AUDITORIA Y ASEGURAMIENTO
ASESORAMIENTO TRIBUTARIO
CONSULTORIA GERENCIAL Y DE T.I.
BPO DE CONTABILIDAD Y NÓMINA

sfaicolombia sfaicolombia

SFAI

Boletín No. 284 - Octubre de 2022

IMPLEMENTAR UN MARCO DE GESTIÓN DE RIESGOS EMPRESARIALES (ERM)

Por: *Rodrigo García Ocampo (CPA, MBA, MGE, MGR)*
Socio - Director
Email: *rgarcia@sfai.co*

En un mundo como el que hoy vivimos, el éxito empresarial dependerá en gran medida de cómo se evitar la materialización de riesgos para que los resultados de la empresa no se vean afectados; es por eso que, las empresas, cualquiera sea su tamaño, requieren de herramientas que identifiquen, limiten o eliminen amenazas internas o externas para que sus operaciones no se vean afectadas.

Para limitar la materialización de riesgos, se necesita de la Gestión de Riesgos Empresariales (ERM, por su siglas en inglés).

La reducción de los impactos de los riesgos en las empresas no es una tarea fácil dado que el entorno cada día es variante y las empresas necesitan adaptarse rápidamente a esos cambios para no perder terreno en lo avanzado, por lo que amenazas como factores macroeconómicos externos, incluidas las presiones inflacionarias, los cuellos de botella en la cadena de suministro y los obstáculos legislativos, debe evaluar continuamente para administrar el riesgo de manera proactiva y efectiva.

¿Qué es la gestión de un ERM?

La gestión de un ERM es el proceso interactivo que las empresas utilizan para gestionar el riesgo frente a amenazas internas y externas conforme a su actividad, donde se debe identificar el riesgo y clasificarlo para luego trabajar en su reducción o mitigación a través de estrategias de gestión de riesgos.

Objetivos del programa ERM

Un programa ERM comienza con los siguientes cinco pasos, que interactúan y se perfeccionan con el tiempo para dar cuenta de los cambios que ocurren en cualquier negocio:

- Defina la perspectiva empresarial y sus políticas de transparencia.
- Defina el apetito y la tolerancia al riesgo e implemente una estrategia que le permita medir si los resultados son los esperados.
- Establezca el alcance de cómo se manejan las decisiones relacionadas con el riesgo.
- Defina e implemente las políticas para el gobierno del riesgo.
- Revisar y actualizar los pasos anteriores durante las evaluaciones internas mediante el seguimiento, la supervisión y la auditoría.

El Marco ERM

Los marcos de gestión de riesgos empresariales (ERM) son herramientas que ayudan a estructurar y determinar la respuesta al riesgo. La gestión de riesgos debe supervisar todos los aspectos de la empresa, por lo que, personas, equipos de trabajo, divisiones, sitios de operación y cualquier otra parte la empresa debe estar cubierta por el marco ERM en todo momento.
Los ERM tiene un enfoque de arriba hacia abajo, que incluye una visión completa y detallada de las operaciones de la empresa. Además, debe identificar y responsabilizar al personal expuesto a riesgos, por lo que el uso de software especializados facilita el proceso.

Los marcos ERM son herramientas que guían la política de riesgos de la empresa conforme a su actividad, por lo que se pueden encontrar diferente marcos ERM, tales como:

- The Committee of Sponsoring Organizations of the Treadway Commission Framework o Marco COSO, es un sistema para gestionar el riesgo en las empresas, usada globalmente por lo que se puede encontrarse en muchas empresas en uso.
- Control Objectives For IT (COBIT) es una estrategia de gobierno de TI que alinea los objetivos empresariales y de TI para reducir el riesgo.
- El cumplimiento de la Ley Sarbanes-Oxley (SOX) para las empresas que cotizan en bolsa reduce el riesgo de manipulación de acciones. También es un requisito reglamentario para las empresas que cotizan en EE. UU.
- Gobierno, Riesgo y Cumplimiento (GRC) es un estándar industrial de facto basado sobre las mejores prácticas para hacer crecer un negocio. Este es un proceso de revisión interactivo basado en principios de gobierno, riesgo y cumplimiento.

