INSTITUTO DE INVESTIGACIÓN
CIENTÍFICA, CONTABLE Y FINANCIERA
FACULTAD DE CIENCIAS CONTABLES, AUDITORÍA
SISTEMAS DE CONTROL DE GESTIÓN Y FINANZAS
UNIVERSIDAD AUTÓNOMA GABRIEL RENÉ MORENO

NÚMERO DE GRUPO
240

XIII FERIA FACULTATIVA DE EMPRENDEDURISMO INNOVACIÓN Y TRANSFERENCIA DE TECNOLOGÍA

CATEGORÍA
EXPOSICIÓN

INTEGRANTES

JUANES MALDONADO JOSUE MARVIN	Reg. 219124515
ARAMAYO SILVANA KENIA	Reg. 215002431
SONCO QUISPE ALVARO	Reg. 221014624

DOCENTE GUIA

LIC. PINTO VIRUEZ MARIO GERARDO

INDICE

INFORME COSO
(I, II, III y IV)

INFORME COSO I (1992)

INTRODUCCION

El Informe COSO 1 fue desarrollado en 1992 por el Committee of Sponsoring Organizations of the Treadway Commission (COSO) con el objetivo de crear un marco universal para el control interno. Se ha convertido en una referencia fundamental para el desarrollo de sistemas efectivos de control interno, especialmente en el ámbito de la auditoría interna y la gestión de riesgos. Este modelo fue ampliamente adoptado después de la publicación de la Ley Sarbanes-Oxley en 2002, que exigió a las empresas una mayor transparencia y control sobre los informes financieros.

El propósito del modelo es ofrecer una estructura integrada que permita a las organizaciones alcanzar sus objetivos en las áreas de:

- Eficiencia y eficacia operativa.
- Confiabilidad de los informes financieros.
- Cumplimiento de las leyes y regulaciones.

MARCO CONCEPTUAL

El informe COSO se basa en la premisa de que un sistema de control interno eficaz puede mitigar los riesgos y proteger los intereses de las partes interesadas (accionistas, empleados, clientes, reguladores, etc.). La estructura del marco permite a las empresas adaptar los principios del control interno a sus propias necesidades y a los cambios en el entorno operativo.

OBJETIVOS DEL CONTROL INTERNO

El marco de COSO 1 reconoce tres categorías de objetivos:

- **Objetivos operativos:** Se centran en la eficiencia y efectividad de las operaciones de la empresa. El control interno debe ayudar a garantizar que los recursos se utilicen de manera eficiente y que los resultados de las operaciones sean los esperados.

- **Objetivos de información financiera:** Buscan asegurar que los informes financieros sean fiables, precisos y presentados de acuerdo con las normativas aplicables, como las Normas Internacionales de Información Financiera (NIIF) o los Principios de Contabilidad Generalmente Aceptados (PCGA).
- **Objetivos de cumplimiento:** Están diseñados para garantizar que la empresa cumpla con todas las leyes y regulaciones aplicables, evitando sanciones legales, multas y otros riesgos de no conformidad.

Estos objetivos están interrelacionados, y el éxito en cada área refuerza el control general de la organización.

COMPONENTES DEL INFORME COSO 1

1. **AMBIENTE DE CONTROL**

El ambiente de control establece el tono de la organización, influenciando la conciencia y la actitud de las personas hacia el control interno. Es el componente fundamental que afecta todos los demás. Incluye:

- **Valores éticos y conducta:** Las normas éticas establecidas por la alta dirección deben ser claras y comunicadas en toda la organización. Esto refuerza la importancia del comportamiento adecuado y la responsabilidad.
- **Gobierno corporativo:** La junta directiva y los comités, como el comité de auditoría, deben tener un rol activo en la supervisión del control interno. Su independencia y competencia son cruciales para asegurar que el control sea eficaz.
- **Asignación de autoridad y responsabilidad:** Las responsabilidades deben estar claramente definidas. Las líneas jerárquicas bien establecidas facilitan una supervisión efectiva y una mejor toma de decisiones.
- **Recursos humanos:** La contratación, capacitación y retención de personal competente es vital para el ambiente de control.

Ejemplo práctico: Una empresa con un ambiente de control sólido fomenta una cultura de ética y transparencia en la que los empleados se sienten responsables de reportar irregularidades.

