COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Controles Internos COSO Framework

Septiembre 2018

Profesor: Msc. Rafael Salas Mercado

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Perfil

Ejecutivo senior, con extensa experiencia en la administración de grandes empresas, gestión integral de riesgos, gobierno corporativo y foco en el resultado. He ocupado diferentes posiciones gerenciales en las áreas de Gestión Empresarial de Riesgos, Operaciones, Tecnología y Creación y Transformación de Negocios en corporaciones internacionales como Zurich y Citibank. Poseo 20 años de experiencia en el sector financiero en banca, seguros, pensiones y valores. En relación a trabajos para el Estado, trabajé en el segmento de la regulación y varios proyectos gubernamentales interinstitucionales. Durante el ejercicio de mis funciones gerenciales he desarrollado habilidades para mejorar la rentabilidad y la productividad usando las mejores practicas de administración, gestión de empresas y tecnologías de información.

2

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Agenda

Sesión 1: Introducción a Controles Internos según COSO.
Sesión 2: Vinculación de Gestión de Riesgos y Control Interno.
Sesión 3: Taxonomía de los Controles Internos.
Sesión 4: Como Implementar un marco de Control Interno – P. 1.
Sesión 5: Como Implementar un marco de Control Interno – P. 2.
Sesión 6: Requerimientos de la Circular 565/2018

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Introducción

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Las organizaciones están siendo continuamente conducidas hacia la **aplicación de estándares más elevados de Control Interno y Administración y Gestión de Riesgos**

Mision de COSO

"... Proporcionar liderazgo intelectual a través del **desarrollo de marcos generales y orientaciones sobre la Gestión del Riesgo, Control Interno y Disuasión del Fraude**, diseñado para mejorar el desempeño organizacional y reducir el alcance del fraude en las organizaciones."

www.coso.org/aboutus.htm

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Principios

El **Marco de COSO 2013** mantiene la definición de Control Interno y los cinco componentes de control interno, pero al mismo tiempo incluye **mejoras y aclaraciones con el objetivo de facilitar el uso y su aplicación en las Entidades**.

Puntos de Interés

A través de esta actualización, COSO propone desarrollar el marco original, empleando **"principios" y "puntos de interés"** con el objetivo de **ampliar y actualizar los conceptos de control interno** previamente planteado sin dejar de **reconocer los cambios en el entorno** empresarial y operativo.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

17 Inclusión de **diecisiete principios de control** que representan el elemento fundamental **asociados a cada componente del control** y que estos deben de estar operando en forma conjunta.

Proporciona **"puntos de interés"**, o características importantes de los principios; al tiempo que reconoce que el **diseño y la implementación de controles relevantes** para cada principio y componente, **requiere de juicio y serán diferentes de acuerdo a la organización**.

77

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Responsabiliza a la administración quien deberá asegurar que **cada uno de los componentes y principios relevantes del control interno deben estar presente y en funcionamiento** con el fin de contar con un sistema eficaz de control interno.

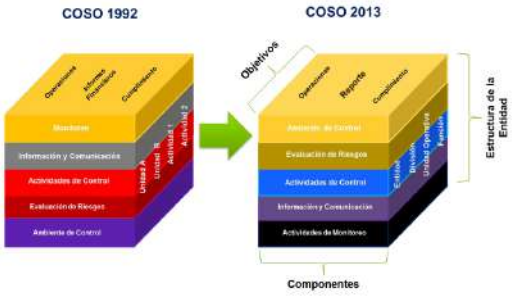
Concluyendo que **una deficiencia importante en un componente o principio de control no se puede mitigar con eficacia por la función de otros componentes y principios de control.**

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

- **Adaptabilidad** del Marco de COSO
- Inclusión de **buenas prácticas de Gobierno**
- Fortalece la rendición de cuentas
- Relevancia del fraude
- Mayor nivel de **competencia de los funcionarios**
- Integración de conceptos como **riesgo inherente, nivel de tolerancia**
- Consideraciones sobre los servicios de ***out-sourcing*** **y como la Administración los monitorea**
- Relevancia de los **Sistemas de Información**, se relaciona con 14 de los 17 principios el tema de TI

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Los Cambios



COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

De los cinco componentes de Control Interno que establece COSO, se deberán considerar los **17 principios** que representan los conceptos fundamentales relacionados con los componentes para el establecimiento de un **efectivo Sistema de Control Interno**

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Definición de Control Interno

El control interno es un proceso llevado a cabo por:

- El consejo de administración,
- La dirección (Gerente General y Gerentes)
- El resto del personal de una entidad.

Esta diseñado con el objeto de proporcionar un grado de seguridad razonable en cuanto a la consecución de objetivos:

- Operativos
- De información
- De Cumplimiento

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

En la práctica

- Esta orientado a la consecución de los objetivos operativos, de información y cumplimiento
- Es un proceso de tareas y actividades continuas, no es un fin en si mismo.
- Las tareas y actividades deben ser ejecutadas por personas de todos los niveles. *No son manuales y procedimientos.*
- Es capaz de proporcionar una seguridad razonable a la alta dirección y a los accionistas.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

En la evidencia

- Es un conjunto de normas y procedimientos de Control Interno.
- Tiene una estructura.
- Tiene sistemas.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Entendiendo el Cubo

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Objetivos

Cada entidad tiene una misión, la cual determina los objetivos y las estrategias necesarias para cumplirla. Los objetivos pueden ser establecidos mediante un proceso estructurado o informal dependiendo de la entidad, y **junto con la evaluación de los puntos fuertes y débiles de la entidad, y de las oportunidades y amenazas del entorno, define una estrategia global.**

Es responsabilidad de la Administración y la Alta Dirección establecer los objetivos del negocio y **es necesario fijar los objetivos con carácter previo al diseño e implementación del sistema de control interno**, con el fin de controlar y mitigar de manera adecuada los riesgos que afectan a dichos objetivos.

Los objetivos deben complementarse, estar relacionados entre sí y ser coherentes con las capacidades y expectativas de la entidad y las unidades empresariales y sus funciones.
Establecer objetivos **es un requisito previo para un control interno eficaz**. Los objetivos **proporcionan las metas medibles** hacia las que la entidad se mueve al desarrollar sus actividades.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Objetivos

Esta responsabilidad está establecida en los procesos de la administración, como se presenta a continuación:

- Determinar los objetivos estratégicos y seleccionar la estrategia dentro del contexto de la entidad establecido en su misión y visión.
- Establecer los objetivos de la entidad y desarrollar la tolerancia al riesgo con base en los requerimientos de la entidad según las circunstancias.
- Alinear los objetivos con la estrategia de la entidad y el apetito general del riesgo.
- Establecer los objetivos generales y específicos para la entidad y sus niveles según sean las circunstancias.

El Marco Integrado de Control Interno establece **tres categorías de objetivos** que permiten a las organizaciones centrarse en diferentes aspectos del control interno.

- **Objetivos operativos**
- **Objetivos de Información**
- **Objetivos de Cumplimiento**

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Objetivos Operativos

Estos objetivos se relacionan con el cumplimiento de la misión y visión de la entidad.
Hacen referencia a la efectividad y eficiencia delas operaciones, incluidos sus objetivos de rendimiento financiero y operacional, y la protección de sus activos frente a posibles pérdidas. (Balanced scorecard)

Por lo tanto, **estos objetivos constituyen la base para la evaluación del riesgo en relación con la protección de los activos de la entidad, y la selección y desarrollo de los controles necesarios para mitigar dichos riesgos.**

Los objetivos operativos deben reflejar el entorno empresarial, industrial y económico en que se involucra la entidad; y **están relacionados con el mejoramiento del desempeño financiero, la productividad, la calidad, las prácticas ambientales, y la innovación y satisfacción de empleados y clientes**.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Objetivos de Información

Estos objetivos se refieren a la preparación de reportes para uso de la organización y los accionistas, teniendo en cuenta la veracidad, oportunidad y transparencia.
Estos reportes relacionan la **información financiera y no financiera interna y externa** y **abarcan aspectos de confiabilidad, oportunidad, transparencia** y demás conceptos establecidos por los reguladores, organismos reconocidos o políticas de la entidad.
La presentación de **informes a nivel externo** da respuesta a las regulaciones y normativas establecidas y a las solicitudes de los grupos de interés, y los **informes a nivel interno** atienden a las necesidades al interior de la organización tales como: la estrategia de la entidad, plan operativo y métricas de desempeño.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Objetivos de Información

Reportes Financiero Externo
- Cuentas anuales
- Estados financieros intermedios
- Publicación de resultados
- Distribución de utilidades

Reporte Financiero Interno
- Estados financieros de las divisiones
- Cash-flow / Presupuesto
- Cálculos de Covenant

Reportes No Financiero Externo
- Informe de Control Interno
- Memoria de sostenibilidad
- Plan estratégico
- Custodia de activos

Reporte No Financiero Interno
- Utilización de activos
- Encuestas de satisfacción del cliente
- Indicadores clave de riesgo
- Reportes al consejo

Requisitos para la información

Relevancia
Representación exacta
Comparabilidad
Verificabilidad
Oportunidad
Comprensibilidad

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Objetivos de Cumplimiento

Están relacionados con el cumplimiento de las leyes y regulaciones a las que está sujeta la entidad. La entidad debe desarrollar sus actividades en función de las leyes y normas específicas.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Componentes

El sistema de control interno está divido en cinco componentes integrados que se relacionan con los objetivos de la empresa:

- **entorno de control,**
- **evaluación de los riesgos,**
- **actividades de control,**
- **información y comunicación**
- **actividades de monitoreo y supervisión**.

Un adecuado entorno de control, una metodología de evaluación de riesgos, un sistema de elaboración y difusión de información oportuna y fiable por de la organización y un proceso de monitoreo eficiente, apoyados en actividades de control efectivas, se constituyen en poderosas herramientas gerenciales.

Los cinco componentes 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.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

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.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Entorno de Control

Un entorno de control ineficaz puede tener consecuencias graves, tales como pérdida financiera, pérdida de imagen o un fracaso empresarial.

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.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Entorno de Control

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 atmosfera 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.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

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.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

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.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Actividades de Control

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.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

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.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Información y Comunicación

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.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Información y Comunicación

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.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Información y Comunicación

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, y 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.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Actividades de 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.

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.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Pincipios

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Ambiente de control

01/ La organización demuestra compromiso por la **integridad y valores éticos.**

02/ El Consejo de Administración demuestra una independencia de la administración y **ejerce una supervisión del desarrollo y el rendimiento** de los controles internos.

03/ La Administración establece, con la aprobación del Consejo, las **estructuras, líneas de reporte y las autoridades y responsabilidades** apropiadas en la búsqueda de objetivos.

04/ La organización demuestra un **compromiso a atraer, desarrollar y retener personas**competentes en alineación con los objetivos.

05/ La organización **retiene individuos comprometidos** con sus responsabilidades de control interno en la búsqueda de objetivos.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Evaluación de Riesgos

06/ La organización **especifica objetivos**con suficiente claridad para permitir **la identificación y valoración de los riesgos** relacionados a los objetivos.

07/ La organización **identifica**los riesgos sobre el cumplimiento de los objetivos a través de la entidad **y analiza los riesgos** para determinar cómo esos riesgos deben de administrarse.

08/ La organización **considera la posibilidad de fraude**en la evaluaciónde riesgos para el logro de los objetivos.

09/ La organización **identifica y evalúa cambios** que pueden impactar significativamente al sistema de control interno.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Actividades de control

10/ La organización elige y desarrolla **actividades de control que contribuyen a la mitigación de riesgos** para el logro de objetivos a niveles aceptables.

11/ La organización elige y desarrolla **actividades de control generales sobre la tecnología**para apoyar el cumplimiento de los objetivos.

12/ La organización **despliega actividades de control a través de políticas** que establecen lo que se espera **y procedimientos** que ponen dichas políticas en acción

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Información y comunicación

13/ La organización obtiene o genera y usa **información relevante y de calidad**para apoyar el funcionamiento del control interno.

14/ La organización **comunica información internamente, incluyendo objetivos y responsabilidades sobre el control interno**, necesarios para apoyar funcionamiento del control interno.

15/ La organización **se comunica con grupos externos** con respecto a situaciones que afectan el funcionamiento del control interno.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Actividades de monitoreo

16/ La organización **selecciona, desarrolla, y realiza evaluaciones** continuas y/o separadas para comprobar cuando los componentes de control interno están presentes y funcionando.

17/ La organización **evalúa y comunica deficiencias de control interno** de manera adecuada a aquellos grupos responsables de tomar la acción correctiva, incluyendo la Alta Dirección y el Consejo de Administración, según sea apropiado.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Ejercicio

- Dibujar la estructura de control interno
- Traer las políticas, normas, procedimientos de Control Interno.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Puntos de Interés

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Ambiente de control

1.- La organización demuestra compromiso con la integridad y los valores éticos

Establece el tono de la gerencia. la Junta Directiva, la Alta Gerencia y el personal supervisor están comprometidos con los valores y principios éticos y los refuerzan en sus actuaciones.
Establece estándares de conducta. La integridad y los valores éticos son definidos en los estándares de conducta de la entidad y entendidos en todos los niveles de la organización y por los proveedores de servicio externos y socios de negocios.
Evalúa la adherencia a estándares de conducta. Los procesos están en su lugar para evaluar el desempeño de los individuos y equipos en relación con los estándares de conducta esperados.
Aborda y decide sobre desviaciones en forma oportuna. Las desviaciones de los estándares de conducta esperados en la entidad son identificadas y corregidas oportuna y adecuadamente.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Ambiente de control

2. El consejo de administración demuestra independencia de la dirección y ejerce la supervisión del desempeño del sistema de control interno.

