

# Guía para la gestión de riesgos empresariales

## PREGUNTAS FRECUENTES

**protiviti**<sup>®</sup>  
Independent Risk Consulting

# Guía para la gestión de riesgos empresariales: Preguntas frecuentes

	Nº de página
<b>Introducción</b>	1

## Los fundamentos

1. ¿Qué es la gestión de riesgos empresariales (ERM)?	3
2. ¿Por qué implementar ERM?	3
3. ¿Cómo se compara el alcance de ERM con los enfoques de gestión de riesgos existentes?	5
4. ¿Cuál es la propuesta de valor para implementar ERM?	7
5. ¿Qué empresas están implementando ERM?	9
6. Si las empresas no están implementando ERM, ¿qué están haciendo?	10
7. ¿Quién es responsable de ERM?	11
8. ¿Cuáles son los pasos que las empresas pueden tomar de inmediato para implementar ERM?	11
9. ¿Es ERM aplicable a organizaciones más pequeñas y menos complejas?	11
10. ¿Por qué las empresas que han intentado implementar ERM han fracasado en sus esfuerzos?	11
11. ¿La implementación de ERM asegura el éxito de un negocio?	12
12. ¿Cuál es la diferencia entre ERM y gestión?	12
13. ¿Qué significa "implementar ERM"?	12
14. En general, ¿cuánto tiempo lleva implementar ERM?	13
15. ¿Hay alguna forma de comparar el nivel de inversión requerido para implementar ERM?	13
decisión. ¿No gestionan con éxito empresas que ya aplican ERM?	14
17. ¿Cuánto tiempo ha existido ERM y por qué hay un enfoque renovado en él?	14
18. ¿Qué porcentaje de empresas públicas cuentan actualmente con un proceso o sistema ERM? 19 ¿Hay algún ejemplo de ERM eficaz tal como se aplica en la práctica?	15
20. ¿Cómo varía la aplicación de ERM según la industria?	decisión
21. ¿Hay alguna organización que no necesite implementar ERM?	decisión
22. ¿Cuáles son los mandatos regulatorios para implementar ERM?	decisión
23. ¿Los estándares para implementar ERM son diferentes para las empresas públicas y privadas?	17
24. ¿Deben las empresas tener procesos sofisticados en todas las áreas de gestión de riesgos para obtener los beneficios de ERM?	17

## Gestión de riesgos empresariales de COSO: marco integrado

25. ¿Qué es COSO?	17
26. ¿Por qué se creó COSO Enterprise Risk Management – Marco Integrado?	18
27. ¿Qué es la gestión de riesgos empresariales de COSO: marco integrado?	18
28. ¿Cómo podemos obtener el framework COSO ERM?	19

## Índice (continuación)

	Nº de página
29. ¿Cómo se desarrolló el marco COSO ERM?	19
30. ¿Cómo usamos el marco COSO ERM?	20
31.     ¿Están obligadas las empresas a utilizar el marco COSO ERM?	20
32.     ¿El marco integrado de gestión de riesgos empresariales de COSO reemplaza o reemplaza el marco integrado de control interno de COSO?	20
33. ¿Cómo se compara COSO Enterprise Risk Management – Marco Integrado con el Control Interno COSO – ¿Marco Integrado?	20
34.     ¿El nuevo marco COSO amplía el enfoque de ERM más allá del enfoque tradicional del modelo de gestión de riesgos en el riesgo asegurable? ¿Si es así, cómo?	21
35.     ¿Existen otros estándares y marcos y, de ser así, qué promulgan y cómo se relaciona con ellos el marco integrado de gestión de riesgos empresariales de COSO?	21
36. ¿Cuál es el punto de vista de la Comisión de Bolsa y Valores (SEC) con respecto a ERM?	21
37. ¿Cuáles son los entregables cuando se implementa el marco COSO ERM?	21
38.     ¿Puede una empresa adoptar “parcialmente” el marco integrado de gestión de riesgos empresariales COSO con éxito?	22

## El papel de la dirección ejecutiva

39. ¿Quién debería participar en el proceso de ERM y cómo?	23
40.     ¿Debe el director general participar plenamente en el proceso o sistema de ERM para que tenga éxito, o puede delegarlo en otra persona?	23
41. ¿Cómo se beneficiará la alta dirección del apoyo a la implementación de ERM?	24
42. ¿Cómo debería la dirección ejecutiva evaluar la ERM?	24
43. ¿Cuál es el papel del CIO en un entorno ERM?	24
44. ¿Cuál es el papel de la tesorería y los seguros en un entorno ERM? 45.	25
¿ERM requiere informar a la dirección ejecutiva? Si es así, ¿qué tipos de informes son los más adecuados para la dirección ejecutiva?	25

## El papel del director

46. ¿Cómo se relacionan la ERM y la gobernanza?	26
47. ¿Por qué los directores deberían preocuparse por si sus empresas implementan ERM?	26
48. ¿Cómo debe ver el comité de auditoría la ERM?	27
49. ¿Cómo debe la junta ejercer la supervisión de la implementación de ERM?	28

## El papel del director de riesgos

50.     ¿Debería nuestra organización tener un director de riesgos (CRO) y, de ser así, cuál es su función?	30
51. ¿Cuáles son los conjuntos de habilidades del CRO?	32
52.     ¿A quién reporta el CRO?	32

## Índice (continuación)

	Nº de página
<b>La Estructura de Supervisión de la Gestión de Riesgos</b>	
53. ¿Cuál es el objetivo principal de la estructura de supervisión de la gestión de riesgos?	33
54. ¿Cómo se consideran los temas de compensación al organizar la supervisión de la gestión de riesgos? ¿Estructura?	33
55. ¿Existe una estructura de supervisión organizacional recomendada?	34
56. ¿Cómo se relaciona la estructura de supervisión de la gestión de riesgos con la estructura organizacional existente de la entidad?	35
57. ¿La implementación de ERM requiere la identificación de propietarios de riesgos individuales?	40
<b>El papel de la auditoría interna</b>	
58. ¿Qué funciones desempeña la auditoría interna en la implementación de ERM?	40
59. ¿Debe la auditoría interna liderar el esfuerzo de ERM?	42
60. ¿Debe la auditoría interna integrar el marco COSO ERM en su trabajo?	42
61. ¿Acaso auditoría interna no ha evaluado la aplicación de ERM dentro de la organización?	42
62. ¿Apoya el Instituto de Auditores Internos (IIA) la gestión de riesgos empresariales de COSO? marco integrado?	42
63. ¿Los estándares del IIA requieren el uso de COSO Enterprise Risk Management – Integrated Estructura? Por ejemplo, ¿cuál es la relación de ERM con el Estándar IIA 2010.A1 (que requiere que la auditoría interna realice una evaluación de riesgos anual) y 2110.A2 (que requiere una evaluación de riesgos amplia alineada con el marco COSO)?	42
<b>Visión y objetivos de la gestión de riesgos</b>	
64. ¿Cómo desarrolla la dirección una visión compartida del papel de la gestión de riesgos en la organización? ¿Cuál es el uso práctico de una visión compartida?	43
65. ¿Cómo define la administración las metas y objetivos de administración de riesgos de la entidad?	44
66. ¿Qué es el “apetito de riesgo” y en qué se diferencia de los “umbrales de riesgo”, “tolerancias” o “límites”? 67. ¿Existe una metodología definida para calibrar el desempeño con tolerancias al riesgo?	46
68. ¿Cómo se traducen la visión y los objetivos de la gestión de riesgos en los Infraestructura ERM?	47
	49
<b>Realización de evaluaciones de riesgos</b>	
69. ¿Cuál es la relación entre la evaluación de riesgos y la gestión de riesgos?	51
70. ¿Cuál es la relación entre la evaluación de riesgos y la evaluación del desempeño?	51
71. ¿Cuáles son los componentes de una declaración de objetivos efectiva y por qué los objetivos importantes para una evaluación de riesgos eficaz?	52
72. ¿Cuál es la diferencia entre un evento y un riesgo?	52
73. ¿Por qué la definición de riesgo de COSO no incorpora la noción de que el riesgo incluye al alza como así como inconveniente?	52
74. ¿Cómo articulamos el concepto de riesgo inherente para que pueda usarse efectivamente como criterios de evaluación?	53

## Índice (continuación)

	Nº de página
75. ¿Existe un lenguaje de riesgo respaldado oficialmente que podamos usar para nuestra organización?	53
76. ¿En qué medida la organización define estrictamente el riesgo para la empresa en su conjunto, cuando la organización tiene una variedad de negocios diferentes?	55
77. ¿Qué son los mapas de riesgos y cómo se utilizan adecuadamente durante el proceso de evaluación de riesgos?	55
78. ¿Cuál es una forma efectiva para que una organización realice una evaluación de riesgos?	56
79. ¿Cuáles son los errores y trampas comunes durante el proceso de evaluación de riesgos?	58
80. ¿Cómo identificamos, entendemos y aplicamos las interrelaciones entre los riesgos?	60
81. ¿Cuál es el nivel apropiado de profundidad al evaluar el riesgo?	61
82. ¿Quién debe participar durante el proceso de evaluación de riesgos?	61
83. ¿Cómo se relaciona la evaluación de riesgos con la cuantificación de riesgos y se debe utilizar la cuantificación de riesgos durante la evaluación de riesgos?	61
84. ¿Tiene algún valor utilizar información cualitativa al evaluar el riesgo?	61

## Primeros pasos: establecer las bases

85. ¿Cuáles son los mejores pasos a seguir para empezar?	62
86. ¿Es ERM otro "proyecto"?	64
87. ¿Hay cosas específicas que una organización debe lograr el primer año?	64
88. ¿Quién es responsable de "lidiar la carga" para implementar ERM?	64
89. ¿Quién debe patrocinar la implementación de ERM?	---
90. ¿Cómo se obtiene la aceptación de los altos ejecutivos clave?	---
91. ¿Cómo obtenemos aceptación entre nuestros gerentes operativos?	---
92. ¿Podemos aprovechar la infraestructura existente para no crear más gastos generales?	67
93. ¿Qué tipos de habilidades se necesitan para implementar ERM?	67
94. ¿Necesitamos poner un nombre a una iniciativa de ERM, es decir, no es ERM solo una buena práctica comercial? con otro nombre?	67
95. ¿Las empresas generalmente agregan personal a tiempo completo para desarrollar e implementar con éxito un proceso y sistema de ERM, o normalmente utilizan personal existente que dedica sus esfuerzos a esta iniciativa a tiempo parcial o completo?	68
96. ¿Qué pasos toma la administración para sentar las bases?	68
97. ¿Cómo decide la administración sobre las capacidades básicas apropiadas?	69
98. ¿Por qué tener un lenguaje común y hay ejemplos? 99 ¿Hay ejemplos de un esquema de clasificación de procesos?	69
100. ¿Cómo se mejora el diálogo sobre el riesgo y sus causas fundamentales, impulsores y fuentes?	69
101. ¿Cómo se mejora el intercambio de conocimientos sobre gestión de riesgos?	70
102. ¿Qué significa aumentar la conciencia o la sensibilidad al riesgo de una organización?	71

## Índice (continuación)

	Nº de página
<b>Tomando una Vista de Proceso – Construyendo Capacidades</b>	
103. ¿Qué pasos toma la administración para desarrollar capacidades de gestión de riesgos?	72
104. ¿Cómo decide la dirección sobre las capacidades adecuadas de gestión de riesgos?	74
105. ¿Cómo mejora la administración las evaluaciones de riesgos de la organización?	74
106. ¿Cómo se relacionan el establecimiento de objetivos, la identificación de eventos y la evaluación de riesgos?	74
107. ¿Qué tan importante es la evaluación de riesgos para el esfuerzo de ERM?	74
108. ¿Qué respuestas alternativas están disponibles para gestionar el riesgo?	74
109. ¿Qué factores debe considerar la gerencia al evaluar las respuestas alternativas al riesgo?	78
110. ¿Cuáles son los elementos de la infraestructura de gestión de riesgos, por qué son importantes y cómo se consideran?	82
111.       ¿Existe un modelo que nos ayude a establecer nuestras prioridades al implementar ERM y monitorear nuestro progreso a medida que mejoramos nuestras capacidades de gestión de riesgos?	83
112. ¿Cuáles son las técnicas alternativas para medir el riesgo y cuándo se implementan?	92
113. ¿Cómo influye ERM en los informes de gestión?	95
114. ¿Qué productos de software de gestión de riesgos están disponibles actualmente para ayudar a las empresas a implementar ERM?	96
115. ¿Ha alcanzado el mercado de software ERM una madurez tal que existen soluciones establecidas y líderes claros?	96
116. ¿Qué criterios debemos usar para evaluar las alternativas de software? ¿Existen diferentes priorizaciones de funcionalidad?	97
117.       ¿Es preferible el software de ERM especializado a las plataformas más amplias para el cumplimiento, la gobernanza y la gestión de riesgos?	99
118. ¿Cómo respalda la funcionalidad del software los objetivos de ERM?	99
119. ¿Cuáles son las principales categorías y características de los proveedores de software ERM exitosos?	100
120.       ¿Es mejor diseñar primero un proceso de ERM y luego seleccionar el software de ERM adecuado? ¿O viceversa?	101
121. ¿Qué son los informes de panel o cuadro de mando y cómo se utilizan en un entorno de ERM?	101
122. Para las empresas de servicios financieros, ¿es la medición del capital económico un requisito previo para la adopción de ERM?	104
123. ¿Cómo se aplica la mejora continua a la gestión de riesgos?	104
124. ¿Cuáles son las sinergias y diferencias entre ERM y las "iniciativas de calidad" (p. ej., Six Sigma, Lean, TQM, etc.)?	106
<b>Llevándolo al siguiente nivel: capacidades mejoradas</b>	
125. ¿Qué pasos toma la administración para mejorar las capacidades de gestión de riesgos?	107
126. ¿Cómo decide la administración sobre las capacidades de mejora apropiadas?	108
127. ¿Qué es una "visión de cartera" de riesgos y cómo se aplica en la práctica?	108
128. ¿Cómo cuantifica la administración los riesgos en toda la empresa?	109

## Llevándolo al siguiente nivel: capacidades mejoradas

125. ¿Qué pasos toma la administración para mejorar las capacidades de gestión de riesgos?	107
126. ¿Cómo decide la administración sobre las capacidades de mejora apropiadas?	108
127. ¿Qué es una "visión de cartera" de riesgos y cómo se aplica en la práctica?	108
128. ¿Cómo cuantifica la administración los riesgos en toda la empresa?	109

## Índice (continuación)

	Nº de página
129. ¿Cómo usa la administración ERM para mejorar el desempeño comercial?	112
130. ¿Cómo debemos integrar nuestro enfoque ERM con nuestro proceso de planificación estratégica?	115
131. ¿Deberíamos completar nuestro proceso de planificación estratégica antes de realizar nuestra primera evaluación de riesgos, o viceversa?	116
132. ¿Es posible fusionar con éxito las evaluaciones de riesgo que realizan las empresas como resultado de ERM, el cumplimiento de Sarbanes-Oxley, la planificación de la continuidad del negocio, la auditoría interna y diversas actividades de cumplimiento relacionadas con el lugar de trabajo, el medio ambiente y otras reglamentaciones?	116
133. ¿Cómo utiliza la administración ERM para establecer una ventaja competitiva sostenible?	116

### Construyendo un Caso de Negocios Convinciente

134. ¿Cómo construimos un caso de negocios convincente para ERM?	118
135. ¿Cómo seleccionamos las capacidades apropiadas para nuestra solución ERM?	119
136. ¿Cuáles son los factores clave de éxito o las medidas de éxito al evaluar la eficacia y el impacto de la implementación de ERM, es decir, cómo podemos saber si un enfoque de ERM ha tenido éxito?	121

### Hacer que suceda

137. ¿Qué es la gestión de viajes y por qué es relevante para la implementación de ERM?	123
138. ¿Qué es la gestión de programas y por qué es relevante para la implementación de ERM?	125
139. ¿Cómo podemos evaluar cuantitativa y cualitativamente los beneficios de implementar ERM en términos de mejorar el desempeño?	127
140. ¿Cómo se gestiona la implementación del ERM?	128
141. ¿Cómo sabemos cuándo hemos terminado?	128
142. Dado que tenemos tantas otras cosas en marcha, ¿cómo podemos asumir algo como la implementación de ERM?	128
143. ¿Qué estándares deben usar las empresas para evaluar su enfoque de ERM?	128
144. ¿Hay algún peligro que se deba evitar al implementar un enfoque de ERM?	128

### Relevancia para el cumplimiento de Sarbanes-Oxley

145. ¿La Ley Sarbanes-Oxley de 2002 (SOA) exige que las empresas adopten ERM? ¿Hay alguna otra ley y reglamentos que exigen ERM?	130
146. ¿Puede ERM ayudar a los oficiales certificadores con la descarga de su certificación SOA Sección 302? y responsabilidades de evaluación de la Sección 404?	130
147. ¿Cómo se relaciona ERM con el cumplimiento de SOA?	130
148. ¿Debe una decisión de implementar ERM considerar el esfuerzo para cumplir con SOA?	130
149. ¿Debería la administración ampliar el enfoque en el cumplimiento para administrar el riesgo comercial?	131
150. Como empresa pública, ¿por qué queríamos tomar ERM justo después de la Sección 404? ¿cumplimiento?	131
151. ¿Cómo se basa la autoevaluación en el cumplimiento de la Sección 404? ¿Por qué la autoevaluación contribuir a la evolución hacia ERM?	132

## Índice (continuación)

	Nº de página
152. ¿Qué significa integrar el cumplimiento de los artículos 404 y 302? ¿Cómo tal integración se basa en un proceso de autoevaluación establecido y en el cumplimiento de la Sección 404? ¿Por qué dicha integración contribuye a la evolución de una empresa hacia ERM?	134
153. ¿Cómo se basa el cumplimiento de otras leyes y reglamentos aplicables en el cumplimiento de las Secciones 404 y 302? ¿Por qué dicho cumplimiento contribuye a la evolución hacia ERM?	137
154. ¿Cómo se construye la eficacia y eficiencia operativa sobre las iniciativas de cumplimiento? Por que ¿Contribuyen la eficacia y la eficiencia operativas a la evolución hacia ERM?	137
<b>Otras preguntas</b>	
155. ¿La implementación de COSO Enterprise Risk Management – Marco Integrado evitará el fraude?	139
156. ¿Alguna de las empresas que han divulgado públicamente sus procesos de ERM ha recibido comentarios positivos de los analistas?	139
157. ¿Los analistas y otros dentro de la comunidad inversora o las agencias calificadoras expresaron su puntos de vista sobre cómo un enfoque de ERM que funcione de manera efectiva afectaría sus puntos de vista de una empresa?	139
158. ¿Toda la información sobre riesgos y gestión de riesgos puede clasificarse como información privilegiada entre abogado y cliente y, por lo tanto, no ser detectable?	139
159. Dado que se supone que toda esta información es detectable, ¿crea ERM más riesgo de litigio para las empresas?	140
160. ¿Existen casos judiciales en los que la administración de una empresa o su directorio hayan sido considerados deficientes por no contar con un adecuado sistema de gestión de riesgos?	140
161. ¿Existen riesgos asociados con la falta de un proceso de ERM y, de ser así, cuáles son?	140
162. ¿Es posible vincular un sistema ERM con el desempeño y la compensación de un empleado? ¿Alguna empresa está haciendo esto?	140
163. ¿Existe una certificación, calificación u otro mecanismo de evaluación de terceros para ERM?	140
164. ¿Cómo se relaciona ERM con el Acuerdo de Capital de Basilea que requiere que las instituciones financieras informen sobre el riesgo operativo?	141
165. ¿Cuál es la diferencia entre ERM y un estándar internacional como ISO?	141
166. ¿Cómo se integra COSO Enterprise Risk Management – Marco integrado con marcos como COBIT, ISO 17799, BITS, NIST Special Publication 800-53 e ITIL?	141
167. ¿Qué está pasando en otros países con respecto a la gestión de riesgos? Son estos desarrollos que impactan positivamente el desempeño de la compañía y el gobierno corporativo?	141
168. ¿Existe un formato para comunicar nuestro proceso de gestión de riesgos a nuestros clientes con el fin de alinearnos y cumplir con sus requisitos?	141
<b>Acerca de Protiviti Inc.</b>	142

## Introducción

En la desafiante economía global actual, las oportunidades comerciales y los riesgos cambian constantemente. Existe la necesidad de identificar, evaluar, administrar y monitorear las oportunidades y riesgos comerciales de la organización. La pregunta es: ¿Cómo toma una organización pasos prácticos para vincular oportunidades y riesgos al administrar el negocio? Y además: ¿Qué tiene que ver esto con la gestión de riesgos?

En agosto de 2004, el Comité de Organizaciones Patrocinadoras (COSO) de la Comisión Treadway emitió su Marco Integrado de Gestión de Riesgos Empresariales después de completar un proyecto de desarrollo que abarcó un período de tres años. El marco, que incluye un resumen ejecutivo y técnicas de aplicación, amplía el marco integrado de control interno emitido anteriormente para proporcionar un enfoque más sólido y extenso en la gestión de riesgos empresariales (ERM). Como se explica en el prólogo del marco: "Si bien [el marco] no pretende reemplazar el marco de control interno y no lo reemplaza, sino que incorpora el marco de control interno dentro de él, las empresas pueden decidir buscar este marco de gestión de riesgos corporativos tanto para satisfacer sus necesidades de control interno y avanzar hacia un proceso de gestión de riesgos más completo".

En Protiviti, creemos que la implementación de ERM debe integrarse con el establecimiento de estrategias. ERM redefine la propuesta de valor de la gestión de riesgos elevando su enfoque de lo táctico a lo estratégico. ERM se trata de diseñar e implementar capacidades para administrar los riesgos que importan. Cuanto mayores sean las brechas en el estado actual y el estado futuro deseado de las capacidades de gestión de riesgos de la organización, mayor será la necesidad de una infraestructura ERM para facilitar el avance de las capacidades de gestión de riesgos a lo largo del tiempo.

El nuevo marco de COSO proporciona criterios contra los cuales las empresas pueden comparar sus prácticas y procesos de gestión de riesgos. El marco proporciona un lenguaje común que fomenta la comunicación entre ejecutivos, directores, auditores y asesores, y alentamos a todas las personas interesadas en implementar ERM a leerlo y comprenderlo.

Muchos están haciendo preguntas sobre la propuesta de valor de ERM y los pasos prácticos sobre cómo implementarlo. Si bien no tenemos todas las respuestas, intentamos abordar en esta publicación algunas de las preguntas más frecuentes con respecto a ERM. Esta publicación está diseñada para responder a sus preguntas sin tener que leer material con el que ya está familiarizado. A menudo se refiere al marco COSO, que los lectores pueden obtener en [www.coso.org](http://www.coso.org). Ofrece ideas, sugerencias y puntos de vista a los ejecutivos responsables de la implementación de ERM. Está diseñado para usarse como una herramienta de referencia y no como un libro para leer de cabo a rabo. Se complementa con el Número 6 del Volumen 2 de The Bulletin, "Gestión de riesgos empresariales: Consejos prácticos de implementación", que brinda una descripción general para ejecutivos y directores de nivel C y está disponible en [www.protiviti.com](http://www.protiviti.com).

---

A medida que las empresas adquieran más experiencia en la implementación de ERM, esperamos actualizar esta publicación de vez en cuando. Si lo hacemos, publicaremos información en [www.protiviti.com](http://www.protiviti.com). Protiviti publica periódicamente perfiles de ejecutores de ERM en KnowledgeLeaderSM para proporcionar ejemplos de casos de ERM y planea publicar un libro que incluya dichos perfiles de vez en cuando.

Esta publicación no pretende ser un análisis legal ni un "libro de recetas" detallado de los pasos a seguir en cada situación. En consecuencia, las empresas deben buscar asesores apropiados para obtener asesoramiento sobre cuestiones específicas a medida que evalúan sus circunstancias únicas.

protiviti inc.

enero de 2006



## LOS FUNDAMENTOS

### 1. ¿Qué es la gestión de riesgos empresariales (ERM)?

COSO define ERM como "un proceso, realizado por la junta directiva, la gerencia y otro personal de una entidad, aplicado en el establecimiento de estrategias y en toda la empresa, diseñado para identificar eventos potenciales que pueden afectar a la entidad y administrar el riesgo para estar dentro de su riesgo. apetito, para proporcionar una seguridad razonable con respecto al logro de los objetivos de la entidad". Esta definición es amplia por una razón. Refleja ciertos conceptos fundamentales, cada uno de los cuales se analiza en las páginas 5 a 9 del marco COSO ERM. Como se resume en la página 5 del marco, "la gestión del riesgo empresarial es:

- Un proceso, en curso y que fluye a través de una entidad
- Realizado por personas en todos los niveles de una organización
- Aplicado en el establecimiento de estrategias
- Se aplica en toda la empresa, en todos los niveles y unidades, e incluye tomar una cartera a nivel de entidad vista del riesgo
- Diseñado para identificar eventos potenciales que afecten a la entidad y gestionar el riesgo dentro de su apetito por el riesgo
- Capaz de proporcionar una seguridad razonable a la administración y al directorio de una entidad
- Orientado al logro de objetivos en una o más categorías separadas pero superpuestas: es "un medio para un fin, no un fin en sí mismo".

ERM se trata de establecer la supervisión, el control y la disciplina para impulsar la mejora continua de las capacidades de gestión de riesgos de una entidad en un entorno operativo cambiante. Avanza la madurez de las capacidades de la empresa en torno a la gestión de sus riesgos prioritarios. Antes de que una empresa pueda afirmar que está aplicando ERM, debe abordar TODOS los conceptos anteriores incorporados en la definición de COSO.

### 2. ¿Por qué implementar ERM?

Usando la definición de ERM articulada en la Pregunta 1, el objetivo primordial para implementar ERM es proporcionar una seguridad razonable a la gerencia y al directorio de una entidad de que se lograron los objetivos comerciales de la entidad. En las páginas 1 a 4 del marco, COSO establece que ERM ayuda a la gerencia a alinear el apetito por el riesgo y la estrategia, mejorar las decisiones de respuesta al riesgo, reducir las sorpresas y pérdidas operativas, identificar y administrar los riesgos entre empresas, brindar respuestas integradas a múltiples riesgos, aprovechar oportunidades y mejorar el despliegue de capital. Estamos de acuerdo con el punto de vista de COSO y lo discutiremos más en esta publicación.

Creemos que hay seis razones fundamentales para implementar ERM. Cada uno sirve para ayudar a elevar la gestión de riesgos a un nivel estratégico. Las seis razones son:

- (1) Reducir la variabilidad inaceptable del desempeño: ERM ayuda a la gerencia a (a) evaluar la probabilidad y el impacto de eventos importantes y (b) desarrollar respuestas para evitar que ocurran esos eventos o gestionar su impacto en la entidad si ocurren. La mayoría de las empresas se centran en los riesgos tradicionales que se conocen desde hace algún tiempo. Pocas empresas tienen un proceso sistemático para anticipar riesgos nuevos y emergentes. Por lo tanto, muchas empresas a menudo se enteran de los riesgos críticos demasiado tarde o por accidente, lo que genera la "extinción de incendios" y la gestión de crisis que agota los recursos y crea nuevas vulnerabilidades. La lente estratégica de ERM amplía el enfoque tradicional de la gestión de riesgos en los riesgos catastróficos y de baja probabilidad a una visión más amplia de la reducción del riesgo de erosión de fuentes críticas de valor empresarial. ERM ayuda a la gerencia a mejorar la consistencia del desempeño operativo al aumentar el énfasis en reducir la volatilidad de las ganancias, evitar sorpresas relacionadas con las ganancias y administrar las deficiencias de los indicadores clave de rendimiento (KPI). ERM mejora la gestión de los crecientes costos de mitigación de riesgos y la tasa de éxito en el logro de los objetivos comerciales.

(2) Alinear e integrar diferentes puntos de vista de la gestión de riesgos: hay muchos silos dentro de las organizaciones con un punto de vista sobre la gestión del riesgo, por ejemplo, tesorería, riesgo asegurable, EH&S, TI y dentro de las unidades de negocio. La mentalidad de silo inhibe la asignación eficiente de recursos y la gestión de riesgos comunes en toda la empresa. Cuando hay múltiples funciones que gestionan múltiples riesgos, existe la necesidad de un marco común.

Por ejemplo, algunas organizaciones son:

- Evaluar la necesidad de un director de riesgos (CRO), incluida la función, autoridad y Líneas de reporte
- Integración de la gestión de riesgos en actividades críticas de gestión, por ejemplo, establecimiento de estrategias, planificación, gastos de capital y due diligence de M&A y procesos de integración
- Vincular la gestión de riesgos a decisiones más eficientes de asignación de capital y transferencia de riesgos
- Aumentar la transparencia mediante el desarrollo de medidas cuantitativas y cualitativas de riesgos y riesgos. rendimiento de la gestión
- Agregar exposiciones de riesgo comunes a través de múltiples unidades de negocio con el objetivo de comprender las mayores amenazas al valor de la empresa y formular una respuesta integrada al riesgo

(3) Fomentar la confianza de la comunidad inversora y las partes interesadas: a medida que los inversores institucionales, las agencias calificadoras y los reguladores hablan más sobre la importancia de la gestión de riesgos en sus evaluaciones de las empresas, se puede solicitar a la gerencia que divulgue y comente sobre las capacidades de la organización para comprender y gestionar el riesgo. Permitir a las partes interesadas realizar evaluaciones informales sobre si los rendimientos son adecuados en relación con los riesgos asumidos. A medida que las empresas aumenten la transparencia de sus riesgos y sus capacidades de gestión de riesgos, y mejoren la madurez de sus capacidades en torno a la gestión de riesgos críticos, la dirección podrá articular con mayor eficacia qué tan bien están manejando los problemas existentes y emergentes de la industria.

(4) Mejorar el gobierno corporativo: ERM y el gobierno corporativo están inextricablemente vinculados. Cada uno aumenta al otro. ERM fortalece la supervisión de la junta, fuerza una evaluación de las estructuras de supervisión existentes a nivel de la alta dirección, aclara las funciones y responsabilidades de la gestión de riesgos, establece las autoridades y los límites de la gestión de riesgos y comunica de manera efectiva las respuestas a los riesgos en apoyo de los objetivos comerciales clave. Todas estas actividades están relacionadas con la buena gobernanza. Del mismo modo, el gobierno corporativo efectivo marca la pauta para (a) comprender los riesgos y las capacidades de gestión de riesgos y (b) alinear el apetito por el riesgo con el comportamiento de búsqueda de oportunidades de la entidad. Los directores a menudo preguntan: "¿Cuáles son los riesgos, cómo se gestionan y cómo se sabe?"

(5) Responder con éxito a un entorno empresarial cambiante: a medida que el entorno empresarial continúa cambiando y el ritmo del cambio se acelera, las organizaciones deben mejorar en la identificación, priorización y planificación del riesgo. ERM ayuda a la gerencia a evaluar los supuestos subyacentes al modelo comercial existente, la efectividad de las estrategias en torno a la ejecución de ese modelo y la información disponible para la toma de decisiones. ERM impulsa a la gerencia a identificar escenarios futuros alternativos, evaluar la probabilidad y la gravedad de esos escenarios, identificar riesgos prioritarios y mejorar las capacidades de la organización en torno a la gestión de esos riesgos. A medida que cambia el entorno, surgen nuevos riesgos y se escalan de manera oportuna para la acción y posible divulgación. Estas actividades afectan la asignación de recursos para la organización en su conjunto.

(6) Alinear la estrategia y la cultura corporativa: ERM ayuda a la gerencia a crear conciencia sobre el riesgo y una cultura abierta y positiva con respecto al riesgo y la gestión del riesgo. En tal entorno, las personas pueden plantear problemas sin temor a represalias. Con respecto a asuntos de importancia para toda la empresa, ERM a menudo centraliza el establecimiento de políticas y crea enfoque, disciplina y control. Aclara la distinción entre comportamientos de asunción de riesgos y evitación de riesgos, mejora las herramientas para cuantificar las exposiciones al riesgo, aumenta la responsabilidad por la gestión de riesgos en toda la empresa y facilita la identificación oportuna de cambios en el perfil de riesgo de una entidad. ERM fomenta el equilibrio tanto en las actividades empresariales como en las actividades de control de la organización, de modo que ninguno sea desproporcionadamente fuerte en relación con el otro.

### 3. ¿Cómo se compara el alcance de ERM con los enfoques de gestión de riesgos existentes?

Los enfoques tradicionales de gestión de riesgos se centran en proteger los activos tangibles informados en el balance de una empresa y los derechos y obligaciones contractuales relacionados. El énfasis de ERM, sin embargo, está en mejorar la estrategia comercial. El alcance y la aplicación de ERM son mucho más amplios que la protección de activos físicos y financieros. Con un enfoque de ERM, el alcance de la gestión de riesgos abarca toda la empresa y la aplicación de la gestión de riesgos tiene como objetivo mejorar y proteger la combinación única de activos tangibles e intangibles que componen el modelo de negocios de la organización. Este punto de vista es consistente con la afirmación de COSO de que ERM se aplica tanto en la empresa como en el establecimiento de estrategias.

Dado que las capitalizaciones de mercado a menudo superan significativamente los valores históricos del balance, la aplicación de la gestión de riesgos a los activos intangibles es de vital importancia. Así como los posibles eventos futuros pueden afectar el valor de los activos físicos y financieros tangibles, también pueden afectar el valor de los activos intangibles clave, por ejemplo, los activos de los clientes, los activos de los empleados/proveedores y los activos de la organización, como las marcas distintivas de la entidad, que diferencian estrategias, procesos innovadores y sistemas propietarios. Esta es la esencia de lo que ERM aporta a la organización: la elevación de la gestión de riesgos a un nivel estratégico al ampliar su aplicación a TODAS las fuentes de valor, no solo las físicas y financieras.

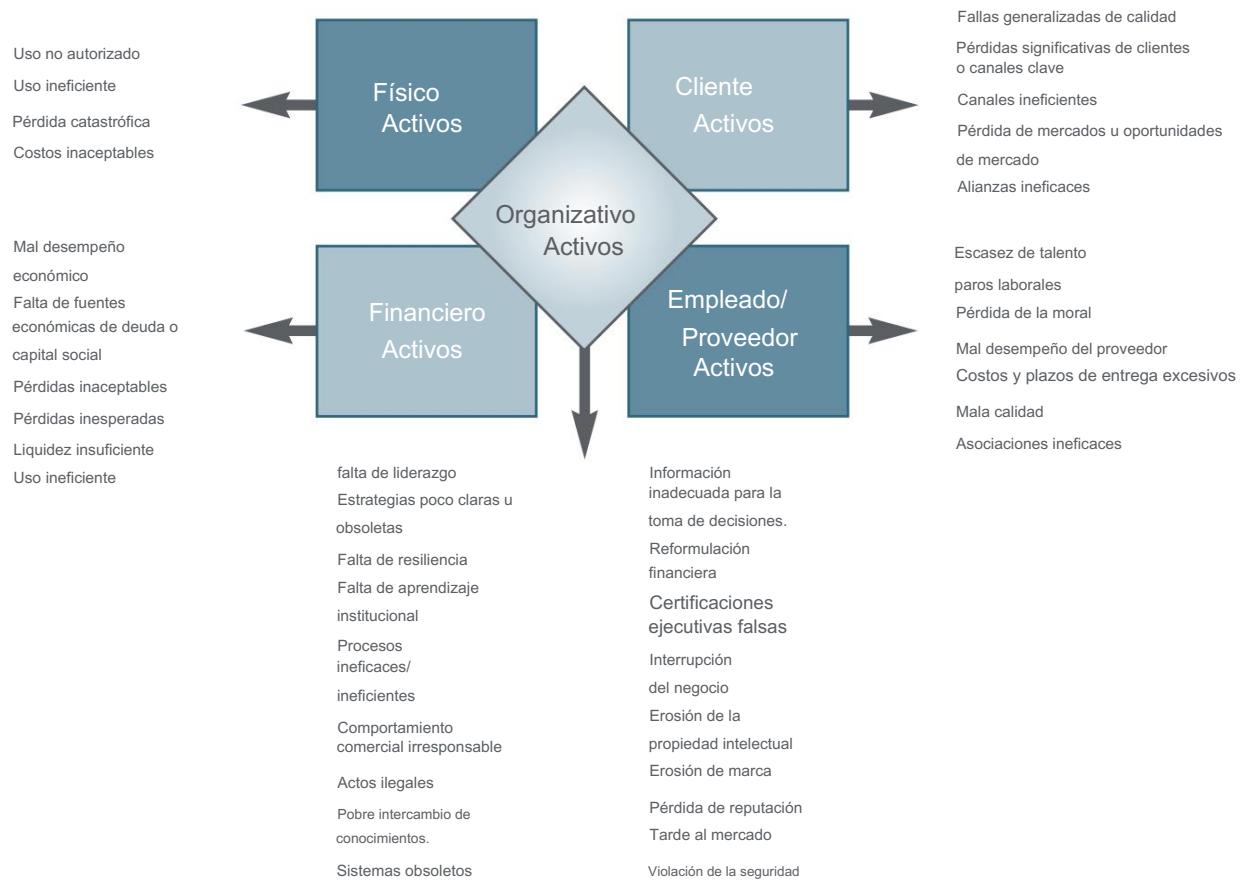
Las cinco categorías amplias de activos que representan fuentes de valor y los ejemplos dentro de cada categoría se ilustran a continuación<sup>1</sup>:



Estas cinco categorías de activos incluyen fuentes de valor subyacentes a la estrategia comercial de una organización. Al poner el énfasis en el establecimiento de estrategias, ERM hace que la gestión de riesgos pase de ser una disciplina de evitar y cubrir apuestas a una habilidad diferenciadora para mejorar y proteger el valor de la empresa, ya que la gerencia busca hacer las mejores apuestas en la búsqueda de nuevas oportunidades de crecimiento y rentabilidad. ERM fortalece el comportamiento de búsqueda de oportunidades al ayudar a los gerentes a tener confianza en su comprensión de los riesgos y en las capacidades disponibles dentro de la organización para administrar esos riesgos.

1. Descifrando el código de valor: vea lo que importa, invierta en lo que importa y administre lo que importa en la nueva economía, Richard ES Boulton, Barry D. Libert y Steve M. Samek, HarperCollins, 2000.

El proceso de evaluación de riesgos puede conducir a respuestas de riesgo más integrales cuando la administración identifica posibles eventos futuros que podrían afectar cada categoría de activos críticos para la ejecución del modelo comercial de la empresa. El siguiente esquema ilustra las categorías de posibles eventos futuros que podrían considerarse durante una evaluación de riesgos:



Las fuentes de valor de una empresa, ya sean tangibles o intangibles, son inherentes a su modelo de negocio. Se ven afectados por fuentes de incertidumbre que deben entenderse y gestionarse a medida que una organización trabaja para lograr sus objetivos de desempeño. Pueden ser externos o internos. Por ejemplo, los riesgos ambientales son incertidumbres que surgen en el entorno externo y que afectan la viabilidad del modelo de negocios de la empresa.

Los riesgos de proceso son incertidumbres que afectan la ejecución del modelo comercial y, por lo tanto, a menudo surgen internamente dentro de los procesos comerciales de la organización. Debido a que el conocimiento y la información inadecuados generan más incertidumbre, los riesgos de la información para la toma de decisiones son incertidumbres que afectan la relevancia y confiabilidad de la información que respalda las decisiones de la administración para proteger y mejorar el valor de la empresa. Estas tres amplias categorías (entorno, proceso e información para la toma de decisiones) brindan la base para comprender las fuentes de incertidumbre en cualquier negocio. Como ilustra la Pregunta 75, estas categorías de riesgo incluyen muchas subcategorías de posibles eventos futuros que podrían convertirse en el punto central para evaluar el riesgo y formular respuestas adecuadas al riesgo.

En resumen, la incertidumbre sobre el futuro crea riesgo y ERM amplía el enfoque de la gestión de riesgos a todas las fuentes importantes de valor empresarial. Al comprender las variables externas e internas clave que contribuyen a la incertidumbre en un negocio y monitorear las tendencias en esas variables a lo largo del tiempo, la gerencia puede administrar el negocio de manera más efectiva y aprovechar el potencial del modelo comercial de la empresa. La siguiente tabla proporciona ejemplos de eventos observables para ilustrar este punto.

ESTABLECER CATEGORÍA	EJEMPLO DE EXPOSICIONES	ALGUNAS VARIABLES ILUSTRATIVAS O EVALUAR LA INCERTIDUMBRE
Físico	instalaciones físicas	una probabilidad de moneda de la strophie de: Máxima pérdida posible Pérdida máxima previsible Pérdida normal
	rendimiento de producción	la probabilidad de ocurrencia de efectos cambia en el backlog
financiero	et activos monetarios et s	cambio en el interés xchang y la tasa de inflación cambio en el interés
	Flujo de efectivo del plan de	xchang y las tasas de inflación ustomer default roability cuelga en
	negocios Cuentas por cobrar totales	el petróleo, metales, energía y otros
	ommodity holdings quity	precios cuelga en el precio de las existencias
	holdings	
Cliente	base de clientes	cambio en la calidad del servicio inde
	flujos de eventos	Cambio en el precio de la competencia Rentabilidad Probabilidad de ocurrencia
empleado/proveedor	grupo de empleados	Cambio en el cambio Índice de preparación Salud y seguridad Incidente Moneda Probabilidad
	proveedor estratégico m	cambio en el rendimiento justo a tiempo cambio en las calificaciones de calidad cambio en los precios de las materias primas
Organización	imagen aleatoria	dificultad para vivir corrió romise
	Estrategia diferenciadora	cambio en la calidad y el desempeño de los costos en relación con el competidor cambio en las expectativas y los deseos de los clientes
	procesos innovadores	Nuevas innovaciones tecnológicas que dejan obsoletas las capacidades de proceso existentes

Para cualquiera de las variables clave mencionadas anteriormente que son relevantes para un negocio, existen posibles eventos futuros que brindan el contexto para evaluar y administrar el riesgo. Un principio subyacente en el establecimiento de estrategias ilustra aún más este contexto: cuanto mayor sea la dispersión de posibles eventos o resultados futuros, mayor será el nivel de exposición de la organización a rendimientos inciertos. La sensibilidad de una organización al riesgo es una función de (1) la importancia de sus exposiciones a cambios y eventos futuros, (2) la probabilidad de que ocurran esos cambios y eventos futuros y (3) su capacidad para gestionar las implicaciones comerciales si cualquier combinación de esos posibles cambios y eventos futuros ocurren. La infraestructura ERM de la organización facilita el avance de las capacidades de gestión de riesgos para proporcionar un mejor conocimiento e información sobre las variables (o riesgos) clave de la empresa y sus capacidades en torno a la gestión de los efectos de los cambios en esas variables (o riesgos).

#### 4. ¿Cuál es la propuesta de valor para implementar ERM?

Los directores y directores ejecutivos enfrentan muchos desafíos. Deben enfocar sus organizaciones para capitalizar las oportunidades emergentes. Deben invertir continuamente recursos escasos en la búsqueda de actividades comerciales prometedoras, aunque inciertas. Deben administrar el negocio frente a circunstancias en constante cambio. Y mientras hacen todas estas cosas, al mismo tiempo deben estar en condiciones de brindar seguridad a los inversionistas, directores y otras partes interesadas de que sus organizaciones saben cómo proteger y mejorar el valor empresarial.

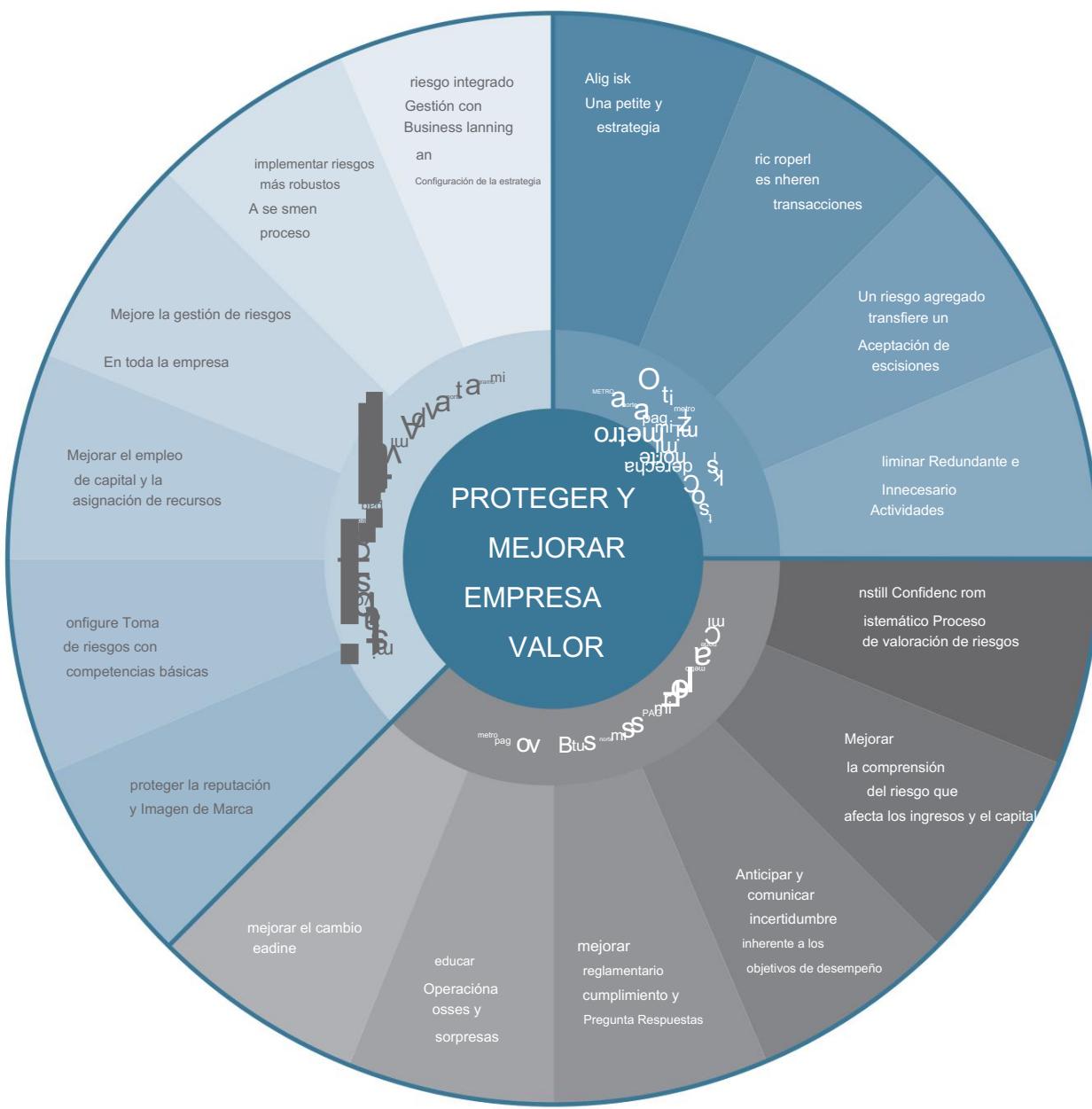
En medio de perfiles de riesgo en constante cambio, los directores y directores ejecutivos necesitan un mayor nivel de desempeño de todas las disciplinas dentro de la organización, incluida la gestión de riesgos.

ERM ayudará a los directores y directores ejecutivos a enfrentar estos desafíos al establecer la supervisión, el control y la disciplina para impulsar la mejora continua de las capacidades de gestión de riesgos de una entidad en un entorno cambiante.

entorno operativo. ERM redefine la propuesta de valor de la gestión de riesgos al proporcionar una organización con los procesos y herramientas que necesita para ser más anticipatoria y eficaz en la evaluación, aceptando y gestionando las incertidumbres que enfrenta a medida que crea valor sostenible para las partes interesadas. Poniendo Mejorar continuamente las capacidades de gestión de riesgos que realmente importan para la ejecución exitosa de la modelo de negocio, ERM eleva la gestión de riesgos a un nivel estratégico.

A medida que se implementa ERM para avanzar en la madurez de las capacidades de la organización para administrar los riesgos prioritarios, ayuda a la gerencia a mejorar y proteger con éxito el valor de la empresa de tres maneras. Primero, ERM se enfoca en establecer una ventaja competitiva sostenible. En segundo lugar, optimiza el costo de administrar el riesgo. Y tercero, ayuda a la gerencia a mejorar el desempeño del negocio. Estas contribuciones redefinen el valor propuesta de gestión de riesgos para una empresa.

El siguiente esquema ilustra la propuesta de valor de ERM:



Los puntos ilustrativos anteriores se discuten a lo largo de este libro.

Estas contribuciones de valor agregado de ERM conducen a posiblemente el mayor beneficio único que brinda la gestión de riesgos para el éxito de un negocio: infundir una mayor confianza en la junta directiva, el director ejecutivo y la gerencia ejecutiva. Estas partes interesadas deben saber que los riesgos y las oportunidades se identifican sistemáticamente, se analizan rigurosamente y se administran de manera rentable en toda la empresa, de manera consistente con el apetito por el riesgo y el modelo comercial de la empresa para crear valor. Bajo ERM, los ejecutivos conocen mejor los riesgos inherentes a sus operaciones. Entienden el proceso mediante el cual se identifican los riesgos, asignan la propiedad del riesgo de manera oportuna y aseguran que las respuestas al riesgo se formulen oportunamente y se controlen de manera efectiva. También aportan técnicas sistemáticas de evaluación de riesgos a nuevas empresas que asumen riesgos. Insisten en que los planes de negocios incorporen un enfoque de riesgo, para que sean más sustantivos y robustos. En resumen, en un entorno de ERM, los supuestos que subyacen al modelo de negocios se cuestionan periódicamente y, si es necesario, se refinan en un ciclo dinámico de mejora y cambio continuos.

Es vital entender que la articulación anterior es genérica. Debido a que una propuesta de valor genérica no es suficiente para impulsar las decisiones de la alta gerencia para invertir en infraestructura ERM, debe complementarse con una articulación más granular que sea posible gracias a una evaluación de riesgos empresariales y un análisis de brechas en torno a las capacidades existentes de la entidad para administrar sus riesgos prioritarios. Como explicamos en nuestra respuesta a la Pregunta 85, cuanto mayor sea la brecha entre el estado actual y el estado futuro deseado de las capacidades de gestión de riesgos de la organización, mayor será la necesidad de una infraestructura ERM para facilitar el avance de esas capacidades a lo largo del tiempo. Esta comprensión mejora la especificidad de la propuesta de valor de ERM, haciéndola más convincente.

En resumen, una infraestructura ERM que funcione de manera efectiva puede convertirse en uno de los diferenciadores fundamentales entre los meros sobrevivientes y los pioneros de la industria. Más allá de brindar los beneficios anteriores, la redefinición de la propuesta de valor de la gestión de riesgos se sumará a la historia del CEO con las partes interesadas en el entorno exigente de hoy. Una infraestructura de ERM estimula y refuerza los comportamientos deseados dentro de la organización en consonancia con sus objetivos comerciales, estrategias y metas de desempeño. Un enfoque de ERM diferencia el modelo comercial de la empresa y ayuda a construir su imagen y reputación con los clientes, proveedores, empleados y los mercados de capital, todos los cuales son claves para sostener un negocio exitoso.

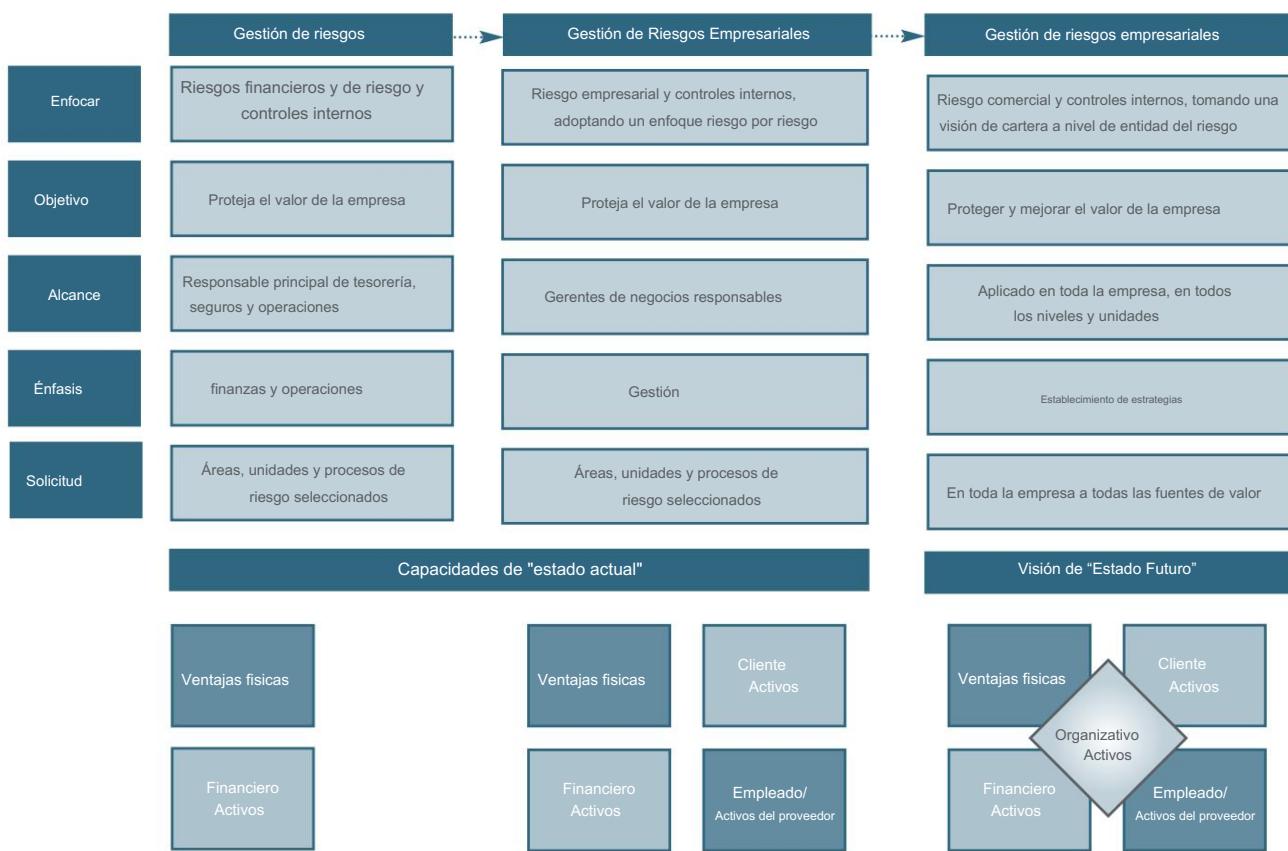
##### 5. ¿Qué empresas están implementando ERM?

Pocas empresas, si es que hay alguna, pueden afirmar que han implementado ERM por completo, tal como lo define COSO. Para la mayoría de las empresas, el abismo entre el modelo tradicional de gestión de riesgos y ERM, como se analiza en la pregunta 6, es simplemente demasiado abrumador para abordarlo. Por ejemplo, la definición de COSO (consulte la Pregunta 1) establece que ERM se "aplica... en toda la empresa". Un enfoque integral de toda la empresa en la gestión del riesgo es un alto estándar de implementación para la mayoría de las empresas debido a los cambios de comportamiento necesarios para superar la gestión convencional del riesgo en silos, que las empresas han tenido durante mucho tiempo. Por esa razón, en los últimos años, ERM ha sido perseguido más por organizaciones visionarias que por la corriente principal de las empresas.

ERM es un enfoque "mejor de su clase" que consta de diferentes técnicas que diferentes empresas han implementado de diferentes maneras. Las instituciones de servicios financieros probablemente estén más avanzadas en función de las capacidades que han implementado para administrar los riesgos crediticios y de mercado en toda la empresa. Sin embargo, incluso esas instituciones tienen mucho camino por recorrer para abordar el riesgo operativo en toda la empresa.

## 6. Si las empresas no están implementando ERM, ¿qué están haciendo?

La mayoría de las empresas están aplicando el modelo tradicional de gestión de riesgos en sus negocios, lo que convierte a ERM en un "estado de objetivo futuro", como lo ilustra el siguiente esquema:



La evolución del modelo tradicional de gestión de riesgos a ERM mencionado anteriormente no es fácil. Bajo los enfoques tradicionales de gestión de riesgos, el proceso está fragmentado, el riesgo se considera negativo (algo que debe evitarse), se acepta un comportamiento reactivo y ad hoc, y la actividad de gestión de riesgos está orientada a transacciones (o basada en costos), enfocada estrechamente y funcionalmente. -impulsado. Bajo ERM, tal como lo define COSO, el proceso está integrado, el riesgo también se considera positivo (reconociendo que las empresas exitosas deben asumir riesgos cuando aprovechan las oportunidades), se espera un comportamiento proactivo y la actividad de gestión de riesgos es estratégica (o de valor). basada), ampliamente enfocada e impulsada por procesos.

El modelo tradicional de gestión de riesgos se centra en gestionar las incertidumbres en torno a los activos físicos y financieros. ERM se centra en toda la cartera de activos de la empresa, incluidos sus activos intangibles, como los activos de los clientes, los activos de los empleados y los proveedores, y los activos organizacionales, como las estrategias diferenciadoras, las marcas distintivas, los procesos innovadores y los sistemas patentados. Muy pocas empresas han implementado un enfoque verdaderamente empresarial en todos los aspectos del negocio. Las empresas en las primeras etapas de desarrollo de su infraestructura ERM a menudo sientan las bases con un lenguaje común, una estructura de supervisión de gestión de riesgos y un proceso de evaluación de riesgos en toda la empresa. Algunas empresas han evolucionado hacia etapas más avanzadas, como las instituciones de la industria de servicios financieros que gestionan los riesgos crediticios y de mercado.

Algunas empresas aplican ERM en unidades específicas, como en la gestión del riesgo de precio de las materias primas de una unidad comercial a nivel de toda la empresa.

#### 7. ¿Quién es responsable de ERM?

Debido a que el énfasis está en el establecimiento de la estrategia, la propiedad comienza en la parte superior de la organización con la dirección ejecutiva y cae en cascada hacia abajo en la organización hasta los gerentes funcionales y de unidad. Las preguntas 39 a 45 analizan el papel de la dirección ejecutiva. La junta directiva proporciona supervisión (el papel de los directores se analiza en las Preguntas 46 a 49). Además, está el director de riesgos (o ejecutivo equivalente), cuya función se analiza en las Preguntas 50 a 52. También puede haber uno o más comités de gestión de riesgos, según la naturaleza y complejidad de los riesgos y la necesidad de cruce, coordinación funcional y entre unidades. Las preguntas 53 a 57 explican las funciones respectivas de estos ejecutivos en el contexto de la estructura de supervisión de la gestión de riesgos.

#### 8. ¿Cuáles son los pasos que las empresas pueden tomar de inmediato para implementar ERM?

Hay pasos que cualquier organización puede tomar a partir de mañana por la mañana. Los ilustraremos en este libro. Por ejemplo, las organizaciones pueden:

- Adoptar un lenguaje de riesgo común. Consulte la pregunta 75.
- Llevar a cabo una evaluación de riesgos empresariales para identificar y priorizar los riesgos críticos de la organización. Consulte las preguntas 69 a 84.
- Realizar un análisis de brechas de las capacidades actuales y deseadas en torno a la gestión de riesgos críticos. Consulte las preguntas 110 y 111.
- Articular la visión, las metas y los objetivos de la gestión de riesgos (consulte las Preguntas 64 y 65), junto con una propuesta de valor convincente (consulte las Preguntas 4 y 134 a 136) para proporcionar la justificación económica para seguir adelante.
- Avanzar en la capacidad de gestión de riesgos de la organización para uno o dos riesgos críticos, es decir, comenzar con un área de riesgo donde la alta dirección sabe que se necesitan mejoras para ejecutar con éxito la estrategia empresarial.

Si bien existen otros pasos posibles, los anteriores son un excelente comienzo y brindan una vista simplificada para comenzar con la implementación de ERM. También es importante hacer un inventario de lo que ya se ha hecho y lograr éxitos tempranos visibles. La clave es mantener el esfuerzo simple y enfocado mediante la integración de las actividades relacionadas con ERM en la estrategia y el plan de negocios.

#### 9. ¿Es ERM aplicable a organizaciones más pequeñas y menos complejas?

Todas las organizaciones enfrentan riesgos comerciales, independientemente de su tamaño. Las organizaciones ignoran el riesgo bajo su propio riesgo. Ninguna organización puede darse el lujo de mantenerse firme con sus capacidades de gestión de riesgos existentes; por lo tanto, cada organización debe evaluar cómo puede mejorar su gestión de riesgos. El marco COSO es útil para este propósito porque le da a cada organización un marco con criterios contra los cuales comparar sus capacidades de gestión de riesgos existentes. COSO señala en la página 13 de su marco publicado:

Si bien algunas entidades pequeñas y medianas pueden implementar componentes de ERM de manera diferente a las grandes, aún pueden tener una gestión de riesgos empresarial efectiva. Es probable que la metodología... sea menos formal y menos estructurada en las entidades más pequeñas que en las más grandes, pero los conceptos básicos deben estar presentes en todas las entidades.

#### 10. ¿Por qué las empresas que han intentado implementar ERM han fracasado en sus esfuerzos?

Pocas empresas han implementado ERM, como lo define COSO. Por ejemplo, la definición de COSO deja en claro que la aplicación de ERM debe ser "en toda la empresa, en cada nivel y unidad, e incluye tomar una visión de riesgo de cartera a nivel de entidad". A menos que la implementación de ERM se aplique de manera uniforme en toda la empresa

y es un enfoque holístico e integral en todos los riesgos clave del negocio, no es realmente para toda la empresa. Además, a menos que la implementación de ERM esté estrechamente vinculada a la evaluación y formulación de la estrategia comercial, no cumple con los requisitos de COSO. Si bien algunas empresas han comenzado su viaje para implementar ERM, pocas lo han completado.

#### 11. ¿La implementación de ERM asegura el éxito de un negocio?

ERM no garantiza el éxito de un negocio. Brinda mejor información a los gerentes y un proceso más sólido para que lo implementen, pero no necesariamente transforma a un mal gerente en un buen gerente.

COSO señala que “las limitaciones resultan de la realidad de que el juicio humano en la toma de decisiones puede ser defectuoso, las decisiones sobre cómo responder al riesgo y establecer controles deben considerar los costos y beneficios relativos, las fallas pueden ocurrir debido a fallas humanas, como errores simples o errores, los controles se pueden eludir debido a fallas humanas, como errores simples o equivocaciones, los controles se pueden eludir mediante la colusión de dos o más personas, y la administración tiene la capacidad de anular las decisiones de gestión de riesgos empresariales”. La definición de COSO también se refiere a “seguridad razonable”. Según COSO, “la seguridad razonable refleja la noción de que la incertidumbre y el riesgo se relacionan con el futuro, que nadie puede predecir con precisión”. Además, COSO establece en la página 8 del marco:

La seguridad razonable no implica que la gestión de riesgos corporativos falle con frecuencia. ... El efecto acumulativo de las respuestas al riesgo que satisfacen múltiples objetivos y la naturaleza multipropósito de los controles internos reducen el riesgo de que una entidad no logre sus objetivos. ... Sin embargo, puede ocurrir un evento incontrolable, un error o un incidente de informe inadecuado. En otras palabras, incluso la gestión eficaz del riesgo empresarial puede fracasar. La seguridad razonable no es una seguridad absoluta.

#### 12. ¿Cuál es la diferencia entre ERM y gestión?

ERM es una parte integral de la gestión de una organización, pero no impulsa todo lo que hace la gestión.

COSO establece que “[m]uchos juicios aplicados en la toma de decisiones de la gerencia y las acciones gerenciales relacionadas, aunque forman parte del proceso de gestión, no son parte de la gestión de riesgos empresariales”. COSO proporciona varios ejemplos en la página 14 del marco. Por ejemplo, las elecciones de la gerencia en cuanto a los objetivos comerciales relevantes, las respuestas específicas al riesgo y la asignación de los recursos de la entidad son decisiones de la gerencia y no forman parte de ERM. Dicho esto, la gestión de riesgos no es una ocurrencia tardía ni un apéndice de las actividades de gestión existentes del negocio principal. En un entorno ERM, la gestión de riesgos se integra eficazmente con el establecimiento de estrategias, la planificación empresarial, la medición del rendimiento y otras disciplinas empresariales.

#### 13. ¿Qué significa “implementar ERM”?

Creemos que la implementación de ERM debe enfatizar el establecimiento de estrategias. Como explicamos en nuestra respuesta a la Pregunta 85, la aplicación depende de los riesgos prioritarios de cada organización (definidos en el contexto de su estrategia comercial) y las brechas en torno a la gestión de esos riesgos. ERM no es una solución de “talla única” en un estante. La gerencia debe decidir la naturaleza de la solución ERM en función del tamaño, los objetivos, la estrategia, la estructura, la cultura, el estilo de gestión, el perfil de riesgo, la industria, el entorno competitivo y los medios financieros de la organización. Según COSO, estos y otros factores afectan la forma en que se aplica el marco ERM.

La implementación de ERM requiere que la gerencia tome los siguientes pasos:

- (a) Identificar y comprender los riesgos prioritarios de la organización para proporcionar un contexto.
- (b) Utilizar el marco COSO para definir el estado actual de las capacidades de gestión de riesgos de la organización.
- (c) Usar el marco COSO para definir el estado futuro deseado de la gestión de riesgos de la organización capacidades.
- (d) Analizar y articular el tamaño de la brecha entre (b) y (c) y la naturaleza de las mejoras necesaria para cerrar la brecha, que es una función de (i) las capacidades y experiencia existentes de la organización y (ii) el deseo de la gerencia de mejorar y superarse.

(e) Con base en el análisis en (d), desarrolle un caso de negocios para abordar la brecha para proporcionar la justificación económica del esfuerzo general para implementar las mejoras de infraestructura de ERM.

(f) Organizar un plan que promueva las capacidades de infraestructura ERM deseadas y aborde los problemas de cambio relacionados con la ejecución del plan.

(g) Proporcionar la supervisión y la facilitación necesarias para asegurar la integración y coordinación efectivas de la esfuerzo general.

Consulte nuestra respuesta a la Pregunta 85 para obtener más consejos sobre cómo comenzar.

COSO afirma que ERM es “un medio para un fin, no un fin en sí mismo”. La tendencia hacia ERM reconoce que los riesgos son complejos y están interrelacionados, y que el entorno empresarial no se está volviendo más simple. Por lo tanto, existen beneficios significativos que se pueden lograr al evaluar y administrar el riesgo de manera integral en toda la empresa. El proceso de implementación de ERM es fundamentalmente un proceso de educación, creación de conciencia, desarrollo de aceptación y, en última instancia, asignación de responsabilidad y aceptación de la propiedad. Debido a que los riesgos seguirán cambiando y evolucionando a medida que el mercado global cambie y evolucione, la implementación de ERM debe verse como un compromiso de mejora continua y no como un evento.

#### 14. En general, ¿cuánto tiempo lleva implementar ERM?

Está de moda ver las iniciativas empresariales como actividades discretas con objetivos claros y calendarios bien definidos. Si bien ERM ciertamente no es una excepción desde el punto de vista de la aplicación de la disciplina de gestión de proyectos, es mucho más que un proyecto. ERM es un viaje, lo que significa que es un proceso de crecimiento en el que la organización integra la gestión de riesgos con el establecimiento de estrategias para mejorar la eficacia de sus capacidades de gestión de riesgos a lo largo del tiempo.

