

EL CONTROL INTERNO - COSO (CONCEPTOS BÁSICOS)

Por M.Sc. Pedro Bejarano Velásquez



1. Introducción

Los problemas de fraude y corrupción han existido desde que se inició la actividad comercial como tal en el mundo, no obstante la llegada y consolidación de la globalización (finales del siglo XX), también ha influido en el aumento de los problemas de corrupción y fraudes detectados en las empresas y organizaciones, que han involucrado incluso corporaciones internacionales. Los negocios pueden verse afectados por diferentes tipologías de fraude, en mayor o menor medida, dependiendo del sector en el que operan, involucrando en muchos casos a directivos y profesionales de la contabilidad y auditoría; de hecho, entre los casos más conocidos de fraude y corrupción, en las últimas décadas, podemos citar:

Cendant (Años 90)

Cendant se convirtió en el mayor fraude de los años 90, con casi 17.000 millones de euros; protagonizó el primer gran escándalo corporativo en Wall Street, antes de que salieran de debajo de las alfombras los fraudes en la eléctrica Enron y la telefónica WorldCom, que minaron la confianza de los inversores y obligaron a las autoridades reguladoras en todo el mundo a reforzar las normas contables (utilizó una contabilidad falsa para aumentar las ganancias reportadas de la compañía).

Enron (2001)

La mayor empresa distribuidora de energía de EEUU ocultó durante años sus pérdidas millonarias. Los balances falsificados de la empresa, ascendían a 74.000 millones de dólares. Es considerado como el mayor fraude corporativo en la historia de los Estados Unidos. Uno de los acreedores de Enron en 2001, fue Lehman Brothers. El banco recibió una compensación de 195 millones de euros antes de que quebrara en 2008.

Worldcom (2002)

Worldcom fue una empresa importante del sector de las telecomunicaciones con sede en Estados Unidos, que se declaró en quiebra en julio del año 2002, protagonizando uno de los mayores escándalos financieros de la llamada globalización de capitales. Worldcom se situaba como la segunda telefónica más importante de EE.UU, y llevó a cabo la falsificación de sus cuentas (escándalo contable en apenas un año) por una cantidad aproximada de 4.000 millones de dólares. Pérdidas estimadas: 107.000 millones de dólares en activos. Según destaparon las investigaciones el cerebro encargado de este "maquillaje" de los estados contables fue Bernard Ebbers (fue condenado en 2005 a 25 años de prisión).

Merck (2002)

El laboratorio Merck, a mediados de 2002 registró como ingresos de una de sus filiales (Medco) 14.340 millones de euros que no recibió, con la finalidad de equilibrar las cuentas, pero el ingreso no le pertenecía por lo que adoptó la cifra solo para inflar las ganancias.

Parmalat (2003)

A principios de diciembre de 2003, el grupo Parmalat se vio obligado a revelar un agujero en sus cuentas (doble contabilidad) que alcanzaban a 4.000 millones de euros, al demostrarse falsa, en un documento del Bank of America, una financiación desde las Islas Caimán.

Jérôme Kerviel - Société Générale (2007)

Es considerado el artífice del mayor fraude de la historia, causando unas pérdidas a Société Générale (uno de los bancos más grandes de Europa) por más de 6.100 millones de dólares. Esto dio lugar a un desajuste financiero que hizo tambalearse los mercados en todos los continentes. A lo largo de 2007 Jérôme llevó a cabo operaciones especulativas que pasaron inadvertidas por el banco gracias a que empleó un complejo sistema para ocultar operaciones bajo falsas transacciones. En conclusión, apostó una suma asombrosa a que ciertas acciones subirían o bajarían y falló estrepitosamente.

Bernard Madoff Investment Securities (2009)

Como resultado de la crisis financiera (2008), el FBI descubrió el fraude sistemático de Bernard Madoff. Durante más de 50 años administró un fondo de inversión basado en un sistema Ponzi ilegal (estafa piramidal), una forma de fraude que atrae a los inversores a pagar beneficios a los inversores anteriores con fondos de inversiones más recientes. Consiguió malversar más de 64.000 millones de dólares. La corte suiza estima que en 2009 alrededor de 3 millones de personas en todo el mundo se vieron directa o indirectamente afectadas por el fraude de Madoff. En 2009 Fue condenado a 150 años de prisión.

Las distintas formas que adoptan estas irregularidades, casi siempre relacionadas al control interno, tienen características y consecuencias diferentes como: alteración de la información financiera, sobrevaloración y subvaloración de ingresos y gastos, registro de ingresos y gastos en períodos incorrectos, gastos y pasivos ocultos, etc.; por lo que se requieren métodos de prevención y detección adaptados a cada caso,

Como consecuencia de los problemas de corrupción y fraudes detectados en las organizaciones en los últimos años (algunos de los cuales ya citamos), se ha fortalecido e implementado el control interno en diferentes países. Está claro que no es un tema inherente solamente a los contadores, sino también una responsabilidad de los miembros de los consejos de administración y dirección de las organizaciones. A partir de ello es que se han trabajado diferentes modelos de control, como COSO (EE.UU.) y COCO (Canadá), aunque existen muchos más, como por ejemplo: Cadbury (Reino Unido); Vienot (Francia), Peters (Holanda), King (Sudáfrica); MICIL (Marco Integrado de Control Interno Latinoamericano), etc.

2. El Modelo COSO

2.1. El Origen del Estudio COSO - Comité de Organizaciones Patrocinadoras de la Comisión Treadway (Committee of Sponsoring Organizations of the Treadway Commission)

Por el año 1985 en EEUU se formó la Comisión Nacional para Emisión de Informes Fraudulentos, conocida como la Treadway Commission, a fin de identificar las causas de proliferación de informes fraudulentos; en 1987 esta comisión solicitó realizar un estudio para realizar un estudio con la finalidad de desarrollar una definición común de control interno y un marco conceptual sobre el mismo.

En 1988, el Comité de Organizaciones Patrocinadoras de la Comisión Treadway (Committee of Sponsoring Organizations of the Treadway Commission), conocido como COSO, seleccionó a Coopers & Lybrand¹ para estudiar el control interno.

¹ Coopers & Lybrand puede rastrear su historia hacia 1854. Cooper Brothers & Co se inició cuando William Cooper (1826 – 1871), comenzó su firma de contabilidad. A él se unieron sus hermanos

El Modelo COSO, (**Committee of Sponsoring Organizations of the Treadway Commission**) – Comité de Organizaciones Patrocinadoras de la Comisión Treadway, comisionado por los cinco organismos profesionales financieros más importantes de los Estados Unidos, fue definido en 1992, tras cinco años de estudio y discusión, de modo que surgió un nuevo marco conceptual del control interno, publicado en el documento “**Enfoque Integrado de Control Interno**” – **Integral Control – Integrated Framework**” (conocido como COSO I), con el objetivo fundamental de integrar las diversas definiciones y conceptos vigentes en ese momento; este enfoque de control interno reconocido internacionalmente, fue adoptado por el sector público y privado en USA, por el Banco Mundial y el BID, habiéndose extendido rápidamente por todo Latino América; de hecho aplicable también en nuestro país.

2.2. El Comité de Organizaciones Patrocinadoras de la Comisión Treadway (Committee of Sponsoring Organizations of the Treadway Commission)

El Comité estaba conformado por cinco instituciones representativas en Estados Unidos en el campo de contabilidad, finanzas y auditoría interna:

- American Accounting Association – AAA – Asociación de Contadores Públicos Norteamericanos
- American Institute of Certified Public Accountants – AICPA – Instituto Norteamericano de Contadores Públicos Certificados: Contadores CPA que forman parte de empresas de contabilidad que hacen auditorías externas de estados financieros.
- Financial Executive Institute – FEI – Asociación internacional de Ejecutivos de Finanzas:
- Institute of Internal Auditors – IIA – Instituto de Auditores Internos: Auditores encargados de la evaluación de los sistemas de control interno en el interior de las organizaciones.
- Institute of Management Accountants – IMA – Instituto de Contadores Empresariales: Contadores que trabajan en empresas.

“A nivel organizacional, se realiza la necesidad de que la alta dirección y el resto de la organización comprendan cabalmente la trascendencia del control interno, su incidencia sobre los resultados de la gestión, el papel estratégico de la auditoría y, esencialmente, la consideración del control como un proceso integrado a las operaciones de la empresa y no como un conjunto de reglas” (OLACEFS, 2015).

Luego de más de 25 años de aplicación del primer informe de COSO, se actualizaron e implementaron 3 modelos más: COSO 2 (2004), COSO 3 (2013) y COSO 4 (2017); cuyos contenidos y componentes se resumen a continuación:

años más tarde. En 1997 se fusiona con la firma Price Waterhouse y Coopers; considerándose hoy en día una de las firmas de auditoría más grandes del mundo.

2.3. COSO I (1992)

Componentes

En el informe original, COSO identificó los **cinco componentes** de control interno:

1. Ambiente de control

Es la base del sistema de control interno, y aporta disciplina a la estructura. En él se apoyan los restantes componentes y resulta fundamental para concretar los cimientos de un control interno eficaz y eficiente, pues marca la pauta del funcionamiento de la organización e influye en la forma de actuación de sus funcionarios. **Es la actitud general de sus administradores y empleados hacia la importancia del control interno.**



El entorno de control marca la pauta del funcionamiento de una organización e influye en la concienciación de sus empleados respecto al control. Es la base de todos los demás componentes del control interno, aportando disciplina y estructura. (Coopers & Lybrand. 2007)

Consiste en acciones, políticas y procedimientos que reflejan las actitudes generales de los altos niveles de la administración, directores y propietarios de una entidad en cuanto al control interno y su importancia para la organización, tiene gran influencia en la manera como se estructuran las actividades de una empresa, se establecen los objetivos y se valoran los riesgos.

