interno, para un área particular de auditoría, típicamente se completa al inicio de la auditoría. Cualquier deficiencia o debilidad notada en los cuestionarios indica áreas que deberían enfocarse durante las pruebas de campo. Las preguntas formuladas en los cuestionarios de control interno se usan frecuentemente para respuestas de sí / no, lo cual permite identificar rápidamente las excepciones. Sin embargo, no se debe confiar solamente en la ausencia de un control prescrito, como evidencia para respaldar un hallazgo de deficiencia. Estos cuestionarios deberían utilizarse como una herramienta de familiarización en las etapas tempranas del planteamiento o revisión de controles y seguimiento de excepciones para determinar si la falta de control es significativa, o si la ausencia está mitigada por controles compensatorios, o si el control identificado es innecesario o antieconómico en el ambiente específico.

Los cuestionarios de control, normalizados, eficientes, provén respuestas sí / no fáciles de entender y de modificar. Sin embargo, pueden limitar una revisión concienzuda desde que su foco es muy estrecho, no suficientemente detallado y desalientan un detallado análisis desde que el revisor está solamente marcando casilleros.

Los cuestionarios de control se usan frecuentemente como el paso inicial en el proceso de evaluaciones control para obtener un entendimiento básico de la estructura de control.

RESUMEN

En una entidad, independientemente de su giro, el riesgo es inherente en todas las actividades de negocios, los inversionistas, es decir, los dueños y directivos, necesitan evaluar sus objetivos y su tolerancia al riesgo, primeramente identificando los riesgos, evaluándolos y posteriormente dando una respuesta pronta al mismo.

En virtud de lo anterior, una de las tareas de los directivos o dueños es establecer y mantener los procesos de gobierno corporativo de la entidad y obtener aseguramiento concerniente a la efectividad de la administración de riesgos y sus correspondientes procesos de control.

Dichos directivos delegan sus funciones a equipos multidisciplinarios o a expertos de implantación de métodos y procedimientos y algunos de estos directivos lo dejan en manos de sus auditores externos o internos, no obstante a ello, a cualquier persona que le sea delegado, tendrá que medir los riesgos debiendo auxiliarse de herramientas tales como los diagramas de flujos, cuestionarios o desarrollo de mapeos.

Una vez obtenido lo anterior se llevará a cabo la posibilidad de implementación de controles para fortalecer los mismos y poder acotar los riesgos, todo ello será posible si el costo de la implementación de los mismos no excede los beneficios por dicha implementación.

BIBLIOGRAFÍA

SUGERIDA

Autor	Capítulo	Páginas
IMCP (2009)	Boletín 5020 el muestreo en la auditoría	1-18

Instituto Mexicano de Contadores Públicos. (2006). *Normas y procedimientos de auditoría y normas para atestiguar*. (26ª ed.) México: IMCP. [En 2010 la versión las llama Normas Internacionales de Auditoría, ISA, del inglés. De cualquier manera, **siempre consultar las vigentes**.]

Unidad 3.

Modelos de control interno

OBJETIVO PARTICULAR

Conocer los elementos y características de los diferentes modelos de Control Interno, así como su ámbito de aplicación en el entorno de las entidades.

TEMARIO DETALLADO

(18 horas)

3. Modelos de control interno

- 3.1. Modelos de control de negocios
  - 3.1.1. CoCo
  - 3.1.2. COSO, ERM, SMALL
  - 3.1.3. Cadbury
- 3.2. Modelos de control de tecnología de la información
  - 3.2.1. CobiT (*Control Objectives for Information and Related Technology*)
  - 3.2.2. Information Technology Control Guidelines (Canadá)

INTRODUCCIÓN

La globalización y los constantes avances tecnológicos han propiciado el desarrollo de nuevos modelos de trabajo en relación con el control interno, que permiten satisfacer los requerimientos presentes de las organizaciones. Los modelos de control de negocios y de tecnología de información surgen como una propuesta que busca implementar nuevas formas para mejorar y perfeccionar el control en las organizaciones. En esta unidad se analizarán las características de algunos de los modelos de control de negocios y de tecnología de información más utilizados en la actualidad.

3.1. Modelos de control de negocios

En la evolución de la teoría del control interno se definió, en un principio, a los controles como mecanismos o prácticas para prevenir o identificar actividades no autorizadas, más tarde se incluyó en el concepto el asunto de lograr que las cosas se hagan. Actualmente, se define al control como un proceso que aumenta las posibilidades de que se logren los objetivos de la organización.

La globalización y los constantes avances tecnológicos han propiciado el desarrollo de nuevos modelos de trabajo en relación con el control interno, que permitan satisfacer los requerimientos presentes de las organizaciones.

Los modelos de control de negocios surgen como una propuesta que busca implementar nuevas formas para mejorar y perfeccionar el control en las organizaciones.

Estados Unidos fue uno de los primeros países en desarrollar un modelo de control interno, el llamado informe COSO, publicado en 1992. Este modelo propone un mejoramiento del control interno y del gobierno corporativo en las organizaciones.

A partir de la divulgación del informe COSO, se han publicado en varios países del mundo diversos modelos de Control, así como numerosos lineamientos para un mejor gobierno corporativo; los más conocidos, además del COSO (EEUU), son los siguientes: Coco (Canadá), Cadbury (Reino Unido), Vienot (Francia), Peters (Holanda) y King (Sudáfrica) [véase, Espinosa, 2002].

En los últimos años estos modelos han resurgido con una fuerza impresionante, en consecuencia de la presión pública para un mejor manejo de los recursos públicos o privados en cualquier tipo de organización, ante los numerosos escándalos financieros ocurridos en las últimas décadas.

En nuestro continente, los modelos COSO y COCO han sido los más adoptados, por ello, a continuación, se hace una muy breve descripción del enfoque y estructura que cada uno plantea.

COSO Committee of Sponsoring Organizations

El modelo o informe COSO (véase, Banxico, 2000, pp. 3-5) es un modelo que propone un nuevo marco conceptual de control interno capaz de integrar las diversas definiciones y conceptos utilizados sobre este tema.

El Control Interno-Marco Integrado, mejor conocido como el Modelo de Control COSO, fue desarrollado por la Comisión Nacional sobre Reportes Financieros Fraudulentos de los Estados Unidos de Norteamérica (*The Committee of Sponsoring Organizations of the Treadway Comision*) en septiembre de 1992, en su elaboración participaron representantes de organizaciones profesionales de contadores, de ejecutivos de finanzas y de auditores internos.

El modelo COSO, tanto con la definición de Control que propone, como con la estructura de Control que describe, impulsa una nueva cultura administrativa en todo tipo de organizaciones y ha servido de plataforma para diversas definiciones y modelos de Control a nivel internacional (véase, Espinosa, 2002).

El modelo ha tenido gran aceptación y difusión en los medios financieros así como en los consejos de administración de las organizaciones, resalta la necesidad de que los administradores y altos directores presten atención al Control Interno; tal como COSO

lo define, enfatizando la necesidad de los comités de auditoría y de una calificada auditoría tanto interna como externa, recalcando la necesidad de que el control interno forme parte de los diferentes procesos y no de mecanismos burocráticos.

Definición de Control

El modelo COSO define al Control Interno como:

> "Un proceso efectuado por el Consejo de Administración la Dirección y el resto del personal de una organización, diseñado para proporcionar una seguridad razonable respecto al logro de los objetivos dentro de las siguientes áreas: efectividad, eficiencia de las operaciones, confiabilidad de la información financiera y cumplimiento con las leyes y normas aplicables".

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

La concepción del **control** como un proceso implica que se trata de un medio para alcanzar un fin y, por lo tanto, el control no es un fin en sí. Forma parte de los procesos básicos de la administración (planeación, ejecución y supervisión), para que funcione con efectividad, requiere ser construido "dentro" de la infraestructura de la organización, es decir, los controles deben ser incorporados en los sistemas que operan los procesos no añadidos o superpuestos a tales sistemas.

Para este modelo, el control interno es el 'corazón' de una organización, la cultura, las normas sociales y ambientales que la gobiernan.

El COSO establece como premisa fundamental que todo el personal dentro de su ámbito de actuación en una organización tiene participación y responsabilidad en el proceso de Control. Porque que los sistemas de Control son diseñados, establecidos y operados por el personal e igualmente son modificados para finalmente ser evaluados, este modelo de Control asigna una gran importancia a los aspectos de competencia, honorabilidad y actitud del factor humano.

En este modelo, todos los miembros de la organización son responsables del control interno, el nivel de responsabilidad depende de la función que realicen en la empresa, como se muestra a continuación:

PUESTO	FUNCIONES
La administración	O cualquier denominación para el máximo ejecutivo, en el cual recae, en primer lugar, la responsabilidad del control, el cual debe liderar y revisar la manera en que los miembros controlan el negocio. Éstos, a su vez designan responsables de cada función, establecen políticas y procedimientos de control interno más específicos. La responsabilidad se organiza en cascada.
Responsables de las funciones financieras	Los directores financieros y sus equipos tienen una importancia vital porque sus actividades están vinculadas con el resto de las unidades operativas y funcionales de una entidad. Normalmente, están involucrados en el desarrollo de presupuestos y en la planificación financiera. Controlan, siguen y analizan el rendimiento, no sólo desde una perspectiva financiera sino también, en muchas ocasiones, en relación con el resto de operaciones de la entidad y el cumplimiento de requisitos legales. El director financiero, el jefe de contabilidad, así como otros responsables de las funciones financieras de una entidad son claves para determinar la forma en que la administración ejerce el control.
Consejo de administrativo	La administración es responsable ante el Consejo, el cual debe ofrecer asesoría, pautas de actuación y conocer a profundidad las actividades de la entidad. Debe estar preparado para una posible falla de la administración a través de una comunicación con los niveles altos, con los responsables financieros, jurídicos y de auditoría. Muchos consejos de administración llevan a cabo sus tareas a través de comités. Sus funciones y la importancia de sus trabajos varían de una entidad a otra, pero suelen incluir las áreas de auditoría, remuneraciones, finanzas, nombramientos, etcétera. Cada comité puede dar un énfasis específico en determinados elementos del control interno.
Comité de auditoría	El comité, o en su defecto el consejo, está en una posición privilegiada, tiene autoridad para interrogar a los directivos sobre la forma en que

	están asumiendo sus responsabilidades en cuanto a la información financiera, y para asegurar que se tomen medidas correctivas. El comité está, en ocasiones, en la mejor posición dentro de una entidad para identificar situaciones en las que los altos directivos intenten eludir los controles internos o tergiversar los resultados financieros y actuar en consecuencia. Por ello, existen situaciones en las que el comité o el consejo deben afrontar asuntos o circunstancias graves. En este sentido, la Comisión *Treadway* ha emitido directrices generales sobre la estructura y funciones que debe tener el comité de auditoría.
Comité de auditoría	El comité, o en su defecto el consejo, está en una posición privilegiada, tiene autoridad para interrogar a los directivos sobre la forma en que están asumiendo sus responsabilidades en cuanto a la información financiera, y para asegurar que se tomen medidas correctivas. El comité junto con o además de una función de auditoría interna fuerte, está en ocasiones en la mejor posición dentro de una entidad para identificar situaciones en las que los altos directivos intenten eludir los controles internos o tergiversar los resultados financieros y actuar en consecuencia. Por ello, existen situaciones en las que el comité o el consejo deben afrontar asuntos o circunstancias graves. En este sentido, la Comisión Treadway ha emitido directrices generales sobre la estructura y funciones que debe tener el comité de auditoría.
Auditores internos	Desempeñan un papel importante en la evaluación de la eficiencia de los sistemas de control y recomiendan mejoras a los mismos. Según las normas emitidas por el *Institute of Internal Auditors,* los auditores internos deben revisar: “La confiabilidad, la integridad de la información financiera, operativa y los procedimientos empleados para identificar, medir, clasificar y difundir dicha información.” “Los sistemas establecidos para asegurar el cumplimiento de políticas, planes, procedimientos, leyes y normativas” “Los medios utilizados para la salvaguarda de activos y verificar la existencia de los mismos”. “Las operaciones para cerciorarse de si los resultados son coherentes con los objetivos y las metas establecidas y si se han llevado a cabo según los planes previstos”. Todas las actividades de una entidad recaen dentro del ámbito de responsabilidad de los auditores internos (AI). Los AI sólo pueden ser imparciales cuando no están obligados a subordinar su juicio al juicio de otros. El principal medio de asegurar la objetividad de auditoría es la asignación de personal adecuado para esta función, evitando posibles conflictos de intereses y prejuicios.

	La función de AI no tiene como responsabilidad principal el establecimiento del sistema de control interno.
Otros empleados	El control interno es hasta cierto punto responsabilidad de todos los empleados; casi todos producen información utilizada en el sistema de control o realizan funciones para efectuar el control.
Auditoría externa	Contribuyen al logro de los objetivos, aportan opinión independiente y objetiva, contribuyen directamente mediante la auditoría a los estados financieros.

Tabla. Responsabilidades del personal en relación al control interno (Cabay y Quezada, 2010, pp. 28-29)

3.1.1. CoCo

Este modelo (véase, Banxico, 2000) fue dado a conocer por el Instituto Canadiense de Contadores Certificados (CICA) a través de un consejo encargado de diseñar y emitir criterios o lineamientos generales sobre control, el consejo denominado *The Criteria of Control Board.*

El modelo *Canadian Criteria of Control Committee* o COCO es producto de una profunda revisión del Comité de Criterios de Control de Canadá sobre el reporte COSO y cuyo propósito fue hacer el planteamiento de un modelo más sencillo y comprensible, ante las dificultades que en la aplicación del COSO enfrentaron inicialmente algunas organizaciones. El resultado es un modelo conciso, dinámico, encaminado a mejorar el Control, el cual describe y define al Control en forma casi idéntica a lo que hace el modelo COSO.

El propósito del COCO es desarrollar orientaciones o guías generales para el diseño, evaluación y reportes sobre los sistemas de control dentro de las organizaciones.

Estructura del Control

El cambio importante que plantea el modelo canadiense consiste en que en lugar de conceptualizar al proceso de Control como una pirámide de componentes y elementos interrelacionados, proporciona un marco de referencia a través de veinte criterios

generales, que el personal en toda la organización puede usar para diseñar, desarrollar, modificar o evaluar el Control.

Los **criterios** son elementos básicos para entender y, en su caso, aplicar el sistema de control COCO. Se requieren adecuados análisis y comparaciones para interpretar los criterios en el contexto de una organización en particular, y para una evaluación efectiva de los controles implantados.

El llamado **ciclo de entendimiento básico del control**, como se representa en el modelo, consta de cuatro etapas que contienen los veinte criterios generales, conformando un ciclo lógico de acciones a ejecutar para asegurar el cumplimiento de los objetivos de la organización, el cual se muestra a continuación:

PROPÓSITO
1. Los objetivos deben ser comunicados.
2. Se deben identificar los riesgos internos y externos que afecten el logro de objetivos.
3. Las políticas para apoyar el logro de objetivos deben ser comunicadas y practicadas, para que el personal identifique el alcance de su libertad de actuación.
4. Se deben establecer planes para guiar los esfuerzos.
5. Los objetivos y planes deben incluir metas, parámetros e indicadores de medición del desempeño.

COMPROMISO
1. Se deben establecer y comunicar los valores éticos de la organización. 2. Las políticas y prácticas sobre recursos humanos deben estar consistentes de los valores éticos de la organización así como el logro de sus objetivos. 3. La autoridad y responsabilidad deben estar claramente definidas y consistentes de los objetivos de la organización, para que las decisiones se tomen por el personal apropiado. 4. Se debe fomentar una atmósfera de confianza para apoyar el flujo de la información.

APTITUD
1. El personal debe tener los conocimientos, habilidades y herramientas necesarios para el logro de objetivos. 2. El proceso de comunicación debe apoyar los valores de la organización. 3. Se debe identificar y comunicar información suficiente y relevante para el logro de objetivos. 4. Las decisiones y acciones de las diferentes partes de una organización deben ser coordinadas. 5. Las actividades de control deben ser diseñadas como una parte integral de la organización.

EVALUACION Y APRENDIZAJE
1. Se debe monitorear el ambiente interno y externo para identificar información que oriente hacia la reevaluación de objetivos. 2. El desempeño debe ser evaluado contra metas e indicadores. 3. Las premisas consideradas para el logro de objetivos deben ser revisadas periódicamente. 4. Los sistemas de información deben ser evaluados nuevamente en la medida en que cambien los objetivos y se precisen deficiencias en la información. 5. Debe comprobarse el cumplimiento de los procedimientos modificados. 6. Se debe evaluar periódicamente el sistema de control e informar de los resultados.

El COCO parte de la idea de que la unidad más pequeña en una organización es la persona, tomada individualmente y una persona ejecuta una tarea guiada por el entendimiento de:

- Su **propósito** (objetivo).
- El apoyo en su capacidad o aptitud para **alcanzarlo** (información, herramientas y habilidades).
- El sentido de **compromiso** para realizar debida y oportunamente su tarea.
- Que la misma persona debe vigilar y **evaluar** su desempeño.

En este modelo, es importante reiterar que la misma persona deberá vigilar y evaluar su desempeño, al igual que su entorno, para aprender de la experiencia pudiendo así ejecutar mejor su tarea para introducir los cambios necesarios.

La estructura del modelo canadiense requiere de creatividad para su interpretación y aplicación, es adaptable a cualquier organización una vez que se adecúa a las necesidades de sus propios intereses, o usarla de referencia para desarrollar un modelo propio.

Para que este modelo funcione exitosamente se requiere de un alto grado de compromiso de los involucrados así como de un cabal entendimiento de los objetivos tanto generales como específicos de las operaciones de la empresa.

También es necesario un claro entendimiento de las fortalezas y debilidades de la organización, su relación con los riesgos y la oportunidad de alcanzar, de la mejor manera, los objetivos de la misma.

3.1.2. COSO, ERM, SMALL

> La premisa subyacente en la gestión de riesgos corporativos es que las entidades existen con el fin último de generar valor para sus grupos de interés. Todas se enfrentan a la ausencia de certeza y el reto para su dirección es determinar cuánta incertidumbre se puede aceptar mientras se esfuerzan en incrementar el valor para sus grupos de interés.

La incertidumbre implica riesgos y oportunidades y posee el potencial de erosionar o aumentar el valor. La gestión de riesgos corporativos permite a la dirección tratar eficazmente la incertidumbre y sus riesgos y oportunidades asociados, mejorando así la capacidad de generar valor.

Se maximiza el valor cuando la dirección establece una estrategia y objetivos para encontrar un equilibrio óptimo entre los objetivos de crecimiento y rentabilidad y los riesgos asociados, además de desplegar recursos de forma eficaz y eficientemente a fin de lograr los objetivos de la entidad.

La gestión de riesgos corporativos incluye las siguientes capacidades:

Alinear el riesgo aceptado y la estrategia
En su evaluación de alternativas estratégicas, la dirección considera el riesgo aceptado por la entidad, estableciendo los objetivos correspondientes y desarrollando mecanismos para gestionar los riesgos asociados.

Mejorar las decisiones de respuesta a los riesgos
La gestión de riesgos corporativos proporciona rigor para identificar los riesgos y seleccionar entre las posibles alternativas de respuesta a ellos: evitar, reducir, compartir o aceptar.

Reducir las sorpresas y pérdidas operativas
Las entidades consiguen mejorar su capacidad para identificar los eventos potenciales y establecer respuestas, reduciendo las sorpresas y los costes o pérdidas asociados.

Identificar y gestionar la diversidad de riesgos para toda la entidad
Cada entidad se enfrenta a múltiples riesgos que afectan a las distintas partes de la organización y la gestión de riesgos corporativos facilita respuestas eficaces e integradas a los impactos interrelacionados de dichos riesgos.

Aprovechar las oportunidades
Mediante la consideración de una amplia gama de potenciales eventos, la dirección está en posición de identificar y aprovechar las oportunidades de modo proactivo.

Mejorar la dotación de capital
La obtención de información sólida sobre el riesgo permite a la dirección evaluar eficazmente las necesidades globales de capital y mejorar su asignación.

Estas capacidades, inherentes en la gestión de riesgos corporativos, ayudan a la dirección a alcanzar los objetivos de rendimiento y rentabilidad de la entidad y prevenir la pérdida de recursos. La gestión de riesgos corporativos permite asegurar una información eficaz y el cumplimiento de leyes y normas, además de ayudar a evitar daños a la reputación de la entidad y sus consecuencias derivadas. En suma, la gestión de riesgos corporativos ayuda a una entidad a llegar al destino deseado, evitando ‘baches y sorpresas por el camino’.

Eventos Riesgos y Oportunidades
Los eventos pueden tener un impacto negativo, positivo o de ambos tipos a la vez. Los que tienen un impacto negativo representan riesgos que pueden impedir la

creación de valor o erosionar el valor existente. Los eventos con impacto positivo pueden compensar los impactos negativos o representar oportunidades, que derivan de la posibilidad de que ocurra un acontecimiento que afecte positivamente al logro de los objetivos, ayudando a la creación de valor o a su conservación. La dirección canaliza las oportunidades que surgen, para que reviertan en la estrategia y el proceso de definición de objetivos, y formula planes que permitan aprovecharlas.

Definición de la Gestión de Riesgos Corporativos
La gestión de riesgos corporativos se ocupa de los riesgos y oportunidades que afectan a la creación de valor o su preservación. Se define de la siguiente manera:

La gestión de riesgos corporativos es un proceso efectuado por el consejo de administración de una entidad, su dirección y restante personal, aplicable a la definición de estrategias en toda la empresa y diseñado para identificar eventos potenciales que puedan afectar a la organización, gestionar sus riesgos dentro del riesgo aceptado y proporcionar una seguridad razonable sobre el logro de los objetivos.

Esta definición recoge los siguientes conceptos básicos de la gestión de riesgos corporativos:

- Es un proceso continuo que fluye por toda la entidad.
- Es realizado por su personal en todos los niveles de la organización.
- Se aplica en el establecimiento de la estrategia.
- Se aplica en toda la entidad, en cada nivel y unidad, e incluye adoptar una perspectiva del riesgo a nivel conjunto de la entidad.
- Está diseñado para identificar acontecimientos potenciales que, de ocurrir, afectarían a la entidad y para gestionar los riesgos dentro del nivel de riesgo aceptado.
- Es capaz de proporcionar una seguridad razonable al consejo de administración y a la dirección de una entidad.
- Está orientada al logro de objetivos dentro de unas categorías diferenciadas, aunque susceptibles de solaparse.

La definición es amplia en sus fines y recoge los conceptos claves de la gestión de riesgos por parte de empresas y otras organizaciones, proporcionando una base para su aplicación en todas las organizaciones, industrias y sectores. Se centra directamente en la consecución de los objetivos establecidos por una entidad determinada y proporciona una base para definir la eficacia de la gestión de riesgos corporativos.

Consecución de Objetivos
Dentro del contexto de misión o visión establecida en una entidad, su dirección establece los objetivos estratégicos, selecciona la estrategia y fija objetivos alineados que fluyen en cascada en toda la entidad. El presente Marco de gestión de riesgos corporativos está orientado a alcanzar los objetivos de la entidad, que se pueden clasificar en cuatro categorías:

- **Estrategia**: Objetivos a alto nivel, alineados con la misión de la entidad y dándole apoyo.

- **Operaciones**: Objetivos vinculados al uso eficaz y eficiente de recursos.
- **Información**: Objetivos de fiabilidad de la información suministrada.
- **Cumplimiento**: Objetivos relativos al cumplimiento de leyes y normas aplicables.

Esta clasificación de los objetivos de una entidad permite centrarse en aspectos diferenciados de la gestión de riesgos corporativos. Estas categorías distintas, aunque solapables –un objetivo individual puede incidir en más de una categoría– se dirigen a necesidades diferentes de la entidad y pueden ser de responsabilidad directa de diferentes ejecutivos. También permiten establecer diferencias entre lo que cabe esperar de cada una de ellas. Otra categoría utilizada por algunas entidades es la salvaguarda de activos.

Dado que los objetivos relacionados con la fiabilidad de la información y el cumplimiento de leyes y normas están integrados en el control de la entidad, puede esperarse que la gestión de riesgos corporativos facilite una seguridad razonable de su consecución. El logro de los objetivos estratégicos y operativos, sin embargo, está sujeto a acontecimientos externos no siempre bajo control de la entidad; por tanto, respecto a ellos, la gestión de riesgos corporativos puede proporcionar una seguridad razonable de que la dirección, y el consejo de administración en su papel de supervisión, estén siendo informados oportunamente del progreso de la entidad hacia su consecución.

Componentes de la Gestión de Riesgos Corporativos

La gestión de riesgos corporativos consta de ocho componentes relacionados entre sí, que se derivan de la manera en que la dirección conduce la empresa y cómo están integrados en el proceso de gestión. A continuación, se describen estos componentes:

1.- Ambiente interno
Abarca el talante de una organización y establece la base de cómo el personal de la entidad percibe y trata los riesgos, incluyendo la filosofía para su gestión, el riesgo aceptado, la integridad y valores éticos y el entorno en que se actúa.

2.- Establecimiento de objetivos
Los objetivos deben existir antes de que la dirección pueda identificar potenciales eventos que afecten a su consecución. La gestión de riesgos corporativos asegura que la dirección ha establecido un proceso para fijar objetivos y que los objetivos seleccionados apoyan la misión de la entidad y están en línea con ella, además de ser consecuentes con el riesgo aceptado.

3.-Identificación de eventos
Los acontecimientos internos y externos que afectan a los objetivos de la entidad deben ser identificados, diferenciando entre riesgos y oportunidades. Estas últimas revierten hacia la estrategia de la dirección o los procesos para fijar objetivos.

4.- Evaluación de riesgos
Los riesgos se analizan considerando su probabilidad e impacto como base para determinar cómo deben ser gestionados y se evalúan desde una doble perspectiva, inherente y residual.

5.- Respuesta al riesgo
La dirección selecciona las posibles respuestas - evitar, aceptar, reducir o compartir los riesgos - desarrollando una serie de acciones para alinearlos con el riesgo aceptado y las tolerancias al riesgo de la entidad.

6.- Actividades de control
Las políticas y procedimientos se establecen e implantan para ayudar a asegurar que las respuestas a los riesgos se llevan a cabo eficazmente.

7.-Información y comunicación
La información relevante se identifica, capta y comunica en forma y plazo adecuado para permitir al personal afrontar sus responsabilidades. Una comunicación eficaz debe producirse en un sentido amplio, fluyendo en todas direcciones dentro de la entidad.

8.-Supervisión
La totalidad de la gestión de riesgos corporativos se supervisa, realizando modificaciones oportunas cuando se necesiten. Esta supervisión se lleva a cabo mediante actividades permanentes de la dirección, evaluaciones independientes o ambas actuaciones a la vez.

La gestión de riesgos corporativos no constituye estrictamente un proceso en serie, donde cada componente afecta sólo al siguiente, sino un proceso multidireccional e iterativo en que casi cualquier componente puede influir en otro. (Coso, Resumen ejecutivo, pp. 1-3)

[Cabe señalar que no obstante que se dice que son 8 elementos del ERM, en realidad se trata de 5 elementos del COSO, solo que el riesgo es más específico y se apertura con 3 consideraciones analíticas.

ERM significa *Enterprise Risk Management* lo que se le conoce como la Administración de Riesgos Integral, su importancia radica en darle toda la atención a los riesgos. (Identifica el riesgo, evalúa el riesgo y respuesta al riesgo) su publicación fue en septiembre de 2004, y el grupo encargado de desarrollarlo es el despacho Price Waterhouse.]

Relación entre objetivos y componentes
Existe una relación directa entre los objetivos que la entidad desea lograr y los componentes de la gestión de riesgos corporativos, que representan lo que hace falta para lograr aquellos. La relación se representa con una matriz tridimensional, en forma de cubo.

Las cuatro categorías de objetivos estrategia, operaciones, información y cumplimiento están representadas por columnas verticales, los ocho componentes lo están por filas horizontales y las unidades de la entidad, por la tercera dimensión del cubo. Este gráfico refleja la capacidad de centrarse sobre la totalidad de la gestión de riesgos corporativos de una entidad o bien por categoría de objetivos, componente, unidad o cualquier subconjunto deseado.

Eficacia

La afirmación de que la gestión de riesgos corporativos de una entidad es eficaz es un juicio resultante de la evaluación de si los ocho componentes están presentes y funcionan de modo eficaz. Así, estos componentes también son criterios para estimar la eficacia de dicha gestión.

Para que estén presentes y funcionen de forma adecuada, no puede existir ninguna debilidad material y los riesgos necesitan estar dentro del nivel de riesgo aceptado por la entidad.

Cuando se determine que la gestión de riesgos es eficaz en cada una de las cuatro categorías de objetivos, respectivamente, el consejo de administración y la dirección tendrán la seguridad razonable de que conocen el grado de consecución de los objetivos estratégicos y operativos de la entidad, que su información es fiable y que se cumplen las leyes y la normas aplicables.

Los ocho componentes no funcionan de modo idéntico en todas las entidades. Su aplicación en las pequeñas y medianas empresas, por ejemplo, puede ser menos formal y estructurada. Sin embargo, estas entidades podrían poseer una gestión eficaz de riesgos corporativos, siempre que cada componente esté presente y funcione adecuadamente.

Limitaciones

Aunque la gestión de riesgos corporativos proporciona ventajas importantes, también presenta limitaciones. Además de los factores comentados anteriormente, las limitaciones se derivan de hechos como que el juicio humano puede ser erróneo durante la toma de decisiones, que las decisiones sobre la respuesta al riesgo y el establecimiento de controles necesitan tener en cuenta los costes y beneficios relativos, que pueden darse fallos por error humano, que pueden eludirse los controles mediante connivencia de dos o más personas y que la dirección puede hacer caso omiso a las decisiones relacionadas con la gestión de riesgos corporativos. Estas limitaciones impiden que el consejo o la dirección tengan seguridad absoluta de la consecución de los objetivos de la entidad.