EVALUACION DE RIESGOS

La evaluación de riesgos implica identificar, analizar y gestionar riesgos relevantes que puedan impedir el logro de los objetivos. Este proceso permite una anticipación y planificación eficaz para mitigar riesgos potenciales. Los pasos incluyen:

- **Identificación de riesgos:** Implica reconocer los eventos que podrían tener un impacto negativo en la organización.
- **Análisis de riesgos:** Una vez identificados, los riesgos deben ser evaluados en términos de probabilidad y gravedad de su impacto.
- **Respuesta al riesgo:** La organización debe definir su tolerancia al riesgo y establecer medidas para aceptarlo, reducirlo, evitarlo o transferirlo (por ejemplo, mediante seguros).

Ejemplo práctico: En una empresa manufacturera, la evaluación de riesgos puede identificar como posibles riesgos la interrupción de la cadena de suministro, lo que llevaría a diseñar un plan de contingencia para mitigar los impactos.

2. **ACTIVIDADES DE CONTROL**

- Las actividades de control son políticas y procedimientos que aseguran que las acciones necesarias se lleven a cabo para mitigar los riesgos identificados. Estas pueden incluir:
- **Segregación de funciones:** Evitar que una sola persona tenga control total sobre un proceso crítico, reduciendo el riesgo de fraude o error.
- **Autorizaciones y aprobaciones:** Asegurarse de que las transacciones significativas sean autorizadas y aprobadas por personal competente.
- **Controles físicos:** Implementar salvaguardas sobre los activos, como inventarios, efectivo o equipos, para protegerlos contra pérdidas o daños.

Ejemplo práctico: En una organización financiera, se implementan controles de autorización en las transferencias de fondos, donde dos personas deben aprobar cada transacción para garantizar que no haya irregularidades.

INFORMACION Y COMUNICACIÓN

La información y la comunicación se refieren a la recopilación y distribución de información relevante de manera oportuna. Para que el control interno funcione correctamente, es vital que toda la información pertinente fluya adecuadamente, tanto hacia arriba como hacia abajo en la estructura organizacional. Esto incluye:

- **Comunicación interna:** Los empleados deben entender sus responsabilidades y tener acceso a la información necesaria para llevar a cabo sus funciones de manera efectiva.
- **Comunicación externa:** Involucra la divulgación de información financiera precisa a accionistas, reguladores y otros interesados.

Ejemplo práctico: En una empresa pública, la comunicación eficaz implica la publicación periódica de informes financieros para que los accionistas puedan evaluar el desempeño de la empresa.

3. **SUPERVISION/MONITOREO**

La supervisión es un componente clave del control interno, ya que garantiza que los sistemas de control interno sigan siendo efectivos a lo largo del tiempo. La supervisión puede ser continua o llevarse a cabo mediante evaluaciones periódicas. Incluye:

- **Evaluaciones internas:** Los auditores internos deben realizar revisiones regulares del sistema de control interno.
- **Auditorías externas:** Los auditores externos proporcionan una revisión independiente de la efectividad del control interno y la exactitud de los informes financieros.
- **Retroalimentación y mejora continua:** Las deficiencias identificadas durante la supervisión deben corregirse rápidamente, y los sistemas de

control interno deben actualizarse para responder a los cambios en el entorno operativo.

Ejemplo práctico: En una empresa de software, las auditorías internas regulares de los sistemas de seguridad informática aseguran que las políticas de ciberseguridad sigan siendo efectivas y actualizadas.

APLICACIÓN PRÁCTICA Y BENEFICIOS

- ✓ **MEJORA DE LA EFICIENCIA OPERATIVA**

Al proporcionar una estructura clara y predefinida, el informe COSO permite a las empresas organizar mejor sus recursos, optimizar procesos y mejorar la toma de decisiones. Esto lleva a una mayor eficiencia en las operaciones diarias.

- ✓ **CONFIABILIDAD EN LA INFORMACIÓN FINANCIERA**

La implementación de controles sólidos asegura que los datos financieros sean precisos y presentados adecuadamente, lo que reduce la posibilidad de errores, fraudes o incumplimientos normativos.

- ✓ **CUMPLIMIENTO REGULATORIO**

Al adoptar el informe COSO, las organizaciones pueden cumplir más fácilmente con regulaciones locales e internacionales, minimizando riesgos legales y evitando multas o sanciones.

CONCLUSION

El Informe COSO 1 sigue siendo un marco indispensable para las organizaciones que buscan mantener un control interno eficaz. La interrelación de sus cinco componentes garantiza que las empresas puedan gestionar sus riesgos, mejorar la precisión de sus informes financieros y operar de manera eficiente, todo mientras cumplen con las regulaciones aplicables.