Existen también otros marcos especializados para cada tipo de industria como el NIST Cybersecurity Framework. El Instituto Nacional de Estándares y Tecnología (NIST) es parte del Departamento de Comercio de los Estados Unidos. El marco de ciberseguridad del NIST ayuda a las empresas a comprender y reducir su riesgo de ciberseguridad.

Marco NIST protege la red y los datos. Aborda específicamente los riesgos cibernéticos en un negocio, que el Marco COSO no cubre.

Los componentes generales en cualquier marco ERM.

Cada marco ERM sirve para diferentes propósitos; sin embargo, todas ellas comparten unos objetivos fundamentales:

Continuación de la Página No. 1

1. Cree un equipo ERM multifuncional

Al implementar un marco de ERM, seleccione su equipo de ERM. Los integrantes deben corresponder a los dueños de los diferentes procesos que existen en la empresa.

Necesitará ayuda especial de sus administradores de TI. Estos expertos ayudarán con soluciones ERM basadas en software y flujos de trabajo ERP automatizados. Si no tiene una solución ERM, podrá agregarla después de evaluar la tolerancia al cambio de su empresa.

2. Identificar el riesgo

Defina todos los riesgos de su negocio. Los miembros del equipo de ERM identificarán los riesgos en sus respectivos procesos y transmitirán la información para su procesamiento.

3. Evaluar el riesgo

Además de identificar cada riesgo, también debe evaluar su frecuencia y gravedad en el caso que se materialice. Para evaluar el riesgo, asigne los valores de frecuencia y gravedad a cada riesgo y luego multiplique para obtener el valor ponderado.

Utilice formularios de evaluación de riesgos creados para tal fin y cree una tabla que resalte los valores de frecuencia y gravedad, para que el revisor pueda calcular rápidamente el valor ponderado. Alternativamente, también puede crear un rango de valores para los riesgos. Los valores del rango determinarán la necesidad de acciones de mitigación de riesgos.

Además, debe determinar el riesgo umbral averiguando qué nivel de riesgo sería tolerable. Si algún riesgo supera el umbral, debe actuar de inmediato para neutralizarlo o reducirlo.

4. Priorizar el riesgo

Después de identificar los riesgos, cuantifique su impacto en el negocio. Si lo hace, le ayudará a priorizar los riesgos en función de su valor de impacto. Como resultado, podrá abordar primero los riesgos de mayor impacto para su empresa. Esto, a su vez, reducirá el riesgo general para el crecimiento de su negocio.

5. Abordar el riesgo

Una vez haya priorizado los riesgos, resultará más fácil asignar recursos para abordar esos riesgos. Aunque el objetivo es eliminar el riesgo por completo, es posible que eso no siempre sea práctico. Sin embargo, puede reducir el riesgo a niveles tolerables.

6. Optimizar el riesgo

Su tolerancia al riesgo variará según la línea de negocios en la que se encuentre. Deberá evaluar el progreso que está logrando frente a los riesgos y, preguntarse ¿Estamos en el camino correcto para lograr los objetivos? De lo contrario, deberá agregar más recursos.

La optimización del riesgo es un proceso subjetivo. Sin embargo, puede medir objetivamente el progreso comparando los resultados obtenidos con periodo históricos.

7. Seguimiento y Evaluación

Una vez que tenga un marco ERM en funcionamiento, debe monitorear las solicitudes de cambio y realizar evaluaciones de riesgo. Necesitará una solución ERP para realizar un seguimiento de las tareas y gestionar los flujos de trabajo en función a su marco ERM.

SFAI, proporciona años de experiencia con su red de oficinas en más de 114 países para ofrecer servicios construidos bajo necesidades localizadas conforme al tamaño y magnitud de nuestros clientes en: Finanzas Corporativas, Capital Humano, Riesgos Empresariales, Auditoría Externa y Revisoría Fiscal, Asesoramiento Legal y Tributario, BPO Contable y Administrativo y otros servicios de valor que contribuyen al desarrollo de estrategias que alcanzan objetivos. Déjenos conocer sus necesidades en www.sfai.co/contactenos o a través del del WhatsApp +57 318 37 14 596.