Inclusión del Control Interno

El control interno constituye una parte integral de la gestión de riesgos corporativos. Este Marco lo incluye, constituyendo una conceptualización y una herramienta más sólidas para la dirección. El control interno se define y describe en el documento Control Interno

Marco integrado. Dado que éste ha perdurado a lo largo del tiempo y es la base para las reglas, normas y leyes existentes, se mantiene vigente para definir y enmarcar el control interno.

Aunque el presente documento sólo recoge partes de Control Interno
Marco integrado, su estructura entera se incorpora en él a través de referencias.

Roles y Responsabilidades
Todas las personas que integran una entidad tienen alguna responsabilidad en la gestión de riesgos corporativos. El consejero delegado es su responsable último y debería asumir su titularidad. Otros directivos apoyan la filosofía de gestión de riesgos de la entidad, promueven el cumplimiento del riesgo aceptado y gestionan los riesgos dentro de sus áreas de responsabilidad en conformidad con la tolerancia al riesgo. El director de riesgos, director financiero, auditor interno u otros, desempeñan normalmente responsabilidades claves de apoyo. El restante personal de la entidad es responsable de ejecutar la gestión de riesgos corporativos de acuerdo con las directrices y protocolos establecidos.

El consejo de administración desarrolla una importante supervisión de la gestión de riesgos corporativos, es consciente del riesgo aceptado por la entidad y está de acuerdo con él. Algunos terceros, como los clientes, proveedores, colaboradores, auditores externos, reguladores y analistas financieros, proporcionan a menudo información útil para el desarrollo de la gestión de riesgos corporativos, aunque no son responsables de su eficacia en la entidad ni forman parte de ella. (Coso, Resumen ejecutivo, pp. 4-7).

3.1.3. Cadbury

El modelo CADBURY fue desarrollado en el Reino Unido por el comité del mismo nombre y adopta la misma interpretación amplia del control del modelo COSO, pero limita la responsabilidad de los reportes de control a la confiabilidad de la información financiera.

Sus elementos clave son similares, salvo la consideración de los sistemas de información como un componente integrador del control. Este modelo da un mayor énfasis a la evaluación de los riesgos como factor para el correcto funcionamiento de la organización.

3.2. Modelos de control de tecnología de la información

Contar con información oportuna y confiable permite tomar decisiones y realizar operaciones de manera ágil. La rapidez de la tecnología con la que el mundo se está moviendo ha dado lugar a que las empresas optimicen sus procesos de información, convirtiéndose en sus activos más valiosos.

Implementar una solución sistematizada produce muchos beneficios, pero también incrementa el nivel de riesgo, la implementación de un software adaptado a necesidades específicas, genera cambios en los procesos de negocios y de tecnología, lo cual tiene un impacto considerable tanto en los aspectos de control como de seguridad de la información.

De todos los riesgos de negocio, los de tecnología de información pueden ser los más difíciles de comprender y manejar, ya que la tecnología cambia continuamente, cada cambio fluye a través de las compañías y nuevos riesgos. El diseño de los controles se vuelve un factor clave para el éxito, al automatizar un negocio.

El Control Interno y sus esquemas tradicionales de trabajo se han visto impactados por la evolución de los sistemas de información, la aplicación de nuevas estrategias —motivadas por las necesidades de los negocios de expandir sus segmentos de mercado—, la diversificación, aseguramiento de la calidad en sus productos y servicios.

Los sistemas informáticos representan un reto y, una solución, cuando se utilizan como medio de evaluación constante de controles.

La tecnología de información es una herramienta que facilita los procesos de negocios pero también afecta de manera importante el control de las operaciones y el procesamiento de datos.

Los modelos de control de tecnología de información ayudan a comprender estos riesgos y a manejarlos efectivamente al proporcionar un marco claro para su evaluación a través de metodologías de control, monitoreo y medición.

En este tema, se analizarán los aspectos generales de uno de los modelos de control de tecnología de información (TI) más utilizado en la actualidad: el modelo **CobiT**.

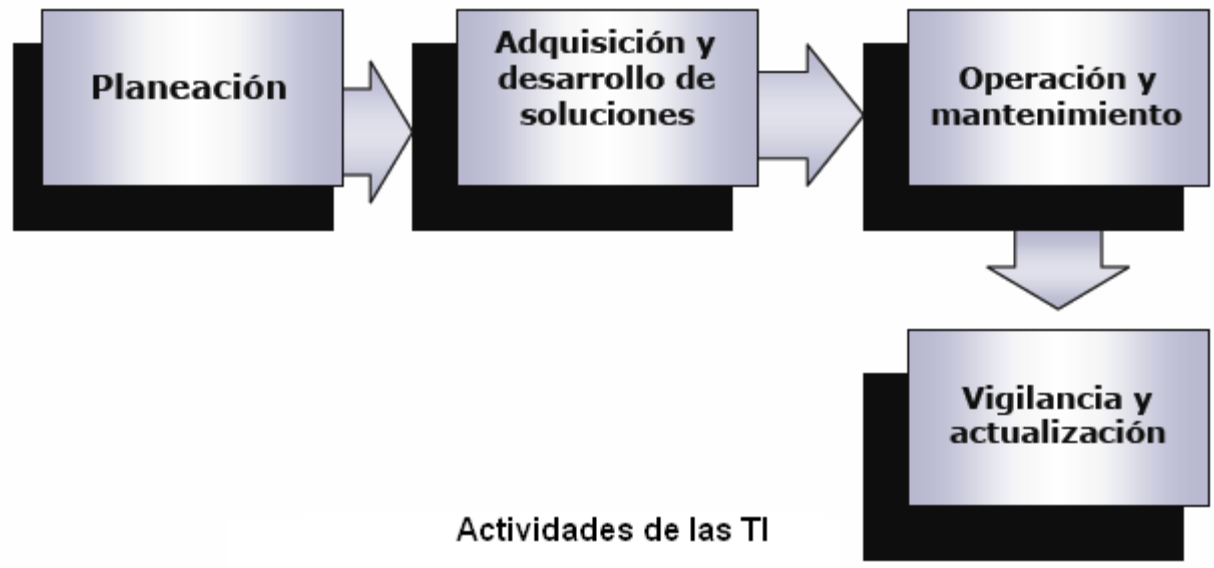
Con la finalidad de comprender cabalmente en qué consisten los modelos de control de tecnología de información, a continuación se analizará brevemente lo que hoy en día se considera tecnología de información (TI).

Tecnología de información (TI)

El término TI (véase, IMCP, 2006) se refiere a:

Elementos de la tecnología de información

Generalmente la TI incluye las siguientes actividades:



Actividades de las TI

Un elemento crítico para el éxito y la supervivencia de las organizaciones es la administración efectiva de la Tecnología de Información (TI). En esta sociedad global (donde la información viaja a través del "ciberespacio" sin las restricciones de tiempo, distancia y velocidad) la TI se ha hecho cada día más importante debido a:

- La creciente dependencia a la información y a los sistemas que proporcionan dicha información.
- La vulnerabilidad de los sistemas.
- El costo de las inversiones actuales y futuras en información y en tecnología de información.
- El potencial que tienen las tecnologías para cambiar radicalmente las organizaciones y las prácticas de negocio, crear nuevas oportunidades y reducir costos.

Por ello, para muchas organizaciones, la información y la tecnología que la soporta representan los activos más valiosos de la empresa.

Las organizaciones exitosas reconocen los beneficios potenciales que la tecnología les puede proporcionar, sin embargo, también comprenden y administran los riesgos asociados con la implementación de nueva tecnología.

La administración de una empresa debe decidir la inversión razonable en seguridad y control en TI y cómo lograr un balance entre riesgos e inversiones en control en un ambiente de TI, frecuentemente, impredecible.

Las empresas deben tener una apreciación y un entendimiento básico de los riesgos y limitantes del empleo de la TI para proporcionar una dirección efectiva y controles adecuados.

CobiT es un modelo de control de TI enfocado a los negocios.

3.2.1. CobiT (Control Objectives for Information and Related Technology)

El ambiente de los negocios: competencias, cambios y costos
La competencia global es ya un hecho. Las organizaciones se reestructuran con el fin de perfeccionar sus operaciones y al mismo tiempo aprovechar los avances en tecnología de sistemas de información para mejorar su posición competitiva.

La reingeniería en los negocios, las reestructuraciones, el *outsourcing*, entre otros, son cambios que impactan la manera en la que operan tanto los negocios como las entidades gubernamentales. Estos cambios han tenido y continuarán teniendo, profundas implicaciones para la administración y las estructuras de control operacional dentro de las organizaciones en todo el mundo.

La especial atención prestada a la obtención de ventajas competitivas y a la economía implica una dependencia creciente en la computación como el componente más importante en la estrategia de la mayoría de las organizaciones.

La automatización de las funciones organizacionales, por su naturaleza, dicta la incorporación de mecanismos de control más poderosos en las computadoras y en las redes, tanto los basados en hardware como en software. Además, las

> características estructurales fundamentales de estos controles están evolucionando al paso de las tecnologías de computación y las redes.
>
> Si los administradores, los especialistas en sistemas de información y los auditores desean ser capaces de cumplir con sus tareas en forma efectiva dentro de un marco contextual de cambios acelerados, deberán aumentar, mejorar, sus habilidades tan rápido como lo demandan la tecnología y el ambiente. Es necesario comprender tanto la tecnología de controles involucrada como su naturaleza cambiante si se desea emitir y ejercer juicios razonables y prudentes al evaluar las prácticas de control que se encuentran en los negocios típicos o en las organizaciones gubernamentales. (CobiT, 1998, pp. 10-11)

En vista de estos continuos cambios, se desarrolló COBIT como un modelo de control de TI enfocado a los negocios que proporciona a las empresas un marco de referencia sobre prácticas de seguridad y control de TI.

Definición

CobiT (Objetivos de Control para la Tecnología de Información) es un modelo de control de TI diseñado por la *Information Systems Audit and Control Foundation* y empresas patrocinadoras como UNISYS y *Price Waterhouse Coopers*, como una fuente de instrucción para los profesionales dedicados a las actividades de control. COBIT contiene estándares para mejorar las prácticas de control y seguridad de las Tecnologías de Información (TI)[8].

CobiT se fundamenta en los Objetivos de Control existentes de la *Information Systems Audit and Control Foundation* (ISACF) y ha sido desarrollado como un estándar generalmente aplicable y aceptado para las buenas prácticas de seguridad así como de control en Tecnología de Información.

[8] La ISACF y los patrocinadores de COBIT declaran que el uso de este producto no asegura un resultado exitoso. No deberá considerarse que este producto incluye todos los procedimientos o pruebas apropiados. Para determinar la conveniencia de cualquier prueba o procedimiento específico, los expertos en control deberán aplicar su propio juicio profesional a las circunstancias de control especiales presentadas por cada entorno de sistemas en particular.

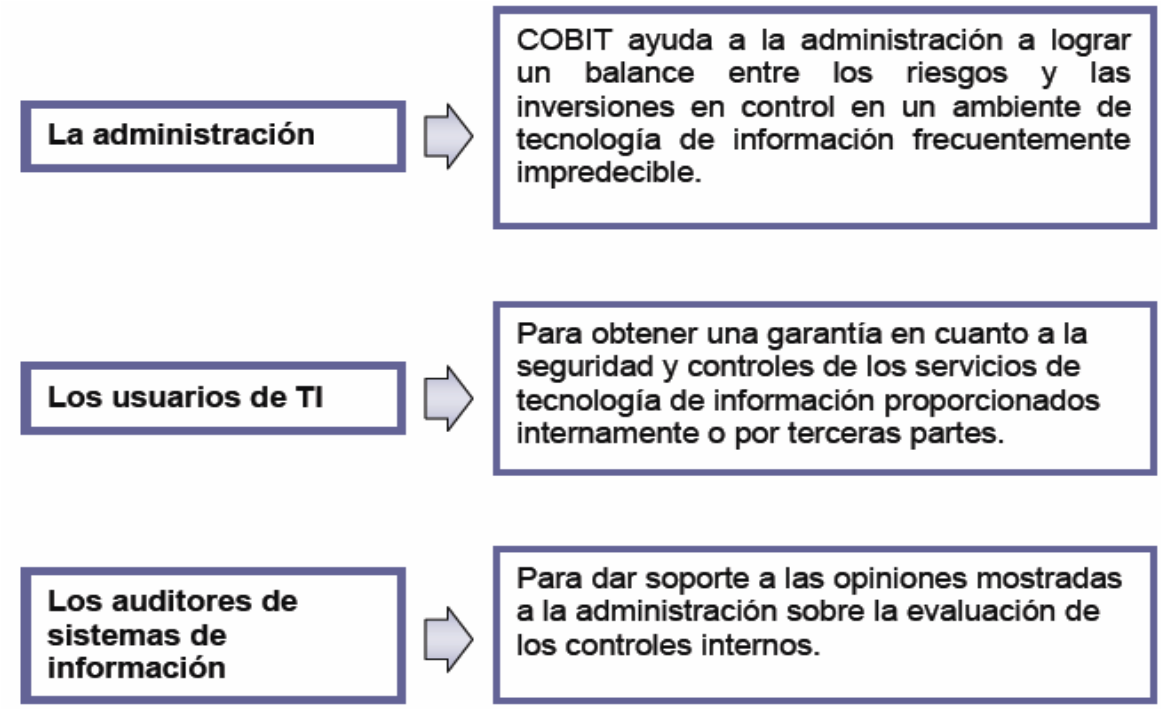
La misión de COBIT “es investigar, desarrollar, publicitar y promocionar objetivos de Control de TI internacionales, actualizados para ser usados por directivos de empresas y auditores” (CobiT, 1998).

Los objetivos de CobiT son:

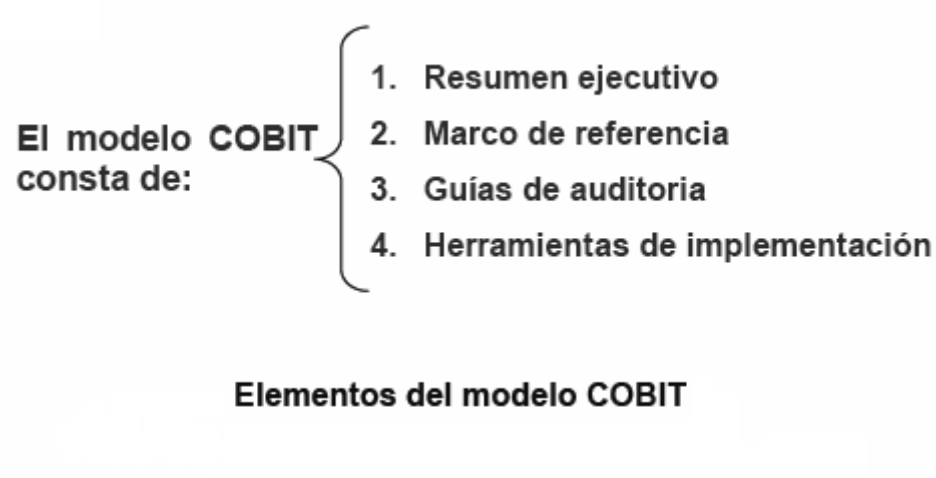
- El desarrollo de políticas claras, buenas prácticas para la seguridad y el control de Tecnología de Información.
- Proporcionar una base que esté estrechamente ligada a los objetivos de negocio, al mismo tiempo que se enfoque a la tecnología de información.
- Proporcionar un marco de referencia definido que ayude al entendimiento y a la administración de riesgos asociados con la TI y con tecnologías relacionadas.

Usuarios

COBIT está diseñado para ser utilizado por:



Contenido



Elementos del modelo COBIT

Resumen ejecutivo

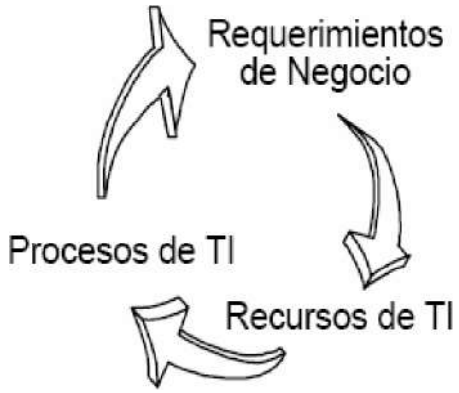
El resumen ejecutivo incluye una síntesis ejecutiva, dirigida a la administración, la cual contiene un entendimiento de los principios y conceptos claves de COBIT.

Marco de referencia

El marco referencial de COBIT proporciona herramientas al propietario de procesos de negocio que facilitan el cumplimiento de esta responsabilidad.

El marco referencial comienza con una premisa simple y práctica:

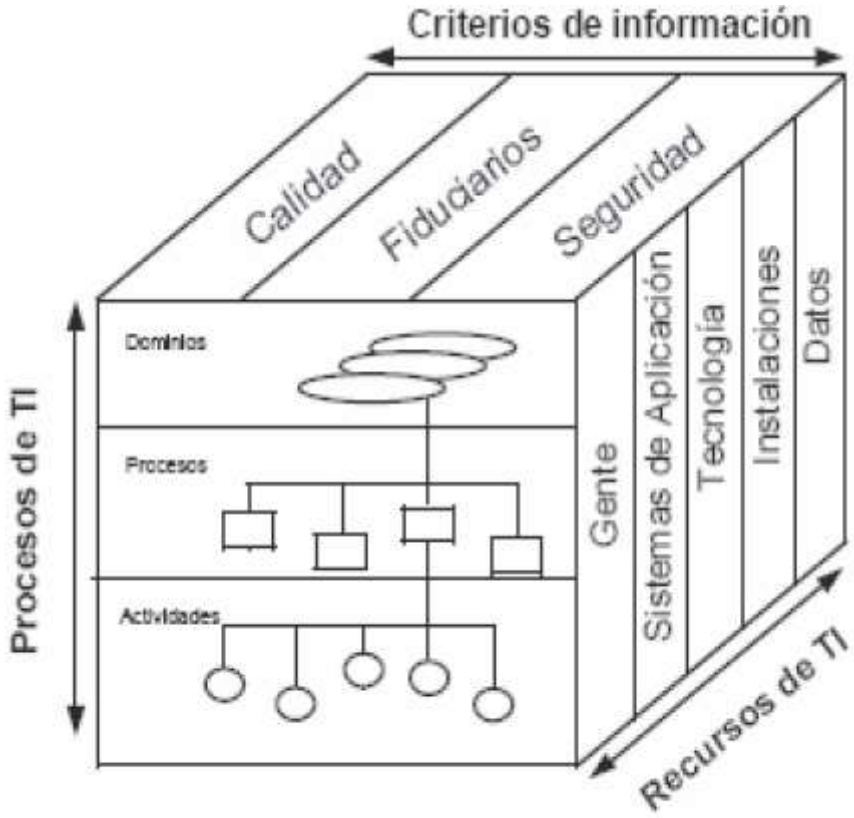
Con el fin de proporcionar la **información que la empresa** (requerimientos del negocio) **necesita** para alcanzar sus objetivos, los **recursos de TI** deben ser administrados por un conjunto de **procesos de TI** agrupados en forma natural.



Por lo tanto, el marco referencial conceptual puede ser enfocado desde tres puntos estratégicos: **a) recursos de TI, b) requerimientos de negocio para la información y c) procesos de TI**.

Por ejemplo, los gerentes de la empresa pueden interesarse en un enfoque de calidad y seguridad. Un gerente de TI puede considerar recursos de TI por los cuales es responsable. Propietarios de procesos, especialistas de TI y usuarios pueden tener un interés en procesos particulares. Los auditores podrán enfocar el marco referencial desde un punto de vista de cobertura de control.

Estos tres **puntos estratégicos** son descritos en el Cubo COBIT que se muestra a continuación:



Puntos estratégicos del modelo COBIT

(CobiT, 1998, p. 15)

a) Recursos de TI

Los recursos de TI identificados en COBIT son:

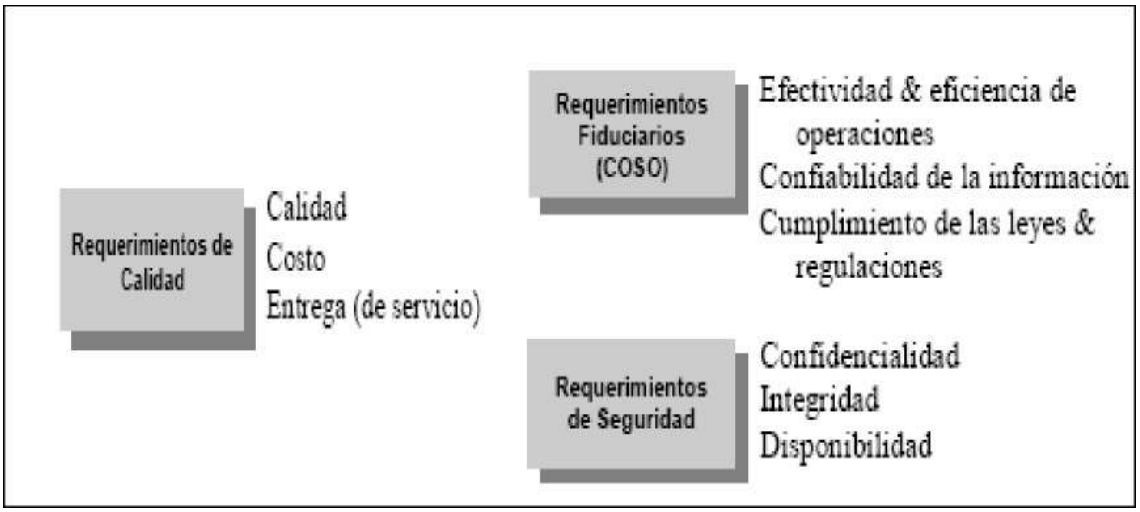
• **Datos**. Los elementos de datos en su más amplio sentido, por ejemplo, externos e internos, estructurados y no estructurados, gráficos, sonido, etcétera.
• **Aplicaciones**. Se entiende como sistemas de aplicación la suma de procedimientos manuales y programados.
• **Tecnología**. La tecnología cubre *hardware*, *software*, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, etcétera.

• **Instalaciones**. Recursos para alojar y dar soporte a los sistemas de información.
• **Personal**. Habilidades del personal, conocimiento, conciencia, productividad para planear, organizar, adquirir, entregar, soportar, monitorear servicios y sistemas de información.

Recursos de TI

b) Requerimientos de negocio

Para satisfacer los objetivos del negocio, la información necesita concordar con ciertos criterios a los que COBIT hace referencia como requerimientos de negocio para la información.



Requerimientos de negocio (CobiT, 1998, p. 13)

Como parte de las buenas prácticas, la documentación es considerada esencial para un buen control y, por lo tanto, la falta de documentación podría ser la causa de revisiones y análisis futuros de controles de compensación en cualquier área específica en revisión.

La información que los procesos de negocio necesita estar proporcionada a través del empleo de recursos de TI. Con el fin de asegurar que los requerimientos de negocio para la información sean satisfechos, deben definirse, implementarse, monitorearse, medidas de control adecuadas para estos recursos.

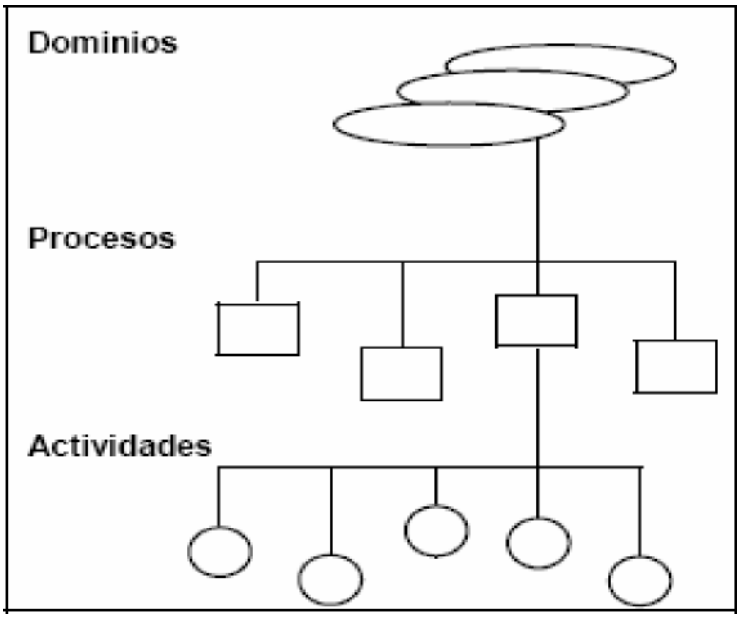
c) Procesos de TI

Existen, en esencia, tres niveles de actividades de TI al considerar la administración de sus recursos. En la base, se encuentran las actividades y tareas necesarias para alcanzar un resultado medible. Las actividades cuentan con un concepto de ciclo de

vida, mientras que las tareas son consideradas más cortas. Algunos ejemplos de esta categoría son las actividades de desarrollo de sistemas, administración de la configuración y manejo de cambios.

La segunda categoría incluye los procesos que son una serie de actividades o tareas conjuntas tareas llevadas a cabo como soporte para la planeación estratégica de TI, evaluación de riesgos, planeación de la calidad, administración de la capacidad y el desempeño.

Al nivel más alto, los procesos son agrupados de manera natural en dominios. Su agrupamiento natural es confirmado frecuentemente como dominios de responsabilidad en una estructura organizacional, y está en línea con el ciclo administrativo o ciclo de vida aplicable a los procesos de TI, como se muestra en la figura siguiente:



Procesos de TI (CobiT, 1998, p. 15)

El marco de referencia de COBIT (1998, pp. 16 y ss.) se integra de un conjunto de treinta y cuatro Objetivos de Control de alto nivel, uno para cada uno de los procesos

de TI, agrupados en cuatro dominios: (1er.) planeación y organización, (2°) adquisición e implementación, (3°) entrega (de servicio) y (4°) monitoreo, los cuales se muestran a continuación:

1er. Dominio: planeación y organización

Este dominio cubre la estrategia, las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

Sus **objetivos de control** son:

- Definición de un plan estratégico de TI.
- Definición de la arquitectura de información.
- Determinación de la dirección tecnológica.
- Definición de la organización y de las relaciones de TI.
- Manejo de la inversión en tecnología de información
- Comunicación de la administración y aspiraciones de la gerencia.
- Administración de recursos humanos.
- Aseguramiento del cumplimiento de requerimientos externos.
- Evaluación de riesgos.
- Administración de proyectos.
- Administración de calidad.

2° Dominio: adquisición e implementación

Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

Sus objetivos son:

- Identificación de soluciones
- Adquisición y mantenimiento de *software* de aplicación
- Adquisición y mantenimiento de arquitectura de tecnología
- Desarrollo y mantenimiento de procedimientos relacionados con tecnología de información
- Instalación y acreditación de sistemas
- Administración de cambios

3° Dominio: Entrega de servicios y soporte

En este dominio se hace referencia a la entrega de los servicios requeridos que abarcan desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. *Incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación*.

• Definición de niveles de servicio • Administración de servicios prestados por terceros • Administración de desempeño y capacidad • Aseguramiento de servicio continuo • Garantizar la seguridad de sistemas • Identificación y asignación de costos • Educación y entrenamiento de usuarios • Apoyo y asistencia a los clientes de TI • Administración de la configuración • Administración de problemas e incidentes • Administración de datos • Administración de instalaciones • Administración de operaciones	

4° Dominio: Monitoreo

"Todos los procesos necesitan ser evaluados regularmente para verificar su calidad y suficiencia en cuanto a los requerimientos de control."

• Monitoreo del proceso • Evaluar lo adecuado del Control Interno • Obtención de aseguramiento independiente • Proveer auditoría independiente	

Dirigiendo estos treinta y cuatro Objetivos de Control de alto nivel, el propietario de procesos de negocio podrá asegurar que se proporciona un sistema de control adecuado para el ambiente de tecnología de información.

Los **Objetivos de Control** son las declaraciones, resultados deseados o propósitos, al implementar procedimientos de control en una actividad particular de TI. Los objetivos de control han sido desarrollados para su aplicación en sistemas de información en toda la empresa.

1. Guías de auditoría

Las Guías de Auditoría contienen los pasos de auditoría correspondientes a cada uno de los treinta y cuatro objetivos de control de TI de alto nivel para proporcionar asistencia a los auditores de sistemas en la revisión de los procesos de TI con respecto a los trescientos dos objetivos detallados de control recomendados para proporcionar a la gerencia certeza o recomendaciones de mejoramiento.

2. Herramientas de implementación

Contiene el conocimiento de la administración y diagnóstico de control de TI, una guía de implementación proporciona lecciones aprendidas por organizaciones que han aplicado CobiT rápida y exitosamente en sus ambientes de trabajo.

El conjunto de herramientas de implementación incluye la **Síntesis Ejecutiva**, proporciona a la administración de una empresa conciencia y entendimiento de CobiT. También se incluyen varios casos de estudio que detallan cómo organizaciones en todo el mundo han implementado CobiT exitosamente. Adicionalmente, se incluyen respuestas a las veinticinco preguntas más frecuentes acerca de CobiT y varias presentaciones para distintos niveles jerárquicos y audiencias dentro de las organizaciones.

En resumen, los Recursos de TI necesitan ser administrados por un conjunto de procesos agrupados en forma natural, con el fin de **proporcionar la información** que la empresa necesita para alcanzar sus objetivos.