Establece las responsabilidades de supervisión de la dirección. La Junta Directiva identifica y acepta su responsabilidad de supervisión con respecto a establecer requerimientos y expectativas.
Aplica experiencia relevante. La Junta directiva define, mantiene y periódicamente evalúa las habilidades y experiencia necesaria entre sus miembros.
Conserva o delega responsabilidades de supervisión.
Opera de manera independiente. La Junta Directiva tiene suficientes miembros, quienes son independientes de la Administración y objetivos en evaluaciones y toma de decisiones.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Ambiente de control

Brinda supervisión sobre el Sistema de Control Interno. La Junta Directiva conserva la responsabilidad de supervisión del diseño, implementación y conducción del Control Interno de la Administración:

- **Entorno de Control:** establece integridad y valores éticos, estructuras de supervisión, autoridad y responsabilidad, expectativas de competencia, y rendición de cuentas a la Junta.
- **Evaluación de Riesgos:** monitorea las evaluaciones de riesgos de la administración para el cumplimiento de los objetivos, incluyendo el impacto potencial de los cambios significativos, fraude, y la evasión del control interno por parte de la administración.
- **Actividades de Control:** provee supervisión a la Alta Dirección en el desarrollo y cumplimiento de las actividades de control.
- **Información y Comunicación**: analiza y discute la información relacionada con el cumplimiento de los objetivos de la entidad.
- **Actividades de Supervisión:** evalúa y supervisa la naturaleza y alcance de las actividades de monitoreo y la evaluación y mejoramiento de la administración de las deficiencias.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Ambiente de control

3. La dirección establece con la supervisión del Consejo, las estructuras, líneas de reporte y los niveles de autoridad y responsabilidad apropiados para la consecución de los objetivos.

Considera todas las estructuras de la entidad. La Administración y la Junta Directiva consideran las estructuras múltiples utilizadas (incluyendo unidades operativas, entidades legales, distribución geográfica, y proveedores de servicios externos) para apoyar la consecución de los objetivos
Establece líneas de reporte. La Administración diseña y evalúa las líneas de reporte para cada estructura de la entidad, para permitir la ejecución de autoridades y responsabilidades, y el flujo de información para gestionar las actividades de la entidad
Define, asigna y delimita autoridades y responsabilidades. La Administración y la Junta Directiva delegan autoridad, definen responsabilidades, y utilizan procesos y tecnologías adecuadas para asignar responsabilidad, segregar funciones según sea necesario en varios niveles de la organización:

- **Junta directiva:** conserva autoridad sobre las decisiones significativas y revisa las evaluaciones de la administración y las limitaciones de autoridades y responsabilidades.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Ambiente de control

- **Alta Dirección:** establece instrucciones, guías, y control habilitando a la administración y otro personal para entender y llevar a cabo sus responsabilidades de control interno.
- **Administración:** guía y facilita la ejecución de las instrucciones de la Alta Dirección dentro de la entidad y sus sub-unidades.
- **Personal:** entiende los estándares de conducta de la entidad, los riesgos evaluados para los objetivos, y las actividades de control relacionadas con sus respectivos niveles de la entidad, la información esperada y los flujos de comunicación, así como las actividades de monitoreo relevantes para el cumplimiento de los objetivos.
- **Proveedores de servicios externos:** cumple con la definición de la administración del alcance de la autoridad y la responsabilidad para todos los que no sean empleados comprometidos.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Ambiente de control

4. La organización demuestra compromiso para atraer, desarrollar y retener a profesionales competentes, en concordancia con los objetivos de la organización

Establece políticas y prácticas. Las políticas y prácticas reflejan las expectativas de competencia necesarias para apoyar el cumplimiento de los objetivos.
Evalúa la competencia y direcciona las deficiencias. La Junta Directiva y la Administración evalúan la competencia a través de la organización y en los proveedores de servicios externos, de acuerdo con las políticas y prácticas establecidas, y actúa cuando es necesario direccionando las deficiencias.
Atrae, desarrolla y retiene profesionales. La organización provee la orientación y la capacitación necesaria para atraer, desarrollar y retener personal suficiente y competente y proveedores de servicios externos para apoyar el cumplimiento de los objetivos.
Planea y se prepara para sucesiones. La Alta Dirección y la Junta Directiva desarrollan planes de contingencia para la asignación de la responsabilidad importante para el control interno

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Ambiente de control

5. La organización define las responsabilidades de las personas a nivel de control interno para la consecución de los objetivos

Hace cumplir la responsabilidada través de estructuras, autoridades y responsabilidades. La Administración y la Junta Directiva establecen los mecanismos para comunicar y mantener profesionales responsables para el desempeño de las responsabilidades de control interno a través de la organización, e implementan acciones correctivas cuando es necesario.
Establece medidas de desempeño, incentivos y premios. La Administración y la Junta Directiva establecen medidas de desempeño, incentivos, y otros premios apropiados para las responsabilidades en todos los niveles de la entidad, reflejando dimensiones de desempeño apropiadas y estándares de conducta esperados, y considerando el cumplimiento de objetivos a corto y largo plazo.
Evalúa medidas de desempeño, incentivos y premios para la relevancia en curso. La Administración y la Junta Directiva alinean incentivos y premios con el cumplimiento de las responsabilidades de control interno para la consecución de los objetivos.
Considera presiones excesivas. La administración y la Junta Directiva evalúan y ajustan las presiones asociadas con el cumplimiento de los objetivos; asimismo asignan responsabilidades, desarrollan medidas de desempeño y evalúan el desempeño
Evalúa desempeño y premios o disciplina losindividuos. La Administración y la Junta Directiva evalúan el desempeño de las responsabilidades de control interno, incluyendo la adherencia a los estándares de conducta y los niveles de competencia esperados, y proporciona premios o ejerce acciones disciplinarias cuando es apropiado

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Evaluación de Riesgos

6. La organización define los objetivos con suficiente claridad para permitir la identificación y evaluación de los riesgos relacionados

Objetivos Operativos:
- Refleja las elecciones de la administración.
- Considera la tolerancia al riesgo.
- Incluye las metas de desempeño operativo y financiero.
- Constituye una base para administrar los recursos.

Objetivos de Reporte Financiero Externo:
- Cumple con los estándares contables aplicables.
- Considera la materialidad.
- Refleja las actividades de la entidad.

Objetivos de Reporte no Financiero Externo:
- Cumple con los estándares y marcos externos establecidos.
- Considera los niveles de precisión requeridos.
- Refleja las actividades de la entidad.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Evaluación de Riesgos

Objetivos de Reporte interno:
- Refleja las elecciones de la administración.
- Considera el nivel requerido de precisión.
- Refleja las actividades de la entidad.

Objetivos de Cumplimiento:
- Refleja las leyes y regulaciones externas.
- Considera la tolerancia al riesgo.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Evaluación de Riesgos

7. La organización identifica los riesgos para la consecución de sus objetivos en todos los niveles de la entidad y los analiza como base sobre la cual determina cómo se deben gestionar

Incluye la entidad, sucursales, divisiones, unidad operativa y niveles funcionales. La organización identifica y evalúa los riesgos a nivel de la entidad, sucursales, divisiones, unidad operativa y niveles funcionales relevantes para la consecución de los objetivos.
Evalúa la consideración de factores externos e internos en la identificación de los riesgos que puedan afectar a los objetivos.
Involucra niveles apropiados de administración. La dirección evalúa si existen mecanismos adecuados para la identificación y análisis de riesgos.
Analiza la relevancia potencial de los riesgos identificados y entiende la tolerancia al riesgo de la organización.
Determina la respuesta a los riesgos. La evaluación de riesgos incluye la consideración de cómo el riesgo debería ser gestionado y si aceptar, evitar, reducir o compartir el riesgo.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Evaluación de Riesgos

8. La organización considera la probabilidad de fraude al evaluar los riesgos para la consecución de los objetivos

Considera varios tipos de fraude: La evaluación del fraude considera el Reporte fraudulento, posible pérdida de activos y corrupción.
La evaluación del riesgo de fraude evalúa incentivos y presiones
La evaluación del riesgo de fraude tiene en consideración el riesgo de fraude por adquisiciones no autorizadas, uso o enajenación de activos, alteración de los registros de información, u otros actos inapropiados.
La evaluación del riesgo de fraude considera cómo la dirección u otros empleados participan en, o justifican, acciones inapropiadas.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Evaluación de Riesgos

9. La organización idéntica y evalúa los cambios que podrían afectar significativamente al sistema de control interno

Evalúa cambios en el ambiente externo. El proceso de identificación de riesgos considera cambios en los ambientes regulatorio, económico, y físico en los que la entidad opera.
Evalúa cambios en el modelo de negocios. La organización considera impactos potenciales de las nuevas líneas del negocio, composiciones alteradas dramáticamente de las líneas existentes de negocios, operaciones de negocios adquiridas o de liquidación en el sistema de control interno, rápido crecimiento, el cambio de dependencia en geografías extranjeras y nuevas tecnologías.
Evalúa cambios en liderazgo. La organización considera cambios en administración y respectivas actitudes y filosofías en el sistema de control interno.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Actividades de control

10. La organización define y desarrolla actividades de control que contribuyen a la mitigación de los riesgos hasta niveles aceptables para la consecución de los objetivos

Se integra con la evaluación de riesgos. Las actividades de control ayudan a asegurar que las respuestas a los riesgos que direccionan y mitigan los riesgos son llevadas a cabo.
Considera factores específicos de la entidad. La administración considera cómo el ambiente, complejidad, naturaleza y alcance de sus operaciones, así como las características específicas de la organización, afectan la selección y desarrollo de las actividades de control.
Determina la importancia de los procesos del negocio. La administración determina la importancia de los procesos del negocio en las actividades de control.
Evalúa una mezcla de tipos de actividades de control. Las actividades de control incluyen un rango y una variedad de controles que pueden incluir un equilibrio de enfoques para mitigar los riesgos teniendo en cuenta controles manuales y automatizados, y controles preventivos y de detección.
Considera en qué nivel las actividades son aplicadas. La administración considera las actividades de control en varios niveles de la entidad.
Direcciona la segregación de funciones. La administración segrega funciones incompatibles, y donde dicha segregación no es práctica, la administración selecciona y desarrolla actividades de control alternativas.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Actividades de control

11. La organización define y desarrolla actividades de control a nivel de entidad sobre la tecnología para apoyar la consecución de los objetivos

Determina la relación entre el uso de la tecnología en los procesos del negocio y los controles generales de tecnología: La dirección entiende y determina la dependencia y la vinculación entre los procesos de negocios, las actividades de control automatizadas y los Controles Generales de tecnología.
Establece actividades de control para la infraestructura tecnológica relevante: la Dirección selecciona y desarrolla actividades de control diseñadas e implementadas para ayudar a asegurar la completitud, precisión y disponibilidad de la tecnología.
Establece las actividades de control para la administración de procesos relevantes de seguridad: la dirección selecciona y desarrolla actividades de control diseñadas e implementadas para restringir los derechos de acceso, con el fin de proteger los activos de la organización de amenazas externas.
Establece actividades de control relevantes para los procesos de adquisición, desarrollo y mantenimiento de la tecnología: la dirección selecciona y desarrolla actividades de control sobre la adquisición, desarrollo y mantenimiento de la tecnología y su infraestructura.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Actividades de control

12. La organización despliega las actividades de control a través de políticas que establecen las líneas generales del control interno y procedimientos.

Establece políticas y procedimientos para apoyar el despliegue de las directivas de la administración: la administración establece actividades de control que están construidas dentro de los procesos del negocio y las actividades del día a día de los empleados a través de políticas estableciendo lo que se espera y los procedimientos relevantes especificando acciones.
Establece responsabilidad y rendición de cuentas para ejecutar las políticas y procedimientos: la administración establece la responsabilidad y rendición de cuentas para las actividades de control con la administración (u otro personal asignado) de la unidad de negocios o función en el cual los riesgos relevantes residen.
Funciona oportunamente: el personal responsable desarrolla las actividades de control oportunamente, como es definido en las políticas y procedimientos.
Toma acciones correctivas: el personal responsable investiga y actúa sobre temas identificados como resultado de la ejecución de actividades de control.
Trabaja con personal competente: personal competente con la suficiente autoridad desarrolla actividades de control con diligencia y continúa atención.
Reevalúa políticas y procedimientos: la administración revisa periódicamente las actividades de control para determinar su continua relevancia, y las actualiza cuando es necesario.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Actividades de control

13. La organización obtiene o genera y utiliza información relevante y de calidad para apoyar el funcionamiento del

Identifica los requerimientos de información: un proceso está en ejecución para identificar la información requerida y esperada para apoyar el funcionamiento de los otros componentes del control interno y el cumplimiento de los objetivos de la entidad.
Captura fuentes internas y externas de información: los sistemas de información capturan fuentes internas y externas de información.
Procesa datos relevantes dentro de la información: los sistemas de información procesan datos relevantes y los transforman en información.
Mantiene la calidad a través de procesamiento: los sistemas de información producen información que es oportuna, actual, precisa, completa, accesible, protegida, verificable y retenida. La información es revisada para evaluar su relevancia en el soporte de los componentes de control interno.
Considera costos y beneficios: la naturaleza, cantidad y precisión de la información comunicada están acorde con, y apoyan, el cumplimiento de los objetivos.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Información y comunicación

14. La organización comunica la información internamente, incluidos los objetivos y responsabilidades que son necesarios para apoyar el funcionamiento del sistema de control interno

Comunica la información de control interno: un proceso está en ejecución para comunicar la información requerida para permitir que todo el personal entienda y lleve a cabo sus responsabilidades de control interno.
Se comunica con la Junta directiva: existe comunicación entre la administración y la Junta Directiva; por lo tanto, ambas partes tienen la información necesaria para cumplir con sus roles con respecto a los objetivos de la entidad.
Proporciona líneas de comunicación separadas: separa canales de comunicación, como líneas directas de denuncia de irregularidades, las cuales sirven como mecanismos a prueba de fallos para permitir la comunicación anónima o confidencial cuando los canales normales son inoperantes o ineficientes.
Selecciona métodos de comunicación relevantes: los métodos de comunicación consideran tiempo, público y la naturaleza de la información.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Información y comunicación

15. La organización se comunica con los grupos de interés externos sobre los aspectos clave que afectan al funcionamiento del control interno

Se comunica con grupos de interés externos: los procesos están en funcionamiento para comunicar información relevante y oportuna a grupos de interés externos, incluyendo accionistas, socios, propietarios, reguladores, clientes, analistas financieros y demás partes externas.
Permite comunicaciones de entrada: canales de comunicación abiertos permiten los aportes de clientes, consumidores, proveedores, auditores externos, reguladores, analistas financieros, entre otros, y proporcionan a la administración y Junta Directiva información relevante.
Se comunica con la Junta Directiva: la información relevante resultante de evaluaciones conducidas por partes externas es comunicada a la Junta Directiva.
Proporciona líneas de comunicación separadas: separa canales de comunicación, como líneas directas de denuncia de irregularidades, las cuales sirven como mecanismos a prueba de fallos para permitir la comunicación anónima o confidencial cuando los canales normales son inoperantes o ineficientes.
Selecciona métodos de comunicación relevantes: los métodos de comunicación consideran el tiempo, público, y la naturaleza de la comunicación y los requerimientos y expectativas legales, regulatorias y fiduciarias.