En el ambiente de control se distinguen **siete factores** a considerar:

- a) Integridad y valores éticos;
- b) Compromiso por la competencia;
- c) Consejo de directores o comité de auditoría;
- d) Filosofía y estilo operativo de la gerencia;
- e) Estructura organizacional;
- f) Asignación de autoridad y responsabilidades y;
- g) Políticas y procedimientos de recursos humanos.

a) Integridad y valores éticos:

Son el resultado de las normas éticas y de conducta de la empresa, así como la forma en que éstos se comunican y refuerzan en la práctica. Incluyen las acciones de la administración para eliminar o reducir iniciativas o tentaciones que podrían llevar al personal de la empresa a cometer actos deshonestos, ilegales o poco éticos.

b) Compromiso por la competencia:

Cuando se habla de competencia se hace referencia al conocimiento y las habilidades que son necesarias para cumplir con una determinada tarea. Cada individuo que hace

vida profesional dentro de una empresa posee una serie de habilidades y destrezas, que al combinarlas con sus conocimientos sobre un área le permite ejecutar una actividad dentro de una empresa. Arens, Elder y Beasley (2007) “el compromiso con la competencia comprende la consideración de los niveles de competencia para trabajos específicos y la forma en que estos niveles se traducen en habilidades y conocimientos necesarios”.

c) *Consejo de directores o comité de auditoría:*

Este debe integrarse con miembros independientes que no sean funcionarios ni empleados y que tampoco tengan otras relaciones con la empresa que puedan desviar su independencia, ya que de esta manera podrá cumplir con su función de supervisión sobre los reportes financieros, e impedir que los ejecutivos dejen a un lado los controles existentes y se comentan actos deshonestos.

d) *Estructura organizacional:*

Se considera otro factor del ambiente de control, ya que una estructura organizacional bien diseñada ofrece la base para planear, dirigir y controlar las operaciones. Es considerada el marco de la planeación y control de las operaciones.

e) *Filosofía y estilo operativo de la gerencia:*

Abarca el enfoque de la gerencia para monitorear riesgos del negocio; las actitudes y acciones de la gerencia hacia el reporte financiero y hacia el procesamiento de la información, funciones contables y el personal

f) *Asignación de autoridad y responsabilidad:*

Incluye cómo se asignan la autoridad y responsabilidad por las actividades operativas y cómo se establecen las relaciones de reporte y las jerarquías de autorización.

2. Evaluación de riesgos:

Según Mantilla (2016), el significado de la valoración de riesgos se orienta en la siguiente idea: “La valoración de riesgos es la identificación y análisis de los riesgos relevantes para la consecución de los objetivos, formando una base para la determinación de cómo deben administrarse los riesgos. Dado que las condiciones económicas, industriales, regulatoras y de operación continuarán cambiando, se necesitan mecanismos para identificar y tratar los riesgos especiales asociados con el cambio”.

Todas las empresas, independientemente de su tamaño, estructura, naturaleza o clase de industria, enfrentan riesgos en todos los niveles. Los riesgos afectan la destreza de la entidad para sobrevivir. Por lo que, la identificación de los objetivos es una condición previa para la valoración de riesgos. Primero, deben definirse los objetivos a fin de que la administración pueda



identificar los riesgos y determinar las acciones necesarias para administrar. La definición de objetivos es una parte clave del proceso administrativo por ser requisito previo para un control interno eficaz.

La evaluación de los riesgos consiste en la identificación y el análisis de los riesgos relevantes para la consecución de los objetivos, y sirve de base para determinar cómo han de ser gestionados los riesgos. Debido a que las condiciones económicas, industriales, legislativas y operativas seguirán cambiando continuamente, es necesario disponer de mecanismos para identificar y afrontar los riesgos asociados con el cambio. (Coopers & Lybrand. 2007)

De acuerdo a Whittington y Pany (2005), los siguientes factores podrían indicar un mayor riesgo a la empresa:

- Cambios en el ambiente de operaciones;
- Personal nuevo;
- Sistemas de información nuevos o reconstruidos;
- Crecimiento rápido;
- Tecnología nueva;
- Líneas de productos o actividades nuevas;
- Reestructuración corporativa;
- Operaciones en el extranjero

3. Actividades de control:

Las actividades de control son las políticas y los procedimientos que ayudan a asegurar que se llevan a cabo las instrucciones de la dirección. Ayudan a asegurar que se toman las medidas necesarias para controlar los riesgos los riesgos relacionados con la consecución de los objetivos de la entidad. Hay actividades de control en toda la organización, a todos los niveles y en todas las funciones. (Coopers & Lybrand. 2007)

Las actividades de control consideradas en la estructura conceptual integrada COSO son las siguientes:

Revisiones de alto nivel: Incluye la comparación del desempeño contra presupuestos, pronósticos, etc.

Procesamiento de la información: Se realiza una variedad de controles a fin de verificar la precisión, integridad y autorización de las transacciones.

Funciones directas o actividades administrativas: Los administradores dirigen las funciones o las actividades revisando informes de desempeño.

Controles físicos: Equipos, inventarios y otros activos se aseguran físicamente en forma periódica son contados y comparados con las cantidades presentadas en los registros de control.

Indicadores de desempeño: Relacionar unos con otros los diferentes conjuntos de datos operacionales o financieros, además de analizar las interrelaciones e investigar y corregir las acciones.

Segregación de responsabilidades: Para reducir el riesgo de error o de acciones inapropiadas. Para ello existen cuatro guías generales que orientan la segregación adecuada de las responsabilidades:

- 1) Contabilidad separada de la custodia de los activos financieros;
- 2) Custodia de activos relacionados separados de la autorización de operaciones;
- 3) Responsabilidad operativa separada de la responsabilidad de registro contable;
- 4) Deberes y responsabilidades del departamento de tecnología de información separado de los departamentos de usuarios.

4. Información y comunicación:

La información y la comunicación son elementos esenciales en una estructura de control interno. La información acerca del ambiente de control, la evaluación de los riesgos y los procedimientos de control y la supervisión son necesarios para que los administradores puedan dirigir las operaciones y garantizar que sean puestas en práctica las normativas legales, reglamentarias y de información. Este componente de control interno, se refiere a los métodos empleados para identificar, reunir, clasificar, registrar e informar acerca de las operaciones de la entidad y para conservar la contabilidad de los activos relacionados.

Hay que identificar, recopilar y comunicar información pertinente en forma y plazo que permitan cumplir a cada empleado con sus responsabilidades. Los sistemas informáticos producen informes que contienen información operativa, financiera y datos sobre el cumplimiento de las normas que permite dirigir y controlar el negocio de forma adecuada. Dichos sistemas no sólo manejan datos generados internamente, sino también información sobre acontecimientos internos, actividades y condiciones relevantes para la toma de decisiones de gestión así como para la presentación de información a terceros. También debe haber una comunicación eficaz en un sentido más amplio, que fluya en todas las direcciones a través de todos los ámbitos de la organización, de arriba hacia abajo y a la inversa.

El mensaje por parte de la alta dirección a todo el personal ha de ser claro: las responsabilidades del control han de tomarse en serio. Los empleados tienen que comprender cuál es su papel en el sistema de control interno y cómo las actividades individuales están relacionadas con el trabajo de los demás. Por otra parte, han de tener medios para comunicar la información significativa a los niveles superiores. Asimismo, tiene que haber una comunicación eficaz con terceros, como clientes, proveedores, organismos de control y accionistas. (Coopers & Lybrand. 2007)

Con relación a este componente, Mantilla (2016) comenta: "... El sistema de información produce documentos que tienen información operacional, financiera y relacionada con el cumplimiento, la cual hace posible operar y controlar el negocio. Ella se relaciona no solamente con los datos generados internamente, sino también con la información sobre sucesos, actividades y condiciones externas necesaria para la toma de decisiones y la información externa de negocios. También debe darse una comunicación efectiva en un sentido amplio, que fluya hacia abajo, a lo largo y hacia arriba de la organización. Todo el personal debe recibir un mensaje claro por parte de la alta administración respecto a qué responsabilidades de control deben asumirse seriamente."

5. Supervisión y seguimiento (Monitoreo):

Los sistemas de control interno requieren supervisión, es decir, un proceso que comprueba que se mantiene el adecuado funcionamiento del sistema a lo largo del tiempo. Esto se consigue mediante actividades de supervisión continuada, evaluaciones periódicas o una combinación de ambas cosas. La supervisión continuada se da en el transcurso de las operaciones. Incluye

tanto las actividades normales de dirección y supervisión, como otras actividades llevadas a cabo por el personal en la realización de sus funciones. El alcance y la frecuencia de las evaluaciones periódicas dependerán esencialmente de una evaluación de los riesgos y de la eficacia de los procesos de supervisión continuada. Las deficiencias detectadas en el control interno deberán ser notificadas a niveles superiores, mientras que la alta dirección y el consejo de administración deberán ser informados de los aspectos significativos observados.

(Coopers & Lybrand. 2007)

Las actividades de monitoreo se refieren a la evaluación continua o periódica de calidad del desempeño del control interno, con el propósito de determinar qué controles están operando de acuerdo con lo planeado y que se modifiquen según los cambios en las condiciones. Mantilla (2016) "Los sistemas de control interno cambian con el tiempo. La manera como se aplican los controles tiene que evolucionar. Debido a que los procedimientos pueden tornarse menos efectivos, o quizás no se desempeñan ampliamente, ello puede ocurrir a causa de la llegada de personal nuevo, la variación de la efectividad del entrenamiento y la supervisión, la reducción de tiempo y recursos u otras presiones adicionales".

El Sistema de control interno puede supervisarse mediante acciones continuas de los administradores o por evaluaciones separadas. Las acciones de monitoreo continuo denominado "monitoreo ongoing", incluyen actos regulares de administración y supervisión, comparaciones, conciliaciones y otras acciones rutinarias. Por desempeñarse en una base de tiempo real reaccionan dinámicamente a las condiciones cambiantes y están integrados a la gestión de la organización, proporcionan una retroalimentación sobre la efectividad de los otros componentes de control interno.

Se realizan evaluaciones separadas que son necesarias para que la administración tenga una seguridad razonable respecto de la efectividad del sistema de control interno, se realizan cada cierto tiempo. Para este tipo de evaluación se debe tener presente: a) el alcance y frecuencia de la evaluación; b) el proceso de evaluación; c) La metodología de evaluación; y; d) el nivel de documentación.

Estos componentes, vinculados entre sí, generan una sinergia y forman un sistema integrado que responde de una manera dinámica a las circunstancias cambiantes del entorno. El sistema de control interno está entrelazado con las actividades operativas de la entidad y existe por razones empresariales fundamentales.

El sistema de control interno es más efectivo cuando los controles se incorporan a la infraestructura de la sociedad y forman parte de la esencia de la empresa.

Mediante controles "incorporados", se fomenta la calidad y las iniciativas de delegación de poderes, se vitan gastos innecesarios y se permite una respuesta rápida ante las circunstancias cambiantes.

(Coopers & Lybrand. 2007)

Lo que se puede lograr con el control interno

De acuerdo a lo que menciona Coopers & Lybrand (2007); el control interno puede ayudar a que una entidad consiga sus objetivos de rentabilidad y rendimiento y a prevenir la pérdida de recursos. Puede ayudar a la obtención de información financiera fiable. También puede reforzar la confianza en que la empresa cumple con las leyes y normas aplicables, evitando efectos perjudiciales para su reputación y otras consecuencias. En suma, puede ayudar a que una entidad llegue adonde quiere ir y evite peligros y sorpresas en el camino.