INFORME COSO 2 (ERM)

INTRODUCCIÓN

El Informe COSO 2, también llamado Gestión de Riesgos Empresariales (ERM), fue introducido en 2004 por el Committee of Sponsoring Organizations of the Treadway Commission (COSO) como una evolución del Informe COSO 1. Este marco amplía la visión tradicional de control interno al incluir un enfoque integral de la gestión de riesgos empresariales, ayudando a las organizaciones a identificar, evaluar y gestionar los riesgos en todas las áreas del negocio, en lugar de limitarse a riesgos financieros y de cumplimiento.

OBJETIVOS DE LA GESTIÓN DE RIESGOS EMPRESARIALES

El Informe COSO 2 organiza la gestión de riesgos en ocho componentes clave, diseñados para ayudar a las organizaciones a cumplir cuatro grandes categorías de objetivos:

- **Objetivos Estratégicos:** Están alineados con la misión y visión de la empresa, y se enfocan en la creación de valor a largo plazo.
- **Objetivos Operacionales:** Enfocados en la eficiencia de las operaciones y el uso efectivo de los recursos.
- **Objetivos de Información:** Garantizan la exactitud, integridad y confiabilidad de la información utilizada para la toma de decisiones.
- **Objetivos de Cumplimiento:** Aseguran que la empresa cumple con las leyes y regulaciones aplicables.

COMPONENTES DEL INFORME COSO 2

El Informe COSO 2 establece ocho componentes interrelacionados que ayudan a las organizaciones a gestionar de manera integral los riesgos empresariales:

AMBIENTE INTERNO

Este componente establece el tono de la organización y proporciona la base sobre la que se construyen los demás componentes. Incluye:

- **Cultura y valores éticos:** Al igual que en el COSO 1, los valores éticos de la organización y el compromiso de la alta dirección son esenciales.

- **Tolerancia al riesgo:** Define el nivel de riesgo que la organización está dispuesta a aceptar para lograr sus objetivos.
- **Filosofía de gestión de riesgos:** Se refiere a la actitud general de la organización frente a la toma de riesgos y cómo se gestionan.

Ejemplo práctico: Una empresa que fomente una cultura de transparencia y proactividad en la identificación de riesgos es más capaz de gestionarlos antes de que se materialicen.

1. ESTABLECIMIENTO DE OBJETIVOS

La definición clara de los objetivos empresariales es crucial para que la gestión de riesgos sea efectiva. Este componente garantiza que los objetivos de la empresa estén alineados con su misión y visión, y que se tenga en cuenta el riesgo al definir dichos objetivos. Es aquí donde se determina cómo los riesgos pueden afectar la consecución de esos objetivos.

- **Objetivos estratégicos:** Se evalúan los riesgos que podrían obstaculizar los planes estratégicos de la organización.
- **Objetivos específicos:** Cada departamento debe establecer sus propios objetivos dentro del marco general de la organización.

Ejemplo práctico: Una empresa de tecnología establece el objetivo de expandirse a nuevos mercados, pero evalúa los riesgos regulatorios y financieros asociados a esa expansión.

2. IDENTIFICACIÓN DE EVENTOS

Este componente implica identificar tanto eventos internos como externos que pueden afectar la consecución de los objetivos de la organización, ya sean riesgos (eventos negativos) u oportunidades (eventos positivos). La identificación de eventos es un proceso continuo que debe adaptarse a los cambios del entorno.

- **Eventos de riesgo:** Amenazas internas como fallos operativos, o externas como desastres naturales.

- **Oportunidades:** Innovaciones tecnológicas o cambios regulatorios que pueden ser aprovechados para generar valor.

Ejemplo práctico: Una empresa del sector energético identifica el riesgo de cambios en la legislación ambiental que podría afectar la viabilidad de sus proyectos, así como la oportunidad de invertir en energías renovables.

EVALUACIÓN DE RIESGOS

Una vez identificados los eventos, se deben evaluar los riesgos para determinar su gravedad y probabilidad. Esto permite priorizar los riesgos que deben ser gestionados primero. La evaluación de riesgos se realiza en dos dimensiones:

- **Probabilidad:** ¿Qué tan probable es que ocurra el riesgo?
- **Impacto:** Si ocurre, ¿cuál sería el efecto sobre la organización?

Las organizaciones pueden usar herramientas como matrices de riesgos para visualizar mejor los riesgos más críticos y tomar decisiones informadas.

Ejemplo práctico: En una empresa de fabricación, la evaluación de riesgos revela que la dependencia de un único proveedor clave representa un riesgo elevado que debe ser gestionado mediante la diversificación de la cadena de suministro.

3. RESPUESTA AL RIESGO

Una vez evaluados los riesgos, la organización debe decidir cómo responder a ellos. Hay varias opciones de respuesta:

- **Evitar:** Eliminar la actividad que genera el riesgo.
- **Reducir:** Implementar controles para mitigar el riesgo.
- **Compartir:** Transferir el riesgo a terceros (por ejemplo, mediante seguros).
- **Aceptar:** Aceptar el riesgo si su impacto es bajo o si no se puede mitigar de manera rentable.