El tiempo requerido para implementar ERM varía, según el estado actual de la gestión de riesgos de la organización, su estado futuro deseado y la medida en que está dispuesta a dedicar recursos para mejorar las capacidades de gestión de riesgos. Además, debido a que ERM requiere un entorno abierto propicio para comunicaciones efectivas sobre riesgos y gestión de riesgos hacia arriba, hacia abajo y en toda la empresa, pueden existir problemas culturales que muchas organizaciones deben superar. Por ejemplo, ERM requiere la eliminación de barreras, funcionales o departamentales, para que se adopte un enfoque verdaderamente holístico, integrado, proactivo, con visión de futuro y orientado a procesos para gestionar todos los riesgos y oportunidades comerciales clave, no solo los financieros. Si hay problemas significativos de gestión de cambios que abordar, se extenderá el período de tiempo para implementar ERM. Si bien hay cosas concretas que cualquier organización puede hacer que tendrán un impacto dentro de los 12 meses, estimamos que la mayoría de las organizaciones requerirán de tres a cinco años para lograr sus objetivos en la implementación completa de su solución ERM.

#### 15. ¿Hay alguna forma de comparar el nivel de inversión requerido para implementar ERM?

Como se señaló en las respuestas a las Preguntas 13 y 14, es difícil generalizar sobre la inversión requerida.

Una de las razones de esto es que los estados actuales y deseados varían para diferentes empresas. ERM también es responsabilidad de cada individuo clave dentro de la organización. COSO afirma que ERM “se ve afectado por la junta directiva, la gerencia y otro personal de una entidad”. Es parte integral de lo que hacen. La gestión de una organización y la gestión del riesgo deben estar indisolublemente unidas. Por lo tanto, la gerencia debe decidir la naturaleza de la solución ERM en función de los hechos y circunstancias de la organización. Dado que el punto de origen y el punto de destino varían según la empresa, el enfoque de cada organización tendrá sus propios elementos distintivos.

Una forma eficaz de determinar el nivel de inversión es comparar la gestión de riesgos existente de la organización con un marco (como el marco COSO) y, utilizando esa comparación como contexto, facultar a un grupo de altos ejecutivos para definir el papel de la gestión de riesgos en la organización. Con base en esta evaluación, el nivel de inversión se puede cotizar en función de las personas, las herramientas y otros recursos necesarios para implementar la infraestructura de ERM deseada. Nuestra respuesta a la Pregunta 85 proporciona un contexto adicional para medir el nivel de inversión al señalar la necesidad de comenzar con una evaluación de riesgos empresariales y un análisis de brechas en torno a la gestión de riesgos críticos de la organización.

16. ¿No manejan con éxito empresas que ya aplican ERM?

Esperaríamos que las empresas que funcionan con éxito estén aplicando muchos aspectos de la infraestructura de ERM. De hecho, es difícil tener éxito sin identificar, evaluar formalmente, responder, controlar y monitorear el riesgo. Sin embargo, sugerimos que pocas empresas en el planeta pueden decir con certeza que sus prácticas de gestión de riesgos no necesitan mejoras adicionales. El mensaje no se trata de lo que las empresas están haciendo actualmente, sino de lo que las empresas deberían hacer para aumentar o mejorar sus capacidades de gestión de riesgos a medida que cambia el entorno operativo. El marco COSO proporciona criterios mediante los cuales las empresas pueden evaluar sus prácticas de gestión de riesgos.

Las empresas siempre se han enfrentado a una variedad de riesgos, pero estos son tiempos en los que el ritmo del cambio y las consecuencias resultantes para una empresa parecen ser mayores que nunca. Algunos ejemplos:

- La globalización ha aumentado la exposición a eventos internacionales. Rara vez las fronteras de los países aíslan empresas de tales eventos. El precio de la energía es un ejemplo de ello.
- La necesidad de una mayor eficiencia, innovación y diferenciación, aunque siempre relevante, ha aumentado en importancia a medida que las empresas buscan nuevas formas de diferenciarse.
- Si bien el riesgo de la competencia continúa siendo una prioridad, el costo del error estratégico está aumentando en el mundo mercado. Los mercados financieros son más volátiles que nunca. Los modelos de negocios obsoletos crean una mano perdedora en el juego. E incluso si el modelo de negocio es el correcto para establecer una ventaja sostenible, es ganador solo si la organización es capaz de ejecutarlo de manera efectiva.
- Comprender y responder a los deseos de los clientes sigue siendo la clave en esta era exigente de cada vez más nichos de mercado enfocados. No seguir el ritmo puede resultar en una rápida erosión de la cuota de mercado.
- La subcontratación se ha vuelto tan común que surgen preguntas sobre cómo aclarar la retención y transferencia de riesgo.
- Lamentablemente, ahora sabemos que puede suceder lo impensable. Los hechos del 11 de septiembre de 2001 han cambiado nuestra forma de pensar sobre el riesgo de interrupción del negocio.
- Debido a los fiascos de información pública altamente publicitados y las altas demandas de los oficiales certificadores, la presentación de informes es ahora un área de riesgo importante ya que las empresas se centran en la sostenibilidad de su proceso de divulgación y estructura de control interno.

Hoy en día, estos y otros riesgos están impulsando un perfil de riesgo en constante cambio que no solo tiene implicaciones financieras, sino también impactos estratégicos y operativos. A medida que los ejecutivos examinan los riesgos que enfrentan sus empresas hoy en día, verán un perfil diferente al que vieron hace algunos años. Y, lo que es más importante, pueden esperar ver incluso riesgos diferentes dentro de unos años. Es por eso que un proceso de evaluación de riesgos empresariales es tan crítico.

Todo se reduce a esto: no son los más fuertes o los más inteligentes los que sobrevivirán y prosperarán en la economía global: son las organizaciones las que mejor pueden adaptarse al cambio. A medida que cambian los mercados y los clientes, cambian los modelos de negocio. A medida que cambia el panorama competitivo, cambian las estrategias comerciales. Además, a menos que la implementación de ERM esté estrechamente vinculada a la evaluación y formulación de la estrategia empresarial, no se está desarrollando todo su potencial. Por eso, incluso las empresas que han alcanzado la excelencia en la gestión de riesgos deben evaluar periódicamente la eficacia de sus capacidades de gestión de riesgos.

17. ¿Cuánto tiempo ha existido ERM y por qué hay un enfoque renovado en él?

Los conceptos y teorías que subyacen a ERM, es decir, una visión de cartera del riesgo, existen desde hace mucho tiempo. La aplicación de estos conceptos y teorías ha surgido en instituciones financieras y tesorerías corporativas de clase mundial a medida que aplican marcos de riesgo, técnicas de atribución de capital y otras metodologías de medición para la gestión del riesgo de mercado y de crédito. Sin embargo, los desarrollos del mercado en los últimos años han dejado en claro que la volatilidad ya no es solo un riesgo de moneda, tasa de interés o valores de acciones.

Las preferencias de los clientes, las ofertas de productos de la competencia, los mercados laborales y la tecnología están cambiando cada vez con mayor frecuencia, y su comportamiento se asemeja al de los mercados financieros. Incluso los ciclos de vida de los modelos de negocios organizacionales se están comprimiendo. El cambio ya no es lineal, sino exponencial. Las empresas exitosas deben innovar y ofrecer soluciones totales que creen nuevas fuentes de valor para sus clientes o mercados o perderán terreno frente a rivales más ágiles y creativos.

La innovación constante también da lugar a nuevos riesgos que deben evaluarse con frecuencia. Esta forma de pensar hace que la estrategia comercial sea un proceso fluido y dinámico, con la gestión de riesgos aumentando ese proceso. Este ritmo creciente de cambio y el reconocimiento de que el cambio es una forma de vida proactiva, junto con técnicas cada vez más efectivas de identificación, medición, informe y planificación de riesgos, han hecho que las empresas observen más de cerca el estado de su gestión de riesgos.

En el pasado, la brecha entre el modelo tradicional de gestión de riesgos y ERM, como se explica en la Pregunta 6, era demasiado amplia para que la mayoría de las empresas la abordaran. Sin embargo, el cumplimiento de Sarbanes-Oxley sentó las bases para implementar capacidades de ERM que no existían anteriormente. Las empresas que han implementado procesos mejorados de divulgación y control interno sobre la información financiera (ICFR) deben analizar más de cerca cómo pueden expandir estas capacidades para abarcar otras actividades comerciales críticas, porque el abismo no es tan grande como lo era antes debido a la continua esfuerzo de cumplimiento requerido por Sarbanes-Oxley. El marco integrado de gestión de riesgos empresariales de COSO proporciona los criterios para ayudar a la gerencia a evaluar lo que se debe hacer. Ese marco abarca el Control Interno COSO - Marco Integrado utilizado por muchas empresas para evaluar la efectividad de su ICFR.

#### 18. ¿Qué porcentaje de empresas públicas cuentan actualmente con un proceso o sistema ERM?

La respuesta corta es que el marco COSO proporciona los criterios necesarios para abordar esta pregunta. Hasta que el marco obtenga más tracción en el mercado y las empresas puedan comparar su gestión de riesgos con el marco para evaluar cuál es su posición, no sabremos la respuesta completa a esta pregunta.

Sin embargo, hay algunas ideas a partir de las cuales podemos inferir cuál es la posición actual de las empresas:

- Una Encuesta global de directores ejecutivos publicada por PricewaterhouseCoopers (PwC) en 2004 indicó que el 39 por ciento de 1400 directores ejecutivos estaban totalmente de acuerdo en que ERM era una prioridad. Si bien este grupo de directores ejecutivos (descrito por PwC como directores ejecutivos "muy comprometidos") reportó beneficios de ERM, la encuesta de PwC informa que el 53 por ciento de ellos está de acuerdo en que tiene la información empresarial que necesita, el 42 por ciento integra ERM con la planificación estratégica, el 29 por ciento informa que la uso de la cuantificación en la mayor medida posible, el 27 por ciento integra ERM en todas las funciones y unidades, y solo el 20 por ciento informa que todos entienden su responsabilidad en relación con la gestión de riesgos. Por el contrario, los CEO restantes (aquellos que no están tan comprometidos con ERM, según la encuesta) reportan porcentajes significativamente más bajos en estas y otras preguntas relacionadas.
- En nuestra investigación durante los últimos 10 años, hemos implementado varias encuestas (con el último estudio en el otoño de 2005) para indagar sobre el nivel de confianza que los altos ejecutivos tienen en la gestión de riesgos de su organización. En todos los casos, alrededor del 60 por ciento de los altos ejecutivos que informaron indicaron que carecían de mucha confianza en que las capacidades de administración de riesgos de su organización fueran efectivas para identificar y administrar todos los riesgos comerciales potencialmente significativos. Nuestra experiencia indica que esta falta de confianza se debe a la ausencia de un proceso sistemático para involucrar a los ejecutivos apropiados en la identificación y priorización de riesgos en toda la empresa. Decidir qué hacer y cómo hacerlo solo se produce después de que los riesgos vitales estén en la pantalla de la gerencia a través de un proceso eficaz de evaluación de riesgos empresariales.
- La falta de transparencia también se extiende al directorio. En un estudio de McKinsey que involucró a 200 directores que representan a más de 500 juntas, publicado justo antes de que se promulgara la Ley Sarbanes-Oxley, el 36 por ciento de los directores indicó que sus juntas no comprendían los principales riesgos de la empresa. Aproximadamente el 40 por ciento de los directores indicaron que carecían de conocimiento sobre cómo identificar, salvaguardar y planificar el riesgo de manera efectiva. El estudio también encontró que el riesgo no financiero recibió solo un "tratamiento anecdótico" en la sala de juntas. No es de extrañar que la gerencia reciba más preguntas de los directores sobre los riesgos y la gestión de riesgos de su empresa.

19. ¿Hay algún ejemplo de ERM eficaz tal como se aplica en la práctica?

Las técnicas de aplicación de COSO brindan ejemplos de los métodos utilizados por diferentes empresas en varios niveles de la organización al aplicar los principios de ERM. Los lectores familiarizados con el marco encontrarán el material útil como ejemplos.

20. ¿Cómo varía la aplicación de ERM según la industria?

En la página 3 de las Técnicas de aplicación, COSO afirma que "debido a la variedad de enfoques y opciones disponibles, incluso organizaciones similares implementan la gestión de riesgos empresariales de manera diferente, ya sea aplicando los conceptos y principios del marco por primera vez o considerando si su gestión de riesgos empresariales existente El proceso, que puede haber sido desarrollado ad hoc con el tiempo, es realmente efectivo". COSO señala que la industria en la que opera una empresa es uno de los atributos que "afectará la forma en que los conceptos y principios del marco se aplican de manera más efectiva y eficiente". La naturaleza de la industria impulsará la naturaleza de los riesgos y las prácticas de gestión de riesgos que la organización adopte para gestionar esos riesgos. Por ejemplo, un banco se centrará en gestionar el riesgo de mercado y de crédito en mayor medida que otras instituciones porque la asunción de esos riesgos es la esencia de su modelo de negocio. Una empresa farmacéutica se centrará en la gestión de su canal de investigación y desarrollo porque ese es el sustento de sus futuras fuentes de ingresos. Una empresa de servicios públicos gestionará los riesgos de conformidad en una instalación de energía nuclear porque esa es la clave de su reputación y viabilidad futura. Sin embargo, independientemente de la industria, los componentes del marco, según lo definido por COSO, aún se aplican.

21. ¿Hay alguna organización que no necesite implementar ERM?

Toda organización exitosa enfrenta riesgos. Según lo articulado por COSO, ERM es un proceso para hacer frente a riesgos y oportunidades. La dirección ejecutiva en la mayoría de las organizaciones, independientemente del sector industrial, se centra en la inversión y el rendimiento, en la oportunidad y la recompensa y en la ventaja competitiva y el crecimiento. Es por eso que ERM es vital para el éxito: ayuda a los gerentes a ganar confianza en que comprenden los riesgos de la organización y tienen las capacidades para administrar esos riesgos.

Toda organización exitosa asume riesgos. Cada elección que hace la gerencia de actuar o no actuar afecta el perfil de riesgo de la organización. ERM puede ayudar a la gerencia a desarrollar una habilidad diferenciadora en la selección de las mejores apuestas para una empresa, dadas las fuerzas competitivas, regulatorias y de otro tipo en el entorno externo. Esta habilidad mejorada vigoriza el comportamiento de búsqueda de oportunidades.

Toda organización exitosa responde al riesgo. La gerencia ejecutiva debe manejar el negocio en medio de las cambiantes realidades del mercado. Deben evaluar cuidadosamente el riesgo y la recompensa a medida que canalizan los recursos hacia las mejores oportunidades, en consonancia con el apetito por el riesgo de la organización. Deben asegurar con confianza a los inversionistas y otras partes interesadas que su organización está administrando el riesgo de manera efectiva mientras prospera en el mercado global. Como si eso no fuera suficiente, frente a Sarbanes-Oxley, el director ejecutivo y el director financiero, como funcionarios certificadores, deben ser campeones de la información pública transparente. Responder a estos y otros riesgos inherentes al modelo de negocio es lo que hacen las organizaciones exitosas.

Una infraestructura ERM ayudará a los ejecutivos y directores a enfrentar estos desafíos. Como se discutió en la Pregunta 23, esta afirmación se aplica tanto a las empresas públicas como a las privadas.

22. ¿Cuáles son los mandatos regulatorios para implementar ERM?

Si bien no existen requisitos regulatorios explícitos que exijan el uso de COSO Enterprise Risk Management – Marco Integrado en este momento, los desarrollos regulatorios han creado un entorno en el que las empresas se beneficiarían de ERM. COSO señaló que, al igual que otros factores que definen el entorno externo, la regulación en sí genera incertidumbre.

En los Estados Unidos, Sarbanes-Oxley ha ocupado los titulares desde su aprobación en julio de 2002 hasta el momento en que se lanzó esta publicación para imprimir. Si bien el enfoque de Sarbanes-Oxley se limita a la confiabilidad de

informes financieros, creemos que las empresas se beneficiarían de un proceso ERM centrado en identificar los riesgos críticos de la empresa para la acción y divulgación oportunas. También hay otros desarrollos en los Estados Unidos, como la Ley PATRIOTA de EE. UU. que requiere regulaciones contra el lavado de dinero de "conozca a su cliente" y la Ley Gramm-Leach-Bliley que requiere que las instituciones financieras protejan y preserven la privacidad de los clientes "no públicos". información. De acuerdo con los requisitos de cotización de la Bolsa de Valores de Nueva York (NYSE), el estatuto del comité de auditoría debe exigir que el comité discuta las políticas con respecto a la evaluación y gestión de riesgos. La NYSE también exige una función de auditoría interna con el fin de proporcionar a la gerencia y al comité de auditoría evaluaciones continuas de los procesos de gestión de riesgos y el sistema de control interno de la empresa. Si bien no es obligatorio, ERM facilitaría el cumplimiento de estos requisitos a través de una infraestructura y un proceso que fortalece el enfoque de la empresa para proteger y mejorar simultáneamente el valor de la empresa.

Fuera de los Estados Unidos, la legislación KonTrag en Alemania requiere que las grandes empresas establezcan sistemas de supervisión de gestión de riesgos y reporten información de controles a los accionistas. Las empresas que cotizan en la Bolsa de Valores de Londres y están constituidas en el Reino Unido deben informar a los accionistas sobre un conjunto de principios definidos relacionados con el gobierno corporativo (conocido como el Código Combinado y respaldado con la orientación proporcionada por el Informe Turnbull). El nuevo Acuerdo de Capital de Basilea, emitido por el Comité de Supervisión Bancaria de Basilea, exige que las instituciones financieras informen sobre el riesgo operativo. Una vez más, un proceso de ERM facilitaría el cumplimiento de estos requisitos. Además, sigue surgiendo legislación tipo Sarbanes-Oxley en países fuera de los Estados Unidos.

#### 23. ¿Los estándares para implementar ERM son diferentes para las empresas públicas y privadas?

El marco COSO se aplica a todas las organizaciones, grandes y pequeñas, públicas y privadas. Los métodos utilizados para aplicar los componentes del marco pueden variar según el tamaño, los objetivos, la estrategia, la estructura, la cultura, el estilo de gestión, el perfil de riesgo, la industria, el entorno competitivo y los medios financieros de la organización.

#### 24. ¿Deben las empresas contar con procesos sofisticados en todas las áreas de gestión de riesgos para realizar la ¿Beneficios de ERM?

El marco COSO no requiere sofisticación en la gestión de riesgos. No es necesario desplegar las técnicas más avanzadas para todos los riesgos. Pocas organizaciones tienen los recursos para hacer eso, y no hay un caso comercial convincente para hacerlo. La sofisticación es una función de (a) la naturaleza de los riesgos que enfrenta una organización, es decir, su complejidad, volatilidad, omnipresencia y susceptibilidad a la medición, y (b) la disponibilidad de soluciones prácticas que la entidad puede poner en práctica. Al evaluar las capacidades de gestión de riesgos deseadas en un área o áreas de riesgo específicas, el problema no es implementar los procesos, competencias, tecnología y conocimiento más sofisticados, sino seleccionar los procesos, competencias, tecnología y conocimiento más apropiados. Esta es una decisión de gestión. Y esa decisión debe tomarse en el contexto del proceso de establecimiento de la estrategia.

Para cada riesgo individual o grupo de riesgos relacionados, la dirección debe evaluar el estado actual de las capacidades de gestión de riesgos de la organización. En ese momento, la dirección debe decidir cuánta capacidad adicional se necesita para lograr los objetivos de gestión de riesgos de la entidad. Además, la gerencia debe abordar los costos y beneficios esperados de mejorar las capacidades de la organización. El objetivo es identificar las exposiciones e incertidumbres más apremiantes de la entidad y centrar las actividades de mejora en los elementos de la infraestructura de ERM necesarios para gestionar esas exposiciones e incertidumbres con mayor eficacia.

---

## LA GESTIÓN DE RIESGOS EMPRESARIALES DE COSO: MARCO INTEGRADO

#### 25. ¿Qué es COSO?

COSO significa "Comité de Organizaciones Patrocinadoras" y es una organización voluntaria del sector privado dedicada a mejorar la calidad de los informes financieros a través de la ética empresarial, controles internos efectivos y gobierno corporativo. COSO se formó originalmente en 1985 para patrocinar la Comisión Nacional de

Informes financieros fraudulentos, una iniciativa independiente del sector privado a la que a menudo se hace referencia como la Comisión Treadway. La Comisión estudió los factores causales que pueden conducir a informes financieros fraudulentos y desarrolló recomendaciones para empresas públicas y sus auditores independientes, para la Comisión de Bolsa y Valores ("SEC" o "Comisión") y otros reguladores, y para instituciones educativas.

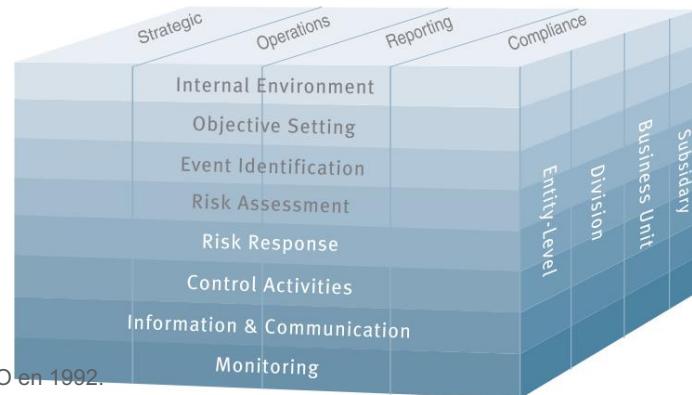
Las organizaciones patrocinadoras son el Instituto Estadounidense de Contadores Públicos Certificados (AICPA), el Instituto de Auditores Internos (IIA), Financial Executives International (FEI), el Instituto de Contadores Administrativos (IMA) y la Asociación Estadounidense de Contabilidad (AAA). COSO hasta ahora ha producido dos documentos, uno en 1992 sobre Controles Internos - Marco Integrado (que es el marco elegido en los Estados Unidos para cumplir con la Sección 404 de Sarbanes-Oxley), y el otro a mediados de la década de 1990 sobre derivados.

## 26. ¿Por qué se creó COSO Enterprise Risk Management – Marco Integrado?

El proyecto para desarrollar este marco comenzó en 2001, antes de que surgieran los escándalos que alimentaron la legislación Sarbanes-Oxley. En el prólogo del marco, COSO indicó que "los últimos años han visto una mayor preocupación y enfoque en la gestión de riesgos, y se hizo cada vez más claro que existe la necesidad de un marco sólido para identificar, evaluar y gestionar el riesgo de manera efectiva". El propósito de COSO era desarrollar un marco que "sería fácilmente utilizable por las gerencias para evaluar y mejorar la gestión de riesgos empresariales de sus organizaciones". COSO continúa señalando que después de las fallas comerciales de alto perfil que ocurrieron durante el período de desarrollo del marco, hubo "llamadas para mejorar el gobierno corporativo y la gestión de riesgos, con nuevas leyes, normas regulatorias y de cotización". Todos estos desarrollos hicieron más apremiante la necesidad de un marco para proporcionar un lenguaje común y dar una dirección y orientación claras.

## 27. ¿Qué es la gestión de riesgos empresariales de COSO: marco integrado?

COSO define ampliamente la ERM como "un proceso, llevado a cabo por la junta directiva, la gerencia y otro personal de una entidad, aplicado en el establecimiento de estrategias y en toda la empresa, diseñado para identificar eventos potenciales que pueden afectar a la entidad y administrar los riesgos para estar dentro de su alcance. apetito de riesgo, para proporcionar una seguridad razonable con respecto al logro de los objetivos de la entidad". El marco abarca, pero no reemplaza, el Control Interno - Marco Integrado publicado por COSO en 1992.



Al igual que su contraparte de control interno, el marco ERM se presenta en forma de matriz tridimensional. La matriz incluye cuatro categorías de objetivos en la parte superior: estratégicos, operativos, de informes y de cumplimiento. Hay ocho componentes de la gestión del riesgo empresarial, que se explican con más detalle a continuación. Finalmente, la entidad, sus divisiones y unidades de negocio se representan como la tercera dimensión de la matriz para la aplicación del marco.

Como lo describe COSO, el marco proporciona ocho componentes para usar al evaluar ERM:

1. Entorno interno: este componente refleja la filosofía de gestión del riesgo empresarial de una entidad, el apetito por el riesgo, la supervisión del directorio, el compromiso con los valores éticos, la competencia y el desarrollo de las personas, y la asignación de autoridad y responsabilidad. Abarca el "tono en la parte superior" de la empresa e influye en el proceso de gobierno de la organización y la conciencia de riesgo y control de su gente.
2. Establecimiento de objetivos: la gerencia establece objetivos estratégicos, que brindan un contexto para los objetivos operativos, de información y de cumplimiento. Los objetivos están alineados con el apetito por el riesgo de la entidad, lo que impulsa los niveles de tolerancia al riesgo para la entidad, y son una condición previa para la identificación de eventos, la evaluación del riesgo y la respuesta al riesgo.

3. Identificación de eventos: la gerencia identifica eventos potenciales que pueden afectar positiva o negativamente a un la capacidad de la entidad para implementar su estrategia y lograr sus objetivos y metas de desempeño. Potencialmente los eventos negativos representan riesgos que proporcionan un contexto para evaluar el riesgo y las respuestas alternativas al riesgo. Los eventos potencialmente positivos representan oportunidades, que la gerencia canaliza nuevamente hacia la estrategia. y procesos de fijación de objetivos.
4. Evaluación de riesgos: La gerencia considera métodos cualitativos y cuantitativos para evaluar la probabilidad e impacto de eventos potenciales, individualmente o por categoría, que podrían afectar el logro de objetivos en un horizonte de tiempo determinado.
5. Respuesta al riesgo: la gerencia considera opciones alternativas de respuesta al riesgo y su efecto sobre la probabilidad del riesgo e impacto, así como los costos versus beneficios resultantes, con el objetivo de reducir el riesgo residual a tolerancias de riesgo deseadas. La planificación de la respuesta a los riesgos impulsa el desarrollo de políticas.
6. Actividades de control: La gerencia implementa políticas y procedimientos en toda la organización, en todos niveles y en todas las funciones, para ayudar a garantizar que las respuestas a los riesgos se ejecuten correctamente.
7. Información y comunicación: La organización identifica, captura y comunica información pertinente información de fuentes internas y externas en una forma y plazo que permita al personal llevar a cabo fuera de sus responsabilidades. La comunicación efectiva también fluye hacia abajo, a través y hacia arriba de la organización. La generación de informes es vital para la gestión de riesgos y este componente la proporciona.
8. Monitoreo: Las actividades en curso y/o evaluaciones separadas evalúan tanto la presencia como el funcionamiento de componentes de gestión de riesgos empresariales y la calidad de su desempeño a lo largo del tiempo.

El proceso de pensamiento que subyace en el marco anterior funciona de la siguiente manera: para cualquier objetivo dado, como las operaciones, la gerencia debe evaluar los ocho componentes de ERM en el nivel apropiado, como el nivel de entidad o unidad de negocio.

## 28. ¿Cómo podemos obtener el framework COSO ERM?

Los interesados pueden obtener el resumen ejecutivo del marco en [www.coso.org](http://www.coso.org). En este sitio pueden \_\_\_\_\_ también haga un pedido de una copia impresa o una copia electrónica del marco integrado, que incluye tres segmentos: el resumen ejecutivo, el marco y las técnicas de aplicación que lo acompañan.

## 29. ¿Cómo se desarrolló el marco COSO ERM?

El Apéndice A del marco COSO ERM describe el proceso. COSO contrató a PricewaterhouseCoopers (PwC) para llevar a cabo el proyecto. PwC obtuvo información de una amplia gama de ejecutivos: director ejecutivo ejecutivos, directores financieros, directores de riesgos, controladores y auditores internos que representan al público y empresas privadas de diversos tamaños y de diferentes industrias y agencias gubernamentales. La entrada también fue obtenida de legisladores, reguladores, auditores externos, abogados y académicos. PwC recibió asesoramiento y consejo de una junta asesora a la junta de COSO. Periódicamente, PwC, el consejo asesor y el COSO la junta se reuniría para discutir el plan del proyecto, el progreso, los borradores del marco y temas y problemas específicos relacionado con completar el marco.

Como se discutió en el Apéndice A del marco, el proyecto constaba de cinco fases: Evaluación, Visualización, evaluación y diseño, preparación para exposición pública y finalización. El documento fue expuesto durante un período de 90 días y el marco fue probado en el campo con empresas seleccionadas. La entrada fue considerado tanto del período de comentarios como de las pruebas de campo. Fuentes publicadas consideradas por el proyecto equipo se incluyeron en el Apéndice D del marco, incluidos dos libros escritos por un administrador de Protiviti director. El Apéndice E incluye un resumen de la consideración del equipo del proyecto de los problemas específicos que surgieron durante el período de comentarios.

### 30. ¿Cómo usamos el marco COSO ERM?

En las páginas 6 y 7, COSO sugiere usos alternativos del marco según el usuario. Por ejemplo:

USUARIO	USOS POSIBLES
directores	<ul style="list-style-type: none"> <li>• Discutir con la gerencia el estado de ERM</li> <li>• Supervisar las actividades de gestión de riesgos</li> <li>• Asegurarse de que estén informados de los riesgos y la gestión acciones para hacerles frente</li> <li>• Considere los aportes de los auditores internos, los auditores externos y otros</li> </ul>
Gerencia senior	<ul style="list-style-type: none"> <li>• Evaluar las capacidades de ERM de la organización</li> </ul>
Directivos y otro personal de la entidad	<ul style="list-style-type: none"> <li>• Considere cómo están llevando a cabo sus responsabilidades a la luz de los componentes del marco</li> <li>• Discutir con los superiores ideas para mejorar ERM</li> </ul>
Auditores internos	<ul style="list-style-type: none"> <li>• Considerar la amplitud de su enfoque en ERM en el plan de auditoría</li> </ul>

COSO también proporcionó sugerencias para reguladores, organizaciones profesionales y educadores.

En resumen, el marco COSO debe usarse como una herramienta de evaluación comparativa para evaluar la efectividad de el proceso ERM implementado, así como actividades específicas de gestión de riesgos en todos los niveles de la organización. El marco puede proporcionar el contexto para definir mejoras en las capacidades de gestión de riesgos.

### 31. ¿Están obligadas las empresas a utilizar el marco COSO ERM?

No. El uso de este marco es opcional. Sin embargo, para poner esta declaración en perspectiva, los lectores deben Entiendo que cuando se emitió en 1992, el Marco Integrado de Control Interno también era opcional. Ahora casi todas las empresas públicas de los Estados Unidos lo están utilizando.

### 32. ¿El COSO Enterprise Risk Management – Marco Integrado reemplaza o reemplaza el Control Interno COSO – ¿Marco Integrado?

No. Ambos marcos son independientes. El Apéndice C del marco ERM aborda esta cuestión. Estados COSO que el control interno está incluido dentro y es una parte integral de ERM. Por lo tanto, el nuevo ERM marco no reemplaza ni reemplaza el marco de control interno. Este punto es importante porque Muchas empresas de EE. UU. están utilizando COSO Internal Control – Integrated Framework para propósitos de cumpliendo con la Sección 404 de Sarbanes-Oxley.

### 33. ¿Cómo se compara COSO Enterprise Risk Management – Marco Integrado con el Control Interno COSO – ¿Marco Integrado?

El Apéndice C del marco de ERM aborda esta pregunta y establece las diferencias entre los dos marcos Por ejemplo, en comparación con el marco de control interno:

- El marco ERM es un enfoque más amplio en la gestión de riesgos y abarca el control interno estructura.
- El marco ERM agregó una nueva categoría, objetivos estratégicos, y amplió el objetivo de informes para incluir informes internos.

- El marco ERM introdujo los conceptos de apetito por el riesgo y tolerancia al riesgo.
- El marco de ERM amplía el componente de evaluación de riesgos en cuatro componentes: establecimiento de objetivos, identificación de eventos, evaluación de riesgos y respuesta al riesgo.

También hay diferencias específicas en los componentes mismos, que se analizan en el Apéndice C del marco. Por ejemplo, las funciones y responsabilidades se amplían para centrarse en la gestión de riesgos frente al control interno. El componente de entorno interno del marco de ERM abarca los siete atributos del componente de entorno de control del marco de control interno, con énfasis en la gestión de riesgos, y agrega tres atributos adicionales: filosofía de gestión de riesgos, cultura de riesgo y apetito de riesgo.

34. ¿El nuevo marco COSO amplía el enfoque de ERM más allá del enfoque tradicional del modelo de gestión de riesgos en el riesgo asegurable? ¿Si es así, cómo?

Sí. El marco COSO ERM se enfoca integralmente en todos los riesgos, no solo en los financieros o asegurables. El marco logra este enfoque más amplio al menos de dos maneras:

- Enfatiza los objetivos estratégicos, operativos, de reporte y de cumplimiento y, por lo tanto, aborda los riesgos al logro de esos objetivos.
- Los ocho componentes de ERM, como lo describe COSO, son lo suficientemente completos y se extienden más allá de la contratación de seguros.

Por lo tanto, cuando COSO usa el término "Gestión de riesgos empresariales", se refiere a un concepto de gestión de riesgos más amplio que el modelo de gestión de riesgos asegurables.

35. ¿Existen otros estándares y marcos y, de ser así, qué promulgan y cómo se relaciona con ellos el marco integrado de gestión de riesgos empresariales de COSO?

De hecho, existen otros estándares, que COSO enumera en el Apéndice D. Estos estándares incluyen:

- Guía de Control Interno para Directores sobre el Código Combinado (Reino Unido)
- Informe King sobre Gobierno Corporativo para Sudáfrica
- Organización Internacional de Normalización – Guía ISO/IEC
- Estándar australiano/neozelandés 4360: Gestión de riesgos
- Un Estándar de Gestión de Riesgos (Instituto de Gestión de Riesgos, Asociación de Seguros y Riesgos) Gestión)

COSO no publicó una reconciliación de estos diversos estándares con su marco ERM. Sin embargo, el equipo del proyecto consideró estos marcos en la fase de Evaluación del proyecto. Además, la Pregunta 164 relaciona la ERM con el Acuerdo de Capital de Basilea que exige que las instituciones financieras informen sobre el riesgo operativo.

Las preguntas 165 y 166 comentan brevemente sobre la relación entre el marco COSO ERM y otros marcos, como COBIT, ISO 17799, BITS, NIST Special Publication 800-53 e ITIL.

36. ¿Cuál es el punto de vista de la Comisión de Bolsa y Valores (SEC) con respecto a ERM?

La Comisión no había emitido una declaración oficial a la fecha de impresión de esta publicación. Sin embargo, un comisionado de la SEC ha abordado periódicamente la importancia de ERM en varios discursos.

37. ¿Cuáles son los entregables cuando se implementa el marco COSO ERM?

Los "productos" varían según las técnicas y herramientas implementadas para implementar los ocho componentes de ERM, la amplitud de los objetivos abordados, la naturaleza de la industria, la naturaleza de los riesgos y el alcance de la cobertura de las unidades de la organización. La infraestructura ERM, que está destinada a proporcionar la

disciplina, enfoque y control para mejorar las capacidades de la empresa en torno a la gestión de sus riesgos prioritarios, puede incluir elementos como los siguientes:

POSIBLE ELEMENTO DE INFRAESTRUCTURA ERM	DISCUSIDO EN PREGUNTAS
Presencia en la agenda del CEO	3, 4, 21, 30, 40, 41, 56, 88-90, 129, 136, 141, 142, 144
Política general de gestión de riesgos	65, 110
Lenguaje de riesgo común	74-76, 98
Proceso de evaluación de riesgos en toda la empresa	65, 69-85, 103, 106, 129, 131
Vista de proceso común	99, 103, 104
Claridad de las funciones y responsabilidades relacionadas con la gestión de riesgos	30, 56, 57, 90, 91, 110, 144
Comité(s) de riesgo enfocado(s)	48, 49, 56, 85
CRO (o ejecutivo equivalente)	50-52, 56
Integración de respuestas de riesgo dentro de los planes de negocios	50, 54, 108, 109, 127, 129, 133
Integración de la gestión de riesgos con el establecimiento de estrategias	3, 4, 41, 49, 56, 66, 67, 85, 108, 109, 111, 129, 131, 133, 135
Alineación del comportamiento organizacional con el apetito de riesgo	45, 49, 53, 54, 56, 65-67, 95, 102, 106, 127, 129, 131, 133
Informe de riesgos	45, 50, 109, 111-113, 121
Proceso de intercambio de conocimientos para identificar las mejores prácticas	51, 91, 101, 103, 111, 121, 123
Formación común	111, 123
Herramientas patentadas para representar una visión de cartera del riesgo	3, 56, 108, 109, 111, 112, 127, 129
Tecnología de apoyo	110, 111, 113-121

Los "productos" adicionales incluyen las capacidades mejoradas en torno a la gestión de los riesgos prioritarios de la empresa.

La propuesta de valor, como se resume en la Pregunta 4, ilustra los beneficios que se pueden lograr a través de un infraestructura ERM.

Tenga en cuenta que existe una relación entre (a) la necesidad de infraestructura ERM por un lado y (b) la naturaleza y el alcance de las brechas en las capacidades de gestión de riesgos por el otro. Cuanto mayores sean las brechas en el estado actual y Cuanto mayor sea el estado futuro deseado de las capacidades de gestión de riesgos de la organización, mayor será la necesidad de ERM infraestructura para impulsar el avance de las capacidades a lo largo del tiempo para cerrar estas brechas. La buena noticia es que el La infraestructura de gestión existente de la mayoría de las empresas ya incluye elementos de la infraestructura ERM.

38. ¿Puede una empresa adoptar "parcialmente" el COSO Enterprise Risk Management – Integrated Marco con éxito?

Al definir ERM, COSO ha indicado que el marco se aplica en toda la empresa. Esto puede ser logrado, sin embargo, dentro de una unidad, subsidiaria o división específica, representando una forma de "parcial adopción" sin dejar de mantener un enfoque en toda la empresa. La aplicación de ERM a las unidades operativas estratégicas funciona porque tales unidades a menudo tienen objetivos y estrategias distintivamente diferentes, manejan grupos de productos, atienden mercados heterogéneos y actúan como centros de ganancias independientes. Por lo tanto, tienen perfiles de riesgo claramente diferentes. La dirección ejecutiva a nivel de matriz puede incluso fomentar, explícita o

implícitamente, un entorno competitivo entre diferentes unidades estratégicas. De ser así, los perfiles de riesgo para unidades de negocios separadas pueden diferir en tal medida que puede ser apropiado evaluarlos y administrarlos por separado. En tales circunstancias, un enfoque descentralizado puede tener más sentido con ERM aplicado en una o más unidades operativas seleccionadas.

En última instancia, tener una visión de toda la empresa significa lograr el mayor nivel posible de rendimiento ajustado al riesgo de los recursos disponibles para los gerentes dentro de los límites empresariales definidos, ya sea para una unidad operativa específica o para la empresa en su conjunto. Desde el punto de vista de la gestión de riesgos, esta visión tiene que ser coherente con la visión de la dirección ejecutiva de la organización. Si la administración adopta una visión centralizada del negocio, una visión empresarial necesariamente debe extenderse a toda la organización. Por otro lado, si la gerencia tiene una visión descentralizada de la organización con diferentes unidades operando de manera autónoma, se aplicaría una visión empresarial a nivel de unidad.

---

## EL PAPEL DE LA DIRECCIÓN EJECUTIVA

39. ¿Quién debería participar en el proceso de ERM y cómo?

Si bien la responsabilidad final de ERM comienza en la parte superior, todas las personas importantes dentro de una organización deben participar en cierta medida en el proceso de ERM. Si bien varios ejecutivos tienen responsabilidades significativas para ERM, incluido el director de riesgos, el director financiero, el director legal y el director ejecutivo de auditoría, el proceso de ERM funciona mejor cuando todos los gerentes clave de la organización contribuyen. El marco COSO establece que los gerentes de la organización “respaldan la filosofía de administración de riesgos de la entidad, promueven el cumplimiento de su apetito por el riesgo y administran los riesgos dentro de sus esferas de responsabilidad de manera consistente con las tolerancias al riesgo”.

Por lo tanto, identificar líderes en toda la organización y obtener su apoyo es fundamental para una implementación exitosa. Un objetivo de ERM es incorporar la gestión de riesgos en la agenda y los procesos de toma de decisiones de la organización. Esto significa que, en última instancia, cada gerente es responsable, lo que solo puede suceder cuando los objetivos de desempeño están claramente articulados y las personas adecuadas son responsables de los resultados.

40. ¿Debe el director general participar plenamente en el proceso o sistema de ERM para que tenga éxito, o puede o se lo delega a otra persona?

El marco COSO establece que el CEO “es el responsable último y debe asumir la responsabilidad” sobre la implementación de ERM. Debido a que ERM, como lo definió COSO, es parte integral del funcionamiento y la gestión de una empresa, la participación del director ejecutivo es vital para el éxito de ERM. Por ejemplo, una solución de ERM efectiva afecta la cultura de la organización, porque establece un entorno en el que las personas pueden levantar la mano y expresar sus problemas sin temor a represalias. Este tipo de ambiente abierto y positivo no es posible sin el apoyo activo y visible del CEO. El CEO marca la pauta al hacer las preguntas difíciles sobre el riesgo y la gestión de riesgos y al demostrar un compromiso para elevar el enfoque de la gestión de riesgos a un nivel estratégico.

Un punto que a menudo se omite en esta discusión es que es importante para el CEO estar involucrado en el proceso. La participación del Gerente General mantiene el foco en un nivel estratégico. El CEO quiere saber las respuestas a al menos dos preguntas sobre el riesgo. En primer lugar, ¿existen exposiciones desconocidas a eventos que puedan cambiar abruptamente la agenda de la organización a “control de daños” en un abrir y cerrar de ojos en caso de que ocurran? En segundo lugar, si tales exposiciones existen, ¿qué se puede hacer de manera rentable para evitar que sucedan los posibles eventos futuros y cómo responderá la organización en caso de que ocurran los eventos? ERM puede ayudar a proporcionar a los directores ejecutivos respuestas a estas dos preguntas, pero solo si el director ejecutivo está lo suficientemente involucrado para garantizar que el proceso se centre adecuadamente en los riesgos estratégicos y de reputación.

El apoyo desde arriba es vital para una infraestructura ERM que funcione de manera efectiva. Para crear y mantener el impulso, la alta gerencia debe demostrar un fuerte compromiso con ERM a través de comunicaciones y acciones consistentes. Este nivel de compromiso surge de un caso comercial convincente. El caso de negocios articula los riesgos prioritarios de la organización, las brechas en torno a la gestión de esos riesgos, la infraestructura de ERM necesaria para cerrar brechas significativas y los costos y beneficios resultantes. El caso de negocio aclara

por qué se necesita la infraestructura ERM, se centra en el panorama general con una visión compartida del estado futuro de la gestión de riesgos dentro de la organización, establece objetivos realistas y desarrolla un plan de acción claro. Un caso de negocios bien articulado ayuda a involucrar al CEO.

#### 41. ¿Cómo se beneficiará la alta dirección del apoyo a la implementación de ERM?

A medida que se enfocan en la inversión y el retorno, en la oportunidad y la recompensa y en la ventaja competitiva y el crecimiento, los directores ejecutivos y sus equipos gerenciales deben buscar oportunidades prometedoras, aunque inciertas, frente a las condiciones cambiantes del mercado. Deben estar en condiciones de asegurar con confianza a los inversores y otras partes interesadas que la organización está gestionando el riesgo de manera eficaz. También deben cumplir con Sarbanes-Oxley y otras leyes y reglamentos aplicables.

Las investigaciones que hemos realizado varias veces desde 1995 (con el estudio más reciente completado durante el otoño de 2005) indican casi consistentemente que aproximadamente 6 de cada 10 altos ejecutivos no tienen mucha confianza en que las capacidades de su organización identifiquen y gestionen todos los riesgos comerciales potencialmente significativos. Los altos ejecutivos pueden obtener una mayor confianza con un proceso efectivo que involucra a todos los que tienen responsabilidades clave dentro de la organización para evaluar y gestionar el riesgo. Nuestra investigación también ha indicado que aproximadamente el 50 por ciento de los altos ejecutivos han realizado cambios significativos en los dos años anteriores y que alrededor del 50 por ciento informa que planea realizar cambios significativos durante los próximos tres años.

Estos resultados no son sorprendentes. El comportamiento de búsqueda de oportunidades se fortalece si los gerentes tienen la confianza de que comprenden los riesgos relacionados y tienen las capacidades para administrar esos riesgos. En un mundo que cambia rápidamente, los enfoques tradicionales de gestión de riesgos no serán efectivos porque están fragmentados y tratan los riesgos como eventos dispares y se compartmentan fácilmente en silos. Si bien el enfoque estricto de las actividades tradicionales de gestión de riesgos en la prevención de pérdidas no es algo malo, tampoco es lo suficientemente bueno porque las actividades no están adecuadamente integradas con la identificación, evaluación y búsqueda de oportunidades de crecimiento. Además, los enfoques actuales de gestión de riesgos están demasiado arraigados en la era de comando y control, lo que significa que es posible que no equilibren de manera efectiva el deseo de control con la necesidad de agilidad, capacidad de respuesta y cooperación multifuncional.

La conclusión inevitable es que el estado actual de la gestión de riesgos no es propicio para infundir la confianza necesaria en la alta dirección de que todos los riesgos comerciales potencialmente significativos están identificados y gestionados. Un enfoque de toda la empresa para la gestión de riesgos comerciales ayudará a los ejecutivos a enfrentar los desafíos que enfrentan al mejorar el vínculo de riesgo y oportunidad durante el proceso de establecimiento de estrategias y posicionar la gestión de riesgos como una habilidad diferenciadora en la gestión del negocio.

#### 42. ¿Cómo debería la dirección ejecutiva evaluar la ERM?

El marco COSO proporciona información sobre la cuestión de cómo la dirección ejecutiva evalúa la aplicación de ERM dentro de la organización. Las cuatro categorías de objetivos, el alcance de la aplicación (a través de la entidad y sus divisiones y unidades de negocio) y los ocho componentes de ERM, según lo define el marco COSO, proporcionan la base para esa evaluación. La gerencia debe evaluar la infraestructura de ERM adecuada que la organización necesita para realizar la visión, las metas y los objetivos de gestión de riesgos elegidos. El caso de negocios proporciona la justificación económica para proceder con una solución ERM. Una vez que se aprueba el caso de negocios, el diseño y la implementación de las capacidades que brindan la solución deseada por la gerencia se reducen a un plan de proyecto que hará que la solución ERM suceda en el marco de tiempo seleccionado por la gerencia. Los factores clave de éxito articulados en el caso comercial se utilizan para evaluar la solución ERM a lo largo del tiempo. En nuestra respuesta a la pregunta 136 se proporcionan ejemplos de medidas de éxito.

#### 43. ¿Cuál es el papel del CIO en un entorno ERM?

Cada solución ERM se ve afectada por la tecnología de varias maneras. Las soluciones de software empresarial son herramientas de información que actúan como habilitadores de ERM, en particular para fines de gestión de riesgos no financieros. A medida que las empresas configuren los sistemas de toda la empresa para que funcionen sin problemas con los sistemas de medición de riesgos, consolidarán mucha más información. Dependiendo de la complejidad e importancia estratégica de estos sistemas

y el número de partes interesadas internas involucradas, el CIO puede desempeñar un papel clave en esta transición.

Además, una solución ERM puede proporcionar los medios para que el CIO ejerza una influencia considerable sobre la gestión de riesgos críticos de TI en toda la empresa. El interés del CIO en ERM se deriva de los problemas generales de gobierno relacionados con las operaciones de TI, los procesos que afectan a TI, los diversos propietarios de aplicaciones y datos en toda la organización y la necesidad de eliminar brechas y superposiciones en la propiedad de los riesgos relacionados con TI. El CIO está en la posición de establecer el tono para la gestión de riesgos de TI en toda la empresa al instruir a los gerentes de unidades de negocios y propietarios de procesos sobre cómo comprender, evaluar y administrar los riesgos y controles de TI, y abordar de manera oportuna cualquier problema de control de TI no resuelto. .

44. ¿Cuál es el papel de la tesorería y los seguros en un entorno ERM?

Los tesoreros y los administradores de riesgos asegurables son partes interesadas vitales desde el punto de vista de la gestión de riesgos. Gestionan exposiciones e incertidumbres relacionadas con (a) activos físicos y financieros en el balance general, (b) las perspectivas de flujos de efectivo futuros esperados de las actividades comerciales principales y (c) diversas obligaciones contractuales de la empresa, entre otras cosas. Sus actividades han sido parte integral del modelo tradicional de gestión de riesgos, como se analiza en la Pregunta 6, durante décadas.

ERM no reemplaza el modelo tradicional de gestión de riesgos, sino que se basa en ese modelo y lo mejora. Desde una perspectiva de tesorería, el proceso de gestión de riesgos a menudo se ha aplicado a los riesgos financieros y de riesgo de forma aislada, ya sea por tipo de riesgo o por unidad o actividad potencialmente expuesta a los riesgos. Un programa de cobertura competente y ejecutado con eficacia ha sido un aspecto importante de las tesorerías regionales y globales competentes durante mucho tiempo, ya que el enfoque clásico de gestión de riesgos en productos y transacciones ha generado valor en muchas industrias y empresas. Por eso, el modelo tradicional de gestión de riesgos tendrá un legado duradero.

Dicho esto, una visión de toda la empresa sugiere que las personas más cercanas a los riesgos deben participar directamente en la gestión de los riesgos. Ya sea que eso signifique que asumen la responsabilidad principal de decidir, diseñar y monitorear o la responsabilidad secundaria de construir y ejecutar (según el diseño) depende de las circunstancias. Es por eso que las tesorerías de vanguardia y las funciones de administración de riesgos asegurables están adoptando una visión más amplia y estratégica del negocio, lo que lleva a sus organizaciones a un enfoque más formal y sistemático para administrar los riesgos operativos y de otro tipo. Los líderes visionarios y progresistas de tesorería, seguros, auditoría interna y otras funciones a nivel corporativo, la mayoría de las veces con el apoyo de la alta dirección, han ayudado a sus organizaciones a comprender el riesgo con mayor claridad y mejorar las capacidades de gestión de riesgos.

45. ¿Exige ERM informar a la dirección ejecutiva? Si es así, ¿qué tipos de informes son los más adecuado para la dirección ejecutiva?

La eficacia de ERM depende en gran medida de la eficacia de la información y la comunicación de la organización, que es uno de los ocho componentes del marco COSO. La presentación de informes es parte integral de este componente porque impulsa la transparencia sobre el riesgo y la gestión del riesgo en toda la organización para permitir la evaluación del riesgo, la ejecución de las respuestas al riesgo y las actividades de control, así como el seguimiento del desempeño. Sin embargo, hay muchas preguntas con respecto a la presentación de informes. Por ejemplo, ¿qué se debe informar específicamente, a quién se deben emitir los informes, con qué frecuencia deben estar disponibles los informes, cómo se utilizan los informes y qué tan detallados deben ser?

La información de gestión de riesgos se puede resumir de muchas maneras: para la empresa en su conjunto, por unidad de negocio, por unidad de riesgo, por geografía y por grupo de productos, por ejemplo. El objetivo es permitir que los tomadores de decisiones evalúen el desempeño de la gestión de riesgos mensual, semanal, diariamente o incluso en tiempo real (lo que es difícil de lograr y rara vez requerido por la dirección ejecutiva), según lo dicten la naturaleza de los riesgos y las circunstancias. Los siguientes son algunos ejemplos de informes de gestión de riesgos que sirven para proporcionar información para la toma de decisiones a la dirección ejecutiva:

- Un resumen de los riesgos de la empresa, desglosados por unidad operativa, ubicación geográfica, grupo de productos, etc.
- Un resumen de las brechas existentes en las capacidades para la gestión de los riesgos prioritarios.

- Un resumen de las inversiones con mejor y peor rendimiento y los motivos.
- A partir de un proceso de “análisis del entorno” o sistema de alerta temprana, un informe de problemas emergentes o riesgos que ameritan atención inmediata.
- Informes de valor en riesgo para evaluar la sensibilidad de las posiciones de cartera existentes a los cambios en las tasas de mercado más allá de los límites especificados, y considerar la exposición de las ganancias o el flujo de efectivo a pérdidas severas.
- Resumen de los análisis de escenarios que evalúan el impacto de los cambios en otras variables clave más allá control de la gerencia (por ejemplo, inflación, clima, actos de la competencia y niveles de desempeño del proveedor) sobre las ganancias, el flujo de caja, el capital y el plan de negocios.
- Informes de riesgo operativo que resumen las excepciones que se han producido frente a las políticas o límites establecidos (es decir, incumplimientos de límites), incluidas las averías significativas, errores, accidentes, incidentes, pérdidas (así como oportunidades perdidas) o “llamadas cercanas” y “casi accidentes”.
- Estudios especiales o análisis específicos para evaluar preguntas sobre eventos específicos o inquietudes anticipadas eso podría “detener el espectáculo”. Por ejemplo, ¿cuál es nuestra exposición en América Latina o Asia?
- Resumen de los hallazgos significativos de las auditorías de procesos comerciales realizadas por auditoría interna o revisiones realizadas por otras partes independientes, como los reguladores de la organización.
- Resumen del estado de las iniciativas de mejora. ¿Están encaminadas las iniciativas de mejora planificadas? Si no, ¿por qué?

Además de los informes anteriores, existe un panel de control o informes de cuadro de mando. Los modelos, el análisis de riesgos y las redes habilitadas para la web permiten agregar información sobre riesgos utilizando elementos de datos comunes para respaldar la creación de un tablero o cuadro de mando de gestión de riesgos para uso de los propietarios de riesgos, gerentes de unidad y ejecutivos gestión. Los informes de tablero y cuadro de mando son lo suficientemente flexibles como para permitir el diseño de informes para abordar necesidades específicas. En

las Técnicas de Aplicación del marco COSO ERM. Se discute más en la Pregunta 121.

## EL PAPEL DEL DIRECTOR

46. ¿Cómo se relacionan la ERM y la gobernanza?

Para responder a esta pregunta, necesitamos establecer un contexto. Sugerimos el siguiente punto de vista:

Los mejores en el mercado global que cambia rápidamente serán aquellos que comprendan mejor sus riesgos. y alinear su toma de riesgos con lo que mejor saben hacer. La gerencia puede utilizar la guía y la información de expertos, directores experimentados mientras trabajan para lograr este objetivo. La gobernanza es el proceso mediante el cual los directores Supervisar las decisiones y acciones de la dirección ejecutiva de manera constructiva, en consonancia con leyes y regulaciones aplicables, a medida que la gerencia formula y ejecuta estrategias para lograr objetivos Una gobernanza eficaz ofrece garantías a los inversores y otras partes interesadas clave de que la empresa conduce sus asuntos con integridad e informa su desempeño de manera justa y transparente.

Si aceptamos el punto de vista anterior con respecto a la gobernanza, entonces ERM y el proceso de gobernanza son inextricablemente vinculado. La buena gobernanza facilita la implementación de ERM porque ERM se basa en transparencia. Por el contrario, una infraestructura ERM que funcione de manera efectiva brindaría mayor confianza a la junta y a la gerencia ejecutiva que los riesgos y oportunidades están siendo identificados sistemáticamente, rigurosamente analizados y gestionados con eficacia a nivel de toda la empresa. Así, los dos van de la mano.

47. ¿Por qué los directores deberían preocuparse por si sus empresas implementan ERM?

Una encuesta trimestral de McKinsey a 1000 directores realizada en marzo de 2005 informó que los directores quieren dedicar más tiempo al riesgo y la estrategia. Según McKinsey, “este reenfoque parece reflejar tres fuerzas en el trabajo entre los directores: un déficit de conocimiento sobre la estrategia actual y futura de sus empresas, un

cierta falta de confianza en la dirección y voluntad de asumir un papel global más activo". Así directores Quiere respuestas de la gerencia a las siguientes preguntas:

- ¿Cuáles son sus riesgos críticos para la ejecución del modelo de negocio y la estrategia? ¿Cómo lo sabes?
- ¿Cómo está gestionando los riesgos críticos? ¿Son los riesgos asumidos consistentes con el riesgo de la organización? ¿apetito? ¿Cómo lo sabes?
- Cuando hay cambios significativos en los riesgos subyacentes que enfrenta la organización, ¿está informando al abordar de manera oportuna?

Si los directores desean una mayor participación en la formulación de la estrategia y la evaluación del riesgo, es probable que comiencen por trabajar con la dirección ejecutiva para entender la posición estratégica actual de la empresa tan claramente como posible. A su vez, la gerencia ejecutiva debe acomodar a la junta desarrollando y proponiendo un número de opciones estratégicas alternativas a largo plazo para la revisión de la junta. Trabajando juntos, gestión y el tablero prueba y desafía estas estrategias opcionales antes de elegir la más adecuada, teniendo en cuenta cuenta el riesgo relativo y la recompensa. ERM aumenta este proceso al garantizar la integración adecuada del riesgo.

#### 48. ¿Cómo debe ver el comité de auditoría la ERM?

ERM se enfoca ampliamente en los riesgos comerciales, mientras que el comité de auditoría históricamente ha limitado su enfoque a riesgos de información pública y financiera. Sin embargo, este enfoque limitado podría expandirse un poco con el tiempo. La Bolsa de Nueva York Los requisitos de cotización especifican que, al abordar los deberes y responsabilidades del comité de auditoría, el estatuto del comité debe establecer que el comité debe discutir las políticas de la administración con respecto al riesgo evaluación y gestión de riesgos. El marco ERM proporciona un contexto para esta discusión. Por ejemplo, un El proceso de evaluación de riesgos en toda la empresa proporciona una visión fresca de los riesgos nuevos y emergentes para la acción oportuna. y posible divulgación. Debido a que la evaluación de riesgos es un componente del control interno y la evaluación de El control interno debe basarse en el riesgo, el comité de auditoría puede querer investigar la efectividad de este proceso. Un proceso de evaluación de riesgos en toda la empresa también es un primer paso efectivo para implementar ERM.

Al analizar la evaluación de riesgos y la gestión de riesgos con la alta dirección, el comité de auditoría debe:

- Discutir la exposición de la organización a posibles eventos futuros (p. ej., pérdidas catastróficas, fraude, actos ilegales, litigios, etc.) que podrían afectar su imagen de marca y reputación.
- Comprender la evaluación de la administración de los riesgos de la información financiera y preguntar a los auditores externos si estar de acuerdo con esa apreciación.
- Comprender los puntos débiles relacionados con la información financiera que dan lugar a riesgos significativos, por ejemplo, la reservas, contingencias, valuaciones, cálculos y áreas de divulgación que requieren juicio significativo.
- Comprender el alcance de la autoevaluación y el monitoreo a nivel de entidad y de proceso para gestionar el riesgo de información financiera.
- Comprender la evaluación del riesgo del auditor interno y el plan de auditoría basado en esa evaluación.
- Indagar si existen gestores encargados de identificar, evaluar, gestionar y monitorear los riesgos críticos, y si el comité debe reunirse de vez en cuando con esos gerentes para discutir las implicaciones de sus actividades para la información pública y financiera.
- Comprender los resultados de las evaluaciones de riesgo empresarial de la gerencia y las implicaciones para el público y informes financieros.

Por supuesto, el comité de auditoría puede ampliar las actividades anteriores para abordar otros aspectos de la evaluación de riesgos y gestión de riesgos; sin embargo, la mayoría de los comités se centran y tienen las manos ocupadas con el público y problemas de información financiera. Por lo tanto, ese enfoque se enfatiza en los puntos anteriores. Otros comités de la junta, como el comité de finanzas o un comité de riesgo designado, puede enfatizar otros riesgos comerciales a través de sus respectivas actividades.

49. ¿Cómo debe la junta ejercer la supervisión de la implementación de ERM?

En el Resumen Ejecutivo del marco ERM, COSO establece lo siguiente:

El consejo debe discutir con la alta dirección el estado de la gestión del riesgo empresarial de la entidad. y proporcionar supervisión según sea necesario. El directorio debe asegurarse de estar informado de los riesgos más significativos, junto con las acciones que está tomando la administración y cómo está asegurando una administración eficaz del riesgo empresarial.

Así como una empresa necesita un proceso para adquirir materiales de calidad a un costo competitivo de sus proveedores, también necesita un proceso para gestionar y reducir sus riesgos a un nivel aceptable. Sin un proceso, la gestión de riesgos es una actividad reactiva ad hoc que está fragmentada en toda la empresa. Con el propósito de inculcar la disciplina para mejorar continuamente las capacidades de la organización en torno a la gestión de sus riesgos prioritarios, ERM infraestructura ofrece una alternativa. Porque conduce a capacidades de gestión de riesgos que son repetitivas, definido y administrado, ERM puede ayudar a la junta a comprender mejor el apetito de riesgo de la administración y en Ganar confianza en los informes de la administración sobre el riesgo y el desempeño de la gestión de riesgos.

La supervisión anticipada y proactiva requiere un fuerte énfasis en la participación directa de la junta en la política establecimiento, evaluación de riesgos y formulación de estrategias. A través de las actividades de sus diversos comités, juntas mejorar la calidad del proceso de supervisión agregando valor a la evaluación de la administración de la organización riesgos Una vez que los riesgos son identificados y originados, las juntas deben asegurarse de que la administración evalúe el opciones para gestionar los riesgos críticos, lo que lleva a políticas que aclaran responsabilidades, autoridades y responsabilidades Por ejemplo, entre otras cosas, la junta debe cerciorarse de que:

- Se fomenta y recompensa el crecimiento y la innovación sin crear una exposición inaceptable al riesgo.
- El apetito por el riesgo inherente al comportamiento de búsqueda de oportunidades de la organización en el desarrollo de nuevos productos y nuevos mercados se aclara, entiende y gestiona.
- Los límites y límites definidos excluyen claramente comportamientos y acciones que están fuera de la estrategia y inaceptable.
- Las medidas de desempeño y los objetivos no fomentan un comportamiento excesivamente arriesgado.
- Cuando se seleccionan las estrategias, se toma una visión de toda la empresa, en lugar de una unidad más estrecha o una visión funcional. optimizar el riesgo y la recompensa para la empresa en su conjunto.
- Existen controles internos y controles y contrapesos efectivos en las áreas de alto riesgo.

La supervisión eficaz también es reactiva e interactiva. La junta debe determinar que la administración tiene en su lugar el capacidades apropiadas para ejecutar respuestas de riesgo aprobadas. La propiedad del riesgo y la responsabilidad personal deben ser suficientemente enfocados para que se diseñen e implementen los procesos adecuados de gestión y control de riesgos por personal competente. Propietarios del riesgo: el individuo, el grupo, la función o la unidad autorizada para realizar tomar decisiones y tomar medidas dentro de los límites establecidos para gestionar uno o más riesgos prioritarios – debe designarse en un manera oportuna para que cada riesgo clave tenga un nombre. Para los riesgos críticos, las capacidades existentes a menudo deben estar en un mayor estado de madurez que las capacidades para riesgos menos significativos. Por lo tanto, la junta debe asegurarse de que la dirección determina que se asignan suficientes recursos a la gestión de estos riesgos.

A continuación se proporcionan ejemplos de las preguntas que los directores pueden hacer a la gerencia sobre ERM.

Con respecto a la estrategia:

- ¿Involucra la gerencia al directorio de manera oportuna durante el proceso de formulación de la estrategia y discutir el apetito de riesgo de la gerencia?
- ¿Involucra la gerencia a la junta cuando toma decisiones para aceptar o rechazar riesgos significativos?

- ¿Está la empresa asumiendo riesgos significativos que el directorio no comprende (p. ej., si una unidad operativa o grupo de productos está obteniendo rendimientos superiores en relación con los competidores, ¿se debe a que toma significativamente más riesgos que los competidores)?
- ¿Los riesgos críticos inherentes al modelo de negocios de la organización son completamente entendidos y gestionados por personal con los conocimientos, habilidades, herramientas e información necesarios? ¿Cómo lo sabes?
- ¿La junta comprende los riesgos comerciales prioritarios y cómo se abordan esos riesgos?
- ¿Están los riesgos clave de la empresa en una lista? ¿Está actualizada la lista?
- ¿Hay suficiente tiempo durante las reuniones de la junta para discutir los riesgos clave y si hay riesgos significativos? lagunas en las capacidades para gestionar esos riesgos?

Con respecto a la política:

- ¿Cómo fomenta y premia la dirección el crecimiento y la innovación sin crear problemas inaceptables? exposición al riesgo? Por ejemplo, ¿existen fronteras y límites definidos que especifiquen claramente los comportamientos que están fuera de la estrategia y fuera de los límites?
- ¿Están equilibradas las actividades empresariales y las actividades de control de la empresa de manera que ninguna demasiado desproporcionadamente fuerte en relación con el otro? ¿Son los riesgos inherentes a la búsqueda de oportunidades comportamiento entendido y manejado? ¿Cómo lo sabes?

Con respecto a la ejecución:

- ¿Comprende la gerencia las incertidumbres inherentes a sus estrategias para lograr los objetivos de negocio? objetivos y metas de desempeño? ¿Cómo lo sabes?
- ¿Existen garantías adecuadas de que las respuestas a los riesgos y las actividades de control relacionadas y la información y los procesos de comunicación están operando de manera efectiva? ¿Cómo lo sabes?
- ¿Existen planes de contingencia efectivos para responder en caso de una crisis? ¿Cómo lo sabes?
- ¿Existe un sistema de alerta temprana o un panel de control del equipo ejecutivo para los riesgos de "misión crítica"?
- ¿Existen procesos efectivos para identificar continuamente el riesgo, medir su impacto y evaluar el riesgo? capacidades de gestión (por ejemplo, las actividades de control relacionadas, los procesos de información y comunicación, y actividades de seguimiento)? ¿Cómo lo sabes?
- ¿Existen gerentes responsables de identificar, evaluar y gestionar los riesgos críticos a quienes los directores debe reunirse de vez en cuando?

Con respecto a la transparencia:

- ¿Existe un proceso eficaz para la presentación de informes fiables sobre los riesgos y el desempeño de la gestión de riesgos? Como hacer ¿sabes?
- ¿Existe una estructura organizativa que respalde el proceso de elaboración de informes de gestión de riesgos? Cómo ¿Sabes?

El propósito de la junta al dirigir preguntas a la gerencia con respecto a la gestión de riesgos es comprender los riesgos a los que se enfrenta la organización en el contexto de los objetivos de negocio establecidos y determinar si la entidad cuenta con las estrategias y capacidades adecuadas para gestionar sus riesgos clave. El MRE COSO. El marco proporciona una excelente herramienta de evaluación comparativa para que los directores la utilicen para dirigir y enfocar su supervisión. actividades relacionadas con la gestión de riesgos. Esta evaluación debe realizarse al menos una vez al año.

Con el tiempo, la mejor manera de involucrar a la junta es a través de la información. Esto no significa necesariamente proporcionar al directorio los mismos informes preparados para la gerencia ejecutiva. Si bien por regla general el riesgo

información de gestión dada a la junta no debe ser demasiado detallada, el nivel de granularidad a menudo es una cuestión de preferencia personal. El objetivo de los informes de gestión de riesgos al directorio es Directores de posición para ejecutar su función de supervisión. Los siguientes son algunos ejemplos de informes de gestión de riesgos que ayudará a alargar la memoria de la placa:

- Un resumen de alto nivel de los principales riesgos para la empresa en su conjunto, desglosados por unidad operativa, ubicación geográfica, grupo de productos, etc., junto con brechas significativas en las capacidades de gestión de riesgos
- Un resumen de las inversiones con mejor y peor desempeño y las razones por las cuales
- Informe de problemas emergentes o riesgos que requieren atención inmediata
- Resumen de eventos de riesgo significativos, por ejemplo, excepciones significativas versus políticas o límites establecidos
- Resumen de cambios significativos en variables clave fuera del control de la gerencia (por ejemplo, tasas de interés, tipos de cambio, etc.) y el efecto sobre las ganancias, el flujo de caja, el capital y el plan de negocios
- Resumen del estado de las iniciativas de mejora

Algunos de estos informes pueden ser similares a los informes recibidos por la gerencia ejecutiva, como se describe en nuestro respuesta a la pregunta 45.