Lo que no se puede lograr con el control interno

Infortunadamente, algunas personas tienen expectativas mayores e irreales. Consideran que:

- *El control interno puede asegurar el éxito de una entidad, esto es, el cumplimiento de los objetivos básicos del negocio, o cuando menos, la supervivencia.* Incluso un control interno eficaz solamente puede “ayudar” a que una entidad logre sus objetivos. Puede proporcionar información administrativa sobre el progreso de la entidad, o hacia su consecución. Pero no puede cambiar una administración ineficiente por una buena. Asimismo, los cambios en la política o los programas gubernamentales, las acciones que tomen los competidores o las condiciones económicas pueden estar fuera del control de la dirección. El control interno no asegura éxito ni supervivencia.
- *El control interno puede asegurar la confiabilidad de la información financiera y el cumplimiento de las leyes y normas aplicables.* Esta convicción también es equivocada. Un sistema de control interno, no importa que tan bien ha sido concebido y operado, puede proveer solamente seguridad razonable -no absoluta- a la administración y a la junta directiva mirando la consecución de los objetivos de una entidad. Las posibilidades de éxito se ven afectadas por las limitaciones que son inherentes a todos los sistemas de control interno, por ejemplo los juicios en la toma de decisiones pueden ser defectuosos, y las fallas pueden ocurrir por simples errores o equivocaciones. Adicionalmente los controles pueden esquivarse mediante la confabulación de dos o más personas y, por otra parte la dirección tiene la capacidad de eludir el sistema. Otro factor restrictivo consiste en que el diseño de un sistema de control interno debe reflejar el hecho de que existen restricciones sobre los recursos y que los beneficios de los controles han de ser considerados con relación con los costos correspondientes.

Relación entre objetivos y componentes

Según Coopers & Lybrand (2007), existe relación directa entre los objetivos, aquellos que una entidad busca conseguir, y los componentes, aquellos que se requieren para conseguir los objetivos. Las relaciones pueden describirse mediante una matriz tridimensional, la cual es presentada en la siguiente figura.

- Las tres categorías de objetivos: operacionales, de información financiera y de cumplimiento se representan en las columnas verticales.

- Los cinco componentes se representan por filas.
- Las unidades o actividades de una entidad, las cuales el control interno relaciona, se describen mediante la tercera dimensión de la matriz.

Cada fila de componentes “cruza” las tres categorías de objetivos y es aplicable a las tres. Hay un ejemplo en forma de una sección extraída de la matriz; la información financiero y no-financiero procedente de fuentes tanto internas como externas (que es parte del componente de Información y Comunicación=) es necesaria para gestionar eficazmente las operaciones empresariales, formular estados financieros fiables y determinar si la entidad está cumpliendo la legislación aplicable. Otro ejemplo (que no es descrito de manera separada en la ilustración), sería que el

establecimiento y ejecución de políticas y procedimientos de control para asegurar que se están llevando a cabo los planes, programas y otras directrices de la administración (que representan el componente actividades de control) es también relevante para todas las tres categorías de objetivos.

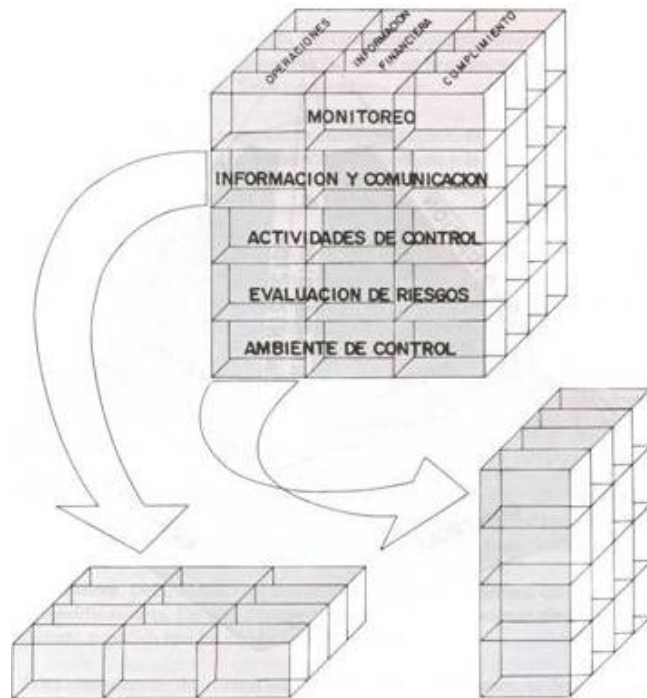
Asimismo, los cinco componentes tienen relevancia para cada categoría de objetivos. Por ejemplo, en la categoría de eficacia y eficiencia de las operaciones los cinco componentes son aplicables e importantes para su consecución. Esto se refleja de manera separada en la parte inferior derecha de la ilustración.

El control interno es relevante para toda la empresa, o para una de sus partes. Su relación se refleja con la tercera dimensión, que representa las filiales (subsidiarias), divisiones u otras unidades del negocio y las actividades funcionales o de otro tipo, como compras, producción y mercadeo. Por lo tanto, uno puede centrar su atención en cualquier célula de la matriz. Por ejemplo, se podría considerar aisladamente la célula situada en la parte inferior izquierda delantera, que representa el ambiente de control y su relación con los objetivos operacionales de una división determinada de la empresa

Eficacia

Los sistemas de control interno de las diferentes entidades funcionan a distintos niveles de eficacia. De manera similar, un sistema determinado puede funcionar de forma diferente en momentos distintos. Cuando un sistema de control interno alcanza los siguientes estándares, puede considerarse un sistema “eficaz”.

Seguindo a Coopers & Lybrand (2007), el control interno puede considerarse eficaz en cada una de las tres categorías, si el consejo de administración y la dirección tienen seguridad razonable de que:



- Disponen de información adecuada sobre hasta qué punto se están logrando los objetivos operacionales de la entidad.
- Los estados financieros publicados se preparan de forma fiable.
- Se cumplen las leyes y normas aplicables.

Puesto que el control interno es un proceso, su eficacia se mide a través del tiempo. La determinación de cuando un sistema particular de control interno es eficaz es un juicio resultante de evaluar si los cinco componentes se dan y funcionan eficazmente.

Actividades de Gestión y Control Interno

Considerando que el control interno es una parte del proceso administrativo, los componentes se discuten en el contexto de lo que la administración está haciendo en la ejecución de un negocio. No todo lo que la administración hace, sin embargo, es un elemento del control interno. El establecimiento de objetivos, por ejemplo, que es una importante responsabilidad administrativa, es un pre-requisito para el control interno. De manera similar, muchas decisiones y acciones de la administración no representan control interno. La siguiente tabla presenta una lista de las acciones administrativas más comunes e indica cuales se consideran componentes del control interno. (El significado de este listado tampoco es total y no representa una vía única para describir las actividades de la administración).

Actividades de gestión	Control Interno
Definición de objetivos, declaración de la misión y valores de la entidad	
Planeación estratégica	
Establecimiento de factores del ambiente de control	✓
Definición de los objetivos para cada actividad	
Identificación y análisis de riesgos	✓
Gestión de riesgos	
Dirección de las actividades de gestión	✓
Identificación, captura y comunicación de información	✓
Monitoreo (supervisión)	✓
Acciones correctivas	

Fuente: Coopers & Lybrand /2007)

2.4. COSO II - ERM (2004)

Hacia fines de Septiembre de 2004, como respuesta a una serie de escándalos, e irregularidades que provocaron pérdidas importante a inversionistas, empleados y otros grupos de interés, como los casos de Enron, WorldCom y otras empresas, con recientes acontecimientos, nuevamente el Committee of Sponsoring Organizations of the Treadway Commission, publicó el **Enterprise Risk Management - Integrated Framework (Marco Integrado de Gestión de Riesgos (COSO II ó COSO ERM))** y sus Aplicaciones técnicas asociadas, el cual amplía el concepto de control interno, proporcionando un foco más robusto y extenso sobre la identificación, evaluación y gestión integral de riesgo.

La Gestión de Riesgos

De acuerdo al informe COSO II-ERM (Enterprise Risk Management - Administración de Riesgos de la Empresa), la gestión de riesgos corporativos se ocupa de los riesgos y oportunidades que afectan a la creación de valor o su preservación. Se define (la Gestión de Riesgos) de la siguiente manera:

“Es un proceso efectuado por el consejo de administración de una entidad, su dirección y restante personal, aplicado en la definición de la estrategia y en toda la entidad y diseñado para identificar eventos potenciales que puedan afectar a la organización y gestionar sus riesgos dentro del riesgo aceptado, proporciona una seguridad razonable sobre el logro de objetivos.”

La definición recoge los siguientes conceptos 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.
- 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.

Este nuevo enfoque no sustituye el marco de control interno anterior (COSO I), sino que lo incorpora como parte de él, pasa a ser parte integral, permitiendo a las compañías mejorar sus prácticas de control interno o decidir encaminarse hacia un proceso más completo de gestión de riesgo.

A **nivel organizacional**, este documento destaca la necesidad de que la alta dirección y el resto de la organización comprendan cabalmente la trascendencia del control interno, la incidencia del mismo sobre los resultados de la gestión, el papel estratégico a conceder a la auditoría y esencialmente la consideración del control como un proceso integrado a los procesos operativos de la empresa y no como un conjunto pesado, compuesto por mecanismos burocráticos.

A **nivel regulatorio o normativo**, el Informe COSO ha pretendido que cuando se plantee cualquier discusión o problema de control interno, tanto a nivel práctico de las empresas, como a nivel de auditoría interna o externa, o en los ámbitos académicos o legislativos, los interlocutores tengan una referencia conceptual común, lo cual hasta ahora resultaba complejo, dada la multiplicidad de definiciones y conceptos divergentes que han existido sobre control interno.