Ejemplo práctico: Una empresa internacional decide reducir el riesgo cambiario utilizando coberturas para protegerse contra fluctuaciones adversas en el valor de las monedas.

ACTIVIDADES DE CONTROL

Las actividades de control son políticas y procedimientos que ayudan a asegurar que las respuestas al riesgo se implementen de manera efectiva. Estas actividades se extienden a todas las áreas de la organización y pueden incluir desde revisiones y verificaciones hasta autorizaciones y medidas de seguridad.

- **Controles preventivos:** Se diseñan para evitar la ocurrencia de un riesgo.
- **Controles correctivos:** Se aplican para corregir fallos en el sistema.

Ejemplo práctico: Una empresa de servicios financieros implementa revisiones automáticas para detectar transacciones sospechosas como parte de su actividad de control contra fraudes.

INFORMACIÓN Y COMUNICACIÓN

La gestión de riesgos solo será efectiva si la información relevante se comunica de manera oportuna y precisa. Esto incluye tanto la comunicación interna (dentro de la organización) como la externa (a accionistas y reguladores).

- **Comunicación interna:** Todos los niveles de la organización deben estar informados sobre los riesgos y sus respectivas responsabilidades en la gestión de esos riesgos.
- **Comunicación externa:** Involucra la divulgación de información a partes interesadas externas, como reguladores y accionistas.

Ejemplo práctico: Una empresa de productos de consumo utiliza un sistema de comunicación interna para alertar rápidamente a la alta dirección sobre riesgos potenciales en su cadena de suministro.

SUPERVISIÓN/MONITOREO

La supervisión garantiza que todo el proceso de gestión de riesgos funcione correctamente y que los controles implementados sean efectivos. Esto incluye tanto la supervisión continua como las revisiones periódicas. La auditoría interna y externa juegan un papel crucial aquí.

- **Supervisión continua:** Monitoreo regular de riesgos clave.

- **Evaluaciones periódicas:** Revisiones más detalladas que se realizan con cierta frecuencia para asegurar que los controles y respuestas siguen siendo adecuados.

Ejemplo práctico: Una empresa multinacional realiza auditorías internas anuales para revisar la efectividad de los controles establecidos en sus filiales.

APLICACIÓN PRÁCTICA Y BENEFICIOS

✓ VISIÓN INTEGRAL DEL RIESGO

El Informe COSO 2 permite a las organizaciones ver los riesgos desde una perspectiva más amplia, gestionando tanto riesgos estratégicos como operativos y financieros. Esto facilita una toma de decisiones más informada y proactiva.

✓ CREACIÓN DE VALOR

Una gestión de riesgos eficaz no solo protege a la organización contra pérdidas, sino que también identifica oportunidades para crear valor, como aprovechar cambios regulatorios o nuevas tecnologías.

✓ MEJORA DEL CUMPLIMIENTO

Al integrar el cumplimiento normativo dentro del proceso de gestión de riesgos, las organizaciones pueden evitar sanciones y proteger su reputación, asegurando que cumplan con todas las leyes y regulaciones aplicables.

CONCLUSIÓN

El Informe COSO 2 ofrece una visión más completa y estratégica de la gestión de riesgos empresariales. Al extender el marco de control interno para incluir riesgos operativos, estratégicos y financieros, ayuda a las organizaciones a gestionar mejor los riesgos, identificar oportunidades y mejorar el valor empresarial. La interrelación de los ocho componentes permite que las organizaciones adapten este marco a sus necesidades particulares, promoviendo una gestión de riesgos efectiva y sostenible.

INFORME COSO III (2013)

INTRODUCCIÓN

El Informe COSO 2013 (COSO III) fue una actualización significativa del marco original de COSO 1992. Si bien el objetivo general del modelo sigue siendo proporcionar un marco sólido para el control interno, el COSO 2013 aborda nuevas necesidades derivadas del entorno empresarial moderno, como avances en tecnología, globalización, y mayor enfoque en la gobernanza corporativa y la transparencia.

El marco actualizado tiene como objetivo mejorar la eficacia del control interno y ayudar a las organizaciones a alcanzar sus objetivos, centrados en:

- Eficacia y eficiencia de las operaciones.
- Fiabilidad de los informes financieros.
- Cumplimiento de leyes y regulaciones.

¿POR QUÉ SE ACTUALIZÓ EL MARCO COSO?