## EL PAPEL DEL DIRECTOR DE RIESGOS

50. ¿Nuestra organización debe tener un director de riesgos (CRO) y, de ser así, cuál es su función?

Como campeón de ERM, el CRO facilita la ejecución del proceso y la infraestructura de ERM. su papel puede ser consultivo (evaluar y recomendar) o autoritario (aprobar) o ambos, dependiendo del riesgo área. Con la asistencia de una función de personal (la función de gestión de riesgos comerciales (BRMF) descrita en Pregunta 56), el CRO apoya a la junta (o a un comité de la junta designado), al director ejecutivo, al ejecutivo (o un comité de gestión de riesgos designado) y los gerentes de la unidad de negocio y de la unidad de apoyo. El CRO:

- Establece y comunica la visión de ERM de la organización.
- Trabaja con un grupo autorizado de altos ejecutivos para definir el rol apropiado de riesgo gestión en la organización.
- Ayuda a la alta dirección a comunicar esa función a la organización.
- Determina e implementa una infraestructura ERM adecuada.
  - Ayuda a la gerencia a integrar la gestión de riesgos con el proceso de gestión estratégica.
  - Desarrolla y comunica las políticas y límites de gestión de riesgos, según lo aprobado por el CEO y el comité ejecutivo (o un comité de gestión de riesgos designado).
  - Identifica brechas de propiedad del riesgo y superposiciones que requieren resolución para garantizar la propiedad adecuada de la riesgos prioritarios. Supervisa las acciones planificadas para llenar los vacíos y aclarar las superposiciones, trabajando con el comité ejecutivo (o comité de gestión de riesgos designado) según lo dicten las circunstancias.
  - Trabaja con los ejecutivos apropiados para establecer el ambiente de control que (1) monitorea el riesgo a través la empresa, (2) supervisa y hace cumplir las políticas y límites de gestión de riesgos, (3) inculca la disciplina para cerrar brechas significativas en las capacidades de gestión de riesgos y (4) asegura que la cultura organizacional los problemas se gestionan con eficacia.
  - Asiste al CEO y al comité ejecutivo (o un comité de gestión de riesgos designado) con seguimiento de los riesgos críticos de la empresa.
  - Dirige la BRMF (ver Pregunta 56) con respecto a (a) la recopilación, agregación, resumen y evaluación de los puntos de datos obtenidos de las unidades de negocio y las unidades de apoyo (consulte la Pregunta 56) con respecto a

desempeño de la gestión de riesgos y exposiciones a posibles eventos futuros, y (b) el montaje y distribución de informes de gestión de riesgos. •

Establece, comunica y facilita el uso de metodologías, herramientas y técnicas

- Establece marcos propicios, como un lenguaje común de riesgos, con los que facilitar la recopilación, análisis, síntesis e intercambio de datos, información y conocimiento.
- Valida las metodologías de medición existentes para determinar la integridad de los datos subyacentes y la fiabilidad de los informes.
- Facilita el intercambio de las mejores prácticas de gestión de riesgos en toda la empresa.
- Facilita las evaluaciones de riesgos en toda la empresa y supervisa las capacidades en torno a la gestión de la prioridad riesgos en toda la organización.
  - Coordina la aplicación de la evaluación de riesgos en toda la organización para obtener una visión de toda la empresa de riesgo
  - Facilita periódicamente evaluaciones en toda la empresa de políticas, procesos, competencias, informes y sistemas para identificar brechas significativas en las capacidades en torno a la gestión de riesgos críticos.
  - Trabaja con unidades de negocio y unidades de soporte (ver Pregunta 56) para establecer, mantener y continuamente mejorar las capacidades de gestión de riesgos en toda la empresa.
  - Según lo solicitado, consulta y asiste a los gerentes de las unidades de negocio y las unidades de soporte (ver Pregunta 56) durante su evaluación del riesgo y formulación de respuestas al riesgo.
  - Lleva a cabo educación y capacitación en gestión de riesgos de vez en cuando.
- Implementa informes de riesgo apropiados para la junta, el comité de auditoría y la alta gerencia.
  - Desarrolla metodologías de medición y métodos de seguimiento, que agregan exposiciones al riesgo y rendimiento de la gestión de riesgos a nivel de toda la empresa.
  - Apoya la presentación de informes de exposiciones al riesgo y el seguimiento de los resultados al directorio, al director ejecutivo y al ejecutivo (o un comité de gestión de riesgos designado).
  - Asiste al CEO y al comité ejecutivo (o un comité de gestión de riesgos designado) con decisiones de asignación de capital y recursos.

Ser verdaderamente objetivo y posicionado efectivamente dentro de la organización para mejorar la apariencia de objetividad, el CRO debe estar aislado e independiente de las operaciones de la unidad de negocio. Sin embargo lo es no es inusual que una o más unidades de riesgo (ver Pregunta 56) informen al CRO si él o ella es responsable de gestión global de determinados riesgos.

Además de las actividades anteriores, el CRO también puede proporcionar una visión independiente con respecto a los proyectos propuestos, planes de negocios y transacciones. El CEO y la junta a menudo desean una evaluación objetiva de que los riesgos resultantes de una transacción o trato se desglosan en sus componentes fundamentales con una visión equilibrada para que puedan ser medidos y evaluados y gestionados sistemáticamente. La dirección ejecutiva y los directores deben Esté atento a los gerentes que ven el mercado a través de lentes "color de rosa" para completar una transacción. sin considerar sus méritos o consecuencias para la empresa en su conjunto. Es por eso que algunas empresas pueden establecer una unidad de control o supervisión de riesgos estratégicos dirigida por un CRO independiente de las unidades de negocio.

Una unidad de control o vigilancia de riesgos estratégicos trabaja con las unidades operativas para desagregar los planes de negocios y transacciones en los riesgos componentes que la organización está asumiendo. Con base en ese entendimiento, el unidad puede entonces recomendar cómo mejorar los planes y transacciones propuestos mitigando algunos de los exposiciones a la baja que presentan obstáculos potenciales. Esta es la función ideal de una estructura de supervisión: algún individuo, grupo o comité que actúa como una unidad de riesgo para ayudar a las unidades operativas a separar las cosas y comprender los temas importantes y la esencia de lo que podría suceder, y luego rápida y

comunicar sucintamente esa comprensión. El objetivo es mejorar los planes de negocio propuestos y transacciones por lo que es más probable que tengan éxito en la creación mientras protegen el valor de la empresa. Los medios por los cuales se cumple este rol, ya sea por un CRO, por una unidad de riesgo estratégico independiente o por algún otro grupo, corresponde a la alta dirección decidir.

51. ¿Cuáles son los conjuntos de habilidades del CRO?

Las CRO exitosas tienen varios atributos comunes. Tienen la capacidad de operar con eficacia y ganar respeto en todos los niveles del negocio, ya sea con los directores y el CEO o con la unidad de negocio y los gerentes de unidad y empleados. Tienen un amplio conocimiento de todas las áreas clave del negocio. Buenas CRO no se sienten intimidados por la jerarquía y la posición dentro de la organización, y obtienen su influencia a través de una comunicación activa de cuatro vías y estilo de intercambio de conocimientos.

Los CRO son altos ejecutivos con al menos 12 a 15 años de experiencia. Poseen los siguientes conjuntos de habilidades:

- Son capaces de pensar estratégicamente, es decir, poseen la autoridad y los recursos para monitorear la desempeño de las unidades de riesgo y los propietarios del riesgo en asuntos de importancia para la empresa en su conjunto.
- Comprenden que las organizaciones deben asumir riesgos para competir y prosperar en el mercado global.
- Tienen excelentes habilidades de comunicación y facilitación.
- Son capaces de organizar y motivar a otros, quienes en muchos casos pueden estar en una posición más alta.
- Tienen la capacidad de trabajar con todos los niveles de gestión.
- Tienen una fuerte presencia y pueden interactuar eficazmente con la alta dirección.
- Tienen experiencia previa informando a juntas y comités de auditoría.
- Al articular sus evaluaciones, son concisos y directos bajo fuego en sus comunicaciones con altos directivos y directores.
- Pueden analizar con eficacia cantidades significativas de datos e información, y desglosarlos hasta los puntos clave que ayudan a la alta dirección a analizar el riesgo en una situación dada.
- También tienen la capacidad de acumular, resumir e interpretar informes de riesgo de las unidades de negocio, unidades de riesgo, unidades de apoyo y unidades de aseguramiento (ver pregunta 56).

La experiencia previa en auditoría, evaluación de riesgos o gestión de riesgos es una ventaja.

52. ¿A quién reporta el CRO?

Si la gerencia desea nombrar un CRO, él o ella debe estar posicionado dentro de la organización para mejorar su objetividad, tanto de hecho como en apariencia. A menudo, el CRO es el máximo campeón de ERM, ya que es aplicado a todas las unidades y divisiones de la empresa. Como campeón del proceso de ERM, el CRO no tiene responsabilidad en la gestión de riesgos específicos, pero opera en un papel consultivo y de colaboración, con autoridad conferida por el comité ejecutivo (o un comité de gestión de riesgos designado), el director ejecutivo o la junta (o un comité de la junta). Si bien este modelo se puede esbozar de muchas maneras, la consulta y el enfoque de campeón de proceso colaborativo es el que muchas organizaciones generalmente están adoptando en práctica, principalmente debido a limitaciones culturales. La variante principal en la práctica es si el CRO reporta al CEO, a otro alto ejecutivo (es decir, el CFO) o al comité ejecutivo (o a un comité de gestión de riesgos designado). También estamos viendo algunos CRO con líneas punteadas que informan al comité de auditoría (o a un comité de gestión de riesgos, si existe) de la junta.

---

## LA ESTRUCTURA DE SUPERVISIÓN DE LA GESTIÓN DE RIESGOS

53. ¿Cuál es el objetivo principal de la estructura de supervisión de la gestión de riesgos?

Una estructura de supervisión que funcione eficazmente incorpora varios de los elementos de la infraestructura de ERM presentados en nuestra respuesta a la Pregunta 37. Una estructura de supervisión logra muchas cosas. Por ejemplo:

- Proporciona dirección para la asignación de recursos (como capital) a las actividades de gestión de riesgos.
- Facilita el desarrollo del apetito por el riesgo de la organización y reafirma ese apetito por el riesgo, según lo aprobado por el directorio y la gerencia ejecutiva, en conjunto con sus actividades de supervisión.
- Establece la infraestructura ERM adecuada para la organización, incluidas las políticas de riesgo, métricas, informes y seguimiento.
- Asegura que los propietarios de riesgos apropiados sean designados oportunamente.
- Determina que los recursos y el personal son suficientes, que existen incentivos para los comportamientos deseados y que las prácticas de contratación, retención y capacitación funcionan según lo previsto.
- Se asegura de que los gerentes en todos los niveles estén cooperando y sean participantes activos en el ERM proceso.
- Delinea las funciones y responsabilidades específicas relativas a la asunción de riesgos frente a la supervisión de riesgos.
- Brinda seguridad de que los planes de comunicación son coherentes y se ejecutan adecuadamente.

La estructura de supervisión de la gestión de riesgos facilita la mejora continua de las capacidades de la organización en torno a la gestión de sus riesgos prioritarios. La estructura de supervisión, guiada por metas, objetivos y políticas de gestión de riesgos, tiene por objeto ayudar a los directores y al director general a equilibrar la asunción de riesgos de la organización con su apetito por el riesgo. El desafío de la gerencia es mantener en equilibrio el lado empresarial y el lado de control de la empresa y evitar que cualquiera de estas dos actividades gane un grado de fuerza desproporcionado en relación con la otra. La actividad empresarial desenfrenada y desenfocada conduce a una asunción de riesgos excesivos y a un comportamiento poco ético. Un énfasis excesivo en el control conduce a un comportamiento disfuncional y de aversión al riesgo. Ninguno de estos extremos es tan deseable como un equilibrio razonable.

El objetivo final de mejorar continuamente las capacidades de gestión de riesgos y lograr el equilibrio es proteger y mejorar el valor de la empresa. Por ejemplo, si el lado de generación de negocios de la organización asume riesgos sin tener en cuenta el apetito de riesgo de la entidad, es posible que no preste atención a las señales de advertencia colocadas por el lado de control. Eso puede hacer que una unidad de negocios, así como toda la organización, se metan en muchos problemas muy rápidamente. Por el contrario, si el lado del control de la organización se convierte en la pesadilla de todos los negociadores, sofocará la creatividad y la asunción de riesgos empresariales que conlleva ser un jugador exitoso en el mercado. Debido al cambio constante en el entorno operativo, las condiciones extremas y fuera de balance son indeseables, independientemente de si la empresa tiene un apetito de riesgo bajo o alto.

54. ¿Cómo se consideran los temas de compensación al organizar la supervisión de la gestión de riesgos?  
¿estructura?

Si bien las respuestas claras a esta pregunta son esquivas debido a la importancia de los hechos y circunstancias de la organización, podemos señalar algunos de los problemas. A menudo hay una mirada de problemas de compensación que deben abordarse para asegurarse de que ni el lado empresarial ni el lado de control de la organización se adelanten demasiado el uno al otro.

Por ejemplo, si el lado de control es un grupo de "negativos" que no son particularmente creativos para hacer que los buenos tratos sean mejores o los tratos marginales buenos, no serán respetados ni utilizados de manera efectiva por los "negociadores". Si detienen constantemente nuevas oportunidades comerciales sin descubrir formas de solucionar los problemas, no se considerarán como valor agregado. Por otro lado, si los gerentes de unidad se enfocan en cerrar tratos a cualquier costo y no hay controles y equilibrios, la organización puede estar expuesta a

riesgo inaceptable. Debido a que la compensación es un determinante crítico del comportamiento, los problemas de compensación deben ser cuidadosamente considerado. Idealmente, la CRO necesita ser independiente y objetiva sin un interés creado en si se aprueban planes de negocios, acuerdos y transacciones. Por ejemplo, la compensación de incentivos de la CRO podría estar relacionado con el desempeño general de la empresa.

El comportamiento se ve fuertemente influenciado cuando la rendición de cuentas por los resultados está vinculada al sistema de recompensas. En consecuencia, en gestión de riesgos, es importante que las expectativas de desempeño creen incentivos para "resultados" equilibrados, es decir, "la producción sin calidad" no debe ser el objetivo. Con un enfoque equilibrado en producción, calidad, costo y tiempo, los gerentes tienen fuertes incentivos para establecer objetivos realistas, comprender los riesgos y adoptar medidas objetivas.

Aún así, quedan preguntas: ¿Cómo se recompensa a los gerentes? ¿Debería recompensarse a la organización de control por permitir más negocios para completar con éxito, o debería ser un muro que no se puede traspasar? Al mismo tiempo, ¿Se debe recompensar a los gerentes de las unidades de negocios por tener una visión más amplia de toda la empresa o por tomar una decisión empresarial? perspectiva de la unidad? Estas son preguntas importantes porque la forma en que los gerentes de las unidades de negocios y los llamados "los artistas" son compensados pueden generar un estilo de gestión arrogante y de confrontación y una "cultura guerrera" en el que los ejecutivos compiten entre sí para obtener la mayor cantidad de capital posible asignado a su unidad iniciativas, independientemente de las consecuencias para la empresa en su conjunto. Estos gerentes pueden volverse peligrosos a medida que buscan nuevas fuentes de negocios sin una visión equilibrada de toda la empresa en cuanto a las desventajas y como al alza y, al hacerlo, podrían superar significativamente el apetito por el riesgo de la entidad tal como se entiende y aprobado por la junta. Por lo tanto, tener una visión independiente del riesgo, ya sea a través del ejecutivo comité, un CRO o una unidad de riesgo independiente – es especialmente vital para gestionar el riesgo, en toda la empresa, dentro del apetito de riesgo establecido. Con respecto a los informes de riesgo, una CRO o una unidad de riesgo independiente puede aumentar la proceso de gobierno al hacer posible una "memoria más larga" en el CEO y la junta y crear una fuerte responsabilidad de las unidades operativas para cumplir con los resultados prometidos.

#### 55. ¿Existe una estructura de supervisión organizacional recomendada?

Como se señaló en la Pregunta 53, la estructura de supervisión de la gestión de riesgos facilita la mejora continua de la capacidades de la organización para administrar sus riesgos prioritarios y ayuda a los directores y al CEO a asignar recursos y equilibrar la asunción de riesgos de la organización con su apetito por el riesgo. No hay una talla para todos estructura para lograr estos objetivos.

Hay modelos organizativos alternativos. Las técnicas de aplicación del marco COSO ilustran enfoques alternativos, junto con los beneficios y desafíos relacionados. El principal diferenciador entre los alternativas radica en las respuestas a las siguientes preguntas:

- ¿Quién es responsable de identificar, evaluar y responder al riesgo?
- ¿Se hace de forma centralizada?
- ¿Lo hacen las distintas unidades de la organización?
- ¿Se realiza tanto a nivel central como por unidades de la organización?

Según las Técnicas de Aplicación:

Muchas empresas descubren que, a medida que crecen en tamaño y complejidad, pueden aplicar con mayor eficacia principios y disciplinas de gestión de riesgos empresariales al empujar gran parte, si no toda, la responsabilidad al líneas de negocio y unidades funcionales de soporte. Al mismo tiempo, una pequeña infraestructura central de apoyo aborda los riesgos más generalizados de toda la entidad.

El Marco Integrado de Gestión de Riesgos Empresariales de COSO fue diseñado para aplicarse a todo tipo de entidades: públicas y privadas, pequeñas y grandes, con fines de lucro y sin fines de lucro. Así que el marco fue diseñado para proporcionar un enfoque basado en principios en lugar de establecer reglas rígidas.

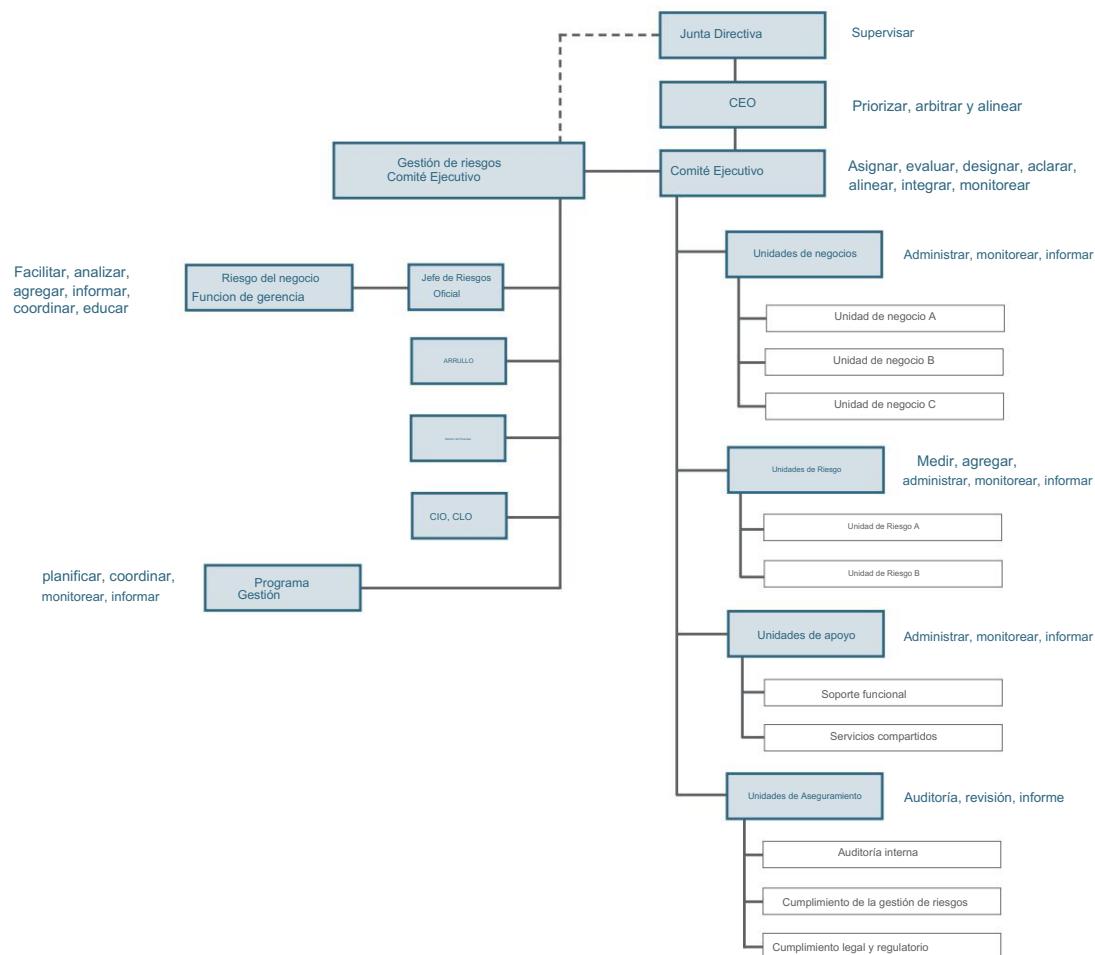
Si bien seleccionar la estructura organizativa adecuada es más un arte que una ciencia, debe existir una estructura de toma de decisiones para superar el atasco de brechas y superposiciones en la gestión de riesgos. responsabilidades que existen en muchas organizaciones. La clave es aprovechar la estructura de gestión existente y tener en cuenta el modelo de negocio, los objetivos, la cultura y el apetito por el riesgo de la entidad. para los más pequeños organizaciones, la estructura de supervisión puede ser tan simple como el comité ejecutivo ejerciendo su función gerencial prerrogativa para identificar y priorizar riesgos, asignar propietarios de riesgos, analizar brechas, aprobar planes de acción y monitorear resultados. Para organizaciones más grandes y complejas, un director de riesgos y/o un ejecutivo de gestión de riesgos puede ser necesario un comité. La pregunta 56 proporciona información sobre las posibles piezas del rompecabezas y proporciona algunas preguntas de diagnóstico a tener en cuenta al seleccionar la estructura organizativa adecuada.

#### 56. ¿Cómo se relaciona la estructura de supervisión de la gestión de riesgos con el sistema organizativo existente de la entidad? ¿Estructura?

Se necesita una estructura de supervisión organizacional para supervisar la gestión de riesgos. Porque una supervisión eficaz estructura a menudo incluye un comité de la junta, un comité de trabajo de la alta dirección, un alto ejecutivo responsable de ERM, estatutos formales y descripciones de trabajo, y autorizaciones claras y líneas de informes, debe integrarse con las estructuras y procesos de gestión existentes. La estructura de supervisión aclara la problemas de propiedad del proceso para que todos los que importan, de arriba a abajo en la organización, también tengan un papel que desempeñar en la gestión del riesgo.

##### Una estructura de supervisión de referencia

Una estructura de supervisión de referencia nos ayuda a comprender los elementos potenciales de la estructura de supervisión y cómo está integrado dentro de la organización existente.



El esquema de la página anterior ilustra cómo se puede integrar ERM dentro de la organización existente. Describe cómo los directores, los altos ejecutivos, las unidades y las funciones desempeñan un papel fundamental en el funcionamiento de la infraestructura de ERM. Al ver el esquema, reconozca que las unidades de negocios, las unidades de soporte y las unidades de aseguramiento ya existen en la mayoría de las organizaciones. Por otro lado, las unidades de riesgo pueden existir o no, y brindan una alternativa para que la gerencia considere.

Los elementos esenciales de la estructura organizativa, como se ilustra en el esquema anterior, y las funciones y responsabilidades relacionadas con ERM en toda la organización se analizan a continuación.

- La Junta Directiva proporciona una función de supervisión, con énfasis en la comprensión de los riesgos prioritarios, la aprobación de políticas de gestión de riesgos para riesgos críticos y la determinación de que las respuestas de riesgo para esos riesgos sean efectivas. Esta actividad de supervisión también puede ser realizada por el comité de auditoría, por un comité de gestión de riesgos (si lo hay) y por otros comités (como el comité de finanzas).
- El Gerente General es el “ejecutivo de riesgo integral”. Él/ella es responsable en última instancia de las prioridades de ERM, estrategias y políticas, y actúa como ejecutor final en asuntos tales como alinear objetivos, estrategias y apetito de riesgo, eliminar brechas y superposiciones en las responsabilidades y autoridades de gestión de riesgos, y resolver conflictos internos significativos. El RMEC y otros componentes de la estructura de supervisión de la gestión de riesgos están diseñados para respaldar la delegación de estas responsabilidades por parte del director ejecutivo. El CEO también garantiza que la implementación de ERM se aplique en el establecimiento de estrategias.
- El Comité Ejecutivo de Gestión de Riesgos (RMEC) coordina la toma de decisiones, por ejemplo, recomienda tolerancias y perfiles de riesgo al director ejecutivo y al directorio en el contexto de la estrategia comercial de la empresa. Evalúa metodologías de medición de riesgos. Establece marcos de asignación de capital. Desarrolla políticas de riesgo y estructuras de límites para toda la empresa y específicas. Asigna propietarios de riesgos significativos. Evalúa la eficacia de la infraestructura existente para gestionar riesgos específicos y garantiza que se realicen las mejoras necesarias para cerrar las brechas. Si bien el Comité Ejecutivo podría retener estas responsabilidades para sí mismo, muchos miembros de ese comité también pueden servir en el RMEC. Un RMEC separado puede ser apropiado si hay mucho por hacer con respecto a mejorar las capacidades de gestión de riesgos. En tales casos, el RMEC supervisa el desarrollo de la infraestructura de ERM necesaria para permitirle monitorear las políticas y los límites de riesgo e informar al comité ejecutivo y al directorio sobre el cierre de brechas en torno a la gestión de los riesgos prioritarios. La RMEC ha presentado informes lineales a la junta, como se indica en el esquema, ya que garantiza que los directores reciban la información adecuada sobre los riesgos de la empresa. La junta le asigna periódicamente la tarea de dar seguimiento a consultas específicas. Puede o no asumir el rol de un comité de riesgo enfocado responsable de administrar un riesgo específico (ver la discusión de las Unidades de Riesgo en la página siguiente).
- El Director de Riesgos (CRO) es miembro del RMEC y reporta al Director General o a un alto ejecutivo de alto rango. El CRO supervisa la función de gestión de riesgos comerciales (ver más abajo) y es un campeón clave de ERM. El CRO también puede tener autoridad para administrar riesgos seleccionados a nivel de toda la empresa (consulte las Preguntas 50 a 52). Él o ella debe presidir el RMEC y tener una relación de reporte con la junta. El CRO también debe facilitar la integración de la evaluación y gestión de riesgos en los procesos normales y continuos de planificación estratégica y comercial de la organización.
- Para reunir a la parte superior de la organización y sus unidades de negocio y sus actividades, un Business Risk Management Function (BRMF) proporciona "marcos habilitadores". Estas herramientas son el lenguaje común que facilita la recopilación, el análisis y la síntesis de datos y la presentación de informes de exposiciones y resultados del proceso de forma agregada en toda la empresa. El BRMF generalmente reporta a un alto ejecutivo (es decir, un CRO) y/o al RMEC. Su estatuto generalmente es definido por el ejecutivo senior designado y/o RMEC y es aprobado por el comité ejecutivo de la organización.
- Reportando al RMEC (o al CRO), la función de Gestión de Programas proporciona la supervisión necesaria para asegurar la integración y coordinación efectivas de múltiples proyectos llevados a cabo durante el ciclo de vida del viaje de ERM. Para soluciones ERM relativamente simples, esta función será innecesaria. Para soluciones más complejas, ERM puede lograrse en etapas a lo largo del tiempo en forma de múltiples proyectos relacionados. En tales casos, puede ser necesaria una disciplina de gestión de programas. Consulte la pregunta 138 para obtener más información.

- Las Unidades de Negocio son las operaciones de línea de la empresa con objetivos, estrategias, mercados, clientes y productos. Las unidades de negocios exitosas conocen a su competencia, a sus clientes, a sus oportunidades y sus riesgos. Administran y monitorean las operaciones para generar ingresos, satisfacer clientes, aumentar la calidad, comprimir el tiempo del ciclo y reducir los costos. Ofrecen productos y servicios a segmentos de mercado objetivo a un precio suficiente para cubrir los costos y riesgos relacionados y generar rendimientos ajustados al riesgo para los accionistas. Informan de sus actividades al director general y al comité ejecutivo.

El riesgo debe ser una cuestión prioritaria para los ejecutivos de las unidades de negocio. Las unidades de negocios a menudo toman riesgos cuando introducir un nuevo producto, entrar en un nuevo mercado o invertir en una nueva iniciativa de I+D. tienen muchos exposiciones relacionadas con las relaciones con los clientes, las relaciones con los proveedores, el "grupo de talentos" de los empleados y los bienes propios que administran. Estas exposiciones y las incertidumbres que las afectan deben ser entendidos y la unidad de negocio debe tener las capacidades para gestionarlos. En esencia, primera línea la dirección de la unidad de negocio es responsable y es la primera línea de defensa contra muchos de los riesgos inherentes a su modelo de negocio elegido.

Unidades de negocios:

- Alinear sus prioridades, tolerancias y estrategias de riesgo con las políticas y pautas de toda la empresa.
- Orientar las actividades comerciales y de desarrollo de productos para crear nuevas fuentes de valor consistentes con el apetito de riesgo general de la empresa.
- Identificar, generar y medir el riesgo.
- Benchmarking de procesos y compartir mejores prácticas con el objetivo de mejorar continuamente las medidas y procesos
- Asignar responsabilidades y responsabilidades de gestión de riesgos a los gerentes clave
- Informar sobre la calidad general de las respuestas a los riesgos, las actividades de control y la información y comunicación, aplicada a riesgos específicos
- Las Unidades de Riesgo son un componente opcional de una solución ERM, y pueden o no existir ya dentro de la organización. Las unidades de riesgo gestionan riesgos específicos que son inherentes al modelo de negocio de la empresa pero que son o bien no están gestionados por las unidades de negocio o bien se gestionan de forma más eficaz en toda la empresa, coherente con una visión de cartera. El objetivo de una unidad de riesgos es hacer la gestión de riesgos relacionados con una o más riesgos una competencia central de la organización. Las unidades de riesgo pueden ser responsables de tales riesgos como riesgo de tipo de interés, riesgo de tipo de cambio, riesgo de precio de las materias primas, riesgo crediticio, riesgo meteorológico y riesgo catastrófico. Evalúan, agrupan, reducen, transfieren y explotan los riesgos de los que son responsables. Trabajan con las unidades de negocio cuando dichas unidades consideran asumir riesgos que no tienen el conocimiento y especialización para gestionar. Las unidades de riesgo son a menudo un importante contribuyente a la ejecución de los objetivos de la organización. estrategia de negocios. Pueden consistir en una función o una unidad autónoma dentro de la organización, y puede ser responsable ante un comité de riesgo enfocado de altos ejecutivos.

Por ejemplo, cuando se considera una transacción, trato o inversión propuesta (la "inversión propuesta"), el componente de riesgo de tasa de interés puede ser asignado a tesorería o a la "mesa IR", que evalúa este componente de riesgo en el contexto de la cartera de riesgo de tasa de interés agregada existente de la empresa. Eso la evaluación se convierte en una parte integral de la evaluación general del riesgo de la inversión propuesta. Si el se consuma la inversión propuesta, el componente de riesgo de tasa de interés se administra en una empresa en lugar de una transacción independiente o una base unitaria. La exposición incremental puede compensarse frente a otros riesgos de tasa en el grupo consolidado de exposiciones de tasa de interés de la empresa. o puede ser cubierto para transferir el riesgo a través de una transacción de derivados. O puede aceptarse el riesgo sin más acción para explotar el mercado como un "puro juego" sobre las tasas.

Para ser eficaces, las unidades de riesgo deben crear las capacidades necesarias para gestionar los riesgos que las unidades de negocio no tienen o no pueden administrar porque carecen de las competencias para hacerlo. Las unidades de riesgo dan soporte al modelo de negocio de crear valor empresarial al proporcionar a los directores y al CEO la seguridad de que los riesgos asumidos no exceder el apetito de riesgo de la empresa. Al hacerlo, las unidades de riesgo contribuyen significativamente a la protección de valor de la empresa. Pero si se benefician de asumir riesgos, también evolucionan al "estado de creación de valor" (por ejemplo, GMAC y GE Capital).

Las unidades de riesgo también ayudan a los gerentes comerciales a identificar y evaluar todos los riesgos y supuestos comerciales asociados con una transacción, trato o inversión propuestos. Ayudan al director general y al consejo de administración asegurándoles que las personas y las herramientas más capaces se han empleado con respecto al componente de riesgo que gestiona la unidad. Por lo tanto, las unidades de riesgo pueden encargarse de suscribir riesgos específicos asumidos por unidades de negocios con respecto a transacciones, acuerdos e inversiones específicos. Al hacerlo, se aseguran de que se adopte una visión de cartera del riesgo a nivel de toda la empresa.

- El éxito en ERM en última instancia está determinado por la medida en que los gerentes de línea y funcionales cooperan y participan activamente en el proceso. Los gerentes funcionales son responsables de las Unidades de Soporte. Gestionan actividades como recursos humanos, sistemas de información y gestión de instalaciones. Las unidades de soporte trabajan en estrecha colaboración con las unidades de negocios y las unidades de riesgo para administrar los riesgos relacionados con sus conjuntos de habilidades especializadas. Los gerentes responsables de ciertas unidades de apoyo, como el director de información y el director legal, pueden participar en el RMEC para coordinar ciertas actividades relacionadas con la gestión de riesgos para que puedan integrarse de manera más efectiva.
- Las Unidades de Aseguramiento juegan un papel importante en la validación. Incluyen el cumplimiento de la gestión de riesgos, la auditoría interna y la revisión del valor en riesgo. En algunas organizaciones, estos grupos pueden ser uno y el mismo. Realizan auditorías y revisiones periódicas o continuas para brindar garantías al RMEC y al directorio de que los procesos críticos se están desempeñando de manera efectiva, las medidas clave y los informes son confiables y las políticas establecidas cumplen. La auditoría interna, por ejemplo, está experimentando una transición porque el enfoque de auditoría tradicional basado en el cumplimiento del pasado no es lo suficientemente dinámico o prospectivo para funcionar de manera efectiva en un entorno de ERM.

Nuevamente, no estamos sugiriendo que haya nada nuevo con ninguno de los componentes anteriores. La discusión anterior proporciona un contexto para las preguntas de diagnóstico proporcionadas a continuación.

#### Muchas variaciones son posibles

Si bien no hay nada nuevo en ninguno de los componentes anteriores, los directores, ejecutivos senior, unidades y funciones participantes TODOS desempeñan un papel vital dentro de la organización en la identificación y gestión del riesgo. Toda organización debería tener ordinariamente unidades de negocio, soporte y aseguramiento. Las unidades de riesgo, por su parte, son opcionales en función de la complejidad de los riesgos inherentes al modelo de negocio.

Al evaluar la estructura de supervisión organizacional para la gestión de riesgos, existen muchas variaciones posibles. A menudo, las empresas implementan un enfoque en el que el CRO adopta un enfoque de consulta y colaboración con las unidades de negocio. Para ser eficaz, una estructura de supervisión debe estar diseñada para tener "dientes" de modo que pueda servir como "árbitro" y patrocinador para hacer avanzar a la organización hacia un entorno de ERM e inculcar el enfoque, la disciplina y el control para mejorar las capacidades de gestión de riesgos. . El acceso al CEO y al directorio cuando surgen riesgos significativos y problemas de propiedad del proceso es vital. La responsabilidad por las actividades de asunción de riesgos siempre debe deslindarse de las actividades de seguimiento y supervisión de riesgos. Por lo tanto, el director general, el comité ejecutivo y el directorio deben conferir la autoridad de supervisión a las personas apropiadas.

#### Algunas preguntas de diagnóstico a considerar

A continuación se presentan algunas preguntas a tener en cuenta al evaluar la estructura de supervisión organizacional para la gestión de riesgos. Como se señaló en la Pregunta 55, hay muchos modelos alternativos a considerar. Si bien es difícil generalizar, las distinciones entre estas alternativas se pueden resumir en términos de varios principios de diseño relacionados con las funciones y autoridades en varios niveles de la organización. Estos principios se expresan mediante las siguientes preguntas:

- ¿Cuál es el papel de la junta y el director ejecutivo? La gestión eficaz del riesgo comienza en la parte superior.
- ¿Existe la necesidad de un RMEC? ¿El comité ejecutivo tiene tiempo para concentrarse en los temas o es necesario designar un comité separado?
- Si hay un RMEC, ¿quién está en él? ¿Cuáles son sus funciones y responsabilidades? ¿Cómo interactúa el comité con el proceso de establecimiento de la estrategia?

- ¿La organización designa a un solo oficial para asumir ciertas responsabilidades generales para el riesgo? gerencia, por ejemplo, un "CRO" o un ejecutivo equivalente? En caso afirmativo:
  - ¿Es este funcionario independiente de las actividades comerciales principales?
  - Si no existe un solo oficial de riesgos, ¿existe un comité (o grupo equivalente) con responsabilidades?
- Si hay un solo oficial de riesgos O un comité de riesgos (o grupo equivalente) con responsabilidades generales para gestión de riesgos:
  - ¿A quién le reporta el oficial o comité, por ejemplo, al CEO o al RMEC?
  - ¿Cuáles son las responsabilidades generales asumidas por el oficial o comité?
  - Cuál es la naturaleza de los riesgos integrados en:
    - ° ¿La descripción del trabajo del oficial?
    - ° ¿Los estatutos del comité?
  - Si existe una RMEC, ¿cuál es su composición?
  - ¿Cuáles son las funciones y responsabilidades, tal como se resumen en la descripción del trabajo y/o estatuto?
  - ¿El rol es consultivo (evaluar y recomendar) o autoritario (aprobar) o ambos?
  - ¿Las funciones de gobierno (p. ej., auditoría interna, supervisión/cumplimiento de la gestión de riesgos y valor en riesgo) revisión) incluidas o separadas, es decir, ¿informan al oficial o comité o a otra persona o algún otro grupo?
    - ° Tenga en cuenta que la función de auditoría interna debe tener una línea de responsabilidad Comité de Auditoría.
- Si hay un solo responsable de riesgos:
  - ° ¿Existe un RMEC en funcionamiento con el que trabaje ese ejecutivo? ° ¿Hay personal de apoyo adecuado?
- ¿Cuáles son las funciones y responsabilidades de la unidad de negocio y la gestión divisional?
- ¿Cuáles son las funciones y responsabilidades de la gestión de la unidad de apoyo?
- ¿Existen riesgos únicos inherentes al modelo de negocio de la organización que requieran una o más unidades de riesgo para albergar, desarrollar y mantener las competencias necesarias para evaluarlas y gestionarlas?
- ¿Qué funciones independientes de validación y cumplimiento existen? ¿A quién reportan estas funciones? Ejemplos de tales funciones incluyen la auditoría interna, la supervisión/cumplimiento de la gestión de riesgos y el valor en revisión de riesgos.
- ¿Hay claridad en cuanto a las funciones y responsabilidades para gestionar los riesgos prioritarios?
  - ¿Sabe cuáles son sus riesgos prioritarios?
  - ¿Cómo se determina la responsabilidad por la gestión del riesgo?
  - Quién "posee" la responsabilidad de identificar, evaluar y gestionar riesgos específicos y a través de qué canales informan resultados? ¿Hay un propietario del riesgo asignado para administrar cada riesgo prioritario? (Ver Pregunta 57.)
    - ° ¿Hay vacíos (sin dueño de un riesgo) que llenar?
    - ° ¿Existen superposiciones (demasiados propietarios de un riesgo) que deben eliminarse?
  - ¿Cómo se alinean las prácticas de compensación con los comportamientos deseados?

- ¿Las tareas de gestión de riesgos están equilibradas a nivel central y local? ¿Si es así, cómo? ¿Está claro qué tareas se van a llevarán a cabo centralmente y qué tareas serán ejecutadas por las unidades de negocio?

Dependiendo de las respuestas a estas y otras preguntas relevantes, se diseña una estructura de supervisión adecuada. Recuerde: Diseñe la estructura de supervisión sobre los procesos de gestión existentes y manténgala lo más simple posible.

Si bien la discusión anterior puede parecer compleja, se proporciona para presentar los problemas involucrados en el diseño de la estructura de supervisión adecuada. Esto es necesario porque, como se señaló anteriormente, no existe una solución única para todos.

#### 57. ¿La implementación de ERM requiere la identificación de propietarios de riesgos individuales?

Sí. Ya sea a través del comité ejecutivo o RMEC (como se analiza en la Pregunta 56), la resolución de las cuestiones de propiedad del proceso para riesgos críticos es una de las tareas más importantes en la implementación de ERM.

¿Quién decide las capacidades necesarias para gestionar un riesgo dado? ¿Quién diseña estas capacidades? ¿Quién ejecuta? ¿Quién monitorea el desempeño? Es posible que la gerencia no tome las decisiones finales sobre todas estas preguntas con respecto a cada uno de los riesgos clave de la empresa, pero se asegura de que las responsabilidades, las autoridades y las responsabilidades estén definidas y articuladas claramente para que un individuo, un grupo o una unidad designada sea responsable de gestionar cada riesgo.

La persona, grupo o unidad responsable a la que nos referimos es el "propietario del riesgo". El llamado propietario del riesgo tiene la responsabilidad, la autoridad y la rendición de cuentas para gestionar el riesgo. Los propietarios del riesgo, como mínimo, deben decidir, diseñar y monitorear. Deciden sobre las respuestas al riesgo y diseñan las capacidades para gestionar los riesgos de acuerdo con la respuesta al riesgo seleccionada. Estas capacidades preferiblemente deberían abordar la fuente o las causas raíz del riesgo. El diseño específico debe considerar las políticas necesarias, el proceso específico y las actividades de control, las habilidades necesarias, los informes de gestión, las metodologías, los sistemas y los datos de apoyo. Los propietarios de riesgos supervisan estas capacidades a lo largo del tiempo para asegurarse de que funcionan según lo previsto. Si se observan lagunas, las corrigen en el momento oportuno.

Los propietarios de riesgos pueden optar por subcontratar la responsabilidad de crear y ejecutar capacidades. Sin embargo, si lo hacen, eso no compromete su propiedad del riesgo. El comité ejecutivo (o RMEC) se asegura de que se designen propietarios de riesgos para cada riesgo crítico y supervisa el desempeño de los propietarios de riesgos a lo largo del tiempo.

---

## EL PAPEL DE LA AUDITORÍA INTERNA

#### 58. ¿Qué funciones desempeña la auditoría interna en la implementación de ERM?

El director ejecutivo de auditoría (CAE) y la auditoría interna pueden desempeñar uno o más de los siguientes roles junto con la implementación de ERM en una organización:

- Educador: Muchos altos ejecutivos no entienden ERM. El DEA puede ayudarlos a comprender y utilizar el marco COSO ERM a través de la educación periódica a lo largo del tiempo. Si el DEA elige implementar el marco COSO ERM al desarrollar planes de auditoría enfocados, comunicar los resultados de la auditoría y hacer presentaciones, él o ella educará a los ejecutivos y directores en los diversos componentes de ERM.
- Facilitador: ERM requiere evaluaciones de riesgo de calidad. La auditoría interna puede desempeñar un papel de liderazgo dentro de la organización al facilitar las evaluaciones de riesgos y la formulación de respuestas a los riesgos. La auditoría interna también puede desempeñar un papel consultivo para ayudar a la organización a traducir las evaluaciones de riesgos en respuestas a los riesgos.
- Coordinador: en la medida en que la solución ERM de la organización utilice un lenguaje común y otros "marcos habilitadores", la auditoría interna puede desempeñar un papel de coordinación de valor agregado para garantizar una implementación uniforme en toda la empresa. El CAE puede ser un proponente de un lenguaje común.

- Integrador: la auditoría interna puede ayudar con (a) la recopilación, el análisis y la síntesis de datos relacionados con el riesgo alimentados de múltiples fuentes en toda la empresa y (b) el informe de exposiciones y resultados de auditoría en un base agregada de toda la empresa.
- Evaluador: Auditoría interna puede utilizar los ocho componentes del marco COSO ERM para evaluar el riesgo gerencia, ya sea para la organización como un todo o para una división, subsidiaria o unidad. Además, auditoría interna puede evaluar:
  - La efectividad del componente de Ambiente Interno, como lo define el marco COSO ERM
  - La eficacia del proceso de evaluación de riesgos, teniendo en cuenta el Objetivo-Establecimiento, Evento Componentes de identificación, evaluación de riesgos y respuesta a riesgos del marco COSO ERM
  - La eficacia de las políticas y procedimientos de control relacionados con respuestas a riesgos específicos, tal como se explica en el componente de actividades de control
  - La calidad y confiabilidad de la información y la comunicación que respaldan la gestión de la organización. respuestas de riesgo seleccionadas
  - La eficacia del seguimiento, tal como lo define el componente Seguimiento

Los roles anteriores son consistentes con las actividades de aseguramiento y consultoría previstas por The Institute of Internal Auditores (El IIA) en su definición de auditoría interna. El IIA ha afirmado el siguiente punto de vista:

Las organizaciones deben comprender plenamente que la dirección sigue siendo responsable de la gestión de riesgos. Los auditores internos deben brindar asesoramiento y cuestionar o apoyar la toma de decisiones de la administración, según opuestos a tomar decisiones de gestión de riesgos. La naturaleza de las responsabilidades de la auditoría interna debe documentarse en el estatuto de auditoría y ser aprobado por el comité de auditoría.

De acuerdo con el punto de vista anterior, el IIA ha identificado roles centrales para la auditoría interna en ERM implementación, así como roles que no son apropiados para la auditoría interna. Ejemplos de auditoría interna básica roles incluyen lo siguiente:

- Dar aseguramiento de los procesos de gestión de riesgos
- Dar seguridad de que los riesgos están correctamente evaluados
- Evaluación de los procesos de gestión de riesgos
- Evaluar el reporte de riesgos clave
- Revisión de la gestión de riesgos clave

Las funciones que el IIA ha indicado que la auditoría interna no debe asumir son:

- Establecimiento del apetito por el riesgo
- Autorizar y dictar la implementación de los procesos de gestión de riesgos
- Asumir el papel de la gerencia para brindar garantías sobre los riesgos y el desempeño de la gestión de riesgos
- Toma de decisiones sobre respuestas al riesgo
- Implementar respuestas de riesgo en nombre de la gerencia
- Aceptar la responsabilidad por la gestión de riesgos

Además, entre estos dos extremos, el IIA ha señalado que existen otras “funciones legítimas de auditoría interna”, siempre que existan las salvaguardas apropiadas. Estos roles incluyen:

- Facilitar la identificación y evaluación de riesgos
- Coaching gerencial en respuesta a riesgos

- Coordinación de las actividades de ERM
- Consolidación de la información sobre riesgos
- Mantenimiento y desarrollo del marco ERM
- Promoción del establecimiento de ERM
- Desarrollar una estrategia de gestión de riesgos para la aprobación de la junta

59. ¿Debe la auditoría interna liderar el esfuerzo de ERM?

No lo recomendamos. La gerencia implementa ERM como parte integral de las actividades de la organización.

Como se señaló en nuestra respuesta a la Pregunta 58, el DEA y la auditoría interna pueden desempeñar muchas funciones de valor agregado, incluyendo la promoción e introducción de ERM y la generación de interés en el proceso. En esencia, el CAE puede proporcionar la chispa que puede ayudar a iniciar el viaje de ERM. Sin embargo, la auditoría interna no debe funcionar en el papel de la gerencia. En última instancia, ERM debe ser impulsado desde la parte superior de la organización.

60. ¿Debe la auditoría interna integrar el marco COSO ERM en su trabajo?

Cuando se emitió COSO Internal Control – Integrated Framework en 1992, los DEA visionarios lo adoptaron como un marco para la planificación de la auditoría, la ejecución de la auditoría y la presentación de informes sobre los resultados de la auditoría. Ese marco no era requerido en ese momento, pero los DEA que lo usaron descubrieron que actualizó el enfoque de auditoría de su función y mejoraron el valor aportado a sus organizaciones a través de los resultados de auditoría que comunicaron a gerencia y la junta. Si bien el nuevo marco ERM no es un requisito ni un mandato, predicen que los CAE visionarios lo implementarán como parte de las actividades de su función tal como lo hicieron hace años con el Control Interno – Marco Integrado. Como todos estos cambios, el objetivo será aumentar el valor auditoría interna contribuye a la organización.

61. ¿Auditoría interna no ha evaluado la aplicación de ERM dentro de la organización?

No necesariamente. ERM nunca se ha definido como un estándar, bajo el debido proceso, hasta que COSO emitió el ERM estructura. En el pasado, ERM se definía como la gente elegía definirlo. En el futuro, las empresas ahora pueden comparar su visión de la gestión de riesgos con el marco COSO.

Además, muchos auditores internos han evaluado varios aspectos de la gestión de riesgos de su organización. El marco COSO ahora les da la oportunidad de echar un nuevo vistazo a su enfoque.

62. ¿Apoya el Instituto de Auditores Internos (IIA) la gestión de riesgos empresariales de COSO? marco integrado?

Sí. El IIA fue un ferviente partidario durante todo el desarrollo del marco.

63. ¿Los estándares del IIA requieren el uso de COSO Enterprise Risk Management – Integrated Estructura? Por ejemplo, ¿cuál es la relación de ERM con el Estándar IIA 2010.A1 (que requiere auditoría interna para realizar una evaluación de riesgo anual) y 2110.A2 (que requiere una amplia evaluación de riesgos alineada con el marco COSO)?

Los estándares del IIA no incluían tal requisito en el momento en que se imprimió esta publicación. El COSO Gestión de riesgos empresariales: el marco integrado proporciona información sobre los enfoques para mejorar el riesgo metodologías de evaluación. Por lo tanto, los auditores internos pueden usar el marco para aumentar su riesgo anual. metodologías de evaluación. Si la administración está implementando ERM, la auditoría interna debe incorporar este actividad en el proceso de evaluación de riesgos y planificación de auditorías. En otras palabras, una vez que una organización comienza su viaje de ERM, tiene sentido que la auditoría interna amplíe su enfoque de auditoría utilizando el marco de ERM.

Como miembro de COSO, el IIA claramente tuvo aportes y apoyó el diseño, la lógica y el espíritu del marco ERM. Por lo tanto, la aplicación del marco por parte de los auditores internos debe considerarse deseable y apropiada a la luz de los estándares IIA existentes. El estándar 2110.A2 respalda claramente los conceptos del marco.

## VISIÓN Y OBJETIVOS DE LA GESTIÓN DE RIESGOS

64. ¿Cómo desarrolla la dirección una visión compartida del papel de la gestión de riesgos en el  
¿organización? ¿Cuál es el uso práctico de una visión compartida?

El primer paso para implementar una solución ERM implica desarrollar una visión compartida del papel de la gestión de riesgos en la organización. Un grupo de trabajo de altos ejecutivos debe estar facultado para articular este papel y definir metas y objetivos relevantes para la empresa en su conjunto y sus unidades de negocio. Sobre la base de una comprensión de las unidades comerciales y los riesgos clave, esta articulación proporciona una "visión general" de cómo organizar la gestión de riesgos de la entidad y debe alinearse con los objetivos comerciales y la estrategia de la organización. Se basa en una evaluación de riesgos de toda la empresa y un análisis de brechas para los riesgos prioritarios de la organización.

Por lo tanto, la "visión de gestión de riesgos" es una visión compartida del papel de la gestión de riesgos en la organización y las capacidades deseadas para gestionar sus riesgos clave. Se evalúa periódicamente con el espíritu de mejora continua. Para que sea útil, la visión de la gestión de riesgos debe basarse en capacidades específicas que deben desarrollarse para mejorar el desempeño de la gestión de riesgos y ejecutar la respuesta al riesgo seleccionada por la gerencia.

Las capacidades de gestión de riesgos consisten en la infraestructura de ERM, así como las capacidades específicas que se relacionan con la gestión de los riesgos prioritarios. Para ilustrar:

- (1) La definición de las capacidades específicas en torno a la gestión de los riesgos prioritarios comienza con la selección de los riesgos prioritarios y la determinación del estado actual de la capacidad de gestión de riesgos. Una vez que se determina el estado actual para cada uno de los riesgos clave, se evalúa el estado futuro deseado con el objetivo de avanzar en la madurez de las capacidades en torno a la gestión de esos riesgos. Consulte la Pregunta 111 para ver ejemplos que ilustran las capacidades de gestión de riesgos en diferentes etapas de madurez.
- (2) En nuestra respuesta a la Pregunta 37 se enumeran ejemplos de elementos de la infraestructura de ERM. Incluyen, entre otras cosas, una política general de gestión de riesgos, un proceso de evaluación de riesgos en toda la empresa, integración de respuestas de riesgo con planes comerciales, presencia en el directorio y la agenda del CEO, un comité de riesgos autorizado, claridad de las funciones y responsabilidades de la gestión de riesgos, tablero y otros informes de riesgos, y herramientas patentadas para representar una visión de cartera del riesgo.

Cuanto mayores sean las brechas en el estado actual y el estado futuro deseado de las capacidades de gestión de riesgos de la organización (punto (1) anterior), mayor será la necesidad de infraestructura de ERM (punto (2) anterior) para facilitar el avance de las capacidades de gestión de riesgos sobre tiempo.

Una vez que la solución de ERM es aclarada por las capacidades de gestión de riesgos requeridas para cerrar brechas significativas y brindar los resultados deseados por la gerencia, se necesita un caso de negocios para justificar la economía de implementarla. Luego se desarrolla un plan para construir y probar las capacidades requeridas e integrarlas en los procesos existentes de la empresa. Este plan se supervisa frente a hitos apropiados a lo largo del tiempo. El marco COSO ERM se puede utilizar para comparar la gestión de riesgos de la organización al comienzo de este proceso, durante el proceso y, una vez que la dirección complete todos los hitos de su plan, al final del proceso.

En resumen, la visión de la gestión de riesgos es un "llamado a la acción" para impulsar a la organización a identificar, diseñar y construir las capacidades de gestión de riesgos necesarias para cerrar brechas significativas y hacer que las respuestas de riesgo seleccionadas por la gerencia sucedan. Proporciona un sentido de propósito y enfoca el desarrollo posterior de metas y objetivos de gestión de riesgos más específicos. El siguiente es un ejemplo de una declaración de visión general de gestión de riesgos de una empresa global con más de 60 unidades operativas:

La Gestión de Riesgos Empresariales es un proceso continuo y un elemento del Gobierno Corporativo. Promueve eficiente y una evaluación eficaz del riesgo, aumenta la concienciación sobre el riesgo y mejora la gestión del riesgo en todo el Grupo. Esto incluye anticipar y evitar amenazas y pérdidas, así como identificar y aprovechar oportunidades.

La visión de la gestión de riesgos debe abordar la necesidad de mejorar la organización en la gestión de riesgos. a través de las capacidades colectivas y coordinadas de funciones, departamentos y unidades específicas. Por ejemplo, la declaración de visión anterior afirma que la gestión de riesgos comerciales es un proceso continuo y una parte integral elemento de gobierno corporativo centrado en la creación y protección del valor de la empresa. Un individuo o la función no puede realizar esta visión por sí sola.

#### 65. ¿Cómo define la administración las metas y objetivos de administración de riesgos de la entidad?

Una vez que se articula la visión compartida, se deben definir las metas y los objetivos generales de gestión de riesgos. mientras que un declaración de la visión es a menudo una aspiración, las metas y objetivos normalmente deben describir en términos simples lo que se va a cumplir. Deben ser procesables por la organización. Deben definirse en el contexto de la estrategia comercial de la organización. Por ejemplo, algunos objetivos comunes de gestión de riesgos elegidos por empresas para enmarcar su enfoque ERM incluyen lo siguiente:

- Desarrollar una comprensión común del riesgo en múltiples funciones y unidades de negocios para que podamos administrar riesgo de forma rentable en toda la empresa.
- Lograr una mejor comprensión del riesgo para obtener una ventaja competitiva.
- Cree salvaguardas contra sorpresas relacionadas con las ganancias.
- Desarrollar y mejorar capacidades para responder de manera efectiva a riesgos catastróficos críticos y de baja probabilidad.
- Lograr ahorros de costos a través de una mejor gestión de los recursos internos.
- Asignar el capital de manera más eficiente.

Las metas y objetivos de la gestión de riesgos deben ser coherentes con el negocio de la empresa y apoyarlo. objetivos y estrategias. Por lo tanto, el modelo de negocio de la organización proporciona un contexto importante para gestión de riesgos. Por ejemplo:

- Se dirige a los mercados y geografías en los que la empresa hace negocios.
- Especifica los productos y servicios que brinda a esos mercados, los canales que utiliza para acceder a esos mercados y las características por las que diferencia sus productos y servicios a los ojos de los cliente.
- Se basa en muchos elementos importantes: en los procesos a través de los cuales la entidad convierte materiales y mano de obra en productos y servicios; sobre los empleados que la entidad contrata, capacita y retiene; sobre los proveedores y clientes con los que la organización hace negocios; y sobre los accionistas y prestamistas que suministrarle capital.

Los riesgos comerciales son inherentes a todos estos elementos. A medida que la empresa ejecuta su estrategia, crea y aumenta su exposición a la incertidumbre. Por lo tanto, los objetivos y estrategias comerciales proporcionan el contexto para comprender los riesgos que la empresa desea asumir. COSO afirmó este punto al establecer el "establecimiento de objetivos" como un componente del marco ERM.

Al definir las metas y objetivos de la gestión de riesgos, la gerencia debe hacer "preguntas difíciles", como los que se enumeran a continuación:

- ¿Cuáles son nuestros objetivos y estrategias comerciales? ¿Cuáles son nuestros objetivos financieros, por ejemplo, rentabilidad, tamaño y el crecimiento de los ingresos? ¿Qué valores queremos construir y reforzar?

- ¿Qué mercados elegimos? ¿Qué posición relativa de mercado buscamos? ¿Para qué sirve nuestro modelo de negocio? ganar en nuestros mercados elegidos?
- ¿Qué posibles eventos futuros específicos enfrentamos? ¿Están relacionados?
- ¿Qué tan sensibles son nuestras estrategias, mercados, ganancias y flujo de efectivo a la ocurrencia de eventos futuros? ¿Qué tan riesgosos son nuestros activos tangibles e intangibles para crear valor? ¿Cuáles son los factores de pérdida que afectan esos activos?
- ¿Qué eventos futuros específicos podrían, si ocurrieran, afectar la capacidad de nuestra organización para lograr sus objetivos? objetivos relacionados con la calidad, la innovación, la oportunidad, la seguridad, el cumplimiento, etc., y para ejecutar sus estrategias ¿exitosamente? ¿Qué eventos afectarían nuestra participación de mercado?
- ¿Cuán capaces somos de responder a eventos fuera de nuestro control que puedan ocurrir en el futuro?
- ¿Sabemos cuáles son nuestros rendimientos esperados, ajustados por riesgo? ¿Varían los rendimientos ajustados al riesgo según ¿unidad de negocio? ¿Por producto principal? ¿Por geografía?
- Finalmente, si decidimos aceptar las exposiciones inherentes a nuestro modelo de negocio que dan lugar a nuestro actual riesgos, ¿tenemos suficiente capital para absorber pérdidas significativas no previstas en caso de que se produzcan?

Las preguntas anteriores proporcionan un contexto poderoso para definir las metas y objetivos de la gestión de riesgos.

El siguiente es un ejemplo de una declaración de la visión, misión, metas y objetivos de la gestión de riesgos:

Visión:

Contribuir a la creación, optimización y protección del valor empresarial mediante la gestión de nuestros riesgos comerciales como creamos valor en el mercado.

Misión:

Crear un enfoque integral para anticipar, identificar, priorizar, gestionar y monitorear la cartera de riesgos comerciales que afectan a nuestra organización. Establecer las políticas, procesos comunes, competencias, responsabilidades, informes y tecnología habilitadora para ejecutar ese enfoque con éxito.

Metas y objetivos:

- (1) Diseñar y ejecutar un proceso global de gestión de riesgos de negocios integrado con nuestra estrategia proceso de gestión:
  - Integrar la gestión de riesgos comerciales con nuestros procesos de formulación de estrategias y planificación comercial;
  - Articular nuestras estrategias para que sean entendidas en toda nuestra organización; • Establecer KPI diseñados para impulsar comportamientos consistentes con nuestra estrategia; y
  - Premiar la articulación y gestión eficaz de los riesgos clave.
- (2) Asegurar que las preguntas de propiedad del proceso se aborden con claridad para que los roles, responsabilidades y las autoridades se entienden correctamente.
- (3) Diseñar y ejecutar un proceso global para monitorear y reevaluar el perfil de riesgo del cuartil superior e identificar brechas en la gestión de esos riesgos, con base en cambios en los objetivos de negocio y en el entorno externo. y entorno operativo interno.
- (4) Definir estrategias de gestión de riesgos y responsabilidades claras y pasos de acción para construir y ejecutar capacidades de gestión de riesgos y mejorárlas continuamente.
- (5) Supervisar continuamente la información proporcionada a los responsables de la toma de decisiones con el fin de ayudarles a medida que gestionar los riesgos clave y proteger los intereses de los accionistas.

66. ¿Qué es el "apetito de riesgo" y en qué se diferencia de los "umbrales de riesgo", "tolerancias" o "límites"?

El marco COSO ERM define el "apetito de riesgo" de la siguiente manera:

El apetito de riesgo es la cantidad de riesgo, en un nivel amplio, que una entidad está dispuesta a aceptar en busca de valor. Refleja la filosofía de gestión de riesgos de la entidad y, a su vez, influye en la cultura y el estilo operativo de la entidad. Muchas entidades consideran cualitativamente el apetito por el riesgo, con categorías como alto, medio o bajo, mientras que otras adoptan un enfoque cuantitativo, reflejando y equilibrando objetivos de crecimiento, rentabilidad y riesgo. Una empresa con un mayor apetito por el riesgo puede estar dispuesta a asignar una gran parte de su capital a áreas de alto riesgo como los mercados emergentes. Por el contrario, una empresa con poco apetito por el riesgo podría limitar su riesgo a corto plazo de grandes pérdidas de capital invirtiendo solo en mercados maduros y estables.

El marco COSO ERM define "tolerancia al riesgo", que es un término que a menudo se usa indistintamente con términos como "umbral de riesgo" o "límite de riesgo", de la siguiente manera:

La tolerancia al riesgo es el nivel aceptable de variación en relación con el logro de un objetivo específico y, a menudo, se mide mejor en las mismas unidades que se utilizan para medir el objetivo relacionado.

Con base en las definiciones de COSO de estos términos, podemos hacer las siguientes observaciones:

El apetito por el riesgo es estratégico. Según COSO, es un "poste indicador" en el establecimiento de estrategias. El modelo de negocios de la organización proporciona un contexto importante para evaluar el apetito por el riesgo al aclarar las actividades que realiza la entidad, quiénes son sus clientes, cuáles son sus productos y cómo y en qué mercados realiza negocios.

Una comprensión profunda de los objetivos comerciales, la estrategia y las operaciones de una organización es muy útil al articular los riesgos que elige aceptar y los riesgos que elige evitar a medida que crea valor. A medida que la empresa ejecuta su estrategia, crea y aumenta su exposición a la incertidumbre. Por lo tanto, los objetivos y estrategias comerciales brindan el contexto para comprender los riesgos que la empresa elige asumir.

El apetito por el riesgo también puede establecer límites en torno al comportamiento de búsqueda de oportunidades, lo que afecta los objetivos y estrategias de la entidad.

El apetito por el riesgo se relaciona principalmente con el modelo de negocio, mientras que la tolerancia al riesgo se relaciona principalmente con los objetivos de la entidad. El apetito por el riesgo de una organización refleja tanto su capacidad para asumir el riesgo como una comprensión más amplia del nivel de riesgo que puede asumir con seguridad y gestionar con éxito durante un período prolongado. El apetito por el riesgo es la medida en que una organización expone su capital y fuentes de valor a la explotación de oportunidades estratégicas y la retención de la variabilidad del desempeño y la exposición a pérdidas.

Toda organización tiene un apetito por el riesgo, ya sea que lo reconozca explícitamente o no. El apetito por el riesgo se expresa a través de las acciones o inacciones de una entidad. Representa la "visión del mundo" de la dirección ejecutiva, que impulsa sus decisiones estratégicas. Es inherente a la estrategia de la organización ya la ejecución de esa estrategia, tanto en la forma de riesgos asumidos como de riesgos evitados. Al definir ERM, COSO estableció un estándar para que la gerencia administre el riesgo dentro del apetito por el riesgo de la entidad, tal como lo entendió y acordó la junta directiva.

La dirección tiene en cuenta el apetito por el riesgo al definir objetivos, formular estrategias, asignar recursos, establecer tolerancias al riesgo y desarrollar capacidades de gestión de riesgos. La junta considera el apetito por el riesgo cuando aprueba las acciones de la gerencia. Si se articula explícitamente, el apetito por el riesgo proporciona una dirección general para la gestión del riesgo y se fundamenta durante el proceso de establecimiento de objetivos.

Mientras que el apetito por el riesgo es estratégico, la tolerancia al riesgo es táctica. La tolerancia al riesgo se define dentro del contexto del objetivo relacionado utilizando las métricas establecidas para medir el desempeño en relación con ese objetivo. Las tolerancias al riesgo establecen los límites de la variabilidad del rendimiento. Una vez que se establecen las tolerancias, se monitorean las medidas de rendimiento para garantizar que el rendimiento se gestione dentro de esos límites. Por lo tanto, las tolerancias al riesgo se utilizan para garantizar que la variabilidad del rendimiento se reduzca a un nivel aceptable.

La tolerancia al riesgo puede reflejarse de manera diferente para diferentes tipos de objetivos, incluidos los objetivos relacionados con la variabilidad de las ganancias, la exposición a las tasas de interés, el cumplimiento de las leyes y regulaciones y la adquisición, el desarrollo y la retención de personas. La tolerancia al riesgo relacionada con todos estos objetivos se expresa de manera diferente. En efecto, las tolerancias al riesgo abordan la pregunta: "¿Cuánta variabilidad estamos dispuestos a aceptar mientras perseguimos un

dado el objetivo comercial? La orientación sobre esta pregunta es importante ya que ayuda a los gerentes a evaluar su exposición en términos de los riesgos a la baja que están autorizados a aceptar cuando buscan un rendimiento al alza. A medida que los gerentes buscan oportunidades de crecimiento y nuevas fuentes de rentabilidad, las tolerancias y los límites de riesgo son una herramienta eficaz para contrarrestar las presiones sobre ellos para tener éxito y producir resultados. En otras palabras, las tolerancias y los límites de riesgo ayudan a los gerentes a comprender que las acciones emprendidas con el objetivo de tener éxito y producir resultados no se pueden ejecutar a toda costa y sin tener en cuenta las posibles consecuencias para la organización en su conjunto si algo sale mal.

#### 67. ¿Existe una metodología definida para calibrar el desempeño con tolerancias al riesgo?

Calibrar el desempeño con tolerancias al riesgo requiere una metodología de medición, un proceso de seguimiento y un compromiso de mejora continua. Esto a menudo se describe como el ciclo "Planificar-Hacer-Verificar-Actuar".

La "planificación" implica establecer objetivos y las correspondientes tolerancias al riesgo, así como decidir sobre las respuestas al riesgo. "Hacer" se refiere al diseño e implementación de capacidades de gestión de riesgos. El desempeño del monitoreo cae dentro de la categoría de "verificación". La mejora continua basada en la verificación de resultados es "actuar".

La metodología de medición es la pieza central del ciclo, porque facilita todas las demás tareas y es equivalente a "gestionar por los hechos". El mensaje es que una metodología de medición efectiva está directamente relacionada con el objetivo de desempeño. En la gestión de riesgos, este concepto se aplica mejor a aquellos riesgos que son susceptibles de medición.

Como se señaló en la Pregunta 66, COSO define "tolerancia al riesgo" como "la variación aceptable en relación con el logro de un objetivo". Hay tres tipos diferentes de tolerancia al riesgo, cada uno de los cuales está vinculado de alguna manera a la distribución utilizada para representar todas las fuentes de incertidumbre asociadas con el valor futuro de una exposición. Estos tres tipos de tolerancia al riesgo no pretenden ser mutuamente excluyentes en una situación dada, ya que los tres podrían ser relevantes al mismo tiempo. Se presentan para capturar las tres formas en que los administradores de riesgos tienden a pensar sobre la tolerancia al riesgo.