Estructura de COSO II

COSO II-ERM, a diferencia de COSO I, ahora consta de 8 elementos o componentes (antes 5) interrelacionados con cada uno de sus 4 categorías de objetivos (antes 3); según Abella Rubio (2006), se describen así:

Componentes:

- **Ambiente interno.** El ambiente interno de la compañía es la base sobre la que se sitúan el resto de elementos, e influye de manera significativa en el establecimiento de los objetivos y de la estrategia. En el entorno de ese ambiente interno, la dirección establece la filosofía que pretende establecer en materia de gestión de riesgos, en función de su cultura y su "apetito" de riesgo.
- **Establecimiento de objetivos.** Los objetivos deben establecerse con anterioridad a que la dirección identifique los posibles acontecimientos que impidan su consecución. Deben estar alineados con la estrategia de la compañía, dentro del contexto de la visión y misión establecidos.
- **Identificación de acontecimientos o eventos.** La incertidumbre existe y, por tanto, se deben considerar aspectos externos (económicos, políticos, sociales...) e internos (infraestructuras, personal, procesos, tecnología..) que afectan a la consecución de los objetivos del negocio. Resulta pues imprescindible dentro del modelo la identificación de dichos acontecimientos, que podrán ser negativos (que implican riesgos), o positivos (que implican oportunidades e incluso mitigación de riesgos).
- **Evaluación de riesgos.** Para poder establecer el efecto que determinados acontecimientos pueden tener en la consecución de los objetivos impuestos por la dirección, es necesario evaluarlos desde la doble perspectiva de su impacto económico y de la probabilidad de ocurrencia de los mismos. Para ello es necesaria una adecuada combinación de técnicas cuantitativas y cualitativas. La evaluación de riesgos se centrará inicialmente en el riesgo inherente (riesgo existente antes de establecer mecanismos para su mitigación), y posteriormente en el riesgo residual (riesgo existente tras el establecimiento de medidas de control).
- **Respuesta al riesgo.** La dirección debe evaluar la respuesta al riesgo de la compañía en función de cuatro categorías: evitar, reducir, compartir y aceptar. Una vez establecida la respuesta al riesgo más adecuada para cada situación, se deberá efectuar una reevaluación del riesgo residual.
- **Actividades de control.** Se trata de las políticas y procedimientos que son necesarios para asegurar que la respuesta al riesgo ha sido la adecuada. Las actividades de control deben estar establecidas en toda la organización, a todos los niveles y en todas sus funciones.



- **Información y comunicación.** La adecuada información es necesaria a todos los niveles de la organización, de cara a una adecuada identificación, evaluación y respuesta al riesgo que permita a la compañía la consecución de sus objetivos. Además para conseguir que ERM funcione de manera efectiva es necesario un adecuado tratamiento de los datos actuales e históricos, lo que implica la necesidad de unos sistemas de información adecuados. Por su parte, la información es la base de la comunicación que implica una adecuada filosofía de gestión integral de riesgos.
- **Monitoreo (Supervisión).** La metodología ERM debe ser monitorizada, para asegurar su correcto funcionamiento y la calidad de sus resultados a lo largo del tiempo. El modo en que esta supervisión se lleve a cabo dependerá fundamentalmente de la complejidad y el tamaño de la organización.

Objetivos

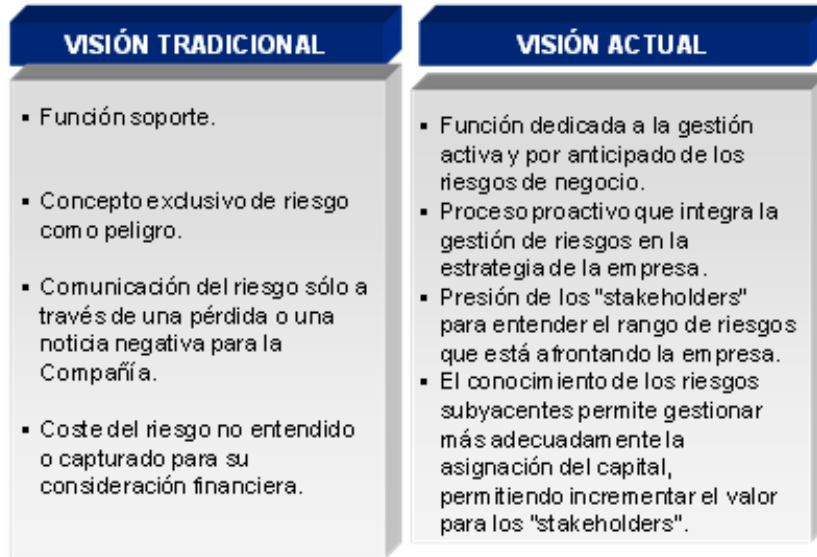
Dentro de este contexto, el modelo divide los objetivos de las compañías en cuatro categorías diferentes:

- **Objetivos estratégicos.** Se trata de los objetivos establecidos al más alto nivel, y relacionados con el establecimiento de la misión y visión de la compañía.
- **Objetivos operativos.** Se trata de aquellos relacionados directamente con la eficacia y eficiencia de las operaciones, incluyendo por supuesto objetivos relacionados con el desempeño y la rentabilidad.
- **Objetivos relacionados con la información suministrada a terceros.** Se trata de aquellos objetivos que afectan a la efectividad del reporting de la información suministrada (interna y externa), y va más allá de la información estrictamente financiera.
- **Objetivos relacionados con el cumplimiento regulatorio.** Se trata de aquellos objetivos relacionados con el cumplimiento por parte de la compañía con todas aquellas leyes y regulaciones que le son de aplicación.

2.5. Comparación de los Modelos COSO I y COSO II

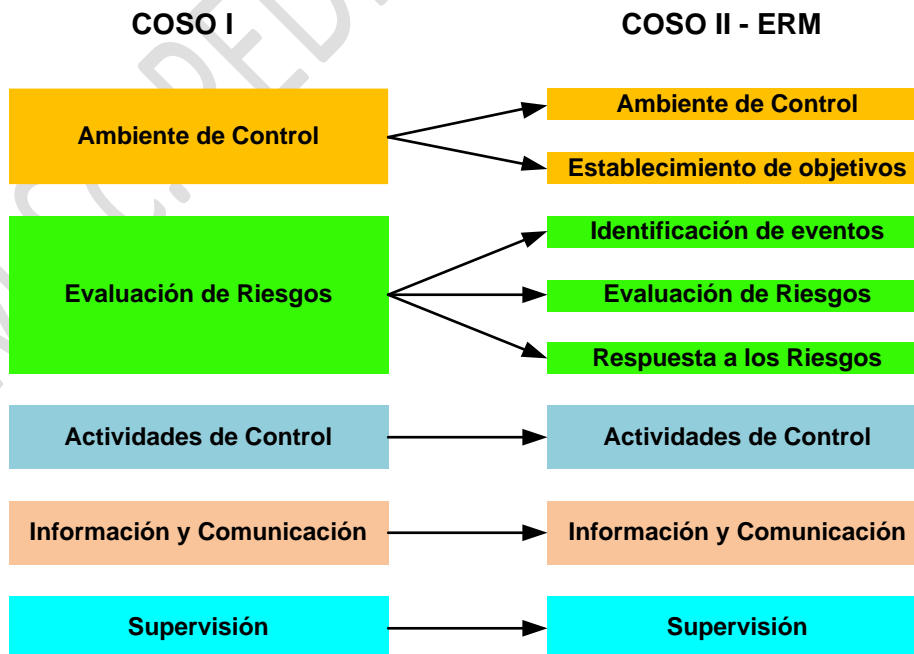
Aunque se considera que COSO II - ERM (Marco Integrado de Administración de Riesgo Empresarial) se integra a COSO I (Marco Integrado de control Interno), no obstante se pueden ver algunos aspectos que los diferencian.

Visión:



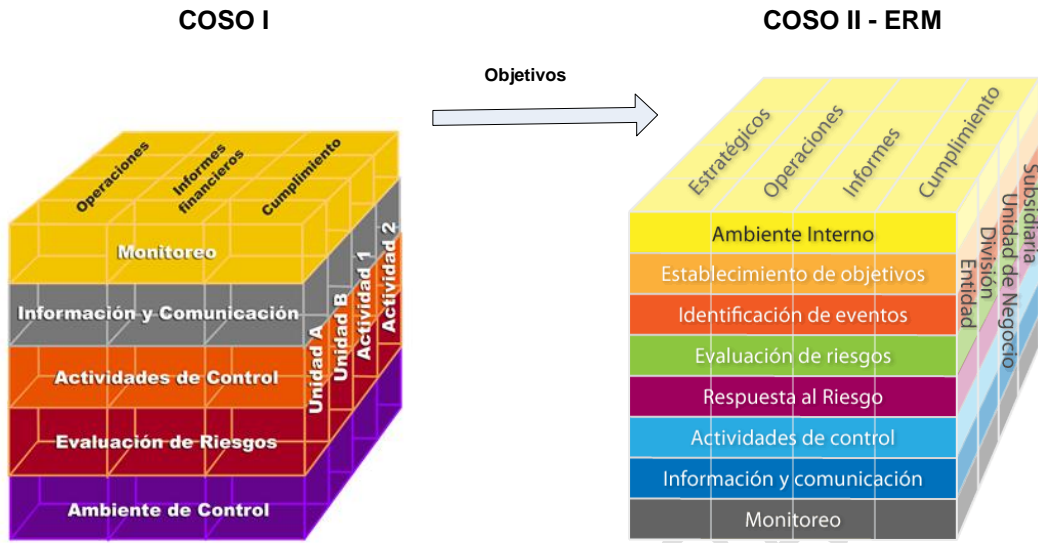
Fuente: Informe COSO II, Gestión de Riesgos Corporativos –

Relación de Componentes:



Elaborado por Pedro Bejarano V.

Objetivos



M.Sc. PEDRO BEJARANO V.