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Actividades de monitoreo

16. La organización selecciona, desarrolla y realiza evaluaciones continuas y/o independientes para determinar si los componentes del sistema están presentes y funcionando

Considera una combinación de evaluaciones continuas e independientes: la administración incluye un balance de evaluaciones continuas e independientes.
Considera tasa de cambio: la administración considera la tasa de cambio en el negocio y los procesos del negocio cuando selecciona y desarrolla evaluaciones continuas e independientes

Establece un punto de referencia para el entendimiento: el diseño y estado actual del sistema de control interno son usados para establecer un punto de referencia para las evaluaciones continuas e independientes.
Uso de personal capacitado: los evaluadores que desarrollan evaluaciones continuas e independientes tienen suficiente conocimiento para entender lo que está siendo evaluado.

Se integra con los procesos del negocio: las evaluaciones continuas son construidas dentro de los procesos del negocio y se ajustan a las condiciones cambiantes.
Ajusta el alcance y la frecuencia: la administración cambia el alcance y la frecuencia de las evaluaciones independientes dependiendo el riesgo.
Evalúa objetivamente: las evaluaciones independientes son desarrolladas periódicamente para proporcionar

COSO COMMITTEE OF SPONSORING ORGANIZATIONS OF THE TREADWAY COMMISSION

Actividades de monitoreo

17. La organización evalúa y comunica las deficiencias de control interno de forma oportuna a las partes responsables de aplicar medidas correctivas, incluyendo la alta dirección y el consejo, según corresponda

Evalúa resultados: la Administración o la Junta Directiva, según corresponda, evalúa los resultados de las evaluaciones continuas e independientes.
Comunica deficiencias: las deficiencias son comunicadas a las partes responsables para tomar las acciones correctivas y a la Alta Dirección y la Junta Directiva, según corresponda.
Supervisa acciones correctivas: la administración monitorea si las deficiencias son corregidas oportunamente.

NOESIS
CONSULTING

RIESGOS, AUDITORIA Y CONTROLES INTERNOS

¿QUÉ ES?

La Auditoria Basada en Riesgos es una forma de conducir auditorias de diferentes tipos:

- De procesos
- De sistemas de información
- Operativa
- De sistemas de gestión
- De Estados Financieros

¿QUÉ ES?

Basa su planeación y desarrollo en los riesgos críticos, es decir, los que pudieran causar el mayor impacto negativo en la consecución de los **objetivos de la organización**:

- Objetivos estratégicos
- Objetivos operacionales
- Objetivos de información
- Objetivos de cumplimiento

Objetivos Estratégicos

La misión de una entidad establece en amplios términos lo que se aspira a alcanzar. Es importante que la dirección con la ayuda del consejo establezca expresamente la razón de ser de la entidad. A partir de esto, la dirección fija los objetivos estratégicos, formula la estrategia y establece los correspondientes objetivos operativos, de información y de cumplimiento para la organización.

Los objetivos estratégicos son de alto nivel, están alineados con la misión y visión de la entidad y le dan su apoyo. Reflejan la opción que ha elegido la dirección en cuanto a cómo la entidad creará valor para sus grupos de interés.

Objetivos operativos

Se refieren a la eficacia y eficiencia de las operaciones de la entidad e incluyen otros sub-objetivos orientados a mejorar ambas características mediante la movilización de la empresa hacia sus metas finales.

Los objetivos operativos deben reflejar los entornos empresarial, sectorial y económico en los que actúa la entidad.

Un conjunto claro de objetivos operativos, vinculados a subjetivos, es esencial para el éxito. Los objetivos operativos proporcionan un punto de focalización para orientar la asignación de recursos.

Objetivos de información

Se refieren a la fiabilidad de la información. Incluyen la información interna y externa e implican la financiera y no financiera. Una información fiable proporciona a la dirección datos seguros y completos, adecuados para la finalidad pretendida, y le presta apoyo en su toma de decisiones y en el seguimiento de las actividades y rendimiento de la entidad.

La información también está relacionada con los documentos preparados para su difusión externa, como es el caso de los estados financieros y sus notas de detalle, los comentarios y análisis de la dirección y los informes presentados a entidades reguladoras.

Objetivos de cumplimiento

Se refieren al cumplimiento de leyes y normas relevantes. Dependen de factores externos y tienden a ser similares entre entidades, en algunos casos, y sectorialmente, entre otros.

Las entidades deben llevar a cabo sus actividades y a menudo acciones concretas de acuerdo con las leyes y normas relevantes. Las leyes y normas aplicables establecen pautas mínimas de conducta, que la entidad integra en sus objetivos de cumplimiento.

El historial de cumplimiento de una entidad puede afectar positiva o negativamente a su reputación en la comunidad y el mercado.

¿Para qué ?

Confirma si las operaciones, los productos o servicios se ajustan a lo establecido en la Misión, la Visión, los objetivos estratégicos, las reglas del negocio, las buenas y mejores practicas de control interno y seguridad y las normas legales aplicables.

Objetivo Principal

La Auditoria Basadas en Riesgos evalúa y verifica que los procesos auditados satisfagan los objetivos y necesidades de la organización de manera eficaz, eficiente y segura, enfatizando en que los activos y recursos utilizados en las operaciones del negocio **estén provistos de los controles** y seguridades necesarias **para reducir los riesgos** inherentes a niveles aceptables de riesgo residual.

Objetivo 1

La auditorias “basadas en riesgos” satisfacen dos grandes objetivos: el primero es evaluar **la “efectividad” del control interno en los procesos**.

Es decir, determinar la capacidad de los controles establecidos para reducir los riesgos potenciales críticos a niveles aceptables de riesgo residual.

Los resultados de esta evaluación son la base para determinar la naturaleza y extensión de las pruebas de auditoría necesarias (de cumplimiento y sustantivas)

Objetivo 2

El segundo objetivo es verificar el cumplimiento de los controles para los riesgos críticos que presenten efectividad “Apropiada” (pruebas de cumplimiento) y verificar los objetivos que pudieran ser impactados por los eventos de riesgo que presentan debilidades de control (pruebas sustantivas). Las pruebas se realizan individualmente para una muestra de las áreas organizacionales y terceros que intervengan en el proceso y que requieran pruebas.

CONCEPTOS FUNDAMENTALES DE GESTIÓN DE RIESGOS

Concepto de Riesgo

Riesgo	Riesgo de Tecnología	Administración del Riesgo
Posibilidad de que suceda algún evento que tendrá un impacto sobre **el cumplimiento de los objetivos**. Se expresa en términos de probabilidad y consecuencias. **Riesgo Inherente:** Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto. **Riesgo Residual:** Nivel de riesgo que permanece luego de tomar medidas de tratamiento del riesgo. El riesgo en su tendencia más común es valorado como una amenaza, en este sentido, los esfuerzos institucionales se dirigen a reducirlo, evitarlo, transferirlo o mitigarlo; sin embargo, el riesgo puede ser analizado como una oportunidad, lo cual implica que su gestión sea dirigida a maximizar los resultados que estos generan.	Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el **cumplimiento de la misión**.	"Un proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al **logro de los objetivos**. El enfoque de riesgos no se determina solamente con el uso de la metodología, sino logrando que la evaluación de los riesgos se convierta en una parte natural del proceso de planeación y administración empresarial."

Riesgo en Procesos y Actividades

El Riesgo está vinculado con todo proceso de negocios; se podría afirmar que no hay actividad que deje de incluir el riesgo como una posibilidad éstos hacen parte de cualquier actividad que se realice.

Entre las clases de riesgos que pueden presentarse están:

Riesgo Estratégico: Se asocia con la forma en que se administra la Entidad, su manejo se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.

Riesgos de Imagen: Están relacionados con la percepción y la confianza de las partes interesadas hacia la institución.

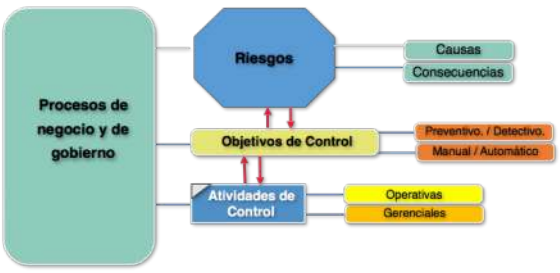
Riesgos Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los procesos, sistemas de información, de la definición de los procesos, de la estructura de la entidad, des las habilidades y capacidades de sus recursos humanos, de la articulación entre los procesos y dependencias.

Riesgos Financieros: Se relacionan con el manejo de los recursos de la entidad que incluyen la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.

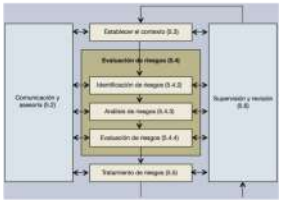
Riesgos de Cumplimiento: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, regulatorios, contractuales, de ética pública (trasparencia, honestidad, trato justo, etc.)

Riesgos de Tecnología: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la Misión y Visión.

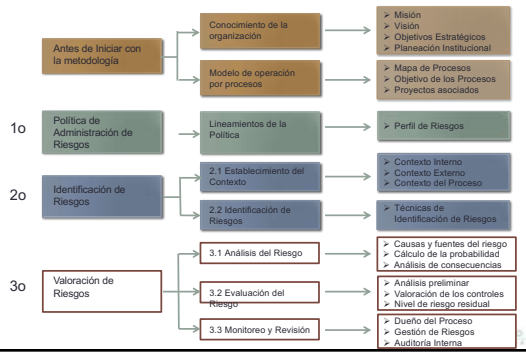
Riesgo en Procesos y Actividades



METODOLOGÍA



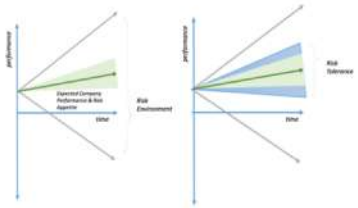
LA METODOLOGÍA DE GESTIÓN DE RIESGOS



POLÍTICA DE GESTIÓN DE RIESGOS

1. Establece el mandato
2. Define roles y responsabilidades y el gobierno de la Gestión Integral de Riesgo.
3. Establece principios
4. Define el perfil de riesgos (apetito y tolerancia) para cada tipo de riesgo.
5. Establece la necesidad de incorporación en todos los procesos de la organización.

Establecimiento del apetito de Riesgo



Matriz de Riesgo Institucional

- ✓Debe ser clara y específica para valorar el impacto de los diferentes tipos de riesgo adecuadamente.
- ✓Establece el límite de la tolerancia al riesgo.
- ✓Establece los niveles de involucramiento en el tratamiento de los riesgos.
- ✓Nos brinda una mirada general de todos los riesgos residuales de la empresa.
- ✓Es útil para la planificación de la gestión empresarial como de las unidades de aseguramiento y auditoría.

Establece la Tolerancia y Responsabilidad

PROBABILIDAD		10%	22%	35%	50%	100%	
Casi seguro	5	2	3	4	4	4	100%
Probable	4	2	3	4	4	4	50%
Posible	3	2	2	3	4	4	33%
Improbable	2	1	1	2	3	3	8%
Raro	1	1	1	1	2	2	3%
		1	2	3	4	5	
		Bajo	Menor	Moderado	Mayor	Extremo	

IMPACTO

4	Riesgo extremo, requiere acción inmediata
3	Riesgo alto, necesita atención de la alta gerencia
2	Riesgo moderado, necesita responsable gerencial
1	Riesgo bajo, administrar con procedimientos de rutina

Debe definirse el Impacto claramente para cada tipo de Riesgo

Impacto en las utilidades			
	5	Extremo	Perdida mayor a 870101 Bs
	4	Mayor	Perdida entre 616001 Bs y 870100 Bs
	3	Moderado	Perdida entre 385001 Bs y 616000 Bs
	2	Menor	Perdida entre 175001 Bs y 385000 Bs
	1	Bajo	Perdida hasta 175000 Bs
Impacto legal/regulatorio			
	5	Extremo	Procesos legales significativos, perdida de la licencia, detención de la alta gerencia.
	4	Mayor	Sanciones altas del regulador, ejecución de garantías, procesos costosos como medidas de mitigación.
	3	Moderado	Incumplimiento de normativa que puede conducir a sanciones
	2	Menor	Incumplimiento de normativa que debe ser reportado.
	1	Bajo	Incumplimiento de normativa interna no reportable.
Reputación			
	5	Extremo	Cobertura negativa de largo plazo en los medios de comunicación nacionales que ocasionan pérdida de mercado.
	4	Mayor	Cobertura negativa de corto plazo en los medios de comunicación nacionales.
	3	Moderado	Cobertura negativa de corto plazo en los medios de comunicación locales.
	2	Menor	Noticia negativa en los medios de comunicación locales.
	1	Bajo	Noticia en los medios de comunicación locales que es resulta inmediatamente
Continuidad			
	5	Extremo	Interrupciones que afectan la continuidad de la operación de la compañía (licencia, perdida de clientes, etc)
	4	Mayor	Interrupciones que afectan a los clientes importantes y son sancionados.
	3	Moderado	Interrupciones que afectan los servicios de la mayoría de los clientes y pueden ser sancionados
	2	Menor	Interrupciones que afectan el SLA para algunos clientes sin afectar a la normativa
	1	Bajo	Interrupciones que pueden ser solucionadas sin afectar SLA o normativa

Proceso de Identificación de Riesgos

Identificación de Riesgo → ¿En qué consiste?

En esta etapa se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas. (NTC ISO31000, Numeral 2.15).

Input

Establecimiento del contexto

Definición de los parámetros internos y externos que se han de tomar en consideración para la administración del riesgo. Se debe establecer el contexto interno, externo de la entidad y el contexto del proceso.

Identificación del riesgo

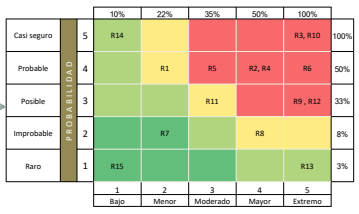
Se realiza determinando las causas, fuentes del riesgo y los eventos con base en el análisis de contexto para la entidad y del proceso, que pueden afectar el logro de los objetivos.