¿Cuál es el mensaje? Al desarrollar una política relacionada con la tolerancia al riesgo de la empresa, se debe tener cuidado de relacionar la política con el tipo de tolerancia relevante. Cada tipo de tolerancia tendrá implicaciones diferentes y, por lo tanto, cada uno requerirá políticas diferentes.

Los siguientes son los tres tipos de tolerancia al riesgo:

- Variabilidad en el logro de los rendimientos esperados: Esta articulación de la tolerancia a menudo se denomina "variabilidad del desempeño", que es el grado de variación en torno al valor esperado, o el nivel de incertidumbre en la media, o como explica COSO, en el logro de un objetivo. Representa la incertidumbre que la organización está dispuesta a soportar en la realización de sus expectativas, o en el logro de sus objetivos.
- La gerencia tiene expectativas sobre el desempeño de un activo, un producto, un sistema, una unidad de negocios, etc.
- Cuanta más incertidumbre haya sobre el valor final realizado, mayor será la incertidumbre de la dirección. En el caso de exposiciones distribuidas según una curva de campana, este tipo de tolerancia se refleja en el apetito de riesgo de la compañía por la varianza. Cuanto mayor sea la varianza aceptada por los gerentes, mayor será su tolerancia a la variabilidad del desempeño.

Las preguntas relevantes que ilustran el enfoque de la gerencia en la comprensión de este tipo de tolerancia incluyen:

- ¿Qué volatilidad estamos dispuestos a aceptar en tipos de interés y tipos de cambio?
- ¿Cuán crucial es para nosotros lograr las ganancias y el flujo de caja previstos? ¿Cuál es el nivel mínimo de ganancias y flujo de efectivo que podemos aceptar?
- Susceptibilidad a eventos extremos: Esta articulación de la tolerancia a menudo se denomina exposición a pérdidas o impulsor de pérdidas, que es una exposición a pérdidas catastróficas. La exposición a eventos extremos puede ocurrir sin afectar necesariamente el grado de variación, por lo que este es un tipo diferente de incertidumbre. De hecho, los dos tipos de incertidumbre pueden ocurrir simultáneamente. Considerando una curva de campana, esta forma de tolerancia se refleja en el gusto de la empresa por la curtosis. Si bien es un término estadístico bastante oscuro, la curtosis se refiere a qué tan "gordas" son las colas de la distribución, lo que significa qué tan probable es que sucedan eventos extremos. Cuanto más "gordas" las colas, más

mayor es la probabilidad de que haya resultados extremos en la distribución de posibles eventos futuros.

Por lo tanto, los gerentes deben al menos reconocer en el proceso de planificación que existe una posibilidad estadística, por remota que sea, de que suceda algo extremo.

Un ejemplo concreto podrían ser los accidentes relacionados con los viajes aéreos. Estos accidentes son raros, pero cuando ocurren, a menudo son catastróficos y muy visibles. Una aerolínea podría identificar los factores que afectan la probabilidad de que ocurra un accidente, por ejemplo, error del piloto, inexperiencia del piloto, malas prácticas de mantenimiento, hielo en las alas, mal diseño del avión, etc. La aerolínea exitosa maneja su exposición a estos factores para mantener las probabilidades de un evento extremo, como un accidente, tan estadísticamente insignificantes como para hacer que los viajes aéreos sean seguros a los ojos del consumidor.

Una pregunta relevante para este tipo de tolerancia es:

- ¿Qué tan expuestos estamos a la interrupción del negocio, pérdidas sustanciales de activos físicos, problemas catastróficos de salud y seguridad, o daños irreparables a la reputación y la imagen debido al incumplimiento sistemático de nuestra promesa de marca?

- Inconsistencia con el apetito por el riesgo deseado: Esta articulación de la tolerancia al riesgo es el tema estratégico para definir el apetito por el riesgo de la organización en el contexto de su modelo de negocios para crear y proteger el valor de la empresa. Como se explica más detalladamente en la Pregunta 66, el apetito por el riesgo es la elección de la administración de la distribución de posibles eventos futuros o la evaluación de la administración sobre si la forma de distribución de los posibles eventos futuros es consistente con los objetivos comerciales de la empresa. En este contexto, la gerencia debe abordar cuestiones tales como si quieren asumir este tipo de riesgos o si este es el negocio en el que quieren estar. Por ejemplo, el director ejecutivo puede estar tomando una sobredosis de riesgo más allá de un nivel aceptable con una adquisición o crecimiento. estrategia. En tales casos, puede haber incongruencias en el modelo de negocios porque no logra equilibrar de manera efectiva la creación de valor empresarial con el apetito por el riesgo considerado aceptable por la junta. Por lo tanto, la distribución de una exposición puede estar muy sesgada, exponiendo el valor de la empresa a un riesgo inaceptable. Alternativamente, la distribución tiene otras características, que son difíciles de gestionar para la empresa o que no coinciden con su apetito por el riesgo. O la organización puede haber retenido una exposición que es inconsistente con sus objetivos comerciales y su apetito por el riesgo.

Para ilustrar, suponga que una empresa produce una parte que debe subcontratar a un proveedor que tenga la experiencia y los procesos para producir esa misma parte a un costo menor con una calidad comparable o superior. En este caso, la empresa no tiene la distribución agregada deseada de posibles eventos futuros aceptables porque los riesgos que asume al fabricar la pieza en sí misma no son consistentes con sus competencias básicas. Por lo tanto, este tipo de tolerancia al riesgo se expresa en términos de cuán dispuesta está la empresa a desviarse de su apetito de riesgo deseado, ya sea para la empresa en su conjunto (todas las exposiciones combinadas) o a nivel de la exposición individual (una unidad de negocio individual). , Por ejemplo).

Las preguntas relevantes incluyen:

- ¿Qué tan bien alineada está la distribución general de riesgos que estamos asumiendo con nuestro apetito por el riesgo?
- ¿Hemos alineado nuestra toma de riesgos con nuestras competencias básicas, es decir, lo que hacemos mejor?
- ¿Toleramos o cerramos el comportamiento fuera de la estrategia?

En resumen, el modelo de negocios primero debe ser consistente con el apetito de riesgo deseado de la organización.

Luego, la organización debe alinear sus mercados, productos, procesos, personas, tecnología y lugares de operación con ese modelo. De lo contrario, el juego se pierde antes de que comience y la gestión de riesgos se convierte en una ocurrencia tardía.

Todas las preguntas ilustrativas incluidas en esta respuesta son de naturaleza estratégica. Una vez que los gerentes comprenden estas tres ilustraciones de la tolerancia al riesgo, pueden evaluar mejor cómo se puede articular la tolerancia al riesgo a través de las políticas de gestión del riesgo, así como medir y gestionar las respuestas alternativas al riesgo.

68. ¿Cómo se traducen la visión y los objetivos de gestión de riesgos en el ERM apropiado?  
¿Infraestructura?

Una vez que la visión de la gestión de riesgos y las metas y objetivos relacionados (incluido el apetito por el riesgo y el tolerancia), la gerencia define las capacidades necesarias para implementar la infraestructura ERM que realizará la visión y logrará las metas y objetivos establecidos. Las "capacidades" surgen de una combinación adecuada de políticas, procesos, competencias, informes, metodologías y tecnologías. Porque las empresas tienen diferentes objetivos, estrategias, estructura, cultura, apetito de riesgo y finanzas no obstante, no hay dos enfoques iguales para implementar la infraestructura ERM. Por lo tanto, los diversos las capacidades que respaldan la infraestructura de ERM para una empresa pueden diferir de las de otra empresa.

Recomendamos organizar el proceso de definición de capacidades de gestión de riesgos en tres fases. La primera fase sienta las bases. La segunda fase construye capacidades para riesgos críticos. La tercera fase mejora capacidades existentes de gestión de riesgos. Estas tres fases proporcionan una hoja de ruta sugerida de ocho pasos para abordando los ocho componentes del marco COSO ERM, como se ilustra a continuación:

LA HOJA DE RUTA DE ERM →

COMPONENTE DE COSO ESTRUCTURA	ESTABLECER LA BASE		DESARROLLAR CAPACIDADES			MEJORA LAS CAPACIDADES		
	Adoptar común idioma	Establecer supervisión y gobernanza	Evaluar el riesgo y desarrollar respuestas	Diseño/ implementar capacidades	Continuamente mejorar capacidades	Cuantificar el riesgo toda la empresa	Mejorar empresa actuación	Establecer sostenible competitivo ventaja
Ambiente interno	X	X	X	X	X	X	X	X
Establecimiento de objetivos			X	X		X	X	X
Identificación de eventos	X	X	X			X XX X		
Evaluación de riesgos	XXXXX							
Respuesta a los riesgos			X XX X XX X					
Actividades de control		X		X		X XX X		
Información/ Comunicación	X		X XX X XX X					
Supervisión		X		X		X XX X		

Por ejemplo, como se analiza más adelante en la Pregunta 96, la fase SET FOUNDATION incluye el paso "adoptar lenguaje común." Hay varios elementos posibles a considerar al formular un lenguaje común para su uso en la gestión de riesgos, incluido un modelo de riesgo, un glosario de gestión de riesgos, una clasificación de procesos y otros marcos relevantes. Estos elementos sugeridos de un lenguaje común no pretenden ser integrador, ya que existen otros que pueden facilitar la adopción de un lenguaje común.

El mismo proceso de pensamiento también se aplica a los otros siete pasos. Todo elemento potencial relacionado con un no es necesario implementar un paso en particular. Los elementos sugeridos proporcionados en esta publicación son ilustrativo y destinado a proporcionar un punto de partida para que la gerencia lo considere. Solo las necesidades de gestión seleccionar aquellos elementos que se consideren esenciales para construir y mejorar las capacidades de gestión de riesgos. Mientras que la Los componentes de COSO proporcionan el marco de evaluación necesario para evaluar la eficacia de ERM infraestructura y capacidades de gestión de riesgos subyacentes, las tres fases y los ocho pasos descritos anteriormente proporcionar la hoja de ruta de cómo la administración puede llegar del Punto A al Punto B.

Las tres fases para mejorar la infraestructura de ERM y las capacidades de gestión de riesgos se presentan brevemente a continuación:

- **ESTABLECER LAS BASES:** toda organización debe establecer las bases adoptando un lenguaje común y estableciendo una supervisión y un gobierno efectivos. A medida que la gerencia coordina sus esfuerzos, se necesita un lenguaje común para comunicarse. Las organizaciones que combinan un lenguaje común con un proceso de evaluación de riesgos en toda la empresa dan fe de discusiones más efectivas en los niveles más altos de la organización, particularmente durante el proceso de establecimiento de la estrategia. Estas discusiones dan como resultado una mejor comprensión del riesgo y conducen a respuestas de riesgo más oportunas y enfocadas. Con respecto a la supervisión y el gobierno, la junta que trabaja con y a través del CEO debe comprender cuáles son los riesgos clave, quién los gestiona y la eficacia del desempeño. Deben preguntar si existen brechas significativas en las capacidades de gestión de riesgos y si se están tomando medidas para cerrar esas brechas. El objetivo final del proceso de supervisión es brindar seguridad a la junta directiva y al director ejecutivo de que las actividades empresariales y las actividades de control de la organización están razonablemente equilibradas para que ninguna sea desproporcionadamente más fuerte que la otra.
  
- **DESARROLLAR CAPACIDADES:** Establecer las bases pone en marcha algunos de los elementos del ERM infraestructura necesaria para construir y mejorar continuamente las capacidades en torno a la gestión de los riesgos prioritarios. El objetivo es diseñar e implementar capacidades repetidas y bien definidas para evaluar, administrar y monitorear el riesgo y desplegar esas capacidades en toda la empresa. Los tres pasos de la fase de "construir capacidades" se relacionan con el proceso mediante el cual la gerencia ejecuta tareas específicas con respecto a la gestión del riesgo. Los tres pasos de esta fase son, primero, evaluar el riesgo y desarrollar respuestas, seguido por diseñar e implementar capacidades y culminar con la mejora continua de las capacidades, todo lo cual contribuye a un ciclo interminable para mejorar el desempeño de la gestión de riesgos a lo largo del tiempo. El desarrollo de procesos y herramientas uniformes para identificar, obtener y medir el riesgo genera confianza en que todos los posibles eventos futuros potencialmente significativos se identifiquen y se evalúen los riesgos relacionados, proporcionando una base para asumir el riesgo con conocimiento y evaluar y formular respuestas al riesgo. Una vez que se seleccionan las respuestas de riesgo apropiadas, se diseñan e implementan las capacidades para ejecutarlas. Estas capacidades incluyen las actividades de control, información y comunicación, y los componentes de monitoreo, como se explica en el marco COSO. Una vez implementadas, las capacidades de gestión de riesgos se mejoran continuamente con el tiempo. Fundamental para todas estas tareas es la recopilación y el análisis de información para la toma de decisiones. Los procesos comunes allanan el camino para definir, organizar y reportar información en toda la empresa. Proporcionan un proceso sistemático para implementar mejoras en la infraestructura ERM de la organización.
  
- **MEJORAR LAS CAPACIDADES:** Esta fase mejora la gestión de riesgos existente de la organización capacidades e integra aún más la gestión de riesgos con el proceso de establecimiento de estrategias. Consta de tres pasos: cuantificar el riesgo en toda la empresa, mejorar el rendimiento de la empresa y establecer una ventaja competitiva sostenible. Estos pasos conducen a capacidades más avanzadas, a medida que evoluciona el estado del arte. Por ejemplo, la medición del desempeño ajustado al riesgo ha evolucionado en las instituciones financieras de clase mundial y se considera una "mejor práctica" para administrar los riesgos crediticios y de mercado. Las metodologías de medición VaR (Value at Risk) y EaR (Earnings at Risk) son cada vez más aceptadas tanto por las empresas corporativas como por los reguladores. Cada vez más, estas y otras capacidades se consideran invalables para asignar capital y medir el desempeño en función de los riesgos inherentes a la cartera de negocios. Mejoran las capacidades de gestión de riesgos establecidas al fortalecer el vínculo con las tolerancias de riesgo definidas y mejorar la evaluación del desempeño comercial.

Como regla general, cuanto más maduras sean las capacidades de una organización en términos de habilidades, procesos y metodologías de apoyo y tecnología comprometida con la gestión de riesgos, más eficaz será la organización en la implementación de ERM. Las tres fases descritas anteriormente para desarrollar capacidades de gestión de riesgos están estructuradas para brindar una guía general sobre la secuencia adecuada de pasos durante el proceso de implementación de ERM.

Por ejemplo, cuando diseñe una solución de ERM, comience con el establecimiento de las bases PRIMERO. Después de sentar las bases, ENTONCES proceda a desarrollar capacidades en torno a los riesgos prioritarios, con énfasis en cerrar las brechas significativas. ENTONCES, concéntrese en las mejoras seleccionadas.

El concepto de secuenciación reconoce que las capacidades de gestión de riesgos que funcionan de manera efectiva proporcionan una base para implementar mejoras posteriores. "Demasiado lejos, demasiado rápido" es una historia demasiado familiar en la gestión de riesgos.

El modelo de negocio y la cultura de la organización, la madurez relativa de sus capacidades de gestión de riesgos, el grado de centralización o descentralización, su apetito por el riesgo, la comparabilidad de los perfiles de riesgo relacionados con las diferentes unidades de negocio dentro de la empresa y otros factores deben sopesarse al decidir qué capacidades para construir y mejorar a medida que la organización implementa su solución ERM. Cuantas más capacidades mejoradas tenga la dirección, mayor será la alineación de las políticas, los procesos, las personas, la tecnología y el conocimiento de gestión de riesgos, y mayor será el grado de integración con los procesos estratégicos y operativos.

---

## REALIZACIÓN DE EVALUACIONES DE RIESGO

69. ¿Cuál es la relación entre la evaluación de riesgos y la gestión de riesgos?

La evaluación de riesgos es el proceso de identificar, obtener y evaluar riesgos individuales y las interrelaciones entre los riesgos. Proporciona un enfoque sistemático para analizar el impacto de posibles eventos futuros en el logro de los objetivos de una organización. El proceso de evaluación de riesgos en sí generalmente comprende una evaluación de los datos disponibles y la aplicación del juicio para determinar la importancia de los posibles eventos futuros y la probabilidad de que ocurran. Una evaluación de riesgos eficaz conduce a la formulación de respuestas a los riesgos.

Por lo tanto, la actividad de evaluación de riesgos se lleva a cabo con un fuerte sesgo hacia la determinación de la necesidad de nuevas medidas.

La gestión de riesgos, por otro lado, abarca la evaluación de riesgos, así como las actividades asociadas con la gestión de riesgos. Estas actividades incluyen políticas, procesos, competencias, informes, metodologías y sistemas. Los ocho componentes de COSO Enterprise Risk Management – Integrated Framework proporcionan un punto de vista para comprender lo que implica la gestión de riesgos cuando se aplica durante el establecimiento de la estrategia y en toda la empresa. Este marco incluye tres componentes: establecimiento de objetivos, identificación de eventos y evaluación de riesgos, que son esenciales para evaluar los riesgos de manera efectiva.

70. ¿Cuál es la relación entre la evaluación de riesgos y la evaluación del desempeño?

La evaluación de riesgos es una actividad prospectiva aplicada a posibles eventos futuros para identificar el impacto potencial en el logro de los objetivos y la probabilidad de ocurrencia en un horizonte de tiempo definido. La evaluación del desempeño es una actividad retrospectiva aplicada para evaluar el desempeño de una unidad, un proceso o una función frente a un objetivo o estándar predeterminado durante un período de tiempo establecido.

La evaluación de riesgos está relacionada con la evaluación del desempeño porque ambas actividades se aplican a los objetivos. Por ejemplo, como se explica en el marco COSO, la evaluación de riesgos comienza con el establecimiento de objetivos para establecer un contexto efectivo para identificar posibles eventos futuros que crean riesgos y oportunidades. La evaluación de un riesgo debe considerar deseablemente la tolerancia al riesgo de la gerencia, que COSO define como "el nivel aceptable de variación en relación con el logro de un objetivo específico". La tolerancia al riesgo a menudo se mide mejor usando las mismas unidades que las que se usan para medir el objetivo relacionado.

La evaluación del desempeño trata directamente con la medida de un objetivo, que a menudo se aplica durante la actividad de evaluación del desempeño. La evaluación del desempeño requiere un objetivo o estándar predefinido, definido en el contexto de un objetivo. La tolerancia al riesgo a menudo se establece utilizando medidas de rendimiento establecidas como marco para definir los límites de la variabilidad de rendimiento aceptable. Una vez que se establecen las tolerancias, se monitorean las medidas de rendimiento para garantizar que el rendimiento se gestione dentro de esos límites. Por lo tanto, la tolerancia al riesgo se utiliza para garantizar que la variabilidad del rendimiento se reduzca a un nivel aceptable. Los operadores entienden instintivamente la evaluación del desempeño porque eso es lo que hacen en el día a día. Por ejemplo, una vez que se identifican las brechas de desempeño, los operadores a menudo se enfocan en comprender la causa raíz de las brechas, diseñar e implementar mejoras de procesos para cerrar las brechas y monitorear el desempeño para garantizar que las brechas

no vuelvas aemerger. Si las brechas vuelven a surgir, el ciclo de mejora comienza de nuevo para eliminarlas. La evaluación de riesgos, por otro lado, es una actividad más difícil de aplicar para los operadores, porque trata con eventos futuros potenciales en lugar de eventos pasados históricos. Cuando la evaluación del riesgo y la evaluación del desempeño se combinan de manera efectiva, el enfoque de la administración se vuelve más anticipatorio y menos reactivo.

71. ¿Cuáles son los componentes de una declaración de objetivos efectiva y por qué los objetivos son importantes para una evaluación de riesgos efectiva?

Los objetivos son importantes para una evaluación de riesgos porque articulan lo que una entidad se esfuerza por lograr. Una declaración de objetivos efectivamente articulada es realista, comprensible, medible, creíble y factible.

Se utiliza para establecer el objetivo o la meta de una organización, unidad de negocio, proceso o función. En el contexto de ERM, es importante porque el efecto del riesgo se observa y mide a medida que impacta en el logro de los objetivos comerciales. Los objetivos proporcionan el contexto para identificar posibles eventos futuros, que a su vez proporcionan la base para realizar una evaluación de riesgos.

72. ¿Cuál es la diferencia entre un evento y un riesgo?

Son conceptos relacionados. Según COSO Enterprise Risk Management – Integrated Framework, un evento es "un incidente o suceso, de fuentes internas o externas a una entidad, que afecta el logro de los objetivos". COSO define un riesgo como "la posibilidad de que un evento ocurra y afecte negativamente el logro de los objetivos". Los eventos pueden tener un impacto negativo o un impacto positivo. Un evento con un impacto negativo en el logro de un objetivo representa un riesgo, que puede impedir la creación de valor o erosionar el valor empresarial existente. Un evento con un impacto positivo representa una oportunidad. Así, un evento es la circunstancia que impacta un objetivo y crea la condición para un riesgo, SI tiene un efecto negativo. Por ejemplo, el hecho de que un proveedor no proporcione un componente de producción clave es un evento. Como resultado, se presenta el riesgo de no cumplir con los plazos de producción, junto con la consecuencia relacionada de entregas tardías a los clientes.

Bajo el marco COSO, la identificación de eventos precede a la evaluación de riesgos. Hay eventos (por ejemplo, cambios en el mercado, en los sistemas, en los productos de la competencia, en el personal, etc.) que pueden generar cambios en la visión del riesgo de la organización. Comprender estos factores internos y externos ayuda a que la identificación y evaluación de riesgos sea más relevante, ya que las condiciones dentro y fuera de la empresa cambian constantemente.

73. ¿Por qué la definición de riesgo de COSO no incorpora la noción de que el riesgo incluye tanto al alza como a Abajo?

COSO define un "riesgo" como "la posibilidad de que ocurra un evento y afecte negativamente el logro de los objetivos". Algunos de los que respondieron al borrador de exposición de ERM argumentaron que la definición de riesgo no debe centrarse únicamente en la probabilidad de que sucedan cosas malas. Estos encuestados argumentaron que muchos riesgos también tienen un lado positivo y, por lo tanto, deberían incluir la probabilidad de que sucedan cosas buenas. En efecto, argumentaron que el riesgo es la distribución de todos los eventos o resultados futuros posibles, tanto positivos como negativos, en el desempeño de una empresa durante un horizonte de tiempo determinado debido a cambios en las variables subyacentes clave. Los encuestados también señalaron que el marco de ERM sería más relevante si incorporara la probabilidad y la importancia de las oportunidades en la definición de riesgo.

COSO consideró cuidadosamente este tema tanto antes como después de la emisión del borrador de exposición de ERM. Como se discutió en la Pregunta 72, COSO usa el término "evento" para capturar los aspectos positivos y negativos de "lo que puede suceder" en el futuro. Los eventos pueden tener un impacto negativo o positivo en una empresa. Un evento futuro potencial que podría tener un impacto negativo es un riesgo, mientras que un evento futuro potencial que podría tener un impacto positivo es una oportunidad. Con base en los aportes obtenidos de los usuarios clave y los grupos de partes interesadas y los resultados de las pruebas de campo, COSO concluyó que la mayoría de los posibles usuarios del marco de ERM tienden a pensar en el riesgo solo en términos de "desventajas". En otras palabras, la mayoría de los usuarios ven el riesgo como algo relacionado con la imposibilidad de lograr objetivos importantes. Por lo tanto, COSO concluyó que ampliar la definición de riesgo para incluir el potencial de "ventaja" nublaría los conceptos y frustraría un objetivo principal del marco de proporcionar un lenguaje común para ERM.

74. ¿Cómo articulamos el concepto de riesgo inherente para que pueda usarse efectivamente como criterios de evaluación?

El riesgo inherente es un aspecto esencial de la evaluación de la importancia de un riesgo y se define en el marco COSO ERM como "el riesgo para una entidad en ausencia de cualquier acción que la administración pueda tomar para alterar la probabilidad o el impacto del riesgo". En un entorno de evaluación de riesgos, el riesgo inherente generalmente se considera en el contexto del impacto de un riesgo en el logro de un objetivo comercial sin procesos de gestión específicos o controles internos establecidos. Si bien este concepto es fácil de describir en un nivel, es al mismo tiempo difícil de aplicar en la práctica durante una evaluación de riesgos. Para muchas personas, es difícil pensar en los riesgos sin tener en cuenta los procesos o controles existentes.

Una forma de describir el riesgo inherente es el riesgo presente en una actividad empresarial. Por lo tanto, los participantes en una evaluación de riesgos visualizan un escenario en el que la unidad de negocios bajo evaluación se forma recientemente en el mismo entorno operativo y bajo las mismas circunstancias en que opera la unidad actual. Luego, los participantes pueden hacer la pregunta: "¿Cuál es el impacto del riesgo identificado antes de que se implementen políticas o procedimientos de control?"

Algunos argumentan que un enfoque de riesgo inherente no es tan intuitivo como un enfoque de "riesgo residual" en el que se consideran las políticas y procedimientos actuales durante la evaluación. Si bien un enfoque de riesgo residual puede ser más fácil de entender para algunos, puede pasar por alto un riesgo crítico porque los participantes están de acuerdo en que el impacto potencial del riesgo en el logro de los objetivos comerciales es insignificante debido a sus percepciones colectivas sobre la efectividad de la gestión de riesgos existente. capacidades. Si se ignoran los riesgos críticos, es posible que la gerencia ni siquiera sepa que existen, y se pierde la oportunidad de compartir las respuestas al riesgo, las actividades de control y las mejores prácticas. El marco COSO señala que el riesgo debe evaluarse sobre una base de riesgo residual después de considerar las respuestas de riesgo seleccionadas para mitigar los riesgos significativos.

75. ¿Existe un lenguaje de riesgo respaldado oficialmente que podamos usar para nuestra organización?

A la fecha de esta publicación, no tenemos conocimiento de un lenguaje o modelo de riesgo autorizado adoptado por COSO o cualquier otra organización. La intención de COSO era permitir flexibilidad en las organizaciones para agrupar eventos potenciales en categorías. COSO señala que "la categorización de eventos... permite a la gerencia considerar la integridad de sus esfuerzos de identificación de eventos". Este es el propósito central de un lenguaje común. La gerencia comienza una evaluación de riesgos con (a) una hoja de papel en blanco con toda la puesta en marcha que implica la elección o (b) un lenguaje común que permite a las personas ocupadas con diversos antecedentes y experiencias comunicarse más efectivamente entre sí e identificar problemas relevantes más rápidamente. COSO proporciona un ejemplo de categorías de eventos que consisten en factores externos y factores internos en el marco (consulte el Anexo 4.2 en la página 34 del marco).

Las fuentes de incertidumbre que una empresa debe comprender y gestionar pueden ser externas o internas. Además, el riesgo tiene que ver con el conocimiento. Cuando la gerencia carece de conocimiento, hay mayor incertidumbre. Por lo tanto, las fuentes de incertidumbre también se relacionan con la relevancia y confiabilidad de la información sobre el entorno externo e interno. Estos tres grandes grupos (entorno, proceso e información para la toma de decisiones) brindan la base para un marco propicio que resume las fuentes de incertidumbre en un negocio.

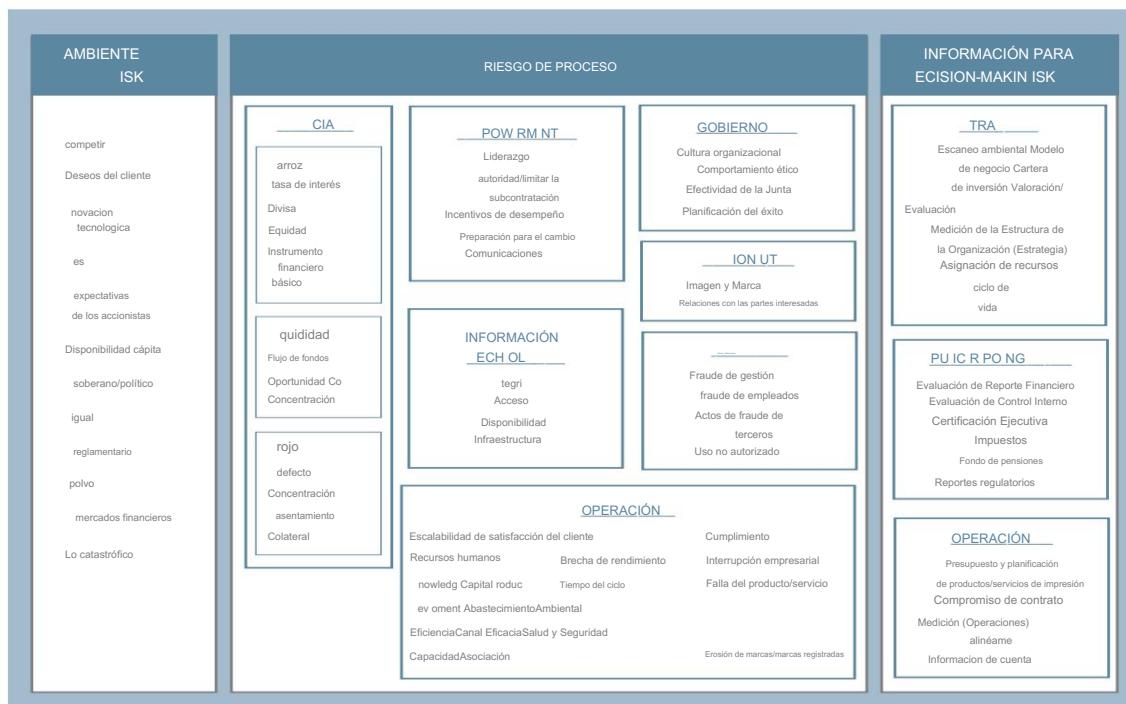


- El riesgo ambiental surge cuando fuerzas externas pueden afectar el desempeño de la entidad, o hacer que sus elecciones con respecto a sus estrategias, operaciones, relaciones con clientes y proveedores, estructura organizacional o financiamiento sean obsoletas o ineficaces. Estas fuerzas externas incluyen las acciones de competidores y reguladores, cambios en los precios de mercado, innovación tecnológica, cambios en los fundamentos de la industria, la disponibilidad de capital u otros factores fuera de la capacidad directa de control de la empresa.
- El riesgo de proceso surge cuando los procesos internos no logran los objetivos para los que fueron diseñados al respaldar el modelo de negocios de la entidad. Por ejemplo, las características de los procesos de bajo rendimiento, o los riesgos de los procesos, incluyen una mala alineación con los objetivos y estrategias comerciales, clientes insatisfechos y operaciones inefficientes. También incluyen diluir (en lugar de crear o preservar) el valor empresarial; y no proteger importantes activos financieros, físicos, de clientes, empleados/proveedores, conocimientos e información de pérdidas inaceptables, toma de riesgos, apropiación indebida o uso indebido.
- El riesgo de información para la toma de decisiones surge cuando la información utilizada para respaldar las decisiones de negocios es incompletos, desactualizados, inexactos, tardíos o simplemente irrelevantes para el proceso de toma de decisiones. Estos riesgos son incertidumbres que afectan la confiabilidad de la información utilizada para respaldar las decisiones para crear y proteger el valor de la empresa.

Estos tres grupos de riesgo están interrelacionados. Los riesgos ambientales y los riesgos de proceso que enfrenta la empresa están impulsados por las realidades externas e internas del negocio. La información para el riesgo de toma de decisiones se ve directamente afectada por la efectividad y confiabilidad de los sistemas de procesamiento de información y los procesos informales de "recopilación de inteligencia" para capturar datos relevantes, convertir esos datos en información y proporcionar esa información a los gerentes apropiados en forma de informes escritos oportunos, y comunicaciones orales. El riesgo de proceso a veces es indistinguible de la información para el riesgo de toma de decisiones porque se necesita información para tomar decisiones informadas sobre un proceso. Un flujo constante de información debería proporcionar a los responsables de la toma de decisiones los conocimientos que necesitan sobre el entorno externo y el rendimiento de los procesos de la empresa para que puedan gestionar los riesgos de la organización de forma eficaz. En resumen, estos tres grupos de riesgo proporcionan una base amplia sobre la cual se pueden identificar y detallar categorías de riesgo más específicas.

Los tres grupos de riesgo se representan utilizando el Protiviti Risk ModelSM que se muestra a continuación.

#### MODELOS DE RIESGO PROTIVITISM



Usando este modelo, se pueden identificar ejemplos de eventos dentro de cada categoría de riesgo relevante enumerada en el modelo. Por ejemplo, el riesgo de pérdida catastrófica es la incapacidad de mantener las operaciones, proporcionar productos y servicios esenciales o recuperar los costos operativos como resultado de un desastre mayor. La incapacidad de recuperarse de tales eventos de manera competente podría dañar la reputación de la empresa, la capacidad de obtener capital y las relaciones con los inversores. Hay dos fuentes de eventos que pueden conducir a una pérdida catastrófica:

- Eventos incontrolables: Desastres por guerra, terrorismo, incendio, terremoto, clima severo e inundaciones y otros eventos similares que están completamente fuera del control de la empresa. Si bien estos eventos no pueden prevenirse o incluso predecirse, sus efectos en los activos y operaciones de la organización pueden administrarse.
- Eventos controlables: algunos eventos pueden tener efectos tan catastróficos en una empresa como desastre incontrolable. Por ejemplo, los desastres ambientales, las violaciones generalizadas de la salud y la seguridad, los acuerdos inmobiliarios subacuáticos espectacularmente grandes, los altos costos de los litigios que acaparan los titulares, las enormes pérdidas de los derivados, el fraude comercial masivo y las pérdidas significativas en la participación de mercado debido a que no se abandonaron las estrategias que ya no existen. trabajar. Las actividades comerciales que contribuyen a estos eventos están bajo el control de la empresa, es decir, pueden verse afectadas por las decisiones de la administración o por la eficacia del entorno de control interno.

COSO recomienda un enfoque de “arriba hacia abajo”, es decir, la gerencia define los objetivos de la organización y las categorías de riesgo relacionadas que impactan esos objetivos. Luego se identifican eventos específicos dentro de cada categoría. Por lo tanto, el uso de un lenguaje de riesgo comercial común comienza en un nivel estratégico, comenzando con un modelo como el de la página anterior, y luego se adapta a las circunstancias únicas de cada unidad comercial. Un modelo bien conceptualizado es un trampolín para discusiones más profundas y una comprensión del riesgo, un paso esencial o "bloque de construcción" hacia ERM.

76. ¿En qué medida la organización define estrictamente el riesgo para la empresa en su conjunto, cuando el organización tiene una variedad de negocios diferentes?

Un lenguaje de riesgo común comienza en un nivel estratégico para la empresa en su conjunto y se adapta a unidades, geografías y productos específicos. Este enfoque “en cascada” tiene la ventaja de identificar los riesgos que son comunes en toda la empresa. Sin embargo, para las unidades operativas con perfiles de riesgo distintivos, el lenguaje de riesgo general debe personalizarse para abordar los riesgos únicos que enfrentan esas unidades. La distinción es importante. Los riesgos comunes a todas las unidades de negocio impulsan las respuestas al riesgo en toda la empresa. Los riesgos exclusivos de las unidades individuales impulsan las respuestas de riesgo específicas de la unidad.

77. ¿Qué son los mapas de riesgos y cómo se utilizan adecuadamente durante el proceso de evaluación de riesgos?

El mapeo de riesgos es probablemente la herramienta más utilizada por las empresas para identificar y priorizar los riesgos asociados con sus actividades comerciales. El uso más efectivo del mapeo de riesgos ocurre cuando se integra con la planificación comercial y se usa para identificar áreas que requieren un análisis más profundo y respuestas de riesgo específicas. Por ejemplo, como técnica de clasificación y priorización, el mapeo de riesgos es especialmente útil para facilitar el diálogo. Desde una perspectiva de toma de decisiones, es más una herramienta direccional que accionable.

La técnica básica es intuitiva y fácil de entender. Los gerentes de las unidades de negocios evalúan sus riesgos utilizando criterios predeterminados. Sus evaluaciones a menudo abordan un conjunto de posibles eventos futuros identificados por la alta dirección o, alternativamente, posibles eventos futuros identificados por la dirección de la unidad. Una vez que se identifican eventos futuros potenciales bien definidos, se trazan en una cuadrícula o mapa de acuerdo con su impacto en el logro de los objetivos comerciales y la probabilidad de que ocurran.

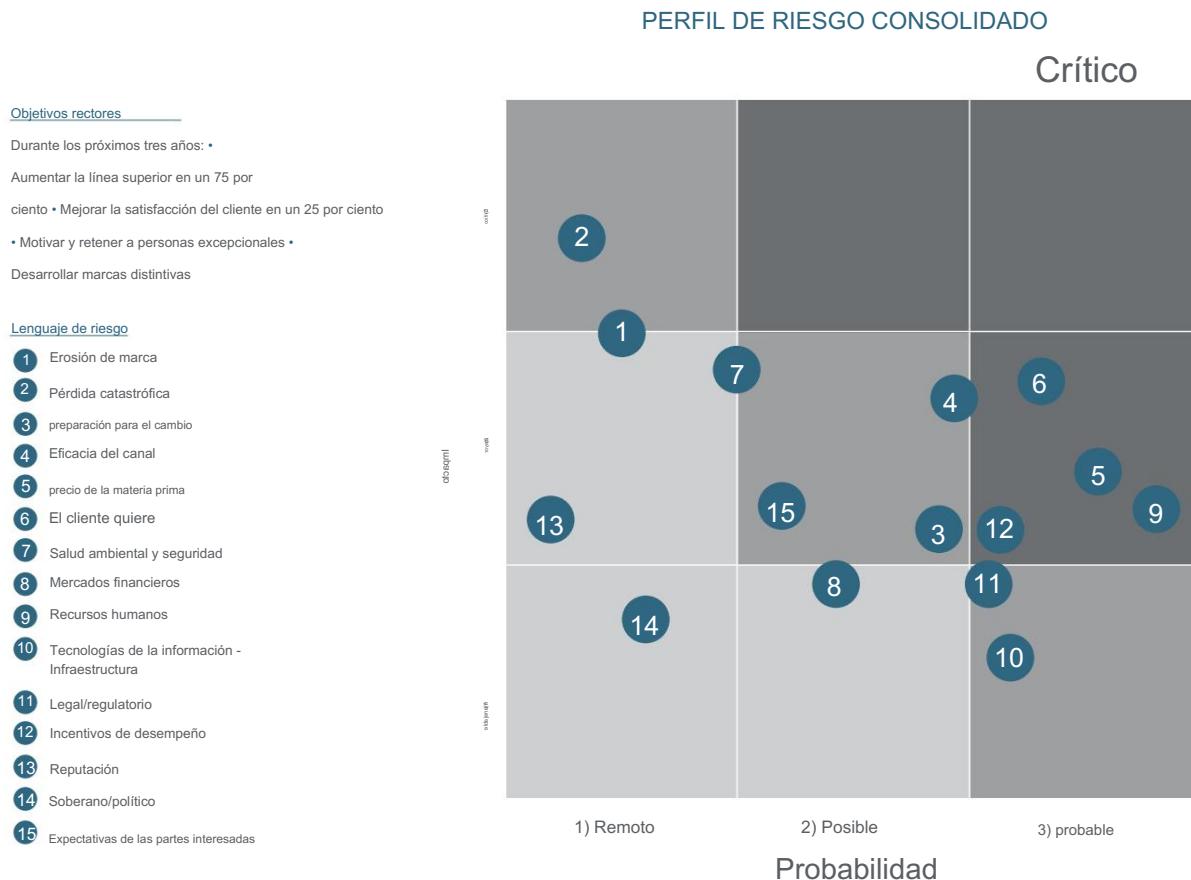
El siguiente es un comentario sobre estas evaluaciones:

- Impacto: La gerencia califica la importancia del riesgo para el negocio en términos del efecto sobre el logro de los objetivos comerciales. La herramienta de mapeo de riesgos es lo suficientemente flexible para considerar otros criterios, incluido el impacto financiero potencial, el impacto en la ejecución de estrategias clave y el costo potencial para el negocio en términos de pérdidas de capital, ganancias, flujo de efectivo y valor de marca. Cuanto mayor sea la importancia del impacto, más grave será el riesgo. Al calificar el impacto, el horizonte temporal es un factor que debe ser claramente

definido. Por ejemplo, una empresa podría evaluar la importancia del riesgo para la ejecución de su estrategia durante los próximos tres años. Otro podría evaluar el riesgo considerando un plan de negocios de un año. horizonte (el marco de tiempo dentro del cual operan muchos gerentes de unidad). Si el horizonte de tiempo no es claro y articulado consistentemente, los participantes en el proceso se confundirán. Por ejemplo, algunos problemas, como como escasez de capacidad, puede ser bastante grave a corto plazo para una empresa de fabricación. Sin embargo, la mayoría de los riesgos, incluida la capacidad, son un problema menor a largo plazo porque la administración tiene más flexibilidad para hacer ajustes. Por lo tanto, la gerencia debe definir el horizonte de tiempo explícitamente. Separado los mapas de riesgo son apropiados para eventos que pueden ocurrir a corto, mediano o largo plazo.

- Probabilidad: Utilizando el mismo horizonte temporal que el utilizado para determinar el impacto, la dirección evalúa la probabilidad de que ocurra un evento potencial identificado, o dos o más eventos potenciales. Cuanto mayor sea el probabilidad de ocurrencia, mayor es la probabilidad. Al estimar la probabilidad, el evaluador debe considerar la calidad de la evaluación en sí. ¿Qué tan probable es el evento riesgoso? Si los métodos estadísticos son no se usa, entonces, ¿cómo sabe que las probabilidades seleccionadas son razonables? Si bien las estadísticas no son necesario en esta etapa del proceso de evaluación, el personal con más conocimientos debe priorizar la riesgos En esta etapa, la gerencia a menudo busca una estimación de orden de magnitud (en contraposición a una número exacto). Hay técnicas disponibles para aplicar el juicio de un "jurado de expertos" para lograr esta evaluación para riesgos críticos no sujetos a una medición rigurosa.

A continuación se muestra un ejemplo de mapa de riesgos:



78. ¿Cuál es una forma efectiva para que una organización realice una evaluación de riesgos?

Hay muchas formas de realizar una evaluación de riesgos. Por ejemplo, las empresas pueden realizar entrevistas o encuestas de personal clave, revisar documentos clave, realizar talleres facilitados, realizar revisiones específicas o utilizar cualquier combinación de estas opciones. La siguiente tabla analiza cada una de estas opciones:

	ENTREVISTAS	ENCUESTAS EN LÍNEA	ENCUESTAS EN PAPEL	REVISIÓN DE DOCUMENTO	TALLERES FACILITADOS	REVISIONES OBJETIVAS
<b>DESCRIPCIÓN</b>	Entrevistas individuales con partes interesadas para identificar eventos potenciales y priorizar el riesgo asociado	Encuesta en línea que consta de una lista de verificación de eventos o riesgos O una solicitud abierta	Encuesta impresa que consta de una lista de verificación de eventos o riesgos O una solicitud abierta	Revisión de documentos públicos existentes, revisiones regulatorias, informes de auditoría, estudios de propósito especial y otros materiales	Un taller en persona o en línea al que asistieron las partes interesadas clave	Estudios especiales o análisis específicos para evaluar preguntas sobre eventos específicos o anticipados, preocupaciones
<b>VENTAJAS</b>	<ul style="list-style-type: none"> <li>La interacción brinda la oportunidad de:           <ul style="list-style-type: none"> <li>- "Preparar el escenario"</li> <li>- Hacer las preguntas de seguimiento apropiadas</li> <li>- Sondear/comprender las causas raíz subyacentes</li> <li>- Aclarar dudas, si es necesario.</li> <li>- Cubrir temas delicados más a fondo.</li> </ul> </li> <li>Más información y profundidad sobre el futuro potencial eventos</li> </ul>	<ul style="list-style-type: none"> <li>Puede ser accedido por los participantes sin limitaciones de tiempo o geografía</li> <li>Puede respaldar el proceso con enlaces a definiciones de riesgo y recursos adicionales</li> <li>Puede entregarse de manera eficiente a bajo costo, aunque no tan rentable como en línea</li> <li>Se puede administrar a un gran número de personas</li> <li>Autodocumentación e informes</li> <li>Eficiente, fácil de administrar a grandes números y geografías</li> <li>Las escalas estandarizadas pueden conducir a una agregación común</li> <li>Puede rastrear el estado</li> </ul>	<ul style="list-style-type: none"> <li>Puede ser completado por los participantes sin limitaciones de tiempo o geografía</li> <li>Se puede entregar de manera eficiente a bajo costo, aunque no tan rentable como en línea</li> <li>Se puede administrar a un gran número de personas</li> <li>Estandarizado las escalas pueden conducir a la agregación común</li> </ul>	<ul style="list-style-type: none"> <li>Alcance integral</li> <li>Basado en hechos</li> <li>Puede proporcionar una base para cuantificar el riesgo</li> <li>Se requiere menos tiempo de las partes interesadas durante el proceso de recopilación de datos</li> <li>No limitado a documentos internos</li> </ul>	<ul style="list-style-type: none"> <li>La interacción entre los participantes informados crea una imagen amplia de los eventos potenciales y el impacto comercial relacionado</li> <li>La interacción estimula descubrimiento de áreas de riesgo previamente no identificadas, que pueden permanecer sin ser detectadas en otros formatos de eventos</li> <li>La estructura proporciona un uso eficiente del tiempo</li> <li>La colaboración genera consenso en torno a los riesgos prioritarios y su impacto</li> <li>Similar a las entrevistas, la interacción brinda la oportunidad de:           <ul style="list-style-type: none"> <li>- "Preparar el escenario"</li> <li>- Hacer preguntas de seguimiento apropiadas</li> <li>- Sondear/comprender las causas raíz subyacentes</li> <li>- Aclarar dudas, si necesario</li> <li>- Cubrir temas delicados más a fondo.</li> </ul> </li> <li>La discusión y la colaboración con respecto a los riesgos prioritarios pueden proporcionar insumos de calidad para la planificación de la respuesta a los riesgos.</li> </ul>	<ul style="list-style-type: none"> <li>Las mismas ventajas señaladas para las revisiones de documentos</li> <li>Realizado por expertos en la materia</li> <li>Se adapta a la comprensión profunda</li> <li>potenciales específicos y el impacto comercial relacionado</li> <li>Puede aplicarse sobre una base macro o micro</li> <li>Puede integrar perspectivas externas/internas</li> <li>Puede proporcionar el riesgo recomendado</li> <li>Pueden responder</li> </ul>
<b>ASUNTOS</b>	<ul style="list-style-type: none"> <li>Tiempo intensivo</li> <li>Desafíos de programación</li> <li>La logística debe ser administrada</li> <li>El entrevistador debe agregar subjetivamente los puntos de datos</li> <li>Las entrevistas individuales no apoyan directamente consenso edificio</li> </ul>	<ul style="list-style-type: none"> <li>Seguimiento limitado</li> <li>Se requiere tiempo posterior a la encuesta para revisar y comprender las respuestas</li> <li>Riesgo de malinterpretación</li> <li>La profundidad de las respuestas puede ser limitada</li> <li>Las respuestas individuales no ganan directamente consenso desde la perspectiva de los demás</li> </ul>	<ul style="list-style-type: none"> <li>Los mismos problemas observados para las encuestas en línea</li> <li>No se considera "mejor práctica"</li> <li>Mayor tiempo transcurrido para enviar y recibir</li> <li>En comparación con las encuestas en línea, más tiempo y esfuerzo para:           <ul style="list-style-type: none"> <li>- Distribuir</li> <li>- Apoyo</li> <li>- Proceso</li> <li>- Monitorear el progreso</li> <li>- Compilar resultados</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>Mayor costo para revisar y analizar el material existente</li> <li>A menudo no mira hacia el futuro</li> <li>Puede que no refleje realidades empresariales actuales</li> <li>Si no está enfocado, puede perder tiempo y dinero</li> </ul>	<ul style="list-style-type: none"> <li>La eficacia depende del facilitador y de una estructura suficiente</li> <li>Requiere planificación anticipada</li> <li>Logísticamente desafiante para organizar la hora y la ubicación de los participantes</li> <li>Puede llevar mucho tiempo debido a la cantidad de personas y la necesidad de aclarar las definiciones de los eventos</li> </ul>	<ul style="list-style-type: none"> <li>Las expectativas deben estar claramente establecidas</li> <li>Debe tener un alcance cuidadoso</li> <li>A menudo requiere más tiempo que otras opciones</li> </ul>

Como se señaló anteriormente, cualquier combinación de estas opciones es adecuada.

Para las empresas que no han completado una evaluación de riesgos en toda la empresa, recomendamos el uso de un taller facilitado que convoque una reunión de las partes interesadas clave para evaluar y priorizar los riesgos. Los talleres de evaluación de riesgos empresariales a menudo son atendidos por miembros del equipo de alta gerencia y también pueden incluir participantes que poseen conocimiento de toda la empresa sobre cumplimiento, tecnología de la información, marketing u otras actividades integrales para la misión central de la organización.

El uso de un taller de riesgos facilitado para evaluar los riesgos ofrece ciertas ventajas sobre una evaluación realizada por una sola persona. Identificar un grupo de partes interesadas con conocimientos y llevarlos a un entorno colaborativo con el fin de evaluar el riesgo puede identificar de manera eficiente los riesgos que surgen en toda la empresa y lograr un consenso y alineación con respecto a los riesgos prioritarios y las posibles acciones a tomar para mitigar esos riesgos.

Además, las sesiones grupales pueden facilitar el aprendizaje al aclarar las diferencias en las perspectivas, crear conciencia sobre las exposiciones más importantes de la organización, sacar a la luz problemas delicados o no reconocidos anteriormente y promover la comunicación entre áreas de responsabilidad individuales. Estas sesiones pueden ir precedidas de entrevistas, una encuesta de riesgos y/o una revisión de documentos para facilitar la reducción de la lista de riesgos a una más manejable con el fin de llevar a cabo el taller dentro del tiempo asignado.

#### 79. ¿Cuáles son los errores y trampas comunes durante el proceso de evaluación de riesgos?

En nuestra respuesta, nos centraremos principalmente en los talleres de riesgo. Los talleres de riesgo inefficientes ocurren por muchas razones: falta de planificación, no adherirse a la agenda, falta de reglas básicas claras y no buscar el aporte de todos los participantes, por nombrar algunos. Para que el proceso de evaluación de riesgos sea efectivo, la gerencia debe tener cuidado de evitar errores comunes y posibles peligros. Estos se indican a continuación:

- Falta de aclaración y entendimiento común del significado o definición de riesgo: Aplicar demasiado Reducir el enfoque al significado del riesgo puede llevar a la gerencia a pasar por alto eventos y problemas potenciales. Es importante considerar todos los objetivos comerciales relevantes como contexto para una evaluación de riesgos.
- No incluir a todas las partes interesadas: No incluir a todas las partes interesadas en el taller, encuesta o proceso de la entrevista puede ser fatal. Las "partes interesadas" incluyen cualquier persona directamente afectada por los temas en discusión o cuya falta de inclusión podría socavar el logro del resultado deseado.
- No considerar o dar el peso adecuado a las posiciones informadas: En una evaluación de riesgo grupal entorno, SIEMPRE habrá uno o dos individuos que saben mucho más sobre un riesgo que los demás. El propósito de la evaluación es escuchar, considerar y aprender de todos los que tienen conocimiento de un riesgo en particular. Por lo tanto, es importante crear un entorno abierto para compartir toda la información sobre un riesgo y llegar a la mejor comprensión posible. La evaluación efectiva de la probabilidad y el impacto de un posible evento futuro no es necesariamente el resultado del número total de votos o respuestas.  
El diálogo suele ser más importante que el proceso de votación durante una evaluación de riesgos.
- Con respecto a un taller de riesgo facilitado:
  - Establecer objetivos poco claros o poco realistas: es importante trabajar con el patrocinador de la reunión para establecer objetivos de la reunión que todos entiendan y acepten.
  - No estructurar la agenda de la reunión para el éxito: una vez que se establecen los objetivos de la reunión, es importante organizar la reunión para garantizar que se alcancen los objetivos. Por ejemplo, tenga en cuenta lo siguiente:
    - ° Guíe al patrocinador de la reunión a través de la agenda propuesta para asegurarse de que esté de acuerdo con ella.
    - ° Si bien el tiempo siempre es limitado, asegúrese de haber asignado suficiente para lograr sus objetivos. Si no lo hace, revise los objetivos para alinearlos con el tiempo disponible.
  - ° Considere cuidadosamente si hay algún aspecto de la agenda que pueda ser diferente de lo que los participantes podrían esperar. Si este es el caso, considere cómo comunicar la decisión de diseño (p. ej., cambio de enfoque, reordenación de la información, etc.) a los participantes de la reunión. Por ejemplo, antes

a una evaluación de riesgos, a los participantes se les puede proporcionar un modelo de riesgo (como se ilustra en la Pregunta 75) y se les puede pedir que consideren la probabilidad de ocurrencia y el impacto potencial de diferentes eventos futuros posibles. Debido a la necesidad de ahorrar tiempo durante la sesión, se toma la decisión de diseñar la agenda para combinar estos dos criterios en una sola evaluación de "nivel de riesgo" para usar durante el taller. Si este cambio no se presenta adecuadamente a los participantes, la diferencia entre su expectativa, que se creó a través de su preparación para la sesión, y la actividad real aplicada durante el taller, puede crear confusión y hacer que el facilitador y el proceso pierdan credibilidad.

Revise los materiales de apoyo (como documentos de planificación estratégica, informes de gestión interna, objetivos comerciales declarados, etc.) cuidadosamente si se incorporarán a un taller. No asuma que todos los participantes están familiarizados con el material, lo entienden y lo apoyan. Verifique los hechos con anticipación.

- Poner muy poco énfasis en la discusión: Recuerde que aunque votar es interesante durante un evento de riesgo taller, es sólo un medio para un fin. La discusión es igual de importante.
- Dejar que las fallas tecnológicas distraigan el proceso: si la tecnología no funciona como debería durante un taller de riesgos (por ejemplo, está usando teclados de votación y solo obtiene nueve votos cuando se supone que debe obtener 10), no permita que el dificultad técnica interrumpir la reunión. Trate de llevar a cabo el taller sin resaltar que las cosas no están funcionando.
- No involucrar a todos: es común que los facilitadores se sientan hipnotizados por la discusión y se pierdan los puntos clave de la discusión. Deben prestar atención a los participantes, observar el ritmo y el tono de la conversación e involucrar a las personas, haciendo que el tiempo de todos sea lo más productivo posible. Si los participantes se aburren o se distraen, el facilitador debe ponerse a trabajar. La participación se correlaciona con el valor percibido recibido de la evaluación.
- No crear un ambiente “seguro” y abierto: Fomentar la comunicación abierta, con acuerdo sobre el uso de la información. Identifique y, si es necesario, conozca y comprenda a la persona que podría socavar los resultados del taller. Por ejemplo, podría ser el director ejecutivo, el presidente de la junta o la persona más importante de la sala. También podrían ser personas que tienden a dominar la discusión. No solo desea saber si comprenden el material que se presenta, sino que también debe asegurarse de que comprendan y apoyen los objetivos del taller. Una evaluación de riesgos facilitada no puede tener éxito sin un entorno abierto en el que pueda tener lugar un debate sincero.
- No aclarar roles y responsabilidades: los facilitadores deben comunicar el enfoque y planificar una agenda con anticipación. Siempre debe haber un solo facilitador. Resuelva las expectativas para que no haya contradicciones entre el facilitador, el experto en la materia y otros miembros del equipo, lo que puede interrumpir el flujo de la reunión.
- Instalaciones deficientes: la forma y el tamaño de la sala son importantes durante un taller de riesgos. Trate de evitar las mesas de conferencias, si es posible. La capacidad del facilitador para moverse dentro de un entorno en "forma de U" apoya la interacción del grupo. Esta dinámica puede y debe aplicarse para crear un entorno sólido para la comunicación. Anima a los participantes a involucrarse más. • Con respecto al establecimiento de las reglas básicas para una evaluación de riesgos:

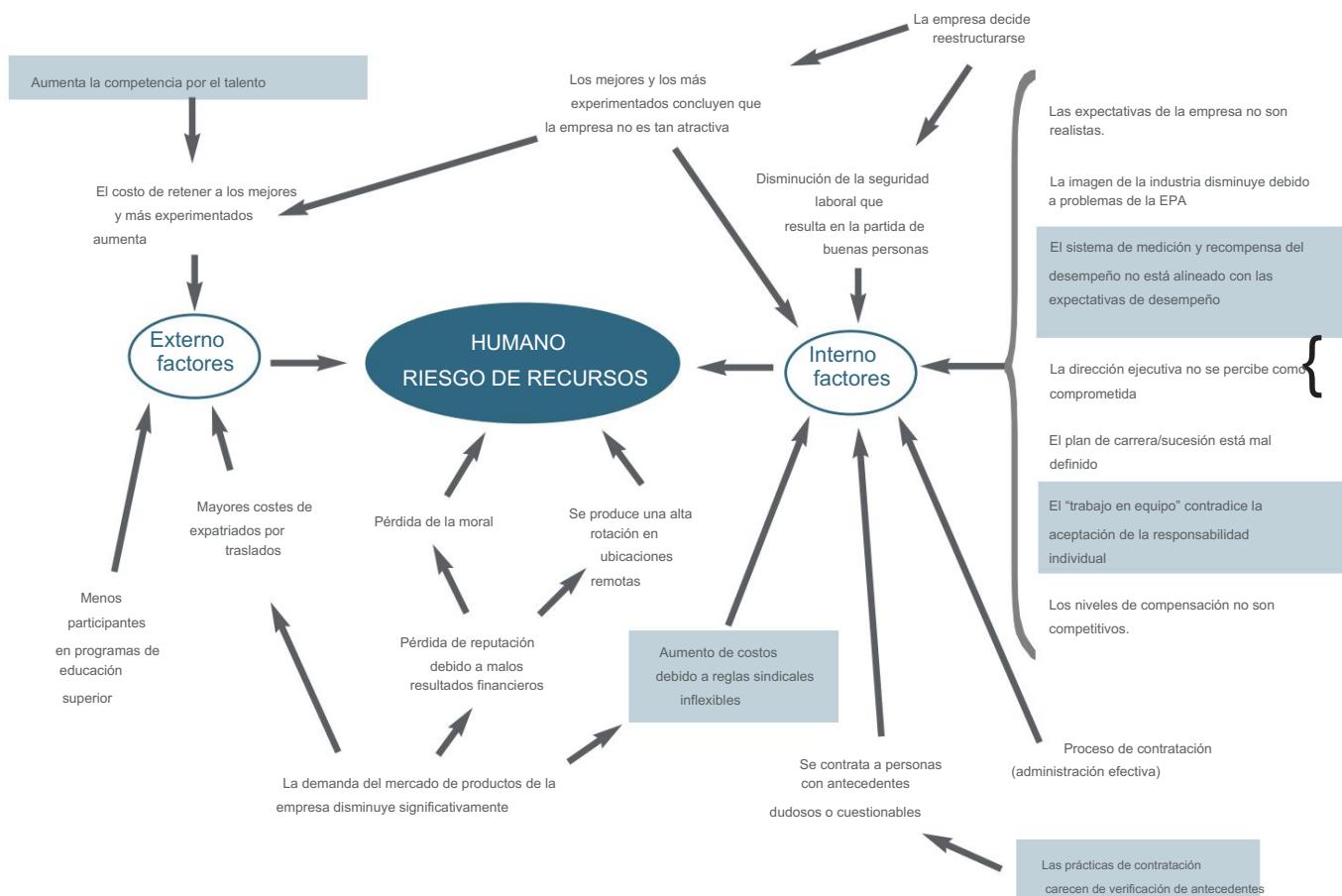
- Falta de comprensión por parte de los participantes de cómo aplicar los criterios de evaluación de manera consistente: Los participantes deben comprender los criterios para evaluar el impacto y la probabilidad de ocurrencia. Si existe confusión en la aplicación de la escala utilizada durante la evaluación, el proceso no será exitoso.
- Confusión sobre el riesgo inherente: Esta es un área que confunde a muchos participantes en una evaluación de riesgos. Ver nuestra respuesta a la pregunta 74.
- Confusión sobre el horizonte temporal: Esta es otra área que confunde a los participantes. Vea nuestra respuesta a Pregunta 77.
- No reconocer que el futuro es inherentemente incognoscible: en la superficie, este punto es obvio. Sin embargo, muchos gerentes a menudo evalúan el futuro con una perspectiva de "estimación de un solo punto". Por eso es importante estar abierto a una amplia gama de posibilidades durante una evaluación de riesgos. El arte y la ciencia de la evaluación de riesgos deben aplicarse para crear la mayor probabilidad de éxito en la identificación de posibles eventos futuros, la evaluación de su probabilidad e impacto y la formulación de respuestas de riesgo rentables.

- Pasar por alto los eventos del entorno externo debido a la percepción de que están fuera de control de la dirección: una evaluación de riesgos debe centrarse en todos los posibles eventos futuros de consecuencia, ya sean controlables o no. Por ejemplo, si bien la gerencia puede no tener control directo sobre los resultados políticos y legislativos, existen actividades de mitigación potenciales que solo pueden desarrollarse mediante la evaluación de esta categoría de riesgo. Para ilustrar, estas actividades pueden incluir cabildeo, campañas de concientización, planes para responder a cambios en el entorno político, etc.
- Ignorar las interrelaciones entre riesgos: Los participantes de una evaluación de riesgos deben reconocer que existen interrelaciones causa-efecto entre múltiples eventos, con la ocurrencia de algunos eventos que causan o desencadenan la ocurrencia de otros eventos. Este es un punto que requiere reflexión y consideración durante el proceso de evaluación de riesgos.

#### 80. ¿Cómo identificamos, entendemos y aplicamos las interrelaciones entre los riesgos?

El marco COSO establece: "Dónde los eventos potenciales no están relacionados, la gerencia los evalúa individualmente... Pero cuando existe una correlación entre los eventos, o los eventos se combinan e interactúan para crear probabilidades o impactos significativamente diferentes, la gerencia los evalúa en conjunto. Si bien el impacto de un solo evento puede ser leve, el impacto de una secuencia o combinación de eventos puede ser más significativo".

La mayoría de las personas pueden visualizar cómo evaluar un evento individual. La pregunta que muchos hacen es: "¿Cómo evalúa múltiples eventos interrelacionados?" Existen varios enfoques para identificar y comprender las interrelaciones entre los riesgos. Uno, un mapa de factores de riesgo, se ilustra a continuación:



El hilo común en todos los enfoques, incluido el de la ilustración anterior, se reduce a evaluar la siguiente pregunta: ¿La ocurrencia de un evento, ya sea individualmente o en combinación con otros eventos, hará que suceda otro evento o, alternativamente, afectará, impactar o contribuir a la severidad de otro evento? Por ejemplo, siguiendo un patrón de análisis como el que se acaba de ilustrar, se puede describir un modelo de interrelaciones entre eventos para una categoría de riesgo ("riesgo de contratación y retención"). A través del refinamiento de este análisis de causa y efecto, la gerencia puede seleccionar los eventos más críticos (los que están sombreados en la ilustración anterior) y enfocar su atención adicional en comprenderlos.

Al examinar los eventos críticos relacionados con múltiples categorías de riesgo, la gerencia puede evaluar las interrelaciones entre esos eventos. Esta comprensión de los posibles eventos futuros para generar por qué, cómo y dónde se originan los riesgos de la entidad sienta las bases para desarrollar herramientas de medición y seguimiento que aborden el riesgo a través de una visión de cartera.

81. ¿Cuál es el nivel apropiado de profundidad al evaluar el riesgo?

El juicio sobre el nivel de profundidad en el que se evalúan los riesgos se realiza dentro del contexto de los objetivos y eventos que se evalúan. Para elaborar una respuesta adecuada al riesgo, debe haber suficiente claridad en cuanto a la naturaleza del riesgo, incluido cómo, por qué y dónde se origina. La comprensión de la naturaleza del riesgo facilita el desarrollo de una estrategia de mitigación. Si los riesgos se evalúan a un nivel demasiado alto, es difícil identificar el problema preciso y la gerencia no podrá decidir qué hacer después de completar la evaluación. Al mismo tiempo, si la evaluación se lleva a cabo a un nivel demasiado granular, los problemas del "panorama general" se pierden en un mar de detalles y será difícil completar la evaluación de riesgos en un tiempo razonable.

Por lo tanto, el evaluador puede encontrar útil un lenguaje común para agregar múltiples eventos de riesgo con el fin de realizar la evaluación de riesgos. Luego, los riesgos prioritarios pueden desglosarse en posibles eventos futuros relevantes al formular una respuesta de riesgo adecuada. La experiencia es el mejor maestro en cuanto al nivel apropiado de profundidad para realizar una evaluación de riesgos. En última instancia, el objetivo no es la evaluación de riesgos en sí, sino ir más allá de la página impresa de la evaluación de riesgos hacia pasos prácticos en el plan de negocios.

82. ¿Quién debe participar durante el proceso de evaluación de riesgos?

La participación apropiada en el proceso de evaluación de riesgos está influenciada por el objetivo de la evaluación de riesgos y el alcance de los riesgos que se evalúan. A nivel de entidad, debe incluirse la dirección ejecutiva. En algunos casos, se pueden incluir personas con conocimientos específicos de riesgos, problemas y operaciones comerciales únicos para proporcionar información sobre sus áreas específicas. En los demás casos, podrá contratarse el consejo de administración.

A nivel de unidad, la gestión de la unidad y los propietarios de procesos clave deben incluirse en el proceso de evaluación.

83. ¿Cómo se relaciona la evaluación del riesgo con la cuantificación del riesgo y se debe utilizar la cuantificación del riesgo?  
durante la evaluación de riesgos?

La evaluación de riesgos mejora y es más sólida cuando se cuantifican los riesgos. Cuando se cuantifica el riesgo, se puede monitorear contra la tolerancia al riesgo establecida por la administración (ver Pregunta 67). Las medidas de riesgo se analizan con más detalle en nuestra respuesta a la Pregunta 112.

84. ¿Tiene valor usar información cualitativa al evaluar el riesgo?

Sí. Debido a que el futuro es inherentemente un "desconocido", a menudo es necesario realizar evaluaciones cualitativas del impacto y la probabilidad de riesgo utilizando la mejor información disponible. Algunos riesgos no se prestan a la medición cuantitativa porque los eventos relacionados ocurren con poca frecuencia y, si ocurren y cuando ocurren, están sujetos a una gama tan amplia de posibles resultados en términos de gravedad que es difícil, si no imposible, determinarlos. cuantificarlos. Cuando ese es el caso, los gerentes más cercanos a la fuente del riesgo son las personas mejor posicionadas para comprender su naturaleza y las causas fundamentales. Considere el riesgo para una organización de fabricación de automóviles cuando una conexión eléctrica defectuosa conduce a la falla de los frenos para un modelo de automóvil en particular. El impacto directo de administrar el programa de recuperación e incurrir en costos de garantía para ese modelo en particular puede proyectarse en base a información cuantitativa. El impacto en las ventas de otros modelos y el tiempo y costo para superar los efectos del daño a la reputación de la empresa en general es un juicio cualitativo que se evalúa mejor

a través del aporte colectivo de marketing, ventas, producción y economistas. Al aplicar datos cualitativos, es útil obtener perspectivas de múltiples personas, ya que la visión del riesgo de cualquier persona se limitará a su propia experiencia y puede verse afectada por su propio interés personal en el resultado de la evaluación.

La información cualitativa es más efectiva cuando se usa junto con métricas confiables y otros datos cuantitativos. Cuando no se dispone de métricas fiables, la información cualitativa suele ser direccional en el mejor de los casos (es decir, sirve como indicador de áreas específicas para una mayor investigación y análisis) y no es eficaz para impulsar las decisiones de gestión.