Resumen

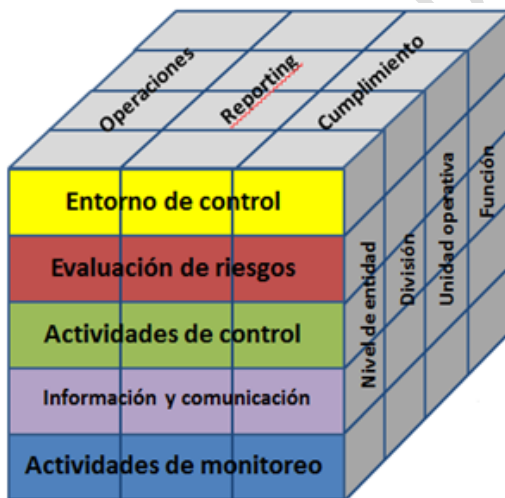
	COSO I	COSO II
Definición	<p>Es un proceso efectuado por el consejo de administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos dentro de las siguientes categorías:</p> <ul style="list-style-type: none"> -Eficacia y eficiencia de las operaciones; -Fiabilidad de la información financiera -Cumplimiento de la leyes y normas que sean aplicables 	<p>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</p>
Finalidad	<p>Facilitar un modelo en base al cual las entidades evalúen sus sistemas de control y decidan cómo mejorarlos.</p> <p>Integrar diversos conceptos de control interno dentro de un marco en el que se pueda establecer una definición común e identificar los componentes de control.</p> <p>Visión del riesgo a eventos negativos.</p>	<p>Ampliar el concepto de control interno a través de la identificación, evaluación y gestión integral de riesgo.</p> <p>Extender la visión del riesgo a eventos negativos o positivos, o sea, a amenazas u oportunidades.</p>
Componentes	<ol style="list-style-type: none"> 1. Entorno de control. 2. Evaluación de riesgos. 3. Actividades de control. 4. Información y comunicación. 5. Supervisión. 	<ol style="list-style-type: none"> 1. Ambiente interno 2. Establecimiento de objetivos 3. Identificación de eventos 4. Evaluación de riesgos 5. Respuesta a los riesgos 6. Actividades de control 7. Información comunicación 8. Supervisión
Objetivos	<ol style="list-style-type: none"> 1. Eficacia y eficiencia de las operaciones. 2. Fiabilidad de la información financiera. 3. Cumplimiento de las leyes y normas que sean aplicables 	<ol style="list-style-type: none"> 1. Objetivos estratégicos Eficacia y eficiencia de las operaciones. 2. Fiabilidad de la información financiera. 3. Cumplimiento de las leyes y normas que sean aplicables

2.6. COSO III (2013)

Con la emisión del Informe COSO III, el año 2014 existían tres Informes COSO y hacia fines del 2014 solo quedaron dos Marcos vigentes. El primero de ellos, publicado el año 1992, que surge cuando la Comisión Treadway, emite el documento denominado Marco Integrado del Control Interno, o también llamado COSO I, este marco es reconocido como la guía principal para diseñar, implementar y llevar a cabo el control interno y la evaluación de su eficacia. La organización proporciona liderazgo intelectual y orientación sobre el control interno, la gestión del riesgo empresarial, y la disuasión del fraude.

Recordamos COSO I, consta de cinco componentes relacionados entre sí, se derivan de la manera en que la dirección gestiona la empresa y están integrados en el proceso de dirección, los componentes del control son los siguientes: 1. Ambiente de control; 2. Evaluación de riesgos; 3. Actividades de control; 4. Información y Comunicación; 5. Monitoreo. Sus objetivos son: a) Eficacia y eficiencia de las operaciones; b) Fiabilidad de la información financiera; c) Cumplimiento de las leyes y normas que sean aplicables.

Después de más de 20 años de la emisión de COSO I, en mayo de 2013, se publicó la actualización del marco integrado de control interno (o también llamado COSO III) que sustituye al marco original de 1992. La lógica lleva a pensar que el nuevo Marco Integrado COSO III debería ser la continuación de ERM o COSO II; sin embargo, su objetivo es actualizar y reemplazar COSO I, por lo que COSO II, sigue siendo complementario a COSO III. Otro de los objetivos de este nuevo Marco es aclarar los requerimientos del control interno, actualizar el contexto de la aplicación del control interno a muchos cambios en las empresas y ambientes operativos, así como ampliar su aplicación al expandir los objetivos operativos y de emisión de informes.



Según (OLACEFS, 2015), en la versión 2013, COSO mantuvo los cinco componentes funcionales, pero dejó de utilizar la representación piramidal. Actualmente, el sistema aparece como un cubo, en el cual el ambiente (entorno) de control se ubica en la parte superior, para dar la idea de que el compromiso con el control interno debe fluir de la cima, toda vez que la alta dirección como responsable del sistema en primera instancia, deben propiciar un ambiente idóneo para el funcionamiento del control interno.

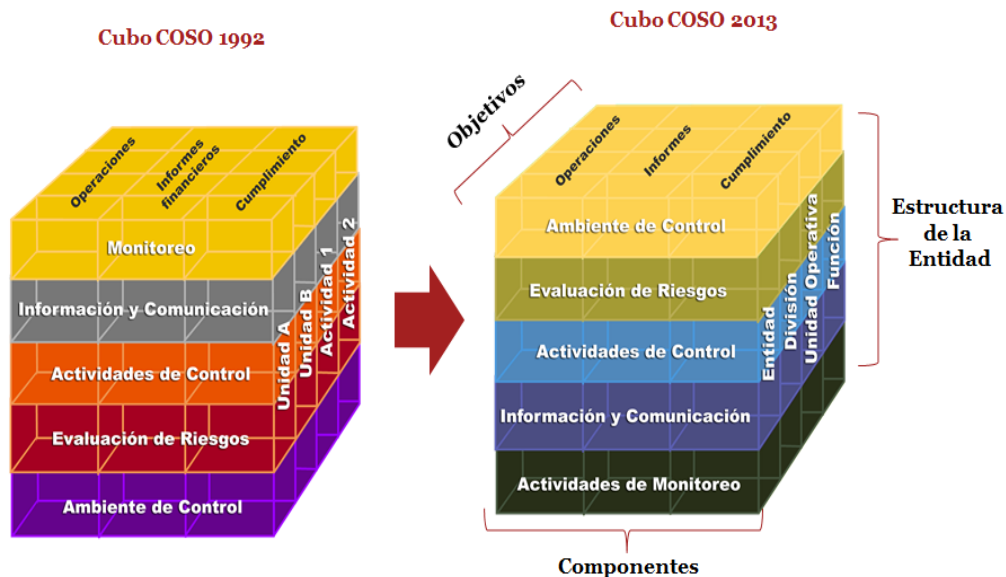
En esta nueva entrega del Informe COSO III (realizado por PricewaterhouseCoopers PWC, bajo la dirección del Consejo de COSO), los **cinco componentes** se asocian con una serie de

diecisiete principios, y éstos a su vez, se relacionan con **setenta y ocho puntos de interés** que son indicativos del cumplimiento de los principios. La definición de los principios constituye una formalización de los conceptos fundamentales presentes en el marco original. El marco describe una serie de puntos de interés que son manifestaciones prácticas de esos principios. De acuerdo con el enfoque, los cinco componentes funcionales y los principios correspondientes son obligatorios, pero los puntos de interés no lo son, debido a que la dirección puede determinar que algunos de estos puntos de

interés no son adecuados o relevantes y puede identificar y tener en cuenta otros puntos de interés con base en las circunstancias específicas de la organización

La transición de COSO I a COSO III, se produce durante el año 2014, puntualmente COSO I estuvo vigente hasta el 15 de diciembre de 2014, terminado el periodo de transición COSO I fue derogado. En EEUU, la transición es obligatoria para todas las organizaciones registradas en la SEC (Securities and Exchange Commission) cuyo marco de control interno sea COSO. La certificación requerida por la sección 302 de la Ley Sarbanes-Oxley ²(107 th Congress, 2002) debe hacer referencia a que en el año 2014 se llevó a cabo la transición a COSO III. En el caso de las organizaciones obligadas a presentar auditoría de los estados financieros y del control interno sobre la información financiera, en el dictamen el auditor, deberá mencionar que el marco de control interno sobre la información financiera aplicado al 31 de diciembre de 2014 es el marco vigente a la fecha, COSO III.

Las observaciones y comentarios que se han realizado luego del lanzamiento de COSO III, referentes a ¿qué impulsó la actualización del Marco original?, son principalmente en base al entorno de los negocios que cada día es más cambiante y complejo, debido además a la globalización de los mercados y las operaciones, cambios en los modelos de negocios, demandas y complejidad de normas, regulaciones y estándares, uso y dependencia de la tecnología que evoluciona.



Los conceptos en COSO III son similares a aquellos de COSO I. La principal diferencia es que este nuevo Marco añade discusiones más detalladas acerca de cada componente (ambiente de control, evaluación de riesgos, actividades de control, información y comunicación, y monitoreo). Por ejemplo, en COSO I está el componente de evaluación de riesgos, el cual se sigue conservando en COSO III, incluyendo el riesgo inherente, tolerancia al riesgo, las formas de manejar los riesgos y la vinculación entre riesgo de las actividades de evaluación y control. En el resumen ejecutivo del control interno del marco

² La Ley Sarbanes-Oxley, cuyo título oficial en inglés es Sarbanes-Oxley Act of 2002, (30 de julio de 2002), es una ley de Estados Unidos también conocida como la Ley de Reforma de la Contabilidad Pública de Empresas y de Protección al Inversionista. Se promulgó en Estados Unidos con el propósito de monitorizar a las empresas que cotizan en bolsa de valores, evitando que la valorización de las acciones de las mismas sean alteradas de manera dudosa, mientras que su valor es menor. Su finalidad es evitar fraudes y riesgo de bancarrota, protegiendo al inversionista.

integrado, se afirma que COSO III toma la esencia de COSO I y enfatiza que los cinco componentes de COSO deben estar presentes y funcionando conjuntamente de manera integrada; es decir, deben estar diseñados y ser efectivos.

Objetivos

Por ser de interés para el tema abordado, resulta conveniente enfatizar que COSO 2013 establece tres categorías de objetivos que permiten a las organizaciones abordar diferentes aspectos de control interno, lo cual se refleja en las directrices de la INTOSAI en materia de control interno:

- **De operación.** Se refiere a la eficacia y la eficiencia de las operaciones de la entidad, donde se incluyen metas de desempeño operativo y financiero, así como la protección de los activos contra pérdidas.
- **De informes.** Se refiere a los reportes internos y externos, financieros y no financieros que deben elaborarse y presentarse en términos de fiabilidad, oportunidad, transparencia y otras condiciones establecidas por los organismos reguladores, órganos normativos o políticas internas de la entidad.
- **De cumplimiento.** Se refiere a la adhesión y observancia de las leyes y reglamentos a los que está sujeta la entidad.

Componentes

Los componentes (1. Entorno de Control, 2. Evaluación de Riesgos, 3. Actividades de Control, 4. Información y Comunicación, y 5. Supervisión) deben funcionar de manera integrada para reducir a un nivel aceptable el riesgo de no alcanzar un objetivo. Los componentes son interdependientes, existe una gran cantidad de interrelaciones y vínculos entre ellos. Así mismo, dentro de cada componente el marco establece 17 principios que representan los conceptos fundamentales y son aplicables a los objetivos operativos, de información y de cumplimiento. Los principios permiten evaluar la efectividad del sistema de control interno.

Para determinar que el Sistema de Control Interno es efectivo se requiere que los cinco componentes y los principios estén presentes y funcionando.

Presentes: la determinación de que los componentes y los principios relevantes existen en el diseño y la implementación del sistema de control interno para lograr los objetivos especificados.

Funcionando: la determinación de que los componentes y los principios relevantes continúan existiendo en la dirección del sistema de control interno para lograr los objetivos especificados.