Desde la publicación del marco original en 1992, el mundo de los negocios cambió drásticamente:

- El auge de la tecnología transformó los procesos operacionales.
- Se introdujeron nuevas regulaciones, como la Ley Sarbanes-Oxley (SOX), que exigieron controles más rigurosos.
- Las expectativas de las partes interesadas aumentaron en términos de transparencia y gestión de riesgos.

La actualización de 2013 fue diseñada para asegurar que el marco de control interno se mantuviera relevante y aplicable a los desafíos modernos.

OBJETIVOS DEL CONTROL INTERNO

El Informe COSO 2013 mantiene las mismas tres categorías de objetivos que el marco de 1992, pero refina su enfoque para el contexto moderno:

- **Objetivos Operacionales:** Se centran en la eficacia y eficiencia de las operaciones.

- **Objetivos de Información:** Aseguran la confiabilidad, la precisión y la transparencia de los informes financieros y no financieros.
- **Objetivos de Cumplimiento:** Garantizan el cumplimiento de las leyes, reglamentaciones y políticas internas de la organización.

COMPONENTES DEL INFORME COSO 2013 (COSO III)

El COSO 2013 reafirma los cinco componentes del control interno del marco original, pero introduce una estructura más clara con la inclusión de 17 principios que explican detalladamente cómo aplicar los componentes. Estos componentes se presentan como parte de un "cubo de control interno", en el que se puede observar la interrelación de los objetivos y los componentes.

AMBIENTE DE CONTROL

El ambiente de control sigue siendo el fundamento del sistema de control interno y establece la cultura organizacional, influyendo en la ética y la integridad en toda la empresa. Este componente abarca:

- **Compromiso con la integridad y los valores éticos:** La alta dirección debe establecer y mantener una cultura ética.
- **Supervisión por parte de la junta directiva:** La junta directiva debe supervisar eficazmente el sistema de control interno.
- **Estructura organizativa:** La asignación de roles y responsabilidades debe estar clara y alineada con los objetivos del control interno.
- **Compromiso con la competencia:** La organización debe asegurarse de que su personal tenga las habilidades necesarias para llevar a cabo sus responsabilidades.
- **Responsabilidad:** Los empleados deben ser responsables de su desempeño en relación con los controles internos.

Ejemplo práctico: Una empresa que refuerza los valores éticos y crea canales claros para que los empleados reporten violaciones ayuda a mejorar el ambiente de control.

1. **EVALUACIÓN DE RIESGOS**

La evaluación de riesgos ahora se detalla más en COSO 2013, reconociendo que el control interno debe adaptarse continuamente a los riesgos emergentes. Incluye:

- **Especificación de objetivos:** La empresa debe establecer objetivos claros que permitan la identificación y evaluación de riesgos.
- **Identificación de riesgos:** La organización debe identificar y analizar los riesgos que puedan afectar el logro de los objetivos.
- **Evaluación de riesgos de fraude**: Se deben evaluar los riesgos de fraude en toda la organización.
- **Evaluación de los cambios:** La empresa debe evaluar los cambios internos y externos que puedan impactar el control interno.

Ejemplo práctico: Una empresa global puede evaluar los riesgos asociados con nuevas regulaciones internacionales que afectan sus operaciones en múltiples jurisdicciones.

ACTIVIDADES DE CONTROL

Las actividades de control son las políticas y procedimientos que se implementan para mitigar los riesgos identificados. En COSO 2013, esto incluye:

- **Selección y desarrollo de actividades de control:** La organización debe seleccionar y desarrollar actividades de control para mitigar los riesgos a niveles aceptables.
- **Controles tecnológicos:** Las actividades de control deben incluir medidas específicas para abordar riesgos tecnológicos.
- **Políticas y procedimientos:** Las políticas y procedimientos deben ser claras y seguidas de manera consistente.

Ejemplo práctico: Una empresa de comercio electrónico establece controles automáticos en sus sistemas para prevenir fraudes y errores en las transacciones online.

INFORMACIÓN Y COMUNICACIÓN

La información y la comunicación siguen siendo fundamentales para un sistema de control interno eficaz. Este componente asegura que se recopile, procese y distribuya la información relevante a tiempo. Incluye:

- **Uso de información relevante:** La empresa debe utilizar información relevante y de calidad para apoyar los controles internos.
- **Comunicación interna:** La comunicación dentro de la organización debe fluir adecuadamente, asegurando que los empleados comprendan sus roles en el sistema de control interno.
- **Comunicación externa:** La organización debe comunicar la información relevante a partes externas, incluidas las autoridades regulatorias y otras partes interesadas.