Debe tomarse en cuenta que estos procesos pueden ser aplicados a diferentes niveles dentro de una organización. Por ejemplo, algunos de estos procesos serán aplicados al nivel corporativo, otros al nivel de la función de servicios de información, otros al nivel del propietario de los procesos de negocio.

3.2.2. Information Technology Control Guidelines

La identificación de controles convenientes es un riesgo que proviene con el desarrollo y el uso de la tecnología de información. Las *pautas del control de la tecnología de información* es un modelo desarrollado por el Instituto Canadiense de Contadores (*Canadian Institute of Chartered Accountants*- CICA) que proporciona medios prácticos de identificar, de entender, de determinar y de poner controles en la ejecución de la tecnología de información en todos los tipos de empresas.

La primera publicación de este modelo fue en 1970 y ha tenido diversas modificaciones debido a los cambios extensos ocurridos en la tecnología de información. Actualmente el modelo incluye: objetivos del control, estándares mínimos del control y técnicas del control, aplicables a cualquier tipo de empresas y en cualquier nivel de la organización. Este **modelo** asume que los usuarios tendrán **capacidad y experiencia** en el campo del control de la tecnología de información y requiere del juicio de los usuarios para decidir la aplicación de alguna de las técnicas del control presentadas.

Las pautas de control ponen énfasis en las actividades y en las responsabilidades, y sus principios son:

a) La **independencia de la tecnología**, que asegura que el modelo se pueda aplicar en todos los niveles de tecnología permitiendo que surjan nuevas tecnologías.

b) La **gerencia de riesgo**, que describe diferentes tipos de riesgos y de relaciones entre riesgo y control.

La última publicación de este modelo [Vista previa] se integra de los siguientes capítulos: responsabilidad de la gerencia y del control de riesgo; planeamiento de la tecnología de información; sistemas de información, adquisición, desarrollo y mantenimiento; ayuda de las operaciones de computadora y de los sistemas de información; seguridad de la tecnología de información; continuidad del negocio y planeamiento de la recuperación del desastre.

RESUMEN

Como se ha visto, en esencia, todos los modelos hasta ahora conocidos, persiguen los mismos propósitos, y las diferentes definiciones, aunque no son idénticas, muestran gran similitud, sin embargo, el COSO es el modelo mayormente adoptado, sobre todo en países de Latinoamérica, debido, principalmente, a las relaciones comerciales que se tienen con Estado Unidos. Para que estos nuevos modelos funcionen se necesita un cambio radical en la cultura y esquemas de control en las organizaciones que deberá estar soportado por la decisión de los más altos niveles directivos de la misma.

BIBLIOGRAFÍA

SUGERIDA

Autor	Capítulo	Páginas
IMCP. Normas de Auditoría y Normas para Atestiguar [Preferentemente la edición más actual]	Boletín 3050 Estudio y evaluación de control interno	1-21
Colmenares (2011)	I y II	20-50
Poch (1989)	Manual de control interno	25-35

Colmenares Barbosa, Jessica Deisy. (2001). *Diseño de un sistema integral de control interno basado en el modelo COSO para el esquema de negocio de una tienda de conveniencia.* México, posgrado, FCA-UNAM. [Vista previa]

Instituto Mexicano de Contadores Públicos. (2006). *Normas y procedimientos de auditoría y normas para atestiguar*. (26ª ed.) México: IMCP. [En 2010 la versión las llama Normas Internacionales de Auditoría, ISA, del inglés. De cualquier manera, siempre consultar las vigentes.]

Poch y Torres, Ramón. (1989). *Manual de control interno*. Barcelona: Escuela de alta dirección y administración.

Unidad 4.
Normatividad nacional sobre del estudio y evaluación del control interno y su metodología

OBJETIVO PARTICULAR

Analizar la normatividad nacional existente, a fin de entender los requisitos que se deben cumplir en cuanto a su estudio y análisis en los distintos ámbitos de aplicación (internos y externos).

TEMARIO DETALLADO

(24 horas)

4. Normatividad nacional sobre el estudio y evaluación del control interno y su metodología

- 4.1. Comisión de Auditoría del Instituto Mexicano de Contadores Público
  - 4.1.1. Boletines
  - 4.1.2. Guías
- 4.2. Métodos de evaluación
- 4.3. Otras Normas Nacionales (Fiscales o Sectoriales)

INTRODUCCIÓN

Como profesional, el auditor externo adquiere responsabilidad, no sólo con la persona que contrata sus servicios, sino con los usuarios de dicha información que utilizan el resultado de su trabajo como base para tomar decisiones. Es debido a este carácter de responsabilidad social, por lo que la profesión, desde sus inicios, se ha preocupado por asegurar que el desempeño de servicios profesionales se efectúe con un alto nivel de calidad.

Debido a que el trabajo del auditor requiere el empleo del juicio profesional, no es posible establecer procedimientos uniformes, sin embargo, existen fundamentos que son la base para que el auditor realice su trabajo, en términos generales a estos fundamentos básicos del trabajo de auditoría se les llama **Normas de auditoría**, (véase IMPC, 2006, Boletín 1010).

Las normas de auditoría son emitidas por la Comisión de Normas y Procedimientos de Auditoría del IMCP. Las normas son los lineamientos que rigen la actuación del auditor. Estas normas requieren que el auditor realice como parte de su auditoría un estudio y evaluación del Control interno establecido en la empresa sujeta a revisión.

En este tema se conocerá en qué consiste esta evaluación, cuál es su finalidad y cómo se realiza. Se analizará la normativa emitida por la Comisión de Normas, aplicable al tema y los nuevos pronunciamientos emitidos con relación con el tema de fraude, su implicación en la auditoría de EEFF, con el Estudio y evaluación del control interno.

4.1. Comisión de Auditoría del Instituto Mexicano de Contadores Público

El Instituto Mexicano de Contadores Públicos (IMCP)

Desde los inicios de la contaduría pública en nuestro país, los miembros de la profesión sintieron la necesidad de agruparse no sólo para uniformar su práctica profesional y autoimponerse una serie de normas de carácter tanto ético como técnico, sino también para proteger los intereses de los usuarios, de sus servicios y del público en general.

Fue así que en 1917 se formó la primera agrupación profesional, denominada Asociación de Contadores Públicos, contó con once miembros. Años más tarde, el 6 de octubre de 1923 se constituyó el Instituto de Contadores Públicos titulados de México, cuya finalidad era agrupar a los miembros de la profesión.

En **1965** el IMCP adquirió el carácter de Organismo Nacional, con el propósito de representar a la profesión contable nacional, obtuvo en 1977 el reconocimiento oficial de Federación de Colegios de Profesionistas.

En la actualidad, la constitución y funcionamiento del IMCP están regulados por sus estatutos y reglamentos, en vigor desde el 30 de octubre de 1987.

Uno de los **objetivos fundamentales** del IMCP consiste en propugnar por la unificación de criterios, lograr la implantación, aceptación de normas, principios, procedimientos básicos de ética y actuación profesional por parte de sus asociados.

Para cumplir con este objetivo, el IMCP cuenta con un **Comité Ejecutivo Nacional**, el cual incluye una vicepresidencia de legislación para coordinar y vigilar el trabajo de las comisiones emisoras de disposiciones fundamentales en materia de: estatutos, ética profesional, educación profesional continua, normas y procedimientos de auditoría (Véase, IMCP: Historia).

Origen de la CONPA

Una de las comisiones normativas más antiguas y trascendentes del IMCP es la **Comisión de Normas y Procedimientos de Auditoría** (denominada así desde octubre de 1971), la cual fue establecida en el año de 1955, con el propósito de determinar los procedimientos de auditoría recomendables para el examen de los estados financieros que sean sometidos a la opinión del contador público. [Hoy día es CONAA o Comisión de Normas de Auditoría y Aseguramiento.]

Objetivos

Los objetivos de la Comisión son:

- Determinar las normas de auditoría a que deberá sujetarse el contador público independiente que emita dictámenes para terceros, con el fin de confirmar la veracidad, pertinencia o relevancia y suficiencia de información de su competencia.
- Determinar procedimientos de auditoría para el examen de los estados financieros que sean sometidos a dictamen de contador público.
- Determinar procedimientos en cualquier trabajo de auditoría, en sentido amplio, que realice el contador público cuando actúe en forma independiente.
- Hacer las recomendaciones de índole práctica que resulten necesarias como complemento de los pronunciamientos técnicos de carácter general emitidos por la propia Comisión teniendo en cuenta las situaciones particulares que con mayor frecuencia se presentan a los auditores en la práctica de su profesión.

Integración de la Comisión

Los integrantes de la Comisión son propuestos por el Comité Ejecutivo Nacional (Comité) del IMCP. Posteriormente, se procede a hacer la designación oficial de sus miembros, quienes desempeñarán sus cargos durante un periodo de dos años.

Para ser miembro de la Comisión, se deben reunir los siguientes requisitos de calidad:

- Gozar de prestigio profesional en el desempeño de sus actividades.
- Tener cuando menos seis años de desempeño profesional.
- Ser el responsable del área técnica o tener una posición destacada en la entidad en que se desarrolle.
- Ser socio de la firma a que pertenezca en el desempeño de la contaduría pública independiente.
- Haber actuado como expositor o conferenciante en cursos, seminarios o haber sido profesor en instituciones de enseñanza donde se imparta la carrera de contaduría pública.

Normativa emitida por la CONPA

Los boletines emitidos[9] por esta Comisión se clasifican de la siguiente forma:

a) Normas de auditoría	Las normas de auditoría son los requisitos mínimos de calidad relativos a la personalidad del auditor, al trabajo que desempeña y a la información que rinde como resultado de dicho trabajo.
b) Procedimientos de auditoría	Los procedimientos de auditoría son el conjunto de técnicas de investigación aplicables a una partida o a un

[9] La normativa emitida por la CONPA se actualiza y modifica constantemente y cada año el IMCP emite un compendio de las mismas, el cual actualmente incluye 67 boletines comprendidos en 7 series.

	grupo de hechos o circunstancias examinadas, mediante las cuales el contador público obtiene las bases necesarias para fundamentar su opinión. Los procedimientos constituyen la opinión de los miembros de la Comisión, con respecto a la mejor forma de realizar el trabajo de auditoría. Su aplicación deberá hacerse a juicio del auditor de acuerdo con las circunstancias.
c) Otras declaraciones	Las otras declaraciones son los medios a través de los cuales la Comisión da a conocer políticas, programas, estudios, ejemplos, opiniones, guías, etcétera.

La Comisión considera que independientemente de la obligación de normar la actuación del contador público como auditor independiente que asegure alta calidad de sus servicios, tiene el compromiso de promover y patrocinar la publicación de elementos materiales que contribuyan al desarrollo profesional del contador público en el campo de la auditoría, a mantener y aumentar su capacidad técnica, integrar una doctrina profesional de alto nivel y adaptada a las circunstancias y modalidades especiales de este trabajo en nuestro país.

Publicación de los pronunciamientos normativos emitidos por la CONPA

El compendio de boletines emitidos por la CONPA se publica anualmente, ya que generalmente cambia por la emisión de nuevos pronunciamientos o bien la modificación o actualización de los ya existentes. Lo publica el IMCP con el nombre de: “Normas y procedimientos de auditoría”.

Normas de Auditoría generalmente aceptadas

Como profesional, el auditor externo adquiere **responsabilidad**, no solamente con la persona que contrata sus servicios, sino con los usuarios de dicha información que utilizan el resultado de su trabajo como base para tomar decisiones. Es debido a este carácter de responsabilidad social, por lo que la profesión, desde sus inicios, se ha preocupado por asegurar que el desempeño de servicios profesionales se efectúe con un alto nivel de calidad. (Véase, IMPC, 2006: Boletín 1010 y 1020)

Debido a que el trabajo del auditor requiere en gran medida del empleo del *juicio profesional*; no es posible establecer procedimientos uniformes. Sin embargo, existen fundamentos que son la base para que el auditor realice su trabajo, en términos generales a estos fundamentos básicos del trabajo de auditoría se les llama: *Normas de auditoría*.

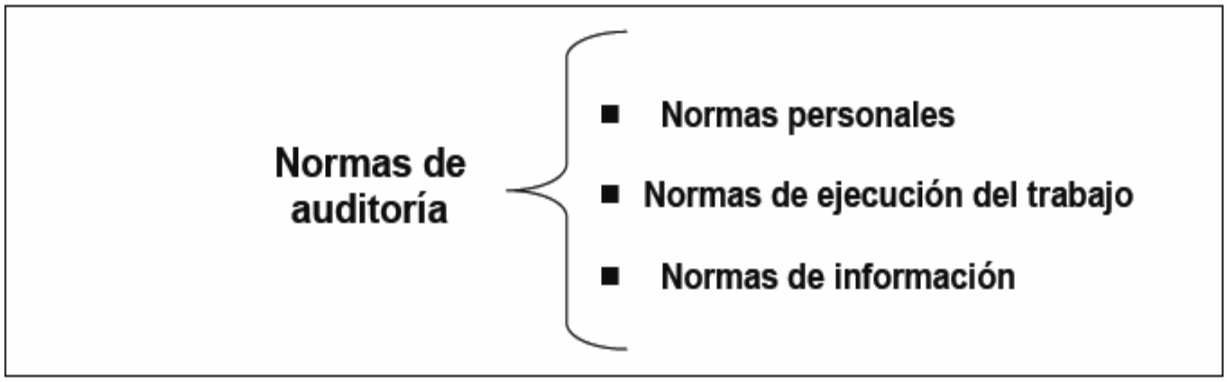
El *juicio profesional* se refiere al empleo de los conocimientos técnicos y experiencia necesarios para seleccionar posibles cursos de acción en el diseño y la aplicación de sus procedimientos de auditoría.

A) Concepto

Las normas de auditoría son los requisitos mínimos de calidad relativos a la personalidad del auditor, al trabajo que desempeña y a la información que rinde como resultado de dicho trabajo.

B) Clasificación

Las normas de auditoría se clasifican en:



Clasificación de normas de auditoria

Normas personales

Las normas personales se refieren a las cualidades que el auditor debe tener para asumir, dentro de las exigencias que el carácter profesional de la auditoría impone, un trabajo de este tipo. Dentro de estas normas existen cualidades que el auditor debe tener pre-adquiridas antes de asumir un trabajo profesional de auditoría y cualidades que debe mantener durante el desarrollo de toda su actividad profesional. Se dividen en:

	a) Entrenamiento técnico y capacidad profesional b) Cuidado y diligencia profesionales c) Independencia

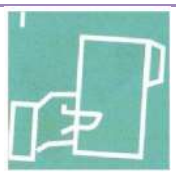
Normas de ejecución del trabajo

Se refieren a los elementos básicos e indispensables en la ejecución del trabajo de auditoría, se clasifican en:

	1. Planeación y supervisión 2. Estudio y evaluación del control interno 3. Obtención de evidencia suficiente y competente

Normas de información

Las normas de información se refieren a los requisitos mínimos de calidad que se deben considerar en la preparación y presentación del dictamen o informe del auditor.

	1. Aclaración de la relación con estados o información financiera y expresión de opinión. 2. Bases de opinión sobre estados financieros.

Estudio y Evaluación del Control Interno

Concepto

El Estudio y Evaluación del Control Interno (EyECI) se efectúa para cumplir con la segunda norma de ejecución del trabajo que señala: El auditor debe realizar un estudio y evaluación adecuado del control interno existente, que le sirva de base para determinar el grado de confianza que va a depositar en él y le permita determinar la naturaleza, extensión y oportunidad que dará a los procedimientos de auditoría (véase, IMPC, 2006: Boletín 1010).

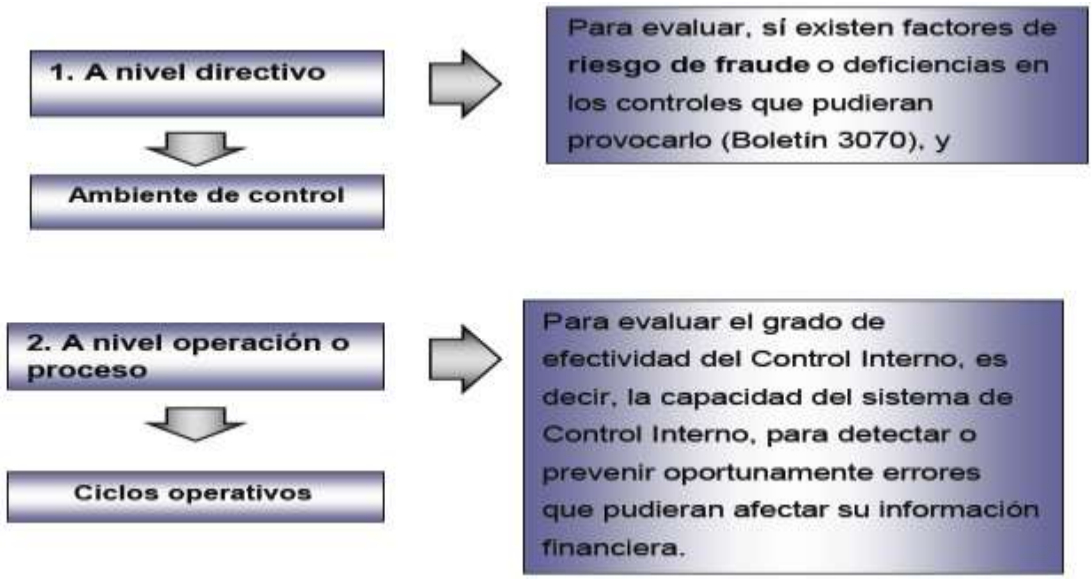
Es decir, el auditor debe estudiar y evaluar el control interno de la empresa cuyos EEFF va a auditar (véase, Mendivil, 2000, p. 29).

El conocimiento, evaluación del control interno deben permitir al auditor establecer una relación específica entre la calidad del control interno de la entidad y la naturaleza, así como oportunidad de las pruebas de auditoría. Por otra parte, el auditor deberá comunicar las debilidades o desviaciones al control interno que haya detectado (situaciones que informar), véase, Boletín 3050 (IMCP, 2006).

Finalidad

La finalidad del EyECI es verificar si los controles establecidos por la empresa aseguran el procesamiento confiable de la información contable y por tanto, permiten el cumplimiento de cada una de las aseveraciones efectuadas por la administración en los EEFF.

El EyECI se realiza:



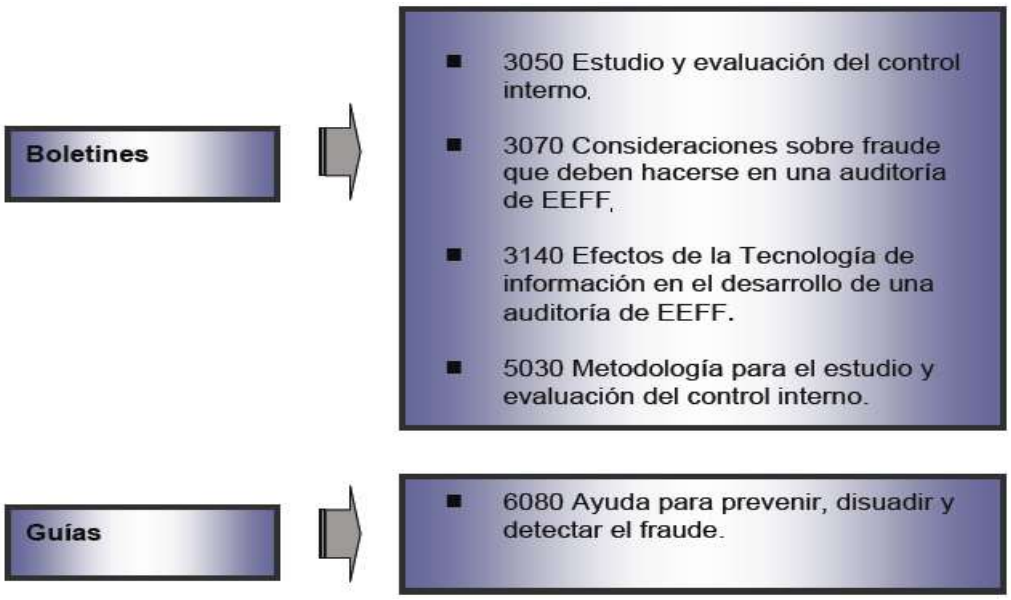
Estudio y evaluación del control interno

Los resultados de la evaluación del Control Interno (CI) son una parte importante del diseño y determinación de las pruebas de auditoría que aplicará el auditor para llevar a cabo su revisión.

4.1.1. Boletines normativos

Pronunciamientos normativos emitidos por la CONPA aplicables al EyECI

Actualmente los boletines y guías emitidos por la CONPA en materia de Control interno son:



Boletines y guías de la CONPA

A continuación, se presenta un resumen de cada uno de los boletines y guías mencionados con la finalidad de que el alumno conozca la normativa vigente, aplicable al EyECI.

Boletín 3050 Estudio y evaluación del control interno

Concepto

El estudio y evaluación del control interno se efectúa con el objeto de cumplir con la norma de ejecución del trabajo que requiere que: "El auditor debe efectuar un estudio y evaluación adecuado del control interno existente, que le sirva de base para determinar el grado de confianza que va a depositar en él y le permita determinar la naturaleza, extensión y oportunidad que va a dar a los procedimientos de auditoría".

Alcance

Este boletín trata sobre el estudio y evaluación del control interno que el auditor efectúa en una revisión de EEFF practicada conforme a las Normas de Auditoría Generalmente Aceptadas.

Objetivos

Los objetivos de este boletín son:

	a) Definir los elementos de la estructura del Control interno. b) Establecer los pronunciamientos normativos aplicables a su estudio y evaluación, como un aspecto fundamental al diseñar la estrategia de auditoría. c) Señalar los lineamientos que deben seguirse al informar sobre debilidades o desviaciones al control interno.

Estructura del Control interno

a) Concepto

La estructura de control interno de una entidad consiste en las políticas y procedimientos establecidos para proporcionar una seguridad razonable de poder lograr los objetivos específicos de la entidad.

b) Elementos

La estructura del control interno se integra de los siguientes cinco elementos:

I. El ambiente de control
II. La evaluación de riesgos
III. Los sistemas de información y comunicación
IV. Los procedimientos de control
V. La vigilancia

La división del control interno en cinco elementos proporciona al auditor una estructura útil para evaluar el impacto de los controles internos de una entidad en la auditoría. Sin embargo, esto no necesariamente refleja cómo una entidad considera e implementa su control interno; asimismo, la primera consideración del auditor refiere a cómo un control específico afecta las aseveraciones en los EEFFF más que su clasificación en uno de los elementos de control interno, antes mencionados, en particular.

I. Ambiente de control

Representa la combinación de factores que afectan las políticas y procedimientos de una entidad, fortaleciendo o debilitando sus controles.

Se integra por los siguientes factores:

- **Actitud de la administración hacia los controles internos establecidos**: El hecho de que una entidad tenga un ambiente de control satisfactorio depende de la actitud y las medidas de acción que tome la administración que de cualquier otra

cosa. Si el compromiso para ejercer un buen control interno es deficiente, seguramente el ambiente de control será deficiente.

La **efectividad** del control interno depende en gran medida de la integridad y de los valores éticos del personal que diseña, administra y vigila el control interno de la entidad.

- **Estructura de organización de la entidad**:
  Si el tamaño de la estructura de la organización no es apropiado para las actividades de la entidad, o el conocimiento y la experiencia de los gerentes y personal clave no es la adecuada, puede existir un mayor riesgo en el debilitamiento de los controles.

  Funcionamiento del consejo de administración y sus comités: las actividades del consejo de administración y otros comités (como el de auditoría) pueden ser importantes para fortalecer los controles, siempre y cuando éstos sean participativos e independientes de la administración.

- **Métodos para asignar autoridad y responsabilidad**: el auditor debe verificar que la asignación de autoridad y responsabilidad esté acorde con los objetivos y metas organizacionales, que éstos se hagan a un nivel adecuado, sobre todo las autorizaciones para cambios en políticas o prácticas.

- **Métodos de control administrativo para supervisar y dar seguimiento al cumplimiento de las políticas y procedimientos, incluyendo la función de auditoría interna**: el grado de supervisión continua sobre la operación que lleva a cabo la administración, da al auditor una evidencia importante de si el sistema de control interno está funcionando adecuadamente y de si las medidas correctivas se realizan en forma oportuna.

- **Políticas y prácticas de personal**: la existencia de políticas y procedimientos para contratar, entrenar, promover y compensar a los empleados, así como la existencia de códigos de conducta u otros lineamientos de comportamiento, fortalecen el ambiente de control.

- **Influencias externas que afectan las operaciones y prácticas de la entidad**: la existencia de canales de comunicación con clientes, proveedores y otros entes externos que permitan informar o recibir información sobre las normas éticas de la entidad o sobre cualquier cambio en las necesidades de la misma, así como el seguimiento a dichas comunicaciones, fortalecen los controles de una entidad.

La calidad del ambiente de control es una clara indicación de la importancia que la administración de la entidad le da a los controles establecidos.

II. La evaluación de riesgos

El propósito de la evaluación de riesgos de la entidad es el de identificar, analizar y administrar riesgos que pueden afectar los objetivos de la entidad.

Por ejemplo, la evaluación de riesgos puede contemplar cómo la entidad considera la posibilidad de operaciones no registradas o cómo identifica y analiza estimaciones o provisiones importantes en los EEFF.

Los **riesgos relevantes** para la emisión de reportes financieros incluyen eventos o circunstancias externas e internas que pueden ocurrir y afectar la habilidad de la entidad en el registro, procesamiento, agrupación o reporte de información, consistente con las aseveraciones de la administración en los EEFF.

Algunos de estos riesgos pueden ser:

a) **Nuevo personal**: el nuevo personal puede tener un enfoque diferente en relación con el control interno.

b) **Crecimientos acelerados**: un crecimiento acelerado en las operaciones puede forzar los controles y crear el riesgo de que éstos no se realicen o se ignoren.

c) **Nuevas tecnologías**: la incorporación de nuevas tecnologías dentro de los procesos productivos o los sistemas de información pueden cambiar los riesgos asociados con el control interno.

d) **Cambio en pronunciamientos contables**: la adopción de un nuevo pronunciamiento contable o un cambio en los ya existentes, puede afectar los riesgos relacionados con la preparación de los estados financieros.

El auditor deberá investigar cómo realiza el cliente la evaluación de riesgos relevantes de la entidad, y cuáles son las medidas que realiza para su administración y manejo.

III. Los sistemas de información y comunicación

Los sistemas de información consisten en los métodos y registros establecidos para identificar, reunir, analizar, clasificar, registrar y producir información cuantitativa de las operaciones que realiza una entidad económica.

La calidad de los sistemas generadores de información afecta la habilidad de la administración para tomar decisiones, para controlar las actividades de la entidad y en la preparación de reportes financieros confiables y oportunos.

El auditor debe obtener un entendimiento de las formas que la entidad utiliza para informar las funciones, responsabilidades y cualquier aspecto importante en relación con la información financiera.

El auditor debe revisar que el sistema contable establecido en la entidad, cuente con métodos y registros que:

- Identifiquen y registren únicamente operaciones reales y autorizadas por la Administración.
- Describan oportunamente todas las operaciones con el detalle necesario que permita su adecuada clasificación
- Cuantifiquen las operaciones en unidades monetarias
- Registren las operaciones en el periodo correspondiente.
- Presenten y revelen adecuadamente dichas operaciones en los EEFF.

El auditor debe obtener un entendimiento de las formas que la entidad utiliza para informar las funciones, responsabilidades y cualquier aspecto importante con relación a la información financiera.

IV. Los procedimientos de control

Son los procedimientos y políticas que establece la administración, proporcionan una seguridad razonable, de que se logrará en forma eficaz y eficiente los objetivos específicos de la entidad.

Los controles persiguen diferentes objetivos y se aplican en distintos niveles de la organización y del procesamiento de las operaciones. Atiende a su naturaleza, los controles pueden ser: preventivos o de detección.

Los controles están dirigidos a cumplir con los siguientes objetivos:

- Autorización
- Segregación de funciones
- Registro de operaciones
- Custodia de activos
- Verificaciones y valuación de las operaciones registradas

El hecho de que la administración establezca formalmente controles, no necesariamente significa que éstos operen efectivamente. El auditor debe evaluar la manera en que la entidad ha aplicado los controles, su uniformidad de aplicación, qué persona las ha llevado a cabo y, finalmente, basado en dicha evaluación, determinará el grado de efectividad de dichos controles.

V. La vigilancia

Una importante responsabilidad de la administración es **establecer y mantener los controles internos**, así como vigilarlos con el objetivo de identificar si están operando efectivamente o si deben modificarse cuando existen cambios importantes.

La vigilancia es un proceso que asegura la eficiencia del control interno a través del tiempo, incluye la evaluación del diseño y operación de procedimientos de control en forma oportuna y aplica medidas correctivas cuando es necesario.

Este proceso se lleva a cabo a través de actividades en marcha (en el momento en que se realizan las operaciones normales), evaluaciones separadas o por la combinación de ambas. La existencia de un departamento de auditoría interna o de una persona que realice funciones similares, contribuye en forma significativa en el proceso de vigilancia.

El auditor debe conocer los tipos de actividades que la entidad lleva a cabo para vigilar el adecuado funcionamiento del control interno sobre la información financiera, incluyendo cómo esas actividades son utilizadas para iniciar acciones correctivas.

Estudio y Evaluación del Control interno

a) Consideraciones generales

Al evaluar una estructura de control interno el auditor deberá considerar los siguientes aspectos:

- Tamaño de la entidad.
- Características de la actividad económica en la que opera.
- Organización de la entidad.
- Naturaleza del sistema de contabilidad y de las técnicas de control establecidas.
- Problemas específicos del negocio.
- Requisitos legales aplicables.