Es importante centrarse en los riesgos más significativos para la entidad relacionados con los objetivos de los procesos y los objetivos institucionales

Output

Proceso de Identificación de Riesgos

Output



Creación de Controles

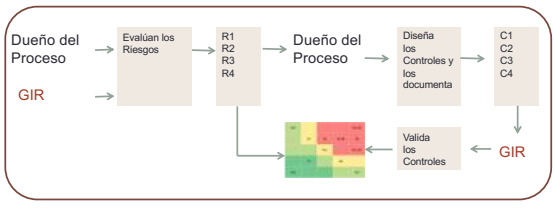
Definición de Controles para mitigar los riesgos.

Transferir, Fondear, Salir

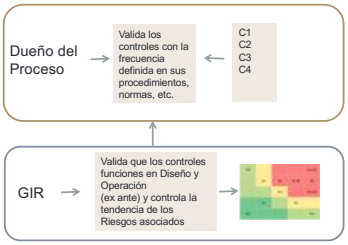
Asegurar el riesgo, reservar, salir de la operación o del negocio.

ROLES Y RESPONSABILIDADES

IDENTIFICACIÓN DE RIESGOS

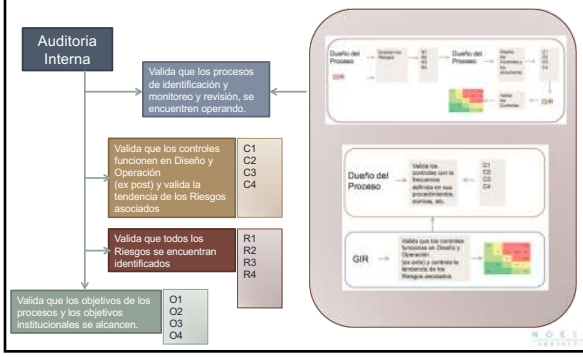


Monitoreo y Revisión
1ª y 2ª líneas de defensa

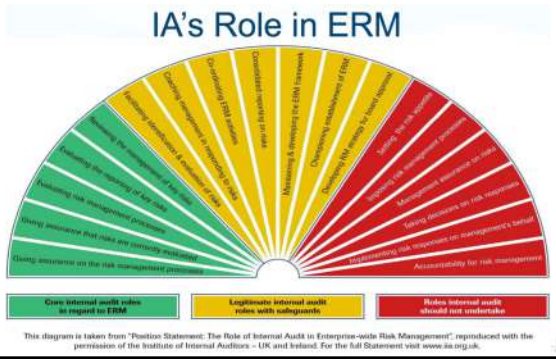


Modelo 3 lineas de defensa

Monitoreo y Revisión
3ª linea de defensa



Rol de Auditoria en Gestión de Riesgos



Roles fundamentales de la **auditoría** interna respecto al ERM

- Brindar aseguramiento sobre procesos de gestión de riesgo.
- Brindar aseguramiento de que los riesgos son correctamente evaluados.
- Evaluación de los procesos de gestión de riesgo.
- Evaluación de reporte de riesgos claves.
- Revisión del manejo de los riesgos claves.

Roles **legí**timos de **auditorí**a interna que deben realizarse con salvaguarda

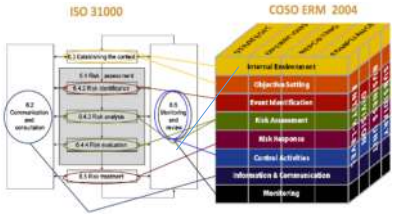
- Facilitación, identificación y evaluación de riesgos.
- Entrenamiento a la gerencia sobre respuesta a riesgos.
- Coordinación de actividades de ERM.
- Consolidación de reportes sobre riesgos.
- Mantenimiento y desarrollo del marco de ERM.
- Defender el establecimiento del ERM.
- Desarrollo de estrategias de gestión de riesgo para aprobación de la junta.

Roles que **auditoría** interna NO debe realizar

- Establecer el apetito de riesgo.
- Imponer procesos de gestión de riesgo.
- Manejar el aseguramiento sobre los riesgos.
- Tomar decisiones en respuesta a los riesgos.
- Implementar respuestas a riesgos a favor de la administración.
- Tener responsabilidad de la gestión de riesgo.

COSO ERM

Framework: ISO 31000 vs COSO ERM



Fácil de entender y explicar a otros
Una mejor guía de Como Hacer en el momento de la implementación
Mas foco en los riegos que en los controles internos
Flexible y fácil de adaptar e implantar.

Se une al framework de Controles Internos de COSO
Tiene una mejor discusión sobre el apetito de riesgo
Es mas fuerte en el gobierno corporativo
Difícil de entender tiene 120 normas y esta mas enfocado en los controles internos

Resumen

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

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

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

Objetivos de ERM

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

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

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

Objetivos de ERM

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

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

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

Componentes de la Gestión de Riesgos Corporativos

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

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

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

Componentes de la Gestión de Riesgos Corporativos

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

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

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

Componentes de la Gestión de Riesgos Corporativos

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

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

REGLAMENTO DE CONTROL INTERNO Y AUDITORES INTERNOS

Artículo 1° - (Sistema de Control Interno) Se entiende por Sistema de Control Interno al conjunto de políticas y procedimientos establecidos por la entidad supervisada para proveer una seguridad razonable en el logro de los objetivos operativos, de información y de cumplimiento.

1. **Objetivos operativos:** Hacen referencia a la efectividad y eficiencia de las operaciones de la entidad, incluidos sus objetivos de rendimiento financiero y operacional, así como la protección de sus activos frente a posibles pérdidas;
2. **Objetivos de información:** Hacen referencia a la información financiera y no financiera interna y externa y deben abarcar aspectos de confiabilidad, oportunidad, transparencia, u otros conceptos establecidos por organismos reconocidos o políticas de la propia entidad;
3. **Objetivos de cumplimiento:** Hacen referencia al cumplimiento de las leyes y regulaciones a las que está sujeta la entidad.

Artículo 2° - (Componentes del Sistema de Control Interno) El Sistema de Control Interno de la entidad supervisada debe contemplar, como mínimo, los siguientes cinco (5) componentes interrelacionados:

a. Ambiente Interno;
b. Evaluación de Riesgos;
c. ActividadesdeControl;
d. Información y Comunicación; **e.** ActividadesdeMonitoreo.

Todos los componentes, se consideran esenciales para el adecuado funcionamiento del Sistema de Control Interno, debiendo los mismos estar en operación en todo momento.

Artículo 3° - (Ambiente Interno) El Ambiente Interno considera el carácter y la actitud del Directorio y la Alta Gerencia sobre el control y la gestión de los riesgos, la integridad y valores éticos, la forma en que la Gerencia General asume autoridad y responsabilidad, así como la supervisión ejercida por el Directorio, que estimula y promueve la conciencia y el compromiso del personal con la entidad supervisada.
Para el efecto, la entidad supervisada debe mantener políticas y procedimientos actualizados que reflejen, mínimamente, de manera clara:

a. La actitud del Directorio para la gestión de riesgos de la entidad;
b. Los principios y valores contenidos en el Código de Ética, así como las acciones correctivas a ser asumidas en caso de identificar incumplimientos al mismo;
c. La visión del Directorio;
d. La estructura organizativa;
e. La asignación de autoridad y responsabilidades;
f. La segregación de funciones;
g. La gestión de recursos humanos, que considere la guia y el entrenamiento necesarios para atraer, desarrollar y retener personal suficiente y competente para alcanzar los objetivos.

Artículo 4° - (Evaluación de Riesgos) Es la que permite a una entidad supervisada considerar la amplitud con que los eventos potenciales impactan en la consecución de objetivos. El Directorio debe evaluar estos acontecimientos desde una doble perspectiva (probabilidad e impacto), un doble enfoque (riesgo inherente y riesgo residual) y usar una combinación de métodos cualitativos y cuantitativos. Los impactos positivos y negativos de los eventos potenciales deben examinarse, individualmente o por categoría, en toda la entidad supervisada.
Como parte de este componente, la entidad supervisada debe considerar los siguientes aspectos:

a. El Directorio debe fijar y aprobar los objetivos estratégicos, así como los objetivos operativos, de información y de cumplimiento, con el propósito de identificar los eventos, evaluar los riesgos y responder a los mismos. Estos objetivos deben estar alineados a la visión, misión y apetito al riesgo de la entidad supervisada, ser medibles, contar con indicadores de su cumplimiento, además de ser específicos y estar plasmados en el Plan Estratégico de la entidad supervisada.
b. El Directorio debe identificar, conocer y comprender los eventos potenciales tanto internos como externos, que de ocurrir, afectarán a la consecución de los objetivos, así como determinar si representan oportunidades o si pueden afectar negativamente al logro de los mismos.

Los eventos con impacto negativo que representan riesgos, deben ser evaluados y atendidos por el Directorio de la entidad supervisada. Los eventos con impacto positivo representan oportunidades que el Directorio debe reconducir hacia la estrategia y al proceso de fijación de objetivos.
Para la identificación de eventos, la entidad supervisada debe utilizar técnicas o métodos debidamente formalizados, tales como:

i. Los inventarios e indicadores de eventos;
ii. Los talleres de trabajo, de los cuales debe existir constancia de su realización;
iii. Las entrevistas;
iv. Los cuestionarios y encuestas;
v. El análisis de flujo de procesos;
vi. El seguimiento de datos de eventos que generan pérdidas.

c. El Directorio de la entidad supervisada debe determinar cómo responder a los riesgos relevantes o significativos una vez evaluados los mismos. Las respuestas pueden ser:

i. Evitar el riesgo: tomar acciones a efectos de discontinuar las actividades que generan riesgo;
ii. Reducir el riesgo: tomar acciones a efectos de reducir o minimizar el impacto, la probabilidad de ocurrencia del riesgo o ambos;
iii. Compartirelriesgo:tomaraccionesaefectosdereducirelimpactoolaprobabilidad de ocurrencia al transferir o compartir una porción del riesgo;
iv. Aceptar el riesgo: no tomar acciones que afecten el impacto y probabilidad de ocurrencia del riesgo.

Al considerar su respuesta, el Directorio debe evaluar su efecto sobre la probabilidad e impacto del riesgo, así como los costos y beneficios y seleccionar aquella que sitúe el riesgo residual en un nivel aceptable por éste, priorizando los riesgos con mayor impacto en los objetivos de la entidad, además de factores como el grado de adaptabilidad de la entidad, la complejidad de los riesgos, la velocidad a la que se materializan los riesgos, la duración de los riesgos y la capacidad de la entidad para retornar un riesgo a un nivel aceptable.

d. El Directorio y la Alta Gerencia deben identificar y evaluar los cambios que podrían afectar significativamente al sistema de control interno, entre éstos los cambios debidos a factores externos (el marco regulatorio, el entorno económico, el mercado, entre otros), así como los cambios en el modelo de negocios y la Alta Gerencia de la entidad.

Artículo 5° - (Actividades de Control) Las Actividades de Control son las políticas y procedimientos aprobados por el Directorio para asegurar que se llevan a cabo las respuestas a los riesgos a los cuales se encuentra expuesta la entidad supervisada. Las Actividades de Control, tales como aprobaciones, autorizaciones, verificaciones, conciliaciones, revisiones del funcionamiento operativo, seguridad de los activos y segregación de funciones u otros, deben tener lugar a través de toda la organización, en todos los niveles y en todas las funciones.

Las Actividades de Control apoyarán en las respuestas a los riesgos a los que se encuentra expuesta una entidad supervisada, con el propósito de lograr una atención oportuna. Asimismo, éstas deben ser parte integral de sus operaciones diarias y ser desarrolladas en el marco de una estructura de control que sea apropiada al tamaño, la naturaleza, complejidad de las operaciones y el nivel de riesgo definido como tolerable. Dichas actividades se establecerán en tres (3) niveles:

a. Revisiones del Directorio y Comité de Auditoría. Comprende la revisión y análisis de informes planteados por la Alta Gerencia o Auditoría Interna al Directorio y el Comité de Auditoría, según corresponda, que permita analizar los avances en el logro de los objetivos contenidos en el Plan Estratégico y las medidas propuestas para su cumplimiento.
b. Controles Gerenciales. Consiste en la revisión y seguimiento que efectúa la Alta Gerencia a los informes y actividades que realizan las instancias operativas. Estos informes deben ser precisos y medibles, permitiendo la toma de decisiones.
c. Control de Operaciones. Comprende la implementación de:
    1. Controles físicos. Medidas de seguridad que restringen el acceso físico a los activos de la entidad supervisada, tales como efectivo, valores y otros activos financieros. Las actividades de control incluyen entre otros a las limitaciones físicas, custodia doble, arqueos e inventarios periódicos.
    2. Controles de accesos lógicos. Medidas de seguridad que registren el acceso lógico a los activos y sistemas de información de la entidad supervisada. Las actividades incluyen entre otros, perfiles de seguridad, monitoreo de las actividades de los usuarios de Sistemas de Información, políticas de seguridad en el acceso, en el marco de lo dispuesto en el Reglamento para la Gestión de Seguridad de la Información, contenido en la Recopilación de Normas para el

3. Controles cruzados. Actividades o funciones que deben ser verificadas por al menos dos (2) funcionarios responsables de la entidad supervisada, así como el doble control de activos y firmas dobles.
4. Verificaciones y conciliaciones. Verificación de los detalles de transacciones, de las actividades y las conciliaciones periódicas de los movimientos de efectivo con los registros contables y estados de cuenta que sirven para identificar actividades y registros que necesitan corregirse. Los resultados de estas verificaciones deben ser reportados a los niveles gerenciales apropiados.
5. Segregación de funciones. Separación de responsabilidades de la diversidad de actividades que intervienen en la consecución de objetivos específicos, con el fin de reducir el riesgo de manipulación de datos financieros y/o malversación de activos. La entidad supervisada debe segregar mínimamente las siguientes funciones:
    i. Atención al público y registro contable;
    ii. Custodia de activos y registro contable;
    iii. Registro y ejecución de operaciones, diferenciando adicionalmente las de cartera propia o de clientes y/o participantes (si corresponde);
    iv. En el Departamento o Área de Sistemas, se deben mantener separadas las funciones de: Desarrollo y Pruebas y Producción, Seguridad Informática y Operaciones;
    v. Cualquier otra función donde surjan conflictos de interés que no sean mitigados por otros mecanismos de control.