---

## PRIMEROS PASOS: ESTABLECER LAS BASES

85. ¿Cuáles son los mejores pasos a seguir para empezar?

Para las organizaciones que eligen ampliar su enfoque de gestión de riesgos a ERM, existen cinco pasos prácticos de implementación para comenzar. Si bien estos pasos brindan una vista simplificada de la tarea de implementar ERM, el proceso de implementación no ocurre de la noche a la mañana y, por cierto, no es fácil de lograr. ERM es un viaje.

Estos pasos proporcionan un punto de partida para ese viaje. Es importante que todos estos pasos cuenten con el apoyo de la alta dirección y que se hayan establecido las bases adecuadas para obtener la aceptación de todos los participantes.

**PASO 1:** Realice una evaluación de riesgos empresariales (ERA) para evaluar y priorizar los riesgos críticos.

Una ERA identifica y prioriza los riesgos de una empresa y proporciona información de calidad con el fin de formular respuestas de riesgo efectivas, incluida información sobre el estado actual de las capacidades en torno a la gestión de los riesgos prioritarios. Es una evaluación de riesgos que abarca toda la organización, incluidas las unidades comerciales críticas, las áreas funcionales y los procesos comerciales. Abarca los componentes de establecimiento de objetivos, identificación de eventos y evaluación de riesgos del marco COSO ERM y proporciona una visión holística de la cartera del riesgo. Se aplica utilizando la estrategia empresarial como contexto. Las preguntas 69 a 84 brindan orientación sobre la realización de evaluaciones de riesgos.

Si una empresa no ha identificado y priorizado sus riesgos, ERM se convierte en una venta difícil para la alta gerencia porque la propuesta de valor solo puede ser genérica. El uso de los riesgos prioritarios de la entidad para identificar brechas proporciona la base para mejorar la especificidad de la propuesta de valor de ERM. Los riesgos se priorizan tomando como marco de referencia la estrategia de negocio.

**PASO 2:** Articular la visión de la gestión de riesgos y respaldarla con una propuesta de valor convincente utilizando las lagunas en torno a los riesgos prioritarios.

Este paso proporciona la justificación económica para seguir adelante. La “visión de gestión de riesgos” es una visión compartida del papel de la gestión de riesgos en la organización y las capacidades deseadas para gestionar sus riesgos clave. Se discute más en las Preguntas 64 y 65. Para que sea útil, esta visión debe basarse en capacidades específicas que deben desarrollarse para mejorar el desempeño de la gestión de riesgos y lograr las metas y objetivos seleccionados por la gerencia.

Las “capacidades de gestión de riesgos” incluyen las políticas, los procesos, las competencias, los informes, las metodologías y la tecnología necesarios para ejecutar la respuesta de la organización a la gestión de sus riesgos prioritarios. También consisten en lo que llamamos “infraestructura ERM”. En términos de tomar decisiones sobre si mejorar la infraestructura ERM, hay dos puntos a tener en cuenta:

Punto (1): La definición de las capacidades específicas en torno a la gestión de los riesgos prioritarios comienza con la priorización de los riesgos críticos (consulte el Paso 1 con respecto a la realización de una ERA) y la determinación del estado actual de las capacidades en torno a la gestión de esos riesgos. Una vez que se determina el estado actual de las capacidades para cada uno de los riesgos clave, se evalúa el estado deseado con el objetivo de identificar brechas y avanzar en la madurez de las capacidades de gestión de riesgos para cerrar esas brechas.

Punto (2): La infraestructura de ERM consiste en las políticas, los procesos, la supervisión de la organización y los informes establecidos para inculcar el enfoque, la disciplina y el control apropiados en torno a la mejora continua de las capacidades de gestión de riesgos. Los ejemplos de elementos de la infraestructura ERM incluyen, entre otros

cosas, una política general de gestión de riesgos, un proceso de evaluación de riesgos en toda la empresa, presencia de la gestión de riesgos en la agenda de la junta directiva y del director general, uno o más comités de riesgos autorizados, claridad de las funciones y responsabilidades de la gestión de riesgos, tablero y otros informes de riesgos, y herramientas patentadas que retratar una visión de cartera del riesgo.

¿Cuál es el mensaje? Cuanto mayor sea la brecha entre el estado actual y el estado deseado de las capacidades de gestión de riesgos de la organización [Punto (1)], mayor será la necesidad de una infraestructura ERM [Punto (2)] para facilitar el avance de esas capacidades de gestión de riesgos a lo largo del tiempo. Un grupo de trabajo de altos ejecutivos debe estar facultado para articular el papel de la gestión de riesgos en la organización y determinar la estructura y el cronograma para hacerlo realidad. Este grupo debe articular un caso comercial convincente que defina las capacidades esperadas de la solución ERM y la justificación económica para seguir adelante.

Las entradas anteriores facilitan este proceso.

PASO 3: Mejorar la capacidad de gestión de riesgos de la organización para uno o dos riesgos prioritarios.

Este paso enfoca a la organización en mejorar su capacidad de gestión de riesgos en un área donde la gerencia sabe que se necesitan mejoras. Como cualquier otra iniciativa, ERM debe comenzar en alguna parte.

Los posibles puntos de partida incluyen:

- Cumplimiento de iniciativas corporativas o de gobierno como la Ley Sarbanes-Oxley o Basilea II
- Evaluar los resultados de la evaluación de riesgos en toda la empresa para identificar áreas prioritarias además de los informes financieros (por ejemplo, otros riesgos de cumplimiento, riesgos de tecnología de la información, riesgos operativos seleccionados, etc.)
- Integración de ERM con las estructuras y procesos de gestión existentes (p. ej., gestión estratégica, planificación comercial anual, lanzamiento de nuevos productos o expansión de canales, iniciativas de calidad, medición y evaluación del desempeño, producción en el extranjero y planificación de subcontratación, etc.)

PASO 4: Evaluar la capacidad de la infraestructura ERM existente y desarrollar una estrategia para mejorarlala.

Se necesita disciplina para mejorar las capacidades en torno a la gestión de riesgos críticos. Las políticas, los procesos, la organización y los informes que inculcan esa disciplina se denominan "infraestructura ERM". El propósito de la infraestructura ERM es eliminar brechas significativas entre el estado actual y el estado deseado de las capacidades de la organización en torno a la gestión de sus riesgos clave. Algunos ejemplos de infraestructura ERM se proporcionaron anteriormente cuando se discutió el Paso 2. Otros ejemplos incluyen un lenguaje de riesgo común y otros marcos, intercambio de conocimientos para identificar las mejores prácticas, capacitación común, un director de riesgos (o ejecutivo equivalente), definición de apetito de riesgo y riesgo, tolerancias, integración de respuestas de riesgo con planes de negocios y tecnología de apoyo. La infraestructura de ERM se analiza con más detalle en la Pregunta 37.

La infraestructura de ERM facilita tres cosas muy importantes con respecto a la implementación de ERM. En primer lugar, establece una comprensión basada en hechos sobre los riesgos de la empresa y las capacidades de gestión de riesgos. En segundo lugar, asegura que haya propiedad sobre los riesgos críticos. Finalmente, impulsa el cierre de brechas significativas. Si la estructura de supervisión organizacional existente proporciona la disciplina, el enfoque y el control para hacer que estas cosas sucedan, entonces se necesitan muy pocos cambios organizacionales para hacer avanzar la implementación de ERM.

La infraestructura de ERM no es única para todos. Lo que funciona para una organización puede no funcionar para otras.

Los elementos de la infraestructura de ERM varían según las técnicas y herramientas implementadas para implementar el marco COSO, la amplitud de los objetivos abordados, la cultura y el apetito por el riesgo de la organización, la naturaleza de sus riesgos y el alcance de la cobertura deseada en todas las unidades operativas de la organización. La gerencia decide los elementos necesarios de la infraestructura ERM de acuerdo con estos y otros factores. Al tomar esta decisión, la gerencia considera los elementos de la infraestructura de ERM que ya existen.

PASO 5: Actualice la ERA para el cambio y avance en las capacidades de gestión de riesgos para riesgos clave.

En esta etapa, la organización ha avanzado en sus capacidades para uno o dos riesgos prioritarios (consulte el Paso 3) y ha implementado la infraestructura de ERM (consulte el Paso 4) para que estas mejoras sucedan. Ahora la gerencia está en condiciones de ampliar el enfoque a otros riesgos prioritarios actualizando la ERA para el cambio y determinando el

estados actuales y deseados para cada riesgo prioritario utilizando la estrategia de negocio como contexto. El objetivo es avanzar en la madurez de las capacidades en torno a la gestión de los riesgos prioritarios.

Las capacidades de gestión de riesgos deben diseñarse y avanzar, de acuerdo con los recursos finitos de una organización. Para cada riesgo prioritario, la dirección evalúa la madurez relativa de las capacidades de gestión de riesgos de la empresa. A partir de ahí, la gerencia debe tomar una decisión consciente: ¿Cuánta capacidad adicional necesitamos para brindar una seguridad razonable de que lograremos nuestros objetivos comerciales? Además, ¿cuáles son los costos y beneficios esperados de aumentar las capacidades de gestión de riesgos? El objetivo es identificar las exposiciones e incertidumbres más apremiantes de la organización y centrarse en la mejora de las capacidades para gestionar dichas exposiciones e incertidumbres. La infraestructura de ERM que la administración ha elegido implementar impulsa el progreso hacia este objetivo.

El modelo de madurez de la capacidad discutido en nuestra respuesta a la Pregunta 111 proporciona un marco para evaluar la madurez de las capacidades de gestión de riesgos de una organización. Con este modelo, la gerencia califica las capacidades de la empresa en áreas de riesgo clave, identifica las brechas según el nivel de capacidad deseado en áreas específicas y cambia el diálogo sobre las métricas operativas para incorporar el énfasis apropiado en la madurez del proceso. La infraestructura de ERM garantiza que el proceso de evaluación se base en hechos y sea realizado con integridad por los propietarios de riesgos participantes. Cuando existan brechas inaceptables, la empresa debe organizar actividades apropiadas para construir, probar e integrar con el tiempo las capacidades esperadas, como se describe en el caso de negocios.

#### 86. ¿Es ERM otro “proyecto”?

No. ERM es un viaje porque representa un compromiso con la mejora continua. Debido a que los riesgos de una organización cambian constantemente, sus capacidades de gestión de riesgos deben mejorar constantemente.

ERM proporciona el enfoque, la disciplina y el control para hacer que eso suceda con el tiempo dentro del contexto del proceso de establecimiento de la estrategia.

#### 87. ¿Hay cosas específicas que una organización debería lograr el primer año?

La organización debe comprender los objetivos generales de gestión de riesgos y obtener la aceptación de la alta dirección. Idealmente, la organización debería sentar las bases adoptando un lenguaje común y estableciendo una supervisión y una gobernanza eficaces. Sobre la base de estos elementos de la infraestructura de ERM, la organización construye el proceso apropiado con énfasis inicialmente en un proceso continuo de evaluación de riesgos en toda la empresa. Durante el primer año, las empresas también deben considerar lo siguiente:

- Inventariar las actividades que pueden estar ocurriendo en toda la empresa para mejorar la gestión de riesgos capacidades y aprovechar esas actividades.
- Aprovechar los resultados de evaluaciones de riesgos anteriores tanto como sea posible para obtener información sobre las áreas prioritarias.
- Tener en cuenta el estado actual de las capacidades existentes utilizando el modelo de madurez de capacidades (ver Pregunta 111) y evitar la ingeniería excesiva del proceso.
- Concéntrese en lograr éxitos visibles.

#### 88. ¿Quién es responsable de “liderar la carga” para implementar ERM?

La dirección ejecutiva es responsable de liderar la implementación de ERM. Deben demostrar un compromiso con ERM a través de acciones consistentes para crear y mantener el impulso de la iniciativa. Vea nuestras respuestas a las Preguntas 7, 39, 40 y 89.

89. ¿Quién debe patrocinar la implementación de ERM?

Si bien pueden delegar responsabilidades específicas a otros, el director ejecutivo y el equipo de gestión ejecutiva deben ser los patrocinadores finales de la implementación de ERM. Consulte las preguntas 39 y 40.

90. ¿Cómo se obtiene la aceptación de los altos ejecutivos clave?

Aumentar las capacidades de ERM requiere un enfoque enfocado y disciplinado que sea consistente con la estructura y cultura de la organización y con la filosofía operativa de la gerencia. Las siguientes son sugerencias para obtener la aceptación de los altos ejecutivos:

- Compromiso y apoyo de la alta dirección: La disciplina comienza en la parte superior con un director ejecutivo y una dirección ejecutiva comprometidos que demuestren su apoyo a ERM a través de acciones coherentes que creen y mantengan el impulso de la iniciativa. Deben decidir si seguir adelante y, una vez que se tome esa decisión, deben brindar un apoyo inquebrantable. Para obtener su aceptación, la iniciativa ERM debe integrarse con los procesos de gestión existentes y vincularse a cuestiones importantes que están claramente en la agenda de la alta dirección. La gerencia ejecutiva tendrá poco apetito por un apéndice o superposición.
- Con la asistencia de la gerencia ejecutiva, desarrolle un sólido caso de negocios que aclare por qué mejorar la gestión de riesgos es la única opción: Un caso de negocios aborda los puntos de presión internos y externos que crean la necesidad de cambio, así como el estado de preparación y las estructuras existentes que pueden impulsar o restringir el cambio. La dirección ejecutiva debe responder a la siguiente pregunta: "¿Cuál es el papel de la gestión de riesgos en nuestra organización?" Como se discutió en la Pregunta 85, el caso de negocios debe basarse en los riesgos prioritarios de la organización y en las brechas en las capacidades en torno a la gestión de esos riesgos. Debe afirmar y explicar por qué la gestión de riesgos es parte integral del establecimiento de la estrategia. Consulte las Preguntas 134 a 136 para obtener más información sobre el caso comercial.
- Concéntrese en el panorama general con una visión compartida convincente: una vez que se ha establecido la necesidad, la gerencia debe proporcionar una visión convincente y compartida del estado de la meta futura que brinde dirección para un cambio positivo. Esta visión debe describir claramente el alcance, las metas y los objetivos de la iniciativa de ERM y articular "qué hay para mí" para todos los que se espera que contribuyan al proceso de diseño e implementación. Esta visión debe articular una propuesta de valor que destaque las brechas inaceptables en las capacidades de gestión de riesgos (consulte la Pregunta 85) y proporcione una justificación económica para cerrar esas brechas.
- Establezca metas realistas: los objetivos de gestión de riesgos no deben exceder la capacidad de la empresa para ejecutar las capacidades de gestión de riesgos. Por ejemplo, no se puede esperar que una organización en la etapa inicial o repetible en áreas de riesgo específicas, como se explica con más detalle en la Pregunta 111, funcione en el estado administrado de la noche a la mañana. Los objetivos deben ser comprensibles, medibles y procesables.
- Desarrolle un plan de acción claro: un plan bien definido para el cambio proporciona una hoja de ruta para que la organización avance, así como hitos para monitorear el progreso. Este plan apoya el caso de negocios.
- Hacer uso periódico de puntos de control de gestión: los puntos de control de gestión sirven para muchos propósitos. Lo que es más importante, mantienen el programa dentro del plan y la estrategia, sirviendo tanto como un control de la realidad como una reafirmación del apoyo de la gerencia. También proporcionan la motivación necesaria para hacer avanzar las actividades de diseño e implementación.

91. ¿Cómo obtenemos aceptación entre nuestros gerentes operativos?

El personal operativo tiene muchas exposiciones. Administran inventarios, plantas, equipos y otros activos físicos; productos y procesos; marcas; relaciones externas con clientes y proveedores; y personas talentosas y capacitadas. Estas fuentes de valor se ven afectadas por muchas incertidumbres. Por ejemplo, los cambios en la demografía pueden afectar la demanda de los productos de la empresa por parte de los clientes. También pueden afectar el grupo de talentos.

de personas que realizan tareas calificadas dentro del negocio, elevando así la apuesta en la búsqueda de talento. En tiempos riesgosos de hoy, los operadores pueden beneficiarse al pensar en los riesgos que enfrentarán en el futuro y las alternativas disponibles para gestionar esos riesgos.

Uno de los desafíos que enfrentan los operadores con la gestión de riesgos es la inmediatez del entorno operativo. Los operadores se ocupan de los problemas diarios de calidad, tiempo y rentabilidad. La evaluación de riesgos presenta una desafío porque es una actividad con visión de futuro centrada en un horizonte de tiempo que a menudo se extiende mucho más allá la rutina diaria del entorno operativo.

La aceptación se obtiene primero de los gerentes operativos a través del apoyo de la alta dirección. Además, los gerentes operativos necesitan evidencia convincente de que la solución ERM los ayudará a administrar sus unidades operativas y divisiones con mayor eficacia. Las siguientes son sugerencias para lograr la apropiación y compromiso de los operadores:

- Obtener la participación y el compromiso de las partes interesadas: Identificar líderes clave en toda la organización y obtener su apoyo para la implementación de ERM. Un proceso de cambio eficaz hace que las partes interesadas clave se trasladen a lo largo de un continuo desde la conciencia hasta la aceptación y, en última instancia, hasta la propiedad.
- Establecer responsabilidad por los resultados: La comprensión de las personas y los problemas de responsabilidad es uno de los pasos más vitales del proceso de cambio. Una meta de ERM es incorporar la gestión de riesgos en el agenda diaria y procesos de toma de decisiones de la organización. Esto significa que, en última instancia, cada gerente es el responsable. Esto sólo puede suceder si los objetivos están claramente articulados y las individuos son responsables de los resultados.
- Habilite el cambio centrándose en el "lado humano": con demasiada frecuencia, el enfoque del cambio se limita a aspectos técnicos. asuntos tales como políticas y límites, procesos, medidas, informes, sistemas y datos, todo lo cual define la infraestructura para una respuesta al riesgo. Si bien son importantes, estos no son los únicos objetos de cambio. A lenguaje común, comunicaciones efectivas, conciencia de riesgo e intercambio efectivo de conocimientos también son importante.
- Apoyar el proceso de implementación: El viaje hacia ERM requiere un enfoque sistemático utilizando técnicas sólidas de gestión de proyectos y disciplina. El proceso de implementación debe ser apoyado con recursos dedicados, estándares apropiados, mejores prácticas, medidas y mecanismos de retroalimentación. El uso de pruebas piloto, así como comunicaciones claras con respecto al propósito y la autoridad de la implementación. Los equipos son vitales para empoderar al personal clave para que haga lo que necesita hacer para tener éxito.
- Alinear las medidas de desempeño organizacional, de proceso e individual: Los sistemas de recompensas de la empresa y los planes de incentivos deben estar alineados con el proceso de cambio a través de métricas de desempeño apropiadas.
- Alinear el proceso de cambio con la cultura de la empresa: ERM no puede verse como una iniciativa independiente sino debe convertirse en una parte integral de los procesos comerciales existentes: "la forma en que hacemos las cosas aquí". La gerencia debe basarse en las prácticas actuales que respaldan la visión de la gestión de riesgos y desarrollar nuevas o procedimientos, herramientas y técnicas mejorados que serán aceptados dentro de la organización. Por integrando estos procedimientos, herramientas y técnicas en procesos ya establecidos, gestión logra un "salpicado silencioso" en lugar de implementar "otro programa".

Las prácticas de habilitación del cambio anteriores, así como las prácticas descritas en la Pregunta 90, se resumen en el siguiente cuadro, junto con las consecuencias si no se ejecutan de manera competente. Si se ejecutan, conducen al cambio sostenible. Si no, no pasa nada.



#### 92. ¿Podemos aprovechar la infraestructura existente para no generar más gastos generales?

Si la infraestructura de ERM no se basa en estructuras y procesos de gestión existentes, es probable que sea visto como un apéndice. Al integrar ERM en procesos que ya están implementados, el costo de se reducen los gastos generales. Por ejemplo, la gerencia puede construir una infraestructura de ERM en la gestión estratégica, proceso, el proceso de planificación empresarial, el proceso Six Sigma (u otras iniciativas de calidad), el proceso de la organización medición del desempeño (por ejemplo, el "cuadro de mando integral") y/o el proceso de cumplimiento. Además, la dirección debe tener en cuenta las iniciativas existentes para mejorar la gestión de riesgos. ERM debería no debe implementarse en el vacío.

#### 93. ¿Qué tipos de habilidades se necesitan para implementar ERM?

Depende de la naturaleza de las capacidades necesarias para cerrar brechas significativas y definir el ERM deseado infraestructura. No hay una talla para todos. Las habilidades necesarias dependen de las políticas, procesos, medidas, metodologías y capacidades de los sistemas de gestión decide que la organización requiere. Eso es por qué una evaluación de riesgos empresariales que identifique los riesgos prioritarios y un análisis de brechas en torno a las capacidades para gestionar los riesgos prioritarios son muy importantes.

#### 94. ¿Necesitamos poner un nombre a una iniciativa de ERM, es decir, no es ERM solo una buena práctica comercial con ¿otro nombre?

ERM es definitivamente una buena práctica comercial y las organizaciones pueden llamarlo como quieran. De hecho, no hay requisito o necesidad de llamar a las mejoras e iniciativas de la organización para implementar ERM por ese nombre. Algunas organizaciones integran procedimientos, herramientas y técnicas en procesos ya establecidos, y no etiquete el esfuerzo con un nombre. Su enfoque es mejorar "lo que ya hacemos".

95. ¿Las empresas suelen agregar personal a tiempo completo para desarrollar e implementar con éxito un ERM? proceso y sistema, o normalmente utilizan personal existente que dedica sus esfuerzos a esta iniciativa a tiempo parcial o completo?

Hacen ambas cosas, con énfasis en la última. Nuevamente, depende de lo que la empresa decida implementar. Una evaluación de riesgos empresariales que identifique los riesgos prioritarios y un análisis de brechas en torno a las capacidades para administrar los riesgos prioritarios brindan información sobre las respuestas a esta pregunta.

96. ¿Qué pasos toma la administración para sentar las bases?

Para las empresas que están comenzando, sentar las bases es clave. Hay dos grupos de capacidades a tener en cuenta al establecer las bases: adoptar un lenguaje común y establecer supervisión y gobernanza. Estas capacidades no son una progresión lineal. Pueden abordarse al mismo tiempo, con elecciones con respecto a una que ejerce influencia sobre las elecciones que afectan a la otra. Además, no es necesario seleccionar todas las capacidades básicas posibles al diseñar una solución ERM. La gerencia solo necesita seleccionar las capacidades suficientes para proporcionar un lenguaje común y establecer la supervisión y la gobernanza relacionadas con la gestión de riesgos. Una vez que se establece la base, la gerencia construye los componentes del proceso ERM.

A continuación, se incluye un resumen de ejemplos de posibles elementos a considerar al establecer la base:

#### ESTABLECER LA BASE

	Adoptar Común Idioma	Establecer Supervisión y Gobernanza
¿El Entidad tiene:	¿Un lenguaje común para los riesgos y la gestión de riesgos?	¿Supervisión y gobierno de riesgos efectivos para la empresa en su conjunto?
Possible Capacidades:	<ul style="list-style-type: none"> <li>Componentes personalizados de gestión de riesgos (marco COSO ERM)</li> <li>Modelo de riesgo</li> <li>Glosario de gestión de riesgos</li> <li>Esquema de clasificación de procesos</li> <li>Otros marcos relevantes</li> <li>Diálogo mejorado sobre el riesgo y sus fuentes, impulsores o raíz causas</li> <li>Intercambio más organizado de conocimientos e información sobre riesgos</li> </ul>	<ul style="list-style-type: none"> <li>Política general de gestión de riesgos</li> <li>Comunicaciones de arriba hacia abajo del apetito por el riesgo y la dirección de la gestión del riesgo</li> <li>Estructura de supervisión de la organización, con participación anticipada y proactiva de la junta directiva Comité(s) de supervisión de la gestión de riesgos y rendición de cuentas de la gerencia Alto ejecutivo designado</li> <li>responsable de la gestión de riesgos (p. ej., director de riesgos)</li> <li>Gestión de riesgos y procesos de gobierno integrados Función del personal de gestión de riesgos empresariales</li> </ul>
Valor Proposición:	<ul style="list-style-type: none"> <li>Mayores posibilidades de identificar todos los riesgos clave</li> <li>Las personas de múltiples disciplinas se enfocan en los problemas más rápido</li> </ul>	<ul style="list-style-type: none"> <li>Claridad en cuanto a la función y el propósito de la gestión de riesgos</li> <li>Mejor articulación del apetito por el riesgo, es decir, los riesgos que se deben tomar y los riesgos que se deben evitar</li> <li>Realice tareas de gestión de riesgos más rápido con ejecutivos facultados para actuar</li> </ul>

Los ejemplos anteriores pretenden ser ilustrativos y no incluyen todo.

97. ¿Cómo decide la administración sobre las capacidades básicas apropiadas?

Con respecto a la adopción de un lenguaje común, es una cuestión de juicio, cultura y estilo operativo. El la estructura y la complejidad de la organización son factores adicionales. Lo que funciona para una organización no funcionará trabajar necesariamente para otros. Una buena técnica es probar un marco sugerido o marcos alternativos para probar la aplicación en la práctica y evaluar la aceptación antes de comprometerse a utilizarlos en toda la organización.

Con respecto al establecimiento de supervisión y gobierno, recomendamos que la gerencia considere cuidadosamente todas las "posibles capacidades" resumidas en la respuesta a la Pregunta 96. La estructura de la organización y alcance de la centralización frente al impacto de la descentralización que establece la administración de la estructura de supervisión.

98. ¿Por qué tener un lenguaje común y hay ejemplos?

La comunicación es esencial. La falta de una perspectiva o lenguaje común inhibe la comunicación y la el intercambio de mejores prácticas y, por lo tanto, perjudica la gestión eficaz del riesgo. Además, sin un común lenguaje que respalda un proceso uniforme, todos comienzan con una "hoja de papel en blanco" cada vez que afrontar el tema del riesgo y la gestión del riesgo. Por lo tanto, un lenguaje común es una herramienta para facilitar un diálogo continuo entre los gerentes y empleados de la empresa sobre el riesgo y las capacidades existentes para gestionar el riesgo. Los elementos esenciales de un lenguaje común incluyen:

- Aclarar la terminología que ayuda a la organización con la identificación de riesgos y proporciona una base para la discusión y el análisis en curso
- Un esquema de clasificación de procesos que descomponga el negocio en sus componentes de operación, gestión y soporte. componentes para facilitar la obtención de riesgos y el intercambio de mejores prácticas
- Marcos efectivos que simplifican las comunicaciones sobre las capacidades de gestión de riesgos, permiten evaluaciones basadas en hechos de la capacidad del proceso y centran los esfuerzos de mejora para abordar brechas significativas

Consulte nuestra respuesta a la Pregunta 75 para ver un ejemplo de un lenguaje de riesgo. Vea nuestras respuestas a las Preguntas 110 y 111 para ver ejemplos de marcos probados para evaluar la capacidad del proceso.

99. ¿Hay ejemplos de un esquema de clasificación de procesos?

Un esquema de clasificación de procesos es un resumen de los procesos de una organización y es una herramienta útil al evaluar la fuente de riesgos. Estas categorías de procesos se dividen en subprocessos que se pueden aplicar o personalizado para cualquier negocio o industria. El punto es que la organización debe diseñar su propio marco por organizar su esquema de clasificación de procesos para complementar su lenguaje de riesgo y poblar ese marco con el tiempo.

Hay muchos ejemplos de un esquema de clasificación de procesos. El modelo de Porter es un enfoque que las empresas tienen usado. Protiviti tiene su propio esquema de clasificación de procesos personalizado para diferentes industrias. Hay otros marcos similares disponibles para descomponer un negocio en sus procesos operativos, de gestión y de soporte.

100. ¿Cómo se mejora el diálogo sobre el riesgo y sus causas fundamentales, impulsores y fuentes?

Al buscar el riesgo, la empresa se enfoca en comprender las causas subyacentes, o "impulsores", del riesgo. El abastecimiento de riesgos requiere un análisis eficaz del entorno externo y los procesos internos de la empresa y condiciones. Si bien la identificación de eventos se enfoca en qué eventos pueden suceder en el futuro, el riesgo evaluación es la evaluación de la probabilidad de que ocurra el evento y la gravedad del impacto si el evento ocurre. Los eventos que dan lugar a riesgos potenciales pueden ocurrir fuera de la organización o dentro de su negocio. procesos. Por lo tanto, la gerencia necesita comprender el por qué, cómo y dónde con respecto a los eventos relacionados. para formular una respuesta eficaz al riesgo. Ese es el objetivo del abastecimiento de riesgos.

El abastecimiento de riesgos es el proceso de comprender un riesgo y sus interrelaciones con otros riesgos, así como sus impulsores o causas fundamentales, que son las fuentes últimas de incertidumbre. Determinar el tipo y la naturaleza de los impulsores significativos suele ser un paso crítico hacia el desarrollo de una metodología de medición de riesgos. Por ejemplo, si un fabricante está preocupado por la cantidad de tiempo necesario para llevar un producto completo al mercado, entonces la gerencia de la empresa deberá comprender una serie de procesos comerciales. En particular, deben buscar actividades innecesarias o redundantes que claramente no agregan valor al proceso para lograr el objetivo de "velocidad de comercialización". Este ejercicio podría incluso implicar mirar aguas arriba a los procesos de los proveedores de la empresa, así como aguas abajo a sus canales de distribución. Los límites organizacionales pueden desdibujarse cuando se busca riesgo.

Un lenguaje y un enfoque comunes pueden ayudar a la gerencia a determinar las causas fundamentales o los impulsores de múltiples riesgos y proporcionar una base para medir, controlar y monitorear el riesgo. Los marcos que respaldan el abastecimiento de riesgos (como el ilustrado en nuestra respuesta a la Pregunta 80) ayudan a los administradores de riesgos a comprender el tipo y la disponibilidad de datos de riesgo relevantes que influirán en (a) cómo se puede medir el riesgo y (b) la selección de un respuesta adecuada al riesgo. Abordado de manera sistemática a través del análisis de los factores de riesgo y los procesos comerciales, el abastecimiento de riesgos también puede identificar situaciones de riesgo que los gerentes pueden decidir solucionar de inmediato con los controles internos apropiados.

Las causas fundamentales o las fuentes de riesgo provienen de una variedad de factores, que incluyen:

- Cambios en uno o más factores ambientales externos
- Anomalías o deficiencias en uno o más procesos o sistemas comerciales
- Mala gestión de interfaces entre procesos y actividades
- Errores involuntarios o deliberados
- Interrupciones en el flujo de información que respalda un proceso (el "flujo de información" es la secuencia de actividades que capturan y registran datos comerciales, procesan esos datos en información y, en última instancia, informan información y conocimiento a la gerencia y a terceros)
- Instalaciones o equipos que funcionan mal o no son adecuados para el trabajo para el que se establecieron
- Eventos impulsados internamente que resultan de acciones o inacciones de la gerencia, por ejemplo, comunicaciones deficientes, falta de liderazgo, expectativas e incentivos de desempeño inadecuados, etc.

Los riesgos del entorno externo se obtienen utilizando técnicas analíticas como el análisis de la industria, el análisis de la competencia, el análisis de mercado, el análisis de países, la evaluación comparativa y el análisis de otros datos externos relevantes. Para los riesgos de procesos, los propietarios de procesos y riesgos deben comprender primero los procesos (a través del mapeo de procesos, por ejemplo), y luego buscar las causas raíz del riesgo. Para todos los riesgos (ambiente, proceso e información para la toma de decisiones), los análisis de factores de riesgo son útiles para fines de abastecimiento. Al analizar las causas fundamentales o los impulsores, puede ser necesario comprender los efectos de la cartera de múltiples riesgos que están más allá de las conjeturas intuitivas debido a las complejas interrelaciones entre los riesgos y los factores que los afectan, por ejemplo, los términos de los instrumentos, los impulsores del riesgo ambiental y otras variables.

#### 101. ¿Cómo se mejora el intercambio de conocimientos sobre gestión de riesgos?

Para comunicarse de manera efectiva hacia arriba y hacia abajo en la empresa y entre sus unidades, funciones y departamentos, los gerentes y los empleados necesitan un lenguaje común. Como ocurre con cualquier otra cosa que dependa en gran medida de una comunicación eficaz, la ausencia de un idioma conduce a errores de comunicación y descuidos. Si las personas adecuadas comunican de manera eficaz la información sobre los riesgos (y oportunidades) y coordinan las actividades de gestión de riesgos, la organización estará mejor posicionada para aprender y adaptarse a un entorno cambiante.

Un lenguaje común agrega valor en el sentido de que puede ayudar a los gerentes de procesos o unidades de negocios a identificar y evaluar de manera más efectiva su exposición a eventos potencialmente adversos y diseñar mejores capacidades de gestión de riesgos. Sin embargo, su valor real se hace evidente cuando se despliega dentro de una gestión de riesgos uniforme.

proceso que se aplica a diferentes riesgos en toda la empresa. Solo entonces se obtendrán los beneficios revolucionarios: priorización, abastecimiento, cuantificación, agregación, aprendizaje, intercambio de conocimientos y desarrollo oportuno de respuestas a los riesgos. Un lenguaje común no solo es esencial para la implementación de ERM; también es un primer paso vital en el camino hacia esa capacidad.

Los marcos comunes se traducen en poderosas herramientas para compartir conocimientos que pueden impulsar la mejora continua.

Por ejemplo:

- Internet, las aplicaciones de intranet propietarias y los sistemas de correo electrónico crean oportunidades para sondar a los propietarios de riesgos y sus equipos sobre la probabilidad y el impacto de eventos clave y para compartir conocimientos y experiencias. Por ejemplo, las intranets pueden servir como medio para proporcionar herramientas uniformes de evaluación de riesgos para los gerentes de las unidades de negocios. La combinación de un lenguaje común y un proceso común permite el desarrollo de técnicas de agregación de riesgos basadas en tecnología.
- Si cada unidad de negocio mantiene su propia base de datos de información sobre riesgos y gestión de riesgos, un lenguaje común permite la agregación de puntos de datos comunes para desarrollar una perspectiva de toda la empresa para gestionar los riesgos prioritarios. Este enfoque permite que una función de gestión de riesgos empresariales corporativos acceda a los datos de todas las empresas del grupo y acelere el proceso de intercambio de conocimientos. También es posible el intercambio directo de conocimientos y/o preguntas y respuestas entre las empresas del grupo y está respaldado por las características de la plataforma de discusión "abierta" de la base de datos.
- La comunicación de arriba hacia abajo es una parte integral de la comunicación de cuatro vías. Todos los interesados en el proceso de gestión de riesgos de la organización, por ejemplo, la junta directiva, la alta dirección, los propietarios de gestión de riesgos y los propietarios de procesos de negocio, deben poder comunicarse libremente sobre cuestiones de riesgo de negocio. Las comunicaciones de arriba hacia abajo de la dirección ejecutiva enfatizan la dirección estratégica ("¿Hacia dónde vamos?"), el desempeño general de la organización ("¿Cómo lo estamos haciendo?"), las responsabilidades de gestión de riesgos de los empleados ("¿Qué se espera de usted?") y el propósito de gestión de riesgos. Las comunicaciones de arriba hacia abajo incluyen procesos formales e informales. Funcionan mejor en un entorno respaldado por un marco que incluye un lenguaje de riesgo común.
- La comunicación ascendente también es importante y es mucho más que "denuncias". La gerencia debe proporcionar a los empleados un proceso para comunicar información hacia arriba con respecto a lo que sucede en el entorno externo e interno dentro del negocio. El lenguaje común proporciona un contexto para esta comunicación, que es vital porque sin él, la alta dirección de las grandes organizaciones puede perder el contacto con la realidad.
- La comunicación horizontal entre unidades operativas y divisiones, funciones y departamentos también es fundamental a un intercambio más organizado de información sobre "mejores prácticas" y mejora continua.

#### 102. ¿Qué significa aumentar la conciencia o la sensibilidad al riesgo de una organización?

Una función eficaz de supervisión de la gestión de riesgos, como se articula en la pregunta 56, junto con un proceso uniforme y bien definido de evaluación de riesgos en toda la empresa ayudará a crear una cultura sensible al riesgo y consciente del riesgo, en la que el riesgo se acepte de manera abierta, positiva y proactiva. en todos los niveles de la organización. ERM se trata tanto de la cultura adecuada como de políticas, procesos, personas y sistemas. Es un marco que los gerentes pueden usar para aceptar el riesgo, no para huir de él. Pero algunos preguntan: "¿Qué significa tener una 'cultura sensible al riesgo y consciente del riesgo'?"

Una cultura sensible al riesgo y consciente del riesgo es aquella en la que la gestión del riesgo se integra efectivamente con el establecimiento de la estrategia. En este entorno, las funciones y responsabilidades relacionadas con la gestión de riesgos están claramente articuladas en todos los niveles de la organización para que los gerentes se animen a representar de manera realista los posibles resultados de las posibles transacciones, acuerdos, inversiones y proyectos. Se espera que entiendan y representen la imagen completa. Por ejemplo, deben mirar las ventajas y desventajas en relación con el aprovechamiento de una oportunidad. ¿Qué tan grave sería el daño si las cosas no salen según lo planeado y si la oportunidad potencial al alza compensa adecuadamente a la organización por asumir el riesgo a la baja?

La mayoría de los gerentes de negocios entienden el principio fundamental aquí. Sin embargo, dado que la visión de "riesgo como amenaza" es tan predominante en muchas organizaciones en muchas industrias, es difícil poner en práctica el principio de manera cuidadosa y equilibrada. Por ejemplo, supongamos que tiene una unidad de negocios que está tratando de consumar una transacción importante o está bajo una presión presupuestaria o de ganancias significativa, o está tratando de ganar mucho dinero en un período de tiempo muy corto. El capital está disponible, la competencia es dura y el optimismo empresarial de "puedo hacerlo" abunda en los pasillos y salas de reuniones de la organización. Este perfil de gerentes puede enamorarse muy rápidamente de una oportunidad. Pueden comenzar ignorando el riesgo a la baja y simplemente concentrarse en la oportunidad al alza. Entonces, de repente, sin los controles de supervisión apropiados (incluidos los límites de riesgo apropiados, informes y monitoreo) y sin un proceso sólido de evaluación de riesgos empresariales, la organización termina siendo "dueña" del riesgo resultante de aprovechar esa oportunidad. Si el perfil de riesgo/recompensa no se pondera adecuadamente, es posible que la empresa no se esté compensando adecuadamente por el riesgo que está asumiendo. Eso puede causar problemas a los gerentes, sin mencionar a sus organizaciones.

Entonces, cuando surgen nuevas oportunidades de mercado, negocios y productos, la organización necesita la capacidad de articular y evaluar los eventos clave asociados con el comportamiento de búsqueda de oportunidades. Cuan malo puede ser? ¿Qué tan bueno puede ser? ¿Dónde podemos terminar entre estos dos extremos, incluido el resultado más probable? ESTE es el tipo de proceso analítico sólido que necesita la gerencia ANTES de comprometer capital para la búsqueda de nuevas oportunidades. En esencia, la gerencia debe evaluar las posibles ventajas y desventajas frente al apetito por el riesgo de la entidad.

Una cultura sensible al riesgo y consciente del riesgo es aquella en la que TODO el personal clave de la organización, o como mínimo algun individuo, grupo o unidad independiente, tiene la oportunidad de decir lo que piensa sobre algo que la empresa está intentando hacer. Si las personas no se sienten capaces de articular libremente lo que realmente piensan sobre una transacción en particular, una adquisición, un nuevo producto, un proyecto propuesto u otras oportunidades, no lo van a decir. Entonces la organización ha perdido el beneficio de poner esos puntos de vista sobre la mesa y discutirlos abiertamente con los altos ejecutivos y directores de la organización. El diálogo se centra indebidamente en la oportunidad al alza sin la consideración adecuada del riesgo a la baja relacionado.

La ironía de crear un entorno abierto es que un diálogo sólido puede llevar a la organización a asumir más riesgos, no menos. La verdadera pregunta es: "¿La organización realmente sabe en qué se está metiendo?" Y lo que es igual de importante, ¿qué podría estar faltando si no actúa? Si una empresa tiene un grupo de productos que está tratando de impulsar una idea, la gerencia necesita una visión completamente equilibrada que es tan vital para tomar una decisión informada. Nadie se levantará y dirá: "No creo que esta adquisición, trato o transacción tenga ningún sentido porque estamos pagando el doble de lo que deberíamos", a menos que esté estructuralmente aislado de cualquier repercusión que esa declaración podría tener en su compensación y carrera.

En resumen, una cultura sensible al riesgo y consciente del riesgo es aquella que permite a las personas hablar y luego ser escuchadas por los tomadores de decisiones. Sigue la palabra con la acción, al aislar a las personas de represalias, directas o indirectas. No debe confundirse con la denuncia de irregularidades, que trata un tema diferente. La mayoría de los ejecutivos estaría de acuerdo en que hay muchas buenas ideas con respecto a asumir riesgos y oportunidades. Si bien se necesitan algunos filtros, poner esas ideas sobre la mesa y discutirlas en un entorno positivo y proactivo es de lo que se trata una cultura sensible y consciente del riesgo.

## TOMANDO UNA VISIÓN DE PROCESO – CREANDO CAPACIDADES

103. ¿Qué pasos toma la administración para desarrollar capacidades de gestión de riesgos?

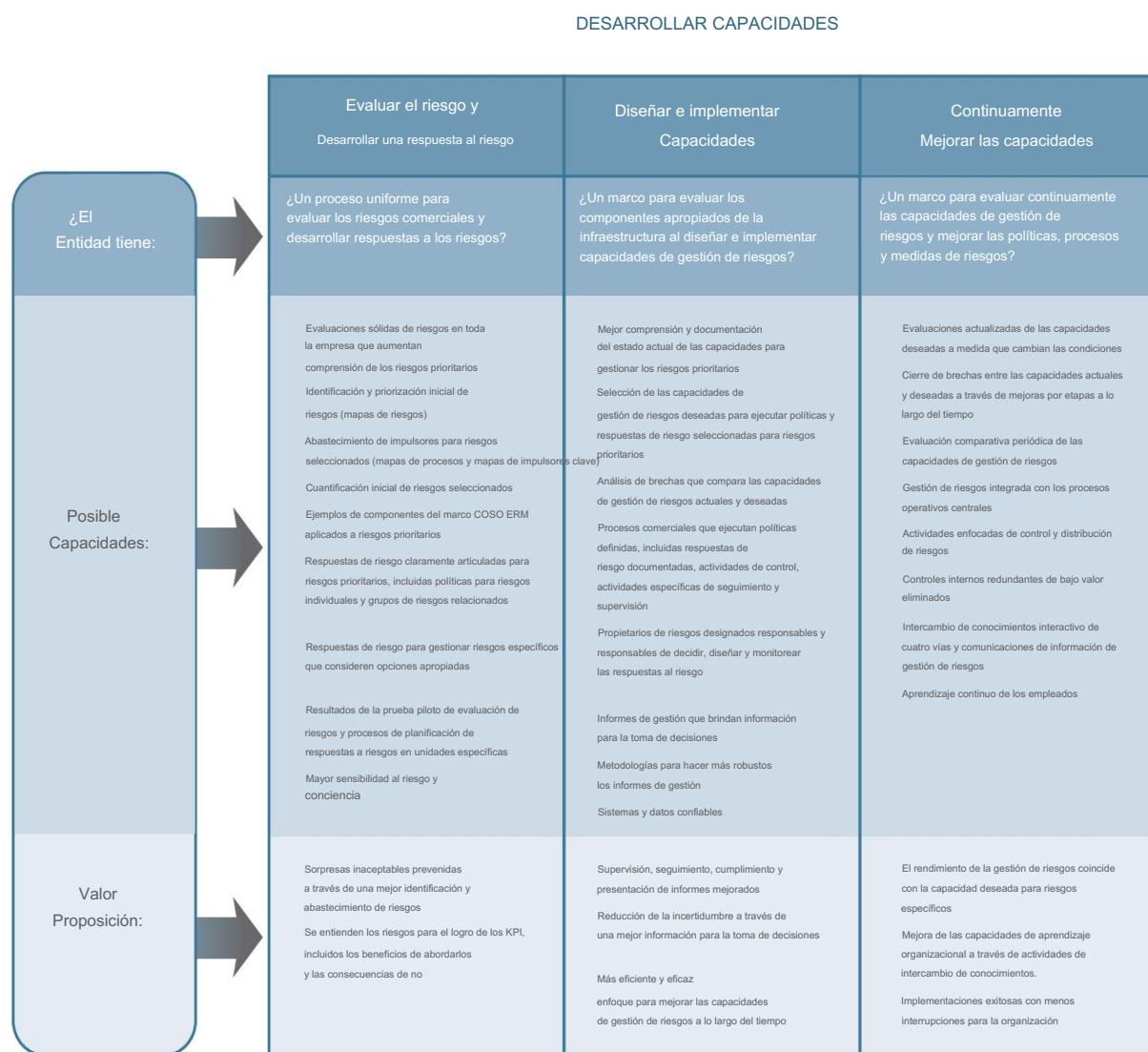
Una vez que la organización ha sentado las bases con elementos de una infraestructura de ERM adecuada (consulte la Pregunta 96), está lista para avanzar en sus capacidades en torno a la gestión de sus riesgos prioritarios. Hay tres pasos que la gerencia debe seguir al desarrollar capacidades de gestión de riesgos:

- El primer paso, evaluar el riesgo y desarrollar respuestas, se aborda una vez que se ha establecido la base adecuada. Incluye un proceso de evaluación de riesgos en toda la empresa, un proceso en torno a la planificación de respuestas a los riesgos prioritarios y el desarrollo de políticas de riesgo específicas.

- El segundo paso, diseñar e implementar capacidades , hace que todo suceda. Las capacidades de gestión de riesgos incluyen los procesos, competencias, informes, metodologías y tecnologías (sistemas y datos) necesarios para implementar una respuesta de riesgo seleccionada y llevar a cabo políticas de riesgo de manera coherente en toda la empresa.
- El tercer paso, mejorar continuamente las capacidades , se relaciona con la mejora continua, una disciplina que se aplica a la gestión de riesgos como lo hace con cualquier otro proceso comercial. La necesidad de mejoras en los procesos, competencias, informes, metodologías y sistemas que se identifiquen a través del monitoreo debe evaluarse e implementarse, de acuerdo con una mentalidad de mejora continua.

Al igual que con el establecimiento de las bases, no es necesario seleccionar todos los elementos sugeridos en esta publicación para desarrollar capacidades de gestión de riesgos al diseñar una solución para cada uno de los riesgos prioritarios de la organización. La gerencia solo necesita seleccionar capacidades suficientes para cada riesgo o grupo de riesgos relacionados para cumplir con los objetivos declarados de la entidad. Una vez que las capacidades deseadas están en su lugar, la gerencia puede implementar las mejoras apropiadas.

A continuación se presenta un resumen de ejemplos de elementos a considerar para cada uno de los tres pasos para desarrollar capacidades de gestión de riesgos:



Los ejemplos anteriores pretenden ser ilustrativos y no incluyen todo.

104. ¿Cómo decide la dirección sobre las capacidades adecuadas de gestión de riesgos?

Con respecto al diseño e implementación de capacidades de gestión de riesgos, es una cuestión de juicio, cultura y estilo operativo. Lo que funciona para una organización no necesariamente funcionará para otra organización.

La gerencia puede probar los componentes de un proceso sugerido para un riesgo determinado o en una unidad determinada para probar la aplicación y aceptación antes de decidir implementarlos en toda la organización.

105. ¿Cómo mejora la administración las evaluaciones de riesgos de la organización?

Las evaluaciones de riesgos se pueden mejorar de muchas maneras. Las evaluaciones de riesgos más efectivas están diseñadas para proporcionar insumos de calidad para la planificación de la respuesta a los riesgos. El liderazgo y el compromiso de la gerencia con un proceso de evaluación son esenciales para dirigir los recursos necesarios para apoyar el proceso. Mejorar los esfuerzos de monitoreo y medición aumenta la probabilidad de que la evaluación se base en información cuantitativa relevante así como en información cualitativa. Otras posibles mejoras incluyen: proporcionar recursos para identificar, evaluar y gestionar riesgos; asignar propietarios de riesgos apropiados para que asuman la responsabilidad de los riesgos prioritarios; integrar los objetivos de gestión de riesgos en las expectativas de desempeño individual y los planes comerciales; y la creación de un entorno abierto que fomente el debate sobre los riesgos comunes en toda la empresa.

106. ¿Cómo se relacionan el establecimiento de objetivos, la identificación de eventos y la evaluación de riesgos?

El "establecimiento de objetivos" ocurre cuando la gerencia establece objetivos estratégicos, que brindan un contexto para establecer objetivos operativos, de informes y de cumplimiento. Los objetivos están alineados con el apetito por el riesgo de la entidad, lo que impulsa los niveles de tolerancia al riesgo para la entidad, y son una condición previa para la identificación de eventos, la evaluación del riesgo y la respuesta al riesgo. Los eventos potenciales futuros se identifican con objetivos específicos en mente.

La identificación de eventos ocurre cuando la gerencia identifica eventos potenciales que pueden afectar positiva o negativamente la capacidad de una entidad para implementar su estrategia y alcanzar sus objetivos. Los eventos potencialmente negativos representan escenarios que brindan un contexto para evaluar el riesgo y la efectividad de las respuestas al riesgo. Los eventos potencialmente positivos representan oportunidades. Según COSO, la gestión canaliza las oportunidades de regreso a la estrategia y los procesos de establecimiento de objetivos.

La evaluación de riesgos ocurre cuando la administración considera métodos cualitativos y cuantitativos para evaluar la probabilidad y el impacto de eventos potenciales, individualmente o por tema o categoría, que podrían afectar el logro de los objetivos. Por lo tanto, para ser eficaz, la evaluación de riesgos requiere objetivos predeterminados y un inventario cuidadoso de posibles eventos futuros.

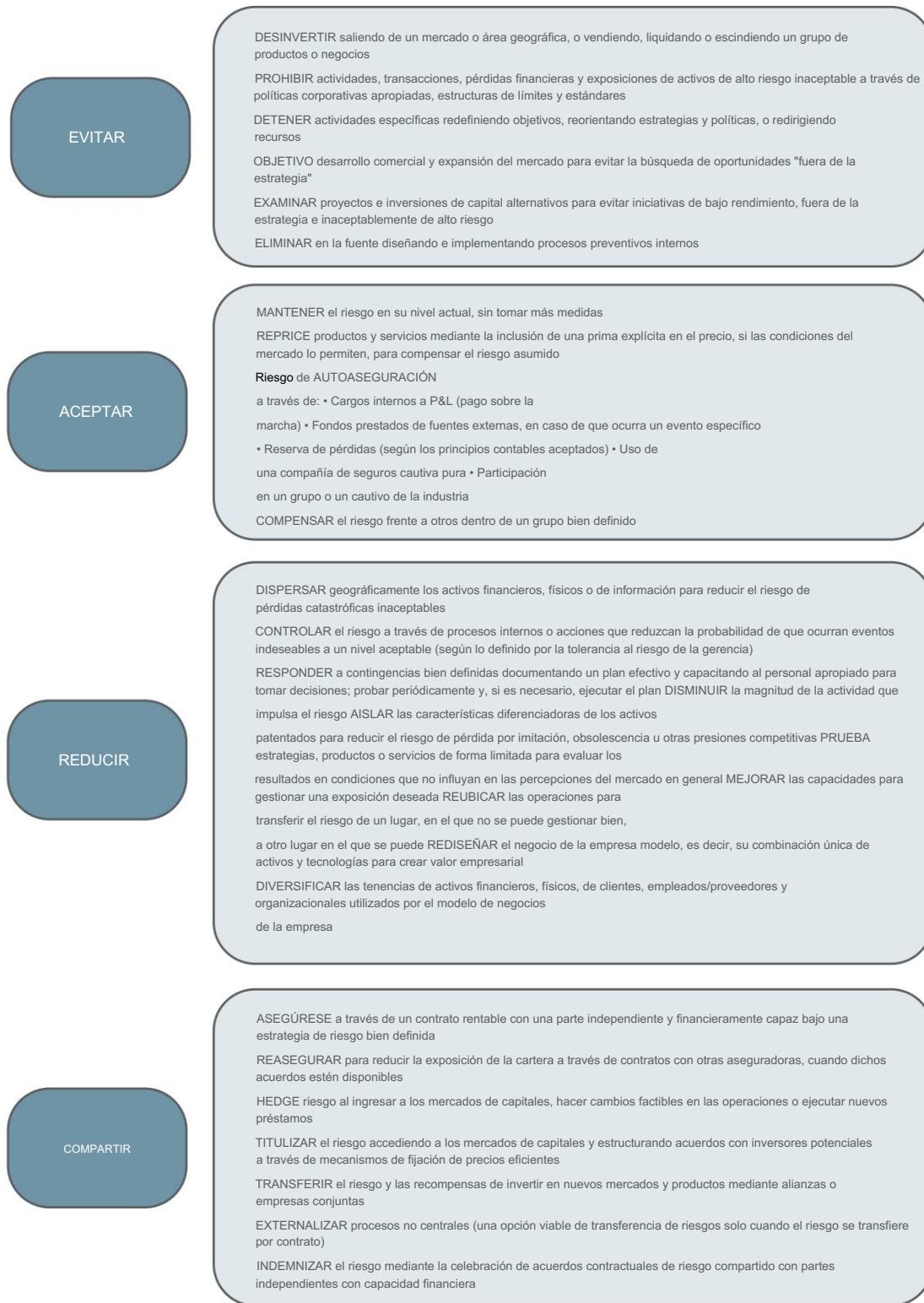
107. ¿Qué tan importante es la evaluación de riesgos para el esfuerzo de ERM?

Se necesita un proceso eficaz de evaluación de riesgos en toda la empresa para identificar los riesgos prioritarios e iniciar un análisis de brechas en torno a las capacidades existentes para gestionar esos riesgos. Las brechas inaceptables relacionadas con los riesgos prioritarios brindan una base para articular la propuesta de valor de avanzar en la infraestructura de ERM de una organización. Una evaluación de riesgos eficaz también proporciona insumos de calidad para la planificación de la respuesta a los riesgos. Por lo tanto, la evaluación de riesgos es de vital importancia para desarrollar capacidades de gestión de riesgos y para la implementación de ERM. Si no se identifican los riesgos prioritarios, es casi imposible definir una propuesta de valor específica que resuene en la alta dirección. Además, los riesgos cambian a medida que cambian el mercado y las condiciones operativas. Cada organización, por lo tanto, necesita un proceso para mantenerse al tanto de los efectos del cambio en sus clientes, proveedores, competidores y operaciones. De eso se trata el proceso de evaluación de riesgos. Se hace referencia a las Preguntas 69 a 84, que abordan el proceso de evaluación de riesgos.

108. ¿Qué respuestas alternativas al riesgo están disponibles para gestionar el riesgo?

Después de la evaluación de riesgos, se desarrollan respuestas de riesgo específicas. Como indica COSO, hay cuatro opciones fundamentales. Son evitar (eliminar el riesgo evitando la exposición a posibles eventos futuros de

ocurriendo), aceptar (mantener el riesgo en su nivel actual), reducir (implementar políticas y procedimientos para reducir el riesgo a un nivel aceptable) y compartir (trasladar el riesgo a una contraparte independiente y con capacidad financiera):



Si bien las respuestas a los riesgos resumidas en la página anterior son, en su mayor parte, sencillas, algunos comentarios aclaratorios son apropiados:

- La organización primero decide si asumir o rechazar un riesgo basándose en una evaluación de si el riesgo es deseable o indeseable. Un riesgo deseable tiene al menos dos características. Primero, es uno que es inherente al modelo de negocio de la entidad o a las operaciones futuras normales. En segundo lugar, la empresa puede medirlo y administrarlo de manera efectiva. Por ejemplo, si no se dispone de medidas confiables dentro de un marco de tiempo razonable con respecto a un riesgo importante, entonces la administración debe considerar seriamente si se debe emprender la actividad que genera el riesgo. La incapacidad de medir un riesgo no hace que desaparezca. Si un riesgo no es deseable, por ejemplo, está fuera de la estrategia, ofrece recompensas poco atractivas o la empresa no tiene la capacidad de medirlo o gestionarlo, entonces se rechaza el riesgo y las respuestas de evitar y compartir son apropiadas. Tenga en cuenta que el apetito por el riesgo de la administración influye en la diferenciación de los riesgos deseables e indeseables.
- Si una entidad asume un riesgo (es decir, elige no evitarlo), hay varias respuestas disponibles. En primer lugar, puede aceptar el riesgo en su nivel actual. En segundo lugar, puede reducir la gravedad del riesgo y/o su probabilidad de ocurrencia. Las actividades de control reducen la probabilidad de ocurrencia. La dispersión geográfica de los activos reduce el impacto de la ocurrencia de un solo evento en la empresa. En tercer lugar, puede compartir el riesgo con una parte independiente con capacidad financiera.
- Las cuatro respuestas (evitar, aceptar, reducir y compartir) abordan acciones que a menudo se aplican a riesgos individuales. Estas opciones también se aplican a grupos de riesgos relacionados que consisten en familias naturales o grupos de riesgos que comparten características fundamentales (por ejemplo, impulsores comunes, correlaciones positivas o negativas, etc.) consistentes con una visión de cartera.
- Como se ilustra en el resumen de respuestas alternativas al riesgo, aceptar puede significar mucho más que simplemente retener un riesgo. Las siguientes son ilustraciones:
  - Incurrir en cargos internos a P&L. Este enfoque prevé pérdidas sobre una base de "pago por uso". Es a menudo se utiliza para hacer frente a las pérdidas que surgen en el curso normal de los negocios.
  - Crear fuentes contingentes de fondos prestados (de fuentes externas en caso de que ocurra un evento de riesgo). Las pérdidas pueden finanziarse con ingresos de fuentes externas cuando el capital de trabajo no es suficiente. Por ejemplo, las fuentes de crédito revolvente disponibles pueden usarse para este propósito. Las compañías de seguros ofrecen instrumentos tales como notas de superávit contingente y bonos de catástrofe para financiar las obligaciones que surgen de un evento catastrófico. El problema, por supuesto, con esta alternativa es si la financiación estará disponible cuando y si se necesita. Además, la empresa sigue obligada a pagar.
  - Reserva de pérdidas bajo principios de contabilidad generalmente aceptados. Una empresa puede constituir una reserva para una pérdida razonablemente estimable cuando es probable que se haya incurrido en un pasivo o en un deterioro del valor de un activo, aunque los siniestros que originaron las pérdidas no hayan sido declarados o aún estén sujetos a resolución final. determinación.
  - Constitución de una compañía de seguros cautiva pura. Este vehículo de autoseguro es una subsidiaria de propiedad total constituida para suscribir los riesgos de su matriz a través de reservas prefinanciadas. En esencia, proporciona un enfoque más formalizado del riesgo de autoaseguramiento, que ofrece la atractiva ventaja de la deducción de impuestos en ciertos países. Usadas de manera efectiva, las cautivas brindan un enfoque disciplinado para la asignación de capital.
 

¿Cuándo se elige esta opción sobre otros enfoques de autoseguro? Con base en los niveles de pérdida esperados, la gerencia debe usar un análisis de costos descontados después de impuestos para comparar el flujo de efectivo y las ganancias de la organización cuando se autoasegura el riesgo versus el prefinanciamiento de reservas a través de una cautiva. Este análisis debe considerar factores tales como el valor del dinero en el tiempo, los costos de oportunidad y el valor de las deducciones por las primas pagadas y la opinión de las autoridades fiscales sobre la deducibilidad de las primas pagadas en cada país. Otros factores importantes a considerar incluyen los requisitos regulatorios de financiamiento, la obtención de beneficios fiscales, el efecto de la cautiva en los estados financieros consolidados y el alcance de la administración cautiva, la operación interna y otros costos incurridos.
  - Participar en una cautiva asociada. Esta estructura incluye cautivas de "propósito especial" de grupos e industrias que suscriben los riesgos de varias firmas independientes y sus afiliadas. Un cautivo de este

La naturaleza está estructurada para que no sea controlada por ninguno de sus clientes. Por lo tanto, como parte no relacionada, su viabilidad a largo plazo depende de la experiencia de pérdida del grupo.

Al analizar esta opción, se deben considerar los factores enumerados anteriormente para las cautivas de propiedad total.

Sin embargo, cuando se considera una cautiva no relacionada, existe una mayor presión por la adecuación del capital proveniente no solo de los reguladores sino también de los consejos de administración de la cautiva que buscan los mejores rendimientos posibles sobre el capital. La regulación sigue avanzando hacia el capital basado en riesgo en el que se analiza la exposición neta de la cautiva por póliza y/o por clase de negocio y se realiza una evaluación de la probabilidad de pérdida por póliza y/o por clase. El resultado es un requisito de capital a largo plazo potencialmente costoso que puede superar con creces los márgenes de solvencia legales actuales.

Esta presión al alza sobre los requisitos de capital podría amenazar la viabilidad de las cautivas a menos que diversifiquen su cartera de coberturas y/o transfieran el riesgo a través del reaseguro. Los requisitos de capital también pueden administrarse coordinando estrechamente los "niveles" de financiamiento de riesgo, comenzando con la cobertura de la primera pérdida por parte de la cautiva, luego agregando el deducible agregado a cargo del asegurado, luego exponiendo el capital social de las cautivas en su totalidad y, finalmente, transferir el riesgo restante a través del reaseguro. De esta manera, las cautivas brindan una puerta de entrada para que las empresas contraten con los principales mercados de reaseguros y, para muchas organizaciones interesadas en acceder a coberturas difíciles de colocar en los mercados de seguros, son una pieza esencial del tejido total de administración de riesgos.

- Otra táctica aceptada es compensar un riesgo con otros riesgos dentro de un grupo bien definido. Por ejemplo, un La compañía de refinación está en la posición de comprar productos energéticos como entradas de materia prima y vender productos refinados como salidas. Los costos de estas entradas y salidas brindan una compensación natural porque los aumentos en el costo de las compras de materia prima de una empresa pueden trasladarse a los clientes por medio de precios más altos del producto. Otro ejemplo es el de un banco de inversión que suscribe un contrato financiero para un cliente que se cubre contra el riesgo de tasas de interés más altas y compra un contrato similar de otro cliente que se cubre contra el riesgo de tasas de interés más bajas. En este caso, las exposiciones generadas por cada riesgo se compensan en el libro del banco de inversión.

- La formulación de una respuesta al riesgo no es necesariamente una cuestión de seleccionar una opción sobre otra. La mejor respuesta puede ser una combinación de opciones. Por ejemplo, al gestionar la seguridad en el lugar de trabajo, una organización puede desear implementar actividades de control apropiadas para reducir el riesgo de salud y seguridad dentro de sus procesos comerciales tanto como sea posible, obtener un seguro de compensación para trabajadores adecuado para compartir una parte del riesgo residual y aceptar el resto residual. riesgo a través de deducibles.

- Algunos creen que el riesgo puede explotarse a través de una decisión proactiva y consciente de asumir nuevos riesgos o aumentar los riesgos existentes a medida que la empresa apuesta en la búsqueda de oportunidades de valor agregado. Por ejemplo, la gerencia decide asumir los riesgos inherentes a sus elecciones para ingresar a nuevos mercados, introducir nuevos productos, fusionarse o adquirir otra empresa o explotar otras oportunidades de mercado, todo lo cual da como resultado una configuración diferente del perfil de riesgo de la organización, incluso hasta el punto de aumentar la exposición de la empresa a los riesgos que desea asumir de acuerdo con su modelo de negocio. Aunque en concepto no estaba en desacuerdo con este pensamiento, COSO concluyó que tales acciones constituyen la búsqueda de oportunidades (ver Pregunta 73). Por lo tanto, la decisión de la gerencia de asumir o aumentar los riesgos de la organización es una decisión de la gerencia, no necesariamente la aplicación de ERM. Por ejemplo, algunos argumentan que la administración puede explotar el riesgo ejerciendo su prerrogativa de:

- Diversificar las tenencias de activos financieros, físicos, de clientes, de empleados/proveedores y de la organización utilizados por el modelo de negocio de la empresa.
- Ampliar la cartera de negocios invirtiendo en nuevas industrias, áreas geográficas y/o grupos de clientes.
- Crear nuevos productos, servicios y canales de valor añadido.
- Rediseñar el modelo de negocio de la firma, es decir, su combinación única de activos y tecnologías para la creación de valor.
- Reorganizar procesos a través de reestructuración, integración vertical, tercerización, reingeniería y reubicación
- Asignar capital internamente dentro de la entidad utilizando métodos disciplinados para financiar los riesgos asumidos y dirigir los recursos de la entidad a aquellas oportunidades con la mayor perspectiva de generar los rendimientos deseados.

- Fijar el precio de los productos y servicios para influir en la elección del cliente hacia aquellos productos y servicios que se adapten al perfil de riesgo de la empresa.
- Renegociar los acuerdos contractuales existentes para remodelar el perfil de riesgo, es decir, transferir, reducir o tomar arriesgarse de otra manera.
- Arbitraje de discrepancias de precios mediante la compra de valores u otros activos en un mercado de forma inmediata. reventa en otro.
- Influir en los reguladores, la opinión pública, los legisladores y los encargados de establecer normas a través de actividades de cabildeo enfocadas, activismo político, relaciones públicas, etc.

Bajo el marco COSO ERM, muchas de las tácticas anteriores son ejemplos de oportunidades de explotación.

- Aplicado en el establecimiento de estrategias, ERM proporciona el enfoque que inculca la disciplina para impulsar a las empresas a comprender bien sus competencias básicas para que puedan alinear su toma de riesgos con sus procesos, habilidades, tecnología y conocimiento. Las cuatro respuestas ( evitar, aceptar, reducir y compartir ) reflejan las elecciones de la gerencia para actuar. ¿Qué pasa si la gerencia decide no responder? Diferir es otra opción de gestión en circunstancias en las que una exposición puede tener más valor en el futuro que en la actualidad, dependiendo de cómo se desarrolle el futuro. Por ejemplo, muchos proyectos de investigación y desarrollo no se convierten en productos rentables. Aquellos que lo hacen pueden volverse lo suficientemente rentables como para compensar con creces el costo de todo el programa de I+D. Dado que la gerencia no siempre puede distinguir los proyectos exitosos de los proyectos fallidos, es posible que prefiera mantener todas las exposiciones potencialmente buenas debido a su valor de opción; ese valor es la posibilidad de que sean rentables en el futuro. Tales evaluaciones son posibles en muchas situaciones comerciales. El valor de diferir la decisión de responder –o preservar la opción de tomar una decisión de responder en el futuro– surge de reconocer los hechos tal como son, pero no comprometerse en exceso cuando no es necesario hacerlo.
- La exposición a un evento puede ser deseable, pero la incertidumbre sobre su momento puede ser inaceptable para gestión. Por lo tanto, si bien la gerencia puede optar por aceptar un riesgo, se pueden tomar acciones para alterar las características de tiempo del riesgo. Por ejemplo, una entidad puede anticipar que las tasas de interés subirán (o bajarán) en un futuro cercano y, por lo tanto, puede decidir acelerar (o retrasar) sus actividades de endeudamiento. O una empresa de administración de activos puede tratar de estructurar el momento de los retiros de varios fondos para que pueda administrar mejor sus activos sin mantener una posición de efectivo innecesariamente grande (y costosa). Muchos de estos cambios en el momento de una decisión comercial u otras actividades comerciales son posibles.