Por ejemplo, una estructura de organización con una delegación formal de autoridad, podrá influir favorablemente en el ambiente de control de una entidad grande. Sin embargo, una entidad pequeña, con participación efectiva del dueño-gerente, en general no requiere de procedimientos contables extensos, ni de registros contables sofisticados o procedimientos de control formales, tales como políticas escritas, seguridad de la información o procedimientos para obtener cotizaciones competitivas.

b) Evaluación preliminar. Al iniciar el estudio y evaluación del control interno de una entidad, el auditor deberá:

- Comprender el ambiente de control establecido por la Administración para detectar errores potenciales.
- Describir y verificar su comprensión de los procedimientos de control de la Administración, incluyendo aquellos relativos a la evaluación de riesgos.
- Conocer los procesos de mayor riesgo de la entidad y evaluar su importancia.
- Evaluar el diseño de los sistemas de control en los procesos de mayor riesgo, para determinar si es probable que sean eficaces para prevenir o detectar y corregir los errores potenciales identificados.
- Seleccionar los procesos a evaluar, diseñar las pruebas aplicar determinando **la naturaleza y el alcance de las mismas.**
- **Documentar** (Con memorandums, gráficas o diagramas) su conocimiento y comprensión de la estructura de control interno, como parte del proceso de planeación de la auditoría.

c) Pruebas de cumplimiento

Las pruebas de cumplimiento son pruebas diseñadas por el auditor, para comprobar si uno o más procedimientos de control interno estaban en operación durante el periodo auditado.

Su finalidad es reunir evidencia suficiente para concluir si los sistemas de control establecidos por la administración, prevendrán, detectarán y corregirán errores potenciales que pudieran tener un efecto importante en los EEFF.

Estas pruebas implican el examen de documentación de operaciones para buscar la presencia o ausencia de atributos específicos (controles de detección).

d) Resultados del EyECI

Con base en los resultados obtenidos de la aplicación de las pruebas de cumplimiento, se determina el grado de efectividad de los controles (alto, medio, bajo) y el riesgo de control de los EEFF.

El **grado de efectividad** de los controles, se determina considerando:

- si los controles probados prevén o detectan errores antes o durante el proceso de las operaciones y,

- si los controles probados permiten que se cumpla con los objetivos de procesamiento de información, autorización, salvaguarda, segregación de funciones y evaluación.

El **riesgo de control** (véase, Boletín 3030, en IMCP, 2006) representa el riesgo de que los errores importantes, al agregarse a otros errores que pudieran existir en un rubro específico de los EEFF, no sean prevenidos o detectados de forma oportuna por el sistema de control interno contable en vigor.

Por lo tanto, **a menor efectividad del control interno, el riesgo de control es mayor y a la inversa**.

El riesgo de control, combinado con otros dos riesgos (inherente y de detección) le permiten al auditor determinar la naturaleza, el alcance y la oportunidad de sus pruebas auditoría (sustantivas).

Es decir, con base en la combinación del riesgo inherente, de control y detección, el auditor determina el tipo pruebas que aplicará (**naturaleza**), el porcentaje de revisión (**alcance o extensión**) y el momento (**oportunidad**) en el que deberá aplicar sus pruebas. A mayor efectividad del control interno, disminuye la posibilidad de que los EEFF contengan aseveraciones equivocas, se reduce también el riesgo de que existan irregularidades (**fraude**) que pudieran tener un impacto significativo en los EEFF, y por lo tanto el trabajo del auditor disminuye.

e) Comunicación de situaciones a informar

En virtud de que las expectativas de los usuarios con respecto a la responsabilidad del auditor para informar por escrito sobre debilidades o desviaciones relacionadas con la estructura del control interno se han incrementado, ha sido necesario definir las situaciones que informar, así como la forma y contenido de dicho informe.

Las situaciones que informar son asuntos que llaman la atención del auditor y que en su opinión deben comunicarse al cliente, ya que representan deficiencias importantes en el diseño u operación de la estructura del control interno, que podrían afectar negativamente la capacidad de la organización para registrar, procesar, resumir y reportar información financiera uniforme con las afirmaciones de la administración en los EEFF.

Esta comunicación se debe hacer con personas de alto nivel de autoridad y responsabilidad, tales como el consejo de administración, el dueño de la entidad o con quienes haya contratado al auditor, preferentemente por escrito, y deberá ser documentada en los papeles de trabajo.

Algunas de estas situaciones pueden ser:

- Diseño inadecuado de la estructura del control interno en general.
- Ausencia de una adecuada segregación de funciones.
- Falta de revisión y aprobación adecuada de las operaciones, pólizas contables o reportes emitidos.
- Medidas deficientes para la protección de activos.

f) Forma y contenido del informe

El informe donde se comunican las situaciones por informar debe contener:

- La indicación, el propósito de la auditoría, esto es, emitir una opinión sobre los estados financieros y no proporcionar una seguridad del funcionamiento de la estructura del control interno.

- Los aspectos considerados como "situaciones que informar".
- Las restricciones establecidas para la distribución de tal comunicación.

El auditor deberá considerar si debe comunicar los asuntos importantes durante el curso de la auditoría o al concluirla, en función de la urgencia de una acción correctiva inmediata.

Boletín 5030 Metodología para el EyECI

Alcance

Este boletín incluye los procedimientos recomendados para el estudio y evaluación del control interno. Los procedimientos señalados en este boletín son aplicables al estudio y evaluación de la estructura del control interno, cuando éstos se realizan como parte de una auditoría de EEFF conforme con las normas de auditoría generalmente aceptadas.

Es importante señalar, que existen diversos enfoques válidos para realizar dicho estudio y evaluación, que pueden ser aplicables según el criterio del auditor.

Objetivo

El objetivo de este boletín es comunicar los procedimientos de auditoría recomendados para realizar y documentar el EyECI durante el proceso de planeación de una auditoría de estados financieros.

Procedimientos recomendados para el estudio de los elementos de la estructura del control interno

1. Procedimientos aplicables a la evaluación del ambiente de control

El ambiente de control es el resultado conjunto de diversos factores que afectan la efectividad global del control interno.

El auditor debe evaluar si el ambiente de control promueve sistemas contables confiables y procedimientos de control efectivos.

Para evaluar adecuadamente los factores del ambiente de control, el auditor deberá investigar y documentar en sus papeles de trabajo, lo siguiente:

En relación con las características e integridad de la administración y su habilidad para desarrollar sus funciones, el auditor debe investigar y documentar:

- La posible participación de la administración en actos ilegales.
- Actitud de la administración para aceptar riesgos anormales de alto nivel en la toma de decisiones.
- Cambios continuos de bancos, abogados o auditores.
- Existencia de dificultades personales significativas u otras influencias en quienes integran la administración que pudieran afectar su integridad, actitudes o desempeño.
- Si la administración está concentrada en una persona o en un grupo pequeño.
- Si existe alguna persona que sin ser accionista, ni tener en la entidad un puesto ejecutivo, ejerza influencia significativa en los asuntos de la entidad.

El auditor debe evaluar y documentar el compromiso de la administración sobre lo razonable de los EEFF, y considerar:

- Si la administración de la entidad aplica agresivamente la normativa contable.

- Si se rehúsa a aceptar y registrar los ajustes de auditoría o si busca distorsionar los resultados.
- La probable existencia de un número significativo de operaciones con partes relacionadas fuera del curso normal de los negocios.

En relación con el diseño y mantenimiento de los sistemas contables y controles internos efectivos, el auditor debe revisar si existe:

- Falta de interés de la administración por las deficiencias que lleguen hacerse de su conocimiento.
- Establecimiento de políticas con respecto a prácticas de negocios, conflicto de intereses y código de conducta.
- Establecimiento de procedimientos que prevengan actos ilegales.

Otras situaciones que el auditor deberá observar y considerar son las siguientes:

- El grado de rotación del personal en puestos clave.
- Si la empresa ha cumplido con fecha de cierre o de entrega de información.
- El número de errores ocurridos en auditorías anteriores.

Con respecto a la estructura organizacional, el auditor deberá considerar, entre otros, los siguientes aspectos:

- Lo apropiado de ésta con respecto al tamaño y a la naturaleza de la entidad.
- Si los recursos humanos y materiales de las áreas de finanzas, contabilidad y sistemas son adecuados.

- La complejidad de la estructura, por ejemplo, si tiene sucursales, afiliadas, etcétera.
- Si el grado de supervisión y control son adecuados al tamaño y naturaleza de la empresa.

El auditor deberá verificar el funcionamiento del Consejo de administración y sus comités, y considerar para ello:

- La experiencia y reputación de sus miembros.
- Si es adecuado en relación con la naturaleza y tamaño de la entidad.
- La periodicidad con la que se reúnen para establecer objetivos y políticas, revisar el desempeño de la entidad y tomar acciones adecuadas y si se preparan oportunamente y firman las minutas de las juntas.
- El grado de autoridad y los recursos con los que cuenta el consejo o el comité para cumplir adecuadamente sus funciones de vigilancia del proceso de la información financiera.

En cuanto a métodos para la adecuada asignación de autoridad y responsabilidad, el auditor debe verificar:

- Que se hayan dado a conocer los objetivos generales y particulares de la entidad de manera clara y comprensible.
- Que la entidad cuente con un organigrama general y particular de cada una de sus áreas.
- Si existen descripciones de puestos, delineando funciones específicas, relaciones jerárquicas y restricciones, y que estén establecidas claramente responsabilidades y niveles de autoridad.
- Si cuenta con políticas por escrito referentes a: prácticas de negocios, conflicto de intereses y código de conducta.

- La documentación de los sistemas de cómputo, indicando los procedimientos para autorizar operaciones y aprobar cambios a los sistemas existentes.
- Si existe un proceso formal de planeación y presupuesto como herramienta para vigilar los resultados y objetivos del negocio.
- Si la empresa cuenta con un departamento de auditoría interna, su posición organizacional, la competencia de sus colaboradores y las funciones que desempeña.

En relación con las políticas y prácticas de personal, el auditor deberá verificar que la entidad cuente con:

- Procedimientos y políticas por escrito para reclutar, contratar, capacitar, evaluar, promover, compensar y proporcionar al personal los recursos necesarios para que pueda cumplir con sus responsabilidades asignadas.
- Descripciones de trabajo adecuadas para cada puesto.
- Canales adecuados de comunicación hacia todos los niveles de personal que proporcionen un flujo oportuno y eficiente de información de carácter general, de negocios, técnica, etcétera.

2. Procedimientos aplicables a la revisión de la evaluación de riesgos

El auditor debe evaluar cuáles son los procedimientos que ayudan a la entidad, y con ello, identificar, analizar, administrar los riesgos, y cómo mide su impacto en la información financiera.

Tomar decisiones de negocios, como ampliar las líneas de crédito para obtener más clientes, puede traer consigo un problema potencial de cuentas incobrables, que debe ser neutralizado a través de procedimientos de control más rigurosos, por ejemplo, mediante análisis de crédito más estrictos.

3. Procedimientos aplicables a la revisión de los sistemas de información

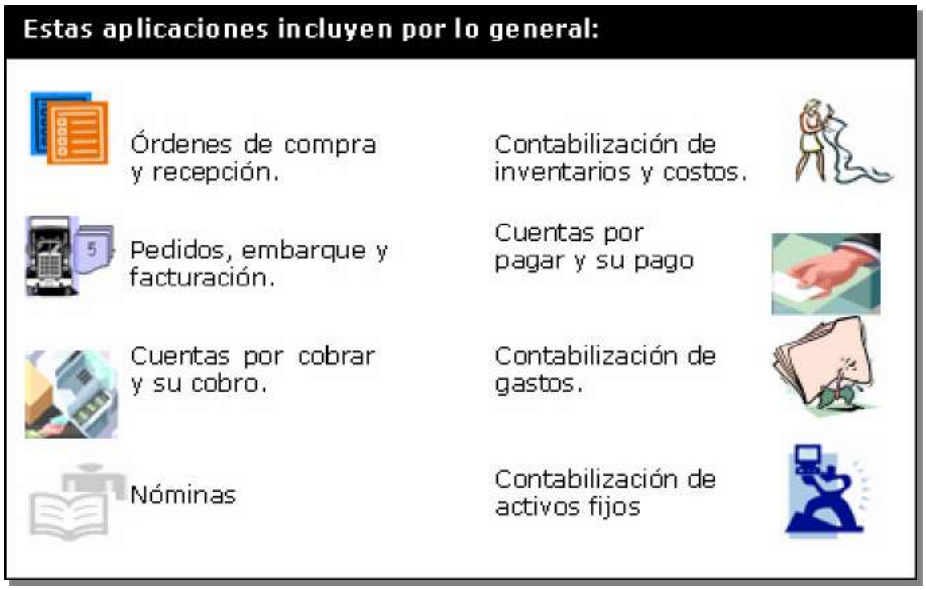
El auditor deberá obtener un conocimiento general del sistema contable de los medios y formas utilizadas por la administración para comunicar a las distintas áreas de la organización las funciones y responsabilidades de cada una de ellas, relacionadas con la operación del sistema de control interno.

Ese conocimiento, le permitirá al auditor identificar los riesgos específicos asociados con el control interno y desarrollar un plan de auditoría adecuado. La información necesaria puede obtenerse como parte del proceso de planeación, de pláticas con las gerencias de finanzas y de procesamiento de datos con la asesoría de un especialista en computación, cuando así se requiera.

El uso de **Tecnología de Información** (TI) es un elemento importante en el proceso de la información contable, independientemente del tamaño de la entidad. Para determinar la naturaleza y el grado de conocimientos que se requiere sobre el uso de TI (véase, Boletín 3140 *Efectos del de la TI en el desarrollo de una auditoría de EEFF*) y la necesidad de ayuda de un especialista, el auditor deberá determinar:

- El grado en que se utilizan.
- La complejidad del entorno y el volumen de operaciones que se procesan.
- La importancia de la TI para la entidad.

El auditor deberá conocer el sistema contable y las principales aplicaciones que lo alimentan.



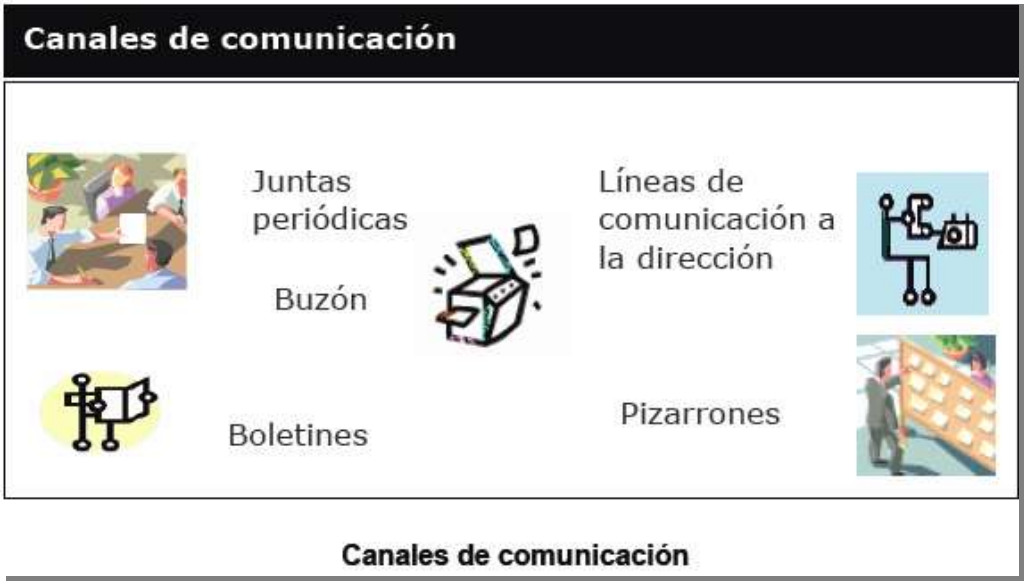
Aplicaciones del sistema contable

El auditor deberá elaborar una lista de las aplicaciones contables más importantes (ejemplo: ventas/cuentas por cobrar) y de las cuentas de los EEFF relacionadas. Por cada aplicación deberá:

- Elaborar una breve descripción general que incluya el propósito de la aplicación; controles del usuario y programados; función en el inicio de las operaciones, e historia de los errores de proceso.
- Describir el perfil de la aplicación, determinando el volumen de las operaciones y referir el nivel de complejidad del procesamiento.
- Definir las funciones clave (ejemplo: preparación de facturas, actualización de archivos, emisión de informes) y la frecuencia de su uso (ejemplo: diario).
- Verificar la historia del sistema, señalando las fechas o periodos de adquisición, instalación y/o modificación.

Procedimientos aplicables a la revisión de los sistemas de comunicación

El auditor verificar cómo son comunicados los asuntos relevantes (memorandos, manuales, etcétera), la frecuencia y los canales de comunicación implementados tales como:



Canales de comunicación

4. Procedimientos aplicables a la revisión de los procedimientos de control

Los controles son los procedimientos establecidos por la administración de una entidad; para proporcionar una seguridad razonable del logro de sus objetivos; sin embargo, el hecho de que existan formalmente políticas o procedimientos de control, no significa que estén operando con eficacia, por lo cual, el auditor deberá confirmar este hecho, cerciorarse de la uniformidad de aplicación de los procedimientos y de qué personas llevan a cabo esas aplicaciones.

Por lo general, no es necesario probar todos los procedimientos de control identificados en las gráficas de flujo de operaciones, memorandos descriptivos o cuestionarios que contribuyen al logro total o parcial de los objetivos de control.[10]

Es importante probar aquellos procedimientos de control cuyos objetivos son considerados clave en función de los riesgos de auditoría implicados.

[10] La planeación de una auditoría no requiere entender en su totalidad los procedimientos de control para cada cuenta o tipo de transacción.

El alcance con que se deberán probar estos procedimientos de control, dependerá de factores como:

- La importancia del área en relación con los saldos de las cuentas presentadas en los EEFF.
- La importancia de los objetivos de control dentro del sistema contable.
- La importancia de un procedimiento de control en particular para el logro de un objetivo de control.

5. Procedimientos aplicables a la revisión de la vigilancia

Normalmente la evaluación de la vigilancia de las operaciones es documentada junto con la evaluación de los controles internos claves de la entidad.

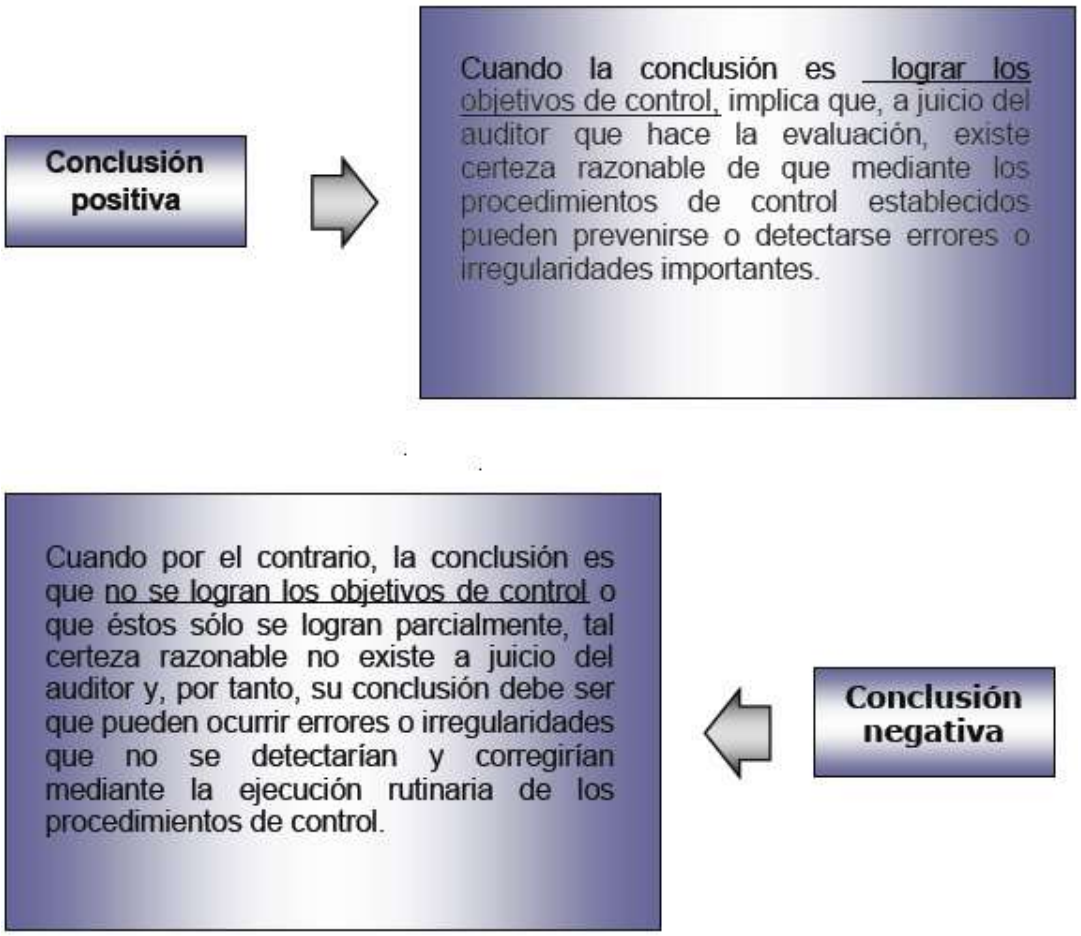
Por ejemplo, si los sistemas de la entidad emiten un listado de saldos contrarios de proveedores, y éstos son revisados por auditoría interna dentro de los dos meses siguientes, es probable que el auditor deba aplicar pruebas de auditoría para cerciorarse de que los saldos contrarios importantes, determinados al cierre del ejercicio, han sido analizados y en su caso, registrado las correcciones relativas dentro del ejercicio.

Por cada elemento evaluado, el auditor deberá documentar a través de cuestionarios, diagramas de flujo, o por medio de memorandos descriptivos, las investigaciones efectuadas.

Evaluación de la estructura del control interno

La evaluación de la estructura del control interno es una etapa clave del trabajo de auditoría, en la cual el juicio del auditor tiene un papel relevante, al decidir si su entendimiento del ambiente de control, del sistema contable, de los sistemas de comunicación, y de aquellos procedimientos de control identificados como fundamentales para el logro total o parcial de los objetivos de control, le permiten

prevenir o descubrir errores o irregularidades importantes que pueden afectar los EEFF de la entidad.



Resultados de la evaluación del control interno

Por ejemplo, un archivo maestro puede estar deficientemente controlado, lo que posibilitaría la emisión de facturas a precios no autorizados que distorsionarían tanto las ventas como los saldos de las cuentas por cobrar.

El grado en que se logra un objetivo de control en particular, depende de las respuestas a las siguientes preguntas básicas:

• ¿Qué podría salir mal?	• ¿Evitarían los procedimientos de control existentes, que esto sucediera?
• Si sucediera, ¿se descubriría en la ejecución normal de las actividades?	• Si así fuera ¿cuándo?
• Si no se descubriera el error o la irregularidad en forma oportuna,	• ¿Qué efecto tendría esto en los saldos que aparecen en los EEFF de la entidad?

Si al contestar las preguntas anteriores se concluye que podrían ocurrir errores o irregularidades que pueden afectar, en sentido relevante, los saldos de los EEFF de la entidad, será necesario contestar una pregunta más:

- ¿Qué pruebas sustantivas específicas deben diseñarse para determinar el efecto de los errores o irregularidades, si los hubiere, sobre los EEFF, y en su caso, registrar la corrección correspondiente?

Diseño de pruebas sustantivas

Una vez efectuada la evaluación del control interno, el auditor podrá diseñar en forma congruente con dicha evaluación las pruebas sustantivas que le permitan obtener la evidencia necesaria para emitir una opinión sobre los EEFF de la entidad.

Una **prueba sustantiva** está diseñada para llegar a una conclusión con respecto al saldo de una cuenta. Las pruebas sustantivas incluyen técnicas como: confirmaciones, observación física, cálculo, inspección, investigación, etcétera.

La **naturaleza** (tipo de prueba) y **alcance** (porcentaje de revisión) de las pruebas sustantivas dependen del tipo y volumen de errores que pudieran ocurrir en los procesos contables de la entidad y que no fueran detectados por los procedimientos de control interno establecidos en ella.

Por lo tanto, a menor cantidad de errores de importancia de control que pudiera ocurrir, menor será el alcance de las pruebas sustantivas, y a la inversa.

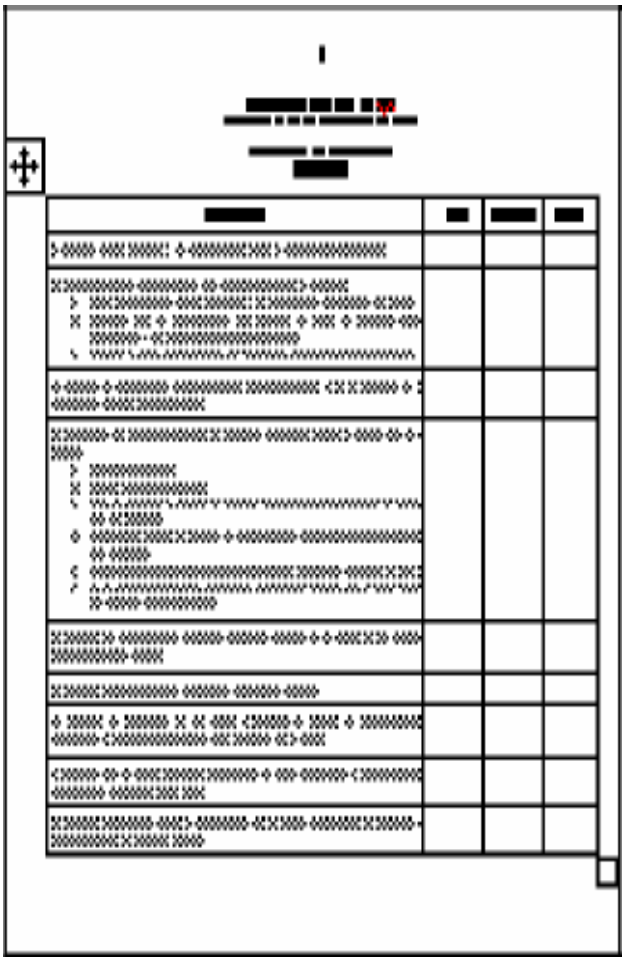
Programa de auditoría

Las pruebas de cumplimiento y las pruebas sustantivas,[11] que se diseñen como resultado de la evaluación del control interno, deben consignarse en el programa de auditoría.

El programa de auditoría es un documento preparado por el auditor, el cual contiene de manera lógica y ordenada la descripción de cada uno de los procedimientos de auditoría que se aplicarán[12] para la revisión de una operación o de una cuenta.

[11] Los programas de auditoría de pruebas sustantivas son la culminación del proceso de planeación y reflejan, por tanto, los juicios hechos por el auditor para realizar su revisión.
[12] Los procedimientos de auditoría se ejecutan en el orden en el cual se encuentran en el programa.

Además de la descripción de las pruebas, el programa de auditoría incluye columnas para que el personal que realice dichos procedimientos, plasme su nombre, la fecha de ejecución del procedimiento, el índice donde se puede encontrar el papel de trabajo en el cual realizó la prueba. Por ello constituyen una guía de ejecución y supervisión del trabajo.



Boletín 3070 Consideraciones sobre fraude que deben hacerse en una auditoría de EEFF

Los casos conocidos de fraude generan una demanda creciente de un mejor control interno. El fraude constituye una gran preocupación, tanto para la iniciativa privada como para las entidades gubernamentales, debido al impacto negativo en sus ingresos, en el bienestar general de la organización. Aun con los esfuerzos de los auditores, la mayoría de los fraudes pasan desapercibidos por la dificultad para identificarlos y corregirlos. La mayoría de los fraudes requieren conocimientos especializados, utilización de técnicas de investigación casi de detective y el

establecimiento de mecanismos destinados a la prevención de fraudes que no forman parte de las actividades usuales de auditoría.

Con el objetivo de que el Contador Público considere adecuadamente, dentro de su auditoría, el riesgo de fraude en los estados financieros a dictaminar, la CONPA emitió en 2004 el nuevo Boletín 3070 “Consideraciones sobre fraude que deben hacerse en una auditoría de estados financieros”.

Alcance

Este boletín es aplicable a las autoridades de EEFF que se realizan de acuerdo con las normas de auditoría y no se refieren a otros servicios solicitados al auditor, relativos a detección o prevención de fraudes.

Objetivo

Los objetivos de este boletín son:

a) describir y presentar las características de fraude,
b) establecer pronunciamientos normativos y
c) proporcionar guías sobre las consideraciones de fraude que debe contemplar el auditor al diseñar los procedimientos que aplicará en la auditoría de EEFF para cumplir con las normas.

A las **distorsiones provocadas** en el **registro de las operaciones** y en la **información financiera** o actos intencionales para **sustraer o malversación de activos** (robo), u **ocultar obligaciones** que tienen o pueden tener un impacto significativo en los estados financieros sujetos a examen.

Clasificación del fraude

Existen dos tipos de fraude de interés para auditoría:

1. Fraudes relacionados con la información financiera.
2. Fraudes provenientes del robo o la malversación de activos.

A continuación, se explican las características de cada uno de ellos.

1. Fraudes relacionados con información financiera

Son producidos por distorsiones, alteraciones o manipulaciones intencionales de las cifras presentadas o por omisiones en las cantidades o revelaciones de los EEFF y que causan que éstos no estén presentados, en todos sus aspectos importantes, de conformidad con las bases contables correspondientes.