Según lo descrito por Gonzales Martínez (2015), a continuación se desarrolla el concepto de cada uno de los componentes:

1. Entorno de control

Es el ambiente donde se desarrollan todas las actividades organizacionales bajo la gestión de la administración. El entorno de control es influenciado por factores tanto internos como externos, tales como la historia de la entidad, los valores, el mercado, y el ambiente competitivo y regulatorio. Comprende las normas, procesos y estructuras que constituyen la base para desarrollar el control interno de la organización.

Este componente crea la disciplina que apoya la evaluación del riesgo para el cumplimiento de los objetivos de la entidad, el rendimiento de las actividades de control, uso de la información y sistemas de comunicación, y conducción de actividades de supervisión. Para lograr un entorno de control apropiado deben tenerse en cuenta aspectos como la estructura organizacional, la división del trabajo y asignación de responsabilidades, el estilo de gerencia y el compromiso.

Un entorno de control ineficaz puede tener consecuencias graves, tales como pérdida financiera, pérdida de imagen o un fracaso empresarial. Por esta razón, este componente tiene una influencia muy relevante en los demás componentes del sistema de control interno, y se convierte en el cimiento de los demás proporcionando disciplina y estructura.

Una organización que establece y mantiene un adecuado entorno de control es más fuerte a la hora de afrontar riesgos y lograr sus objetivos. Esto se puede obtener si se cuenta con:

- Actitudes congruentes con su integridad y valores éticos.
- Procesos y conductas adecuados para la evaluación de conductas.
- Asignación adecuada de responsabilidades.
- Un elevado grado de competencia y un fuerte sentido de la responsabilidad para la consecución de los objetivos.

Por esta razón, el Entorno de control está compuesto por el comportamiento que se mantiene dentro de la organización, e incluye aspectos como:

- La integridad y los valores éticos de los recursos humanos,
- La competencia profesional,
- La delegación de responsabilidades,
- El compromiso con la excelencia y la transparencia,
- La atmósfera de confianza mutua,
- La filosofía y estilo de dirección,
- La estructura y plan organizacional,
- Los reglamentos y manuales de procedimientos,
- Las políticas en materia de recursos humanos y
- El Comité de Control.

2. Evaluación de riesgos

Este componente identifica los posibles riesgos asociados con el logro de los objetivos de la organización. Toda organización debe hacer frente a una serie de riesgos de origen tanto interno como externo, que deben ser evaluados.

Estos riesgos afectan a las entidades en diferentes sentidos, como en su habilidad para competir con éxito, mantener una posición financiera fuerte y una imagen pública positiva. Por ende, se entiende por riesgo cualquier causa probable de que no se cumplan los objetivos de la organización

De esta manera, la organización debe prever, conocer y abordar los riesgos con los que se enfrenta, para establecer mecanismos que los identifiquen, analicen y disminuyan. Este es un proceso dinámico e iterativo que constituye la base para determinar cómo se gestionaran los riesgos.

3. Actividades de control

En el diseño organizacional deben establecerse las políticas y procedimientos que ayuden a que las normas de la organización se ejecuten con una seguridad razonable para enfrentar de forma eficaz los riesgos.

Las actividades de control se definen como las acciones establecidas a través de las políticas y procedimientos que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos con impacto potencial en los objetivos.

Las actividades de control se ejecutan en todos los niveles de la entidad, en las diferentes etapas de los procesos de negocio y en el entorno tecnológico, y sirven como mecanismos para asegurar el cumplimiento de los objetivos. Según su naturaleza pueden ser preventivas o de detección y pueden abarcar una amplia gama de actividades manuales y automatizadas. Las actividades de control conforman una parte fundamental de los elementos de control interno.

Estas actividades están orientadas a minimizar los riesgos que dificultan la realización de los objetivos generales de la organización. Cada control que se realice debe estar de acuerdo con el riesgo que previene, teniendo en cuenta que demasiados controles son tan peligrosos como lo es tomar riesgos excesivos.

Estos controles permiten:

- Prevenir la ocurrencia de riesgos innecesarios.
- Minimizar el impacto de las consecuencias de los mismos.
- Restablecer el sistema en el menor tiempo posible.

En todos los niveles de la organización existen responsabilidades en las actividades de control, debido a esto es necesario que todo el personal dentro de la organización conozca cuáles son las tareas de control que debe ejecutar. Para esto se debe explicitar cuáles son las funciones de control que le corresponden a cada individuo.

4. Información y comunicación

El personal debe no solo captar una información sino también intercambiarla para desarrollar, gestionar y controlar sus operaciones. Por lo tanto, este componente hace referencia a la forma en que las áreas operativas, administrativas y financieras de la organización identifican, capturan e intercambian información.

La información es necesaria para que la entidad lleve a cabo las responsabilidades de control interno que apoyan el cumplimiento de los objetivos. La gestión de la empresa y el progreso hacia los objetivos establecidos implican que la información es necesaria en todos los niveles de la empresa. En este sentido, la información financiera no se utiliza solo para los estados financieros, sino también en la toma de decisiones.

Por ejemplo, toda la información presentada a la Dirección con relación a medidas monetarias facilita el seguimiento de la rentabilidad de los productos, la evolución de deudores, las cuotas en el mercado, las tendencias en reclamaciones, etc.

La información está compuesta por los datos que se combinan y sintetizan con base en la relevancia para los requerimientos de información. Es importante que la dirección disponga de datos fiables a la hora de efectuar la planificación, preparar presupuestos, y demás actividades.

Es por esto que la información debe ser de calidad y tener en cuenta los siguientes aspectos:

- **Contenido:** ¿presenta toda la información necesaria?
- **Oportunidad:** ¿se facilita en el tiempo adecuado?
- **Actualidad:** ¿está disponible la información más reciente?
- **Exactitud:** ¿los datos son correctos y fiables?

- **Accesibilidad:** ¿la información puede ser obtenida fácilmente por las personas adecuadas?

La comunicación es el proceso continuo e iterativo de proporcionar, compartir y obtener la información necesaria, relevante y de calidad, tanto interna como externamente.

La comunicación interna es el medio por el cual la información se difunde a través de toda la organización, que fluye en sentido ascendente, descendente y a todos los niveles de la entidad. Esto hace posible que el personal pueda recibir de la Alta Dirección un mensaje claro de las responsabilidades de control.

La comunicación externa tiene dos finalidades: comunicar de afuera hacia el interior de la organización información externa relevante, y proporcionar información interna relevante de adentro hacia afuera, en respuesta a las necesidades y expectativas de grupos de interés externos.

Para esto se tiene en cuenta:

- Integración de la información con las operaciones y calidad de la información, analizando si ésta es apropiada, oportuna, fiable y accesible
- Comunicación de la información institucional eficaz y multidireccional.
- Disposición de la información útil para la toma de decisiones.
- Los canales de información deben presentar un grado de apertura y eficacia acorde con las necesidades de información internas y externas.

La comunicación puede ser materializada en manuales de políticas, memorias, avisos o mensajes de video. Cuando se hace verbalmente la entonación y el lenguaje corporal le dan un énfasis al mensaje. La actuación de la Dirección debe ser ejemplo para el personal de la entidad.

Un sistema de información comprende un conjunto de actividades, involucra personal, procesos, datos y/o tecnología, que permite que la organización obtenga, genere, use y comunique transacciones de información para mantener la responsabilidad y medir y revisar el desempeño o progreso de la entidad hacia el cumplimiento de los objetivos.

5. Supervisión del sistema de control – Monitoreo

Todo el proceso ha de ser monitoreado con el fin de incorporar el concepto de mejoramiento continuo; así mismo, el Sistema de Control Interno debe ser flexible para reaccionar ágilmente y adaptarse a las circunstancias.

Las actividades de monitoreo y supervisión deben evaluar si los componentes y principios están presentes y funcionando en la entidad.

Es importante determinar, supervisar y medir la calidad del desempeño de la estructura de control interno, teniendo en cuenta:

- Las actividades de monitoreo durante el curso ordinario de las operaciones de la entidad.
- Evaluaciones separadas.
- Condiciones reportables.

- Papel asumido por cada miembro de la organización en los niveles de control.

Es importante establecer procedimientos que aseguren que cualquier deficiencia detectada que pueda afectar al Sistema de Control Interno sea informada oportunamente para tomar las decisiones pertinentes. Los sistemas de control interno cambian constantemente, debido a que los procedimientos que eran eficaces en un momento dado, pueden perder su eficacia por diferentes motivos, como la incorporación de nuevos empleados, restricciones de recursos, entre otros.

Componentes y Principios de COSO III

Entorno de Control	Evaluación de riesgos	Actividades de Control	Información y Comunicación	Supervisión (Monitoreo)
1. Demuestra compromiso para con la integridad y valores éticos	6. Especifica los objetivos con suficiente claridad para permitir la identificación y evaluación de los riesgos.	10. Selecciona y desarrolla las actividades de control que contribuyen a la mitigación de riesgos.	13. Obtiene y usa información relevante y de calidad para soportar el funcionamiento del control interno	16. Dirige evaluaciones continuas y/o separadas.
2. Ejerce responsabilidad por la vigilancia (supervisión)	7. Identifica y analiza de riesgos para determinar cómo se deben mitigar.	11. Selecciona y desarrolla los controles generales sobre la tecnología	14. Internamente comunica la información, incluyendo objetivos y responsabilidades	17. Evalúa y comunica las deficiencias de control interno en forma oportuna
3. Establece estructura, autoridad y responsabilidad para el logro de los objetivos	8. Evalúa el riesgo de fraude.	12. Despliega mediante políticas y procedimientos que las ponen en acción	15. Comunica a partes externas materias relativas al control interno	
4. Demuestra compromiso para con la competencia	9. identifica y analiza los cambios que podrían impactar el sistema de control interno			
5. Refuerza la responsabilidad				

Fuente: Obtenido de revista Heads Up, Deloitte. Volumen 20, No. 17

Puntos de interés o de enfoque (atributos)

A continuación se muestran los puntos de interés o enfoque, ordenados por componentes y principios (OLACEFS 2015):

Componente 1: Entorno (ambiente) de Control:

Principios	Puntos de interés o enfoque
1.1. Compromiso con la integridad y los valores éticos	1.1.1 Establece el tono en la cima (directiva y alta gerencia) 1.1.2 Establece estándares de conducta 1.1.3 Evalúa la adhesión a estándares de conducta 1.1.4 Aborda y decide sobre desviaciones de manera oportuna
1.2. Supervisión independiente de la junta directiva	1.2.1 Establece responsabilidades de supervisión 1.2.2 Aplica experiencia relevante 1.2.3 Funciona (opera) independientemente 1.2.4 Proporciona supervisión al sistema de control interno 1.2.5 Supervisión al sistema de control interno
1.3. Estructura, líneas de reporte, autoridad y responsabilidad	1.3.1 Considera todas las estructuras de la entidad 1.3.2 Establece líneas de reporte 1.3.3 Define, asigna y delimita autoridades y responsabilidades
1.4. Atraer, retener y mantener personal competente	1.4.1 Establece políticas y prácticas 1.4.2 Evalúa las competencias y corrige las deficiencias 1.4.3 Atrae, desarrolla y retiene personal competente 1.4.4 Planifica y se prepara para la sucesión
1.5. Definir responsables por el control interno y la consecución de objetivos	1.5.1 Hace cumplir la responsabilidad (rendición de cuentas) mediante estructuras, autoridades y responsabilidades 1.5.2 Establece medidas de desempeño, incentivos y recompensas 1.5.3 Evalúa las medidas de desempeño, incentivos y recompensas para relevancia continua 1.5.4 Considera presiones excesivas 1.5.5 Evalúa el desempeño y recompensa o disciplina a los individuos

Componente 2: Evaluación del Riesgo:

Principios	Puntos de interés
2.1. Especificación de objetivos claros y adecuados	2.1.1 Objetivos operacionales 2.1.2 Objetivos de reporte financiero externo 2.1.3 Objetivos de reporte no financiero externo 2.1.4 Objetivos de reporte interno 2.1.5 Objetivos de cumplimiento
2.2. Identificación y análisis de los riesgos	2.2.1 Incluye entidad, subsidiaria, división, unidad operativa y niveles funcionales 2.2.2 Analiza los factores internos y externos 2.2.3 Involucra a niveles adecuados de la administración 2.2.4 Estima la importancia de los riesgos identificados 2.2.5 Determina cómo responder a los riesgos
2.3. Evaluación del potencial de riesgos de fraude	2.3.1 Considera varios tipos de fraude 2.3.2 Evalúa incentivos y presiones 2.3.3 Evalúa oportunidades 2.3.4 Evalúa las actitudes y las racionalizaciones
2.4. Identificación y análisis de cambios significativos	2.4.1 Evalúa los cambios en el entorno externo 2.4.2 Evalúa los cambios en el modelo de negocio 2.4.3 Evalúa los cambios en el liderazgo

Componente 3: Actividades de Control:

Principios	Puntos de interés
3.1. Selección y desarrollo de actividades de control que contribuyen a la mitigación de los riesgos	3.1.1 Integración con la evaluación de riesgos 3.1.2 Considera los factores específicos de la entidad 3.1.3 Determina los procesos empresariales relevantes 3.1.4 Evalúa una mezcla de tipos de actividades de control 3.1.5 Considera en qué nivel se aplican las actividades 3.1.6 Toma en cuenta la segregación de funciones
3.2. Selección y desarrollo de controles generales de la TI	3.2.1 Determina la dependencia entre el uso de TI en los procesos del negocio y los controles generales de TI 3.2.2 Establece actividades de control relevantes a la infraestructura de TI 3.2.3 Se establecen actividades de control relevantes para el proceso de gestión de seguridad 3.2.4 Se establecen actividades de control relevantes para los procesos de adquisición, desarrollo y mantenimiento de TI
3.3. Controles implementados a través de políticas y procedimientos	3.3.1 Se establecen políticas y procedimientos para permitir la implementación de las directrices de la administración 3.3.2 Establece la responsabilidad y rendición de cuentas por la ejecución de las políticas y los procedimientos 3.3.3 Se realizan de forma oportuna 3.3.4 Se toman acciones correctivas 3.3.5 Se lleva a cabo usando personal competente 3.3.6 Se evalúan las políticas y los procedimientos

Componente 4: Información y Comunicación:

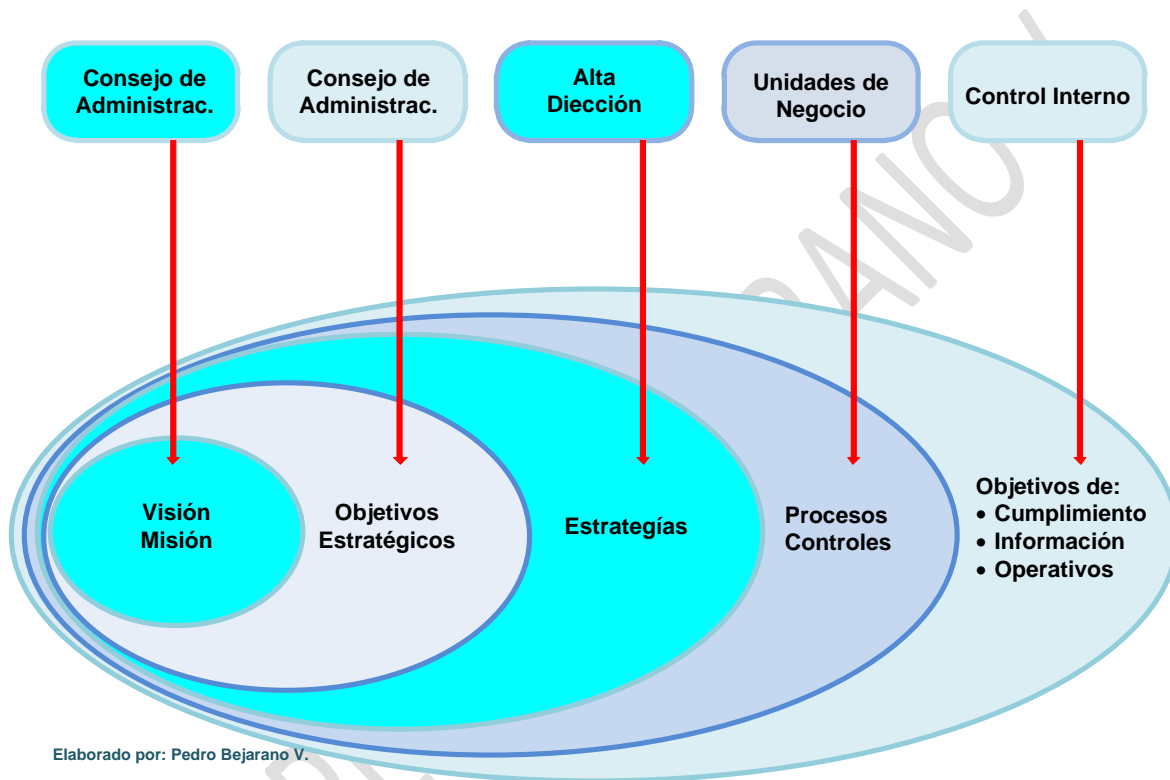
Principios	Puntos de interés
4.1. Información relevante obtenida, generada y usada	4.1.1 Identifica los requerimientos y requisitos de la información 4.1.2 Captura fuentes internas y externas de datos 4.1.3 Procesos de datos relevantes 4.1.4 Mantiene la calidad a lo largo del procesamiento 4.1.5 Considera los costos y los beneficios
4.2. Información de control interno comunicada internamente	4.2.1 Se comunica información de control interno 4.2.2 La administración se comunica con el consejo directivo 4.2.3 Proporciona líneas de comunicación independientes 4.2.4 Selecciona métodos relevantes de comunicación
4.3. Información de control interno comunicada externamente	4.3.1 Se comunica a partes externas 4.3.2 Permite comunicaciones entrantes 4.3.3 Se comunica con el consejo directivo 4.3.4 Proporciona líneas de comunicación independientes 4.3.5 Selecciona métodos relevantes de comunicación

Componente 5: Actividades de Monitoreo (Supervisión):

Principios	Puntos de interés
5.1. Evaluaciones continuas y/o separadas completadas	5.1.1 Considera una mezcla de evaluaciones permanentes y separadas 5.1.2 Considera la velocidad del cambio 5.1.3 Establece una comprensión básica 5.1.4 Utiliza personal experto (capacitado) 5.1.5 Se integra con los procesos del negocio 5.1.6 Se ajusta el alcance y la frecuencia 5.1.7 Se evalúa objetivamente
5.2. Evaluación y comunicación de deficiencias de control interno	5.2.1 Evalúa los resultados 5.2.2 Comunica las deficiencias 5.2.3 Monitorea (supervisa) las acciones correctivas

Principales cambios en COSO III con respecto a COSO I

El nuevo marco integrado (COSO III) incluye, a diferencia del marco original (COSO I) está orientado a la planificación, a la consecución de objetivos y a la necesidad e importancia de considerar el potencial de riesgo de fraude al evaluar los riesgos para el logro de los objetivos de la organización, teniendo en cuenta por ejemplo el grado de juicios y estimaciones en informes externos, la naturaleza de la tecnología, y la capacidad de la administración para manipular la información, entre otros.



Los siguientes son algunos de los cambios significativos:

- Refleja los cambios en los entornos de negocio y operativos.
- Codifica los principios de aplicación universal y la articulación de los mismos para usarse en el desarrollo y evaluación de la eficacia de los sistemas de control interno.
- *Expande los objetivos de reportes financieros para ir también a informes internos y externos en un sentido amplio, incluyendo objetivos no financieros (reportes no financieros) tanto a nivel interno y externo. Esta categoría se denomina ahora de "Reporte" e incluye 4 categorías de objetivos de reporte: Financiero Interno, No Financiero Interno, Financiero Externo y No Financiero Externo*
- *Refleja el aumento en la relevancia de la tecnología dentro de los modelos de control interno: Esto es importante porque el número de organizaciones que usan o dependen de la tecnología, y el grado de utilización de la misma han tenido un cambio sustancial en los últimos años (incluye el tema Tecnología de una forma puntual y formal dentro de uno de los 17 principios de COSO).*

- *Incorpora una discusión mejorada de conceptos de Gobernabilidad (Corporate Governance) , se haciendo énfasis en la estructura de gobernanza que debe existir al interior de la organizaciones incluyendo la Junta o Consejo Directivo y sus comités, incluyendo el comité de auditoria, comité de compensaciones, comité de gobernanza, comité de riesgo, entre otros.*
- *Realza la consideración de las expectativas Anti-Fraude, contiene considerablemente más discusiones relacionadas al fraude y también considera la “Evaluación de Potenciales Riesgos de Fraude” como un Principio separado de control interno dentro de su metodología. Es decir, dentro del proceso de evaluación de riesgos tiene que considerarse el riesgo de fraude como un riesgo más que debe enfrentar la organización y buscar los mecanismos para identificar potenciales situaciones donde el fraude puede ocurrir e implementar controles para mitigar dichos riesgos.*

M.Sc. PEDRO BEJARANO V.