Ejemplo práctico: En una gran corporación, la implementación de un sistema de información financiera que informe a tiempo los datos relevantes a todos los niveles, garantiza una mejor toma de decisiones.

SUPERVISIÓN

La supervisión asegura que el control interno siga siendo eficaz con el tiempo. COSO 2013 resalta la importancia de la supervisión continua y las evaluaciones periódicas:

- **Actividades de supervisión continua:** Estas actividades deben integrarse en el día a día de la organización.
- **Evaluaciones periódicas:** Las auditorías internas y externas deben evaluar la eficacia del control interno.
- **Comunicación de deficiencias:** Las deficiencias detectadas deben ser comunicadas a los niveles apropiados de la organización para su corrección.

Ejemplo práctico: Una empresa implementa un sistema de supervisión continua para detectar problemas en tiempo real y corregir deficiencias antes de que se conviertan en fallos significativos.

PRINCIPALES CAMBIOS INTRODUCIDOS EN COSO 2013

COSO 2013 introduce varias mejoras respecto a la versión de 1992:

- **Enfoque en los Principios:** Los 17 principios explican cómo se deben implementar los cinco componentes del control interno, brindando mayor claridad y orientación.
- **Adaptación a la Tecnología:** El marco ahora aborda explícitamente los riesgos relacionados con la tecnología y la importancia de los controles tecnológicos.
- **Mayor Enfoque en el Fraude:** El nuevo marco pone un mayor énfasis en la evaluación de riesgos de fraude, reconociendo la creciente amenaza del fraude financiero y de ciberseguridad.
- **Evaluación del Cambio:** Reconoce la importancia de gestionar los cambios internos y externos que afectan el control interno, tales como nuevas regulaciones o fusiones.

APLICACIÓN PRÁCTICA Y BENEFICIOS

✓ MEJORA EN LA TRANSPARENCIA Y CONFIABILIDAD

COSO 2013 proporciona una mayor claridad en cómo implementar controles efectivos, lo que lleva a una mejor confiabilidad de los informes financieros y operativos.

✓ ADAPTABILIDAD A CAMBIOS TECNOLÓGICOS

El marco actualizado aborda las necesidades tecnológicas actuales, asegurando que las organizaciones gestionen eficazmente los riesgos derivados de la automatización, la digitalización y el cibercrimen.

✓ CUMPLIMIENTO NORMATIVO

El marco ayuda a las organizaciones a cumplir con regulaciones cada vez más estrictas, como la Ley Sarbanes-Oxley, que exige la certificación de la eficacia del control interno en los informes financieros.

CONCLUSIÓN

El Informe COSO 2013 (COSO III) es una evolución necesaria del marco original de 1992. Al proporcionar una estructura más clara y detallada con principios explícitos, el marco actualizado ayuda a las organizaciones a implementar sistemas de control

interno más efectivos, adaptados a los desafíos y riesgos del mundo moderno. La integración de la tecnología y el enfoque en la gestión de fraudes garantizan que las empresas puedan operar de manera eficiente, transparente y en conformidad con las regulaciones actuales.

INFORME COSO IV (2017)

INTRODUCCIÓN

El Informe COSO 2017, titulado oficialmente “Enterprise Risk Management – Integrating with Strategy and Performance” (Gestión de Riesgos Empresariales – Integración con Estrategia y Desempeño), es una actualización y expansión del marco de COSO II (2004). Esta versión de COSO refleja la evolución en la gestión de riesgos empresariales, integrándola con la estrategia y el desempeño organizacional, con el objetivo de ayudar a las empresas a gestionar los riesgos de manera más proactiva y alineada con sus metas estratégicas.

COSO 2017 proporciona un enfoque más holístico, donde la gestión de riesgos no es un proceso independiente, sino una parte integral del proceso de toma de decisiones estratégicas y operativas de la empresa.

¿POR QUÉ SE ACTUALIZÓ EL MARCO DE COSO?

El marco de COSO II (2004) fue útil para ayudar a las organizaciones a establecer un sistema para identificar y gestionar los riesgos, pero no abordaba suficientemente la necesidad de integrar la gestión de riesgos con la estrategia corporativa y el desempeño.

Con la globalización, la transformación digital y los cambios regulatorios, las empresas enfrentan nuevos desafíos. COSO 2017 ofrece una estructura más clara y aplicable, que permite a las organizaciones no solo gestionar los riesgos, sino también identificar oportunidades dentro del proceso.

OBJETIVOS DEL MODELO COSO 2017

El COSO 2017 tiene como objetivo ayudar a las organizaciones a lograr sus objetivos al ofrecer un enfoque estructurado para:

- Mejorar la toma de decisiones estratégicas.
- Alinear la gestión de riesgos con el rendimiento organizacional.
- Proteger y crear valor en las empresas mediante una gestión eficaz de los riesgos.