La información financiera fraudulenta puede ser el resultado de:

- Manipulación, falsificación, distorsión o alteración de los documentos que soportan la información, los registros contables que son la base para la preparación de los EEFF.

• Alteración, distorsión u omisión intencional en las declaraciones de la administración en relación con los EEFFF, eventos, operaciones u otra información significativa.
• No aplicar o aplicar incorrectamente alguna o algunas bases contables que pueden tener efecto significativo en la adecuada clasificación, presentación y revelación de la información financiera, con el propósito de presentar una mejor situación financiera y resultados.

La intención de un acto es muy difícil de determinar, particularmente en asuntos relacionados con estimaciones contables y la aplicación de las Normas de Información Financiera.

Por ejemplo, la insuficiencia de una estimación contable puede ser un error o puede ser el resultado de un acto intencional para presentar mejores cifras en los EEFF.

Aun cuando una auditoría no está diseñada para determinar intenciones, **el auditor tiene la responsabilidad de planear y realizar su examen** para tener una seguridad razonable de que los EEFF están libres de errores, sean éstos intencionales o no.

2. Fraudes provenientes del robo de activos

El robo de activos puede realizarse de diferentes maneras: **alterar** la recepción de productos, **sustraer** activos o hacer que la entidad pague por productos o servicios que no se han recibido (**malversación**), etcétera.

El robo de activos suele estar acompañado de falsificación de documentos y/o de registros contables. Un deficiente control interno sobre los activos puede aumentar la susceptibilidad de que éstos sean sujetos a robo.

Los robos de activos pueden ocurrir debido, por ejemplo, a la presencia de alguna de las siguientes situaciones:

- Falta de segregación de funciones y/o revisiones independientes.
- Inadecuada supervisión por la administración de los empleados responsables de los activos; por ejemplo, de activos en sucursales foráneas.
- Inadecuada investigación de las solicitudes de empleo para puestos con acceso a activos.
- Registro contable inadecuado de los activos.
- Falta de sistemas de autorización y aprobación de operaciones; por ejemplo, de compras.
- Falta de documentación completa y oportuna de operaciones con activos; por ejemplo, notas de crédito de devoluciones de mercancía.
- Falta de vacaciones obligatorias para los empleados que realizan funciones claves de control o de custodia.
- Inadecuado entendimiento por la administración de tecnología de la información, lo que puede permitir a los empleados de esta área de la entidad cometer robos.
- Conducta indicativa de resentimiento o insatisfacción del personal con la entidad en general o con otros empleados.
- Cambios en la conducta o en el estilo de vida de empleados, probables indicadores de que han cometido robos de activos de la entidad.

Factores de riesgo de fraude

Normalmente ciertas condiciones están presentes cuando un fraude ocurre; a estas condiciones se les conoce como factores de riesgo de fraude.

Algunos de estos factores son:

- Presiones para lograr resultados.
- Establecimiento de incentivos sobre metas irreales o inalcanzables.
- Inexistencia, incumplimiento, o bien, ineficiencia de controles.

- Falta de valores éticos, lo cual, contribuye a que las personas acepten cometer actos deshonestos.

La administración tiene una excelente posición para perpetrar fraudes debido a que, con frecuencia, está en posición de manipular directa o indirectamente los registros contables y presentar información financiera fraudulenta.

Normalmente, cuando se presenta información financiera fraudulenta, la administración ha violado los controles, los cuales aparentan estar funcionado en forma efectiva. La administración puede pedir a sus empleados que perpetren el fraude o que le ayuden a realizarlo. La forma en que la administración puede violar los controles puede ocurrir de maneras impredecibles.

Típicamente, la administración y los empleados involucrados en un fraude harán los pasos necesarios para ocultarlo a los auditores y a otros, dentro o fuera de la entidad. El fraude puede ser ocultado al retener evidencia, hacer declaraciones falsas o falsificar documentación.

Por ejemplo, al alterar los reportes de embarque, los empleados o miembros de la administración que han robado efectivo tratarán de ocultarlo falsificando firmas o aprobaciones electrónicas en las autorizaciones de desembolsos.

Una auditoría conducida de acuerdo con **normas**, rara vez involucra la autentificación de estas evidencias debido a que los auditores no están entrenados o no se espera que sean expertos en autentificar firmas o documentos. Adicionalmente, un auditor quizá no descubrirá la existencia o modificación de un documento que se da a través de un arreglo entre la administración y terceras personas involucradas.

El fraude puede ocultarse, a través de la colusión entre la administración, empleados o terceras partes. Esa colusión puede causar que, con base en la evidencia examinada y en la falsedad de esa realidad, el auditor concluya que una operación es adecuada.

Por ejemplo, a través de la colusión, se puede entregar al auditor evidencia falsa de que los controles internos de la compañía están funcionado adecuadamente, o varios individuos pueden explicar consistentemente, sobre resultados inesperados en un procedimiento analítico, o el auditor puede recibir confirmaciones falsas de terceras partes que están en colusión con la administración.

Aún cuando los fraudes usualmente se ocultan y la intención de la administración sobre ciertas operaciones es difícil de fijar, la presencia de determinadas condiciones puede sugerir al auditor la posibilidad de un fraude.

Por ejemplo, la utilización de documentación apócrifa para soportar erogaciones, la falta de estados de cuenta referentes a cuentas de cheques o a inversiones, la ausencia de respuesta o la recepción de copias de respuestas a solicitudes de confirmación enviadas por el auditor en lugar de los originales firmados por quien corresponde, la desaparición de un contrato importante, entre otros. Sin embargo, debe tenerse presente que estas circunstancias pueden resultar de situaciones diferentes a fraude.

Evaluación de riesgo de fraude

“La auditoría de EEFFF no tiene por objetivo el descubrir errores o irregularidades” (Boletín 1020); sin embargo, la responsabilidad del auditor se da cuando dichos errores o irregularidades no se descubrieron por el hecho de no haber cumplido con las normas de auditoría (véase, Hernández, 2004).

De acuerdo con este boletín es necesario que, al hacer auditoría de EEFFF, se considere si existen factores de riesgo de fraude y se evalúe el riesgo de afirmaciones

equivocas contenidas en los EEFFF, con la finalidad de que se diseñen las pruebas de auditoría.

Como se muestra en el diagrama, la evaluación de riesgo de fraude se puede realizar en cuatro etapas:

I. Planeación

En la etapa de planeación, el auditor, con su juicio profesional, debe determinar con qué personal de equipo, y otros especialistas, mantendrá constante comunicación, el intercambio de ideas sobre cómo y dónde considera que la información financiera es susceptible a errores o alteraciones importantes causadas por fraude.

Es importante hacer énfasis en mantener siempre en mente durante todo el trabajo, la posibilidad de la existencia de errores o alteraciones significativas.

La discusión en la etapa de planeación debe documentarse e incluir cómo y cuándo se realizó dicha discusión, los miembros del equipo que participaron y los asuntos discutidos.

II. Procedimientos aplicados

El auditor debe asentar, en sus papeles de trabajo, los procedimientos aplicados para obtener la información necesaria para identificar y evaluar los riesgos de distorsiones significativas en los EEFF debido a fraude.

Cuando el auditor reúna la información que le permita conocer la operación de la entidad debe aplicar procedimientos como preguntas a la administración sobre cómo consideran el riesgo de fraude en la entidad, la forma en que se informa al consejo de administración, al comité de auditoría, al comisario y a otros.

Además, el auditor debe utilizar su juicio profesional para determinar con quién se debe hacer estas indagaciones y la extensión de las mismas.

III. Riesgos de fraude

Deben documentarse los riesgos específicos de distorsiones significativas en los EEFF debido a fraude y que fueron identificados, y una descripción de la respuesta del auditor a esos riesgos.

Cuando el auditor concluya la evaluación de los riesgos de fraude, en respuesta y con escepticismo profesional, debe proceder a obtener y evaluar la evidencia de la auditoría, aplicando por ejemplo: procedimientos adicionales o diferentes.

Cuando los resultados de las pruebas de auditoría identifiquen distorsiones en los EEFF, el auditor debe considerar si esas distorsiones son o no indicativas de fraude; además, si el efecto de ellas en los EEFF no es significativo, el auditor debe evaluar las implicaciones.

Si el efecto es significativo o no es posible evaluarlo, el auditor debe:

- Obtener evidencia adicional.
- Considerar las implicaciones en otros aspectos de la auditoría.
- Discutir el asunto y el enfoque de la investigación posterior con personal de un nivel apropiado de la administración, también puede ser directamente con el consejo de administración, el comité de auditoría o un órgano semejante.
- Sugerir que el cliente consulte con sus asesores legales.

IV. Comunicaciones

Finalmente, el auditor debe evidenciar la naturaleza de las comunicaciones acerca de fraude hechas a la administración.

Cuando un fraude involucra a la alta administración, la comunicación debe hacerse directamente, como ya se mencionó con anterioridad, con el consejo de administración, el comité de auditoría o con algún órgano semejante.

La revelación de posibles fraudes, a otras partes distintas a las ya descritas, no es responsabilidad del auditor, excepto si se trata de cumplimiento a requerimientos contractuales y legales, o en respuesta a un citatorio judicial.

Boletín 3140 Efectos de la Tecnología de Información (TI) en el desarrollo de una auditoría de EEFF

Alcance

Este boletín se refiere al impacto de la TI en una auditoría de EEFF, es obligatorio para auditorías de EEFF de ejercicios que inicien el 1 de enero de 2006 y sustituya al Boletín 5080 “Efectos del procesamiento electrónico de datos en el examen del control interno”.

Este boletín trata sólo del efecto en la auditoría que tiene un ambiente de TI y al EyECI de la TI llevado a cabo por el auditor, para determinar la naturaleza, extensión y oportunidad que dará a sus procedimientos de auditoría.

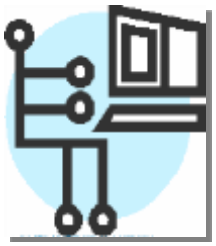
Concepto

Como se ha visto, el Boletín 3050 menciona que el auditor debe conocer, evaluar, y en su caso, probar los sistemas de TI como fundamento del EyECI, documentar adecuadamente sus conclusiones sobre su efecto en la información financiera.

El EyECI incluye el análisis y la comprensión de los métodos utilizados para procesar la información financiera, con objeto de determinar si las técnicas establecidas cumplen con los objetivos de control interno; por lo tanto cuando la TT forma parte del control interno contable (ambiente de TI) y de éste se deriva información sujeta a examen, el auditor debe realizar su estudio y como resultado de dicho trabajo, deberá documentar sus conclusiones sobre el efecto de la TI en sus pruebas de auditoría, ya que la utilización de la TI en las aplicaciones contables de importancia, puede influir en la naturaleza, extensión y oportunidad de los procesamientos de auditoría a realizar.

En auditoría se considera que existe un ambiente de TI en el control interno contable cuando está involucrada una computadora de cualquier tipo o tamaño en actividades que pudieran afectar la confiabilidad de la información financiera de importancia para

la auditoría, tales como el inicio, autorización, registro, procesamiento y reporte de las operaciones importantes, así como la prevención o detección de fraude, incluyendo la segregación de funciones, ya sea que dicha computadora esté operada por la entidad o por terceros.



Un ambiente de TI puede afectar:

- Los procedimientos del auditor para comprender los sistemas de contabilidad y de control interno.
- La evaluación del riesgo específico del negocio.
- El diseño, desarrollo de pruebas de control y de procedimientos sustantivos adecuados para cumplir con el objetivo de la auditoría y el tipo de evidencia que deberá reunirse para lograr conclusiones.
- La decisión de apoyarse en especialistas.

La TI por su complejidad, su constante evolución, requiere de personal con entrenamiento técnico y capacidad profesional adecuados. El auditor debe considerar si se necesitan habilidades especializadas en TI en una auditoría para obtener una comprensión suficiente de los sistemas de contabilidad y del control interno relacionado, para determinar el efecto del ambiente de TI sobre la evaluación del riesgo general, riesgo a nivel de cuenta, de clase de operaciones, para diseñar, realizar pruebas de control y procedimientos sustantivos adecuados.

Pronunciamientos normativos

Al realizar la evaluación un ambiente de TI en una auditoría de EEFF, el auditor deberá:

- Adquirir entendimiento de los sistemas de información financiera y de control interno que le permita planear la auditoría y elaborar un enfoque de auditoría eficiente.
- Tener suficiente conocimiento de TI para planear, dirigir, supervisar y revisar el trabajo realizado.
- Considerar si se requieren habilidades o aptitudes especializadas de TI en una auditoría, y en su caso apoyarse de un especialista.
- Entender el ambiente de TI, su influencia en la evaluación de riesgos inherentes y de control (véase, Boletín 3030), así como en las consideraciones que deben realizarse sobre aspectos de fraude (véase, Boletín 3070)
- Hacer una evaluación de los riesgos implícitos a las aseveraciones importantes de los EEFF.
- Considerar el ambiente el ambiente de TI al diseñar los procedimientos de auditoría.
- Adquirir conocimiento del sistema de TI relacionado con los reportes de información financiera, incluyendo el uso de programas de recuperación y análisis de datos.

La TI puede generar riesgos específicos en el control interno de una entidad, de los que el auditor debe de estar consciente. Entre estos riesgos se incluyen:

- Dependencia de programas que procesen información correcta en forma incorrecta o que procesen incorrectamente información correcta.
- Acceso no autorizado a información que podría resultar en destrucción, modificaciones indebidas de información, incluyendo el registro de operaciones no autorizadas, inexistentes o registro inexacto de operaciones.

- Modificaciones no autorizadas de información en los archivos maestros, de operaciones, a sistemas, programas, o bien dejar de efectuar modificaciones necesarias a sistemas o programas.
- Nuevas tecnologías con mayor grado de complejidad.

Para el diseño de sus procedimientos de auditoría, considerando el ambiente de TI, el auditor deberá:

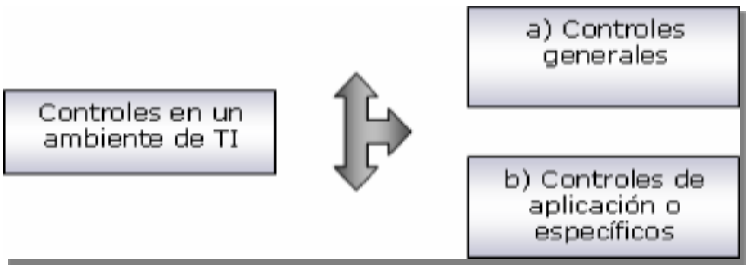
- Conocer y documentar los controles generales.
- Evaluar si dichos controles cumplen con estándares aceptables.
- Seleccionar los controles generales clave.
- Probar los controles clave.
- Concluir del efecto de las debilidades de control identificadas, si las hay.

Controles en un ambiente de TI

Los controles sobre el procesamiento por computadora, que ayudan a lograr los objetivos del control interno, incluyen tanto procedimientos manuales como procedimientos integrados en programas de computadora. Dichos procedimientos comprenden los controles que afectan al entorno de TI (controles de aplicación TI).

Estos controles deben cumplir, como ya ha visto, con cinco objetivos que son: autorización, procesamiento, salvaguarda, verificación, evaluación y segregación de funciones. Para que el control interno funcione en una empresa determinada, es necesario que su estructura organizacional esté diseñada para que los responsables del establecimiento de los procedimientos de control y de su supervisión, tengan la autoridad para cumplir con esos objetivos.

Los controles que intervienen en un ambiente de TI se dividen en:



a) Controles Generales

Son los controles y procedimientos que proveen un soporte para asegurar que los sistemas de aplicación procesan operaciones confiablemente; éstos se pueden aplicar a uno más sistemas y ambientes de procesamiento.

El propósito de los controles generales es establecer un marco de referencia de control global sobre las actividades de TI y proporcionar un nivel **razonable**[13] de seguridad para lograr los objetivos generales de control interno (i.e. efectividad y eficiencia operacional, seguridad en la información financiera y cumplimiento de leyes).

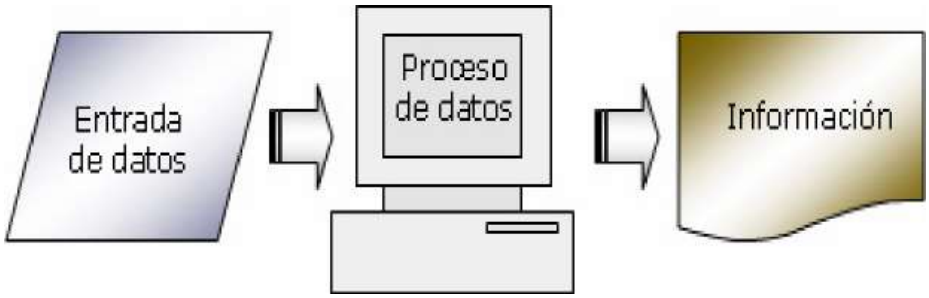
Algunos ejemplos de controles generales de TI pueden ser:

• Controles de seguridad física y ambiental. Relativos al acondicionamiento físico y medidas de seguridad en el área donde se localiza el equipo de cómputo.
• Controles de organización y administración. Diseñados para establecer un marco de referencia organizacional sobre las actividades de TI, por ejemplo: segregación de funciones incompatibles y la capacitación del personal.
• Desarrollo de sistemas y controles de mantenimiento. Diseñados para establecer control sobre: cambios a sistemas, acceso de documentación de sistemas, adquisición de sistemas de aplicación de terceros, entre otros.
• Controles de operación de computadoras y seguridad. Están diseñados para controlar que los sistemas sean usados para propósitos autorizados, el acceso a las operaciones de la computadora es restringido a personal autorizado, sólo se usan programas autorizados y los errores de procesamiento son detectados y corregidos.
• Controles de software de sistemas. Controles diseñados para proporcionar certeza razonable de que el software del sistema (sistema operativo) se adquiere o desarrolla de manera autorizada.
• Controles de entrada de datos. Diseñados para controlar el acceso de datos que alimentan al sistema, el acceso a datos y programas debe estar restringido a personal autorizado.
• Controles de emergencia. Diseñados para la anticipación o solución de problemas con el equipo o los sistemas. Por ejemplo: respaldo de datos, procedimientos de recuperación para usarse en caso de robo, pérdida o destrucción intencional o accidental, etcétera.

b) Controles de aplicación o específicos

Se refieren a los establecidos en la operación del computador que incluye entrada, proceso y salida de datos, es decir, que todos los datos se procesan una sola vez (entrada), sujetos a un proceso de validación (proceso) y que sean la base para producir información confiable y completa (salida).

[13] El término “razonable” es sinónimo de medianamente y se utiliza debido a que no existe la seguridad total de que los controles funcionen o bien de que las personas los apliquen correctamente, siempre existirá el riesgo de errores, descuidos, malos entendidos, etcétera.



El propósito de los controles de aplicación de TI es establecer procedimientos específicos de control sobre las aplicaciones contables para proporcionar seguridad **razonable** de que todas las operaciones están autorizadas, registradas y procesadas completamente, con exactitud y con oportunidad.

Algunos controles de aplicación de TI incluyen:

• Controles sobre los datos de entrada. Están diseñados para proporcionar una seguridad razonable de que las operaciones son autorizadas en forma apropiada antes de ser procesadas por la computadora y las operaciones incorrectas son rechazadas, corregidas, y si es necesario, procesadas nuevamente con oportunidad.
• Controles sobre el procesamiento y sobre los archivos de datos de la computadora. Diseñados para proporcionar certeza razonable de que las operaciones, son procesadas en forma apropiada por la computadora, no están pérdidas, añadidas, duplicadas o cambiadas en forma no apropiada y los errores de procesamiento son identificados y corregidos oportunamente.
• Los controles sobre los datos de salida. Diseñados para proporcionar certeza razonable de que los resultados del procesamiento son exactos, el acceso a los datos de salida está restringido a personal autorizado y los datos de salida se proporcionan al personal autorizado apropiado oportunamente.
• Controles sobre restricciones.- Diseñados para que personas no autorizadas no puedan crear, modificar o borrar información de los archivos de datos o ingresar sin autorización operaciones para su procesamiento.

Revisión de controles de TI

El auditor deberá considerar cómo afectan los controles generales a las aplicaciones de TI importantes para la auditoría.

El control sobre los datos de entrada, procesamiento, archivos de datos y datos de salida puede desempeñarse por personal de TI, por usuarios del sistema, por un grupo de control separado o puede ser programado en el *software* de aplicación.

Los controles de aplicación de TI que el auditor debe probar incluyen: los controles manuales ejercidos por el usuario, los controles sobre los datos de salida del sistema y los procedimientos de control programados.

Evaluación

Los controles generales de TI pueden tener un efecto importante en el procesamiento de operaciones en los sistemas de aplicación. Si estos controles no son efectivos, puede haber un riesgo de que pudieran ocurrir **aseveraciones erróneas y no ser detectadas en los sistemas de aplicación**. Así, las debilidades en los controles generales de TI pueden imposibilitar la prueba de algunos controles de aplicación de TI; sin embargo, los procedimientos manuales ejercidos por los usuarios pueden proporcionar control efectivo al nivel de aplicación. (Cuéllar, Evaluación del riesgo y control interno)

TI en entidades pequeñas y medianas

Los sistemas de información en organizaciones pequeñas o medianas son probablemente menos formales que en las organizaciones de mayor tamaño, pero su función es igualmente importante.

Las entidades pequeñas con participación activa por parte de la administración pueden prescindir de descripciones extensas de los procedimientos contables, registros contables sofisticados, o políticas por escrito. La comunicación puede ser menos formal y más fácil de lograr en una compañía pequeña o mediana. La comunicación implica permitir la comprensión de las funciones y responsabilidades individuales correspondientes al control interno sobre reporte de información financiera.

El auditor debe adquirir suficiente conocimiento del sistema de información relacionada con reporte de información financiera a fin de entender:

- Las operaciones de importancia para los estados financieros.
- Los procedimientos, tanto automatizados como manuales, mediante los cuales se inicien, registren, procesen, y reporten desde que tiene lugar hasta su inclusión en los EEFF.
- Los registros contables correspondientes, ya sean electrónicos o manuales, que sustenten la información, así como cuentas específicas de los EEFF implicadas en el inicio, registro, procesamiento y reporte de operaciones.

- El proceso de reporte de información financiera empleado para la preparación de los EEFF de la entidad, que incluye estimaciones contables y revelaciones importantes.

Cuando se utiliza TI a fin de iniciar, registrar, procesar, o reportar operaciones y otra información financiera para su inclusión en los EEFF, es posible que los sistemas así como programas incluyan controles relacionados con las aseveraciones correspondientes de cuentas importantes o puedan ser determinantes para el funcionamiento eficiente de los controles que dependan de TI.

4.1.2. Guías de Auditoría

Guía 6080 Ayuda a prevenir, disuadir y detectar el fraude [vista previa]

Introducción

Toda entidad está expuesta al fraude, tradicionalmente enfocado a la sustracción de activos o malversación de los mismos. Sin embargo, a últimas fechas ha llamado la atención como tema novedoso, el fraude en la información financiera.

Este último, ha adquirido importancia por la gran cantidad de casos presentados en empresas públicas. Lo anterior, ha provocado que se revisen los aspectos de control y que sea necesario revisar los factores incidentes en el fraude, y con ello recomendar los programas para mitigarlo.

Este documento proporciona a las entidades una guía sobre los temas que inciden en el fraude y las medidas que pueden tomar para prevenir, disuadir y/o detectar el fraude en cualquiera de sus modalidades, incluso el relativo al fraude financiero.

Alcance

Esta guía fue emitida en 2004 como respuesta a las preocupaciones que han manifestado las autoridades, los usuarios de la información financiera y el público en general en relación con el tema de fraude.

El boletín 3070, ya antes analizado, se refiere a las consideraciones sobre fraude que deben hacerse al realizar una auditoría de EEFF, esta guía incluye medidas que al ser implementadas en cualquier empresa ayudan a prevenir, disuadir y detectar el fraude.

Responsabilidad de la administración

Las administraciones de las entidades son las responsables del diseño, implantación de sistemas, procedimientos para la prevención, detección del fraude que junto con el consejo de administración u otro órgano de vigilancia; deben asegurar una cultura y un entorno que fomenten la honradez así como la conducta ética. Sin embargo, debido a las características del fraude, pueden ocurrir distorsiones importantes en los EEFF, a pesar de la presencia de programas y controles como los que se describen en este documento.

El fraude varia, va desde los robos de menor cuantía por parte de los empleados y comportamiento improductivo, hasta la malversación de activos y el fraude a través de emisión de EEFF fraudulentos.

El fraude en los EEFFF puede provocar un efecto adverso, significativo en el valor de mercado de la entidad, en su reputación y en su habilidad para lograr objetivos estratégicos.

Un número de casos altamente publicitados han intensificado el conocimiento de los efectos de la emisión de EEFF fraudulentos, y ha inducido a muchas organizaciones a ser más pro-activas en la aplicación de medidas para prevenir o disuadir su ocurrencia.

La malversación de activos aunque con frecuencia no afecta de manera importante las cifras incluidas en los EEFF, de algún modo puede resultar en pérdidas substanciales si un empleado deshonesto tiene el incentivo y la oportunidad para cometer un fraude.

El riesgo de fraude puede ser reducido por medio de una combinación de medidas y acciones de prevención, disuasión y detección. Sin embargo, el fraude puede ser difícil de detectar porque con frecuencia involucra un encubrimiento a través de la falsificación de documentos o la colusión entre la administración, los empleados, terceras personas o entidades.

Por lo tanto, es importante enfatizar la importancia de la prevención del fraude que podría reducir las oportunidades para cometerlo; y la disuasión, que podría convencer a los individuos para no cometer fraude, debido a la probabilidad de detección y su castigo. Aunque, las medidas de prevención y disuasión son mucho menos costosas que el tiempo y el gasto requeridos para la detección e investigación del fraude.

La administración tiene la **responsabilidad** así como los medios para **implantar medidas para reducir la incidencia del fraude**. Las disposiciones tomadas por una entidad para **prevenir y disuadir** el fraude también pueden ayudar a crear un ambiente positivo en el lugar de trabajo que mejore la habilidad de la entidad para reclutar y retener empleados honestos de alta calidad.

Medidas para prevenir, disuadir y detectar el fraude. Las siguientes son algunas las medidas que la entidad puede implementar para prevenir, disuadir y detectar el fraude.

Crear y mantener una cultura de honestidad y alta ética. Es responsabilidad de la entidad crear una cultura de honestidad y alta ética; comunicar con claridad a cada

empleado lo que es una conducta aceptable, así como las expectativas que se tienen de él. Crear una cultura de honestidad y alta ética incluye:

El **establecimiento del buen ejemplo en los altos niveles de la entidad**. Los directores y funcionarios dentro de la entidad son los que establecen el ejemplo para el comportamiento ético. Investigaciones sobre el desarrollo moral sugieren fuertemente que la honestidad tiene mejor arraigo donde se establece el buen ejemplo. La alta gerencia de una entidad no puede actuar de una manera y esperar que otros dentro de ella actúen de manera diferente.

La alta gerencia debe demostrar a los empleados, a través de hechos y acciones, que el comportamiento deshonesto o poco ético no será tolerado, aun cuando el resultado de la acción beneficie a la entidad. Es más, debe quedar claro que todos los empleados recibirán igual tratamiento, sin importar sus puestos.

Por ejemplo, declaraciones de la administración respecto a la imperante necesidad de cumplir con los objetivos operativos y financieros pueden causar presiones excesivas que lleven a los empleados a cometer fraude para lograrlos.

Establecer metas inalcanzables para empleados les podrá presentar dos alternativas desagradables: fallar o engañar.

En contraste, una declaración de la administración que establezca: “Somos agresivos en nuestra manera de alcanzar nuestros objetivos, pero requerimos emitir información financiera veraz en todo momento,” les indica a los empleados, que la integridad es un requisito. Un mensaje en este sentido, también lleva implícito que la entidad tiene “tolerancia cero” hacia el comportamiento poco ético, incluida la emisión de información financiera fraudulenta.

La piedra angular de un entorno efectivo anti-fraude es una cultura con un sólido sistema de valores, fundamentado en la integridad. Tal sistema de valores se refleja con frecuencia en un código de ética o de conducta (los códigos). Estos **códigos** reflejan los valores fundamentales de la entidad y proporcionan guía a los empleados en las decisiones que toman durante su día de trabajo.

Los códigos pueden incluir temas como la ética, la confidencialidad, conflictos de intereses, propiedad intelectual y fraude. Para que los códigos sean efectivos, éstos deben ser comunicados a todo el personal en una forma entendible.

Creación de un ambiente positivo de trabajo

Las malversaciones ocurren con menos frecuencia cuando los empleados tienen sentimientos positivos respecto a la entidad, que cuando se sienten abusados, amenazados o ignorados.

Sin un entorno positivo en el lugar de trabajo, hay más posibilidad de baja moral entre los empleados, situación que puede afectar la actitud del empleado respecto a la comisión de un fraude contra la entidad.

La falta de interés de la administración por sus empleados, entrenamiento deficiente o pocas oportunidades de promoción, son factores que disminuyen el entorno positivo de trabajo y que pueden aumentar el riesgo de fraude.

A los empleados se les debe:

- Dar la oportunidad para aportar ideas en el desarrollo y actualización de los códigos de ética y conducta de la entidad.
- Proporcionar los medios para obtener consejo dentro de la entidad, antes de que tomen decisiones que podrían tener implicaciones legales o éticas significativas.

- Alentar a que comuniquen sus inquietudes y que se le den los medios para comunicarlas (de manera anónima si lo prefieren), respecto a potenciales violaciones al Código de Ética de la entidad, sin temor a amenazas o castigos.