#### 109. ¿Qué factores debe considerar la gerencia al evaluar las respuestas alternativas al riesgo?

La gerencia debe tomar **decisiones** informadas sobre dónde hacer apuestas, dónde cubrir las apuestas y dónde evitar apostar por completo. Hay muchos factores a considerar cuando se evalúan respuestas alternativas al riesgo. Por ejemplo, las decisiones comerciales y los supuestos de la administración brindan un contexto para evaluar respuestas alternativas al riesgo. Los siguientes son ejemplos:

- Objetivos y estrategias de la dirección: Estos objetivos y estrategias aclaran el qué, dónde, cuándo, quién y cómo del modelo de negocio de la empresa. Se expresan en términos de tácticas a corto plazo, estrategias a mediano plazo y objetivos comerciales a largo plazo, e incorporan restricciones a corto, mediano y largo plazo. Las respuestas a los riesgos deben adaptarse a los objetivos comerciales específicos y las estrategias que respaldan.
- Compensaciones de riesgo y recompensa: estas compensaciones son inherentes a cualquier elección con respecto a la gestión del riesgo, no solo operativamente para cualquier empresa, sino también desde una perspectiva de mercado para una empresa pública. En otras palabras, ¿por qué los inversores compran acciones de la empresa? ¿Están efectivamente asumiendo el riesgo empresarial al que está expuesta la empresa? Por lo tanto, las expectativas de rentabilidad de los inversores afectan potencialmente a los objetivos y estrategias de gestión que impulsan las respuestas al riesgo.
- Capacidades de gestión de riesgos: Las respuestas a los riesgos son tan efectivas como las capacidades de la entidad para ejecutarlas. Si las capacidades para ejecutar no están en su lugar, ¿puede la gerencia reunirlas de manera oportuna para implementarlas dentro del horizonte de planificación elegido por la gerencia (consulte lo siguiente)?

- Horizonte de tiempo: El horizonte de tiempo es el período de tiempo que la administración ha decidido considerar al evaluar el riesgo y las capacidades de gestión del riesgo. Un evento que posiblemente podría ocurrir en el corto plazo confronta a la entidad de inmediato. Por ejemplo, en el corto plazo puede ocurrir un aumento en el costo de las compras de materias primas o energía, una reducción del precio de la competencia o un aumento en las tasas de interés.

La exposición a eventos que pueden ocurrir a largo plazo, por el contrario, representan problemas sobre los que una organización tiene relativamente poca capacidad para abordar a corto plazo, pero que puede esperar gestionar de manera realista a largo plazo. Por ejemplo, la pérdida de reputación debido a una falla sistemática en la calidad del producto o la introducción de un competidor de un proceso de fabricación superior que resulta en costos de producción significativamente más bajos puede ocurrir a largo plazo. Si estos llamados problemas de largo plazo ocurren inesperadamente en el corto plazo, la entidad podría enfrentar una situación de crisis. La reacción de clase mundial de Johnson & Johnson a la crisis de Tylenol distinguió a la empresa en el mercado. Por el contrario, el manejo de Perrier de su crisis de contaminación del agua le costó a la empresa participación de mercado y finalmente fue adquirida. El punto clave es que cualquier desajuste entre la duración de la exposición y el tiempo que la administración necesita para implementar una respuesta al riesgo presenta un riesgo potencialmente crítico para la empresa. Las respuestas al riesgo deben tener en cuenta estos desajustes.

- Financiamiento: las respuestas al riesgo también deben considerar la necesidad de financiamiento del riesgo, que es el medio por el cual una organización paga por los resultados de un evento desfavorable a través de las opciones de la gerencia para compartir o aceptar el riesgo. A continuación se presentan varias observaciones sobre el financiamiento del riesgo:

- La financiación externa resulta de la decisión de compartir el riesgo con una contraparte independiente y financieramente capaz a través de seguros, coberturas u otras formas de contratación.
- La financiación interna del riesgo se logra a través de los propios recursos financieros de la entidad, por ejemplo, varios formas de autoseguro, deducibles de seguros y reservas contables.
- Muchos riesgos se financian internamente, pero no todos se reconocen explícitamente. Una entidad retiene todos sus riesgos a menos que haga algo al respecto. A menos que los riesgos se consideren demasiado insignificantes para justificar un análisis más detallado, la retención no planificada del riesgo no es "gestión de riesgos".
- Si el seguro que protege a la empresa de eventos catastróficos es económico en relación con la pérdida potencial, la retención planificada debe basarse en el sentido común racional. ¿Quién quiere explicarle a la junta que una pérdida de \$50 millones podría haberse asegurado por \$10,000?

- Riesgo residual: Las respuestas al riesgo que eliminan el riesgo son raras. Siempre habrá algún riesgo residual en cualquier respuesta a los riesgos. Cualquier diferencial entre la cobertura provista por la respuesta al riesgo y la exposición misma proporciona el riesgo base; es decir, queda algo de riesgo residual en la empresa. COSO reconoce este punto al sugerir que se debe evaluar el alcance de este riesgo. El riesgo residual surge porque la gerencia busca soluciones prácticas que mantengan el riesgo en niveles tolerables y logren una seguridad razonable, no absoluta. A menudo, las herramientas utilizadas para gestionar un riesgo, como cuando se coloca una cobertura con un contrato de futuros, swaps u opciones, no cubrirán completamente la exposición subyacente que presenta el riesgo. El riesgo residual puede ocurrir porque la respuesta al riesgo no cubre todos los aspectos de la exposición a uno o más eventos, o porque cubre demasiado.

Un ejemplo de lo primero es un elevador de granos que contiene granos con especificaciones de productos diferentes a las especificadas en un contrato de futuros estándar. Un ejemplo de esto último es una entidad que cubre una exposición de energía de dos meses con un contrato de opciones de tres meses. En general, cualquier desajuste entre la cobertura provista por la respuesta al riesgo y la exposición misma presentará un riesgo nuevo o continuo.

- Asunción de riesgos inadvertida: relacionado con el riesgo residual es la situación en la que la gerencia elige una respuesta de riesgo para gestionar un riesgo, pero sin saberlo crea otro riesgo. Un importante fabricante de automóviles descubrió esto cuando compró una gran participación en el metal, el paladio, que era un insumo clave para uno de sus vehículos. El objetivo era gestionar el riesgo de suministro y asegurarse de que no se agotara esta materia prima y paralizara la producción. Esta estrategia funcionó bien hasta que sus ingenieros rediseñaron el automóvil y eliminaron la necesidad de paladio, lo que hizo que las existencias del producto disponible fueran prácticamente inútiles. Esto provocó una pérdida significativa. La gerencia debe asegurarse de que se adopte una visión de toda la empresa cuando se formulen las respuestas a los riesgos.

- Capacidad de gestión de riesgos: A medida que la dirección ejecutiva y de unidad dirige sus esfuerzos hacia la gestión de los riesgos prioritarios, deben diferenciar aquellos riesgos en los que es más fácil obtener mejoras inmediatas. Si bien no pretende ser una sugerencia para ignorar los problemas difíciles, un enfoque en la manejabilidad puede conducir a éxitos tempranos en la formulación de respuestas de riesgo al alcanzar la "fruta madura".

Otros factores a considerar cuando se evalúan respuestas alternativas al riesgo incluyen costos y beneficios, el valor de la opción de esperar versus actuar de inmediato, la efectividad en el logro de las metas establecidas y la interacción con otras respuestas contempladas, de acuerdo con la estrategia comercial de la organización, que podrían producir resultados diferentes de lo esperado.

Al evaluar los factores del entorno externo y los factores de riesgo internos, también es útil considerar la naturaleza de los eventos potenciales y el efecto relacionado sobre los riesgos de la organización antes de formular una respuesta al riesgo.

Los siguientes son ejemplos:

- Incertidumbres del plan de negocios: La incertidumbre surge cuando la gerencia no conoce de antemano el magnitud y dirección del cambio en el valor de una variable clave, por ejemplo, el comportamiento de la competencia, las tasas de interés, los precios de las materias primas, la innovación tecnológica, los movimientos de los precios de las divisas, el desempeño humano, las acciones regulatorias, etc. Sin embargo, los posibles cambios futuros en las variables clave crean incertidumbre para la empresa sólo cuando sus fuentes de valor están expuestas. Comprender verdaderamente las fuentes de incertidumbre relacionadas con cada una de las exposiciones de la empresa (consulte el siguiente punto a continuación) es un proceso vital que sienta las bases para decidir cómo medir y administrar el riesgo. Impulsa preguntas como: ¿Cuáles son las variables clave y los supuestos que subyacen al plan de negocios? ¿Qué variables tienen el mayor impacto en el plan de negocios, suponiendo que el alcance del cambio supere significativamente las expectativas realistas? ¿Qué suposiciones subyacentes al plan de negocios son las más críticas para lograr los objetivos de la gerencia? ¿Dónde están los puntos débiles en el plan de negocios, por ejemplo, las metas de desempeño amplias donde la entidad es más vulnerable a no cumplir con las expectativas? Las respuestas a estas y otras preguntas relacionadas brindan información de calidad para la planificación de la respuesta.
- Exposiciones del plan de negocios: La exposición surge cuando cualquier activo o fuente de valor (ver Pregunta 3) del la empresa se ve significativamente afectada por cambios inesperados en las variables subyacentes clave que resultan de la ocurrencia de un evento. Por ejemplo, una organización está expuesta al riesgo cuando un cambio realizado en una variable clave dentro de un horizonte de tiempo dado resultará en un cambio significativo en uno o más de sus indicadores clave de desempeño (KPI). Cuanto mayor sea el cambio potencial realizado en el rendimiento, ya sea positivo o negativo, mayor será la exposición. Una empresa puede estar expuesta a variaciones en el desempeño debido a su modelo comercial, estrategias, procesos, marcas, clientes, fuerza de trabajo de los empleados, posiciones en el mercado u otras fuentes de ganancias y flujo de efectivo. Este punto es importante porque el establecimiento de estrategias a menudo implica asumir riesgos, y el proceso de toma de riesgos a menudo crea exposiciones nuevas o mayores. La gerencia debe considerar si se necesitan respuestas de riesgo para exposiciones significativas identificadas durante los procesos de evaluación de riesgos y establecimiento de estrategias.
- Variabilidad del rendimiento frente a exposiciones a pérdidas: la exposición de una empresa a posibles eventos futuros puede tener consecuencias positivas o negativas. Esto se ve en la forma en que se evalúan las exposiciones y las incertidumbres. Por ejemplo, supongamos que enumeramos todos los eventos o resultados futuros previsibles, incluidas las estimaciones de los flujos de efectivo netos relacionados con cada posible resultado y sus respectivas probabilidades. Los resultados de este ejercicio representan tanto la exposición al alza (oportunidades) como la exposición a la baja (riesgos) cuando los flujos de efectivo netos futuros esperados de todos los resultados previsibles incluyen resultados tanto positivos como negativos, lo que da lugar a la variabilidad del rendimiento. En la situación en la que solo pueden suceder cosas negativas (como cuando se enumeran las posibles consecuencias de un peligro), la administración enumeraría solo las exposiciones a la baja, es decir, cada resultado previsible da como resultado un flujo de efectivo neto negativo, creando una exposición a pérdidas. El punto es este: la naturaleza del riesgo puede influir en la naturaleza de la respuesta al riesgo.
- Escenarios: ¿Qué evento o combinación de eventos puede ocurrir en el futuro y por qué, cómo y dónde pueden ocurrir? ¿Cuál es el impacto en el negocio? La identificación efectiva de eventos y la evaluación de riesgos abordan estas preguntas y brindan información importante para la formulación de respuestas a los riesgos. Si la gerencia piensa en las interrelaciones entre los posibles eventos futuros durante este ejercicio, el análisis es más sólido.

- Exposiciones controlables versus no controlables: La mayoría de los riesgos ambientales están fuera del control de gestión. El impacto de estos riesgos en el negocio debe gestionarse a través de la respuesta estratégica de la organización. Las unidades de negocio, riesgo y soporte deben desarrollar estrategias a largo plazo, así como aprender a anticipar y ajustarse de manera oportuna a los cambios en el entorno externo. Los riesgos de procesos internos, por el contrario, representan riesgos controlables. Estos riesgos a menudo se abordan a través de políticas, procesos y controles internos.
- Exposiciones operativas frente a exposiciones contractuales: Cada respuesta al riesgo tiene que coincidir con la naturaleza y duración del riesgo que aborda. Por ejemplo, si bien un enfoque fragmentado de funciones separadas que buscan la excelencia funcional y unidades de negocios separadas que operan de manera autónoma para lograr planes de negocios enfocados puede ofrecer protección contractual a corto plazo contra ciertos riesgos, no es tan rentable como las estrategias a largo plazo. que están más enfocados operativamente. Por ejemplo, algunos tesoreros han cubierto las exposiciones cambiarias asociadas con las ventas en el extranjero, lo que permite que el personal de la unidad operativa se concentre en el negocio principal de fabricación. Pero la cobertura puede no ser siempre la mejor respuesta. Los riesgos derivados de las operaciones del día a día solo pueden ser abordados, a largo plazo, mediante soluciones de carácter operativo. Dichas soluciones incluyen cambiar la I+D, el inventario y el abastecimiento de mano de obra a entornos de moneda débil, establecer centros regionales de compensación para "reducir" el riesgo cambiario antes de la cobertura y abordar la fijación de precios del producto en función de los estudios de elasticidad. Es por eso que la mejor respuesta al riesgo a menudo surge cuando una tesorería global o regional trabaja en estrecha colaboración con las unidades operativas para combinar tácticas operativas y de cobertura.

Para ilustrar más, si el tipo de cambio de una empresa surge de un contrato con un cliente extranjero, los derivados de divisas que alinean el plazo de la cobertura con el del contrato son efectivos para protegerse contra movimientos adversos en los tipos de cambio. Por el contrario, si la empresa tiene operaciones en curso en el país extranjero, no existe una cobertura de divisas cuyo tamaño, duración y plazos coincidan exactamente con las actividades comerciales de la empresa. Por lo tanto, los gerentes deben examinar la naturaleza y la duración del riesgo para idear una respuesta operativa. Por supuesto, algunas empresas pueden cuestionar este ejemplo en situaciones en las que la gerencia puede concluir que el ingreso neto de una fuente extranjera es razonablemente predecible. Cuando tales afirmaciones son creíbles, esas organizaciones pueden argumentar que la cobertura es efectiva en tales circunstancias.

Hay otros factores importantes a considerar cuando se formulan respuestas al riesgo. Por ejemplo:

- Problemas de cumplimiento: las situaciones que involucran asuntos de cumplimiento, como leyes y reglamentos, autorizaciones y aprobaciones, manejo de materiales peligrosos, seguridad en el taller y operaciones de plantas de energía nuclear, tienen una cosa en común: el cumplimiento riguroso con estándares predeterminados es la norma establecida. Estos entornos y circunstancias requieren políticas y procedimientos apropiados que reduzcan la probabilidad de incumplimiento a un nivel aceptable (según lo definido por la tolerancia al riesgo de la gerencia).
- Cuestiones generalizadas: ¿La exposición o incertidumbre es aislada o tiene múltiples efectos? A menudo, las empresas encuentran ciertos riesgos que les afectan de manera similar en toda la organización: riesgo regulatorio, riesgo político y litigios, por ejemplo. Cuanto más generalizado es el riesgo, mayor es la necesidad de una respuesta al riesgo.
- Frecuencia esperada: ¿La exposición a la incertidumbre surge de eventos poco frecuentes o de eventos que se repiten regularmente? Los eventos únicos que no se pueden anticipar son difíciles de medir y prácticamente imposibles de controlar, pero la organización puede preparar planes de contingencia. Por el contrario, los eventos recurrentes (p. ej., defectos del producto) deben examinarse cuidadosamente y deben desarrollarse respuestas apropiadas, a menudo a través de mejoras o reingeniería de procesos. Los eventos que ocurren con frecuencia son, en esencia, cuestiones operativas que la gestión debe abordar en lugar de riesgos, porque su ocurrencia es más segura.
- Problemas de infraestructura: una fuente importante de riesgo de proceso se encuentra en las interfaces entre procesos, por ejemplo, los llamados "traspasos" entre áreas funcionales. Las interfaces que no están bajo el control de un propietario del proceso presentan un riesgo significativo de errores y omisiones. Las actividades de control deben diseñarse en estos puntos de interfaz o lo más cerca posible de ellos para reducir el riesgo del proceso a un nivel aceptable.
- Disponibilidad de datos: La disponibilidad de puntos de datos también es un problema para muchas empresas para ciertos tipos de riesgo. Algunos riesgos tienen más puntos de datos disponibles que otros para ayudar a los gerentes a medir y analizar

a ellos. Cuando los datos estén disponibles, la organización puede utilizarlos para diseñar una respuesta al riesgo. Ejemplos de estos tipos de riesgos incluyen la entrega de productos a tiempo, los precios de los productos básicos, las reclamaciones de garantía y el acceso a la seguridad de la tecnología de la información. Cuando los datos no estén fácilmente disponibles, la gerencia debe confiar en el juicio o participar en un conjunto más amplio de exposiciones similares que sea susceptible al proceso de suscripción, por ejemplo, comprar seguros para cubrir riesgos relacionados con exposiciones de pérdidas catastróficas. La aparente falta de datos no hace que el riesgo desaparezca y no significa que no se deba gestionar un riesgo.

Si bien el resumen anterior no es exhaustivo, proporciona una idea de algunos de los temas a considerar al formular respuestas al riesgo.

110. ¿Cuáles son los elementos de la infraestructura de gestión de riesgos, por qué son importantes y cómo se consideraron?

Una infraestructura de gestión de riesgos eficaz proporciona las capacidades para ejecutar respuestas a los riesgos. Hay seis elementos de la infraestructura de gestión de riesgos. Estos elementos son políticas, procesos, competencias, informes, metodologías y tecnología (sistemas y datos). Formular una respuesta al riesgo es un ejercicio académico si no considera estos elementos de infraestructura. Si bien pretende ser más un enfoque iterativo que estrictamente lineal, los seis elementos de la infraestructura a menudo se desarrollan un enlace a la vez, cada elemento impulsado por el anterior. Una vez establecidos para un riesgo determinado o para una cartera de riesgos relacionados, estos seis elementos allanan el camino para implementar capacidades mejoradas.

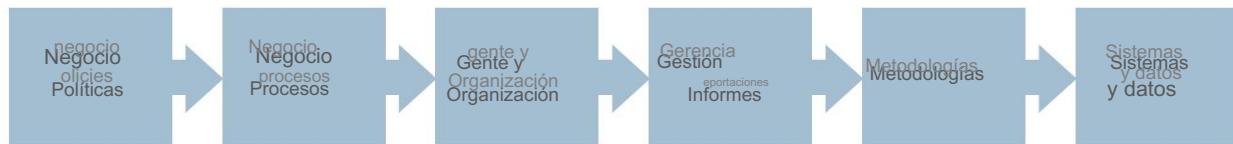
Para explicar más:

- Políticas comerciales: El marco formal de políticas incluye lineamientos específicos, así como los principios más generales que se aplican a todos los aspectos del negocio y la gestión de sus riesgos. Las políticas permiten a los propietarios del riesgo comprender lo que la organización pretende lograr. Las políticas son el vínculo con la estrategia; ponen en juego una estrategia.
- Procesos: Los procesos de la organización son su medio principal para ejecutar sus políticas comerciales. Riesgo las respuestas y las actividades de control se integran deseablemente dentro de los procesos comerciales porque los riesgos se gestionan y controlan mejor lo más cerca posible de la fuente. Las definiciones de procesos deben describir con precisión la secuencia de actividades y tareas que se deben realizar para ejecutar la respuesta de riesgo deseada.
- Competencias: Las personas con los conocimientos, la pericia y la experiencia necesarios ejecutan las funciones de la entidad. procesos. Los roles y responsabilidades de estos propietarios de procesos deben definir y delinear las funciones de toma de riesgos frente a las de monitoreo de riesgos, así como la interacción y los flujos de información y decisión entre las funciones relacionadas. La responsabilidad general de implementar capacidades mejoradas de gestión de riesgos debe recaer en uno o más propietarios de procesos.
- Reportes de gestión: Los reportes de la organización se diseñan de acuerdo a las necesidades de información de los dueños de los procesos. Los informes de gestión deben ser procesables, fáciles de usar, vinculados a responsabilidades bien definidas y preparados con la frecuencia adecuada.
- Metodologías: La solidez de los informes de gestión se ve reforzada o restringida por las metodologías que los respaldan. Las metodologías efectivas ayudan a identificar y priorizar el riesgo, derivar el riesgo a sus impulsores clave y cuantificar el riesgo. También respaldan el análisis de compensaciones de riesgo/recompensa, la diversificación de la cartera, la asignación de capital para absorber pérdidas potenciales, la fijación de precios de productos y servicios para compensar adecuadamente los riesgos asumidos y la planificación de contingencia ante resultados inciertos.
- Sistemas y datos: los sistemas de información respaldan el modelado y la generación de informes que brindan la base necesaria para las capacidades de gestión de riesgos de vanguardia. Brindan información relevante, precisa y oportuna. Las nuevas tecnologías están conduciendo a medidas más refinadas y facilitan la identificación y comprensión de los riesgos, los factores de riesgo y el impacto que tienen en la empresa. Los sistemas de información no solo deben cumplir con los requisitos comerciales actuales de la empresa, sino que deben ser flexibles para futuras mejoras, escalabilidad e integración con otros sistemas.

Si alguno de los elementos de infraestructura antes mencionados es deficiente, la eficacia de los demás elementos puede disminuir significativamente. Por ejemplo, si no se dispone de datos pertinentes y fiables, el valor de los informes a la gerencia se reducen (e incluso pueden ser engañosos). Si los informes no proporcionan información adecuada información, los propietarios del riesgo no pueden ejecutar los procesos de los que son responsables. En consecuencia, el los procesos relacionados no logran alcanzar las políticas establecidas. El efecto, por tanto, es acumulativo.

Los seis elementos de la infraestructura se describen a continuación:

Los elementos clave de la infraestructura deben estar vinculados por diseño:



Riesgo si el elemento es deficiente:



Como se señaló anteriormente, los elementos anteriores generalmente están diseñados de izquierda a derecha. Por ejemplo, las políticas impulsan la diseño de procesos, los procesos dictan la organización de personas y habilidades necesarias, etc. El uso de este La estructura ayuda a organizar el diseño de una respuesta al riesgo utilizando un marco integral y consistente. En en particular, asegura que todos los elementos clave se consideren adecuadamente. Por ejemplo, adecuadamente desarrollar procesos y capacidades de las personas primero, el problema común de poner un énfasis indebido en Se evitan modelos y sistemas. Modelos y sistemas, por tanto, soportan procesos y personas. Lo positivo El impacto de este pensamiento es menos desperdicio al invertir en modelos y sistemas.

Cuando los gerentes comienzan a organizar y alinear la infraestructura de la organización para administrar el riesgo, envían un señal clara de que se toman en serio la gestión de riesgos. Si bien cada elemento individual de la infraestructura es importantes, igualmente críticas son las interrelaciones entre los elementos. Si cualquier elemento de la infraestructura es deficiente, la efectividad de otros elementos puede verse significativamente afectada.

111. ¿Existe un modelo que nos ayude a establecer nuestras prioridades al implementar ERM y monitorear nuestro progreso a medida que mejoramos nuestras capacidades de gestión de riesgos?

El modelo de madurez de la capacidad es una herramienta para ayudar a la gerencia a pensar más claramente acerca de tales preguntas como:

- Cuán capaces queremos que sea nuestra gestión de riesgos a medida que mejoramos nuestras políticas, procesos y medidas para cada uno de nuestros riesgos prioritarios?
- ¿Variamos el rigor y la solidez de nuestras respuestas al riesgo y las actividades de control relacionadas por riesgo?
- ¿Confiamos en unas pocas personas bien calificadas para administrar un riesgo particular de manera ad hoc y apagar incendios regularmente? ¿O mejoramos nuestras capacidades?

Se deben tomar decisiones conscientes al hacer coincidir las capacidades de la organización con el riesgo deseado. respuestas y viceversa. Las capacidades de gestión de riesgos deben ser explícitamente, y dados los recursos finitos, selectivamente—perseguido. Para cada tipo de riesgo individual o grupo de riesgos relacionados, la dirección debe evaluar la madurez relativa de las capacidades de gestión de riesgos de la empresa. A partir de ahí, la gerencia debe hacer una decisión consciente: ¿cuánta capacidad adicional necesitamos para proporcionar una seguridad razonable de que lograr continuamente nuestros objetivos comerciales? Además, ¿cuáles son los costos y beneficios esperados de aumentar capacidades de gestión de riesgos? El objetivo es identificar las exposiciones más apremiantes de la organización y incertidumbres y enfocar la mejora de las capacidades para gestionar esas exposiciones e incertidumbres.

Es por eso que se necesita una herramienta que ayude a la gerencia a pensar claramente sobre el problema de hacer coincidir los capacidades existentes de la organización con sus capacidades deseadas. El siguiente modelo de madurez de capacidad ilustra:



Fuente: Adaptado de Capability Maturity Model: Guidelines for Improving the Software Process, Carnegie Instituto de Ingeniería de Software de la Universidad de Mellon, 1994

¿Qué tan capaz quiere la empresa que sea su gestión de riesgos para cada uno de sus riesgos prioritarios? Eso es lo que pregunta.

Ilustrar cómo se utiliza el modelo de madurez de la capacidad para determinar las mejoras necesarias en el riesgo capacidad de gestión, los cinco estados de madurez pueden examinarse utilizando los seis elementos de infraestructura introducida en nuestra respuesta a la pregunta 110. Explicaremos las interrelaciones entre estos dos marcos y luego discutir su aplicación en la práctica. La explicación de cada estado pretende ayudar organizaciones que deseen una mayor especificidad en cuanto a los criterios para aplicar el modelo.

Como se discutió en nuestra respuesta a la Pregunta 85, la gerencia debe determinar el estado actual de las capacidades de gestión de riesgos para los riesgos prioritarios de la organización. Al comparar el estado actual con el estado futuro deseado, utilizando la estrategia comercial de la organización como contexto, la gerencia puede determinar si existen brechas significativas. La herramienta del modelo de madurez de la capacidad facilita la identificación, el análisis y la presentación de brechas.

## El estado inicial

En el estado inicial de desarrollo, la gestión de riesgos está fragmentada y es ad hoc. La organización gestiona los riesgos individuales en silos y, a menudo, reacciona ante los eventos. Hay una falta general de políticas y procesos formales establecidos, por lo que la organización depende totalmente de las personas que actúan por iniciativa propia para "apagar incendios".

Hay muy poca rendición de cuentas, ya sea por la ausencia de un propietario del riesgo claramente designado (una brecha) o porque hay tantos "propietarios" del riesgo que nadie puede rendir cuentas (una superposición). Demasiados dueños de un riesgo pueden ser tan disfuncionales como no tener ningún dueño de un riesgo, porque nadie puede decidir. Las brechas y superposiciones existentes contribuyen a la falta de rendición de cuentas.

En efecto, las capacidades de gestión de riesgos que existen en el estado inicial generalmente se otorgan a individuos específicos y no tienen una capacidad organizativa. Esto significa que el éxito depende en última instancia de gerentes excepcionales y experimentados que operan por iniciativa propia. El éxito no se puede repetir sin estas mismas personas competentes. Cuando estas personas dejan la organización, la empresa no puede replicar lo que hacen. En última instancia, la eficacia de la organización depende de los esfuerzos y el heroísmo de estas personas.

Además, los problemas significativos de calidad y arquitectura de datos dificultan la capacidad de obtener información para la toma de decisiones. Los costos de recopilación de datos, conciliaciones y otras actividades esporádicas son altos.

Para la mayoría de los riesgos, el estado inicial es inadecuado y no sostenible. Si bien el estado inicial se puede racionalizar para riesgos menos significativos que no son críticos para el plan de negocios, la gerencia debe reconocer que la falta de dirección inherente a este estado es un caldo de cultivo para una crisis que puede alterar la agenda de la gerencia ejecutiva para el "control de daños". en un momento de aviso.

## ATRIBUTOS DE LAS CAPACIDADES DE GESTIÓN DE RIESGOS EN EL ESTADO INICIAL



## El estado repetible

Pasando al estado repetible, vemos evidencia de una estructura de política básica que articula los objetivos y requisitos del proceso. También vemos algunos procesos básicos de gestión de riesgos y actividades de control para lograr los objetivos y requisitos establecidos. Los recursos humanos se asignan a los esfuerzos de gestión de riesgos con personas específicas designadas con funciones, responsabilidades y autoridades definidas. La rendición de cuentas aún puede ser un problema en esta etapa porque los informes no son lo suficientemente rigurosos para responsabilizar a individuos específicos por los resultados. Sin embargo, se están logrando avances con respecto a la mejora de la calidad de los datos a medida que la administración comienza a centrarse en los datos.

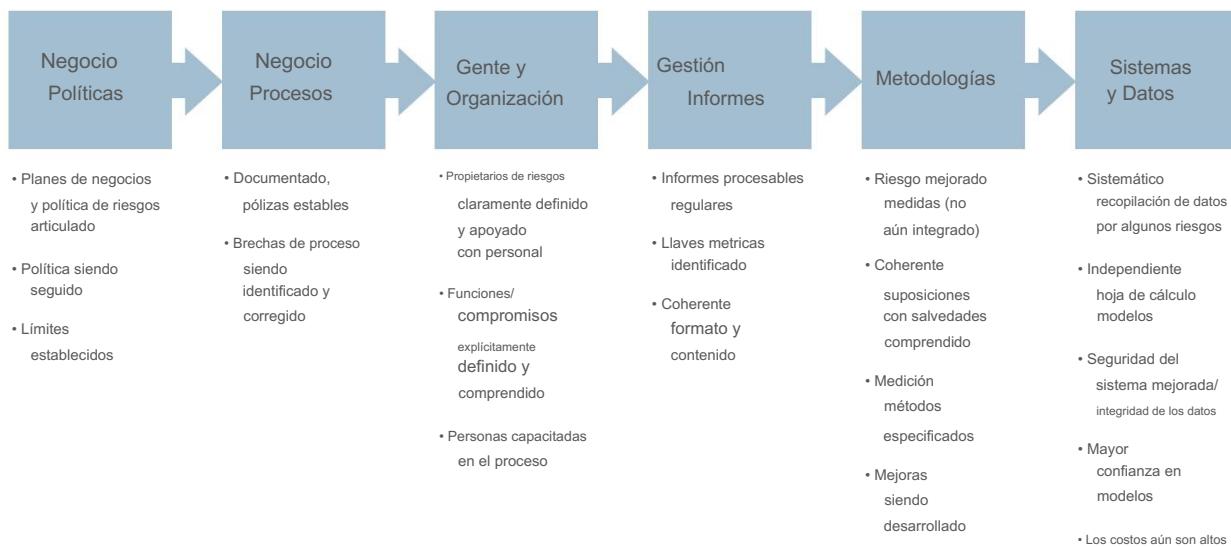
problemas de arquitectura para desarrollar mejor información para unos pocos riesgos seleccionados. Los procesos en marcha muestran algunos evidencia de uniformidad o consistencia entre los segmentos de la empresa. La “repetición” que está teniendo lugar es como resultado de una mayor disciplina en los procesos y directrices establecidas para la gestión de riesgos; sin embargo, hay un mínimo controla la documentación. Las comunicaciones entre las unidades y funciones están mejorando. Gestión de riesgos la educación y la formación refuerzan los objetivos y requisitos del proceso establecidos. Sin embargo, los costos siguen siendo altos.

Todavía se depende de las personas en la etapa repetible. Las personas competentes son y siempre serán una parte vital elemento de infraestructura, al igual que las políticas, los procesos y los informes. Ahora que otros elementos de infraestructura están funcionamiento, cuando una persona capacitada deja la empresa, el vacío no es tan grande como se hubiera tenido estos elementos no han estado en su lugar. Por ejemplo:

- Existe un seguimiento básico de las métricas de producción de calidad, tiempo y costo.
- Los informes básicos de gestión se emiten de manera constante y oportuna, con detalles de apoyo específicos disponibles en una base limitada.
- La recopilación sistemática de datos está facilitando la mejora de los informes, aumentando la confianza general en informes de gestión.
- Existe un proceso para monitorear, capturar y reportar excepciones.
- Existe un mecanismo para capturar mejoras en procesos y metodologías.
- Existen estándares consistentes de integridad de datos y seguridad del sistema, aunque los sistemas y la administración los informes generalmente no son escalables.

Estas mayores capacidades facilitan una mayor clarificación de las funciones y responsabilidades y fomentan más trabajo en equipo eficaz. Sin embargo, aún queda camino por recorrer para alcanzar el estado definido.

#### ATRIBUTOS MEJORADOS DE LAS CAPACIDADES DE GESTIÓN DE RIESGOS EN EL ESTADO REPETIBLE



## El estado definido

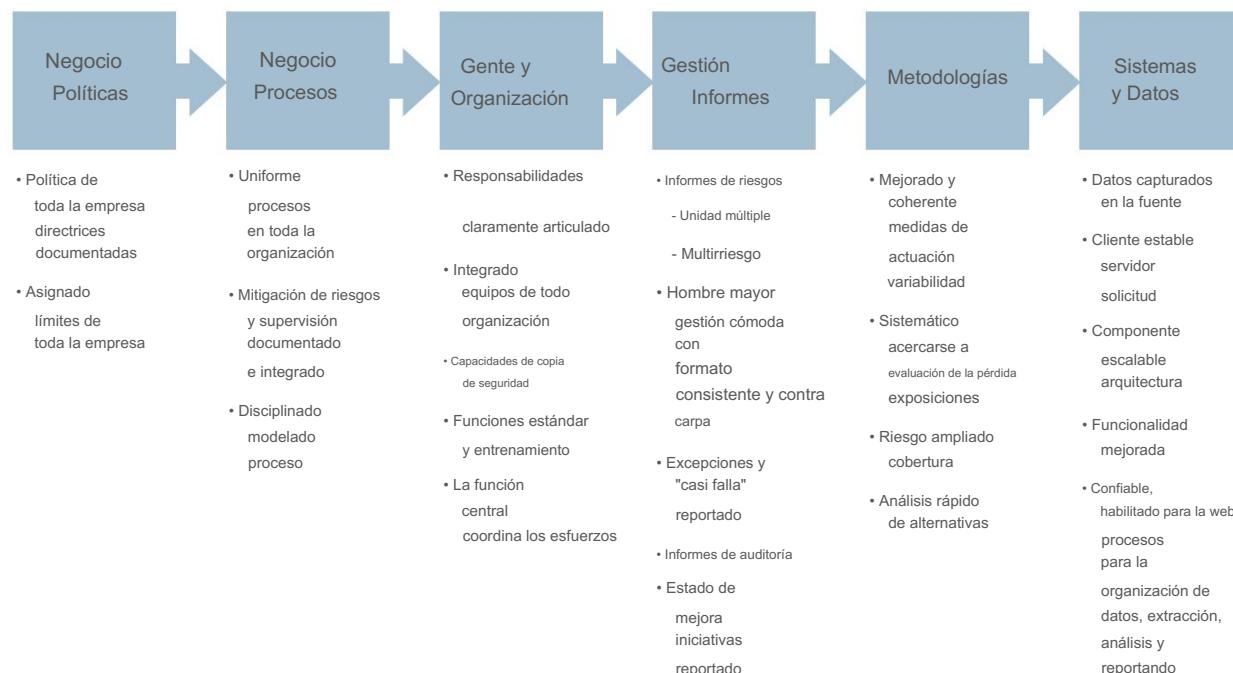
A medida que avanzamos hacia el estado definido, las políticas se desarrollan aún más y los procesos se refinan aún más. El la disciplina del proceso de gestión de riesgos es uniforme en todas las unidades, funciones y capacitación de la empresa. Los procesos para las actividades de mitigación de riesgos y la supervisión de la gestión de riesgos están claramente documentados. Todas las unidades y Los propietarios de riesgos utilizan una versión aprobada y adaptada del proceso de gestión de riesgos definido de la organización, que incluye identificación de eventos, evaluación de riesgos, actividades de control, información/comunicación y seguimiento.

Los otros elementos de infraestructura también están comenzando a tomar forma. La dirección está comprometida con gestionar el proceso a través de una coordinación interfuncional y una documentación de controles más robusta, de modo que que está estandarizado en toda la entidad. La sólida documentación de controles incluye la identificación de los controles y los propietarios responsables de esos controles. Existen mecanismos de verificación para garantizar que las políticas se siguen y los procesos funcionan según lo previsto. Las funciones y responsabilidades están claramente definidas y coherente en toda la organización, con una función central que coordina los esfuerzos, minimiza la duplicación y asegurar la implementación de capacidades de respaldo apropiadas. Los informes de gestión están integrados en procesos de toma de decisiones en toda la organización y contiene resultados cualitativos y métricas cuantitativas de rendimiento.

Los informes más rigurosos y las metodologías que los respaldan aportan mayor claridad a la gestión de riesgos. responsabilidades Los sistemas son más estables y escalables con una funcionalidad mejorada que brinda soporte para procesos confiables y habilitados para la web. Los elementos de datos son más consistentes en toda la empresa y la captura de datos es integrado con las actividades comerciales en curso para que los datos se capturen en la fuente. Finalmente, la tecnología establece un base para todos los demás elementos de la infraestructura.

Es en el estado definido donde vemos evidencia de "toma de decisiones sensible al riesgo y consciente del riesgo". Excepciones y los "cuasi accidentes" se informan oportunamente. Las "lecciones aprendidas" y las deficiencias de control impulsan la mejora iniciativas, que se implementan y reportan en toda la organización.

## ATRIBUTOS MEJORADOS DE LAS CAPACIDADES DE GESTIÓN DE RIESGOS EN EL ESTADO DEFINIDO



## El estado administrado

El estado definido sienta las bases para futuras mejoras de procesos que se produzcan en el estado gestionado. El mejoras adicionales y una mayor sofisticación en este estado superior son principalmente en torno a la mejora cuantificación, y están impulsados por el análisis y la experiencia más rigurosos que son posibles gracias a las capacidades desarrollado en el estado definido. Debido a que el estado administrado es más cuantitativo que el estado definido, existe una mayor énfasis en la medición, agregación y gestión de riesgos en toda la empresa. Por ejemplo, probado en el tiempo, Los modelos integrados y el análisis de riesgos ayudan a los tomadores de decisiones a anticipar los problemas que enfrentan y con apoyando las decisiones que toman. Las medidas de riesgo están vinculadas a los objetivos de desempeño, los sistemas de alerta temprana están en las técnicas de ubicación y asignación de capital se desarrollan y se implementan de manera efectiva. Los límites de riesgo agregado son establecidos y asignados a las unidades operativas. Cuando se exceden los límites predefinidos, se toman acciones correctivas.

En resumen, en el estado gestionado:

- Existe una comprensión constante de las políticas, los procedimientos y los metodologías; los incentivos de los empleados están alineados con las estrategias y los objetivos de toda la empresa.
- Los procesos y productos se definen, comprenden y controlan cuantitativamente; gestión formal de la calidad Las técnicas se aplican para (a) eliminar elementos no esenciales y (b) simplificar y enfocar las actividades del proceso.
- Una familia equilibrada de métricas de calidad, tiempo, costo y riesgo reduce el desperdicio y la repetición del trabajo; la gerencia hace decisiones y aplica el juicio basado en datos cuantitativos, ya que las medidas apropiadas del proceso aumentan la medida de producción ya establecidas.
- Las habilidades y la experiencia requeridas están en su lugar, con modelos a seguir y maestros en evolución y en toda la empresa. La comunicación, la colaboración y el intercambio de conocimientos son más evidentes.
- La organización tiene la capacidad de realizar pronósticos, planificación de escenarios y análisis de tendencias y está preparado para interrupciones significativas, si ocurren.
- Existe un uso y un informe consistentes de objetivos, metas, métricas de desempeño y riesgos en todo el organismo que utiliza sistemas en toda la empresa que brindan informes de panel y capacidades de desglose.

## ATRIBUTOS MEJORADOS DE LAS CAPACIDADES DE GESTIÓN DE RIESGOS EN EL ESTADO ADMINISTRADO



## El estado de optimización

El estado de optimización es el nivel más alto de capacidad. Esta etapa mejora continuamente las capacidades desarrollado durante las etapas anteriores, lo que sugiere que el viaje de la construcción de capacidades de gestión de riesgos es uno que continúa con el tiempo a medida que cambian las condiciones externas e internas. Toda la organización está enfocada en mejora continua a medida que se realizan esfuerzos organizados para eliminar las ineficiencias y el costo/beneficio formal. El análisis se aplica a todas las prácticas de gestión de riesgos. Las mejores prácticas se identifican y comparten de forma rutinaria entre la organización.

Es en esta etapa que la organización alinea completamente sus políticas, procesos, personas, tecnología y gestión de riesgos y el conocimiento. Es también en esta etapa donde la empresa alinea completamente sus medidas en la organización, procesos y niveles individuales. Finalmente, las políticas de riesgo se evalúan a nivel de toda la empresa para equilibrar el riesgo y recompensar, así como comprender y explotar los efectos de la diversificación en múltiples tipos de riesgo.

### ATRIBUTOS MEJORADOS DE LAS CAPACIDADES DE GESTIÓN DE RIESGOS EN EL ESTADO DE OPTIMIZACIÓN



En resumen, en el estado de optimización nos encontramos con una cultura innovadora y de mejora continua, con un fuerte énfasis en mejorar las políticas, procedimientos, metodologías, competencias y sistemas. Prevención de defectos es la norma ya que los propietarios del proceso "incorporan" calidad a través de técnicas de eliminación, simplificación y enfoque y aplicación del análisis de causa raíz de manera consistente en toda la organización. La mejora continua del proceso es impulsado por la retroalimentación cuantitativa y el pilotaje de enfoques innovadores y la actualización continua de conocimientos y habilidades. Iniciativas de mejora corporativa establecidas y aplicadas en toda la empresa (p. ej., Six Sigma) se aplican e integran con la gestión de riesgos.

Estos son los cinco estados del modelo de madurez de capacidades. Nuestra intención al describir cada estado es proporcionar criterios ilustrativos para cada estado y aplicar los seis elementos de infraestructura a cada estado. ahora lo haremos discutir la aplicación en la práctica.

## Aplicación en la práctica

Cada estado sucesivo en el modelo de madurez de la capacidad refleja mejoras adicionales en los atributos para gestionar un riesgo determinado. Cuanto más arriba en la curva sean las capacidades de una empresa, mayores serán sus perspectivas de éxito en la gestión de un riesgo dado o grupo de riesgos relacionados, y menor será su potencial de fracaso.

Si bien las diversas descripciones de capacidades proporcionadas anteriormente son genéricas para la gestión de riesgos, se pueden personalizar para un riesgo o un grupo de riesgos relacionados para proporcionar un modelo para analizar las capacidades necesarias para administrar los riesgos comerciales de la empresa. El uso consistente y basado en hechos de este marco por parte de los propietarios de riesgos de la empresa permite una definición más enfocada de los estados actuales y deseados y promueve la comparabilidad y la comprensión en toda la organización. Junto con los seis elementos de la infraestructura, el modelo proporciona un marco general para definir el nivel adecuado de capacidades de gestión de riesgos y la sofisticación relativa de estas capacidades para cada riesgo prioritario.

El modelo funciona de la siguiente manera. Para cada tipo de riesgo individual o grupo de riesgos relacionados, la dirección evalúa el estado actual de las capacidades de gestión de riesgos de la organización. El estado actual generalmente se refiere a aquellas capacidades que están funcionando actualmente y han estado en su lugar y relativamente estables durante un período de tiempo razonable. El estado actual también puede tener en cuenta **las iniciativas** planificadas actualmente financiadas y en curso para mejorar las capacidades. (Nota: algunos pueden optar por referirse al efecto de las iniciativas planificadas como el "estado mejorado").

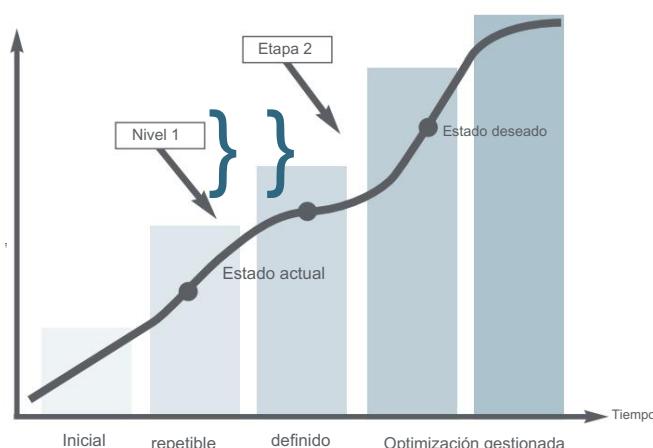
Luego, la gerencia decide cuánta capacidad adicional se necesita para lograr la respuesta de riesgo seleccionada. Esta determinación es el estado deseado. Al evaluar el estado deseado, la gestión debe ser lo más realista posible. El objetivo es seleccionar y diseñar capacidades que proporcionen el "mejor ajuste" con las competencias básicas que se esperaría razonablemente de una organización que ejecuta la estrategia y el modelo comercial de la empresa.

El estado de capacidad deseado puede variar según el riesgo. Por ejemplo, una exposición significativa a cambios en las tasas de cambio puede requerir capacidades al menos en el estado administrado. Algunos riesgos operativos, como operar una planta de energía nuclear, pueden llevar a la gerencia a elegir el estado de optimización porque hay poco margen de error en la operación. Los riesgos de tormentas de viento, incendios, inundaciones y otros peligros, por otro lado, solo pueden garantizar un análisis periódico y la compra de un seguro con poca necesidad de informes de riesgos intrincados de cualquier tipo, una capacidad estatal repetible. Para ciertos riesgos de tecnología de la información, como los riesgos de integridad, confiabilidad y disponibilidad, un estado definido puede ser adecuado. Para los riesgos de seguridad, se puede desear un estado administrado.

Una vez que se identifica y documenta la brecha entre el estado actual y el estado deseado, la gerencia evalúa los costos y beneficios esperados de aumentar las capacidades de gestión de riesgos. Este es el proceso de elaboración de un plan para la transición desde donde se encuentra actualmente la empresa a donde pretende estar. Un análisis de brechas es el medio por el cual las empresas diseñan e implementan una respuesta al riesgo, porque es raro que una empresa implemente una respuesta al riesgo sin ninguna capacidad de ningún tipo. Los pasos prácticos para cerrar las brechas se convierten en una parte integral del plan de negocios de la gerencia.

Para ilustrar, suponga que el estado actual de las capacidades de gestión del riesgo crediticio de una empresa se encuentra en el estado repetible. Supongamos además que la gestión decide que estas capacidades deberían operar en el estado gestionado. ¿Cómo cierra la gerencia esta brecha? ¿Deberían implementarse las mejoras de una sola vez o en etapas, primero avanzando las capacidades al estado definido y luego al estado administrado?

¿Estado?



Hay tres razones por las que “un enfoque por etapas” para el diseño e implementación de capacidades mejoradas Es preferible cerrar la brecha de una vez. Primero, es el más sistemático de los dos enfoques desde un cambio perspectiva de habilitación, es decir, es el enfoque que menos perturba a la organización y está más en línea con la disposición al cambio de su personal. En segundo lugar, el despliegue de la madurez de la capacidad con la gestión soluciones de software ha demostrado que un enfoque por etapas aumenta las posibilidades de una implementación exitosa. En tercer lugar, si bien las mejores prácticas suelen ser útiles y esclarecedoras, no reemplazan el ejercicio de una cuidadosa pensamiento y juicio por parte del personal informado sobre la gestión de riesgos deseada de la empresa capacidades para un riesgo dado. Por lo tanto, el plan de gestión del cambio de la entidad debe abordar cómo el transiciones empresariales del estado actual al estado futuro y con qué rapidez. Uso de los seis elementos de El modelo de madurez de infraestructura y capacidad facilita esta planificación.

Para ilustrar aún más el uso de los dos marcos, a continuación se incluye un resumen de las capacidades en torno a la gestión riesgo de adquisición:



	Negocio Políticas	Negocio Procesos	Gente y Organización	Gestión Informes	Metodologías	Sistemas y Datos
optimizando	Alineado estratégico planes, abastecimiento estratégico total y responsabilidades definidas e integradas	Adquisiciones integradas y procesos y evaluación comparativa continua	Capacidad de adaptarse a entornos cambiantes y demandas de los clientes, subcontratación de no central competencias	Completamente desarrollado seguimiento automatizado y consistente y planificación	Alineado estratégico metodologías que enfatizan continuo mejoramiento	Suite completa de sistemas a través la cadena de suministro para el análisis
Administrado	Mayor ejecución de fuente estratégica; personal alineado con estrategia	Uso efectivo de técnicas formales de gestión de riesgos	Consolidado y suministro apalancado base en su lugar; equipos de productos básicos capacitados	Información de adquisiciones de alta calidad, autoevaluación común	Sofisticado, modelos y herramientas robustos	Almacén de datos de adquisiciones en su lugar y utilizado; tarjetas p y automatización
definido	Adquisición anual planes, estratégico abastecimiento de clave materias primas	Procesos definidos, alianzas estratégicas establecidas	Cuentas por pagar centralizado, formación ofrecida, y equipos de propósito especial	Proveedores clave seguimiento, puntos de referencia estándar y auditorías internas	bien desarrollado modelos disponibles para la toma de decisiones	La organización opera con contratos
repetible	solo ocasional enfoque estratégico en el abastecimiento y políticas informales	Apalancamiento de suministro ocasional; algunos estratégicos asociaciones	Algunos profesionales de adquisiciones en el personal; entrenamiento limitado	Información clave de adquisiciones internas disponible con auditorías que ocurren	Modelos simples que se usan de manera inconsistente	Suite de bastante sistemas efectivos; manual de Procedimientos
Inicial	Adquisiciones no abordadas como una oportunidad estratégica, sin dirección o políticas	Compras no apalancado, sin alianzas estratégicas	Sin liderazgo y falta de personal calificado	Información crítica no disponible y no interna revisión de cuentas	Sin modelos; confianza en la gente	Dispar, ineficiente, adquisitivo, cuentas por pagar sistemas

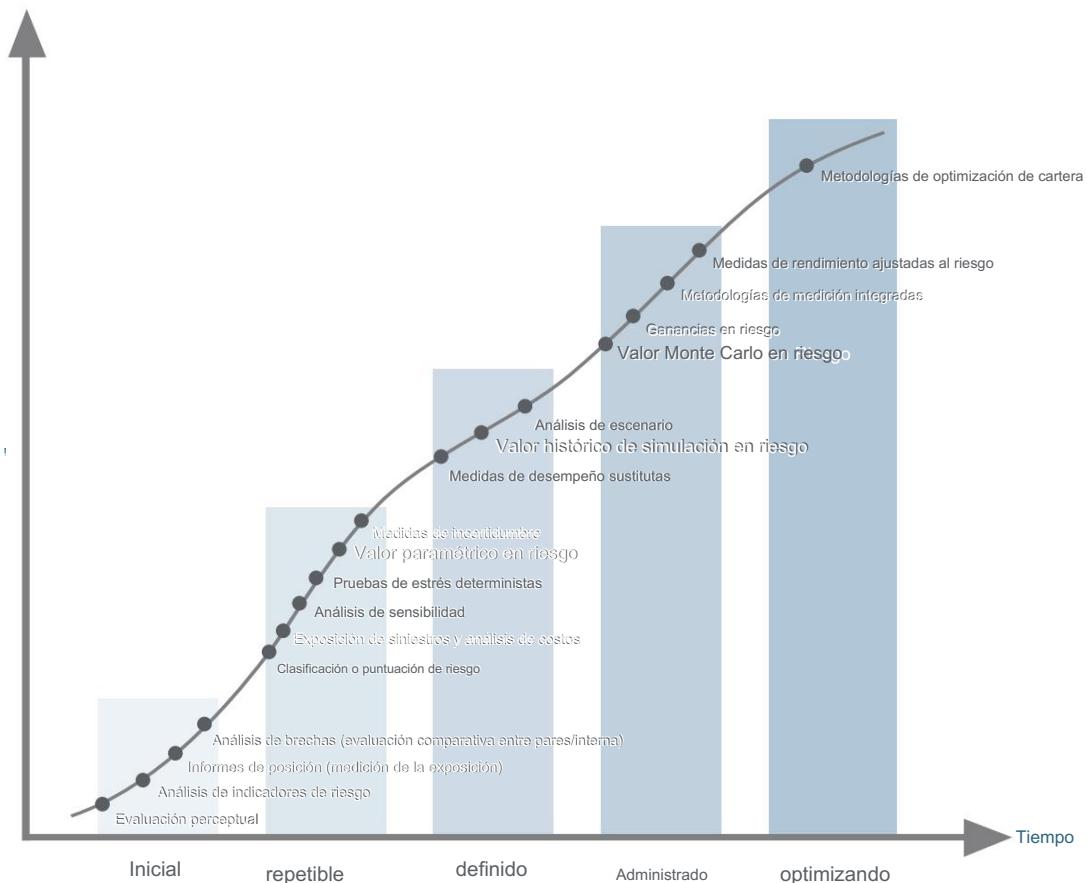
A lo largo del proceso de planificación de la respuesta al riesgo, es importante reconocer que lo que representa “la mejor práctica” en el contexto de un riesgo particular en una empresa puede ser insuficiente o exagerada en el contexto del mismo riesgo en otra empresa. Por ejemplo, las aplicaciones más sofisticadas de valor en riesgo pueden representar las mejores prácticas para administrar el riesgo de mercado en un negocio comercial. Sin embargo, en otro negocio donde solo están involucradas unas pocas transacciones expuestas al riesgo de precio, tal sofisticación puede ser innecesaria debido a la exposición insignificante. No es necesario desplegar los más sofisticados y avanzados Técnicas para todo riesgo. Ninguna organización tiene los recursos para hacer eso. Tampoco hay un negocio viable. razón para hacerlo.

## 112. ¿Cuáles son las técnicas alternativas para medir el riesgo y cuándo se implementan?

A medida que mejoran las capacidades de la organización, también mejoran sus metodologías de medición de riesgos. Hay muchos métodos para medir el riesgo. En el modelo de madurez de la capacidad, hay cinco estados de capacidad: inicial, repetible, definida, gestionada y optimizada. Con cada estado sucesivamente superior, hay un mayor nivel de conocimiento, experiencia y comprensión. Cuanto mayor sea el nivel de capacidad, más sofisticadas serán las metodologías de medición que se pueden implementar de manera efectiva. En el nivel más bajo de capacidad, las técnicas utilizadas suelen ser direccionales, es decir, muestran áreas para un análisis posterior. A medida que aumentan las capacidades, las técnicas de medición disponibles son más confiables y procesables para la toma de decisiones.

En general, el rigor y la sofisticación de la metodología de medición necesaria para un riesgo en particular o un grupo de riesgos relacionados están determinados por la complejidad del entorno (por ejemplo, el número de riesgos y las interrelaciones entre los riesgos), el alcance de la volatilidad esperada y la criticidad del riesgo para la ejecución del modelo de negocio. El nivel de capacidad deseado por la gerencia (como el grado de agregación y vinculación con el desempeño de toda la empresa) también es un factor clave. Los costos de implementación y la disponibilidad de datos relevantes (con cierto nivel de implementación posible incluso con datos escasos o "ruidosos") también son consideraciones. Por ejemplo, las carteras grandes y complejas de materias primas altamente volátiles que pueden tener un efecto significativo en las ganancias pueden requerir técnicas más sofisticadas, incluidos modelos estadísticos y análisis de escenarios. Los modelos basados en simulación, por ejemplo, pueden ser útiles para capturar la interacción de la tasa, el precio u otros factores cuando se trata de carteras complejas o posiciones de riesgo. A continuación, se utilizan análisis de sensibilidad o pruebas de estrés para medir el impacto potencial de los movimientos extremos del mercado en el valor de la cartera.

El siguiente esquema ilustra ejemplos de técnicas de medición de riesgo que son apropiadas en cada estado de madurez a lo largo del modelo de madurez de capacidad:



Medición de riesgos en el estado inicial : en el nivel inicial de capacidad, las actividades de gestión de riesgos son ad hoc. Los métodos de medición implementados en esta etapa deben ser relativamente sencillos y fáciles de aplicar y comprender porque la organización carece del conocimiento y las capacidades básicas de gestión de riesgos para aplicar metodologías más sólidas y complejas. En la etapa inicial, no es suficiente que el poco personal competente en gestión de riesgos que trabaja para la organización comprenda la aplicación de estas metodologías de medición. Debido a que la organización carece, entre otras cosas, de políticas, procesos y conocimientos de gestión de riesgos, es muy probable que estas metodologías de medición se apliquen como un apéndice en lugar de una herramienta integrada. Por lo tanto, la gerencia ejecutiva y de la unidad de negocios tendrá dificultades para traducir los conocimientos que brindan estas metodologías en planes procesables. La organización tampoco estaría generando en el curso normal las entradas de datos que requieren estos métodos. Cuando las personas que usan las herramientas se van, ¿qué hace la organización con las herramientas que nadie más entiende? Por lo tanto, las metodologías de medición deben ser lo más simples y directas posible para que la organización las asimile en las actividades comerciales normales. Las técnicas de autoevaluación, las evaluaciones facilitadas, el análisis de indicadores de riesgo, los informes de posición y los análisis de brechas (usando marcos comunes) son ejemplos de tales técnicas. Estas técnicas son más direccionales que procesables, porque a menudo señalan áreas que requieren más investigación y análisis.

Medición de riesgos en el estado repetible : en esta etapa, las políticas básicas de gestión de riesgos están establecidas, los procesos básicos de gestión de riesgos están establecidos y las actividades básicas de control están instaladas. Las metodologías de medición también tienden a ser algo básicas. Los siguientes son algunos ejemplos:

- Clasificación o puntuación de riesgo: clasifica o puntúa sistemáticamente el nivel de riesgo. A menudo se utiliza para calificar el riesgo crediticio del cliente de manera consistente y para respaldar, administrar y monitorear las decisiones de autorización de crédito, tanto por varios ejecutivos que toman decisiones similares en toda la empresa como por ejecutivos individuales que evalúan a múltiples clientes. Clasificación o puntuación de riesgo:
  - Utiliza plantillas y sistemas analíticos basados en la aplicación de criterios predefinidos y preautorizados.
  - Incrementa la efectividad, eficiencia y consistencia del proceso de recolección de hechos a través de un estructura sustentada en criterios comunes.
  - Incrementa la calidad de la toma de decisiones al exigir a los directivos que apliquen los mismos criterios y pautas a la hora de evaluar los hechos recogidos.
  - Solicita la consulta con una autoridad superior cada vez que surgen situaciones inusuales y atípicas.
- Tenga en cuenta que algunos sistemas de calificación de riesgo crediticio son muy sofisticados. A medida que las organizaciones llevan sus capacidades de gestión del riesgo crediticio a los estados definidos y gestionados, mejoran sus metodologías de puntuación o calificación.
- Exposición de siniestros y análisis de costos: Evalúa las variables que finalmente determinan el costo de varios tipos de reclamos: garantía, litigio, medio ambiente, salud y seguridad, etc. Los tomadores de decisiones utilizan estos datos para decidir las acciones apropiadas a tomar.
- Análisis de sensibilidad: Determina la variación agregada en el desempeño financiero evaluando el impacto atribuible a un pequeño cambio diferencial en uno o más factores de riesgo clave subyacentes en exposiciones individuales en un momento dado.
- Prueba de estrés determinista: Toma una cartera o pronóstico de "caso base" dado y modifica su valor para reflejan los efectos de una situación o evento hipotético, extraordinario pero altamente improbable que resultará en un estrés financiero severo si llegara a ocurrir.
- Valor en riesgo paramétrico: Calcula el valor en riesgo para evaluar el impacto potencial de un subyacente variable, como un tipo de cambio, sobre el valor de una cartera en el futuro. Se basa en el supuesto de que la distribución a partir de la cual se extraerán los valores futuros de la variable subyacente durante el horizonte de tiempo seleccionado es idéntica a una distribución normal supuesta.
- Medidas de incertidumbre: realiza un seguimiento de las variables clave relacionadas con una exposición identificada o una fuente de valor para obtener una medida de la variabilidad del rendimiento esperado. Mientras que las exposiciones informadas en un informe de posición son las medidas brutas nominales (cuentas por cobrar totales, rendimiento de producción o flujos de ingresos),

la incertidumbre es una medida de la variabilidad del rendimiento asociada con los rendimientos de esa medida bruta. Por ejemplo, una exposición cambiaria podría ser de £10 millones, mientras que la métrica de riesgo se definiría como la volatilidad esperada en los tipos de cambio aplicados al valor bruto de la exposición. Ejemplos de Las variables clave para evaluar la incertidumbre se proporcionan en la Pregunta 3.

Medición del riesgo en el estado definido : en la etapa definida, las metodologías de medición reflejan la elementos adicionales de infraestructura que se han implementado, incluidos informes mejorados, más sólidos metodologías y tecnología más estable. Las metodologías de medición son más refinadas en esta etapa.

Los siguientes son ejemplos:

- Medidas de rendimiento sustitutas: utiliza medidas de rendimiento de calidad, tiempo y costo como sustitutos de medir el riesgo. Por ejemplo, puede ser imposible medir directamente el riesgo de satisfacción del cliente. Como hacer mide las consecuencias de los clientes que están insatisfechos con el producto o servicio de la empresa, considerando el comportamiento probable del cliente, la probabilidad de nuevos negocios de reemplazo en períodos futuros, el potencial de pérdida permanente de negocios repetidos y la pérdida de cuota de mercado? Como alternativa sustituto, la empresa puede integrar estadísticas operativas internas, comentarios de los clientes y otros información. Al hacerlo, puede evaluar las medidas de satisfacción del cliente y obtener información sobre qué tan bien es la gestión de sus clientes. Si estas medidas reflejan un desempeño consistentemente positivo a lo largo del tiempo, el empresa puede inferir que está gestionando eficazmente el riesgo de satisfacción del cliente.
- Valor en riesgo de simulación histórica: Calcula el valor en riesgo basado en el supuesto de que el distribución a partir de la cual se extraerán los valores futuros de una variable subyacente sobre el futuro seleccionado horizonte de tiempo es idéntico a la distribución de valores históricos observados durante un período de tiempo específico en el pasado.
- Análisis de escenarios: Determina la variación agregada en el desempeño financiero evaluando el impacto de grandes cambios en los factores de riesgo, definidos por un escenario específico, en exposiciones individuales. Me gusta la sensibilidad el análisis, los escenarios y su impacto en las ganancias se evalúan de manera determinista, es decir, sin evaluación está hecho de la probabilidad de que los eventos realmente ocurran. Sin embargo, el análisis de escenarios es más robusto. metodología de medición que el análisis de sensibilidad porque involucra (1) múltiples variables que son a menudo cambiado dramáticamente durante el procedimiento y (2) pronósticos económicos y modelos para cambiar el precio exposiciones y carteras con base en los cambios y pronósticos asumidos.

Medición del riesgo en el estado gestionado : el estado definido sienta las bases para avanzar hacia el estado gestionado en el que los riesgos se gestionan cuantitativamente y se agregan a nivel corporativo. en el administrado estado, vemos técnicas de medición tales como:

- Valor en riesgo de Monte Carlo: Calcula el valor en riesgo ajustando la distribución de valores posibles para lo que los gerentes creen que estará más cerca de la realidad (lo que realmente sucederá) que una distribución basada únicamente en una muestra histórica.
- Ganancias en riesgo: combina factores operativos, como carga y capacidad, con cambios de mercado en la cálculo del valor en riesgo para ampliar el rango de posibles resultados considerados. Mide la medida a los que las ganancias podrían no alcanzar las expectativas durante el horizonte de planificación, dada la gestión de supuestos en torno a los riesgos clave.
- Metodologías de medición integradas: combina modelos y análisis rigurosos para desarrollar técnicas que se mejoran continuamente con el tiempo. Estas metodologías vienen en una mirada de tipos y grados de complejidad, incluidos modelos de (a) riesgos individuales, (b) grupos de riesgos relacionados y (c) el perfil de riesgo agregado de la empresa. También pueden abordar el entorno comercial de la empresa, teniendo en cuenta factores como la competencia y la dinámica de la industria, las tendencias políticas, la demanda de los clientes, proveedores y condiciones de mercado más amplias (como la interacción entre la demanda y la carga en carteras de energía sensibles al precio).
- Medición del desempeño ajustado al riesgo: Mide el desempeño de la unidad de negocios con base en definiciones de inversión, capital y rendimientos para proporcionar una herramienta de medición y generación de informes de desempeño que alinee los incentivos de los accionistas, la alta dirección y la dirección de las unidades de negocio.

Medición del riesgo en el estado de optimización : la organización se centra en la mejora continua en este escenario. El grado de conocimiento y comprensión del riesgo en esta etapa conduce a metodologías de medición. que se centran en una vista de cartera, o conjuntos de riesgos. En lugar de gestionar los riesgos individuales, la gestión optimiza la gestión de riesgos agrupando los riesgos en familias lógicas donde se miden y gestionan como un portafolio. Una cartera es una agrupación natural de riesgos que comparten características fundamentales, por ejemplo, impulsores comunes, correlaciones positivas o negativas u otras características que hagan susceptibles a los riesgos de la aplicación de metodologías comunes de medición y respuestas al riesgo. Si los riesgos se agregan y gestionan como una cartera, se desarrollan los medios cuantitativos para transferir y titularizar el riesgo. Las transferencias de riesgo también son más eficientes cuando los riesgos son neteados o compensados. Para ilustrar, las exposiciones de divisas se pueden agrupar para determinar la empresa "exposición neta" – cuando esa práctica se corresponde con la filosofía operativa de la organización. Este "riesgo total focus" lleva a los gerentes a desarrollar metodologías patentadas que optimizan el riesgo y el rendimiento en una cartera amplia. base, lo que lleva a una mayor confianza en que las decisiones se basan en una visión completa del negocio. Por ejemplo, los riesgos crediticios se pueden agregar con los riesgos cambiarios para que una medida común se centre en cómo el riesgo crediticio aumenta o disminuye a medida que cambian las tasas de cambio. Los grandes cambios en las tasas de cambio pueden causar cambios en la exposición a contrapartes particulares porque las revaluaciones del mercado pueden afectar su capacidad para pagar sus deudas.

#### 113. ¿Cómo influye ERM en los informes de gestión?

La generación de informes es un elemento crítico de la infraestructura de ERM. A medida que las organizaciones evolucionan hacia soluciones más repetibles, programas de gobierno y cumplimiento sostenibles y automatizados, la tecnología jugará un papel clave en mejorar los métodos y herramientas que permiten los dos componentes COSO: Información y Comunicación, y monitoreando. En concreto, la tecnología puede facilitar la evolución del proceso de gestión de riesgos. Para Por ejemplo, la gestión de riesgos de una empresa puede consistir principalmente en:

- Actividades discretas: estas actividades generalmente enfatizan la documentación dentro de un solo depósito de datos.
- Actividades periódicas: para muchas entidades, estas actividades normalmente se realizan a través de un tipo de autoevaluación. capacidad.
- Actividades continuas: limitadas a un solo repositorio, estas actividades permiten el intercambio continuo de actualizaciones, y notificación de información.
- Actividades continuas en toda la empresa: estas actividades respaldan la automatización de procesos y controles, en tiempo real Informes y monitoreo de indicadores clave de riesgo (KRI) en aplicaciones dispares.

Estas actividades integran procesos de gestión de riesgos en la rutina empresarial diaria, proporcionando así mayor seguridad y una ejecución más eficaz. El objetivo de la infraestructura ERM es integrar aún más estas actividades y mejorarlas continuamente. Los informes de gestión representan una integración y oportunidad de mejora porque vincula el riesgo y el desempeño de la gestión de riesgos con lo que es importante.

Como se discutió en nuestra respuesta a la pregunta 45, la dirección ejecutiva necesita información para tomar decisiones informadas. decisiones con confianza sobre los riesgos prioritarios a los que se enfrenta la organización. Una visión de toda la empresa lleva a una empresa a integrar su información sobre riesgos y el desempeño de su gestión de riesgos capacidades con otra información utilizada en el negocio. Así, la organización mide e informa sobre lo que asuntos importantes: esto significa que TODA su información crítica relacionada con la calidad, el tiempo, el costo y el riesgo debe ser integrado en su cuadro de mando integral. Las empresas comprometidas con ERM trabajan para que esta integración suceda.