El marco promueve la integración del riesgo en cinco componentes interrelacionados, que permiten a las organizaciones comprender mejor su riesgo y tomar medidas más estratégicas.

COMPONENTES DEL MODELO COSO 2017

El marco se estructura en torno a cinco componentes principales, cada uno de los cuales contiene una serie de principios diseñados para guiar la gestión de riesgos de manera más efectiva. Estos componentes son:

GOBERNANZA Y CULTURA

Este componente establece la base para una gestión de riesgos efectiva, ya que la gobernanza dicta la dirección general y las expectativas para la gestión de riesgos, mientras que la cultura influye en cómo se perciben y gestionan los riesgos en la organización.

- **Principio 1:** El Consejo de Administración ejerce la supervisión del riesgo.
- **Principio 2:** La dirección y los líderes de la organización establecen valores y comportamientos que respaldan una cultura sólida para gestionar riesgos.
- **Principio 3:** La organización atrae, desarrolla y retiene personas capaces, alineadas con su estrategia.
- **Principio 4:** Se establecen roles y responsabilidades claras en relación con la gestión de riesgos.

Ejemplo práctico: Una empresa establece un código ético claro y realiza capacitaciones periódicas en todos los niveles sobre la importancia de la integridad y el manejo adecuado de los riesgos.

ESTRATEGIA Y ESTABLECIMIENTO DE OBJETIVOS

Este componente enfoca el proceso de alineación de la gestión de riesgos con la estrategia organizacional. El marco subraya la importancia de considerar los riesgos al definir la estrategia y establecer los objetivos de la empresa.

- **Principio 5:** La organización evalúa las posibles alternativas estratégicas, considerando cómo impacta el riesgo.
- **Principio 6:** La dirección formula objetivos que respaldan la estrategia y que consideran los riesgos relacionados.

- **Principio 7:** La organización analiza los impactos del riesgo en las alternativas estratégicas.
- **Principio 8:** Se establece el apetito de riesgo, es decir, la cantidad de riesgo que la organización está dispuesta a aceptar para alcanzar sus objetivos.

Ejemplo práctico: Una empresa en expansión evalúa los riesgos regulatorios y geopolíticos antes de establecer operaciones en nuevos países.

DESEMPEÑO

En este componente, la organización identifica y evalúa cómo los riesgos pueden afectar el desempeño organizacional. El marco de COSO 2017 reconoce que no todos los riesgos son negativos; algunos pueden presentar oportunidades si se gestionan adecuadamente.

- **Principio 9:** La organización identifica riesgos que podrían afectar la consecución de sus objetivos.
- **Principio 10:** La organización evalúa la severidad de los riesgos, tanto cualitativa como cuantitativamente.
- **Principio 11:** La organización prioriza riesgos, con base en su severidad e impacto en los objetivos estratégicos.
- **Principio 12:** Se implementan respuestas a los riesgos, eligiendo las acciones más adecuadas para gestionar los riesgos (aceptar, mitigar, transferir o evitar).
- **Principio 13:** La organización desarrolla y evalúa un portafolio de riesgos para optimizar la gestión integral de los riesgos.

Ejemplo práctico: Una empresa tecnológica evalúa el riesgo de ciberataques y desarrolla un plan de mitigación que incluye la actualización constante de sus sistemas de seguridad.

REVISIÓN Y REVISIÓN CONTINUA

La revisión del desempeño y la evaluación continua de los riesgos son esenciales para garantizar que los controles y procesos de gestión de riesgos sigan siendo efectivos. La revisión y monitoreo permite a las organizaciones ajustar sus respuestas a medida que cambian las condiciones del entorno.

- **Principio 14:** La organización revisa el desempeño de los riesgos de forma continua y cómo impactan en el logro de los objetivos.
- **Principio 15:** Se implementan procesos para evaluar el riesgo de manera regular, asegurando que los controles funcionen de manera eficaz.

Ejemplo práctico: Una empresa de manufactura realiza auditorías internas trimestrales para revisar cómo sus procesos de gestión de riesgos están impactando en la eficiencia operativa.

INFORMACIÓN, COMUNICACIÓN E INFORME

La comunicación efectiva es crucial para que todas las partes interesadas comprendan los riesgos de la organización y cómo se están gestionando. Este componente asegura que la información fluya de manera adecuada dentro de la organización y hacia partes externas relevantes.