Por ejemplo, algunas compañías usan un buzón que está dirigido a un funcionario responsable, un auditor interno o algún otro funcionario de confianza responsable de investigar y reportar incidentes de fraude o actos ilegales.

Contratar y promover empleados apropiados

Cada empleado tiene un conjunto único de valores y código propio de ética. Cuando enfrentan demasiada presión y una oportunidad de fraude es percibida, algunos empleados se comportarán en forma deshonesta en lugar de evitar sufrir las consecuencias negativas de un comportamiento deshonesto.

Para que una entidad tenga éxito en la prevención del fraude, debe tener políticas efectivas que minimicen la posibilidad de contratar o promover personas con bajos niveles de honestidad, especialmente en puestos de confianza.

Algunos **procedimientos pro activos** de contratación y promoción pueden ser:

- Realizar investigaciones sobre los antecedentes de individuos que están bajo la posibilidad para su contratación o promoción a un puesto de confianza.
- Verificar los datos de escolaridad, puestos anteriores y referencias personales de los candidatos.
- Entrenar periódicamente a todos los empleados sobre los valores, los códigos de ética y conducta de la entidad.
- Realizar revisiones periódicas de desempeño.

Entrenamiento

Los empleados de nuevo ingreso deben recibir entrenamiento en el momento de su contratación, sobre los valores, los códigos de ética y conducta de la entidad. Dicho entrenamiento debe cubrir en forma explícita, las expectativas para todos los empleados respecto a:

- Su obligación de reportar ciertos asuntos.
- Una lista del tipo de asuntos, incluyendo el fraude real o bajo sospecha, que deben ser comunicados junto con ejemplos específicos.
- Información sobre la manera de reportar tales asuntos.

Los empleados deben recibir periódicamente cursos de repaso; debe ser específico para el nivel del empleado dentro de la entidad, ubicación geográfica y responsabilidades asignadas.

Confirmación anual de adherencia al código de ética o de conducta

La administración debe establecer con toda claridad que todo empleado será responsable de actuar dentro de los códigos de ética o de conducta de la entidad.

Todos los empleados de nivel gerencial y de funciones financieras, así como otros empleados en áreas que pueden estar expuestos al comportamiento poco ético (por ejemplo, compras, ventas y comercialización), deben firmar una declaración de adherencia al Código de Ética y de Conducta por lo menos una vez al año.

Disciplina

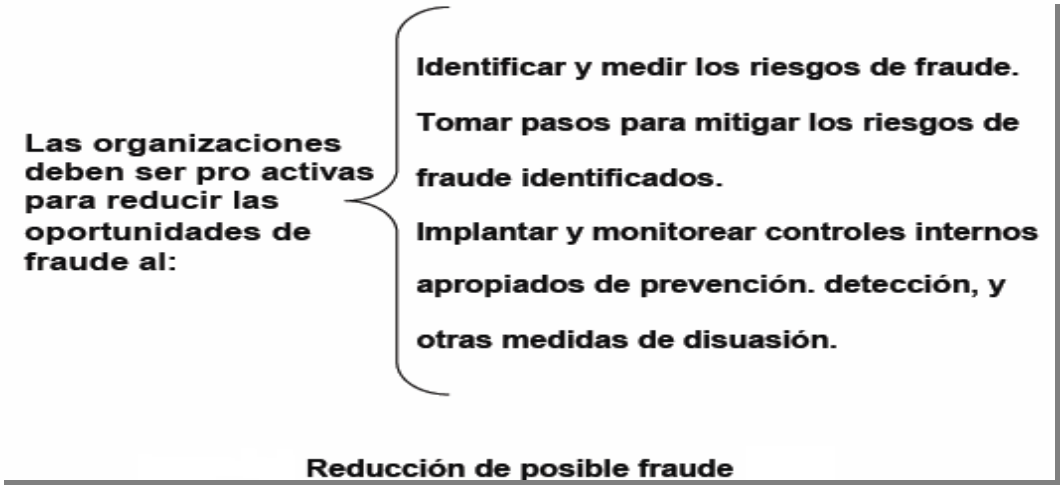
La manera en que la entidad reacciona ante incidentes de sospecha de fraude puede mandar un fuerte mensaje a toda la entidad, ayudando así a reducir el número de ocurrencias en el futuro. Las siguientes acciones se deben tomar en respuesta a un incidente de fraude:

- Una investigación a fondo del incidente.
- Acciones apropiadas y consistentes en contra de los perpetradores.
- Los controles relevantes deben ser evaluados y mejorados.
- Un renovado esfuerzo de comunicación y entrenamiento para reforzar los valores, los códigos de ética y conducta y las expectativas de la entidad.

Las expectativas respecto a las consecuencias de cometer un fraude deben ser comunicadas con claridad a toda la entidad.

Por ejemplo, una declaración por parte de la administración en el sentido de que acciones deshonestas no serán toleradas, los violadores deberán ser despedidos y referidos a las autoridades competentes, establece claramente las consecuencias; puede servir de freno valioso para cualquier malversación.

Evaluación de los procesos y controles en contra del fraude



Reportes financieros fraudulentos ni malversaciones de activos pueden ocurrir sin que se perciba la oportunidad para cometer y encubrir el hecho.

Identificación y medición de los riesgos de fraude

Al identificar los riesgos de fraude, la entidad debe considerar las características organizacionales de la industria y las específicas del país que ejercen influencia sobre el riesgo de fraude. La naturaleza y amplitud de las actividades de evaluación del riesgo de fraude de la administración deben ir de acuerdo con el tamaño de la entidad y la complejidad de sus operaciones.

La administración debe desarrollar una elevada “conciencia de fraude” y un programa adecuado de administración de riesgo del mismo, con supervisión del consejo de administración, del comité de auditoría u órgano similar.

Mitigar los riesgos de fraude

Será posible reducir o eliminar riesgos de fraude al hacer cambios en las actividades y procedimientos de la entidad. Por ejemplo, el riesgo de malversación de fondos puede ser reducido si se implanta un sistema de centralización de fondos para recibir pagos en un solo banco, en lugar de recibir dinero en todas las ubicaciones de la entidad.

El riesgo de corrupción puede reducirse si se monitorean de cerca los procesos de compra.

El riesgo de fraude en los EEFF puede reducirse al implementar el uso de centros de servicios compartidos que proporcionen servicios contables a varios segmentos, afiliadas o a determinadas localidades geográficas de las operaciones de la entidad. Un centro de servicios compartidos puede ser menos vulnerable a la influencia del gerente local de operaciones y es posible que se implanten medidas más extensas de detección de fraude con mayor efectividad.

Implantar y supervisar controles internos apropiados

Algunos riesgos son inherentes al entorno de la entidad, pero la mayoría puede ser enfrentada con un sistema adecuado de control interno.

Una vez hecha la valoración del riesgo de fraude, la entidad puede identificar los procesos, controles y otros procedimientos necesarios para mitigar los riesgos identificados.

Un control interno efectivo incluirá un entorno de control interno adecuadamente desarrollado, un sistema de información efectivo y seguro y actividades de control y supervisión apropiadas.

Dada la importancia de la tecnología de la información en el soporte de las operaciones y en el procesamiento de operaciones, la administración necesita implementar y mantener controles apropiados, ya sean automatizados o manuales, sobre la información generada por los sistemas.

En especial, la administración debe evaluar si se han establecido los controles internos apropiados, en las áreas identificadas por la administración como de riesgo de actividad fraudulenta, así como el establecimiento de controles sobre el proceso de emisión de información financiera. Debido a que el proceso de emisión de información financiera fraudulento puede iniciar en un periodo intermedio, la administración debe evaluar lo apropiado de los controles internos sobre reportes financieros intermedios.

El emitir información financiera fraudulenta a los altos niveles de la administración, involucra la violación de los controles internos dentro del proceso de emisión de información financiera.

En vista de que la alta gerencia tiene la capacidad de anular los controles, de influir a otros a perpetrar o encubrir un fraude, la necesidad de un fuerte sistema de valores y

una cultura ética de emisión de información financiera se hace cada vez más importante.

Lo anterior, ayuda de crear un entorno en el que otros empleados no aceptarán participar en la comisión de un fraude y usarán los procedimientos establecidos para reportar cualquier invitación a cometer un ilícito.

La posibilidad de violación de los controles por parte de la alta gerencia también aumenta la necesidad de establecer medidas apropiadas de supervisión por parte del consejo de administración, del comité de auditoría u órgano de vigilancia semejante.

La emisión de información financiera fraudulenta a niveles inferiores de la administración o de empleados, puede ser frenado, disuadido o detectado por medio de controles apropiados de monitoreo, como requerir que gerentes del más alto nivel supervisen y evalúen los resultados financieros reportados por unidades individuales de operación o subsidiarias. Fluctuaciones inusuales en los resultados de unidades de operación y/o subsidiarias, desviaciones significativas respecto a las fluctuaciones esperadas, podrán indicar alguna manipulación potencial por los gerentes, el personal de unidades departamentales o de operación.

Desarrollo de un proceso apropiado de supervisión

Para prevenir o detectar el fraude, la entidad debe tener implantada una función apropiada de supervisión. La supervisión puede ser de variadas formas, realizada por muchos dentro y fuera de la entidad, bajo la vigilancia global del comité de auditoría u otro órgano de vigilancia semejante.

Algunos de los elementos internos y externos que intervienen en el proceso de supervisión son:

Elementos externos de supervisión

Consejo de administración, comité de auditoría u órgano de vigilancia semejante

El comité de auditoría u órgano de vigilancia tiene la responsabilidad de supervisar las actividades de la administración y de considerar el riesgo de emisión de información financiera fraudulenta que involucra la anulación de controles internos o la colusión.

También debe evaluar la implantación de medidas anti-fraude y la creación de un buen ejemplo. Una supervisión activa por el comité de auditoría puede ayudar a reforzar el compromiso de la administración de crear una cultura de “cero tolerancia” al fraude.

El comité de auditoría de la entidad también debe asegurar que la alta gerencia (en especial el director general) implante medidas adecuadas de **disuasión y prevención** que protejan a los inversionistas, empleados y demás colaboradores.

El comité de auditoría desempeña un importante papel al ayudar al consejo de administración a cumplir sus funciones de supervisión respecto al proceso de emisión de información financiera de la entidad y al sistema de control interno.

El comité de auditoría podrá revisar la razonabilidad de la información reportada por la entidad, comparándola con resultados anteriores, pronosticados, con empresas similares o promedios de la industria. Además, la información recibida en comunicaciones de auditores externos puede ayudar al comité de auditoría en su evaluación del control interno de la entidad y para determinar el riesgo potencial de emisión de información financiera fraudulenta.

Como parte de su responsabilidad de supervisión, el comité de auditoría debe alentar a la alta gerencia a proporcionar un mecanismo por medio del cual se puedan **reportar inquietudes** respecto a conducta poco ética, fraude real o bajo sospecha, o violaciones al código de ética y/o conducta, o a la política de ética de la entidad.

Si la alta gerencia está involucrada en un fraude, es probable que los niveles inferiores de la administración estén conscientes de ello; por lo tanto, el consejo de administración, el comité de auditoría o el órgano de vigilancia, deben considerar el establecimiento de una línea abierta de comunicación con miembros de la administración a uno o dos niveles por debajo de la dirección general, para que comuniquen el fraude o la sola sospecha al consejo de administración u órgano de vigilancia.

El comisario

De acuerdo con la Ley General de Sociedades Mercantiles, es la figura responsable de la vigilancia de las sociedades. Su función principal es realizar un examen periódico de las operaciones, documentación, registros y demás evidencias comprobatorias, en el grado y extensión necesarios, con el propósito de efectuar la vigilancia de las operaciones que la ley les impone, para así rendir su dictamen anual a la Asamblea General Ordinaria de Accionistas, respecto de la veracidad, suficiencia y razonabilidad de la información presentada por el consejo de administración o administrador general único a la asamblea de accionistas para su aprobación.

La información financiera sobre la cual el (los) comisario(s) debe afirmar que es veraz ante la asamblea de accionistas, conlleva una alta responsabilidad que requiere un proceso de análisis y revisión, además de un alto grado de calificación y aptitudes profesionales que deben recaer en un contador público con los conocimientos técnicos acordes con la responsabilidad que implica tal función.

El comisario debe mantener una comunicación constante y permanente con los auditores internos y la administración, a efectos de prevenir situaciones de malversación de activos, así como con los auditores externos a fin de coadyuvar y/o participar en actividades tendientes a prevenir situaciones vulnerables que pudiesen

facilitar la emisión de información financiera fraudulenta, ya que en este último caso, de presentarse, ya no permitiría afirmar dicha información financiera como veraz.

Es conveniente que la función de comisario esté encomendada a un profesional experto en temas financieros, de control y con conocimientos técnicos contables, para que pueda ejercer a plenitud sus funciones.

No es recomendable, el que terceros sin la experiencia ni los conocimientos en materia de reportes financieros, controles y principios contables, realicen la función de comisario, debido a lo complejo y a la alta responsabilidad que esta actividad conlleva.

Auditores externos

Los auditores externos pueden coadyuvar con la administración y el consejo de administración o comité de auditoría mediante la evaluación de los procesos establecidos para la identificación y medición, y con las acciones que se deriven de los riesgos de fraude.

El consejo de administración o comité de auditoría debe mantener un diálogo abierto y continuo con sus auditores externos acerca de los procesos de administración del riesgo y del sistema de control interno, incluyendo la susceptibilidad de la existencia de fraude en la emisión de información financiera o malversación de activos.

Elementos internos de supervisión: administración

La alta gerencia es responsable de supervisar las actividades llevadas a cabo por los empleados, implanta, monitorea procesos y controles. Sin embargo, la administración también puede iniciar, participar, o dirigir, la comisión y encubrimiento de un acto fraudulento. En consecuencia, el comité de auditoría u órgano de vigilancia tiene la responsabilidad de supervisar las actividades de la alta gerencia y de considerar el riesgo de emisión de información financiera fraudulenta que involucra la anulación de controles internos o la colusión.

Auditores internos

Un eficaz equipo de auditoría interna puede ser sumamente útil en la realización de aspectos de la función de supervisión. Sus conocimientos de la entidad podrán permitirles que identifiquen indicadores que pudieran sugerir que se ha cometido un fraude. Las Normas para la Práctica Profesional de Auditoría Interna emitidas por el Instituto de Auditores Internos de los Estados Unidos de América (Normas IIA en inglés) indican lo siguiente: “El auditor interno debe tener conocimientos suficientes para identificar los indicadores del fraude, mas no se espera posea la pericia de una persona cuya responsabilidad primaria es la detección e investigación del fraude.”

Los auditores internos, además, tienen la oportunidad de evaluar los riesgos de fraude y los controles, recomendar acciones para mitigar riesgos y mejorar controles. Pueden utilizar procedimientos analíticos y otros, para aislar anomalías y realizar revisiones detalladas de cuentas de alto riesgo y/o operaciones para identificar fraudes potenciales en los EEFF.

Los auditores internos deben mantener una línea de comunicación **independiente y directa** con los comités de auditoría u órgano de vigilancia, que facilite expresar inquietudes respecto al compromiso de la administración con los controles internos apropiados o para reportar sospechas de fraude que involucren a la administración.

4.2. Métodos de evaluación

Los métodos utilizados para llevar a cabo el EyECI (Estudio y Evaluación del Control Interno) son:

1. Cuestionarios

De acuerdo con las características del negocio (naturaleza, complejidad, tamaño) se diseñan cuestionarios, los cuales consisten en una serie de preguntas que se efectúan al personal de la empresa acerca de su manejo, registros u operaciones.

• Deben ser diseñados de tal forma, que permitan identificar: – A nivel empresa, posibles factores de riesgo de fraude. – A nivel operación, los controles que tiene establecidos la empresa para el cumplimiento de cada una de las aseveraciones a los EEFF. •	

2. Descriptivo

En este método, se llevan a cabo entrevistas con los funcionarios y el personal operativo de la empresa, sobre el desarrollo de las operaciones sujetas a revisión, y se plasman en un PT (explicación detallada), que incluye: área, proceso u operación revisada, y nombre, puesto y firma de la persona que proporcionó la información.

3. Gráfico

El método gráfico se realiza de igual forma que el descriptivo, sólo que en vez de narrar las operaciones en un documento, se realizan diagramas de flujo y/o recorridos de los procesos u operaciones.

Este método normalmente se utiliza para evaluar el CI a nivel operativo, ya que ayuda a identificar fácilmente donde pueden ocurrir errores.

El uso de cualquiera de éstos métodos no es limitativo, la forma y el alcance de la evaluación del CI se verá influida por el tamaño, la complejidad de la entidad y la naturaleza de su estructura de CI.

Por ejemplo, en una entidad grande y compleja, podrán emplearse cuestionarios, descripciones y diagramas, en cambio en una entidad pequeña, un memo descriptivo podrá ser suficiente (Véase, Boletín 3050).

4.3. Otras Normas Nacionales (Fiscales o Sectoriales)

En materia gubernamental el pasado 12 de julio de 2010 con modificación al día 11 de julio de 2011, mediante el Diario Oficial de la Federación, se publicó el Acuerdo por el que se emiten las Disposiciones en Materia de Control Interno y se expide el Manual Administrativo de Aplicación General en Materia de Control Interno.

Dicho acuerdo contempla aspectos sumamente importantes en materia de control interno que para efectos de este apartado solo se analizará lo que más adelante se detalla, sin embargo es importante que el alumno profundice en su estudio ya que su aplicación es de carácter obligatorio para las dependencias y entidades paraestatales de la Administración Pública Federal y la Procuraduría General de la República.

En el Título Segundo, Capítulo II “Estructura del Modelo”, disposición 14 señala lo siguiente:

> 14. En el establecimiento y actualización del Sistema de Control Interno Institucional, las dependencias, las entidades a través de sus Titulares y de los servidores públicos que se ubiquen en los diversos niveles de control interno, observarán lo siguiente:
>
> **I. NORMAS GENERALES DE CONTROL INTERNO**: Los Titulares deberán asegurarse de:
>
> **PRIMERA. Ambiente de Control**: Que exista un entorno y clima organizacional de respeto e integridad con actitud de compromiso y congruente con los valores éticos del servicio público en estricto apego al marco jurídico que rige a la APF, con una clara definición de responsabilidades, desagregación y delegación de funciones, además de prácticas adecuadas de administración de los recursos humanos; alineados en su conjunto con la misión, visión, objetivos y metas institucionales, lo que contribuirá a fomentar la transparencia, rendición de cuentas y el apoyo a la implementación de un Sistema de Control Interno eficaz y eficiente.
>
> **SEGUNDA. Administración de Riesgos**: Que se implementa un proceso sistemático que permita identificar, evaluar, jerarquizar, controlar y dar seguimiento a los riesgos que puedan obstaculizar o impedir el cumplimiento de los objetivos y metas institucionales.
>
> Se analizan los factores internos y externos que puedan aumentar el impacto y la probabilidad de materialización de los riesgos; y se definan estrategias y acciones para controlarlos y fortalecer el Sistema de Control Interno.
>
> La administración de riesgos se realiza en apego a las etapas mínimas del proceso, establecidas en el Título Tercero de las presentes Disposiciones y el Manual.
>
> El análisis y seguimiento de los riesgos, prioritariamente los de atención inmediata, se efectúe en las sesiones del Comité u órgano de gobierno, conforme a lo establecido en el Título Cuarto de estas Disposiciones.
>
> **TERCERA. Actividades de Control Interno**: Que en todos los niveles y funciones de la Institución se establezcan y actualicen las políticas, procedimientos, mecanismos y acciones necesarias para lograr razonablemente los objetivos y metas institucionales.
>
> Dentro de éstas, se incluirán diversas actividades de revisión, aprobación, autorización, verificación, conciliación y supervisión que provean evidencia documental y/o electrónica de su ejecución.

CUARTA. Información y Comunicación: Que existan requerimientos de información definidos por grupos de interés, flujos identificados de información externa e interna y mecanismos adecuados para el registro y generación de información clara, confiable, oportuna y suficiente, con acceso ágil y sencillo; que permita la adecuada toma de decisiones, transparencia y rendición de cuentas de la gestión pública.

La información que se genera, obtenga, adquiera, transforme o conserve se clasifica y se comunica en cumplimiento a las disposiciones legales y administrativas aplicables en la materia.

Los sistemas de información estén diseñados e instrumentados bajo criterios de utilidad, confiabilidad y oportunidad, así como con mecanismos de actualización permanente, difusión eficaz por medios electrónicos y en formatos susceptibles de aprovechamiento para su procesamiento y permitan determinar si se están cumpliendo los objetivos y metas institucionales con el uso eficiente de los recursos.

Que existan canales de comunicación adecuados y retroalimentación entre todos los servidores públicos de la Institución, que generen una visión compartida, articulen acciones y esfuerzos, faciliten la integración de los procesos y/o instituciones y mejoren las relaciones con los grupos de interés; así como crear cultura de compromiso, orientación a resultados y adecuada toma de decisiones.

Implementan procedimientos, métodos, recursos e instrumentos que garantizan la difusión y circulación amplia y focalizada de la información hacia los diferentes grupos de interés, preferentemente automatizados.

QUINTA. Supervisión y Mejora Continua: Que el Sistema de Control Interno Institucional se supervisa y mejora continuamente en la operación, con el propósito de asegurar que la insuficiencia, deficiencia o inexistencia identificada en la supervisión, verificación y evaluación interna y/o por los diversos órganos de fiscalización, se resuelva con oportunidad y diligencia, dentro de los plazos establecidos de acuerdo a las acciones a realizar, debiendo identificar y atender la causa raíz de las mismas a efecto de evitar su recurrencia.

Las debilidades de control interno determinadas por los servidores públicos se hacen del conocimiento del superior jerárquico inmediato hasta el nivel de Titular de la Institución, y las debilidades de control interno de mayor importancia al Titular de la Institución, al Comité y, en su caso, al órgano de gobierno de las entidades.

II. NIVELES DE CONTROL INTERNO: El Sistema de Control Interno Institucional para su implementación y actualización se divide en tres niveles, Estratégico, Directivo y Operativo, los cuales se encuentran vinculados con las Normas Generales a que se refiere la fracción anterior, y son los siguientes:

II.1 ESTRATÉGICO. Tiene como propósito lograr la misión, visión, objetivos y metas institucionales, por lo que debe asegurar que se cumplan los elementos de Control Interno siguientes:

PRIMERA. Ambiente de Control:

a) La misión, visión, objetivos y metas institucionales, están alineados al Plan Nacional de Desarrollo y a los Programas Sectoriales, Institucionales y Especiales
b) El personal de la Institución conoce y comprende la misión, visión, objetivos y metas institucionales;
c) Existe, se actualiza y difunde un Código de Conducta, en apego al Código de Ética de la APF;
d) Se diseñan, establecen y operan los controles con apego al Código de Ética y al Código de Conducta;
e) Se promueve e impulsa la capacitación y sensibilización de la cultura de autocontrol y administración de riesgos y se evalúa el grado de compromiso institucional en esta materia;
f) Se efectúa la planeación estratégica institucional como un proceso sistemático con mecanismos de control y seguimiento, que proporcionen periódicamente información relevante y confiable para la toma oportuna de decisiones;
g) Existen, se actualizan y difunden políticas de operación que orientan los procesos al logro de resultados;
h) Se utilizan TIC's para simplificar y hacer más efectivo el control;
i) Se cuenta con un sistema de información integral y preferentemente automatizado que, de manera oportuna, económica, suficiente y confiable, resuelve las necesidades de seguimiento y toma de decisiones, y
j) Los servidores públicos conocen y aplican las presentes Disposiciones y el Manual.

SEGUNDA. Administración de Riesgos

a) Existe y se realiza la administración de riesgos en apego a las etapas mínimas del proceso, establecidas en el Título Tercero de las presentes Disposiciones.

TERCERA. Actividades de Control:

a) Los Comités institucionales funcionan en los términos de la normatividad que en cada caso resulte aplicable;
b) El COCODI o, en su caso, el órgano de gobierno analiza y da seguimiento a los temas relevantes relacionados con el logro de objetivos y metas institucionales, el Sistema de Control Interno Institucional, la administración de riesgos, la auditoría interna y externa, en los términos
c) Se establecen los instrumentos y mecanismos que miden los avances y resultados del cumplimiento de los objetivos y metas institucionales y analizan las variaciones.
d) Se establecen los instrumentos y mecanismos para identificar y atender la causa raíz de las observaciones determinadas por las diversas instancias de fiscalización, a efecto de abatir su recurrencia.

CUARTA. Informar y Comunicar:

a) Se cuenta con información periódica y relevante de los avances en la atención de los acuerdos y compromisos de las reuniones del órgano de gobierno, de Comités

Institucionales, del COCODI y de grupos de alta dirección, a fin de impulsar su cumplimiento oportuno y obtener los resultados esperados.

QUINTA. Supervisión y Mejora Continua:

a) Las operaciones y actividades de control se ejecutan con supervisión permanente y mejora continua a fin de mantener y elevar su eficiencia y eficacia;
b) El Sistema de Control Interno Institucional periódicamente se verifica y evalúa por los servidores públicos responsables de cada nivel de Control Interno y por los diversos órganos de fiscalización y evaluación, y
c) Se atiende con diligencia la causa raíz de las debilidades de control interno identificadas, con prioridad en las de mayor importancia, a efecto de evitar su recurrencia. Su atención y seguimiento se efectúa en el PTCI.

II.2 DIRECTIVO: Tiene como propósito que la operación de los procesos y programas se realice correctamente, y le corresponde asegurarse de que se cumplan con los elementos de Control Interno siguientes:

PRIMERA. Ambiente de Control:

a) La estructura organizacional define la autoridad y responsabilidad, segrega y delega funciones, delimita facultades entre el personal que autoriza, ejecuta, vigila, evalúa, registra o contabiliza las transacciones; evitando que dos o más de éstas se concentren en una misma persona y además, establece las adecuadas líneas de comunicación e información;
b) Los perfiles y descripciones de puestos están definidos, alineados a las funciones y actualizados. Se cuenta con procesos para la contratación, capacitación y desarrollo, evaluación del desempeño, estímulos y, en su caso, promoción de los servidores públicos;
c) Aplica al menos una vez al año encuestas de clima organizacional, identifica áreas de oportunidad, determina acciones, da seguimiento y evalúa resultados;
d) Los manuales de organización son acordes a la estructura organizacional autorizada y a las atribuciones y responsabilidades establecidas en las leyes, reglamentos, y demás ordenamientos aplicables, así como, a los objetivos institucionales, y
e) Los manuales de organización y de procedimientos, así como sus modificaciones, están autorizados, actualizados y publicados.

TERCERA. Actividades de Control:

a) Las actividades relevantes y operaciones están autorizadas y ejecutadas por el servidor público facultado para ello conforme a la normatividad; dichas autorizaciones están comunicadas al personal. En todos los casos, se cancelan oportunamente los accesos autorizados, tanto a espacios físicos como a TIC´s, del personal que causó baja;
b) Se encuentran claramente definidas las actividades, para cumplir con las metas comprometidas con base en el presupuesto asignado del ejercicio fiscal;
c) Están en operación los instrumentos y mecanismos que miden los avances y resultados del cumplimiento de los objetivos y metas institucionales y se analizan las variaciones por unidad administrativa, y
d) Existen controles para que los servicios se brinden con estándares de calidad.

CUARTA. Informar y Comunicar:

a) El Sistema de Información permite conocer si se cumplen los objetivos y metas institucionales con uso eficiente de los recursos y de conformidad con las leyes, reglamentos y demás disposiciones aplicables;
b) El Sistema de Información proporciona información contable y programático-presupuestal oportuna, suficiente y confiable;
c) Se establecen medidas a fin de que la información generada cumpla con las disposiciones legales y administrativas aplicables;
d) Existe y opera un registro de acuerdos y compromisos de las reuniones del órgano de gobierno, de Comités Institucionales, incluyendo al COCODI y de grupos de alta dirección, así como de su seguimiento, a fin de que se cumplan en tiempo y forma, y
e) Existe y opera un mecanismo para el registro, análisis y atención oportuna y suficiente de quejas y denuncias.

QUINTA. Supervisión y Mejora Continua:

a) Realiza la supervisión permanente y mejora continua de las operaciones y actividades de control, y
b) Se identifica la causa raíz de las debilidades de control interno determinadas, con prioridad en las de mayor importancia, a efecto de evitar su recurrencia e integrarlas al PTCI para su atención y seguimiento.

II.3 OPERATIVO: El propósito es que las acciones y tareas requeridas en los distintos procesos se ejecuten de manera efectiva, por lo que en éste se debe asegurar el cumplimiento de los elementos de Control Interno siguientes:

PRIMERA. Ambiente de Control:

a) Las funciones se realizan en cumplimiento al manual de organización, y
b) Las operaciones se realicen conforme a los manuales de procedimientos autorizados y publicados.