6. Aprobaciones. Operaciones que deben ser verificadas y aprobadas conforme a los procedimientos establecidos por la entidad supervisada, asegurando que el nivel apropiado se encuentra informado de la transacción o situación.
7. Control de personal. Medidas de control respecto al personal de la entidad supervisada, que contemplen mínimamente lo siguiente:
    i. El cumplimiento de los requisitos y competencias necesarias para desempeñar cada uno de los cargos;
    ii. Las evaluaciones al personal de la entidad, así como las evaluaciones a los proveedores de servicios tercerizados y las acciones a seguir en caso de identificar deficiencias. Dichas evaluaciones deben considerar los niveles de competencia esperados, el apego al Código de Ética y a otros estándares apropiados de comportamiento, además de proporcionar premios o ejercer acciones disciplinarias cuando es apropiado;
    iii. Capacitaciónefectiva,conformealoprevistoenlosReglamentosespecíficos y en el Manual de organización y funciones de la entidad supervisada, antes de asignarles tareas o posiciones de mayor responsabilidad.

Artículo6°-(Información y Comunicación) El Directorio debe implementar sistemas de información y comunicación que cubran todas las actividades y permitan a los ejecutivos y funcionarios de la entidad llevar a cabo sus funciones y responsabilidades, de acuerdo al siguiente detalle:

a. Información. La entidad supervisada debe contar con sistemas de información que capturen datos generados de forma interna y externa (entradas), donde la información que emiten (salidas) debe ser accesible, correcta, actualizada, protegida, disponible, suficiente, oportuna, valida, verificable y presentada en un formato lógico que facilite la gestión de riesgos y la toma de decisiones.
La información debe servir a la entidad supervisada en todos sus niveles para identificar, evaluar y responder a los riesgos y estar dirigida al logro de los objetivos.

b. Comunicación. La entidad supervisada debe contar con canales de comunicación eficaces que fluyan en todas las direcciones dentro de la organización tanto hacia los niveles superiores e inferiores, como transversalmente a las otras áreas de ésta, permitiendo dichos canales que todo el personal entienda y lleve a cabo sus responsabilidades de control interno.

Por otra parte, debe contar con canales de comunicación alternativos que permitan denunciar irregularidades, de forma anónima o confidencial, cuando los canales habituales de comunicación sean insuficientes. La selección de estos canales de comunicación debe considerar la oportunidad, audiencia, la naturaleza de la información, requerimientos legales y regulatorios.
Asimismo, debe contar con canales de comunicación pertinentes y oportunos con las partes externas a la entidad supervisada, como ser: acreedores, clientes o participantes, ASFI, accionistas, usuarios internos y externos y otros, que consideren lo señalado en el presente artículo.

El principio de transparencia que rige el Mercado de Valores exige que se proporcione a los participantes del mercado, en igualdad de condiciones, información oportuna, suficiente y de calidad sobre los datos y hechos relevantes que permitan una adecuada formación de precios y la adopción de decisiones debidamente fundamentadas. De esta manera se disminuye el riesgo de desigualdad de oportunidades para actuar en el mercado, derivado del manejo de información privilegiada.
Los sistemas de información y comunicación que guarden y utilicen datos en forma electrónica, deben dejar pistas de auditoría que permitan el seguimiento de las actividades, ser seguros, probados por personas independientes y mantener planes de contingencia, en concordancia con las disposiciones previstas en el Reglamento para la Gestión de Seguridad de la Información, contenido en la Recopilación de Normas para el Mercado de Valores.

Artículo 7° - (Actividades de Monitoreo) El Directorio debe garantizar que se lleven a cabo Actividades de Monitoreo, determinando si los componentes del control interno están presentes y funcionando de manera permanente. Para este propósito todas las áreas de la entidad, la Unidad de Auditoría Interna y Auditoría Externa deben considerar los siguientes aspectos:

a. Conocer el estado del sistema de control interno en un momento determinado del tiempo, como punto de referencia para las siguientes evaluaciones.

b. Realizar evaluaciones continuas o independientes, de acuerdo a la rapidez con la que cambia el Mercado de Valores y los procesos de la entidad, siendo mandatorio que el personal que efectúe las evaluaciones cuente con suficiente conocimiento para entender el sistema de control interno de la entidad.

c. Evaluar y comunicar las deficiencias en forma ascendente, trasladando los temas más importantes a la Alta Gerencia o al Directorio, para la toma de acciones correctivas.

Las diferentes Actividades de Monitoreo pueden contemplar la revisión de informes de liquidez, de operaciones, de planificación y control, así como el monitoreo de los riesgos.

Artículo 8° - (Participantes del Sistema de Control Interno) El Sistema de Control Interno involucra a todos los Directores, Comité de Auditoría, Auditoría Interna, Alta Gerencia y personal de la entidad supervisada.
La participación, funciones y responsabilidades de dichas instancias, deben estar claramente establecidas en los estatutos, políticas, manuales de procedinientos y control interno, así como de de organización y funciones, según corresponda.
La Alta Gerencia es responsable de guiar el desarrollo e implementación de las políticas y procedimientos relacionados al control interno, a través de toda la organización, verificando que éstos sean consistentes con los objetivos de la entidad.

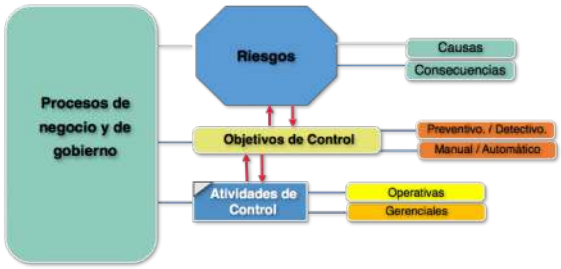
Artículo 9° - (Contratación de proveedores de servicios)
Artículo 10° - (Evaluación del Sistema de Control Interno) El Comité de Auditoría será responsable de la evaluación permanente del diseño, alcance y funcionamiento del Sistema de Control Interno.
La Unidad de Auditoría Interna debe proporcionar una evaluación independiente de los riesgos y actividades de control de los procesos o áreas de la entidad supervisada. Estas evaluaciones deben proveer una perspectiva objetiva e independiente sobre todos los componentes del Sistema de Control Interno.
Asimismo, la Empresa de Auditoría Externa, evaluará anualmente el Sistema de Control Interno de la entidad supervisada, pudiendo considerar los trabajos realizados por las Unidades de Auditoría Interna y de Riesgos.
Artículo 11° - (Documentación) Todas las áreas de la entidad supervisada son responsables de desarrollar y mantener la documentación que sustente el diseño y la efectividad de cada uno de los componentes de control interno, la cual debe ser suficiente para respaldar las afirmaciones de ésta respecto al control interno.
La Alta Gerencia debe documentar cómo fueron considerados los elementos de juicio en la toma de decisiones que afecten significativamente a la entidad.

Artículo 12° - (Apetito al Riesgo) La declaración explicita del apetito al riesgo debe ser informada mínimamente a la Alta Gerencia.
En la determinación de su apetito al riesgo, la entidad supervisada debe considerar factores estratégicos, financieros y operativos, así como su perfil de riesgo y el grado de madurez de su gestión de riesgos, además de estar alineado con la estrategia, los objetivos estratégicos, la misión, la visión y los valores de la misma.
La declaración será utilizada en el proceso de toma de decisiones en los distintos niveles de la entidad supervisada
Artículo 13° - (De los manuales de procedimientos) La entidad supervisada, con base en el volumen y complejidad de las operaciones que realiza, debe elaborar manuales de procedimientos que cuenten con denominación, codificación, fecha de aprobación, fecha de entrada en vigencia, números de páginas, índice y mínimamente contemplen la siguiente información:

a. Objetivo de los procedimientos;
b. Definición(es) o concepto(s);
c. Área(s) de aplicación y/o alcance de los procedimientos;
d. Políticas, normas o reglamentos relacionados a los procedimientos;
e. Descripción de los procedimientos y responsables de su ejecución;
f. Responsables de la elaboración y revisión del manual.

IMPLEMENTANCION DEL SISTEMA DE CONTROL INTERNO

Riesgo en Procesos y actividades



Proceso para la contrucción de ICF

I. Identificar los riesgos (causa – consecuencia)
II. Identificar las actividades de control
III. Identificar los riesgos residuales
IV. Validar con el apetito de riesgo

ACTIVIDADES DE CONTROL

- **Revisiones a alto nivel:** la alta dirección se encarga de revisar los datos reales de funcionamiento en función de los presupuestos, previsiones y datos de periodo previos, además de realizar un seguimiento de las iniciativas importantes.
- **Gestión directa de funciones o actividades:** los directivos que gestionan las funciones o actividades revisan los informes de rendimiento.
- **Procesamiento de la información:** se realiza una variedad de controles para verificar la exactitud, integridad y autorización de las transacciones, controlándose también el desarrollo de nuevos sistemas y modificaciones en los existentes.
- **Controles físicos:** las existencias, equipos y valores se someten a recuentos periódicos y se cotejan con los registros de control.
- **Indicadores de rendimiento:** el contraste de diferentes conjuntos de datos, operativos o financieros, junto con el análisis de relaciones y las acciones de investigación y corrección.
- **Segregación de funciones:** las funciones se dividen en diferentes personas para reducir el riesgo de error o fraude.

DOCUMENTAR CONTROLES

- Identificar Riesgos en sus Casas
- Documentar sus Controles

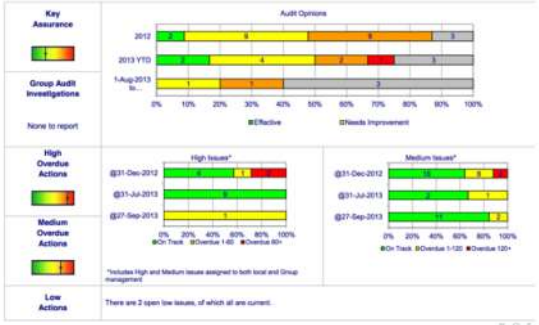
ICF Test – Deficiencias de Controles

Deficiencia de documentación (descripción del control)

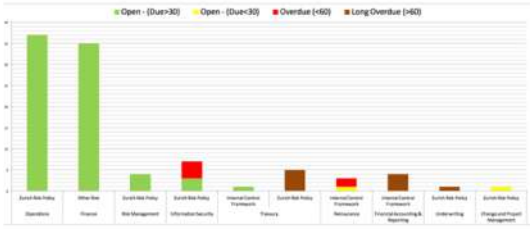
- Los atributos de control no son correctos (frecuencia, automatizado / manual, prevenir / detectar)
- Los riesgos de control no se han asignado correctamente al control
- Las fuentes de referencia no son correctas / completas.
- La persona responsable no es correcta
- La descripción del control no es completa / no es comprensible (se requiere que la actividad de control se escriba para que una tercera persona competente sin conocimiento previo del proceso pueda comprender completamente la actividad de control)
- La descripción no responde a las preguntas **qué, cómo, cuándo, quién**
- La descripción contiene parte de la documentación del proceso.
- Existe un control y está funcionando de manera efectiva, pero no se ha documentado.

INDICADORES DE CONTROL

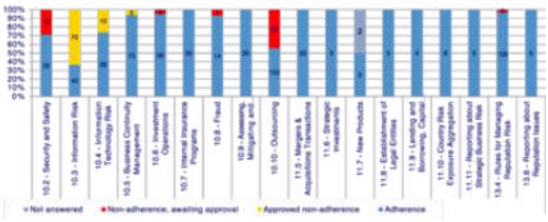
SCORECARD AUDITORIA



SCORECARD PLANES DE ACCION



SCORECARD INCUMPLIMIENTO



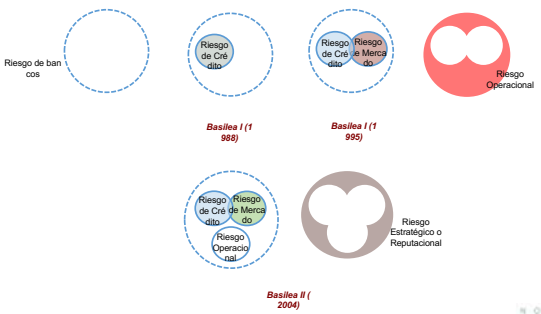
Tips

Cualquiera que sea el área de observación indicada (Monitoreo), cada una de ellas debe contener lo siguiente:

1.- Descripción de la deficiencia encontrada.
2.- Causa del problema
3.- Consecuencia de la debilidad y de ser posible su cuantificación
4.- Acciones correctivas adecuadas para el nivel de riesgo (consecuencia) y la cirscunstancia.

Enterprise Risk Management

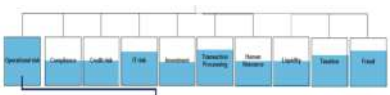
Gestión de riesgos de Bancos



Gestión de riesgos estratégicos

Gestión de riesgos operacionales

Riesgo de ¿Crédito?



- Documentacion transaccional/contractual
- Documentación de procesos
- Diseño de procesos
- Ejecución de procesos
- Falla en productos
- Datos internos y externos
- Reportes internos y externos
- Gestión de cambios y proyectos
- Servicio al cliente e interacciones

La gestión de riesgos operacionales nos permite observar la empres a de una manera holística para crear un mapa detallado de los riesgos. Los gerentes de línea y los gerentes de negocio pueden u sarlo para conducir su negocio de mejor manera

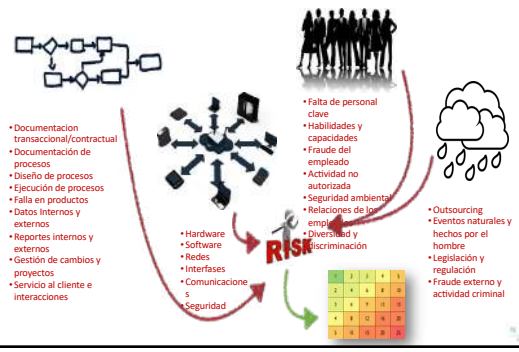
- Falta de personal clave
- Habilidades y capacidades
- Fraude del empleado
- Actividad no autorizada
- Seguridad ambiental
- Relaciones de los empleados
- Diversidad y discriminación

¿Cual es la probabilidad que las fallas en los Controles de gestión de crédito deterioren mi cartera?

¿Cuál es la severidad de las pérdidas?

¿Cómo esta la industria y mis competidores?