- **Principio 16:** La organización utiliza sistemas de información adecuados para capturar y transmitir información relacionada con los riesgos.
- **Principio 17:** La empresa comunica la información de riesgos internamente a las personas que la necesitan para tomar decisiones informadas.
- **Principio 18:** La organización informa externamente sobre los riesgos a las partes interesadas, garantizando transparencia y cumplimiento regulatorio.

Ejemplo práctico: Una organización financiera desarrolla un sistema de reportes automáticos que distribuye informes semanales sobre riesgos clave a los directores de operaciones y cumplimiento normativo.

PRINCIPALES CAMBIOS INTRODUCIDOS EN COSO 2017

El marco de COSO 2017 introduce varios cambios importantes en comparación con versiones anteriores:

- ✓ **Integración con la Estrategia:** El marco ahora pone un fuerte énfasis en la necesidad de alinear la gestión de riesgos con los objetivos estratégicos.
- ✓ **Mayor Enfoque en la Cultura Organizacional:** COSO 2017 reconoce el papel crucial de la cultura en la percepción y gestión de los riesgos.

- ✓ **Alineación con el Desempeño:** Se resalta la importancia de gestionar riesgos no solo para evitar pérdidas, sino también para mejorar el desempeño y crear valor.
- ✓ **Un enfoque proactivo en la Identificación de Riesgos:** COSO 2017 enfatiza la necesidad de identificar riesgos de manera temprana para poder aprovechar oportunidades y mitigar amenazas.

APLICACIÓN PRÁCTICA Y BENEFICIOS

✓ INTEGRACIÓN CON LOS PROCESOS DE NEGOCIO

COSO 2017 proporciona una estructura clara para que las organizaciones integren la gestión de riesgos en su toma de decisiones, haciendo que los riesgos se consideren desde la planeación estratégica hasta las operaciones diarias.

✓ MEJORA EN LA TOMA DE DECISIONES

Al integrar la gestión de riesgos en la estrategia, las empresas pueden tomar decisiones más informadas y optimizadas, basadas en un entendimiento claro de los riesgos y oportunidades.

✓ VALORACIÓN DE OPORTUNIDADES

El nuevo enfoque reconoce que no todos los riesgos son negativos. Gestionar los riesgos de manera eficaz puede ayudar a las empresas a identificar nuevas oportunidades para mejorar el rendimiento.

CONCLUSIÓN

El Informe COSO 2017 ofrece una visión más moderna y holística de la gestión de riesgos, integrando esta disciplina con la estrategia y el desempeño. Las organizaciones que implementen este marco pueden no solo protegerse mejor frente a los riesgos, sino también aprovechar las oportunidades para mejorar su rendimiento y crear valor a largo plazo.

DIFERENCIAS ENTRE LOS MODELOS COSO 1, 2, 3 Y 4

Características	COSO 1 (1992)	COSO 2 ERM (2004)	COSO 3 (2013)	COSO 4 ERM (2017)
Enfoque principal	Control interno (financiero y operativo)	Gestión integral de riesgos empresariales	Control interno (actualizado)	Gestión de riesgos integrada con la estrategia
Objetivo	Garantizar informes financieros confiables, cumplimiento normativo y eficiencia	Alinear la gestión de riesgos con los objetivos estratégicos	Integrar controles internos con el rendimiento organizacional	Gestión de riesgos alineada con la estrategia y el desempeño
Componentes	5 componentes de control interno	8 componentes de ERM	5 componentes de control interno (con 17 principios)	5 componentes de ERM (actualizados)
Principios	No definidos	No definidos	17 principios	Actualización basada en principios clave
Integración con la estrategia	No se enfoca directamente	Algunos elementos estratégicos, pero no central	Mejor integración con los objetivos organizacionales	Enfoque explícito en la integración con la estrategia

Enfoque en la cultura organizacional	Limitado	Limitado	Mayor énfasis en el ambiente de control	Cultura y gobernanza son pilares clave
Enfoque en la tecnología y ciberseguridad	Limitado	Moderado	Énfasis en riesgos tecnológicos	Riesgos tecnológicos más presentes y gestionados a nivel estratégico

CONCLUSIÓN

- ✓ COSO 1992 fue la base para el control interno, enfocado en la fiabilidad financiera.
- ✓ COSO 2004 amplió ese enfoque al incluir una gestión integral de riesgos.
- ✓ COSO 2013 modernizó el control interno, integrando mejor los controles con los objetivos organizacionales y añadiendo un enfoque más claro con 17 principios.
- ✓ COSO 2017 ofrece un marco actualizado para la gestión de riesgos empresariales, alineando la estrategia, el riesgo y el rendimiento organizacional, con un enfoque más proactivo y adaptado a las necesidades actuales.