La generación de informes es especialmente importante, además de inherentemente difícil, cuando se gestiona el riesgo utilizando datos cualitativos. En En ausencia de metodologías cuantitativas sólidas, los informes se pueden generar de varias maneras, que incluyen plantillas de informes estándar, informes filtrados, búsquedas y consultas ad hoc. Como se discutió en la Pregunta 121, Los tableros brindan vistas agregadas de información, lo que permite a los usuarios profundizar más en las áreas de interés. o preocupación por detalles adicionales. Cuando los informes se aumentan a través de aplicaciones empresariales, el ERM solución se vuelve más completa. Las aplicaciones empresariales brindan capacidades de automatización y flujo de trabajo fuera de los requisitos de gobierno específicos. También brindan administración de contenido, soporte para el intercambio de conocimientos y documentos a nivel empresarial, y fuentes de transacciones en vivo para el monitoreo en tiempo real de los KRI.

114. ¿Qué productos de software de gestión de riesgos están disponibles actualmente para ayudar a las empresas con implementando ERM?

Hay tres categorías principales de proveedores de software de gestión de riesgos: (1) herramientas de evaluación de riesgos empresariales (por ejemplo, soporte de decisiones, encuestas y registros de riesgo), (2) herramientas de software de riesgo operativo (por ejemplo, cualitativo y cuantitativa) y (3) soluciones integradas de plataforma de cumplimiento y gestión de riesgos. Cada una de estas categorías se discute a continuación.

Las herramientas de evaluación de riesgos empresariales (ERA) cubren una amplia gama de soporte de decisiones, encuestas y registro de riesgos. herramientas. Los proveedores de soporte de decisiones y encuestas se acercan al mercado desde su fortaleza al permitir facilitado talleres de riesgos, autoevaluaciones de control y/o evaluaciones de riesgos a nivel de entidad. Estos proveedores continúan construyendo sus soluciones agregando la funcionalidad de encuestas basadas en la web para respaldar las evaluaciones de riesgos fuera de una cautiva montaje del taller. También hay varios pequeños proveedores que ofrecen herramientas de registro de riesgos que: admiten uno o más marcos de riesgo; proporcionar un depósito de datos para información de objetivos, procesos, riesgos y controles; apoyo monitoreo continuo, pruebas y planificación de acciones; y proporcionar capacidades básicas de generación de informes. Estas soluciones son relativamente simplistas y poco sofisticados, y generalmente carecen de integración con otras normas de cumplimiento y riesgo. actividades de gestión.

Hay más de una docena de proveedores de software que desarrollan y venden productos especializados para el riesgo operativo. gestión (ORM). Los componentes principales de una solución ORM incluyen la recopilación de datos y la autoevaluación herramientas, creación de escenarios y modelos, exposición al riesgo operativo y calculadoras de capital, y recursos internos y externos. reportes regulatorios. Muchas de estas soluciones fueron desarrolladas inicialmente por los proveedores en colaboración con uno o más clientes, y mejorado con el tiempo. Algunos ofrecen soluciones cualitativas de gestión de riesgos integradas con flujo de trabajo de auditoría interna y plantillas de cumplimiento de Sarbanes-Oxley. Otros tienden a tener una banca/Basilea II orientación al cumplimiento. Otros ofrecen herramientas analíticas y de modelado de riesgo sofisticadas, que incluyen estimación de frecuencia y severidad, cálculo de exposición, cálculo de capital y análisis de escenarios, así como seguimiento de eventos de pérdida.

Finalmente, los proveedores de software empresarial están ingresando agresivamente al mercado de cumplimiento y gestión de riesgos. Estos proveedores están ofreciendo soluciones inicialmente diseñadas para permitir el cumplimiento de Sarbanes-Oxley, pero con claras intenciones de ampliar las capacidades más allá de Sarbanes-Oxley a la gestión de riesgos y otras áreas de cumplimiento. El juego final para estos proveedores es desarrollar una "solución total" para un cumplimiento, una gobernanza y un riesgo más amplios. gestión, con la asistencia y las contribuciones temáticas de los socios de la alianza de consultoría.

115. ¿El mercado de software ERM ha alcanzado la madurez tal que existen soluciones establecidas y líderes claros?

Varios factores están influyendo en el mercado en el momento de la impresión de esta publicación:

- (a) Existe un mandato para centrarse en el control interno sobre la información financiera de la Ley Sarbanes-Oxley, proporcionar una justificación adicional para la inversión en tecnología.
- (b) Hay un énfasis continuo en mejorar el desempeño de la auditoría interna del New York Stock Requisitos para cotizar en bolsa.
- (c) Existe un mayor impulso para comprender y cuantificar el riesgo operativo por parte de los reguladores europeos.
- (d) Muchas empresas tienen la intención estratégica de integrar el cumplimiento sinérgico y la gestión de riesgos actividades, habilitadas por una infraestructura de tecnología de gestión de riesgos y datos comunes.

En la actualidad, se presta cada vez más atención a los riesgos operativos a medida que los reguladores de los servicios financieros de todo el mundo el mundo se enfoca en responder a las recomendaciones de adecuación de capital que surgen de Basilea II Acuerdo del Comité de Supervisión Bancaria de Basilea, un consorcio internacional de reguladores bancarios. Varios Los proveedores de software ingresaron al espacio de gestión de riesgos operativos a fines de la década de 1990, motivados por la innovación. y la automatización que se está produciendo en otras áreas de la gestión de riesgos. Más vendedores ingresaron al mercado después de la El anuncio de Basilea de que la próxima ola de recomendaciones de suficiencia de capital incluiría el riesgo operativo. La entrada de vendedores al mercado no sorprende, dado que más de 100 naciones han accedido a la Disposiciones de Basilea II.

Desafortunadamente, el mercado está madurando mucho más lentamente de lo esperado. Los proveedores actuales son una combinación de la vieja guardia y los nuevos proveedores entrantes. Ninguno está especialmente probado debido a la relativa falta de éxito de cualquiera de los productos establecidos. Los jugadores más nuevos tienden a tener un enfoque más pragmático de la gestión de riesgos y han introducido soluciones más alineadas con los requisitos actuales del mercado. Las soluciones de la competencia ahora son más comparables en términos de funcionalidad y precio. En este momento, no existe un líder claro en el mercado, aunque varias soluciones están ganando cuota de mercado.

Muchas soluciones son relativamente nuevas en el mercado o están en versión beta. Varios proveedores todavía están en la fase de diseño. No existe una solución verdaderamente integrada. Es posible que el mercado se deba a una mayor consolidación, dejando solo un puñado de proveedores de software empresarial y especialistas en riesgo operativo. El software de gestión de riesgos tiende a ser muy diferente entre geografías, con diferentes factores que impulsan la adopción que conducen a diferentes priorizaciones de funcionalidad. Es probable que las soluciones de software que integran los esfuerzos de cumplimiento, gestión de riesgos y auditoría interna sean las más exitosas con el tiempo.

116. ¿Qué criterios debemos usar para evaluar las alternativas de software? ¿Hay diferentes priorizaciones de funcionalidad?

Los criterios para evaluar el software ERM y la prioridad relativa de la funcionalidad pueden variar de una empresa a otra. Los requisitos y el enfoque de la organización suelen impulsar la prioridad relativa. Las características y definiciones importantes de una solución integral para la gestión de riesgos se resumen a continuación para proporcionar criterios para evaluar alternativas. (Nota: ERA = Evaluación de riesgos empresariales; ERM = Gestión de riesgos empresariales; ORM = Gestión de riesgos operativos; IA = Auditoría interna):

CARACTERÍSTICA	DEFINICIÓN DE FUNCIONALIDAD	COMPONENTE COSO ERM	SOLUCIÓN
Definición y objetivos de la entidad	Documentar la jerarquía organizativa e identificar los componentes comerciales para la estructura de informes de riesgos	Entorno interno, fijación de objetivos	ERA, ERM y ORM
Identificación de riesgo	Incorpore un modelo de riesgo común, identifique amenazas y vulnerabilidades potenciales, calcule la probabilidad y el impacto de los eventos, genere factores de riesgo, determine indicadores clave de riesgo y asigne tipos de riesgo a procesos y unidades comerciales.	Identificación de eventos, evaluación de riesgos	ERA, ERM y ORM
Marco de apoyo	Soportar varios marcos regulatorios y/o de riesgo de propiedad	Varios	ERA, ERM y ORM
Control de riesgo y monitoreando	Defina los controles requeridos, responda para mitigar los factores de riesgo, califique la efectividad de los controles, pruebe los controles y estime el riesgo residual	Evaluación de riesgos, respuesta al riesgo, actividades de control	ERM y ORM
Programación y notificación del flujo de trabajo de riesgos	Supervise los cronogramas de evaluación, los perfiles de riesgo y los planes de acción en tiempo real y genere escalamiento y notificación automatizados y escalonados, enrutamiento del personal y manejo de excepciones.  (Nota: Los mejores sistemas admitirán un proceso de flujo de trabajo personalizado para incorporar los requisitos del usuario)	Evaluación de riesgos, respuesta a riesgos, actividades de control, seguimiento	ERM y ORM
Riesgo y auditoría seguimiento de problemas	Implemente avisos automatizados para la escalada de problemas y controle las debilidades para la acción correctiva, y respalde el monitoreo de los planes de acción correctiva.	Respuesta a riesgos, actividades de control, información y comunicación, seguimiento	ERM y ORM

CARACTERÍSTICA	DEFINICIÓN DE FUNCIONALIDAD	COMPONENTE COSO ERM	SOLUCIÓN
Recopilación de datos/ seguimiento de eventos	Registrar información de pérdidas internas, potenciales y externas; monitorear eventos futuros potenciales que aún no han ocurrido; recopilar datos para estimar el potencial de pérdidas futuras; flujo de trabajo de soporte para enrutar información	Información y comunicación, seguimiento	ORM
Autoevaluación de riesgos y controles	Utilizar cuestionarios automatizados que permitan a los propietarios de procesos y/o riesgos ingresar información sobre sus pérdidas y exposiciones, incluida la frecuencia y gravedad de posibles pérdidas futuras, así como la evaluación de las fortalezas y debilidades de las capacidades de gestión de riesgos; determinar los riesgos inherentes; establecer umbrales y límites; y crear modelos de evaluación (Nota: la flexibilidad para definir categorías, preguntas, encuestados y parámetros para los cuestionarios y el mecanismo de distribución para el seguimiento y los procesos de auditoría relacionados con estas evaluaciones también son importantes)	Evaluación de riesgos, riesgo respuesta	ERA, ERM y ORM
Definición y seguimiento de KRI/KPI	Definir una plantilla estándar para indicadores de riesgo/ indicadores de desempeño para uso en toda la empresa; relacionar KRI/KPI con unidades de negocio o procesos específicos y/o con eventos de pérdida específicos; generar alertas de gestión de infracciones de umbral; apoyar la comparación con los puntos de referencia	Respuesta a riesgos, actividades de control, información y comunicación, seguimiento	ERM y ORM
Estimación de frecuencia y severidad y otros análisis estadísticos	Evaluar la importancia de una exposición particular y reconocer la probable frecuencia y gravedad de una pérdida; permitir que estas estimaciones se ingresen manualmente o se deriven en base a datos históricos; la funcionalidad básica incluye evaluaciones rojo-ámbar-verde; Las características más avanzadas brindan la capacidad de derivar estimaciones basadas en datos históricos directamente dentro del sistema y permiten diferentes modelos de puntuación en todos los tipos de riesgo.	Evaluación de riesgos	ERM y ORM
Cálculo de la exposición	Traducir KRI, estimaciones de frecuencia y gravedad e información de autoevaluación en exposiciones cuantificadas, incluidas distribuciones de probabilidad que brindan visibilidad en torno a una variedad de resultados potenciales	Evaluación de riesgos, respuesta a riesgos, información y comunicación	ORM
Guion análisis	Lleve el cálculo de la exposición un paso más allá al permitir que el usuario cambie los supuestos básicos y observe el impacto del cambio en una posible exposición al riesgo: funcionalidad "qué pasaría si".	Evaluación de riesgos, respuesta a riesgos, información y comunicación	ORM
Cálculo de capital	Cambiar el cálculo de exposición a una atribución de capital basada en lineamientos regulatorios externos o, en el caso de capital económico, reglas internas de carga de capital; proporciona la capacidad de admitir diferentes definiciones de capital	Respuesta al riesgo, información y comunicación, seguimiento	ORM
RAROC análisis	Traducir el cálculo de capital en una evaluación de desempeño agregando otro cálculo que tenga en cuenta los ingresos asociados con una unidad comercial en particular y otros costos (distintos del capital)	Respuesta al riesgo, información y comunicación, seguimiento	ORM

CARACTERÍSTICA	DEFINICIÓN DE FUNCIONALIDAD	COMPONENTE COSO ERM	SOLUCIÓN
modelo VaR	Distribución de soporte y enfoque basado en escenarios	Evaluación de riesgos, respuesta a riesgos, información y comunicación, seguimiento	ERM
Informes internos	Mostrar los resultados de diversas evaluaciones y análisis a la línea y la alta dirección; proporcionar flexibilidad para abordar futuros requisitos de informes aún por definir; los informes generalmente se distribuyen a través de la web o el correo electrónico y se generan en varias formas, incluidos los generadores de informes estándar, los informes filtrados, las búsquedas, los tableros y la integración con herramientas de informes de terceros.	Ambiente interno, información y comunicación, seguimiento	ERA, ERM y ORM
Reportes regulatorios	Genere informes de riesgo predefinidos para las entidades reguladoras, los inversores y la junta	Entorno interno, información y comunicación, seguimiento	ORM
Respuesta a los riesgos	Capture estrategias de mitigación de riesgos y apoye el análisis de brechas utilizando marcos relevantes	Respuesta a los riesgos	ERM
Plantillas de cumplimiento	Proporcione plantillas de soporte para otras actividades de gestión de cumplimiento, como el cumplimiento de Sarbanes-Oxley	Varios	ERM
Planificación de auditoría	Apoyar la evaluación anual de riesgos y el desarrollo del plan de auditoría.	Evaluación de riesgos, seguimiento	IA
Gestión de proyectos	Implementar capacidades de gestión de casos y administración de proyectos únicas para la planificación y ejecución de auditorías internas	Supervisión	IA

Los criterios anteriores brindan una perspectiva sobre la funcionalidad que se debe buscar al evaluar las alternativas de software. Como se señaló anteriormente, los requisitos de la empresa y el enfoque de ERM seleccionado suelen impulsar la prioridad relativa de las especificaciones funcionales.

117. ¿Es preferible el software ERM especializado a las plataformas más amplias para el cumplimiento, la gobernanza y la gestión de riesgos?

Sí, a corto plazo hasta que surja una solución total genuina. Esto es particularmente cierto para las soluciones de gestión de riesgos cuantitativos. Sin embargo, es probable que las soluciones de software que integran los esfuerzos de cumplimiento, gestión de riesgos y auditoría interna sean las más exitosas con el tiempo.

118. ¿Cómo respalda la funcionalidad del software los objetivos de ERM?

Centrámonos primero en la gestión de riesgos operativos (ORM) para las instituciones financieras porque ese es un nicho de mercado que los proveedores de software están abordando activamente debido a los requisitos del Acuerdo de Basilea II. Los objetivos de los esfuerzos de ORM se centran principalmente en dos áreas:

- (a) Minimizar las pérdidas debidas al riesgo operativo aumentando la visibilidad de las exposiciones y gestionando la eficiencia de los controles internos que mitigan estas exposiciones.
- (b) Proporcionar a la gerencia estimaciones de pérdidas potenciales para garantizar que haya suficiente capital disponible para proteger la estabilidad institucional y que se logre un rendimiento adecuado para justificar las pérdidas asumidas.

El primero de estos objetivos está habilitado por la funcionalidad de la solución que proporciona recopilación de datos de pérdidas, seguimiento y monitoreo de eventos, autoevaluación e informes de gestión. El segundo de estos objetivos es facilitado por claves

creación de indicadores de riesgo, estimación de frecuencia y severidad con base en técnicas históricas, externas o de modelado, análisis de escenarios y calculadoras de exposición y capital.

ERM se basa en la funcionalidad proporcionada por el software que facilita ORM. Los objetivos de ERM se centran principalmente en mejorar la toma de decisiones estratégicas mediante la evaluación de actividades que crean o destruyen valor empresarial. Este objetivo está habilitado por la funcionalidad de la solución que proporciona definición de riesgo, análisis de brechas de capacidades de gestión de riesgo, documentación de actividades de control, monitoreo a nivel de entidad, programación y notificación de flujo de trabajo, seguimiento de problemas de auditoría y riesgo, modelado de VaR, respuesta de riesgo e informes de gestión. Esta funcionalidad ampliada cumplirá con los requisitos de la mayoría de las empresas.

119. ¿Cuáles son las principales categorías y características de los proveedores de software ERM exitosos?

Hay cuatro categorías principales de proveedores de gestión de riesgos: expertos en gestión de riesgos, expertos en control de procesos, especialistas en software de riesgos y empresas de consultoría. A continuación se proporcionan algunas observaciones generales con respecto a cada una de estas categorías.

Los expertos en gestión de riesgos abordan el mercado desde sus puntos fuertes en el riesgo de mercado o de crédito. Su objetivo es continuar desarrollando sus plataformas de riesgo y brindar más apoyo a los clientes mediante la venta cruzada de funcionalidades adicionales para el riesgo operativo. Estos proveedores suelen ser fuertes en técnicas de modelado y simulación.

También entienden la teoría detrás de los productos financieros complejos y pueden discutir el riesgo de manera efectiva con los analistas cuantitativos empleados por los bancos en sus departamentos de gestión de riesgos.

Las empresas con experiencia en control o auditoría interna en el mercado también han agregado la gestión de riesgos a sus conjuntos de soluciones. Es posible que estos proveedores no tengan tanta experiencia en modelado de riesgos o finanzas cuantitativas como los proveedores de gestión de riesgos, pero saben cómo identificar posibles fallas en los procesos. Esta capacidad en procesos, riesgos y controles tiende a fortalecer a estos proveedores en las áreas de recolección y seguimiento de pérdidas, monitoreo de incidentes y autoevaluación.

Hay relativamente pocos proveedores en el mercado que vendan productos especializados creados únicamente para la gestión de riesgos, e incluso estos especialistas en software de riesgos ahora están intentando reposicionarse como proveedores de soluciones más amplias para el cumplimiento de SOA. Todas estas soluciones recibieron financiamiento de terceros para construir sus respectivos paquetes y, en la mayoría de los casos, este financiamiento provino de una institución financiera.

En general, si bien las empresas de consultoría pueden tener un punto de vista con respecto a la tecnología, es posible que en realidad no ofrezcan una solución de software al mercado. Por ejemplo, en el momento en que se imprimió esta publicación, las cuatro grandes empresas se desprendieron de sus intereses en soluciones tecnológicas patentadas debido a aparentes conflictos de intereses y ahora prefieren asociarse con uno o más proveedores de software para influir en el desarrollo continuo de sus productos.

Si bien hay muchas características que diferencian a los proveedores exitosos, hemos resumido las siguientes como particularmente importantes:

- Conocimiento profundo de la gestión de riesgos: la gestión de riesgos está indisolublemente unida a los procesos comerciales. Los proveedores que mejor entienden los procesos de una organización, incluida la forma en que se administran y los objetivos generales de la organización, están mejor equipados para desarrollar soluciones de software superiores. Las soluciones pueden integrarse dentro de la estructura y los procesos existentes de una organización con una interrupción mínima para el negocio.
- Habilidad para educar a prospectos y clientes: La gestión de riesgos sigue siendo más un arte que una ciencia y muchas veces se debe enseñar antes de que se pueda vender. Los proveedores que tienen una sólida cultura de liderazgo intelectual y evangelización están mejor posicionados para brindar soluciones que marcarán la diferencia.
- Capacidad de ejecución y soporte: las soluciones de gestión de riesgos no deben introducir más riesgos de los que ayudan a mitigar. Si algún proveedor no puede asegurar a sus clientes que proporcionará software de alta calidad y soporte posterior a la implementación, el producto no merece mayor consideración.

- Servicios profesionales: los sistemas de gestión de riesgos no se pueden implementar con éxito hasta que se comprenda correctamente el riesgo y se definan adecuadamente los procesos de negocio subyacentes. Los proveedores de software que tienen expertos internos en la materia o relaciones de alianza con firmas de consultoría tienen una clara ventaja en este sentido.
- Presencia global: las empresas más grandes necesitan el apoyo de proveedores globales. Si bien las empresas locales pueden ayudar a las empresas más pequeñas con sede en el país, solo aquellos proveedores que pueden admitir implementaciones globales merecen la consideración de las multinacionales.
- Dedicación al espacio de mercado: las empresas deben centrarse en proveedores comprometidos con grandes y continuos inversiones en el desarrollo de productos.

Otros indicadores clave incluyen la importancia de los ingresos por gestión de riesgos para la empresa, el tamaño general de la empresa, su capacidad para aprovechar las relaciones existentes para desarrollar tecnología, experiencia en riesgos operativos y financieros, y su participación en el mercado y cambios en la participación a lo largo del tiempo. El éxito a largo plazo depende principalmente de la extensión de las soluciones existentes a áreas más amplias de cumplimiento, gobernanza y gestión de riesgos. Si bien hay varios proveedores dignos de consideración, la administración debe tener en cuenta que tienen fortalezas y debilidades muy diferentes. La gerencia debe estar segura de que los requisitos a largo plazo de la empresa estarán respaldados por el desarrollo continuo del producto y la mejora de la solución seleccionada. Debido a que la mayoría de las soluciones no están totalmente desarrolladas, la gestión dependerá en gran medida de las futuras inversiones del proveedor de software.

Por lo tanto, la gerencia debe comprender los planes futuros y los lanzamientos de productos del proveedor.

**120. ¿Es mejor diseñar un proceso ERM primero y luego seleccionar el software ERM apropiado, o ¿viceversa?**

El software ERM debe apoyar el proceso y no al revés. La gerencia debe tener claras las metas y las definiciones. No creemos que sea una muy buena idea seleccionar un proveedor primero, solo para descubrir más tarde que sus fortalezas y capacidades no están alineadas correctamente con la metodología elegida por la gerencia. Por ejemplo, si la gerencia requiere un enfoque de cuadro de mando, entonces deben seleccionar una solución que realmente pueda automatizar un cuadro de mando. Los seis elementos de infraestructura presentados en la Pregunta 110 brindan un contexto para la necesidad de decidir el proceso antes de elegir el software.

**121. ¿Qué son los informes de panel o cuadro de mando y cómo se utilizan en un entorno de ERM?**

Los modelos, el análisis de riesgos y las tecnologías habilitadas para la web hacen posible agregar información sobre los riesgos utilizando elementos de datos comunes para respaldar la creación de un tablero o cuadro de mando de gestión de riesgos para uso de los propietarios de riesgos, los gerentes de unidad y la gerencia ejecutiva. Los informes de tablero y cuadro de mando son lo suficientemente flexibles como para permitir el diseño de informes para abordar necesidades específicas. En las Técnicas de aplicación de COSO se proporcionan ejemplos de informes de tablero, que a menudo presentan "mapas de calor" o indicadores de "semáforo". marco ERM.

Los informes del tablero respaldan la gestión de riesgos en toda la empresa al proporcionar un marco para identificar, capturar y organizar elementos de datos de riesgo de fuentes externas e internas que están fácilmente disponibles para los propietarios de riesgos. El tablero alberga marcos, plantillas, herramientas e informes habilitados para ayudar a los gerentes de toda la organización a administrar el riesgo de manera consistente y uniforme para que la organización "aprenda una vez" en lugar de "reinventar la rueda" varias veces. Aumenta la eficacia y el valor que aportan las unidades de aseguramiento (consulte la Pregunta 56), brindándoles acceso a un almacén de datos y un "registro de riesgos" repleto de conocimientos e información sobre gestión de riesgos.

Una función de un tablero es agregar datos e información sobre riesgos que son difíciles de cuantificar. Un panel proporciona un depósito de puntos de datos e información sobre cada unidad de negocio, unidad de riesgo y unidad de soporte, incluidos sus respectivos procesos, riesgos, capacidades de gestión de riesgos, controles internos, casi accidentes y eventos de pérdida. Si bien no reemplaza a otros sistemas que brindan a los gerentes de unidad y propietarios de riesgos los números y análisis concretos que necesitan para administrar y controlar el riesgo frente a los límites establecidos, el tablero puede incorporar fuentes de esos sistemas. Para ilustrar, el tablero proporciona, entre otras cosas:

- Un lenguaje común para organizar la información de gestión de riesgos: Un lenguaje común organiza información y datos sobre riesgos, fuentes de riesgo, métricas de riesgo y capacidades de gestión de riesgo para extracción, análisis e informes a nivel de empresa, unidad y proceso.
- Un mecanismo de retroalimentación oportuno: Es útil generar retroalimentación periódica sobre riesgos, gestión de riesgos capacidades, incidentes de riesgo, eventos de pérdida y otros asuntos relevantes a través de metodologías de sondeo que involucrar a los gerentes de unidad, los propietarios de procesos y actividades y los propietarios de riesgos en toda la empresa. Estos Los ejercicios de sondeo son útiles para calificar la gravedad y la probabilidad de los riesgos y para priorizar las brechas. en torno a la gestión de los riesgos prioritarios, de modo que los propietarios de riesgos apropiados puedan ser asignados de manera oportuna y las capacidades de gestión de riesgos pueden mejorarse en las áreas apropiadas. También son útiles cuando perspectivas contrastantes en los diferentes niveles de la organización.
- Un depósito de datos: las plantillas proporcionan los medios para que los administradores y propietarios de riesgos documenten los datos de riesgo en los niveles de organización, unidad operativa, proceso y subproceso utilizando marcos predeterminados, y proporcionar los medios para que los administradores y propietarios de riesgos mantengan esos datos actualizados. Incluyen:
  - Clasificaciones de riesgo, tolerancias al riesgo y riesgo residual
  - Autoevaluaciones de la eficacia de las capacidades de gestión de riesgos y los controles internos críticos
  - Respuestas a los riesgos y actividades de control para abordar los riesgos prioritarios
  - Brechas en las capacidades y el desempeño de la gestión de riesgos
- Informes sobre el estado de las iniciativas: este informe estimula la mejora continua de la gestión de riesgos capacidades y aumenta la visibilidad e inculca la disciplina en toda la organización para ver implementación de las mejoras planificadas hasta su finalización.

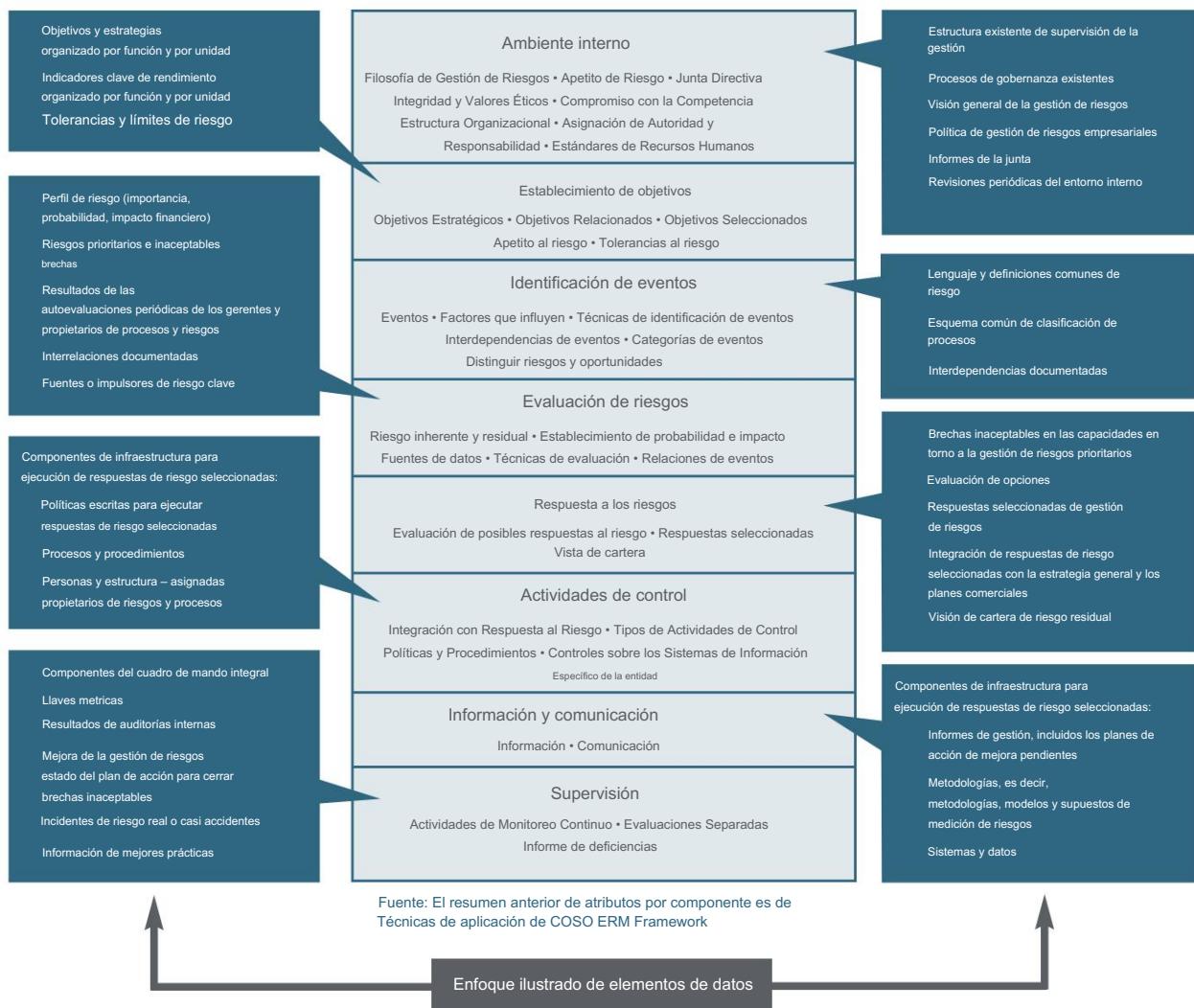
Hay muchas formas en que la administración puede usar el tablero en una organización. Los siguientes son ilustrativos ejemplos:

- La gerencia ejecutiva y de unidad puede usar el tablero para (a) facilitar y mejorar la comunicación de riesgos, supervisión, cumplimiento y seguimiento y (b) alinear la gestión de riesgos con el logro de los objetivos comerciales, objetivos, estrategias relacionadas y métricas clave de rendimiento.
- Los propietarios de riesgos y procesos en toda la organización pueden ingresar datos sobre riesgos, respuestas a riesgos y controles internos y obtenga información sobre el desempeño de la gestión de riesgos y las mejores prácticas.
- Una función central de gestión de riesgos comerciales, una unidad de aseguramiento o una unidad de riesgo (consulte la pregunta 56) puede:
  - Resumen de información utilizando elementos de datos comunes que respaldan el "informe de cuadro de mando" de la el perfil de riesgo de la organización y el desempeño de la gestión de riesgos en los niveles apropiados de la empresa y almacenar aquellos elementos de datos que vinculan unidades operativas, divisiones, procesos y funciones.
  - Usar herramientas de análisis de datos y soporte de decisiones para extraer y analizar datos para identificar tendencias que justifiquen atención, crear información relevante y desarrollar una mirada de informes diferentes para la gestión y el tablero.
  - Resumir la información relevante sobre una empresa, una unidad de negocio, una ubicación geográfica y un producto. base para permitir que los tomadores de decisiones evalúen tendencias mensuales, semanales, diarias o incluso en tiempo real (en aquellos raras circunstancias en las que esta capacidad está garantizada).
  - Desarrollar evaluación comparativa interna y externa, intercambio de conocimientos, técnicas de alerta temprana, escenario evaluación, agregación de riesgos y otras aplicaciones.
  - Ayudar a la alta dirección a respaldar una afirmación de que está cumpliendo con COSO ERM u otros marcos establecidos (p. ej., marco de control interno COSO, Turnbull, Normas de Australia, KonTrag, etc.).
  - Captar las oportunidades de mejora identificadas por la gestión, los propietarios de procesos y riesgos y los auditar y facilitar la identificación de las mejores prácticas para compartir en toda la organización. Apoyo seguimiento del estado de los elementos de acción abiertos para garantizar la ejecución de los planes de acción de mejora.

Los sistemas de información que respaldan la gestión de riesgos deben ser escalables para que puedan mejorarse con el tiempo. A medida que las necesidades de la organización cambian y las mejoras de software están disponibles (consulte las Preguntas 114 a 120 para la discusión de alternativas de software y temas relacionados). La gerencia también necesita asegurarse de que las fuentes de datos e información son confiables y oportunas. A medida que evoluciona como una herramienta de información, seguimiento y referencia, el "panel de administración de riesgos comerciales" crea valor para la organización que sus competidores no pueden replicar fácilmente.

Muchos tipos de datos son relevantes para las necesidades de información de la dirección ejecutiva y los gestores de riesgos, incluyendo datos históricos, datos de transacciones, datos posicionales y datos calculados. Ejemplos de elementos de datos que apoyan las actividades del proceso de gestión de riesgos y estandarizar terminología, definiciones y medidas se presentan a continuación utilizando los ocho componentes del marco COSO ERM:

## ELEMENTOS CLAVE DE CADA COMPONENTE COSO



Implementado junto con sistemas y herramientas de gestión de riesgos basados en la web, paneles de control de gestión de riesgos facilitar el aprendizaje de la organización y estimular la mejora continua de las capacidades de gestión de riesgos mediante el almacenamiento de elementos de datos relevantes que proporcionan un enlace común entre las unidades de negocio de la entidad, el riesgo unidades y unidades de apoyo (ver Pregunta 56 para una discusión de estos términos). Si los propietarios de riesgos y procesos en todo la organización introduce datos en el almacén de datos sobre sus procesos, riesgos, capacidades de gestión de riesgos

y controles internos, la base de datos se puede utilizar para extraer información sobre los riesgos de la empresa y las respuestas a los riesgos y proporcionar los informes de riesgo solicitados por los responsables de la toma de decisiones. Idealmente, estos sistemas deberían basarse o integrarse con el proceso de divulgación establecido para respaldar el cumplimiento de las disposiciones de informes públicos de Sarbanes-Oxley.

122. Para las empresas de servicios financieros, ¿es la medición del capital económico un requisito previo para la adopción de ERM?

No, la medición del capital económico no es un requisito previo para la adopción de ERM. Sin embargo, la medición del capital económico es una herramienta poderosa que permite a las empresas de servicios financieros (a) obtener una medida consistente y comparable de la exposición a través de los diversos tipos de riesgo asumidos y (b) aprovechar al máximo los beneficios de un programa integrado de gestión de riesgos.

El "capital económico" se define como la cantidad de capital que es suficiente para proteger adecuadamente a los accionistas contra el incumplimiento de todos los eventos, excepto de pérdidas extremas. El cálculo se basa en un análisis de todos los riesgos a los que está expuesta la empresa. Las metodologías de medición del capital económico van desde simples modelos de factores estandarizados hasta modelos estadísticos altamente sofisticados.

Para las empresas de servicios financieros, la asunción de riesgos es su propuesta empresarial central: asumir el riesgo crediticio, el riesgo de mercado, el riesgo de liquidez y el riesgo operativo al proporcionar servicios y productos financieros como préstamos, depósitos, inversiones y seguros. El capital económico proporciona una "moneda común" para todos los tipos de riesgo. Con capital económico, las empresas de servicios financieros pueden calcular las ventajas y desventajas de riesgo-recompensa entre alternativas estratégicas, poner precio a sus productos para compensar adecuadamente los riesgos asumidos y establecer estándares de retorno para guiar las decisiones de invertir en nuevos negocios, servicios y productos.

Se espera que la importancia del capital económico y su papel en ERM aumenten con la reciente adopción del Acuerdo de Basilea II por parte del Comité de Supervisión Bancaria de Basilea, un consorcio internacional de reguladores bancarios. Más de 100 países han aceptado las disposiciones de este acuerdo, que exige una variedad de metodologías de medición del capital económico, así como prácticas de gestión de riesgos consistentes con los preceptos de ERM. A pesar de que los reguladores bancarios de EE. UU. exigen que solo las organizaciones bancarias más grandes adopten el Acuerdo (restringiendo el cumplimiento solo a los requisitos más sofisticados del Acuerdo), existe un reconocimiento común entre la industria de servicios financieros más amplia de que el Acuerdo representa la "mejor práctica" para gestión de riesgos. Basilea II también se aplicará a algunas grandes empresas de banca de inversión.

123. ¿Cómo se aplica la mejora continua a la gestión de riesgos?

Debido a que la mejora continua se aplica a la gestión de riesgos tal como se aplica a cualquier otro proceso, la ERM debe verse como un enfoque sistemático para desarrollar y mejorar las capacidades de gestión de riesgos.

La mejora continua es vital para una gestión de riesgos exitosa porque los hechos y las circunstancias cambian constantemente con el tiempo, lo que significa que se puede esperar que los riesgos y las suposiciones de la gerencia sobre el entorno cambien con el tiempo. La pregunta es, ¿cómo se aplica la mejora continua a la gestión de riesgos?

La gerencia puede esperar que el proceso de monitoreo identifique oportunidades para mejorar las capacidades de gestión de riesgos. Sin embargo, existen otras formas en las que se estimula la mejora continua de las capacidades.

A continuación se muestran varios ejemplos:

Un proceso de mejora continua respaldado por políticas, metodologías y herramientas claramente establecidas y enfatizado constantemente en toda la organización es un catalizador eficaz para mejorar TODOS los procesos, incluidos los procesos de gestión de riesgos. Una vez que la organización ha determinado las capacidades deseadas para administrar un riesgo determinado o un grupo de riesgos relacionados y ha implementado con éxito esas capacidades, debe estar siempre atenta a mejorárlas continuamente a medida que cambian los hechos y las circunstancias y el riesgo de que ocurran eventos externos e internos significativos en el futuro evoluciona. Una "organización de aprendizaje" nunca puede darse el lujo de descansar en el mercado global dinámico.

Un proceso de evaluación de riesgos empresariales y un análisis de brechas facilita la identificación de los riesgos prioritarios y destaca las brechas inaceptables en las capacidades en torno a la gestión de los riesgos prioritarios. Estas actividades conducen a

respuestas de riesgo enfocadas que impulsan la mejora en las políticas de gestión de riesgos, procesos, competencias, informes y tecnología. Ver discusión adicional en la Pregunta 85.

Benchmarking compara las capacidades de gestión de riesgos dentro de las unidades de negocio, unidades de riesgo, unidades de apoyo y unidades de aseguramiento (consulte la pregunta 56 para obtener una explicación de estos términos) a las capacidades de los pares o "lo mejor de intérpretes de clase". Cuanto mejor definidas sean las capacidades de una organización, más probable es que se establezca un proceso de evaluación comparativa eficaz. Es especialmente eficaz cuando el directorio y la gerencia ejecutiva establecen o aprueba las prioridades de benchmarking y es informado de los resultados del proceso. Datos de evaluación comparativa también puede ser un catalizador para el cambio cuando se comunica a los propietarios de procesos y riesgos apropiados.

Las comunicaciones de cuatro vías y el intercambio de conocimientos consisten en los procesos y tecnologías de apoyo por en el que hay una transferencia e intercambio continuo de información sobre riesgos y capacidades de gestión de riesgos arriba, abajo y en toda la empresa. Facilitado por la dirección ejecutiva, este intercambio de información de cuatro vías proporciona información sobre la existencia, la naturaleza, la importancia, la probabilidad, la aceptabilidad y la capacidad de gestión del riesgo como así como las respuestas al riesgo de la organización, metodologías de medición, actividades de control y seguimiento procesos. Este intercambio continuo facilita compartir las mejores prácticas e identifica las condiciones que deben ser actuado. Es un poderoso catalizador para estimular la mejora continua.

El aprendizaje de los empleados ayuda a los gerentes de toda la empresa a generar conciencia y lograr la aceptación. y propiedad de la visión, las metas, los objetivos, las políticas y los procesos de gestión de riesgos de la empresa. Empleado El aprendizaje debe enfatizar las siguientes áreas:

- La visión, las metas, los objetivos y las políticas de gestión de riesgos de la empresa
- El lenguaje común de la empresa y otros marcos propios
- Los procesos de la empresa para identificar y buscar riesgos y los métodos y herramientas que respaldan esos procesos, incluyendo cómo esos procesos se comparan con COSO Enterprise Risk Management – Marco Integrado
- Los procesos de autoevaluación implementados y cómo se integran con las actividades comerciales diarias
- Las metodologías de medición de riesgos seleccionadas por la empresa y cómo se utilizan
- Los riesgos prioritarios de la organización y el proceso de evaluación de riesgos de toda la empresa para mantener el riesgo perfil actualizado
- Los elementos de la infraestructura ERM y su importancia y contribución en la construcción y mejora capacidades de gestión de riesgos
- El proceso mediante el cual se determinan las brechas en las capacidades de gestión de riesgos
- Participación en los canales de comunicación establecidos para permitir el flujo de información sobre gestión de riesgos dentro de la empresa
- El compromiso de la empresa con la mejora continua y lo que significa para la gestión de riesgos, para la unidades operativas de la empresa y al empleado individual

Los programas de educación y aprendizaje deben diseñarse para abordar los puntos anteriores y entregarse a personal apropiado.

El seguimiento de la implementación de las mejoras sigue a la identificación y priorización de las mejoras oportunidades y desarrollo de planes de acción. Los esfuerzos de mejora se rastrean contra los establecidos horarios y puntos de control. Actividades de auditoría (por ejemplo, auditorías internas, actividades de cumplimiento de riesgos, auditorías externas o auditorías regulatorias) pueden proporcionar garantías de que las mejoras se están realizando de manera oportuna. De todos modos, eso Corresponde a la dirección tomar la iniciativa para actuar sobre los resultados de las actividades de mejora continua, mantener la personal responsable responsable del seguimiento y control de las acciones realizadas.

124. ¿Cuáles son las sinergias y diferencias entre ERM y las "iniciativas de calidad" (p. ej., Six Sigma, Lean, TQM, etc.)?

ERM es un proceso de nivel empresarial que es parte integral del establecimiento de estrategias. Las iniciativas de calidad, por otro lado, brindan la metodología y las herramientas para ayudar a las organizaciones a comprender, medir y mejorar continuamente la eficiencia y la calidad de sus procesos a un nivel detallado. Por ejemplo, el enfoque Six Sigma se basa en las siguientes actividades: Definir, Medir, Analizar, Mejorar y Controlar. Estas actividades respaldan y brindan información en un proceso de ERM. Proporcionan información detallada a nivel de proceso que luego debe evaluarse dentro del contexto más amplio de la empresa para desarrollar una vista de cartera de riesgos y controles. ERM, por otro lado, debe aplicarse en el establecimiento de estrategias, o de lo contrario su aplicación se vuelve demasiado detallada y engorrosa.

Las iniciativas de calidad pueden verse como metodologías, técnicas y herramientas para su aplicación en un nivel de proceso detallado para abordar objetivos de procesos específicos. La operación de un programa de calidad es una "actividad de control" (uno de los componentes de COSO Enterprise Risk Management – Marco Integrado) con indicadores medibles de desempeño.

Por ejemplo, el proceso Six Sigma puede aumentar de manera efectiva la implementación de ERM de varias maneras:

- Los recursos de Six Sigma pueden ser valiosos para ayudar al equipo de implementación de ERM a comprender el entorno operativo actual. El uso de esquemas de clasificación de procesos para descomponer el negocio, la identificación de procesos comerciales clave, el abastecimiento de impulsores de valor y otros pasos son integrales para comprender el componente de entorno interno de ERM.
- Los marcos y conjuntos de habilidades de Six Sigma pueden ser especialmente útiles para comprender los riesgos que son de naturaleza operativa, incluido el desarrollo de un análisis de brechas de estado actual y futuro. Esto puede complementar o reemplazar ciertos marcos de ERM, como los seis elementos del modelo de madurez de infraestructura y capacidad.
- Los recursos de Six Sigma pueden servir como referencia para comprender las interrelaciones entre los riesgos, por ejemplo, factores de riesgo independientes, así como factores de riesgo dependientes de otros factores de riesgo.
- Un área en la que Six Sigma puede proporcionar un valor significativo es en la planificación y el análisis de la respuesta al riesgo, por ejemplo, la identificación de los responsables del riesgo, el origen de los riesgos dentro de los procesos comerciales clave, la recopilación de un inventario del "estado actual" y el análisis de las brechas del "estado futuro".
- Six Sigma pone énfasis en la identificación de indicadores de desempeño a nivel de proceso; estos indicadores deben traducirse en indicadores de riesgo clave para comprender las exposiciones a la variabilidad del rendimiento y los posibles impulsores de pérdidas.

También existen desafíos al integrar Six Sigma y ERM. El enfoque de Six Sigma tiende a ser impulsado por una perspectiva operativa, lo que a veces lleva a los defensores de Six Sigma a perder el vínculo del "panorama general" con la estrategia. Además, es importante mantener la objetividad y la imparcialidad durante el proceso de evaluación de riesgos. El equipo de gestión debe priorizar el riesgo con los equipos de Six Sigma y ERM proporcionando la información adecuada sin dirigir la dirección de las clasificaciones de riesgo en una dirección particular. Otro tema es el de la percepción. Si la gerencia ve al personal de Six Sigma involucrado en el proceso de evaluación de riesgos, puede enviar mensajes contradictorios. Una evaluación de riesgos empresariales no debe verse como un ejercicio para impulsar una revisión de los procesos comerciales y los controles relacionados. Una evaluación de riesgos empresariales debe centrarse en cuestiones estratégicas, con énfasis en los procesos impulsados por el análisis de brechas en torno a los riesgos prioritarios.

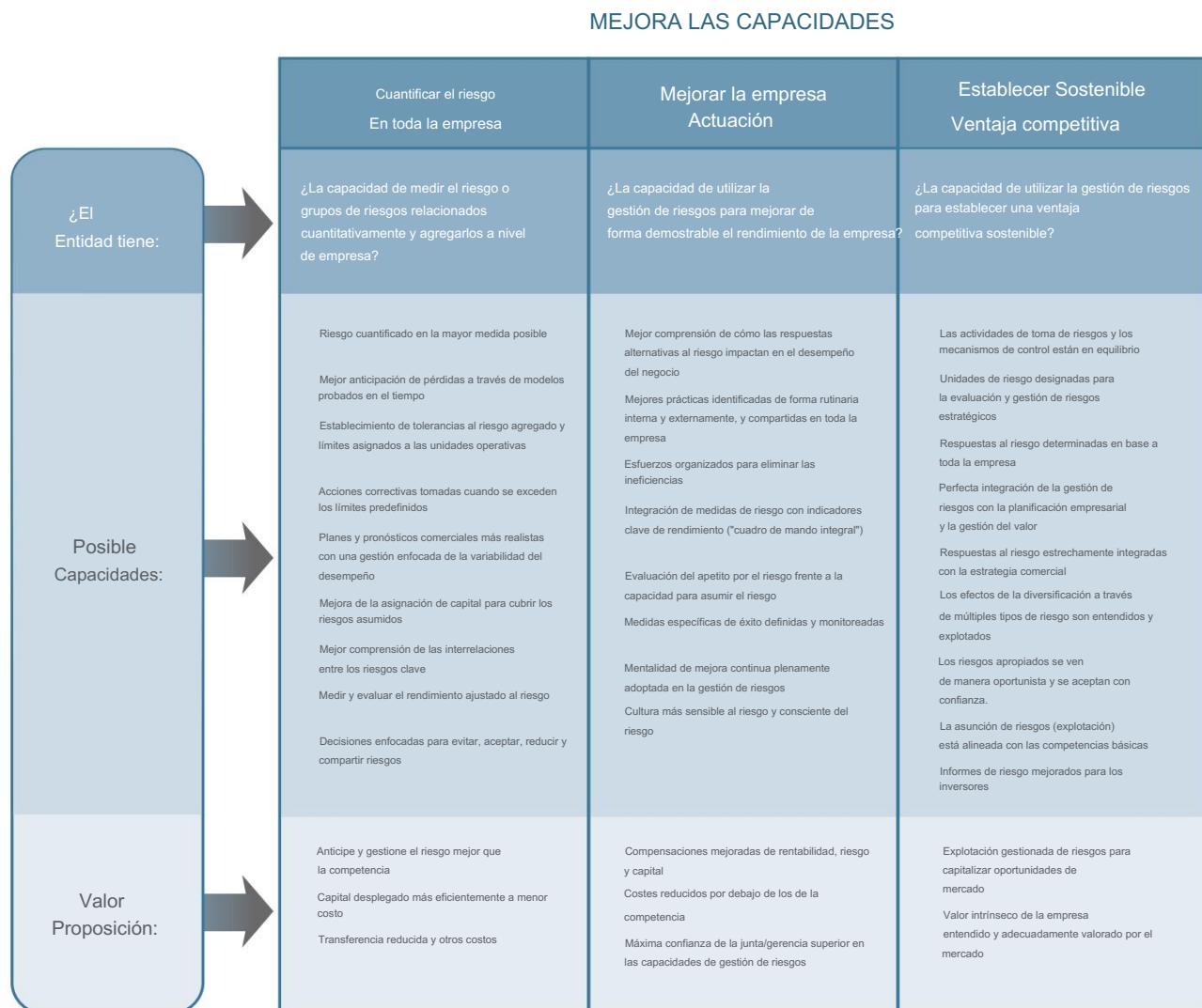
## LLEVÁNDOLO AL SIGUIENTE NIVEL: MEJORANDO LAS CAPACIDADES

### 125. ¿Qué pasos toma la administración para mejorar las capacidades de gestión de riesgos?

Una vez que las empresas han implementado capacidades de gestión de riesgos que están bien definidas y se aplican de manera consistente en toda la empresa, están posicionadas para mejorar el proceso para abordar las necesidades específicas del negocio. Los pasos necesarios para mejorar las capacidades de gestión de riesgos se aplican a aquellos riesgos prioritarios para los cuales la administración ha decidido alcanzar un estado de capacidad "gestionado" u "optimizado" utilizando el modelo de madurez de la capacidad (consulte la Pregunta 111).

Hay tres pasos a seguir cuando se mejoran las capacidades de gestión de riesgos. Estos pasos son cuantificar el riesgo en toda la empresa, mejorar el rendimiento de la empresa y establecer una ventaja competitiva sostenible. Estos pasos pueden tomarse simultáneamente. Representando la vanguardia, estos pasos concluyen la progresión hacia una solución ERM. Los posibles elementos a considerar al mejorar las capacidades brindan información sobre la dirección final del viaje de ERM.

A continuación, se incluye un resumen de ejemplos de posibles elementos a considerar al mejorar las capacidades de gestión de riesgos:



Los ejemplos antes mencionados de capacidades mejoradas de gestión de riesgos pretenden ser ilustrativos y no incluyentes. No es necesario seleccionar todos los elementos sugeridos en esta publicación para mejorar las capacidades de gestión de riesgos al diseñar una solución ERM.

126. ¿Cómo decide la administración sobre las capacidades de mejora apropiadas?

Con respecto a la mejora de las capacidades de gestión de riesgos, es una cuestión de criterio, cultura, estilo operativo, necesidades organizativas, la capacidad deseada por la dirección para gestionar riesgos específicos y la naturaleza del riesgo.

Lo que funciona para una organización no necesariamente funcionará para otra organización. Un factor importante a considerar se relaciona con las expectativas de la comunidad inversora y del mercado. Ya se trate de inversionistas institucionales, agencias calificadoras, autoridades reguladoras o el estándar establecido por los competidores, la administración debe tener en cuenta estas expectativas en sus decisiones con respecto al nivel apropiado de inversión en capacidades mejoradas de administración de riesgos. En esencia, las capacidades mejoradas están destinadas a satisfacer las expectativas y demandas del mercado.

127. ¿Qué es una “visión de cartera” de riesgos y cómo se aplica en la práctica?

Tomar una visión de cartera a nivel de entidad del riesgo al formular respuestas de riesgo es la esencia de un enfoque de toda la empresa. Según COSO:

Los riesgos en diferentes unidades pueden estar dentro de las tolerancias al riesgo de las unidades individuales, pero, tomados en conjunto, los riesgos pueden exceder el apetito de riesgo de la entidad como un todo, en cuyo caso se necesita una respuesta de riesgo adicional o diferente para traer el riesgo dentro de la entidad. Apetito por el riesgo. Por el contrario, los riesgos pueden compensarse naturalmente en toda la entidad donde, por ejemplo, algunas unidades individuales tienen un mayor riesgo mientras que otras son relativamente adversas al riesgo, de modo que el riesgo general está dentro del apetito por el riesgo de la entidad, obviando la necesidad de un riesgo diferente. respuesta.

Una vista de cartera tiene sentido para las actividades dirigidas a lograr un propósito común en toda la empresa. Hay varias razones para ello:

- Los riesgos se suman ya sea que se evalúen por partes o en total: si los riesgos se agregan, los gerentes están posicionados para comprender si aumentan o disminuyen a medida que cambian las condiciones, tanto entre sí como en conjunto frente al apetito de riesgo de la organización. Si bien la agregación puede presentar desafíos desde un punto de vista técnico, se obtiene muy poca perspectiva al examinar los efectos brutos frente a los netos, o exposiciones más pequeñas de forma aislada. Una vista de cartera es poderosa porque puede alterar el enfoque de la administración y la asignación de recursos. Por ejemplo, permite a la organización acelerar su tiempo de respuesta al abordar oportunidades favorables o cambios adversos en el entorno. Actuar sobre una vista de cartera a nivel empresarial le da a la gerencia un mayor apalancamiento, costos operativos o de transacción más bajos y la capacidad de agilizar y optimizar las operaciones, así como planificar respuestas de riesgo contingentes.
- Mayor eficiencia y mejores decisiones: una vista de cartera proporciona los medios cuantitativos para compartir y evitar el riesgo. Compartir el riesgo, por ejemplo, es más eficiente cuando los riesgos se compensan o compensan. Por ejemplo, las exposiciones cambiarias se pueden agrupar para determinar la exposición “neta” de la empresa, cuando esa práctica se corresponde con las operaciones de la organización. Cuando las exposiciones se agrupan, forman una cartera que representa con mayor precisión las realidades del negocio. El objetivo, en última instancia, es evaluar los rendimientos totales en relación con los riesgos totales que conducen a decisiones más informadas. Este “enfoque de riesgo total” lleva a una mayor confianza en que la gerencia está tomando decisiones basadas en una visión integral del negocio.
- Informes y asignación de capital mejorados: análisis que se realizan para identificar las relaciones entre los riesgos y sus impulsos clave para que los riesgos puedan agregarse conducen a informes de riesgos más sólidos. Ayudan a los gerentes a tomar mejores decisiones cuando asignan capital a aquellas actividades comerciales que brindan las mayores perspectivas de rendimientos atractivos en relación con todos los riesgos asumidos y rechazan aquellas actividades que no lo hacen. La alternativa son las conjecturas ineficaces e intuitivas, que no llegarán muy lejos dadas las complejas interrelaciones entre los riesgos y las variables clave que los afectan.

- Simplicidad: si los ejecutivos pueden comunicar de manera efectiva el perfil de riesgo y la salud de la organización, tienen un dispositivo que todos pueden entender y aplicar. Una vista de cartera es una forma de resumir un conjunto complejo de relaciones, es decir, las actividades de la empresa. Cuanto mayor sea la capacidad de expresar en términos simples el estado de cosas de la organización, mayor será la capacidad de gestionar eficazmente su curso en un mercado cada vez más competitivo.

Lograr una vista de cartera no es fácil. Algunos riesgos son más susceptibles de una medición rigurosa que otros.

COSO señala que se puede obtener una vista de cartera centrándose en los principales riesgos o categorías de eventos en las unidades operativas o en el riesgo para la empresa en su conjunto utilizando métricas como capital ajustado al riesgo o capital en riesgo. COSO explica que tales "medidas compuestas son particularmente útiles cuando se mide el riesgo frente a los objetivos establecidos en términos de ganancias, crecimiento u otras medidas de desempeño, a veces en relación con el capital asignado o disponible". COSO sugiere que tales métricas pueden proporcionar información útil para reasignar capital entre unidades de negocios y modificar la dirección estratégica. Para ilustrar, COSO proporciona el siguiente ejemplo:

[Una] empresa manufacturera... adopta una visión de cartera del riesgo en el contexto de su objetivo de ganancias operativas. La gerencia usa categorías de eventos comunes para capturar los riesgos en todas sus unidades de negocios. Luego desarrolla un gráfico que muestra, por categoría y unidad de negocio, la probabilidad de riesgo en términos de frecuencia en un horizonte de tiempo y los impactos relativos en las ganancias. El resultado es una vista compuesta, o de cartera, del riesgo que enfrenta la empresa, con la gerencia y el directorio posicionados para considerar la naturaleza, la probabilidad y el tamaño relativo de los riesgos, y cómo pueden afectar las ganancias de la empresa.

COSO proporcionó un segundo ejemplo en el marco:

[Una] institución financiera pide a las unidades de negocio que establezcan objetivos, tolerancias al riesgo y medidas de desempeño, todo en términos de rendimiento del capital ajustado al riesgo. Esta métrica aplicada de manera consistente facilita que la gerencia despliegue [las] evaluaciones de riesgo combinadas de las unidades en una vista de cartera para la institución en su conjunto, lo que permite a la gerencia considerar los riesgos de las unidades, por objetivo, y considerar si la entidad está dentro de su apetito por el riesgo.

Además, se hace referencia a las páginas 60 a 62 de Técnicas de aplicación para ejemplos adicionales proporcionados por COSO. Una de las ventajas importantes de una vista de cartera es la capacidad de considerar si el riesgo está dentro del apetito de riesgo de la entidad. Una vista de cartera permite a la gerencia reevaluar la naturaleza y el tipo de riesgos que desea y está dispuesto a asumir. En los casos en que la entidad muestre riesgos significativamente menores que el apetito de riesgo de la entidad, la gerencia puede decidir incentivar a los gerentes de unidades de negocios individuales para que acepten mayores riesgos en áreas específicas, esforzándose por mejorar el crecimiento y el rendimiento general de la empresa.

#### 128. ¿Cómo cuantifica la administración los riesgos en toda la empresa?

La agregación de múltiples riesgos no es el resultado final, sino el medio para un fin deseado. Desde una perspectiva empresarial, el "fin deseado" son respuestas de riesgo efectivas en toda la empresa integradas con la estrategia comercial que conducen a un mejor desempeño. Al evaluar si la realización de este objetivo justifica el esfuerzo de recopilar y analizar información sobre riesgos, la gerencia debe hacerse la pregunta: "¿A qué nivel se agregan los riesgos con fines de cuantificación?"

Elegir el nivel correcto de agregación para un riesgo o grupo de riesgos relacionados a menudo depende de quién usará la medida. Por ejemplo, los empleados de nivel operativo, como comerciantes, gerentes de control de inventario o gerentes de marketing, necesitan información muy específica para ejecutar sus trabajos. Al adoptar una visión de toda la empresa de múltiples riesgos interrelacionados, los objetivos de la organización deben definirse en términos de una medida agregada para el grupo de riesgos relacionados. Cuando la medida agregada se determina utilizando una metodología de medición robusta, es posible impulsar la toma de decisiones y gestionar el grupo de riesgos a nivel de toda la entidad que afecta aspectos tales como incentivos de desempeño, cooperación entre unidades, trabajo en equipo interdisciplinario y intercambio de conocimientos en toda la empresa.

Otro factor clave que influye en la decisión de agregar múltiples riesgos es que solo tiene sentido agregar cuando los componentes incluidos en la medida están dirigidos hacia el mismo objetivo común. Si la política operativa de una organización es administrar unidades operativas autónomas, cada una de las cuales es un centro de ganancias independiente, entonces puede ser inapropiado desarrollar una medida agregada para los riesgos comunes dentro de estas unidades. En

tales circunstancias, la gerencia ha optado por no implementar respuestas de riesgo en todas las unidades operativas; por lo tanto, tener medidas agregadas para riesgos clave en todas las unidades no tiene sentido en la mayoría de las circunstancias. Por otro lado, una sociedad de cartera bancaria con múltiples subsidiarias que operan como centros de utilidades separados puede desear agregar el riesgo crediticio, en toda la empresa, porque tiene sentido comercial hacerlo. En esencia, ERM se trata de (1) alinear los objetivos de toda la empresa y los incentivos de la unidad operativa y (2) delineando las tareas de gestión de riesgos que deben ejecutarse centralmente de las tareas que deben ejecutarse localmente. Con una alineación efectiva de objetivos e incentivos y una clara delimitación de responsabilidades, las medidas de riesgo agregado se implementan de manera más efectiva.

Hay varias formas de agregar múltiples medidas de riesgo usando una combinación de una metodología rigurosa y la aplicación del juicio. La navegación de la entidad en el viaje de ERM conducirá a otros enfoques.

- Enfoques de agrupación de riesgos: sugerimos la agregación de riesgos cuyas interrelaciones se entiendan bien dentro de familias lógicas o grupos. Usando este enfoque, la entidad primero determina las interrelaciones entre sus riesgos clave. Los riesgos están correlacionados positiva o negativamente cuando tienen factores de riesgo comunes. De lo contrario, no están correlacionados. Luego, la gerencia "agrupa" los diferentes riesgos para evaluar las alternativas para administrar los riesgos colectivos representados por el grupo. Los riesgos agrupados podrían gestionarse como una cartera. Alternativamente, podría usarse una cobertura basada en un índice agregado, como un índice amplio de acciones, bonos o materias primas (en lugar de, por ejemplo, cubrir los riesgos de los componentes individuales por separado). Si los riesgos son asegurables, sujetos a la disponibilidad y el precio de los productos de seguros, a menudo es más barato cubrir todo el grupo de riesgos que asegurar cada riesgo por separado. En el caso de que las exposiciones en la cartera no estén correlacionadas, el costo neto de transferirlas a una parte independiente, como cobertura o seguro, puede ser menor debido a los beneficios de la diversificación.
- Apetito de riesgo de toda la empresa y tolerancias de riesgo específicas: Los riesgos desenfrenados pueden resultar en variabilidad del rendimiento y exposición a pérdidas inaceptables. Un método para lograr consistencia en el desempeño es articular el apetito por el riesgo para la entidad como un todo, tal como lo prevé la definición de ERM de COSO. En efecto, el apetito por el riesgo aborda la pregunta: "¿Cuánta variabilidad estamos dispuestos a aceptar y cuántas pérdidas estamos dispuestos a absorber a medida que perseguimos nuestros objetivos comerciales generales y ejecutamos nuestras estrategias?" La orientación sobre esta pregunta es importante ya que ayuda a la gerencia a evaluar la exposición en términos del riesgo a la baja aceptable a medida que la empresa busca la ventaja inherente a la ejecución de la estrategia comercial. Si un director ejecutivo está dispuesto a apostar a la empresa en la búsqueda de una adquisición, ¿está dispuesta la junta a aceptar ese nivel de riesgo?

Si bien el apetito por el riesgo en toda la empresa es una evaluación estratégica, debe traducirse en políticas específicas para aclarar los límites dentro de los cuales los gerentes pueden operar y buscar oportunidades. También se puede usar como contexto para establecer tolerancias al riesgo y estructuras de límites para establecer los límites del riesgo aceptable que se puede asumir en unidades individuales y en conjunto con actividades específicas. A medida que los gerentes buscan oportunidades de crecimiento y nuevas fuentes de rentabilidad, las tolerancias y los límites de riesgo son una herramienta eficaz, en combinación con una metodología para agregar medidas de riesgo, para contrarrestar las presiones de "éxito a toda costa" sobre los gerentes para producir los resultados esperados. Las tolerancias y los límites de riesgo de toda la empresa deben ser lo suficientemente amplios para permitir la flexibilidad operativa, pero al mismo tiempo garantizar que el perfil de riesgo agregado de la empresa permanezca dentro del apetito de riesgo de la administración, según lo aprobado por la junta. Estas tolerancias y límites se pueden comunicar de muchas maneras. Por ejemplo, se pueden incorporar a la declaración de política de gestión de riesgos que se pone a disposición de todos los gerentes y empleados clave.

- Tasas mínimas: si bien ciertamente no es una idea nueva, las organizaciones a menudo establecen "tasas mínimas" para evaluar proyectos de capital cuando utilizan técnicas de flujo de caja descontado (DCF). Esta selección es un punto de partida para evaluar los méritos relativos de múltiples proyectos de capital de manera más sistemática. Brinda una mayor seguridad de que se puede esperar que cualquier proyecto seleccionado genere rendimientos al menos iguales, si no superiores, al costo de capital. Sin embargo, hay cuestiones a considerar.
  - La dependencia exclusiva y la aplicación rígida de modelos financieros pueden hacer que las entidades pasen por alto factores difíciles de cuantificar vitales para mantener la ventaja competitiva, como la innovación de productos, la calidad, la reputación y el liderazgo tecnológico.
  - No es raro que las empresas establezcan tasas mínimas arbitrarias muy por encima del costo del capital, lo que lleva a subinversión. Algunos argumentarían que un "buen" proyecto es aquel que proporciona un retorno mayor que el

costo de capital. Por otro lado, la proyección de los flujos de efectivo esperados no es una ciencia exacta, por lo que una tasa crítica más alta sube el listón. La pregunta, entonces, es ¿cuánto más alto? Es cierto que una barra alta elimina de la consideración los proyectos que la administración nunca aprobaría de todos modos. Pero también puede descartar proyectos viables que deberían ser considerados. Parte de la respuesta a este problema radica en la tolerancia al riesgo de la empresa. Cuanto menor sea la tolerancia al riesgo, mayor debe ser la tasa crítica sobre el costo de capital esperado. Después de incorporar su tolerancia al riesgo y el margen para el error de estimación, la gerencia debe tener cuidado al establecer la tasa crítica más alta, de lo contrario, puede resultar en una inversión insuficiente.

- Las tasas mínimas no deben usarse como una regla estricta y rápida en todos los proyectos. Si la administración tiene una única tasa crítica para toda la empresa, el modelo DCF no tendrá en cuenta los riesgos apropiados del proyecto. Si bien es cierto que es subjetivo y difícil de hacer, las tasas mínimas deben establecerse proyecto por proyecto o al menos por unidad de negocio o división para reflejar los diferentes perfiles de riesgo. Por ejemplo, en un negocio donde la estrategia principal es el crecimiento, los proyectos con valores presentes netos más bajos probablemente sean más aceptables que en un negocio con una estrategia de generación de efectivo. Las empresas aún deben asumir primero sus proyectos de capital más atractivos y reconocer que el costo de capital para proyectos posteriores, por ejemplo, proyectos de "mantenimiento" necesarios para sustentar la implementación de estrategias existentes, podría no ser el mismo que el costo de sus principales proyectos de inversión. .

Las tasas mínimas no son infalibles. No pueden permanecer fijos en el tiempo a medida que cambian las condiciones económicas. Además, las inversiones potencialmente marginales a menudo pueden parecer atractivas a medida que las unidades comerciales internas compiten por el capital.