TERCERA. Actividades de Control:

a) Existen y operan mecanismos efectivos de control para las distintas actividades que se realizan en su ámbito de competencia, entre otras, registro, autorizaciones, verificaciones, conciliaciones, revisiones, resguardo de archivos, bitácoras de control, alertas y bloqueos de sistemas y distribución de funciones;
b) Las operaciones relevantes están debidamente registradas y soportadas con documentación clasificada, organizada y resguardada para su consulta y en cumplimiento de las leyes que le aplican;
c) Las operaciones de recursos humanos, materiales, financieros y tecnológicos, están soportadas con la documentación pertinente y suficiente; y aquéllas con omisiones, errores, desviaciones o insuficiente soporte documental, se aclaran o corrigen con oportunidad;
d) Existan los espacios y medios necesarios para asegurar y salvaguardar los bienes, incluyendo el acceso restringido al efectivo, títulos valor, inventarios, mobiliario y equipo u otros que pueden ser vulnerables al riesgo de pérdida, uso no autorizado, actos de corrupción, errores, fraudes, malversación de recursos o cambios no autorizados; y que son oportunamente registrados y periódicamente comparados físicamente con los registros contables;
e) Se operan controles para garantizar que los servicios se brindan con estándares de calidad, y
f) Existen y operan los controles necesarios en materia de TIC's para:

1. Asegurar la integridad, confidencialidad y disponibilidad de la información electrónica de forma oportuna y confiable;
2. Instalación apropiada y con licencia de software adquirido;
3. Plan de contingencias que dé continuidad a la operación de las TIC´s y de la Institución;
4. Programas de seguridad, adquisición, desarrollo y mantenimiento de las TIC´s;
5. Procedimientos de respaldo y recuperación de información, datos, imágenes, voz y video, en servidores y centros de información, y programas de trabajo de los operadores en dichos centros;
6. Desarrollo de nuevos sistemas informáticos y modificaciones a los existentes, que sean compatibles, escalables e interoperables, y
7. Seguridad de accesos a personal autorizado, que comprenda registros de altas, actualización y bajas de usuarios.

CUARTA. Informar y Comunicar:

a) La información que genera y registra en el ámbito de su competencia, es oportuna, confiable, suficiente y pertinente.

RESUMEN

En este tema se mostró un breve compendio de la normativa nacional emitida por la CONPA, aplicable al estudio y evaluación del control interno que realiza el auditor externo como parte de su trabajo.

El EyECI permite al auditor no sólo determinar la efectividad de los controles aplicables las operaciones de una entidad, también le permite identificar posibles factores de riesgo de fraude que pudieran tener un impacto significativo en los EEFF sujetos a revisión.

Se considera que la implementación del sistema de control interno, su vigilancia y funcionamiento son responsabilidad de la administración de una entidad, el estudio que realiza el auditor si bien es parte fundamental de la vigilancia del mismo, su finalidad es contribuir en la determinación de la naturaleza, alcance y oportunidad de las pruebas que el auditor aplicará para llevar a cabo su revisión.

La normativa emitida en esta materia se ha modificado y continúa el estudio para hacer frente a las condiciones actuales de las empresas, pero sobre todo para hacer frente a las nuevas disposiciones legales emitidas en este sentido. [De hecho, no hay que olvidar buscar siempre las versiones vigentes o, al menos, las más actualizadas posibles que se pueda.]

BIBLIOGRAFÍA

SUGERIDA

Autor	Capítulo	Páginas
IMCP [2012] Normas de Auditoría y Normas para Atestiguar	Boletín 3050 Estudio y evaluación de control interno	1-21
IMCP [2012] Guías de auditoría	Boletín 5030 Metodología para el estudio y evaluación de control interno	1-21
IMCP [2012] Guías de auditoría	Boletín 6080 Ayuda para prevenir, disuadir y detectar el fraude	1-27

Instituto Mexicano de Contadores Públicos. (2006). *Normas y procedimientos de auditoría y normas para atestiguar*. (26ª ed.) México: IMCP. [En 2010 la versión las llama Normas Internacionales de Auditoría, ISA, del inglés. De cualquier manera, **siempre consultar las vigentes**.]

Unidad 5.

Normas internacionales aplicables al estudio y evaluación del control interno

OBJETIVO PARTICULAR

Analizar la normatividad internacional existente, así como su relación con el marco normativo nacional, con la finalidad de entender los requisitos que se deben cumplir en cuanto a su estudio y análisis en los distintos ámbitos de aplicación (nacional e internacional).

TEMARIO DETALLADO
(6 horas)

5. Normas internacionales aplicables al estudio y evaluación del control interno

5.1. *International Standards on Auditing* de la *International Federation of Accountant's*

5.2. Sarbanes-Oxley Act

INTRODUCCIÓN

En el año 2000 la empresa ENRON llegó a ser catalogada por la revista especializada *Fortune* como la quinta en importancia en Estados Unidos y la decimotercera a nivel mundial, erigiéndose como el ideal corporativo para otras empresas, valuada en 60,000 millones de dólares en el año 2001. Era, en pocas palabras, símbolo de ganancias y ejemplo de administración eficiente.

Sin embargo, su quiebra junto con el de otras empresas como Worldcom y Xerox, constituyó un parteaguas histórico. Inversiones apoyadas en, pasivos y sin flujos de efectivos, diversificación de negocios en derivados, registros contables sin fundamento, colusión con los auditores, conflictos de interés, son sólo algunas de las irregularidades ocurridas en estas compañías. Lo anterior trajo como consecuencia una caída del sistema financiero estadounidense y la pérdida de credibilidad en la función de auditoría a nivel mundial.

Estas situaciones obligaron a las autoridades financieras estadounidenses a implementar diversas medidas regulatorias al respecto. En julio de 2002 el congreso de Estados Unidos aprobó la ley Sarbanes- Oxley cuyo propósito fundamental es construir y restaurar la confianza en información financiera de empresas públicas, convirtiéndose en la más significativa reforma a las leyes de valores desde su emisión original, (véase, Soní, 2004, p. 29).

A fin de proporcionar un marco normativo de referencia, se presentan algunas de las principales publicaciones o regulaciones que han emitido las autoridades de Estados Unidos en materia de control interno.

No se trata de un estudio de interpretación de leyes o reglamentos, tampoco se incluye la totalidad de las regulaciones que se mencionan sólo se describen algunos párrafos relacionados con el tema de estudio.

5.1. International Standards on Auditing de la International Federation of Accountant's

American Institute of Certified Public Accountants (AICPA)

El Instituto Americano de Contadores Públicos Certificados, AICPA por sus siglas en inglés, es la organización profesional más grande de Contadores Públicos Certificados (CPC) en los Estados Unidos de América (EUA). Se creó en 1936, de la fusión del *American Institute of Accountants* y de la *American Accounting Association*.

En la actualidad cuenta con más de 350,000 miembros, la mayoría laboran en la industria, el gobierno y la educación, en las áreas de: auditoría, contabilidad, impuestos, consultoría, comercial, planificación financiera personal y tecnología de negocio.

La finalidad del AICPA es promover y proteger la profesión de contabilidad en EUA, autorregular la práctica de los CPC, establecer y difundir programas para ayudar a los CPC, a mantener la competencia profesional.

Entre sus funciones se encuentran:

- Preparar y aplicar el examen uniforme de CPC.
- Desarrollar normas profesionales (*Statements on Auditing Standards*).
- Brindar soporte técnico a sus agremiados.
- Mantener las relaciones públicas de la profesión.
- Apoyar a la comunidad académica.

- Representar a la profesión ante el Congreso de EUA y las agencias federales.

Concepto

Como se vio, el AICPA es el organismo encargado de emitir las normas profesionales en materia de auditoría: *Statements on Auditing Standard*-SAS (Declaraciones sobre normas de auditoría).

Las primeras SAS fueron emitidas en 1939 y de ahí hasta la fecha se han emitido nuevas SAS, actualizando o modificando las existentes. Hasta la fecha se han publicado 111 SAS.

Las SAS son las pautas que un auditor (en EEUU) usa para determinar si se han preparado las declaraciones financieras de acuerdo con los *Generally Accepted Accounting Principals* (GAAP), que Son las Normas de Información Financiera Generalmente Aceptados de EEUU, su equivalencia con la normativa en nuestro país serían las Normas de Información Financiera.

Las SAS son trascendentes no sólo en Estados Unidos, su aplicación está contemplada en las normas de auditoría de manera supletoria, además las relaciones comerciales con ese país hacen que se esté cada vez más apegado a ellas, por lo que es muy importante tener conocimiento de las mismas.

En el cuadro siguiente, se muestran algunas de las SAS vigentes a la fecha, las cuales se relacionan con los temas tratados en los capítulos anteriores.

SAS 1	Declaraciones sobre normas de auditoría
SAS 55 y 78	138Comunicaciones sobre el control interno en una auditoría de EEFF
SAS 60	
	139 Comunicación de asuntos relacionados con la estructura de control interno observados en una auditoría.
SAS 82 y 99	Comunicaciones de fraude en una auditoria de EEFF
SAS 90	Comunicaciones al comité de auditoría

SAS (*Statements on Auditing Standard*)

A continuación se muestra una breve síntesis del contenido de cada una de ellas (Véase AICPA, 1998):

SAS núm. 1 Declaraciones sobre normas de auditoría

La **auditoría** comprende una revisión metódica y un examen de lo auditado, incluyendo la verificación de información específica según lo determina el auditor o lo establece la práctica profesional general. El propósito de la auditoría es, usualmente, expresar una opinión o formar una conclusión sobre lo auditado.

El **propósito de una auditoría independiente** es determinar si los EEFF del cliente son presentados de manera razonable en todos los aspectos importantes y de acuerdo con los principios de contabilidad. Esta determinación solamente puede efectuarse después de que el auditor haya realizado una auditoría de acuerdo con las SAS, las cuales se dividen en:

a) Normas Generales
b) Normas para la ejecución del trabajo
c) Normas de información

El auditor también puede ser contratado para informar sobre EEFFF preparados de acuerdo con la base de efectivo, la base de liquidación o en cuanto a su conformidad con los principios contables de otros países.

Las normas de ejecución de trabajo requieren que el auditor reúna evidencia comprobatoria suficiente y competente como base para formular una opinión sobre los EEFFF. La evidencia puede definirse como cualquier información que tenga impacto al determinar que los EEFFF están presentados en forma razonable de acuerdo con los principios contables.

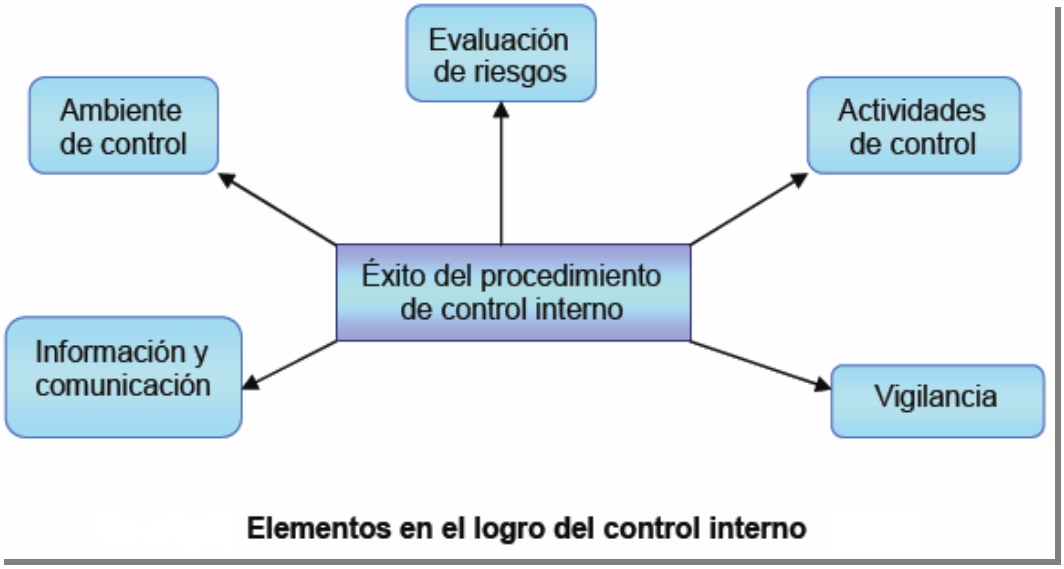
SAS No. 55 y 78 Consideraciones sobre el control interno en una auditoría de EEFF

La SAS 55 da pautas específicas para lograr el objetivo establecido en la segunda norma de auditoría, que requiere obtener una comprensión suficiente del control interno para planear la auditoría.

Describen al **control interno** como un "proceso efectuado por la junta directiva, la gerencia u otro personal de la entidad, diseñado para proporcionar seguridad razonable en cuanto al logro de los objetivos en las siguientes categorías:

1. Confiabilidad de la presentación de información financiera.
2. Eficacia y eficiencia de las operaciones.
3. Cumplimiento de las leyes y regulaciones correspondientes".

Una vez establecidos los objetivos, la gerencia debe establecer, también, el proceso que estimula su cumplimiento y logro por parte de los empleados. Los **cinco elementos** siguientes son básicos para lograr el éxito del procedimiento de control interno:



Elementos en el logro del control interno

La SAS 78 es un complemento a la SAS 55 y requiere que el auditor comprenda el sistema de control interno del cliente para que esto le sirva de base para planear su auditoría. La evaluación del control interno hecha por el auditor determina, en parte, la naturaleza, momento y alcance de los procedimientos de auditoría sustantivos.

SAS No. 60 Comunicación de asuntos relacionados con la estructura de control interno observados en una auditoría

Las situaciones que informar son aquellas que atraen la atención del auditor y que, a juicio suyo, deben comunicarse al comité de auditoría ya que representan deficiencias importantes en el diseño o funcionamiento del control interno que pueden afectar adversamente a la capacidad de la entidad para registrar, procesar, resumir y revelar datos financieros en conformidad con las afirmaciones de la gerencia en los EEFF.

SAS 82 y 99 Consideraciones de fraude en una auditoría de EEFF

La SAS 82 fue emitida en 1997 y en 2002 fue actualizada con la SAS 99 (Consideraciones de fraude en una Auditoría de EEFF) La aplicación de esta norma es obligatoria para las auditorías de EEFF de los periodos que iniciaron el 15 de diciembre de 2002 o posteriores.

De acuerdo con esta norma la responsabilidad del auditor es planear y realizar una auditoría para obtener la seguridad razonable sobre si los estados financieros están libres de errores materiales, causado por error o por fraude. La SAS 99 contiene una guía ampliada de cómo los auditores cumplen sus responsabilidades en relación al riesgo de fraude.

Esta norma requiere que los auditores realicen:

a) Una evaluación del riesgo de fraude considerando:

- Incentivos y/o presiones para perpetrar un fraude.
- Oportunidad para llevar a cabo un fraude.
- Actitud y/o razones para justificar la acción fraudulenta.

b) Investigaciones sobre la administración y el personal clave de la entidad.

c) Revisiones analíticas adicionales de ingresos y egresos durante la planeación.

d) Una evaluación de los programas y controles de la entidad contra el fraude, si han sido diseñados en forma idónea y puestos en operación.

e) El diseño de procedimientos de auditorías adicionales o diferentes para obtener una evidencia más confiable.

SAS 90: Comunicaciones del comité de auditoría

La SAS 90 remplaza a la SAS 61, Comunicación los comités de auditoría y mejora la SAS núm. 71, Información financiera intermedia. Esta norma requiere una discusión entre el auditor, la gerencia y el comité de auditoría.

Se indica que ciertos asuntos relacionados con la auditoría deben comunicarse a los supervisores de la función de presentación de informes financieros. Quien recibe tales

comunicaciones es el comité de auditoría o alguna otra persona que tenga la misma autoridad y responsabilidad.

El propósito de la comunicación es proveer al comité de auditoría información adicional sobre el alcance y resultados de la auditoría que pueden ayudarle a supervisar el proceso de presentación de informes financieros y sus revelaciones correspondientes. La comunicación puede ser por escrito o de forma oral, además esta comunicación debe ocurrir oportunamente, bien sea antes o después de la emisión del dictamen, dependiendo de las circunstancias.

5.2. Sarbanes-Oxley Act

Concepto

En respuesta a la gran cantidad de escándalos contables y corporativos que involucraron, en situaciones de fraude, a importantes empresas de los Estados Unidos de Norteamérica, el Congreso de dicho país aprobó el 30 de julio de 2002 La Ley Sarbanes-Oxley[14] con el afán de proteger a los inversionistas de las empresas públicas reguladas por la Security and Exchange Comisión (SEC).[15]

Objetivo

El propósito fundamental de esta ley es el construir y restaurar la confianza en la información financiera de las empresas públicas, convirtiéndose en la más significativa reforma a las leyes de valores desde su emisión original.

Obligatoriedad

[14] Esta Ley fue promovida por el Senador Paul Sarbanes y el representante de los Estados Unidos Michael Oxley, por lo cual lleva sus nombres.
[15] Es el órgano de vigilancia de las empresas que cotizan en la Bolsa de valores en EUA.

Esta ley contiene una serie de estándares que afecta entre otros a la Administración de las empresas -particularmente empresas cuyo valor de capitalización de mercado sea mayor de 75 millones de dólares-, a los Comités de Auditoría, a los Auditores internos y externos de empresas públicas que cotizan en el mercado bursátil estadounidense (véase, Alcalá, 2004, p. 45 y ss.).

El cumplimiento de las disposiciones de esta ley es obligatorio no sólo para las compañías localizadas en Estados Unidos sino también para las compañías mexicanas registradas en las bolsas de valores estadounidenses y las subsidiarias de compañías de Estados Unidos ubicadas en México.

Estructura

La Ley Sarbanes-Oxley (Ley SOX) consta de once títulos o secciones que van desde la creación de responsabilidades adicionales para los Consejos Directivos de las empresas, hasta sanciones penales. Así mismo, requiere a la SEC la creación o implementación de reglamentos o lineamientos para el cumplimiento de esta nueva Ley.

La ley SOX establece:

- Nuevas regulaciones para los Consejos corporativos y los Comités de Auditoría.
- Nuevos estándares de responsabilidad y penas criminales para la administración corporativa.
- Nuevos estándares de independencia para los auditores externos.
- Creación de una junta supervisora contable de las empresas públicas, que depende de la SEC y se encarga de supervisar a las firmas contables así como de generar estándares de contabilidad.

Contenido

El aspecto central de esta ley se refiere al control en la incidencia de fraudes en una organización, no sólo al fraude por falsedad de declaraciones en los EEFF sino que hace referencia a todos los casos de fraude en los que se desvirtúe de manera importante los EEFF, la malversación de activos y el fraude por corrupción.

El proceso de cumplimiento de esta ley, de manera muy general, es que cada empresa que cotiza en la bolsa a través de una inversión, deuda pública o que esté involucrada en el proceso de fusión o adquisición por parte de empresas públicas deberá tener, por parte de sus directivos, generales y de finanzas, una certificación de la efectividad de sus controles internos acompañados de la opinión del auditor externo, mismos que deberán acompañar a su informe anual.

A partir de esta ley los auditores reportarán a un Comité de Auditoría y no a la administración de la empresa. La característica principal de los integrantes de este Comité de Auditoría es la independencia, que es el motivo principal de esta ley.

La ley está integrada por secciones las cuales establecen diversas disposiciones que constituyen prácticas sanas de negocios que mejoran la reputación de una organización, al enviar mensajes para demostrar que la empresa está llevando a cabo esfuerzos serios en aras de publicar sólo información financiera precisa.

A continuación se presenta un resumen de las secciones de la Ley SOX relacionadas con el Control interno.

1. Sección 404 Reporte sobre el control interno

La sección 404[16] consiste en una evaluación anual por parte de la administración acerca de los controles internos.

[16] La aplicación de esta sección se inició en los ejercicios terminados después del 15 de noviembre de 2004.

Dicha sección establece que es responsabilidad de la administración constituir y mantener una estructura adecuada de control interno y procedimientos para reportar financieramente, así como una evaluación al final del último ejercicio fiscal acerca de la efectividad de los controles y procedimientos (véase, Soní, 2004).

La ley SOX obliga a la **administración** tener mayor control sobre su régimen interno con el único fin de generar confianza y evitar cualquier tipo de fraude.

Para el cumplimiento de esta ley el **ambiente de control** (tratado en capítulos anteriores) se convierte en uno de los componentes clave de control interno de una entidad sobre todo porque establece el tono de la misma, influye en la conciencia de las personas dentro de una organización y es el fundamento de todos los componentes del sistema de control interno.

La **administración** de la compañía siempre ha tenido la **responsabilidad del diseño y mantenimiento del control interno**, con esta ley tiene la responsabilidad de informar anualmente sobre el control interno de la entidad y dar a conocer la información financiera. Los auditores **externos** serán los encargados de **auditar a la administración en cuanto a la efectividad del control interno** y realizarán pruebas independientes incluyendo al ambiente de control, que al contrario de un control a nivel de actividad que se limita a un flujo de procesamiento, el ambiente de control en una estructura dominante afecta a muchas actividades de negocios. Incluye valores éticos y de integridad de la administración, una filosofía operativa y sobre todo el compromiso hacia la competencia organizacional.

La sección 404 requiere que la **administración evalúe e informe de la efectividad del control interno de una compañía sobre la cuestión financiera**, esto representa un cambio considerable en evaluación del control. El ambiente de control es una parte integrante del sistema del control interno por lo tanto debe comprenderse, evaluarse y

ponerse a prueba, primero por la administración y posteriormente por los auditores externos.

Esta sección también requiere un reporte del auditor externo quien debe emitir un informe acerca de la evaluación del control interno hecho por la administración.

En relación con este requerimiento, la sección 103, que redactó el *Public Company Accounting Oversight Board* (PCAOB)[17], adoptará normas especificando la forma en que los auditores externos deberán describir en su reporte de auditoría el alcance de sus pruebas acerca de la estructura de control interno y de los procedimientos que aplicaron al llevar a cabo la revisión requerida por la sección 404.

Para ello, deben presentar asuntos detectados en sus pruebas de los controles internos, una evaluación acerca de los controles y procedimientos, si éstos proporcionan registros razonablemente detallados para reflejar adecuadamente las operaciones y permitir la preparación de EEFF de acuerdo con las bases contables correspondientes, una descripción de debilidades importantes en esos controles internos y de cualquier falta de cumplimiento importante encontrada al hacer las pruebas.

Con la llegada de esta ley, el auditor tiene una serie de nuevas responsabilidades, según (Soní, 2004) que apuntan a:

- Evaluar los controles relativos a fraudes, las deficiencias y los reportes de la administración.
- Obtener un entendimiento del diseño de los controles.
- Probar y evaluar la efectividad operativa de los controles.
- Tener independencia.

[17] Organismo creado en EUA como mecanismo de supervisión para asegurar que el trabajo de los auditores se realizara dentro de los estándares más altos de calidad, independencia y ética.

Además, en relación con la función de auditoría, la ley prohíbe que las firmas registradas de contadores públicos que estén auditando alguna emisora proporcionen, en el mismo ejercicio, cualquiera de los siguientes servicios:

- Servicios de contabilidad u otros relacionados con la preparación de EEFF.
- Implementación y diseños de sistemas de información financiera.
- Avalúos, servicios actuariales, de auditoría interna, de recursos humanos y legales.
- Funciones gerenciales.
- Servicios de banca de inversión y asesoría en inversiones.
- Peritajes no relacionados con la auditoría.

Sección 406 Código de ética

La sección 406 requiere que todas las compañías públicas tengan un código de conducta para la administración y los funcionarios de finanzas, que contenga procedimientos apropiados de cumplimiento y ejecución. De acuerdo con esta ley, las bolsas de valores han hecho extensivo este requisito para que el código cubra a todos los directores, funcionarios y empleados; lo han convertido en una condición para seguir cotizando en bolsa.

Un factor muy importante para lograr un ambiente de control ético y programa de cumplimiento exitoso, es la disposición de la agente para presentarse con información que pueda indicar faltas. Dándose cuenta de la importancia de una comunicación hacia arriba y confidencial, la ley recomienda este tipo de "**dar el aviso**", motivando a las compañías de propiedad pública a tener una cultura más abierta, que aliente a los empleados a comunicar si tienen una creencia razonable de que se ha violado alguna ley.

La **sección 301** precisa que el **Comité de Auditoría** de todas las corporaciones públicas deberá **establecer y supervisar la operación de un sistema que permita la comunicación anónima confidencial de empleados** sobre preocupaciones relativas a asuntos cuestionables de contabilidad y auditoría. El propósito de esta sección es motivar a los empleados a reportar las faltas que se relacionen con información financiera fraudulenta.

Con motivo adicional para motivar a que se revele información para ponerla en acción, la **Sección 806** de la ley dirige a las compañías a adoptar **procedimientos para proteger a los empleados que dan información sobre faltas financieras corporativas**. No se permite a las compañías "destituir, remover, suspender, amenazar, acosar o de cualquier modo discriminar" contra dichos empleados. La ley autoriza castigos penales para los infractores (véase, Vershoor, 2004, p.36).

Sección 302 Certificación de información financiera

En relación con esta sección la SEC aprobó la regla "Certificación de Revelaciones en los reportes trimestrales y anuales de las compañías" el 27 de agosto del 2002. Esta certificación señala que, el director general y el de finanzas certifiquen que han revisado los reportes que se están entregando; éstos no contienen omisiones materiales o información "no verídica" que los EEFF presentan razonablemente en todos los aspectos importantes la situación financiera, resultados de las operaciones y flujos efectivos del emisor.

También deben certificar que en su más reciente evaluación han revelado a los auditores y al comité de auditoría del emisor:

- Todas las deficiencias significativas en el diseño u operación de los controles internos que podrían afectar adversamente la habilidad del emisor para registrar, procesar, sumar, reportar información financiera e identificar todas las debilidades importantes en los controles internos.

- Cualquier fraude, ya sea importante o no, que involucre a la administración o a otros empleados que tengan un papel significativo en los controles internos del emisor.

Repercusiones de la Ley SOX para la profesión contable

Esta legislación ha traído cambios no sólo en el país donde se emitió sino en países como el nuestro, debido a las relaciones económicas con Estados Unidos (véase, Garza, 2006). Uno de los principales cambios ha sido la emisión de la nueva Ley del Mercado de Valores (LMV) decretada por el ex presidente Vicente Fox Quezada el 28 de diciembre de 2005, la cual contempla situaciones similares a las de la Ley Sarbanes-Oxley y regula a las compañías que cotizan en la Bolsa Mexicana de Valores. En materia fiscal, se ha contemplado como propuesta de Reforma al Código Fiscal de la Federación, la modificación de los artículos 5° y 26 para quedar como sigue:

> **Artículo 5°**. Cuando se realicen actos que, en lo individual o en su conjunto, sean artificiales o impropios para la obtención del resultado conseguido, las consecuencias fiscales aplicables a las partes que en dichos actos hayan intervenido, serán las que correspondan a los actos idóneos o apropiados para la obtención del resultado que se haya alcanzado. Se considera que un acto es artificial o impropio cuando se reúnan los siguientes requisitos:
>
> I. Que dichos actos produzcan efectos económicos iguales o similares a los que se hubieran obtenido con los actos idóneos o apropiados.
> II. Que los efectos fiscales que se produzcan como consecuencia de los actos artificiales o impropios, consistan en cualquiera de los siguientes:
>
> a) La disminución de la base o del pago de una contribución.
>
> b) La determinación de una pérdida fiscal, en cantidad mayor a la que legalmente corresponda.
>
> c) La obtención de un estímulo o de cualquier otro beneficio fiscal, presente, pasado o futuro.
>
> **Artículo 5° A**. Cuando se realicen actos o contratos simulados, las consecuencias fiscales aplicables a las partes que en ellos hayan intervenido, serán las que correspondan a los actos o contratos realmente realizados.

Artículo 26. Fracción XVI. Los contadores, abogados o cualquier otro profesionista, que emitan opinión que conduzca a los contribuyentes a la realización de los actos artificiosos o impropios a que se refieren los tres últimos párrafos del artículo 5o. de este Código, por las contribuciones que sean determinadas por la aplicación de dichas disposiciones.

Sin embargo a la fecha, los cambios no se han realizado, por lo que continua pendiente la reforma del Código.

RESUMEN

Como se ha visto, la normativa aplicable al EyECI en el país toma como base a las SAS, por lo que las similitudes son significativas, en gran medida esto ha facilitado las relaciones comerciales entre empresas estadounidenses y mexicanas al unificar, grosso modo, la normativa aplicable en relación con el control y la función de auditoría.

Por lo que se refiere a la Ley SOX, esta nueva reglamentación trae retos u oportunidades, algunos de los beneficios que aporta son:

- Fortalece el papel del comité de auditoría en el proceso de reportes financieros.
- Refuerza las responsabilidades de la administración en la información financiera y en los controles internos.
- Eleva la importancia de la auditoría, la necesidad de seguridad adicional y transparencia.
- Fortalece la supervisión sobre la profesión contable.

Sin embargo, los costos para cumplir con la ley son altos, las compañías registradas ante la SEC tendrán desembolsos elevados y efectuarán un número de pasos adicionales para asegurar su cumplimiento. Al aumentar el alcance de las auditoría aumentan también sus costos, las presiones asociadas a la ley las sufrirán no sólo las compañías que quieren cotizar en Bolsa sino también las firmas que les hacen sus auditorías.

BIBLIOGRAFÍA

SUGERIDA

Autor	Capítulo	Páginas
Cano; Lugo y otros (2009).	1. Auditoría Forense	13 a 26

Cano Castaño, Donaliza; Lugo C, Danilo; Cano Castaño, Miguel. (2009). *Auditoría financiera forense en la investigación de: Delitos económicos y financieros, lavado de dinero y activos, financiación del terrorismo*. (3ª ed.). Bogotá: Ecoe.

Unidad 6.

Tendencias

OBJETIVO PARTICULAR

Dar a conocer al alumno las tendencias nacionales e internacionales sobre el estudio y evaluación del control interno y el o los impactos que se pueden desprender de estos cambios.

TEMARIO DETALLADO

(6 horas)

6. Tendencias

4.1. Proyectos en auscultaciones nacionales e internacionales

INTRODUCCIÓN

Antes de abordar el tema es conveniente aclarar que, debido a que el temario oficial de la asignatura no plantea temas particulares, se incluyen los subtemas mencionados anteriormente debido a la importancia que revisten para el entendimiento de la materia en conjunto.