Componentes de los Modelos del Informe COSO I, II y III

COSO I	COSO II	COSO III
<p>1. Ambiente de Control.</p> <p>2. Evaluación de Riesgos.</p> <p>3. Actividades de Control.</p> <p>4. Información y Comunicación.</p> <p>5. Supervisión o Monitoreo.</p>	<p>1. Ambiente interno. Hace referencia al entorno interno de una empresa y establece la base de cómo el personal percibe y trata los riesgos.</p> <p>2. Establecimiento de objetivos: estratégicos, operativos, de información y de cumplimientos, deben estar alineados con la visión y misión. Teniendo en cuenta que cada decisión conlleva un riesgo que debe ser previsto.</p> <p>3. Identificación de eventos: que pueden afectar al cumplimiento de los objetivos.</p> <p>4. Evaluación de riesgos. Identificar y analizar los riesgos relevantes considerando su probabilidad e impacto sobre los objetivos.</p> <p>5. Respuesta a los riesgos. Determinar las posibles repuestas y acciones frente a los riesgos.</p> <p>6. Actividades de control. Políticas y procedimientos que permiten asegurar que se tomen las acciones necesarias para controlar los riesgos.</p> <p>7. Información y comunicación. Eficaz en contenido y tiempo para permitir a los trabajadores cumplir con sus responsabilidades. Asimismo, debe existir una buena comunicación con los clientes, proveedores, reguladores y accionistas.</p> <p>8. Supervisión. Se monitorea que el proceso de administración de los riesgos sea efectivo a lo largo del tiempo y que todos los elementos del marco COSO funcionen adecuadamente.</p>	<p>1. Ambiente de Control. Pr1: Demuestra compromiso para con la integridad y valores éticos Pr2: Ejerce responsabilidad por la vigilancia (supervisión) Pr3: Establece estructura, autoridad y responsabilidad para el logro de los objetivos Pr4: Demuestra compromiso para con la competencia Pr5: Refuerza la responsabilidad</p> <p>2. Evaluación de Riesgos. Pr6: Especifica los objetivos con suficiente claridad para permitir la identificación y evaluación de los riesgos. Pr7: Identifica y analiza de riesgos para determinar cómo se deben mitigar. Pr8: Evalúa el riesgo de fraude Pr9: identifica y analiza los cambios que podrían impactar el sistema de control interno</p> <p>3. Actividades de Control. Pr10: Selecciona y desarrolla las actividades de control que contribuyen a la mitigación de riesgos Pr 11: Selecciona y desarrolla los controles generales sobre la tecnología Pr12: Despliega mediante políticas y procedimientos que las ponen en acción</p> <p>4. Información y Comunicación. Pr13: Obtiene y usa información relevante y de calidad para soportar el funcionamiento del control interno (Sist. de Informac) Pr14: Internamente comunica la información, incluyendo objetivos y responsabilidades Pr15: Comunica a partes externas materias relativas al control interno.</p> <p>5. Monitoreo Pr16: Dirige evaluaciones continuas y/o separadas. Pr17: Evalúa y comunica las deficiencias de control interno en forma oportuna.</p>

2.7. COSO IV (2017)

En septiembre 2017 la Organización COSO ha presentado oficialmente el tan esperado Gestión de Riesgos Empresarial - Integración con Estrategia y Desempeño (Enterprise Risk Management–Integrating with Strategy and Performance), basado en su predecesor y más conocido como COSO-ERM o Gestión de Riesgos Empresariales-Marco Integrado (Enterprise Risk Management–Integrated Framework) emitido en el año 2004.

Este marco fue actualizado pensando en los cambios constantes del mundo de los negocios y la importancia de una gestión de riesgos que influyen en la estrategia y el desempeño de las organizaciones. Según COSO (2017) su presidente de Robert B. Hirth Jr. dice: "La complejidad del riesgo ha cambiado, han surgido nuevos riesgos y tanto los directivos como los mejorar la concienciación y la supervisión de la gestión de riesgos empresariales, al tiempo que informes de riesgo " y "Nuestro objetivo general es continuar fomentando una cultura."

Este modelo consta de cinco componentes de fácil entendimiento, centrando los cambios en la actual evolución de la gestión de riesgos. Los principios son 20, estos tienen cobertura desde la gobernanza hasta la supervisión, son de apoyo a la gestión de riesgos asociados a la estrategia y objetivos empresariales.



Componentes de COSO IV

Seguendo a COSO (2017), El propio Marco es un conjunto de principios organizados en cinco Componentes interrelacionados:

1. Gobierno y cultura:

El Gobierno marca el tono en la entidad, reforzando la importancia de la gestión del riesgo empresarial y estableciendo responsabilidades de supervisión al respecto. La cultura hace referencia a los valores éticos, a los comportamientos deseados y a la comprensión del riesgo en la entidad.

2. Estrategia y establecimiento de objetivos:

La gestión del riesgo empresarial, la estrategia y el establecimiento de objetivos funcionan juntos en el proceso de planificación estratégica. Se establece un apetito al riesgo y se alinea con la estrategia; los objetivos del negocio ponen en práctica la estrategia al tiempo que sirven de base para identificar, evaluar y responder ante el riesgo.

3. Desempeño:

Es necesario identificar y evaluar aquellos riesgos que puedan afectar a la consecución de los objetivos estratégicos y de negocio. Los riesgos se priorizan en función de su gravedad en el contexto del apetito al riesgo. Posteriormente, la organización selecciona las respuestas ante el riesgo y adopta una visión a nivel de cartera con respecto al nivel de riesgo que ha asumido. Los resultados de este proceso se comunican a las principales partes interesadas en el riesgo.

4. Revisión y monitorización:

Al examinar el desempeño de la entidad, una organización puede determinar cómo funcionan los componentes de gestión del riesgo empresarial con el paso del tiempo en un entorno de cambios sustanciales, y qué aspectos son susceptibles de revisar y modificar.

5. Información, comunicación y reporte:

La gestión del riesgo empresarial requiere un proceso continuo de obtención e intercambio de la información necesaria, tanto de fuentes internas como externas, que fluya hacia arriba, hacia abajo y a lo largo de todos los niveles de la organización

Principios de COSO IV

Los cinco componentes, en el marco actualizado, están respaldados por un conjunto de principios que cubren todo los aspectos, desde el gobierno hasta la monitorización. Son manejables en tamaño, y describen las prácticas aplicables de diferentes formas y para distintos tipos de organizaciones, independientemente de su tamaño, tipo o sector.

Según COSO (2017), la adhesión a estos principios puede proporcionar, a la dirección y el consejo, una expectativa razonable de que la organización entiende y se esfuerza por gestionar los riesgos asociados con su estrategia y los objetivos de la empresa.

Gobierno y Cultura

1. Ejerce la Supervisión de Riesgos a través del Consejo de Administración
2. Establece Estructuras Operativas
3. Define la Cultura Deseada
4. Demuestra Compromiso con los Valores Clave
5. Atrae, Desarrolla y Retiene a Profesionales Capacitados

Estrategia y Establecimiento de Objetivos

6. Analiza el Contexto Empresarial
7. Define el Apetito al Riesgo
8. Evalúa Estrategias Alternativas
9. Formula Objetivos de Negocio

Desempeño

10. Identifica el Riesgo
11. Evalúa la Gravedad del Riesgo
12. Prioriza Riesgos
13. Implementa Respuestas ante los Riesgos
14. Desarrolla una Visión a nivel de Cartera

Revisión y Monitorización

15. Evalúa los Cambios Significativos
16. Revisa el Riesgo y el Desempeño
17. Persigue la Mejora de la Gestión del Riesgo Empresarial

Información, Comunicación y Reporte

18. Aprovecha la Información y la Tecnología
19. Comunica Información sobre Riesgos
20. Informa sobre el Riesgo, la Cultura y el Desempeño

M.Sc. PEDRO BEJARANO V.

Referencias Bibliográficas

- ABELLA RUBIO Ramón. *COSO II y la gestión integral de riesgos del negocio*. Revista: Estrategia Financiera N° 225. Febrero 2006. Madrid. España.
- ARENS Alvin; ELDER Randal; BEASLEY Mark. *Auditoría. Un enfoque integral*. 11ra. edición. Edit. Pearson educación. México D.F. 2007
- COOPERS & LYBRAND. *Los nuevos conceptos del control interno (Informe COSO)*. Edit. Díaz de Santos. Madrid. España. 2007
- COSO Gestión del Riesgo Empresarial-Resumen Ejecutivo 2017. Documento Digital. En línea: Disponible en: <https://auditoresinternos.es/media/items/oso-2018-esp.original.pdf>
- ESTUPIÑAN GAITÁN Rodrigo. *Control Interno y Fraudes, Análisis de Informe COSO I, II y III*. 3ra. Edición. Edit. ECOE. Bogotá. Colombia. 2015
- ESTUPIÑAN GAITÁN Rodrigo. *Control Interno y Fraudes, con base en los ciclos transaccionales: Análisis de Informe COSO I y II*. 2da. Edición. Edit. ECOE. Bogotá. Colombia. 2006
- MANTILLA BLANCO Samuel. *Auditoría del Control Interno*. 3ra. Edición. Edit. ECOE. Bogotá. Colombia. 2016
- OLACEFS. "El control interno desde la perspectiva del enfoque COSO". Documento digital. Noviembre, 2015. En línea. Disponible en: <http://www.olacefs.com/el-control-interno-desde-la-perspectiva-del-enfoque-coso-su-aplicacion-y-evaluacion-en-el-sector-publico-ctpbq/> Consulta (05/09/2019)
- QUALPRO CONSULTING S.C. *Marco Integrado de Control Interno. Modelo COSO III* En línea. Disponible en: <https://www.ofstlaxcala.gob.mx/doc/material/27.pdf>
- SÁNCHEZ MARÍN, Ángela S. et al. *Acercamiento a fraudes contables y sus principales efectos* Revista Digital Trabajos de Grado UDEA, Vol.6, Núm.1 (2012) En línea: Disponible en: <https://aprendeonline.udea.edu.co/revistas/index.php/tgcontaduria/issue/view/2284/showToc> Consulta (25/08/2019)
- VALDIVIESO Carlos. *Principales Cambios en Relación a Coso 1992 y su Uso en la Evaluación del Control Interno*. CLAIN 2014. Documento Digital. En línea. Disponible en: <https://aechile.cl/2014/05/23/coso-2013-principales-cambios-en-relacion-a-coso-1992-y-su-uso-en-la-evaluacion-del-control-interno/> Consulta (05/09/2019)
- WHITTINGTON, O. Ray - PANY Karls (2005). *Principios de auditoría*. 14º edición. Edit. McGraw Hill. México D.F. 2005.