GESTIÓN DE RIESGOS OPERACIONALES



ASFI

Circular ASF/153/12 (11/12) Inicial
ASF/151/15 (11/15) Modificación 1

Libro3°
Título I
Capítulo I
Sección 1
Página 1/4

Artículo 3°.- (Etapas del proceso de gestión integral de riesgos) La gestión integral de riesgos involucra al menos seis etapas adecuadamente estructuradas, consistentes y continuas, de acuerdo a lo siguiente:

a. **Identificación:** Es un proceso que se dirige a reconocer y entender los diferentes tipos de riesgos que existen en las operaciones que realiza la entidad supervisada, y aquellos que pueden surgir de iniciativas de nuevos productos y operaciones;

Esta etapa permite determinar de manera preventiva posibles acciones a seguir, dado que se identifican y clasifican los eventos adversos según el tipo de riesgo al que corresponden, la interrelación que puede existir entre estos, las áreas expuestas y el posible efecto que se produciría en la situación financiera de la entidad supervisada;

b. **Medición:** Es la etapa en la cual la entidad supervisada, a través de las herramientas que desarrolla, cuantifica sus niveles de exposición a los diferentes tipos de riesgos que se encuentran presentes en las operaciones que realiza. La medición efectuada considera la frecuencia e impacto de las pérdidas que podrían acontecer, dada la ocurrencia de eventos adversos;

c. **Monitoreo:** Consiste en el establecimiento de procesos de control al interior de la entidad supervisada, que está asociado entre otros a los sistemas de información que facilitan el seguimiento de la gestión integral de riesgos, ayudando a detectar y corregir oportunamente deficiencias y/o incumplimientos en las políticas, procesos y procedimientos para cada uno de los riesgos a los cuales se encuentra expuesta la entidad supervisada;

d. **Control:** Es el conjunto de actividades que se realizan con la finalidad de disminuir la probabilidad de ocurrencia de un evento adverso, que pueda originar pérdidas a la entidad supervisada;

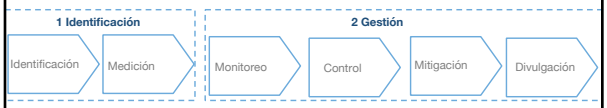
e. **Mitigación:** Corresponde a las acciones realizadas, los mecanismos y/o coberturas implementadas por la entidad supervisada, para reducir al mínimo las pérdidas incurridas, como consecuencia de la materialización de los sucesos o eventos adversos motivadores de riesgos;

f. **Divulgación:** Acción orientada a establecer y desarrollar un plan de comunicación que asegure de forma periódica la distribución de información apropiada, veraz y oportuna, relacionada con la entidad supervisada y su proceso de gestión integral de riesgos, destinada al Directorio u Órgano equivalente, así como a las distintas áreas que participan en la toma de decisiones y en la gestión de riesgos. Esta etapa debe coadyuvar a promover un proceso crítico de auto-diagnóstico sobre la gestión integral de riesgos.

ASFI

Circular ASF/153/12 (11/12) Inicial
ASF/151/15 (11/15) Modificación 1

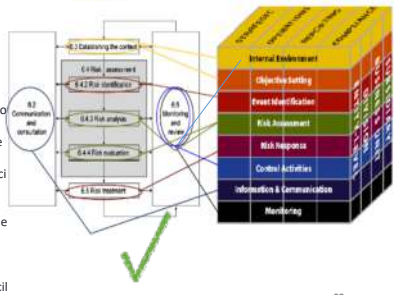
Libro3°
Título I
Capítulo I
Sección 1
Página 1/4



Framework: ISO 31000 vs COSO ERM

ISO 31000

COSO ERM 2004



Fácil de entender y explicar a otros
Una mejor guía de Como Hacer en el momento de la implementación
Mas foco en los riegos que en los controles internos
Flexible y fácil de adaptar e implantar.

Se une al framework de Controles Internos de COSO
Tiene una mejor discusión sobre el apetito de riesgo
Es mas fuerte en el gobierno corporativo
Difícil de entender tiene 120 normas y esta mas enfocado en los controles

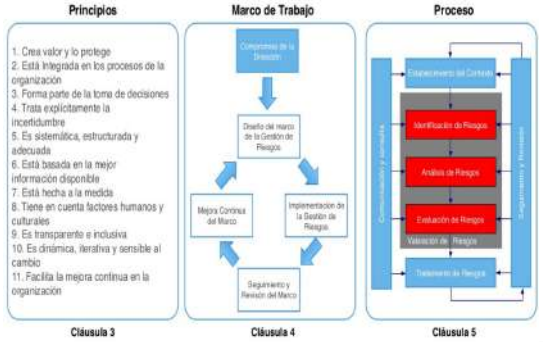
82

ISO 31000 vs Otros

	ISO 31000
Basilea	✓
COBIT 5	✓
ISO 27001 / 27005	✓
ASFI	✓
Otros	✓

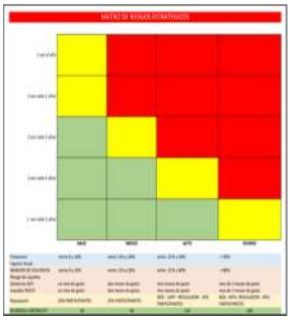
Engineer → risk = hazard
Scenario → risk = event
Manager → risk = uncertainty on objectives
Health → risk = threat (purely negative)
Finance → risk = return
Public sector → risk = discontinuity of service

ISO 31000:2009



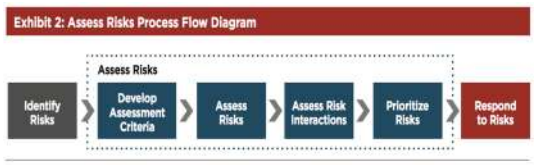
Establecer el contexto

Establecer el contexto



86

Proceso de gestión de riesgos



87

Tipos de Evaluaciones

- Strategic risk assessment. Evaluation of risks relating to the organization's mission and strategic objectives, typically performed by senior management teams in strategic planning meetings, with varying degrees of formality.
- Operational risk assessment. Evaluation of the risk of loss (including risks to financial performance and condition) resulting from inadequate or failed internal processes, people, and systems, or from external events. In certain industries, regulators have imposed the requirement that companies regularly identify and quantify their exposure to such risks. While responsibility for managing the risk lies with the business, an independent function often acts in an advisory capacity to help assess these risks.
- Compliance risk assessment. Evaluation of risk factors relative to the organization's compliance obligations, considering laws and regulations, policies and procedures, ethics and business conduct standards, and contracts, as well as strategic voluntary standards and best practices to which the organization has committed. This type of assessment is typically performed by the compliance function with input from business areas.
- Internal audit risk assessment. Evaluation of risks related to the value drivers of the organization, covering strategic, financial, operational, and compliance objectives. The assessment considers the impact of risks to shareholder value as a basis to define the audit plan and monitor key risks. This top-down approach enables the coverage of internal audit activities to be driven by issues that directly impact shareholder and customer value, with clear and explicit linkage to strategic drivers for the organization.

Tipos de Evaluaciones

- Financial statement risk assessment. Evaluation of risks related to a material misstatement of the organization's financial statements through input from various parties such as the controller, internal audit, and operations. This evaluation, typically performed by the finance function, considers the characteristics of the financial reporting elements (e.g., materiality and susceptibility of the underlying accounts, transactions, or related support to material misstatement) and the effectiveness of the key controls (e.g., likelihood that a control might fail to operate as intended, and the resultant impact).
- Fraud risk assessment. Evaluation of potential instances of fraud that could impact the organization's ethics and compliance standards, business practice requirements, financial reporting integrity, and other objectives. This is typically performed as part of Sarbanes-Oxley compliance or during a broader organization-wide risk assessment, and involves subject matter experts from key business functions where fraud could occur (e.g., procurement, accounting, and sales) as well as forensic specialists.
- Market risk assessment. Evaluation of market movements that could affect the organization's performance or risk exposure, considering interest rate risk, currency risk, option risk, and commodity risk. This is typically performed by market risk specialists.

Tipos de Evaluaciones

- Credit risk assessment. Evaluation of the potential that a borrower or counterparty will fail to meet its obligations in accordance with agreed terms. This considers credit risk inherent to the entire portfolio as well as the risk in individual credits or transactions, and is typically performed by credit risk specialists.
- Customer risk assessment. Evaluation of the risk profile of customers that could potentially impact the organization's reputation and financial position. This assessment weighs the customer's intent, creditworthiness, affiliations, and other relevant factors. This is typically performed by account managers, using a common set of criteria and a central repository for the assessment data.
- Supply chain risk assessment. Evaluation of the risks associated with identifying the inputs and logistics needed to support the creation of products and services, including selection and management of suppliers (e.g., up-front due diligence to qualify the supplier, and ongoing quality assurance reviews to assess any changes that could impact the achievement of the organization's business objectives).[3]

Tipos de Evaluaciones

- Product risk assessment. Evaluation of the risk factors associated with an organization's product, from design and development through manufacturing, distribution, use, and disposal. This assessment aims to understand not only the revenue or cost impact, but also the impact on the brand, interrelationships with other products, dependency on third parties, and other relevant factors. This type of assessment is typically performed by product management groups.
- Security risk assessment. Evaluation of potential breaches in an organization's physical assets and information protection and security. This considers infrastructure, applications, operations, and people, and is typically performed by an organization's information security function.
- Information technology risk assessment. Evaluation of potential for technology system failures and the organization's return on information technology investments. This assessment would consider such factors as processing capacity, access control, data protection, and cyber crime. This is typically performed by an organization's information technology risk and governance specialists.
- Project risk assessment. Evaluation of the risk factors associated with the delivery or implementation of a project, considering stakeholders, dependencies, timelines, cost, and other key considerations. This is typically performed by project management teams.

Medición

¿qué tan grave?
¿qué tan probabl
e?
¿qué impactos tr
ae?

Tipos de Evaluación

La evaluación del riesgo se realiza a menudo como un proceso de dos etapas. Una evaluación inicial de los riesgos y oportunidades se lleva a cabo utilizando técnicas cualitativas seguidas de un tratamiento más cuantitativo de los riesgos y oportunidades más importantes que se prestan a la cuantificación, entendiendo que no todos los riesgos son cuantificables, ejemplo: Riesgo Reputacional.

Evaluación cualitativa
La evaluación cualitativa consiste en evaluar cada riesgo y oportunidad de acuerdo con las escalas descriptivas. El análisis cuantitativo requiere valores numéricos para el impacto y la probabilidad usando datos de una variedad de fuentes.
Este análisis utiliza conformaciones de palabras o niveles descriptivos de la magnitud potencial de las consecuencias y la probabilidad de que éstas ocurran. Estos niveles se pueden ajustar a las circunstancias y se pueden recurrir a distintas descripciones para riesgos diferentes.
Para las evaluaciones cualitativas, las técnicas de evaluación más utilizadas son entrevistas, talleres multifuncionales, encuestas, benchmarking y análisis de escenarios.

Evaluación cuantitativa
Las técnicas cuantitativas van desde el benchmarking y el análisis de escenarios hasta la generación de estimaciones prospectivos (modelos determinísticos) y luego a generar distribuciones prospectivas (modelos probabilísticos).

Algunos de los modelos probabilísticos más poderosos desde el punto de vista de toda la empresa incluyen modelos causales de riesgo que se utilizan para estimar los márgenes de beneficios brutos, los ingresos en efectivo o las ganancias en un horizonte temporal a niveles de confianza dados.

Técnicas de evaluación

Análisis de datos existentes
Revisar los datos internos y externos ayuda a evaluar la probabilidad y el impacto de un riesgo u oportunidad. Las fuentes de datos de ocurrencia de riesgo pueden incluir: informes de auditoría interna y externa, reportes de dominio público y datos internos de eventos de pérdidas y los informes publicados por organizaciones de investigación o reguladores. Si bien confiar en los datos existentes proporciona objetividad, es importante evaluar la relevancia de los datos bajo las condiciones del contexto actual y proyectado. Los ajustes pueden ser justificados usando criterios de expertos en el tema. En estos casos, la justificación de los ajustes debe estar claramente documentada y comunicada.

Técnicas de evaluación

Entrevistas y talleres multifuncionales (brainstorming).
La evaluación puede realizarse a través de entrevistas individuales o reuniones facilitadas de *brainstorming*.

Los talleres de brainstorming son preferibles a entrevistas o encuestas con fines de evaluación, ya que facilitan la consideración de las interacciones de riesgo y evitan el pensamiento en silos. Los talleres mejoran la comprensión de un riesgo reuniendo diversas perspectivas. Al evaluar un riesgo, los participantes, que pertenecen a diferentes áreas pueden traer diferente información sobre las consecuencias, probabilidades e interacciones de riesgo.

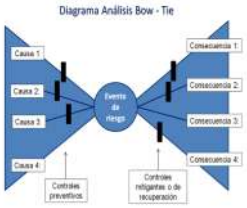
Las entrevistas serán utilizadas para evaluar riesgos conocidos o que el evaluador ya los conoce íntimamente.

Técnicas de evaluación

Análisis de escenarios
El análisis de escenarios permite sensibilizar al análisis. También es útil para evaluar los riesgos y vincularlos con los objetivos estratégicos. Supone la determinación de uno o más escenarios de riesgo, detallando las suposiciones que determinan la gravedad del impacto y la estimación del impacto en un objetivo clave.

Modelos causales de riesgo
El valor en riesgo (VaR),) y las ganancias en riesgo (EaR) son métricas basadas en modelos causales en los que factores de riesgo específicos impulsan la incertidumbre futura de los principales componentes de efectivo o ganancias. Cada factor de riesgo puede modelarse en detalle e incorporarse al modelo general. El uso de un modelo causal de riesgo puede proporcionar una visión de cómo las relaciones históricas podrían desacoplarse y desviarse significativamente de las expectativas. Con el conocimiento de cómo cada factor de riesgo podría variar en el futuro y el impacto de los ingresos en efectivo o ganancias, el riesgo puede ser medido y gestionado de una mejor manera. Independientemente del tipo de modelo, debe establecerse claramente el nivel de confianza sobre las estimaciones de los niveles de riesgo y las suposiciones hechas en el análisis.