En esta unidad se analizarán algunas de las tendencias que han tenido mayor impacto y utilidad hoy en día en materia de control interno.

Estas tendencias están enfocadas a hacer más eficaz el control interno con el objetivo de enfrentar los retos y cumplir las exigencias que imponen las empresas en la actualidad.

6.1. Proyectos en auscultaciones nacionales e internacionales

Circular única de la CNBV

Se debe reconocer que los importantes acontecimientos del 2002, relacionados con fraudes corporativos y contables ocurridos principalmente en los Estados Unidos, afectaron sensiblemente la confianza en las empresas, en su información financiera, en factores relacionados con el proceso de su preparación y la validación de los mismos, así como la confianza en los auditores independientes.

Sus impactos negativos han afectado a toda la profesión, lo que ha dado lugar a regulaciones adicionales que tienen un impacto significativo en la profesión contable, como es el caso de la Ley *Sarbanes-Oxley* o nuevas normas de auditoría, temas tratados en la unidad anterior.

En nuestro país el IMCP ha trabajado en las necesidades actuales de la comunidad financiera y de los organismos reguladores. La Comisión Nacional Bancaria y de Valores (CNBV) como organismo regulador del sistema financiero, emitió el 19 de marzo de 2003 la Circular única, con la finalidad de regular la prestación de los servicios del contador público independiente.

Esta disposición señala que el contador público independiente o cualquier otro miembro de la firma donde desempeñe sus labores, no podrá:

- Preparar la contabilidad ni los EEFF de la emisora, su controladora, subsidiarias, afiliadas o asociadas, así como los datos que utilice como soporte, es decir, una firma de contadores

no podrá ofrecer servicios contables y de auditoría a una misma empresa.

- Operar, supervisar, diseñar o implantar los sistemas de información que soporten los EEFF o generen información significativa para la elaboración de los mismos de la emisora, por ejemplo está prohibido que la firma diseñe programas de cómputo para la empresa que está auditando.
- Realizar valuaciones o avalúos que sean relevantes para los EEFF de la emisora.
- Participar en las decisiones de la emisora, por ejemplo, ser el auditor externo y formar parte del consejo de administración.
- Participar en la auditoría interna y controles contables relativos a los EEFF de la emisora, es decir, la firma de contadores que realice la auditoría externa de EEFF de una empresa no puede ofrecer a esa misma empresa el servicio de auditoría interna.
- Reclutar y seleccionar personal de la emisora para que ocupen el cargo de director general o cualquier de los dos niveles inmediatos inferiores a éste.

(Véase, Tiburcio, 2003, pp. 16 y ss.)

Código de mejores prácticas corporativas

(Véase, Ceballos y Cruz, 2003)

A. Comité de mejores prácticas corporativas

Una práctica muy extendida en el mundo es que cada país recoja su problemática particular, reglamente y sugiera la adopción de prácticas de control que permitan mejorar el gobierno corporativo de las compañías.

Entre los países líderes en la emisión de códigos de mejores prácticas están Estados Unidos, Canadá, Inglaterra, Francia, España, Holanda y Sudáfrica, se conocen

documentos como el *Blue Ribbon Committee*, el *Cadbury Code*, *Greenbury Report and Code of Good Practice.*

Por otro lado organismos multilaterales como la Organización para la Cooperación y Desarrollo Económico, el Banco Mundial y el Fondo Monetario Internacional también han emitido recomendaciones al respecto. En general los códigos establecen principios mínimos y condiciones comunes que permiten mejorar el gobierno corporativo de las empresas.

Para que los inversionistas tengan confianza en el manejo de las empresas es necesario que éstas cuenten con transparencia en su administración y que se fomente una adecuada revelación a los inversionistas.

En este sentido diversos sectores de la economía mexicana han manifestado su interés en que las empresas del país alcancen estándares internacionales que les permitan ser más competitivas transparentando su administración y ofreciendo mayor confianza a los inversionistas nacionales y extranjeros.

Con este objetivo en mente, por iniciativa del Consejo Coordinador Empresarial, se formó un Comité de Mejores Prácticas Corporativas integrado por miembros representativos de los sectores: industrial, gubernamental, financiero y servicios, entre otros.

A continuación se muestran algunos de las empresas que tienen representación el Comité:

- Grupo BAL
- Consejo Coordinador Empresarial
- Instituto Mexicano de Contadores Públicos
- Asociación de Banqueros de México

- Instituto Mexicano de Ejecutivos de Finanzas
- Profesores de Universidades
- Profesionistas Independientes
- Bolsa Mexicana de Valores
- Grupo DESC
- Grupo CARSO
- Comisión Nacional Bancaria y de Valores
- Banco de México
- Secretaria de Hacienda y Crédito Público

La primera labor de este Comité consistió en analizar experiencias internacionales sobre mecanismos que han logrado dar a conocer de manera transparente la información acerca del manejo de las empresas. Se encontró que el medio más utilizado y adecuado para lograr este fin han sido los códigos de mejores prácticas, ya que en éstos se establecen principios que ayudan a lograr armonía entre los diversos participantes de las empresas mejorando así el gobierno corporativo de las mismas.

B. Concepto

Debido a lo anterior, el Comité elaboró el Código de Mejores Prácticas para México, en el cual se establecen recomendaciones prácticas y voluntarias[18], para mejorar el gobierno cooperativo de las empresas mexicanas.

Las recomendaciones del código van encaminadas a definir principios que contribuyen a mejorar el funcionamiento del consejo de administración y a la revelación información a los accionistas.

De manera específica las recomendaciones del código buscan:

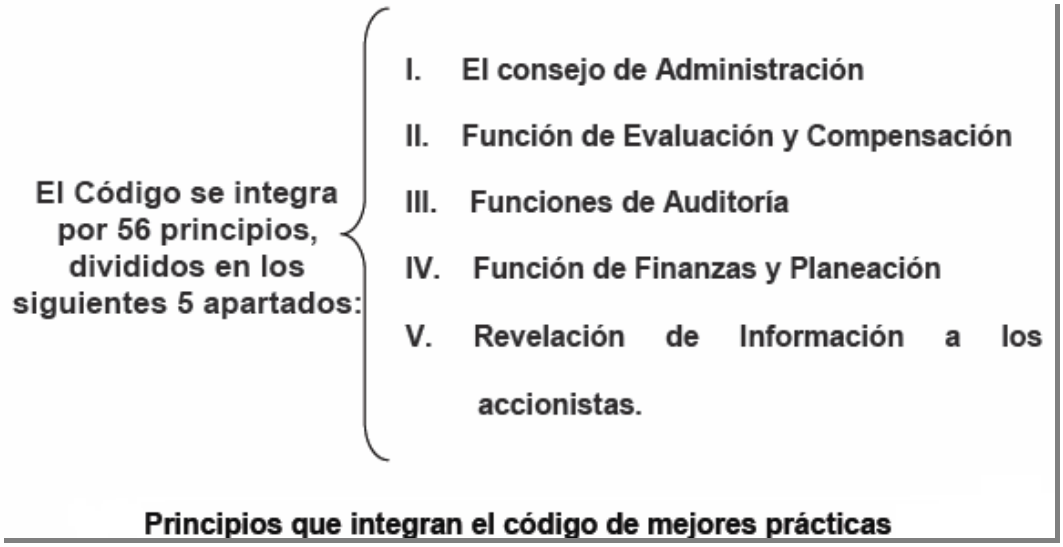
a) Que las sociedades amplíen la información relativa a su estructura administrativa.

[18] Las empresas que cotizan en la Bolsa Mexicana de Valores están obligadas a aplicar las recomendaciones del Código.

b) Que las sociedades cuenten con mecanismos que procuren que su información financiera sea suficiente.

c) Que existan procesos que promuevan la participación y comunicación entre los consejeros.

d) Que existan procesos que fomenten una adecuada revelación a los accionistas.



Principios que integran el código de mejores prácticas

I. El Consejo de Administración Dentro de este apartado se señalan recomendaciones en relación con las funciones, integración, estructura y operación de los consejos de administración, así como también de los deberes de los consejeros.
II. Función de Evaluación y Compensación El Comité recomienda que exista un mecanismo que apoye al consejo de administración en el cumplimiento de la función de evaluación y compensación del director general y de los funcionarios de alto nivel de la empresa.
III. Función de Auditoría

El Comité recomienda que exista un mecanismo que apoye al Consejo en la verificación del cumplimiento de la función de auditoría, asegurándose que las auditorías interna y externa se realicen con la mayor objetividad posible y que la información financiera sea transparente, suficiente y refleje adecuadamente la posición financiera de la empresa.

Controles Internos

En este apartado el código hace recomendaciones en relación con el control interno. En este sentido, el código recomienda la implementación de los siguientes principios:

El sistema de control interno constituye el medio por el cual el consejo asegura que la sociedad opere en un ambiente general de control. Dicho sistema da mayor certeza de que lo acordado por el consejo está siendo llevado a cabo adecuadamente.

Principio 41. Sugiere que se someta a la aprobación del consejo de administración los lineamientos generales del sistema de control interno.

Es importante que los accionistas tengan información sobre la existencia de procesos definidos dentro de los cuales la sociedad opera, ésta cuenta con un proceso administrativo ordenado y que se tengan control adecuado de los activos. Para cumplir con lo anterior los reportes emitidos por los auditores externos e internos pueden servir de apoyo para verificar la efectividad del sistema de control.

Principio 42. Sugiere que se apoye al consejo evaluando la efectividad del sistema de control interno, se emita una opinión sobre los controles financieros y operacionales.

Principio 43.-Sugiere que los auditores externos validen la efectividad del sistema de control interno y emitan un reporte respecto a dichos controles. Se sugiere que la empresa además de dictaminar sus EEFF, contrate específicamente a un contador público independiente (diferente al que le realiza la auditoría de EEFF) para examinar e informar sobre la efectividad del sistema de control interno.
IV. Función de Finanzas y Planeación El comité recomienda que exista un mecanismo que apoye al consejo en la función de finanzas y planeación, en especial en la evaluación de la estrategia a largo plazo del negocio, las principales políticas de inversión y financiamiento. Para cumplir con dicha función se puede apoyar en las estructuras internas de la empresa como lo es el área de finanzas.
V. Revelación de Información a los accionistas Esta sección contiene las recomendaciones aplicables a la información que se presenta a los accionistas a través de las asambleas ordinarias y extraordinarias.

Gobierno Corporativo

Concepto

El gobierno corporativo es, en esencia, la forma en que la entidad se gobierna; es decir, la manera en que el consejo de administración o el órgano supremo (en el caso de entidades gubernamentales) determina el rumbo de la organización, y la forma en que se asegura que esas determinaciones se lleven a cabo. Para ello, monitorea la gestión de la administración general considerando, como uno de los aspectos más importantes, su reacción a los riesgos que pudieran afectar el logro de los objetivos de la entidad (véase, Gutiérrez, 2005).

A través del buen gobierno corporativo, "los intereses se alinean, **las responsabilidades se distribuyen**, **los conflictos** se identifican, se dan a conocer, se les da seguimiento y **se resuelven"** (Cevallos y Cruz, 2003).

Objetivos

El gobierno corporativo busca:

a) La transparencia, objetividad, equidad en el trato de los socios y accionistas de una entidad.
b) La gestión de su junta directiva.
c) La responsabilidad social de sus organismos de control, frente a los grupos de interés como clientes, proveedores, empleados, inversionistas y sociedad en general.

El concepto de gobierno corporativo plantea un **consejo de administración activo** que, a través de comités como el de auditoría, mantengan una estrecha supervisión de la administración de la empresa.

El manejo del gobierno corporativo no implica una doble administración sino por el contrario, una administración fortalecida que cuenta con un proceso de seguimiento, asesoría, soporte respecto al desarrollo y resultado de la empresa.

La Organización para la Cooperación y el Desarrollo Económico (OCDE) emitió en mayo de 1999 sus principios de gobierno corporativo y en términos generales, considera que el marco de gobierno corporativo de una empresa debe:

- Proteger a todos sus accionistas y asegurar un trato equitativo para todos ellos, inclusive minoritario y extranjero.
- Reconocer los derechos de los terceros interesados.
- Revelar de manera precisa y oportuna los asuntos importantes que incidan en el logro de los objetivos del negocio.
- Ser un guía estratégico y efectivo, monitoreando la administración de la empresa.
- En relación con los consejos de administración (en adelante: consejo), señala que las funciones específicas de sus miembros difieren de acuerdo con las leyes de cada país y los estatutos de cada compañía, sin embargo, es importante incluir como funciones los siguientes puntos

  - Revisión y dirección de: los planes de acción principales, políticas de riesgos, presupuestos anuales, planes de negocio y supervisión de gastos mayores e inversiones.
  - Selección, monitoreo, reemplazo de ejecutivos clave y supervisión de los planes de sucesión.
  - Revisión de remuneraciones de ejecutivos clave y de los miembros del consejo, asegurándose que la nominación de estos últimos sea formal y transparente.
  - Supervisión de conflictos de interés de la alta dirección, de miembros del consejo y accionistas, incluyendo uso indebido de los activos de la compañía.

- Asegurar la integridad de los sistemas de información contable y financiera de la empresa, incluyendo la auditoría externa.
- Asegurar una infraestructura de control interno adecuada y suficiente para las necesidades de la organización, garantizando una administración y control efectivo del riesgo.
- Implantar un comité de auditoría que asegure prácticas efectivas de gobierno corporativo que permitan la adecuada supervisión de la administración de la empresa. El Comité deberá contar con la participación de consejeros independientes a la organización.
- Conocer y supervisar adecuadamente la documentación de procesos y sus niveles de cumplimiento.
- Supervisar los niveles de cumplimiento de las leyes aplicables a la empresa.
- Asegurar un proceso suficiente y correcto de revelación de información al interior y exterior de la empresa.

En muchos casos los integrantes del consejo no tienen el tiempo suficiente y la metodología para cumplir con estas responsabilidades, por eso es de suma importancia que los consejeros implanten y soporten el funcionamiento de un comité de auditoría que cuente con la participación de un grupo de profesionales en la materia que asegure y facilite el buen desempeño de las responsabilidades, haciendo sencillo el conocimiento así como seguimiento de asuntos por parte de los integrantes del Consejero.

El gobierno corporativo implica tener a los dueños, directores y personal trabajando juntos por el buen desarrollo de la empresa.

Importancia

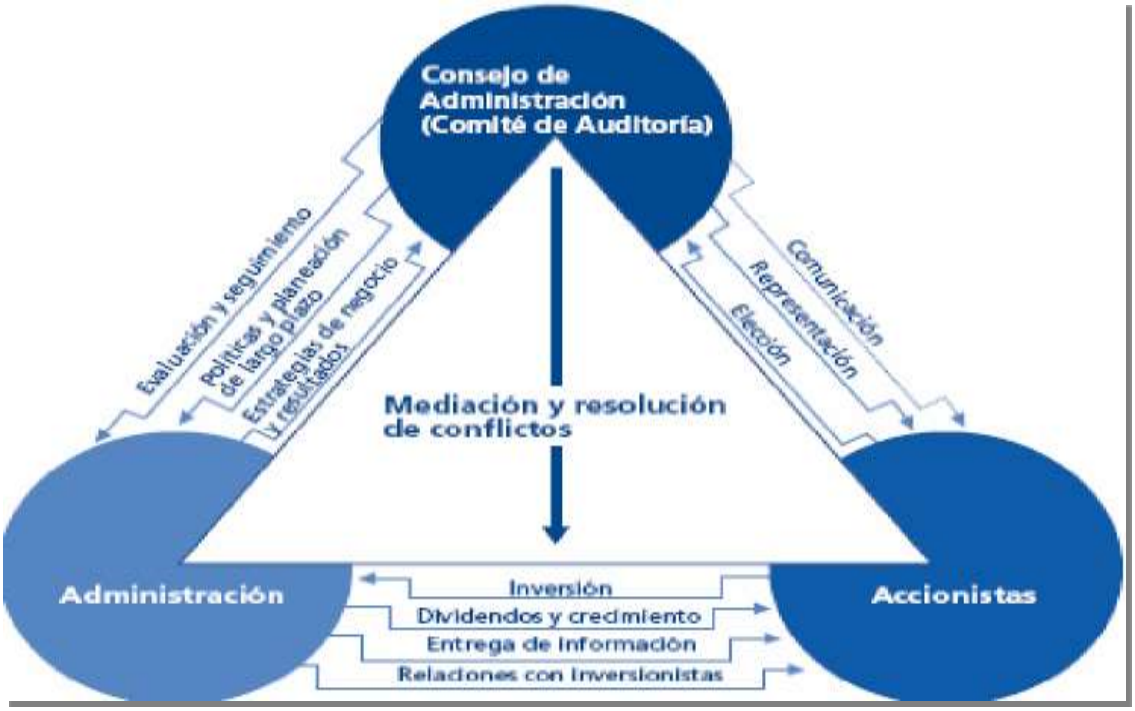
Por lo general los directores generales (o CEO's llamados así por sus siglas en inglés) tienen cierta tendencia en participar y ser los promotores de organizaciones que tengan resultados de corto plazo, mientras que los inversionistas tradicionalmente buscan un negocio estable, productivo y de largo plazo.

El gobierno corporativo existe para mediar intereses y sacar el mayor beneficio de ambas posiciones, las cuales no son excluyentes en sí mismas.

Algunos de los objetivos corporativos en los que existe una posición de conflicto natural entre la administración de la empresa y los accionistas, son:

- Quién y cómo se mantiene el control de la empresa, cuál es el verdadero marco de medición respecto a la efectividad del negocio.
- Cuál es la estructura y naturaleza de capital, inversiones de activo y pasivos que se deben mantener.
- Rentabilidad que debe esperarse en este ejercicio vs. rentabilidad de futuros ejercicios.
- Nombramiento de directores o gerentes clave.
- Cuáles son los derechos de los accionistas y consejeros, principalmente respecto a la administración del negocio.

El siguiente esquema permite identificar las distintas interrelaciones entre los accionistas, el consejo y la administración de la empresa.



Triángulo del gobierno corporativo

El triángulo del gobierno corporativo nos permite identificar claramente las distintas interrelaciones entre los accionistas, el consejo y la administración de la empresa. ¿Quién gobierna y cómo? Es importante recordar siempre que: **los inversionistas son dueños; los directores y gerentes trabajan para los dueños**.

Un gobierno corporativo efectivo, en sí mismo adiciona valor al desarrollo de corto plazo en la compañía y al mismo tiempo genera mayores elementos de valor en el precio de la acción. Así mismo, identifica y reduce aquellas posibilidades de que se presenten riesgos de eventos negativos que limiten o reduzcan el logro de objetivos de negocio (véase, Cevallos y Cruz, 2003).

Ley del mercado de valores

[Vigente]

Concepto

La ley del Mercado de Valores (LMV) Fue decretada por el Presidente Vicente Fox Quezada el 28 de diciembre de 2005, regula las compañías que cotizan en la Bolsa Mexicana de Valores, contempla situaciones similares a la ley Sarbanes-Oxley.

Estructura

La LMV se integra de 423 artículos contenidos en 16 títulos, como se muestra a continuación:

Título I	Disposiciones preliminares
Título II	De las sociedades anónimas del mercado de valores
Título III	De los certificados bursátiles, títulos opcionales y otras disposiciones
Título IV	De la inscripción y oferta de valores
Título V	De las adquisiciones de valores objeto de revelación
Título VI	De los intermediarios del mercado de valores
Título VII	De los asesores en inversiones
Título VIII	De los organismos auto rregulatorios
Título IX	De los sistemas de negociación bursátiles y extrabursátiles
Título X	Del depósito, liquidación y compensación de valores
Título XI	De otras entidades que participan en el desarrollo del mercado de valores
Título XII	De la auditoría externa y otros servicios
Título XIII	De las autoridades financieras
Título XIV	De las infracciones y prohibiciones de mercado y de los delitos
Título XV	De los procedimientos administrativos
Título XVI	Disposiciones finales

Objetivo

El objetivo de esta ley es desarrollar un mercado de valores equitativo, eficiente y transparente; proteger los intereses del público inversionista; minimizar el riesgo sistémico; fomentar una sana competencia.

La LMV regula:

I. La inscripción, actualización, suspensión, cancelación de la inscripción de valores en el Registro Nacional de Valores y la organización de éste.
II. La oferta e intermediación de valores.
III. A las sociedades anónimas que coloquen acciones en el mercado de valores bursátil y extrabursátil.
IV. Las obligaciones de las personas morales que emitan valores, así como de las personas que celebren operaciones con valores.
V. La organización y funcionamiento de las casas de bolsa, bolsas de valores, instituciones para el depósito de valores, contrapartes centrales de valores, proveedores de precios, instituciones calificadoras de valores y sociedades que administran sistemas para facilitar operaciones con valores.
VI. El desarrollo de sistemas de negociación de valores que permitan la realización de operaciones con éstos.
VII. La responsabilidad en que incurrirán las personas que realicen u omitan realizar los actos o hechos que esta ley sanciona.
VIII. Las facultades de las autoridades en el mercado de valores.

Disposiciones en materia de Gobierno corporativo y auditoría

En materia de gobierno corporativo la LMV contempla los siguientes cambios, (véase, Salazar, 2005)

a) Modificar las funciones del consejo de administración de las sociedades anónimas bursátiles, estableciendo que el Consejo se convertirá en un órgano de vigilancia, establecerá las estrategias generales para la buena y sana conducción del negocio.

b) El director general de estas sociedades será el responsable de la gestión, conducción y ejecución de los negocios de manera cotidiana; de la existencia y

mantenimiento de los sistemas de contabilidad, control y registro; del cumplimiento de los acuerdos del consejo y de la asamblea así como de la revelación de información relevante.

c) Desaparece la figura del comisario y las funciones de vigilancia se distribuyen entre el consejo de administración, los comités de auditoría y el auditor externo.

d) La vigilancia de las sociedades anónimas bursátiles y de las personas morales que éstas controlen estará a cargo del consejo de administración mediante el o los comités que se establezcan, así como por la firma que realice la auditoría externa de la sociedad.

e) Los comités estarán integrados por consejeros independientes que no tengan conflicto de intereses garantizando, con esto la imparcialidad de sus recomendaciones. Si el consejo no acatara las recomendaciones del comité, este hecho debe ser revelado a los inversionistas. La función y responsabilidad de los consejeros así como directivos es procurar la creación de valor en beneficio de la sociedad, actuar con lealtad y diligencia.

En materia de gobierno corporativo la LMV contempla los siguientes cambios:

Algunas disposiciones en relación con la función de auditoría externa las establecidas en la LMV son:
Los auditores externos, socios de una firma de Contadores Públicos, deberán ser **honorables**, cumplir con los requisitos personales y profesionales que señale la Comisión Nacional Bancaria y de Valores (CNBV), así como con los requisitos de control de calidad que establezca dicha Comisión.

Tanto la firma, socios de ésta así como el personal que forme parte del equipo de auditoría deberán ser **independientes**.

Por ejemplo, no tener relación de dependencia económica, relaciones financieras, prestar servicios adicionales a los de auditoría y no exceder de determinado número de años como auditor externo:

Se adecua el régimen de infracciones y sanciones, para considerar como delitos graves, algunas conductas que actualmente no se consideran como tales, por ejemplo:

- Los auditores externos responderán por los daños y perjuicios que ocasionen cuando por negligencia inexcusable, el dictamen que proporcionen:

  - Contenga vicios u omisiones que en razón de su profesión.
  - Intencionalmente omitan información relevante de la que tengan conocimiento.
  - Incorporen información falsa o que induzca a error.
  - Sugieran o acepten que una determinada transacción se registre en contravención de las bases contables correspondientes.

- Los auditores externos serán sanciones con prisión de dos a diez años, cuando:

  - Alteren los registros contables.
  - Destruyan u ordenen que se destruyan total o parcialmente, información, documentos o archivos, incluso electrónicos, con el propósito de impedir u obstruir los actos de supervisión de la comisión.
  - Presenten a la comisión documentos, información falsa, alterada con el objeto de ocultar su verdadero contenido o contexto, asienten o declaren ante ésta hechos falsos.

- El auditor externo será sancionado con multa de 200 a 10,000 días de salario cuando omita suministrar a la CNBV los informes, opiniones y demás elementos de juicio en los que sustenten sus dictámenes así como conclusiones.

- Se considera que no se incurrirá en responsabilidad por los daños o perjuicios que ocasionen, cuando los auditores externos actuando de buena fe y sin dolo, rindan su dictamen u opinión:

  - Con base en información proporcionada por la persona a la que otorguen sus servicios.
  - Estén apegados a los procedimientos y, en su caso, metodologías, con que cuenten para realizar el análisis, evaluación o estudio que corresponda a su profesión.

En conclusión con esta ley se mejoran no sólo las prácticas relacionadas con gobierno corporativo, sino que también se establecen reglas precisas respecto a la actuación del auditor externo, con lo cual se motiva al auditor externo a mantener los altos niveles de calidad, ética, independencia y profesionalismo, se fomenta el establecimiento de políticas sanas en las empresas, por lo tanto se brinda mayor protección a los inversionistas.

Informe sobre el examen del control interno relacionado con la preparación de la información financiera

Como se vio anteriormente, la sección 404 de la Ley SOX requiere que la administración evalúe e informe de la efectividad del control interno de una compañía sobre la cuestión financiera. Esta sección señala que el auditor externo será quien deberá llevar a cabo la revisión del control interno hecho por la administración y emitir un informe sobre dicha evaluación.

En este sentido la Comisión de Normas y Procedimientos de Auditoría del IMCP emitió en diciembre de 2006 el boletín 7030 Informe sobre el examen del Control Interno relacionado con la preparación de Información financiera.

El boletín 7030 entro en vigor el 1 de enero de 2007 establece las normas y proporciona guías al contador público (auditor) que es contratado para examinar e informar sobre la efectividad del diseño y operación del sistema de control interno relacionado con la información financiera a una fecha o periodo determinado.

El objetivo de la auditoría del examen del control interno sobre información financiera es expresar una opinión profesional sobre la evaluación de la administración acerca de la efectividad del control interno sobre información financiera de la entidad.

De acuerdo con este boletín para tener una base para expresar una opinión, el auditor externo debe planear y realizar una auditoría, de tal forma que le permita obtener una seguridad razonable acerca de si la entidad mantiene, en todos los aspectos importantes, un control interno efectivo sobre la información financiera a la fecha especificada en la evaluación de la administración.

Para llevar a cabo su revisión el auditor deberá evaluar:

- El diseño y la efectividad operativa del control interno de la entidad.
- El diseño y la efectividad operativa del control interno de un componente de la entidad. Por ejemplo de un área operativa como el área de compras.
- La efectividad del diseño del control interno de una entidad.
- El diseño y la efectividad operativa del control interno de la compañía basado en el criterio de alguna entidad regulatoria. Por ejemplo: En el caso de un banco podrían ser los criterios emitidos por la CNBV.

El auditor que realice un trabajo de esta naturaleza deberá cumplir con las normas para atestiguar (serie 7000 de las Normas y Procedimientos de Auditoría).

El auditor deberá comunicar el resultado de su trabajo al comité de auditoría, al consejo de administración o en su caso al funcionario de mayor nivel jerárquico en la organización. Esta comunicación deberá hacerse por escrito, siguiendo los formatos de informes que se incluyen en este Boletín para tales efectos.

Con la emisión de este boletín, la CONPA permite que este tipo de trabajos que realiza el contador público se lleven a cabo considerando criterios mínimos de aplicación, sin dejar de considerar que cada empresa es diferente y por lo tanto el auditor tendrá que aplicar su juicio profesional en la evaluación de los controles.

RESUMEN

Con el surgimiento de la Ley *Sarbanes-Oxley* de organismos de vigilancia, como el PCAOB, EEUU ha dado un paso muy importante para monitorear y revisar a las compañías públicas que cotizan en sus mercados de valores, con el objeto de disminuir las incidencias de fraude corporativo perfilado contra los inversionistas.

Estas nuevas disposiciones han fomentado el establecimiento de una nueva figura corporativa en las empresas conocido como gobierno corporativo, además del apego a mejores prácticas corporativas y a la creación de los comités de auditoría que fortalecen la función del consejo de administración y, por lo tanto, la confianza de los inversionistas (véase, Soto, 2005).

Nuestro país también está trabajando en materia de regulación de las empresas que cotizan en la bolsa, la emisión de la circular única, así como del código de mejores prácticas, son un ejemplo de nuevas disposiciones que ayudarán a las empresas a ser más transparentes y a hacer más eficiente la calidad de su administración.

En diciembre de 2005 entró en vigor la *ley del mercado de valores* que regula a las compañías que cotizan en la Bolsa Mexicana de Valores. Dicha Ley contempla situaciones similares a las de la Ley *Sarbanes-Oxley*, tiene por objeto desarrollar el mercado de valores en forma equitativa, eficiente y transparente; proteger los intereses del público, fomentar un buen gobierno corporativo así como establecer responsabilidades y sanciones específicas para la función de auditoría externa.

BIBLIOGRAFÍA

SUGERIDA

Autor	Capítulo	Páginas
IMCP (Normas de Auditoría y Normas para Atestiguar)	Boletín 7030 Informe sobre examen del control interno relacionado con la preparación de la información financiera	N/A

Instituto Mexicano de Contadores Públicos. (2006). *Normas y procedimientos de auditoría y normas para atestiguar*. (26ª ed.) México: IMCP. [En 2010 la versión las llama Normas Internacionales de Auditoría, ISA, del inglés. De cualquier manera, **siempre consultar las vigentes**.]

Facultad de Contaduría y Administración
Sistema Universidad Abierta y Educación a Distancia