Técnicas de evaluación



Análisis de riesgos con diagramas de Arboles de Fallas, Arboles de Eventos y Bow-Tie

Los diagramas rompen una compleja ocurrencia de riesgo en sus partes componentes y permiten mostrar las cadenas de eventos que podrían conducir o resultar de la ocurrencia son indispensables para identificar y evaluar las respuestas a los riesgos y los principales indicadores de riesgo. Los diagramas pueden ser cualitativos o servir como base para los modelos cuantitativos. Un diagrama bow-tie combina un árbol de fallos y un árbol de eventos y toma su nombre de su forma. Los modelos probabilísticos construidos sobre diagramas de bow-tie permiten cuantificar los niveles de riesgo inherentes.

Selección de técnicas de valoración de riesgos

La valoración de riesgos puede realizarse en varios grados de profundidad y detalle y utilizando uno o más métodos que varían de simples a complejos.

Las técnicas adecuadas deben mostrar las siguientes características:

- Debe ser justificable y apropiada para la situación u organización
- Debe proporcionar resultados en una forma entendible
- Debe ser capaz de utilizarse en una manera trazable, repetible y verificable

"Un método simple bien hecho, puede proporcionar mejores resultados que un procedimiento más sofisticado pobremente realizado"

Aplicabilidad de las herramientas

MA= Muy Aplicable A= Aplicable NA= No Aplicable

Herramienta y Técnica	Proceso de Valoración del Riesgo				
	Identificación del Riesgo	Análisis del Riesgo			Evaluación del Riesgo
		Consecuencia	Probabilidad	Nivel de Riesgo	
Lluvia de ideas	MA	NA	NA	NA	NA
Entrevistas estructuras o Semi-estructuradas	MA	NA	NA	NA	NA
Delphi	MA	NA	NA	NA	NA
Listas de verificación	MA	NA	NA	NA	NA
Análisis de principales peligros	MA	NA	NA	NA	NA
Estudios de peligros y operatividad (HAZOP)	MA	MA	A	A	A
Análisis de peligros y puntos críticos de control (HACCP)	MA	MA	NA	NA	MA
Valoración de riesgos ambientales	MA	MA	MA	MA	MA
Estructura: "¿Qué sucedería si...? (SWIFT)	MA	MA	MA	MA	MA
Análisis de Escenarios	MA	MA	A	A	A
Análisis de impacto del negocio	A	MA	A	A	A

APLICABILIDAD DE LAS HERRAMIENTAS

Herramienta y Técnica	Proceso de Valoración del Riesgo				
	Identificación del Riesgo	Análisis del Riesgo			Evaluación del Riesgo
		Consecuencia	Probabilidad	Nivel de Riesgo	
Análisis de causa raíz	NA	MA	MA	MA	MA
Análisis del modo y efecto de la falla (AMEF)	MA	MA	MA	MA	MA
Análisis del árbol de falla	A	NA	MA	A	A
Análisis del árbol de eventos	A	MA	A	A	NA
Análisis de causa y consecuencia	A	MA	MA	A	A
Análisis de causa y efecto	MA	MA	NA	NA	NA
Análisis de niveles de protección (LOPA)	A	MA	A	A	NA
Árbol de decisión	NA	MA	MA	A	A
Análisis de confiabilidad humana	MA	MA	MA	MA	A
Análisis de corbata de lazo	NA	A	MA	MA	A
Confiabilidad centrada en mantenimiento	MA	MA	MA	MA	MA

APLICABILIDAD DE LAS HERRAMIENTAS

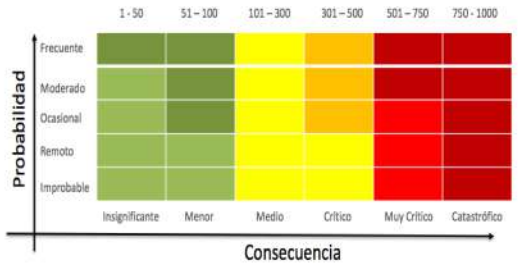
Herramienta y Técnica	Proceso de Valoración del Riesgo				
	Identificación del Riesgo	Análisis del Riesgo			Evaluación del Riesgo
		Consecuencia	Probabilidad	Nivel de Riesgo	
Análisis de condiciones insidiosas (análisis transitorio)	A	NA	NA	NA	NA
Análisis de Markov	A	MA	NA	NA	NA
Simulación Monte-Carlo	NA	NA	NA	NA	MA
Estadística Bayesiana y Redes de Bayes	NA	MA	NA	NA	MA
Curvas FN	A	MA	MA	A	MA
Índices de riesgo	A	MA	MA	A	MA
Matriz de consecuencia y probabilidad	MA	MA	MA	MA	A
Análisis costo beneficio	A	MA	A	A	A
Análisis de decisión multi-criterio	A	MA	A	MA	A

TÉCNICAS DE EVALUACIÓN

Riesgos estratégicos	Brainstorming + consequence/probability matrix
Riesgo operativo	Brainstorming/ structured interviews + consequence/probability matrix
Riesgo de continuidad de negocios	BIA + consequence/probability matrix
Riesgo de seguridad física	Preliminary Hazard Analysis
Riesgos en incidentes de tecnología y seguridad de la información	Bow tie analysis / Root Cause Analysis (RCA)
Cuantificación de riesgo operativo	Scenario Analysis + Montecarlo Simulation
Riesgos de gestión de proyectos	Proyectos simples: Brainstorming/Checklist + Decision Tree + consequence/probability matrix
	Proyectos complejos: Brainstorming/Checklist + Decision Tree + consequence/probability matrix + Montecarlo Simulation

MEDICIÓN DEL RIESGO

Matriz Cruzada:



Fundamento para precisar la evaluación de riesgos

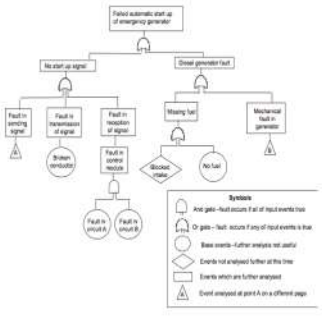


Figure B.2 – Example of an FTA from IEC 60300-3-9

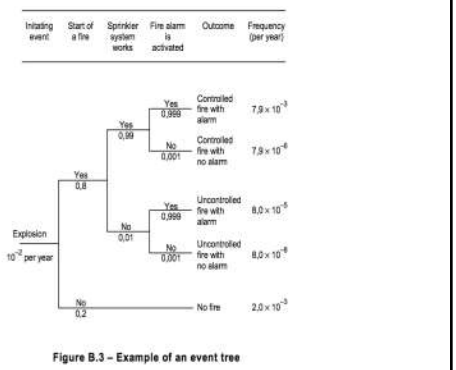


Figure B.3 – Example of an event tree

Controles Internos

Introducción al Internal Control Framework (ICF)

Fevereiro 2011

NOESIS CONSULTING

Controles Internos

MOTIVACIONES INTERNAS Y EXTERNAS

La ocurrencia de eventos críticos en el mundo financiero expuesto públicamente la necesidad de tener un control interno sólido (Sarbanes-Oxley):

Ex.: Enron, WorldCom, AIG, Marsh McLennan

El nuevo enfoque de control interno nos permite estar mejor preparados para afrontar y gestionar las necesidades derivadas de los cambios regulatorios constantes.

Permite a los administradores tener mayor visibilidad de los procesos, riesgos y controles que se aplican en la empresa.

Proporcionarle un entorno único para la verificación y / o análisis de los controles internos.

Sarbanes-Oxley

Public Company Accounting Reform and Investor Protection Act

Federal Office of Private Insurance FOPI

FSA Financial Services Authority

NAIC

making progress . . . together

NOESIS CONSULTING

Controles Internos

Como resultado de la aplicación adecuada de los Controles Internos dentro de la Organización es posible obtener los siguientes beneficios:

- Una mejor comprensión y conocimiento de los riesgos y controles;
- Establecimiento de la propiedad y control de procesos;
- Una mejor comprensión de los procesos y la tecnología de la información de apoyo;
- Al establecer la documentación de diseño de alta calidad y los controles que se pueden utilizar para la formación y transferencia de conocimientos;
- Identificar posibilidades de mejora en la eficiencia y eficacia de los procesos y actividades de control.

NOESIS CONSULTING

Controles Internos

Como resultado de la aplicación adecuada de los Controles Internos dentro de la Organización es posible obtener los siguientes beneficios:

- La validación de la eficacia del proceso por etapas de validación de Gestión (MRCA), realizados por el gestor de procesos;
- Mejor soporte y la documentación del las actividades de auditoría externa e interna;
- Mejorar la calidad, fiabilidad, integridad y transparencia de la información financiera;
- Reducción de los controles redundantes;
- Comunicación unificada entre Auditoría, Riesgos y Cumplimiento.

NOESIS CONSULTING

Internal Control Framework

OBJETIVO

El objetivo principal de ICF es proporcionar **una herramienta** de gestión para el control interno y mejorar su eficacia, que se aplica en un enfoque coherente **en toda la organización**. La metodología de ICF cumple con los requisitos de los entornos en cambio legislativo y reglamentario, mejorar la fiabilidad y la transparencia de la información financiera, asegura que **las áreas de alto riesgo** se abordan adecuadamente por el entorno de control interno y refuerza la responsabilidad de la gestión de negocios. Además de **mejorar el proceso de evaluación y validación** de los controles internos, proporcionan información útil para identificar problemas potenciales en el ambiente de control y posibles mejoras de procesos en toda la empresa.

NOESIS CONSULTING

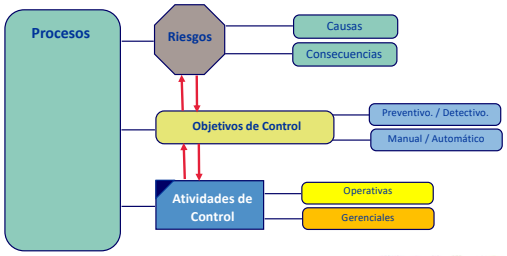
ASPECTOS FUNDAMENTALES DEL INTERNAL CONTROL FRAMEWORK (ICF)

- ***Nivel de control:*** *asociada a los procesos a nivel de empresa (por ejemplo, Gestión de Riesgos, Prevención de Fraude, Gobierno Corporativo, Cumplimiento y regulación, etc.) o el nivel de procesos de negocio (por ejemplo, liquidación, compensación, comisiones, respuestas al regulador ,. etc.)*
- ***Riesgo:*** *basado en el análisis de "¿Qué puede fallar,?" nos permite identificar las causas fundamentales de los riesgos operativos, y en su conjunto, para conocer su impacto y / o consecuencias*
- ***Los objetivos de control:*** *es la base de las actividades de control, es decir, se refieren a la información financiera, operativa y / o cumplimiento.*
- ***Seguimiento de la actividad:*** *Se trata de acciones o procedimientos de control establecidos a nivel local para mitigar un riesgo identificado.*
- ***Validación gerencial de los controles (Managerial Review of Control Activities - MRCA) y las pruebas de control primario (Primary Controls Testing):*** *Es la revisión de cada entorno de control de proceso, llevado a cabo por el personal directivo, a fin de validar y proporcionar evidencia de la capacidad de funcionamiento y eficacia de las actividades de control*

NOESIS CONSULTING

METODOLOGIA DE ICF

Estructura



N O E S I S CONSULTING

Internal Control Framework Workflow

Documentación: Documenta de los procesos en alto nivel, describe el proceso y su flujo y describe las actividades de control, incluyendo la definición de las etapas de validación gestión (MRCA).

Evaluación: Evaluación de las actividades de control en cuanto a la efectividad del diseño y operación, además de documentar los posibles problemas que requieren el desarrollo de un plan de acción.

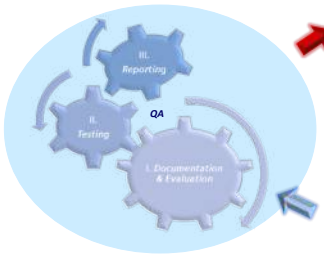
QA: Garantía de Calidad: Los controles deben tener un proceso de garantía de calidad en el diseño.

Pruebas: Las revisiones periódicas por parte del dueño del proceso donde se encuentran las pruebas de control primaria y las pruebas selectivas para el Grupo de Auditoría.

Informes: Informes sobre el estado de los controles internos en el Informe trimestral (controles primarios trimestralmente, otros anualmente,).

N O E S I S CONSULTING

Fases de la Metodología ICF



Gerenciar el Riesgo

Quality Assurance (QA):

Garantía de la calidad de la documentación y de la eficiência de los controles

Efectividad en la imlantación del proyecto y la operatividad del control

Implementar un esquema metodológico de control interno dentro de la organización requiere una comprensión de los procesos de negocios y actividades de control relacionadas con los mismos, así como una visión proactiva de enfoque de riesgo operacional.

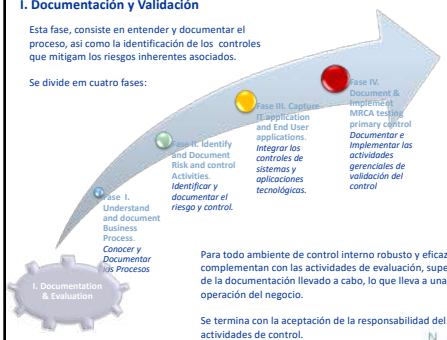
N O E S I S CONSULTING

Fases de la Metodología ICF (cont.)

I. Documentación y Validación

Esta fase, consiste en entender y documentar el proceso, asi como la identificación de los controles que mitigam los riesgos inherentes asociados.

Se divide em cuatro fases:



Para todo ambiente de control interno robusto y eficaz, estas fases se complementan con las actividades de evaluación, supervisión y control de calidad de la documentación llevado a cabo, lo que lleva a una mejora continua de la operación del negocio.

Se termina con la aceptación de la responsabilidad del proceso de todas las actividades de control.

NOESIS CONSULTING 11

Fases de la Metodología ICF (cont.)

I. Documentación y Validación (cont)

I	II	III	IV
Comprender e Documentar los Procesos De Negocio	Identificar y Documentar Los Riesgos y Actividades de Control	Determinar as aplicaciones de Sistemas y EUA	Documentar e Implementar MRCA
¿Cuáles son las actividades, roles, responsabilidades y el flujo de información de los procesos de negocio?	Las actividades de control pertinentes se implementan para mitigar los riesgos?	El proceso está apoyado por algún sistema o End-user application (EUA)?	Como vamos monitorear la eficacia operacional del control?

NOESIS CONSULTING 12

Fases de la Metodología ICF (cont.)

I. Documentación y Validación (cont)

FASE I: Conocer y Documentar los Procesos

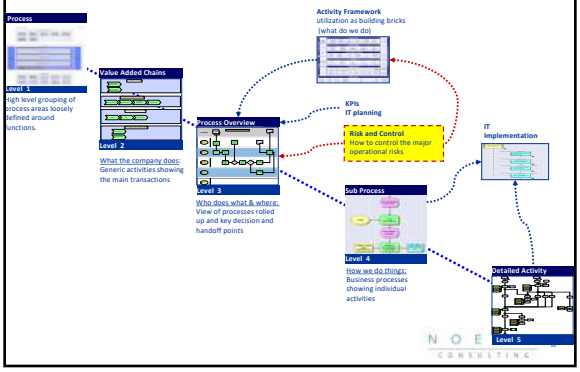
- Objetivo: conocer el proceso de inicio a fin, para responder las siguientes preguntas: **qué** , **quién, cómo** y d**onde** para determinar si las actividades de control son efectivas bajo el punto de vista de su design y operación.

- Los productos de esta fase son:
  - Una narrativa y descripción del proceso al nivel Macro o un Diagrama de flujo en el nivel genera (Flowchart)
  - Validación de las actividades y documentación de las actividades de control, enfocando el esfuerzo en los controles primarios
  - Documentación y planes de acción

- Los actores principales son los Responsables de los procesos en su papel de gerente *y* de la Gerencia de Riesgos, a través del responsable de Controles Internos.

NOESIS CONSULTING 13

Methodología
Implementación – Top Down approach



Internal Control Framework

High-Level Process Narrative

Overview of Process including any sub processes	**COBRANZAS (CBR)** **El área es responsable de la administración y gestión del recibo de prima de seguro.** **Con la ayuda de varios sistemas interconectados, el área gestiona el pago de la parte de entrada y otras cuotas, además de gestionar los ajustes, las cancelaciones y pago de la restitución.** **Las llamadas a los corredores / asegurados se establecen a través de demandas herramienta intermediados por el Call Center.** **Descripción de los objetivos macro de los subprocesos** **Subprocesos: (CBR1) Recibir pagos en efectivo, (CBR2) Cheque de pago en cuotas, (CBR3) Ajustar / cancelar / Restauración de pago, (CBR4) control de solicitudes del cliente.**
Staff Average staffing	1 Supervisor de Cobranza 1 Analista SR 3 Analistas PL 4 Analistas JR
Location Place and number of locations	Minas Brazil Seguros S.A. Rua dos Cantés, 745, 7o andar Centro – Belo Horizonte
Major Application Systems / Interfaces and End-user Applications	FCR, DAC, GAC, SPY, SAP, ABY
Internal Service Providers, if applicable and/or Third Party Service Provider impacting the process	Averbach - Empresa de cobranza terceirizada.
Glossary of Terms e.g. abbreviations such as CFO, EUA	CFO – Chief Financial Officer EUA – End-User Application
Related ICF Processes	PAYMENTS & COLLECTIONS

Internal Control Framework

High-Level Process Narrative

A. Sub process:	CBR1 Recibir Pagos en Efectivo
High Level Description	
Responsible (Function / Title)	

Fases de la Metodología ICF (cont.)

I. Documentación y Validación (cont)

Fase II: Identificar y documentar los riesgos y controles

- Objetivo: identificar los riesgos y sus respectivas actividades de control, determinando "**que puede fallar**" y sus causas

Los controles deben ser identificados por su función como: **Preventivo o Detectivo**, y por su aplicación como: **Manual o Automático**, y adicionalmente si son considerados **Primarios** o no.

Que son los controles Primarios?

Son aquellas actividades de control que en caso de no existir, pueden generar riesgo en las operaciones, riesgo financieros o de cumplimiento y por su esencia no pueden ser mitigados por otros medios.

Son los controles más importantes para la gestión gestión y para las transacciones que garantizan que las actividades se cumplan los objetivos.

NOESIS CONSULTING 14

Fases de la Metodología ICF (cont.)

I. Documentación y Validación (cont)

Fase II: Identificar y documentar los riesgos y controles

- Los controles primarios no son sólo para evitar errores financieros.
- En caso de involucrar a la organización y seguir siendo relevante, como por ejemplo: un cambio organizativo, que tiene sus propios riesgos y por lo tanto requiere controles.
- Los productos de esta fase son la identificación de los controles, su eficacia, la frecuencia de ejecución y los responsables, así como los riesgos operacionales.
- Los principales actores son los responsables del proceso en su calidad de Administrador, junto con la Gerencia de Riesgos, a través del responsable de ICF

NOESIS CONSULTING 15

Fases de la Metodología ICF (cont.)

I. Documentación y Validación (cont)

Fase III - Capturar los sistemas y aplicaciones tecnológicas

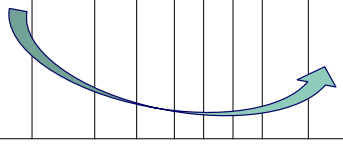
- Objetivo: Identificar, documentar y evaluar las aplicaciones de tecnología de la información que integran a los procesos de apoyo
- Se validan que existan las actividades de control en los sistemas / aplicaciones y si son eficaces en su funcionalidad para el proceso.
- En esta fase debe ser completada con el análisis de TI sobre los controles establecidos automáticos en las aplicaciones.
- Los productos de esta fase son: la identificación de los controles en los sistemas / aplicaciones, su eficacia, así como la frecuencia y responsable.
- Los principales actores son los responsables del proceso en su calidad de Administrador, junto con la Gerencia de Riesgos, a través del responsable de ICF

NOESIS CONSULTING 16

Internal Control Framework

Validación de las Actividades de Control

Control Activity (1), (7)	Description of Local Control Activity (1), (9), (10)	Documentation – Control Activity Comments					Applicable Control Activity? (4)	Evaluation of Design Effectiveness	Evaluation of Operating Effectiveness	MRCA validation step including: Description, Title/ Function, Evidence (9)	Control Activity Class (5)
		Evidence or Reference Sources (8), (10)	Title or Position, Dept. (8), (10)	Frequency (8), (10)	Control Type 1 (2), (6)	Control Type 2 (3), (6)		Satisfactory NI – Needs Improvement U-nsatisfactory	Satisfactory NI – Needs Improvement U-nsatisfactory		
REC 13 Foram estabelecidos processos e controles adequados para monitorar pagamentos que não houve "matching".	Pagamentos que não houve "matching" são extraídos do sistema e controlados pelo analista.	Planilha gerada pelo sistema SPY de tudo que não houve "matching" é gerenciada pelo analista.	Analista de Cobrança	Eventualmente	P-D	M-A	Y	S	S	**Description:** Pagamentos que não houve matching são discriminados em planilha gerada pelo sistema SPY, para análise do analista. **Title:** Analista de Cobrança **Evidence:** A planilha de matching informa os pagamentos que tiveram situação irregular durante o processo de pagamento, esta é extraída por sistema e controlada pelo analista eventualmente.	MAMO



NOESIS CONSULTING

Internal Control Framework

Validación de las Actividades de Control

Control Activity (1), (7)	Description of Local Control Activity (1), (9), (10)	Documentation – Control Activity Comments					Applicable Control Activity? (4)	Evaluation of Design Effectiveness	Evaluation of Operating Effectiveness	MRCA validation step including: Description, Title/ Function, Evidence (9)	Control Activity Class (5)
		Evidence or Reference Sources (8), (10)	Title or Position, Dept. (8), (10)	Frequency (8), (10)	Control Type 1 (2), (6)	Control Type 2 (3), (6)		Satisfactory NI – Needs Improvement U-nsatisfactory	Satisfactory NI – Needs Improvement U-nsatisfactory		
REC01 As políticas e procedimentos relacionados ao ciclo de recebíveis (inclusive as políticas de reconhecimento de receitas, medição, divulgação, IFRS e políticas do Grupo) são documentados e comunicados aos funcionários relevantes. (I, II)	Não tem controle sobre as atualizações dos procedimentos. **As políticas e procedimentos relacionados ao ciclo de recebíveis estão desatualizados.**	As políticas e procedimentos da área estão descritas no Manual de Procedimentos – Área Financeira. Entretanto este documento não está atualizado e não é de conhecimento de todos.	Gerente Financeiro	Eventualmente	P-D	M-A	Y	**NI**	**NI**		POPR

Se genera um issue porque la actividad no se la está realizando.

NOESIS CONSULTING

Fases de la Metodología ICF (cont.)

I. Documentación y Validación (cont)

Fase IV - Documentar e Implementar as atividades de control y acompañamiento (MRCA)

Objetivo: Para dejar evidencia escrita de control de las actividades de supervisión. Los pasos para evaluar el rendimiento de control y se identifican y documentan las actividades asociadas con él sobre una base diaria por los responsables.

Es una fase asociado con el monitoreo y la conciencia con respecto a los controles y el riesgo, donde los principales objetivos son:

- Confirmar la comprensión de las actividades de control por el responsable del proceso y dejar evidencia de conformidad con el mismo trimestre.
- Fortalecer la responsabilidad y el compromiso de los responsables de los procesos en la ejecución de las actividades de control
- determinar de antemano la ineficacia de los controles
- Contribuir a la reducción de las actividades de prueba de control por parte del grupo de auditoría o grupos externos.

NOESIS CONSULTING

17

Internal Control Framework

Ejemplo de MRCA - Managerial Review of Control Activities

La revisión gerencial de las actividades de control es el paso realizado por el Supervisor/Gerente para validar la eficacia operacional de las actividades de control como parte de la operación del día a día.

Description of Local Control Activity	MRCA applicable	MRCA
REC01 El Departamento de Recursos Humanos mantiene políticas y procedimientos aprobados para garantizar que los procedimientos están en cumplimiento con las normas contables IFRS. Estos procedimientos son revisados y aprobados anualmente.	yes	**Brief description:** El gerente se asegura de que el documento correcto está en la carpeta compartida una vez que se se aprobó.. El gerente también se asegura de que el personal es consciente y esta debidamente formado en las políticas y procedimientos del departamento en las reuniones trimestrales con su personal y se tiene establecido un plan de entrenamientos anual. **Responsible:** Gerente del área **Evidence:** El gerente completa el formulario de revisión trimestral, lo firma, escanea y guarda en la carpeta compartida MRCA **Frequency:** Anual

NOESIS CONSULTING

Fases de la Metodologia ICF

I. Documentación y Validación QA

Avaliação Inicial

Validar las actividade de control	Documentar Deficiencias que requieren corrección	Quality Assurance	Sign-off inicial
El control está diseñado apropriadamente para alcanzar el objetivo de control?	Existe un enfoque adequado para abordar las deficiencias de diseño y su eficacia operacional?	Cada processo está documentado de acuerdo con las directrices de O&M	Las actividades de control están de acuerdo con ICF?

NOESIS CONSULTING

Internal Control Framework

Registro de no conformidad (issue) y planes de acción

Validate Issues

Certus Issue ID	SOX Key Rec.	ICF Process	Local Process	Control Activity Ref.	Issue	Classification	Issue Class	Potential F/S Misstatement Impact in USD	Action Plan	Action Plan Responsible	Comments	Compensating Control (yes-no)	Describe the Compensating Control	IT or Non-IT Issue
		Receivables	Receivables-Bad debt Provisioning	REC01-B	Evidence does not exist to support that a proper review of the Ageing Report is occuring. As a result, it can not be determined that a proper review of the Ageing Report is routinely occuring. Lack of review of the Ageing Report may cause misstated Accounts Receivable balances, untimely collection of cash payments, understating account write-offs and improperly valuing the allowance for bad debt reserves. The financial impact would be estimated at $ X,000,000.	Medium	POPR - Policies & Procedures	USD 1,000,000 or less	A checklist will be created by the B&C supervisor which will be used to execute the Ageing Report review on a monthly basis. This checklist will be attached to the first and the last page of the Ageing Report and filed in the B&C manager's locked file acabinet. An archive will be created for past referencing of Ageing Reports.	B&C Manager and B&C Supervisor		Yes	Variance Analysis of affected account balances.	Non-IT

NOESIS CONSULTING

Fases de la Metodologia ICF (cont.)

II. Test

Consiste en validar la eficacia del control, tanto en su diseño como en su operación, cumpliendo con los patrones identificados y definidos en la Fase I, específicamente en relación a la matriz MRCA.

Es el refuerzo de la validación del control desde el punto de vista de dos enfoques: el diseño y la operación.

Esta fase es ejecutada por el personal de IC de la Gerencia de Riesgos para la palicación de los checklist de Eficiancia del Diseño y Eficiencia de la Operación del control. Los responsables de las validaciones son los dueños de los controles.

De la misma forma, esta actividad de validación puede ser realizada por el área de Cumplimiento, Auditiría Interna o Auditoría Externa obteniendo siempre la misma conssistencia procedimental de la ejecución del control.

NOESIS CONSULTING 20

Fases de la Metodologia ICF (cont.)

III. Reporte

Los cambios que ocurrieron en las diferentes etapas de la implemantación de los Controles Internos, los controles o los riesgos serán actualizados trimestralmente. Posteriormente deben ser revisados y aprobados.

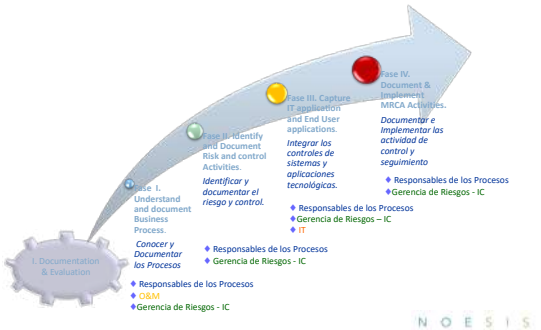
En esta fase el personal de Controles Internos trabaja en conjunto con el responsable del proceso para obtener la aprobación y/o comunicar las actualizaciones realizadas en las actividades de control o en las deficiencias identificados y validados..

En este proceso se dejan las evidencias de las actividades de control asociadas, buscando dejar todos los comentarios documentados.

El producto final de esta fase es el Informe Trimestral de las Actividades de Control Interno (***Sign-Off)*** que se envía al directorio.

NOESIS CONSULTING 21

Responsabilidades



NOESIS CONSULTING 24

Responsabilidades de Auditoría Interna