- Marcos de riesgo: las metodologías de valor en riesgo (VaR), ganancias en riesgo (EaR), margen bruto en riesgo (GMaR) y flujo de caja en riesgo (CFaR) son cada vez más aceptadas por las empresas corporativas y los reguladores como herramientas para: facilitar la asignación de capital basada en el riesgo; medir el rendimiento teniendo en cuenta los riesgos inherentes a una cartera; y fortalecer los vínculos entre el desempeño, la rendición de cuentas y los umbrales de riesgo establecidos. Estas metodologías ayudan a los administradores a considerar los factores críticos al administrar el riesgo, por ejemplo, la sensibilidad de las posiciones de cartera existentes a los cambios en las tasas de mercado más allá de los límites especificados, la liquidez de una cartera, la contribución de cada unidad o producto tanto al riesgo como al rendimiento, y las interrelaciones entre riesgos. En total, estas técnicas ayudan a los gerentes a considerar la exposición de las ganancias o el flujo de efectivo a pérdidas y lograr el apalancamiento objetivo de la entidad y el rendimiento deseado sobre el capital asignado. También facilitan la formulación de orientaciones prospectivas.
- Medición del desempeño ajustado al riesgo: una vez que una organización ha cuantificado sus exposiciones, por ejemplo, mediante el uso de una técnica como VaR, ¿qué hace la administración con esta información? Uno de los usos más significativos de la información sobre riesgos es como factor para ajustar el valor relativo de las diferentes actividades comerciales. El rendimiento del capital ajustado al riesgo es una técnica que incorpora el riesgo de una actividad comercial, como una inversión, en la medición de los rendimientos esperados de esa actividad. Por lo tanto, una inversión más riesgosa (por ejemplo, una inversión en una planta de energía que opere en un país extranjero en desarrollo) tendría que generar un rendimiento mayor que una inversión menos riesgosa (por ejemplo, los bonos del Tesoro de EE. UU.) para ser considerada equivalente. El rendimiento del capital ajustado al riesgo, o RAROC, incorpora el costo de financiar este riesgo en la medición del desempeño. Le dice a la gerencia cuánto mayor debería ser el rendimiento, dado el nivel de riesgo. También proporciona información a la gerencia sobre si el capital asignado es adecuado para cubrir los riesgos asumidos.

Como con cualquier técnica, existen problemas con respecto a RAROC. Dado que no existe una forma correcta de calcular el riesgo esperado de un proyecto o de ajustar el riesgo, el número exacto que se obtenga dependerá del enfoque que se adopte en los cálculos. Usando RAROC, el riesgo se cuantifica con base en distribuciones de probabilidad de retornos observados en datos históricos, consistentes con VaR y otros modelos estadísticos. El resultado previsto es agregar el riesgo de precio y asignar capital en función de la variabilidad de los rendimientos esperados.

Por lo tanto, RAROC proporciona un medio para evaluar el rendimiento, el riesgo y las compensaciones de capital y comparar el desempeño entre diferentes unidades o actividades de la organización, que están sujetas a diferentes niveles de riesgo. RAROC también es una herramienta que puede ser útil para crear puntos de referencia para la organización. El poder de RAROC, por lo tanto, radica en la consistencia de la aplicación. Un enfoque RAROC ajusta los rendimientos del capital en riesgo en todas las clases de activos. Luego, los gerentes pueden usar esa información para establecer límites en el comercio, la inversión u otras actividades comerciales.

Esta discusión sobre la agregación de riesgos no pretende sugerir que las empresas deberían buscar el "santo grail" de medición del riesgo. Existen limitaciones prácticas para medir el riesgo porque el riesgo, por naturaleza, se trata de incertidumbre para afrontar el futuro. El propósito de las metodologías de agregación de riesgos es establecer un base para organizar la variedad de información que necesitan los gerentes cuando toman decisiones críticas. Por lo tanto, la El objetivo es proporcionar mejor información para la toma de decisiones a través de capacidades mejoradas de medición de riesgos. Estas capacidades mejoradas logran cuatro cosas:

- (1) Informes de riesgos más sólidos: los riesgos se agregan en múltiples niveles, por unidad de negocio, producto o geográfica (agregando múltiples tipos de riesgo), por riesgo (agregando el mismo riesgo en una empresa en todas las unidades de negocio) y por inversiones y proyectos específicos.
- (2) Mayor confianza de inversión: con capacidades mejoradas de medición de riesgos, la organización puede buscar oportunidades con mayor confianza sabiendo que comprende los riesgos inherentes a su operaciones futuras normales y que esos riesgos están siendo administrados de manera efectiva.
- (3) Mayor integración y alineación: dado que las medidas agregadas están efectivamente vinculadas a la empresa rendimiento, son posibles respuestas de riesgo más integradas.
- (4) Valoración más alta: todo esto le da a la gerencia una historia más convincente para comunicar a los inversores, lo que a su vez puede conducir a múltiplos de precio/beneficio más altos en las valoraciones de las acciones.

#### 129. ¿Cómo usa la administración ERM para mejorar el desempeño comercial?

La contribución más importante de ERM para mejorar el desempeño del negocio es ayudar a los gerentes a tomar mejores opciones para proteger y mejorar el valor de la empresa. Debido a que las empresas se enfrentan cada vez más futuro incierto, esta contribución puede hacer o deshacer la formulación y ejecución de un negocio exitoso estrategia. Las respuestas a los riesgos deben respaldar los objetivos de creación de valor de la organización mediante la gestión y monitorear la variabilidad del desempeño inherente a sus operaciones futuras, protegiendo la empresa acumulada valor de pérdidas inaceptables y aprovechar las competencias básicas existentes para buscar oportunidades de mercado.

Al administrar el valor empresarial, las organizaciones deben desarrollar una comprensión de las fuentes y los impulsores de valor utilizando los objetivos de negocio y la estrategia como contexto. Esta interpretación proporciona el contexto para la gestión del riesgo. A medida que los altos directivos centran su atención en las perspectivas a largo plazo de la empresa para generando rendimientos superiores, deben:

- (1) Evaluar las variables subyacentes clave en el plan de negocios que están expuestas a la variabilidad del desempeño y que requieren respuestas de riesgo específicas;
- (2) Comprender las exposiciones a pérdidas o los impulsores inherentes al modelo comercial de la empresa que requieren respuestas a riesgos específicos;
- (3) Identificar las incongruencias inherentes al modelo de negocios donde la administración tiene, ya sea a sabiendas o sin saberlo, riesgos aceptados que deben ser evitados, dado el apetito de riesgo de la entidad.

El enfoque de ERM en las tareas críticas de gestión de riesgos: identificar eventos, evaluar riesgos, formular respuestas al riesgo, implementar actividades de control, informar/comunicar y monitorear – proporciona un marco flexible para abordar estos tres temas estratégicamente importantes. La falta de gestión de las exposiciones de la empresa a posibles los eventos futuros que pueden destruir el valor reducirán incluso los planes mejor trazados para crear valor para desperdiciarlo.

Para identificar los impulsores de valor (o las variables subyacentes clave) de manera efectiva, es útil un contexto. Por ejemplo, el valor de las acciones es una medida de valor generalmente aceptada y, por lo tanto, es un ejemplo de un contexto útil para definir el valor de la empresa. El Valor Económico Agregado (EVA) es un ejemplo de tal medida. Otros ejemplos Proporcionar un contexto para definir los generadores de valor inherentes al modelo de negocio Incluir objetivos de negocio y estrategias, objetivos clave de rendimiento y factores clave de éxito vinculados a la creación de valor. Los impulsores de valor se pueden vincular a las variables que influyen en el logro del plan de negocios, por ejemplo, pueden definirse en términos de la variables subyacentes clave que hacen que los ingresos y los gastos suban y bajen.

Una vez que se definen los impulsores de valor clave, se desarrollan indicadores clave de rendimiento. Estos KPI se traducen concepto en acción en el plan de negocios, ya que son las métricas por las cuales el desempeño contra el plan es evaluado y finalmente recompensado. Los KPI se convierten en informes y se utilizan para monitorear el desempeño con el tiempo. Administrar y monitorear el negocio surgirá oportunidades para mejorar procesos, productos y servicios para mejorar el valor empresarial.

Hay varias cuestiones a tener en cuenta al aplicar ERM para mejorar el rendimiento empresarial. Para ilustrar, EVA es un marco útil para medir el desempeño corporativo que tiene en cuenta un cargo de capital reflejando el costo total del capital desplegado en el negocio. Este marco se utiliza para establecer la responsabilidad de los directivos para la creación de valor. La fórmula básica para calcular el EVA es la siguiente:

$$\text{EVA} = \text{NOPAT} - \text{WACoC},$$

Donde, NOPAT es la Utilidad Operativa Neta Despues de Impuestos y WACoC es el Costo Promedio Ponderado de Capital.

Hay al menos cuatro formas de aumentar el valor empresarial en el marco de EVA:

- Crear nuevas oportunidades: la empresa invierte en nuevas actividades comerciales que prometen rendimientos atractivos que se espera superen el WACoC.
- Mejorar el rendimiento: la empresa mejora el rendimiento y aumenta la rentabilidad de los negocios existentes actividades mediante la mejora de políticas, procesos, competencias, informes, tecnología y/o conocimiento en maneras que logran este resultado deseado.
- Cosechar el valor existente: La empresa se retira de las actividades comerciales existentes generando retornos inadecuados, es decir, estas actividades han generado (o se espera que generen) retornos que no excedan el WACoC.
- Ajustar y alinear el costo de capital: la empresa toma medidas específicas para reducir WACoC y/o garantizar los riesgos tomados son consistentes con el apetito de riesgo de la empresa.

Al aplicar una perspectiva de ERM, podemos identificar varias oportunidades para mejorar la gestión de riesgos procesos para mejorar el rendimiento empresarial utilizando la aplicación de EVA, como se describe anteriormente, como contexto:

- Crear nuevas oportunidades: NOPAT solo refleja pérdidas esperadas que son razonablemente estimables. A menos que ajustado específicamente para el riesgo, un WACoC **general** ignora los riesgos relativos inherentes a los negocios individuales unidades y actividades. Para abordar estos riesgos inherentes, la gerencia debe insistir en que la metodología utilizada para calcular el EVA se considera la equivalencia de riesgo de actividades alternativas. Bajo ERM, un proceso debe ser para identificar los principales riesgos inherentes a las unidades de negocio y actividades individuales.

Todo negocio exitoso asume riesgos en la búsqueda de oportunidades de valor agregado. por ejemplo, cuando la dirección decide entrar en nuevos mercados, introducir nuevos productos, adquirir otra entidad o explotar otras oportunidades de mercado, inherentes a estas decisiones, son opciones para asumir un riesgo adicional. cuando el riesgo la gestión está integrada con el establecimiento de la estrategia, estas opciones son transparentes porque los directores y la dirección ejecutiva tiene pleno conocimiento de las consecuencias de asumir riesgos. Ese conocimiento es un resultado de los esfuerzos de la organización para comprender, monitorear y rastrear el riesgo durante el establecimiento de la estrategia proceso. Bajo ERM, existe un proceso para identificar los riesgos prioritarios inherentes a la gestión de acciones planeadas y fijar el precio de las adquisiciones, transacciones y tratos resultantes de esas acciones para compensar adecuadamente a la empresa por los riesgos que está asumiendo. El incumplimiento de esta evaluación puede dar lugar a que la dirección se comprometa a emprender actividades en las que existen riesgos indeseables significativos que excedan el apetito por el riesgo, es decir, variabilidad de desempeño inaceptable, exposición a pérdidas y/o modelo de negocio incongruencias El objetivo es entender completamente las cosas buenas que pueden pasar, las cosas malas que puede suceder y los diversos escenarios intermedios.

Además, luego de la consumación de adquisiciones, transacciones y tratos, existe un proceso para monitorear los riesgos y mitigarlos si posteriormente se determina que son diferentes a los originalmente contemplados por la estrategia. Integrada de manera efectiva con el establecimiento de estrategias, la gestión de riesgos debe fortalecer el comportamiento de búsqueda de oportunidades al ayudar a los gerentes a desarrollar la confianza de que realmente entienden los riesgos y tienen

las capacidades disponibles dentro de la organización para gestionar esos riesgos. El resultado: la gerencia y la junta entienden completamente la desventaja y cuánto podría doler. También saben qué ver con el tiempo.

Dado que el futuro es impredecible, la gerencia debe determinar que la empresa ha asignado suficiente capital para proporcionar un colchón para pérdidas extremas inesperadas o desconocidas incurridas por actividades individuales. Aquí radica una conexión lógica entre ERM y la creación de valor. Si no hubiera riesgos, no habría necesidad de capital social. Así, el capital social es el precio de la exposición a la incertidumbre. Si no hubiera exposición a la incertidumbre, cada organización podría financiar sus actividades con bonos AAA. Dado que esta tierra de fantasía no existe en el mundo real, se necesita capital social para cubrir riesgos inesperados. Cualquier cosa que pueda ser cubierta por un seguro tradicional o con estructuras similares a las de un seguro se vuelve más segura si la contraparte aseguradora tiene una calificación crediticia sobresaliente y no hay lagunas legales que enturbien el proceso de liquidación. En tales condiciones, la necesidad de capital social puede reducirse. ¿Cuál es el punto de? Debido a que la junta y el director ejecutivo deben asumir en última instancia la responsabilidad de asignar el capital de manera efectiva, una evaluación de riesgos puede ser útil para diferenciar los perfiles de riesgo por unidad, actividad o proyecto.

- Mejorar el desempeño: una evaluación de riesgos completa y sólida de una unidad comercial o actividad determinada puede identificar los riesgos prioritarios que exponen los flujos de ingresos y flujos de efectivo futuros a una variabilidad de desempeño inaceptable o exposición a pérdidas. Una vez que se implementa un marco de evaluación de riesgos coherente en toda la empresa, es posible la comparación y la agregación entre las unidades operativas y de soporte. La asignación de capital se vuelve más significativa y las opciones de inversión se vuelven más claras. Un proceso de evaluación de riesgos más sólido reduce la posibilidad de pasar por alto riesgos clave e incurrir en costos de oportunidad inaceptables debido a un comportamiento de aversión al riesgo. Las respuestas a los riesgos pueden entonces evaluarse para reducir los riesgos prioritarios a un nivel aceptable. Al realizar tales evaluaciones, la identificación de eventos o escenarios potenciales puede proporcionar información útil sobre los puntos débiles de la estrategia comercial de la empresa o unidad, así como oportunidades para mejorar el desempeño.
- Cosechar valor existente: Decisiones de salir de un mercado o área geográfica o de vender, liquidar o escindir una grupo de productos o negocio debe evaluarse cuidadosamente. Los gerentes deben comprender el "riesgo relativo" de las diferentes unidades, geografías, productos o mercados. Si el desempeño se mide sin considerar los riesgos asumidos por los gerentes al generar rendimientos para la empresa a través de sus respectivas actividades, una decisión de salida podría resultar en el retiro de un negocio que está generando rendimientos ajustados por riesgo superiores, aunque sus rendimientos brutos, no ajustados por riesgo, puede parecer mediocre en relación con otras actividades. El análisis que respalda esta evaluación podría ser tan simple como un mapa de riesgos preparado para cada unidad de negocio o tan sofisticado como implementar una medición de desempeño ajustada al riesgo. Además, la gerencia debe evaluar durante el establecimiento de la estrategia las consecuencias de tomar medidas para mitigar un riesgo, ya que esa acción podría crear otro riesgo. Una evaluación de riesgos eficaz facilitará la evaluación de alternativas.
- Ajustar y alinear el costo de capital: bajo EVA, este paso es difícil de tomar de una manera que resulte en un cambio sustancial que realmente marque la diferencia. Una razón es que WACoC es más relevante para las unidades y actividades específicas de la empresa que para la empresa en su conjunto, si esas unidades y actividades tienen perfiles de riesgo únicos. Las empresas pueden solucionar este problema asignando diferentes unidades con un WACoC específico relevante para sus actividades específicas, en función de los puntos de referencia de un sustituto basado en el mercado, como una empresa pública específica o un grupo de empresas con actividades y riesgos equivalentes. Si una unidad de negocios se dedica a actividades de alto riesgo, su costo de capital debe ser mayor que el de las empresas de menor riesgo. Si sus actividades son de bajo riesgo, el costo de capital de la empresa invertido en la unidad debería ser correspondientemente más bajo. Las valoraciones de mercado a nivel corporativo a menudo no brindan suficiente transparencia en cuanto a los riesgos asumidos por las diferentes unidades y actividades.

Durante el proceso de establecimiento de la estrategia, las empresas que se toman en serio la gestión de riesgos se esfuerzan por configurar su asunción de riesgos con sus competencias básicas, o lo que mejor saben hacer, evitando restringir indebidamente el comportamiento de aversión al riesgo. El modelo de negocios de toda organización exitosa explota en la mayor medida posible las áreas en las que la empresa sobresale en relación con sus competidores. Sin embargo, al aprovechar estas ventajas, la dirección necesita asegurarse de que la empresa no está jugando su futuro. Una infraestructura ERM (como se analiza en las Preguntas 37 y 56) proporciona la disciplina, el enfoque y el control mediante los cuales la gerencia (a) capitaliza las fortalezas competitivas mientras protege el valor de la empresa, y (b) garantiza que la empresa solo

toma los riesgos que está mejor equipado para manejar dentro de los parámetros de su apetito por el riesgo, mientras minimiza la exposición a aquellas áreas consideradas "fuera de la estrategia" debido a la falta de competencia para administrar.

En resumen, la vinculación de ERM con el desempeño empresarial mejorado se logra de diferentes maneras. Al evaluar los efectos sobre el desempeño comercial de los cambios en el perfil de riesgo de una empresa a partir de la implementación de respuestas de riesgo alternativas, la gerencia puede concentrarse en mejorar el rendimiento esperado para la empresa en su conjunto o, alternativamente, mantener constante el rendimiento esperado y alterar las características de riesgo de la organización..

La gerencia altera las características de riesgo de una entidad al reducir:

- (a) la exposición neta de la empresa;
- (b) la variabilidad de los rendimientos esperados de la empresa causada por fuentes específicas de incertidumbre (tales como exposición a tipos de cambio fluctuantes);
- (c) La probabilidad de dificultades financieras en caso de que se produzcan cambios en variables clave (como cambios en las tasas de interés para una empresa altamente apalancada); o
- (d) Otras incertidumbres en el logro de los rendimientos esperados.

En efecto, la mejora del rendimiento empresarial surge de la integración de la gestión de riesgos con el establecimiento de estrategias. Tal integración significa dos cosas. Primero, significa que el perfil de riesgo de las decisiones estratégicas se evalúa temprano en el proceso de establecimiento de la estrategia, lo que lleva a una estrategia comercial más sólida. En segundo lugar, significa que las políticas, los procedimientos, las medidas y el seguimiento se establecen y se mejoran continuamente para brindar seguridad a la gerencia y al directorio de que la empresa está encaminada para lograr el rendimiento esperado mientras controla su exposición al riesgo aceptada. Estos dos aspectos de un proceso integrado conducen a un mayor enfoque en la mejora del rendimiento empresarial. La conclusión es que la organización solo "aprende una vez" y comparte conocimientos y experiencias para que las capacidades de gestión de riesgos mejoren continuamente y se reduzca la exposición a riesgos inaceptables y errores estratégicos.

#### 130. ¿Cómo debemos integrar nuestro enfoque ERM con nuestro proceso de planificación estratégica?

Una forma es integrar capacidades específicas de ERM con las diversas fases del proceso de establecimiento de estrategias. Este pensamiento se ilustra a continuación:

FASE DE ESTABLECIMIENTO DE ESTRATEGIA	EXPLICACIÓN DE FASE DE ESTABLECIMIENTO DE LA ESTRATEGIA	EXPLICACIÓN DEL COMPONENTE ERM PARA INTEGRAR CON ESTABLECIMIENTO DE ESTRATEGIA
Evaluación estratégica	Obtener una comprensión general de la organización y su entorno operativo.	El entorno interno, la identificación de eventos y la evaluación de riesgos contribuyen significativamente a esta fase, que incluye realizar una evaluación de riesgos integral en toda la empresa e inventariar el estado actual de las capacidades de gestión de riesgos para identificar y generar riesgos.
Desarrollo de estrategias	Identificar alternativas de estrategia, seleccionar las actividades estratégicas apropiadas para emprender y diseñar las mejoras necesarias en la organización	La respuesta al riesgo se relaciona con esta fase porque implica la medición del riesgo, el diseño de las capacidades deseadas de gestión del riesgo y la evaluación del impacto de estas capacidades en el riesgo residual.
formular plan	Articular un enfoque integral para implementar el diseño organizacional y actividades específicas para ejecutar la estrategia, incluida la definición de requisitos de recursos y planes funcionales.	Las actividades de control, información/comunicación y seguimiento son complementarias a esta fase del proceso ya que abordan la gestión y seguimiento del riesgo y proporcionan una visión general de las acciones, métricas e hitos que permiten a la organización cerrar las brechas en sus capacidades y alcanzar sus objetivos

En el establecimiento de la estrategia, la gerencia a menudo se enfoca en seleccionar los impulsores de valor clave descomponiendo los impulsores de valor hasta un nivel apropiado que es lo suficientemente granular para medir y gestionar. Por ejemplo, bajo un marco de valor del accionista, el precio de la acción es una función de las ganancias, la experiencia de gestión, el inversor confianza, las perspectivas económicas y otros factores. Una de estas variables, los ingresos, es una función de ingresos, costos directos e indirectos e impuestos sobre las ganancias antes de impuestos. Los impulsores de los ingresos pueden incluir tales factores como volumen predecible, competitividad de precios, liquidez de clientes, diversificación de clientes, existencia de barreras de entrada y una industria atractiva que ofrece espacio para un crecimiento adicional. Estos factores son valor impulsores de los ingresos. Se pueden descomponer aún más. Por ejemplo, si el volumen predecible es un factor prioritario, podemos determinar impulsores adicionales, por ejemplo, un mercado adecuadamente segmentado, capacidad productiva escalable y un canal de distribución que funcione eficazmente.

Una vez que los impulsores de valor se definen en el nivel deseado de descomposición, la gerencia selecciona los más impulsores críticos y define las fuentes de incertidumbre asociadas con cada uno de esos impulsores. Esto puede ser logrado al priorizar primero los impulsores de valor en función de su contribución al éxito de la negocio. Luego, la gerencia selecciona los impulsores prioritarios para fines de identificación de eventos y riesgos. evaluación. Por lo tanto, los impulsores de valor brindan un contexto tanto para el establecimiento de estrategias como para la evaluación de riesgos. razón por la cual ERM debe integrarse con el establecimiento de estrategias.

131. ¿Deberíamos completar nuestro proceso de planificación estratégica antes de realizar nuestra primera evaluación de riesgos, o viceversa?

La intención del proceso ERM es incorporar el apetito por el riesgo y la gestión del riesgo en el establecimiento de la estrategia. Un la evaluación de riesgos de toda la empresa puede ayudar a la gerencia a determinar si existen riesgos que son inconsistentes con o por encima del apetito por el riesgo de la organización. Debido a que el entorno cambia constantemente, el establecimiento de estrategias es un proceso dinámico que nunca termina. Lo mismo se aplica a la evaluación de riesgos. Por lo tanto, no creemos La gerencia nunca debe formular una estrategia sin evaluar el riesgo. Si no se considera el riesgo durante el establecimiento de la estrategia, los gerentes naturalmente gravitarán hacia las oportunidades con el mayor rendimiento, independientemente del riesgo. La evaluación de riesgos debe realizarse cuando se desarrolla la estrategia, porque los dos procesos se potencian mutuamente.

En aquellas situaciones en las que se realiza una evaluación de riesgos después de que se desarrolla la estrategia comercial, la estrategia debe ser reevaluado para considerar los riesgos importantes identificados durante la evaluación de riesgos SI tales riesgos no fueron considerado cuando se formuló originalmente la estrategia. Las estrategias comerciales a menudo justifican una revisión una vez que los riesgos inherentes a esas estrategias se entienden completamente. Por lo tanto, las metas y objetivos de la entidad pueden ser más refinado cuando se lleva a cabo una evaluación de riesgos en toda la empresa.

132. ¿Es posible fusionar con éxito las evaluaciones de riesgo que las empresas realizan como resultado de ERM, cumplimiento de Sarbanes-Oxley, planificación de continuidad comercial, auditoría interna y diversas actividades de cumplimiento relacionadas con el lugar de trabajo, medio ambiente y otras regulaciones?

Sí, SI se implementa un lenguaje común y un proceso uniforme para realizar esas evaluaciones. un punto a Recuerde, sin embargo, que varias de las áreas mencionadas en la pregunta: cumplimiento de Sarbanes-Oxley, negocios planificación de continuidad, cumplimiento normativo en el lugar de trabajo y cumplimiento normativo ambiental: representan áreas específicas, mientras que ERM aborda el perfil de riesgo total de la empresa. La auditoría interna puede realizar evaluaciones de riesgo integrales o específicamente enfocadas, y puede ayudar en la fusión de estos múltiples evaluaciones en múltiples áreas, siempre que se utilice un lenguaje común y un proceso uniforme.

133. ¿Cómo utiliza la administración ERM para establecer una ventaja competitiva sostenible?

Cuando se implementa como parte integral del proceso de gestión estratégica, una infraestructura ERM puede ayudar administración establecer una ventaja competitiva sostenible. Los siguientes son ejemplos de cómo:

- Integrar la gestión de riesgos con la planificación comercial y el establecimiento de estrategias: Integración con procesos clave, y en particular con la planificación comercial y el establecimiento de estrategias, es un tema común en la implementación de ERM. La definición de ERM de COSO incluye una referencia a "aplicado en el establecimiento de estrategias". Riesgo efectivo La gestión traduce las evaluaciones de riesgo en respuestas de riesgo procesables específicas, impulsando cambios en actividades de control, procesos de información/comunicación y seguimiento.

- Implementar un proceso de evaluación de riesgos más riguroso: identificación de eventos y evaluación de riesgos más rigurosos mejora la calidad de las evaluaciones que respaldan el establecimiento de estrategias y los planes comerciales. Una vez que las unidades de negocio, las unidades de soporte, las unidades de riesgo y las unidades de aseguramiento implementan y utilizan un marco de evaluación de riesgos coherente en toda la empresa (consulte la pregunta 56), se hace posible la comparación y la agregación en toda la empresa. La asignación de capital se vuelve más significativa y las opciones de inversión se vuelven más claras. Un proceso de evaluación de riesgos más sólido reduce la posibilidad de pasar por alto riesgos clave e incurrir en costos de oportunidad inaceptables debido a un comportamiento de aversión al riesgo.
  - Mejorar la gestión de riesgos comunes en toda la empresa: siempre que existan riesgos comunes en toda la empresa, existe la oportunidad de compartir conocimientos y mejores prácticas. Un lenguaje común lo hace posible.
  - Mejorar el despliegue de capital y la asignación de recursos: uno de los objetivos de ERM es optimizar el riesgo, el rendimiento y el capital. Este objetivo conduce a análisis rigurosos para identificar las relaciones entre los riesgos y sus impulsores clave para que los riesgos puedan agregarse para proporcionar informes de riesgo más sólidos. Estos informes ayudan a los gerentes a tomar mejores decisiones al asignar capital a aquellas actividades comerciales que brindan las mayores perspectivas de rendimientos atractivos en relación con los riesgos asumidos y rechazan aquellas actividades que no son tan atractivas. La alternativa son las conjecturas intuitivas ineficaces, que no llevarán muy lejos a los gerentes dadas las complejas interrelaciones entre los riesgos y las variables que los afectan. Por lo tanto, mejorar los rendimientos a través de un proceso superior de asignación de capital es vital para una implementación eficaz de ERM. La gerencia decide si la asunción de riesgos debe ser agresiva o moderada en relación con el capital disponible y las oportunidades alternativas de riesgo-rendimiento.
  - Configure la asunción de riesgos de la empresa con sus competencias básicas: las empresas que se toman en serio su gestión de riesgos configuran su asunción de riesgos con sus competencias básicas, o lo que hacen mejor, evitando comportamientos fuera de estrategia y aversión al riesgo. El modelo de negocios de toda organización exitosa explota en la mayor medida posible las áreas en las que la empresa sobresale en relación con sus competidores. Sin embargo, al aprovechar estas ventajas, la dirección necesita asegurarse de que la empresa no está jugando con su futuro. Una infraestructura de ERM proporciona la disciplina mediante la cual la administración capitaliza las fortalezas competitivas y, al mismo tiempo, protege el valor de la empresa. De hecho, ERM facilita que una empresa asuma los riesgos que está mejor equipada para manejar dentro de los parámetros de su apetito por el riesgo, mientras minimiza la exposición a aquellas áreas que considera "fuera de la estrategia" y carece de competencia para administrar.
  - Aproveche las oportunidades a través de la asunción racional del riesgo: en el nivel más alto de capacidad, ERM ayuda a las empresas a comprender sus riesgos y sus capacidades de gestión de riesgos de manera tan completa que pueden avanzar rápidamente para buscar oportunidades que podrían ser motivo de inquietud en organizaciones menos sofisticadas. Es inevitable que toda empresa exitosa deba asumir riesgos. Pero la toma de riesgos debe ser sabia y mesurada, y no arrogante. La gestión de riesgos brinda transparencia y seguridad a los directores y al CEO de que los riesgos se toman con conocimiento: conocimiento del negocio, conocimiento de los riesgos y conocimiento de los mercados.
- Ese conocimiento es el resultado de los esfuerzos persistentes de la gerencia para comprender, monitorear y rastrear el riesgo.

Estos son ejemplos de cómo la gerencia usa ERM para establecer una ventaja competitiva sostenible.

La formulación de una estrategia de gestión de riesgos en toda la empresa es algo que cualquier organización puede hacer en cualquier momento, independientemente de lo lejos que viaje a lo largo del viaje de ERM. El punto importante es este: el proceso de formulación de la estrategia de toda la empresa es más significativo cuando las medidas de riesgo se agregan a nivel de toda la empresa y la gerencia comprende claramente cómo la gestión de riesgos mejora el rendimiento empresarial. Es por eso que el paso de establecer una ventaja competitiva sostenible es el último paso en el camino hacia ERM.

La comprensión y la gestión eficaz de la relación entre el capital, el riesgo y la recompensa dentro de los límites de la estrategia de riesgo de una organización crean una importante oportunidad de gestión de riesgos. Un enfoque para desarrollar esta capacidad es evaluar la capacidad para asumir riesgos y el apetito para asumir riesgos, y asignar capital en función de este análisis. El apetito por el riesgo de la organización o la voluntad de asumir riesgos refleja tanto su capacidad para asumir riesgos como una comprensión más amplia del nivel de riesgo que puede gestionar con seguridad y éxito durante un período prolongado de tiempo. El apetito por el riesgo es la medida en que una empresa está dispuesta a exponer su capital a la explotación de oportunidades estratégicas y la conservación de la variabilidad del rendimiento y la exposición a pérdidas. Se explica con más detalle en la Pregunta 66.

La prudencia y el sentido común son vitales a la hora de evaluar el apetito por el riesgo. Por ejemplo, ¿tiene sentido asumir todo el riesgo que una organización es capaz de asumir sin reservar capital para nuevas oportunidades de inversión? ¿Es apropiado retener un riesgo significativo cuando las opciones para transferir ese riesgo están disponibles a un costo razonable? Desde el punto de vista de la estrategia, puede ser útil tener una noción del punto en el que se invadiría la capacidad de la organización para asumir riesgos.

---

## CONSTRUYENDO UN CASO DE NEGOCIO COMPULSOR

### 134. ¿Cómo construimos un caso de negocios convincente para ERM?

Una vez que se definen la visión de ERM y los objetivos de gestión de riesgos y se seleccionan las capacidades relevantes, la gerencia está lista para preparar un caso de negocios para continuar. Los objetivos de gestión de riesgos abordan “el qué”. El caso de negocios se refiere al “por qué” y articula la propuesta de valor de ERM. El caso de negocios proporciona la justificación económica del esfuerzo general para construir y mejorar la infraestructura de ERM de la organización y las capacidades de gestión de riesgos. Incluye un punto de vista sobre cómo se verá la solución ERM (es decir, las capacidades seleccionadas), por qué la organización patrocinadora debe construir la solución, el valor incremental que espera de la solución y los proyectos necesarios para avanzar en la realización de la solución. beneficios esperados.

Una propuesta de valor suficientemente granular no es posible sin el conocimiento de los riesgos prioritarios de la organización y las brechas significativas en torno a la gestión de esos riesgos. La pregunta 85 analiza la importancia de una evaluación de riesgos de toda la empresa para obtener este entendimiento. Puede haber muchas razones para desarrollar y mejorar las capacidades de gestión de riesgos. Cada organización debe hacer su propia evaluación de los beneficios esperados para justificar las inversiones requeridas en la infraestructura de ERM y el marco de tiempo en el que se realizarán dichas inversiones. Un caso de negocio documenta esa evaluación y describe cómo se realizarán las capacidades esperadas y los beneficios relacionados con el tiempo a medida que se implemente la solución ERM.

El caso de negocios:

- Define la visión de ERM: El caso de negocio reitera la “visión compartida” de la empresa en cuanto al rol del riesgo gerencia en el negocio. Consulte las preguntas 64 y 65.
- Describe el esfuerzo general: El caso de negocios describe el imperativo de cambio de ERM, es decir, describe el proceso de cambio y el esfuerzo requerido para llevar ese proceso a una conclusión. Como se explica con más detalle en la Pregunta 85, la comprensión de los riesgos prioritarios y de las brechas significativas en torno a la gestión de esos riesgos es vital para articular de manera efectiva el esfuerzo de cambio.
- Analiza los costos y beneficios relacionados: El cambio bajo cualquier circunstancia es difícil de iniciar, pero a menos que se entienda claramente la necesidad de cambiar, no sucederá. El caso de negocios detalla la propuesta de valor de ERM y proporciona un análisis de impacto de valor, incluidas las medidas de éxito. Como se discutió más detalladamente en la Pregunta 4, una propuesta de valor genérica debe complementarse con una articulación más granular que sea posible gracias a una evaluación de riesgos empresariales y un análisis de brechas en torno a las capacidades de la entidad para administrar sus riesgos prioritarios. Cuanto mayor sea la brecha entre el estado actual y el estado futuro deseado de las capacidades de gestión de riesgos de la organización, mayor será la necesidad de una infraestructura ERM para facilitar el avance de esas capacidades a lo largo del tiempo. El caso de negocios debe hacer este punto claramente.
- Proporciona un contexto para monitorear el progreso a lo largo del tiempo: el caso de negocios proporciona el contexto de negocios por realizar el cambio a ERM. Establece las medidas de éxito predefinidas, que proporcionan objetivos cuantitativos y cualitativos contra los cuales evaluar el desempeño. Un análisis de impacto de valor (ver el siguiente punto) también proporciona un contexto para monitorear el progreso contra las proyecciones de referencia y los beneficios netos futuros esperados. Las medidas de éxito son importantes porque proporcionan los medios para saber que la solución ERM “marca la diferencia”. En la pregunta 136 se proporcionan ejemplos de medidas de éxito.

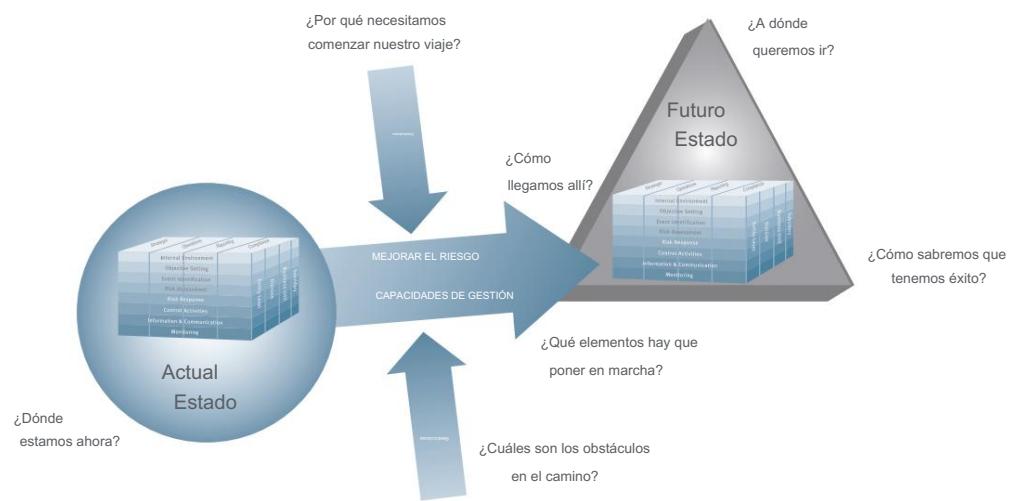
- Explica la justificación económica para seguir adelante: la dirección ejecutiva necesita hechos antes de comprometerse a implementar ERM. El caso de negocios proporciona un marco cuantitativo y cualitativo de los beneficios y costos esperados de ERM para uso de los patrocinadores para obtener la aprobación de la gerencia para proceder. Si es factible, se proporciona un análisis de impacto de valor, respaldado con un modelo económico creíble que proyecta los beneficios netos esperados resultantes de los cambios solicitados para que los patrocinadores del proyecto puedan tomar las decisiones más informadas sobre si realizar o no inversiones en infraestructura de ERM y gestión de riesgos. Dichos análisis cuantitativos, si están disponibles, complementan la evaluación cualitativa. Por ejemplo, ¿mejorará la infraestructura de ERM el proceso de toma de decisiones sobre cuestiones de importancia para la empresa en su conjunto y lo hará más rentable?

El caso de negocio respalda el compromiso de la dirección ejecutiva de seguir adelante con el proceso de implementación. Si bien no existen reglas estrictas sobre cómo se ve el caso de negocios, debe definirse desde arriba y administrarse con participación e involucramiento activos desde arriba. El caso de negocio puede desarrollarse para el viaje ERM general o puede desarrollarse para cada fase principal del viaje ERM. Es un "documento vivo" que proporciona una hoja de ruta para gestionar el esfuerzo general frente a las expectativas.

Por lo tanto, debe actualizarse de vez en cuando a medida que avanza el proceso de cambio.

El proceso de desarrollo del caso de negocios genera la aceptación y el compromiso de las partes interesadas con el viaje de cambio de ERM y ayuda a la gerencia a lograr una comprensión de los requisitos para su éxito. Cuando la organización patrocinadora adopta los aspectos críticos del caso de negocios y está preparada para comprometerse a construir y probar las capacidades que brindan los resultados deseados, el proceso de diseño e implementación puede comenzar.

El siguiente esquema ilustra las preguntas clave que debe abordar un caso de negocio:



Tenga en cuenta que COSO Enterprise Risk Management - Marco integrado se utiliza como contexto para comprender el "estado actual" de la entidad, así como para articular su "estado futuro". Como se discutió en las Preguntas 110 y 111, los seis elementos del modelo de madurez de infraestructura y capacidad también se pueden usar para analizar las brechas en las capacidades en torno a la gestión de los riesgos prioritarios.

El caso comercial debe integrarse con el plan de gestión de viajes, como se analiza en la Pregunta 137, para implementar las diversas capacidades de ERM que brindan los resultados deseados por la administración. Es importante que los problemas críticos de cambio se identifiquen, entiendan y aborden por completo.

### 135. ¿Cómo seleccionamos las capacidades apropiadas para nuestra solución ERM?

Es una cuestión de juicio, cultura, estilo operativo, necesidades organizacionales y capacidad deseada para riesgos específicos. Lo que funciona para una organización no necesariamente funcionará para otra organización. La gerencia debe decidir sobre las capacidades que mejor satisfagan las necesidades de la organización. La gestión de riesgos empresariales debe convertirse en una parte integral de la agenda empresarial.

Nuestro consejo a la hora de diseñar una solución ERM:

- Comience con el riesgo: comience con una evaluación de riesgos de toda la empresa y un análisis de brechas en torno a las capacidades para gestionar los riesgos prioritarios.
- Comience en algún lugar, en cualquier lugar: comience mejorando las capacidades para administrar uno o dos riesgos clave que la gerencia sabe que requieren mejoras.
- Salir de la caja: reenfocar las actividades de gestión de riesgos ad hoc, reactivas y fragmentadas de las funciones y departamentos que operan como silos independientes. Integrar estas actividades con un riesgo común capacidad de generación de informes del tablero de administración.
- Pensar y gestionar estratégicamente: Integrar la gestión de riesgos con el establecimiento de estrategias. buscar entender las interrelaciones entre los riesgos desde un punto de vista de arriba hacia abajo en toda la empresa y, en base a eso comprensión, organizar los riesgos en grupos y familias apropiados. Desarrollar un riesgo más integrado respuestas para aplicar hábilmente marcos analíticos apropiados y metodologías de medición a cada familia o grupo de riesgo significativo. Asegúrese de que alguien sea dueño de los riesgos.
- Nunca esté satisfecho: practique una mentalidad de mejora continua.
- Recuerde, no es ciencia espacial: COSO afirma que los gerentes dentro de una empresa “deben considerar cómo están llevando a cabo sus responsabilidades a la luz del marco ERM y discutir con más ideas del personal superior para fortalecer la gestión de riesgos empresariales”. Ese no es un proceso difícil.

Como se introdujo en la Pregunta 68, los ocho pasos para mejorar las capacidades de gestión de riesgos, organizados en tres fases, brindan orientación sobre la secuencia adecuada durante el proceso de implementación de ERM. Para Por ejemplo, al diseñar una solución ERM, el equipo del proyecto debe sentar las bases primero y luego proceder a construir capacidades de gestión de riesgos. Las capacidades que funcionan efectivamente proporcionan una base para mejorar las capacidades de gestión de riesgos a lo largo del tiempo. Cuantas más capacidades de mejora pone la administración lugar, más valor agregado tendrá la solución ERM y mayor será la alineación de la estrategia de gestión de riesgos, procesos, personas, tecnología y conocimiento.

Los elementos ilustrados proporcionados en esta publicación para cada uno de los ocho pasos se suman al riesgo de la empresa. capacidades de gestión y a la propuesta de valor (beneficios) de la gestión de riesgos. Acompañando a cada avance en las capacidades de gestión de riesgos es un aumento correspondiente en el grado de sofisticación y la grado de compromiso requerido. Por lo tanto, la gerencia debe decidir, conscientemente, hasta dónde llegar. alinear sistemáticamente las estrategias, los procesos, las personas, la tecnología y el conocimiento de la organización mediante mejoras por etapas a lo largo del tiempo.

A medida que la organización avanza hacia la fase de mejora de capacidades, el grado de integración del riesgo se incrementa la gestión con procesos estratégicos y operativos. Como se señaló en la pregunta 85, la empresa los riesgos prioritarios y las brechas significativas en torno a la gestión de esos riesgos proporcionan el contexto para decidir hasta qué punto para tomar la solución ERM. El modelo de negocios y la cultura de la organización, la madurez relativa de sus capacidades de gestión de riesgos, las iniciativas actuales financiadas y en marcha para mejorar las capacidades, el grado de centralización o descentralización, la comparabilidad de los perfiles de riesgo relativos a las diferentes unidades de negocio dentro de la empresa y otros factores deben ser considerados al decidir el nivel de madurez de la capacidades en torno a la gestión de los riesgos prioritarios de la empresa.

Al seleccionar las capacidades deseadas, la gerencia debe reconocer que ERM es un viaje, no un destino. En la Pregunta 85, presentamos y explicamos cinco pasos para comenzar a implementar ERM:

PASO 1: Realice una evaluación de riesgos empresariales (ERA) para evaluar y priorizar los riesgos críticos. En este paso, la dirección entiende los riesgos.

PASO 2: Articular la visión de la gestión de riesgos y apoyarla con una propuesta de valor convincente utilizando lagunas en torno a los riesgos prioritarios. En este paso, la gerencia define la dirección.

PASO 3: Mejorar la capacidad de gestión de riesgos de la organización para uno o dos riesgos prioritarios. Aquí es donde la gerencia enfoca la línea de visión para cerrar brechas inaceptables.

PASO 4: Evaluar la capacidad de la infraestructura ERM existente y desarrollar una estrategia para mejorárla.

A través de la infraestructura de ERM, la gerencia establece responsabilidad y control sobre la mejora continua de las capacidades de gestión de riesgos.

PASO 5: Actualice la ERA para el cambio y avance en las capacidades de gestión de riesgos para riesgos clave. En este punto, la gerencia amplía el enfoque.

Al planificar las capacidades deseadas para construir y mejorar junto con el Paso 2 al Paso 5 anteriores, la secuencia sugerida de fases y pasos presentados en la Pregunta 68 proporcionarán información sobre dónde comenzar y por qué. Si bien no existen reglas estrictas y rápidas, ERM se logra mejor en etapas que comienzan con el desarrollo de un lenguaje común y procesos uniformes. Para ilustrar:

- Establecer las bases: una vez que la alta dirección se compromete a explorar la propuesta de valor de ERM, un grupo de trabajo de altos ejecutivos (un comité ejecutivo de gestión de riesgos [RMEC], por ejemplo), con el apoyo de un director de riesgos (o un alto ejecutivo equivalente), está facultado para construir y mejorar las capacidades de gestión de riesgos de la organización. Estos ejecutivos deben estar respaldados por una función de personal central pequeña y enfocada, como una función de gestión de riesgos comerciales. Al constituir el RMEC y el CRO, el CEO, el comité ejecutivo y la junta directiva definen el alcance de ERM, por ejemplo, ¿qué significa "toda la empresa" y cuáles son sus implicaciones? Al trabajar con los riesgos prioritarios identificados por la evaluación de riesgos empresariales y las brechas significativas en torno a las capacidades para gestionar los riesgos prioritarios, el RMEC y el CRO planifican y coordinan el desarrollo de capacidades que cierran las brechas inaceptables.
- El lenguaje de riesgo de la organización y el esquema de clasificación de procesos comerciales proporcionan un punto de partida útil para identificar y obtener sus riesgos. En la Pregunta 96 se ilustran otros elementos de "Establecer las bases".
- Desarrollar capacidades: en base a la evaluación de riesgos empresariales y el análisis de brechas, el RMEC identifica las áreas que requieren la mayor atención. El estado actual de las capacidades de gestión de riesgos relacionadas con los riesgos prioritarios se documenta formalmente para proporcionar la línea de base para identificar las mejoras necesarias. Se asigna la propiedad del riesgo. Los elementos sugeridos a considerar cuando se desarrollan capacidades se ilustran en la Pregunta 103. El RMEC garantiza que haya responsabilidades claras para gestionar los riesgos prioritarios e identifica áreas para lograr "golpes rápidos" y resultados exitosos para generar impulso para la iniciativa ERM.
- Mejorar las capacidades: una vez que se establecen los cimientos en forma de elementos apropiados de la infraestructura de ERM y una vez que las capacidades en torno a la gestión de riesgos prioritarios están establecidas, la gerencia decide las mejoras necesarias para lograr la visión de la gestión de riesgos y las metas y objetivos relacionados. . Los elementos sugeridos a considerar cuando se mejoran las capacidades se ilustran en la Pregunta 125.

A través de este proceso secuenciado de creación y mejora de capacidades, la gerencia puede colocar los "bloques de construcción" de ERM para la organización. La gerencia debe usar el marco COSO ERM para comparar la gestión de riesgos de la organización en varias etapas a lo largo del viaje de ERM.

136. ¿Cuáles son los factores clave de éxito o las medidas de éxito al evaluar la eficacia y el impacto de la implementación de ERM, es decir, cómo podemos saber si se ha adoptado un enfoque de ERM? ¿exitoso?

La premisa subyacente de ERM es ayudar a los gerentes senior y operativos a tomar mejores decisiones sobre cómo se deben administrar los riesgos en toda la empresa. Si se toman buenas decisiones, ¿cómo sabemos si la decisión hubiera sido diferente si no hubiera existido el proceso ERM de la entidad? Por otro lado, si la gerencia toma una mala decisión, ¿cómo sabemos si se hubiera tomado una mejor decisión si la organización hubiera implementado ERM? ¿Una solución de ERM habría marcado una diferencia en la mejora del proceso de toma de decisiones? Las pruebas son ilusorias a este respecto.

Los siguientes son ejemplos de medidas de éxito que las empresas han utilizado:

- Integración de la evaluación de riesgos en los procesos estratégicos y operativos: A medida que los gerentes hacen del riesgo comercial una parte integral de su agenda cuando evalúan estructuras de acuerdos alternativas, posibles mejoras de procesos, nuevos sistemas, nuevos productos y mercados alternativos, se vuelven más anticipatorios y con visión de futuro. en su toma de decisiones. Un ejemplo es la integración de la gestión de riesgos con los procesos de planificación empresarial y gestión estratégica. El riesgo se evalúa explícitamente de manera abierta y transparente.
- Identificación de riesgos mejorada: el mapeo de riesgos, junto con un lenguaje común, proporciona un medio muy visible para iniciar y mantener un diálogo sobre los riesgos en todos los niveles de la organización. Los propietarios de procesos y actividades, armados con las herramientas y los procesos apropiados, pueden identificar los riesgos de manera más efectiva y contribuir más al desempeño de la empresa a lo largo del tiempo (a diferencia de los propietarios de procesos y actividades que abordan el tema del riesgo como una ocurrencia tardía). Una mejor identificación del riesgo reduce el riesgo de retener el riesgo por ignorancia, lo que reduce la exposición de la empresa a sorpresas inaceptables que pueden afectar la evaluación de su desempeño por parte del mercado financiero.
- Implementación de técnicas analíticas y de alerta temprana más efectivas: Un mayor énfasis en análisis más sistemáticos, cuantitativos y predictivos conduce a decisiones más informadas. Las mejores decisiones, a su vez, conducen a un mejor rendimiento comercial con el tiempo. Un mayor uso de metodologías para anticipar el riesgo y evaluar el impacto de escenarios alternativos en los resultados futuros esperados conduce a una mayor eficacia en la escalada de problemas emergentes a la atención de los ejecutivos apropiados.
- Mejora en medidas, métricas y seguimiento de riesgos específicos: El cambio de "adivinar" a "saber" (o al menos "comprender") es una clara mejora, como lo es de "reaccionar" a "estar preparado". Los informes de gestión que rastrean los riesgos clave proporcionan evidencia de un mejor desempeño a lo largo del tiempo. La información sobre riesgos (respuestas de riesgos, medidas de riesgos, procesos de riesgos, incidentes de riesgos, mejores prácticas, estado de los planes de mejora y otros asuntos relevantes) disponible en todos los niveles de la organización a través de repositorios de datos habilitados para la web facilita los aspectos de intercambio de conocimientos de un enfoque ERM. El uso de herramientas de agregación de riesgos reemplaza las conjeturas intuitivas con análisis basados en hechos.
- Número reducido o evitación de incidentes de riesgo: si una empresa puede demostrar menos incidentes de riesgo o pérdida eventos que el promedio de la industria, tiene una clara evidencia de un rendimiento superior. La seguridad en el lugar de trabajo es un buen ejemplo de un riesgo en el que tal evaluación comparativa es posible. En algunos casos, Y2K por ejemplo, la expectativa es el cumplimiento, ni más ni menos. Algunos cuestionaron el nivel de gastos del año 2000 cuando los aviones no caían del cielo, los ascensores no caían y las armas nucleares no se disparaban. Pero considere el impacto en la reputación y la imagen si los sistemas de misión crítica de una empresa no cumplieran con el Y2K. Es un pensamiento paradójico invertir en una respuesta de reducción de riesgos y luego decepcionarse cuando "no pasa nada".
- Variabilidad de desempeño reducida: si una empresa encuentra menos sorpresas en los resultados informados debido a (a) un proceso de evaluación de riesgos más sistemático y proactivo, (b) medidas mejoradas y (c) controles internos preventivos que evitan incidentes de riesgo en la fuente, esta experiencia puede atribuirse a la gestión de riesgos de la firma. La variabilidad reducida en los ingresos, las ganancias y los flujos de efectivo a lo largo del tiempo puede, en igualdad de condiciones, contribuir a múltiples de precio/ganancias más altos en comparación con las empresas similares que mantienen una mayor volatilidad en los resultados informados. Por supuesto, la dificultad con esta medida es delinejar la contribución de la gestión de riesgos de otras disciplinas de gestión.
- Reducción del costo de capital y mejora del valor para los accionistas: a medida que los analistas, las agencias calificadoras, los reguladores y otras instituciones aprenden a diferenciar entre las capacidades de gestión de riesgos de varias empresas, las organizaciones que puedan implementar las capacidades articuladas en esta publicación deberían disfrutar de un costo más bajo. de capital a lo largo del tiempo en relación con las empresas que eligen no hacer nada. Si la gestión de riesgos de una empresa se considera en el mercado como una habilidad diferenciadora en relación con sus pares, entonces los costos de endeudamiento de la empresa deberían disminuir y las valoraciones de sus acciones deberían aumentar en consecuencia. Si bien es cierto que existe una ausencia de apoyo empírico para esta afirmación, no obstante, es una hipótesis sólida que tienen algunas empresas al implementar ERM.

- Mayor sensibilidad al riesgo y conciencia del riesgo: Un cambio cultural en la organización que conduce a un mayor enfoque y refuerzo de las metas y objetivos de la gestión de riesgos es un indicador de eficacia. Por ejemplo, para lograr un objetivo exigente para un objetivo históricamente alto de días sin lesiones en una organización de fabricación, puede ser necesario un cambio cultural para modificar el comportamiento. Otra situación es cuando una empresa de servicios públicos planifica la implementación de un proceso para evitar futuros cortes de energía. En estos casos, la gestión de riesgos es realmente parte integral de la gestión del negocio, ya que aborda los obstáculos que pueden impedir el logro de un imperativo empresarial declarado por la dirección.
- Integración con informes de KPI: Vemos varias empresas que integran la gestión de riesgos con indicadores de rendimiento (KPI). Por ejemplo, una empresa prepara mapas de riesgo para cada uno de los KPI en su cuadro de mando integral. Este enfoque innovador ofrece a los ejecutivos una priorización integral de riesgos por KPI. Luego se toman medidas para abordar los riesgos significativos que podrían hacer que la empresa no alcance sus metas de desempeño. Este vínculo solo puede ayudar a mejorar el rendimiento con el tiempo.
- El éxito continuo de la empresa: Finalmente, algunos creen que construir y mantener la competitividad ventaja y la producción de aumentos incrementales en los flujos de efectivo y las ganancias por acción son, en sí mismas, medidas indirectas de la eficacia de la gestión de riesgos. Otras medidas tradicionales utilizadas en este sentido incluyen ROI, ROE y valor agregado para los accionistas. Las medidas no financieras útiles incluyen la satisfacción y retención del cliente, la satisfacción de los empleados, el rendimiento del canal, la participación en el mercado y la imagen de marca. Independientemente de las medidas que se utilicen, la empresa debe realizar un seguimiento de su desempeño en relación con sus competidores a lo largo del tiempo. La noción es que si la organización administra sus riesgos de manera efectiva y continúa teniendo éxito en un mercado competitivo, los dos están relacionados. Una vez más, hay otras disciplinas de gestión que contribuyen al éxito de la organización.

---

## HACER QUE SUCEDA

137. ¿Qué es la gestión de viajes y por qué es relevante para la implementación de ERM?

Una vez que la gerencia aprueba la visión, la propuesta de valor y el caso de negocios de ERM, comienza el proceso de implementación de ERM. La implementación de ERM es un viaje. Como con cualquier viaje, el proceso de implementación debe gestionarse. Journey Management organiza las capacidades que definen la solución ERM de la administración en un plan que (1) crea las capacidades necesarias para entregar los resultados deseados y (2) aborda los problemas de gestión de cambios asociados con la ejecución del plan. La gestión del programa (como se analiza en la Pregunta 138) destila el plan de gestión del viaje en un plan de proyecto más granular que diseña e implementa las capacidades de ERM que la gestión decide construir y mejorar. La gestión de viajes proporciona a los patrocinadores una visión de alto nivel en un momento determinado de hacia dónde se dirige el programa ERM. La gestión del programa desglosa el programa para asignar responsabilidades y monitorear la ejecución.

El proceso de gestión del recorrido resume el recorrido de ERM tal como la administración decide definirlo. Debido a que la solución ERM de cada organización es única, el proceso de gestión de viajes también es único. Un plan personalizado de gestión del viaje de ERM identifica, prioriza y secuencia el esfuerzo general necesario para hacer realidad la solución de ERM.

La visión, las metas y los objetivos de ERM, tal como se describen en el caso de negocio, articulan el estado futuro deseado. El plan de gestión del viaje describe cómo se logrará esa visión y las metas y objetivos relacionados con el tiempo. Como un plan de alto nivel, organiza las capacidades de la solución ERM seleccionadas por la administración en un plan secuenciado lógicamente con hitos y puntos de control específicos. La gerencia usa este plan para evaluar el progreso del viaje y, si es necesario, perfeccionar periódicamente la definición del viaje.

Se deben considerar muchos factores clave al organizar el viaje de ERM. Los siguientes son ejemplos:

- Expectativas del patrocinador: ¿Qué quieren los patrocinadores en términos de resultados comerciales? ¿Qué esperan con respecto a beneficios, inversiones, relaciones laborales y protocolo? ¿Cuál es el momento de esas expectativas?

- Problemas de preparación para el cambio: el cambio debe comenzar en la parte superior y descender en cascada hacia la organización. Los patrocinadores internos y personas influyentes del viaje de ERM de una organización y las relaciones entre ellos deben perfilarse y comprenderse para planificar el alcance del viaje y sus objetivos y las comunicaciones relacionadas con la organización. Los roles y expectativas de las partes interesadas brindan un contexto para que los patrocinadores comiencen a pensar en los problemas de preparación para el cambio. Un plan de habilitación de cambios es una parte integral de la gestión del viaje y proporciona una base para que los patrocinadores involucren a las partes interesadas clave en toda la organización.
- Riesgos y restricciones del viaje: los patrocinadores deben comprender los factores de riesgo y las restricciones organizacionales que podrían impedir el progreso del viaje. Estos riesgos y limitaciones requieren una cuidadosa consideración y seguimiento. Proporcionan información para el plan de gestión de viajes. Dado que las organizaciones son dinámicas, se puede esperar que estos riesgos y limitaciones cambien con el tiempo. Por lo tanto, la evaluación de la gerencia sobre ellos debe actualizarse periódicamente a medida que la organización alcanza hitos y comienza nuevas iniciativas.
- Plan de comunicaciones del viaje: las comunicaciones no deben ser ad hoc. El equipo de alta dirección debe respaldar y apoyar visiblemente el proceso de cambio en los puntos de control clave de la implementación. Se necesita un plan bien articulado para delinejar cómo sucederá esto. Ese plan debe abordar las principales actividades específicas del viaje y las capacidades previstas. Además de abordar los riesgos clave del viaje, el plan debe designar a las personas que se espera que desempeñen los roles necesarios y sus respectivas responsabilidades.
- Plan de coordinación del viaje: este plan define la posición de la dirección ejecutiva sobre cómo se planificará y gestionará el viaje del cambio, teniendo en cuenta el alcance, la naturaleza y el momento de las capacidades de ERM planificadas y el cambio esperado. El plan consta de pautas de viaje y un mapa de viaje que coordinan todas las actividades planificadas para que estén alineadas con el caso de negocios y dirigidas hacia el logro de la visión, las metas y los objetivos de la gestión de riesgos.
- Evaluación del desempeño del viaje: Durante el ciclo de vida del viaje, los diversos programas y proyectos planificados deben ser monitoreados y evaluados. Los hitos del viaje designados, los objetivos de desempeño y las medidas brindan un contexto para monitorear el desempeño para que los patrocinadores de ERM puedan determinar si el viaje de cambio está logrando los resultados esperados y, de no ser así, por qué no. Los puntos de control de gestión periódicos también brindan a los patrocinadores la oportunidad de reafirmar el compromiso de mantener el viaje y lograr los objetivos de rendimiento esperados.
- Análisis del impacto del viaje: con el tiempo, los patrocinadores necesitan conocer el impacto del esfuerzo, el ritmo, el tiempo y el enfoque del cambio en la organización y los riesgos, si los hubiera. Con base en su comprensión, los patrocinadores evalúan las acciones inmediatas a tomar, tales como más evaluaciones, comunicaciones, intervenciones y direcciones alternativas a tomar. Se debe actualizar periódicamente una evaluación de impacto a lo largo del ciclo de vida del viaje y se deben tomar acciones preventivas, si es necesario, para reposicionar el viaje de ERM hacia el éxito.
- Secuencia de capacidad de solución: Recomendamos seguir la secuencia de implementación seleccionada primero las capacidades básicas, luego se continúa con la creación de capacidades de gestión de riesgos apropiadas para los riesgos prioritarios y se concluye con la implementación de mejoras seleccionadas a esas capacidades a lo largo del tiempo.

La gestión eficaz del viaje proporciona a los patrocinadores de soluciones la seguridad de que el viaje de ERM se gestiona de forma eficaz. Asegura que dentro de la organización se logre la propiedad, el patrocinio, el compromiso y el liderazgo apropiados para el proceso de cambio. Lo que es más importante, determina que las expectativas del patrocinador y de las partes interesadas se cumplan o superen. El éxito del viaje de ERM está indisolublemente ligado a la capacidad de los patrocinadores para mantener el apoyo de los altos ejecutivos. Ese apoyo continuo brinda impulso para implementar las capacidades adicionales de la solución ERM necesarias para realizar completamente la visión ERM de la administración. Eso solo sucederá si los líderes de la organización están preparados para sostener el viaje de ERM.

Debido a que están interrelacionados, el caso de negocios y el plan de gestión de viajes pueden desarrollarse simultáneamente. El viaje de ERM se centra en la visión, las metas y los objetivos compartidos articulados por el caso de negocio. Además, el viaje está sujeto a cambios. Por ejemplo, el plan de gestión de viajes está expuesto, en todo momento, a los efectos de los cambios en las fuerzas externas e internas sobre los requisitos comerciales y el impacto relacionado en el caso comercial de ERM. En consecuencia, los patrocinadores deben anticipar y acomodar posibles modificaciones al plan de gestión del viaje con planificación proactiva, comunicaciones efectivas, metodologías de diseño flexibles y evaluación periódica del viaje.

138. ¿Qué es la gestión de programas y por qué es relevante para la implementación de ERM?

Para algunas empresas, la implementación de ERM puede ser un proyecto relativamente sencillo. Por otro lado, ERM se logra en etapas en forma de múltiples proyectos relacionados. A ser implementado estos proyectos requieren un enfoque disciplinado y metódico. ¿Cómo sabe la gerencia que los entregables y las capacidades del proyecto relacionado están todos trabajando juntos al unísono para lograr los objetivos finales y objetivos de la visión de ERM de la gerencia? Para soluciones ERM simples, la respuesta puede ser obvia. Para soluciones más complejas, se necesita una disciplina de gestión de programas.

La gestión del programa proporciona la supervisión y la disciplina necesarias para garantizar una integración y una coordinación de múltiples proyectos durante el ciclo de vida del viaje de ERM. Bajo la dirección de la oficina del programa, se utilizan procesos, procedimientos, técnicas y herramientas apropiados para (1) planificar y organizar el trabajo y (2) gestionar la entrega de la solución ERM planificada a lo largo del tiempo. Si bien el CRO puede proporcionar esta supervisión, un La oficina del programa puede ayudar al CRO a administrar la gran cantidad de detalles relacionados con el diseño y la implementación. proceso. Por lo tanto, la oficina del programa puede informar al CRO (o a un ejecutivo equivalente). El objetivo es apoyar el diseño y la implementación de las capacidades que entregan los resultados previstos por el solución ERM de la organización.

La oficina del programa convierte el plan de gestión de viajes, como se analiza en la pregunta 137, en una secuencia lógica, proyectos discretos que construyen las capacidades necesarias para hacer realidad la meta y la visión del estado futuro de la organización. Una vez que se establecen las líneas generales del viaje de ERM en el plan de gestión del viaje, la gestión del proyecto se necesita disciplina si hay múltiples capacidades de solución que requieren múltiples proyectos. Cuanto más complejo sea el esfuerzo, es más probable que se necesite una función de gestión del programa. Si el viaje de ERM se compone de múltiples proyectos relacionados, estos proyectos deben trabajar al unísono e integrarse de manera efectiva para lograr el ERM de la gerencia visión, metas y objetivos. Dependiendo de la complejidad de la solución ERM de la gerencia, el viaje podría incluso constar de dos o más programas discretos, y cada programa consta de múltiples proyectos.

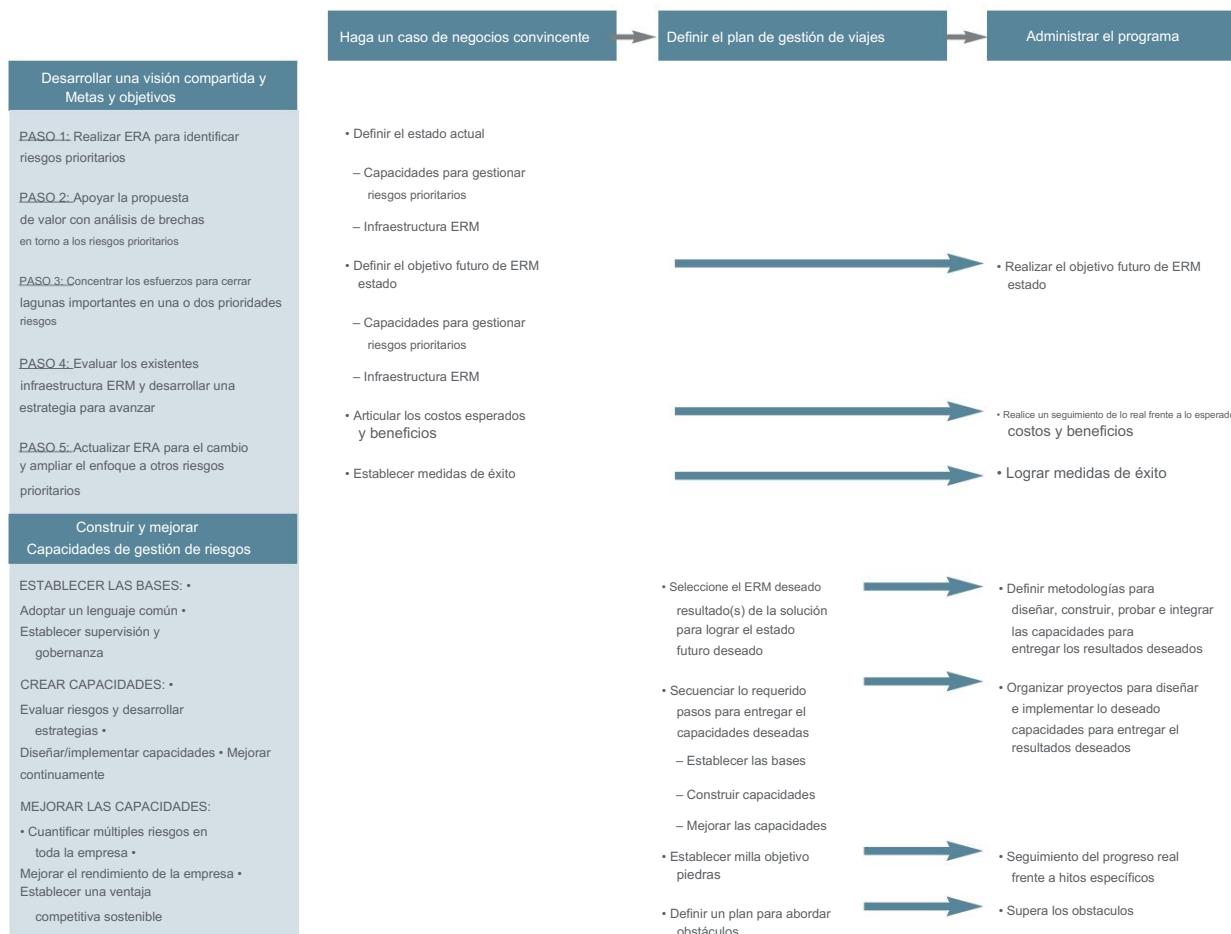
Mientras que el plan de gestión de viajes es estratégico y visionario, la gestión de programas es táctica. El proceso de gestión del programa, entre otras cosas:

- Apoya una evaluación continua del estado del programa y del proyecto, los riesgos y limitaciones del proyecto, el capacidades del proyecto y la eficacia de las actividades de habilitación del cambio.
- Establece las metodologías mediante las cuales se diseñan las capacidades que brindan los resultados de la solución ERM, construido, probado e implementado a través de múltiples iniciativas y proyectos.
- Hace operativa la visión de ERM de la gerencia al transformarla en un programa bien definido de sino proyectos integrados que están organizados y secuenciados de la manera más efectiva para maximizar el posibilidades de éxito frente a hitos y puntos de control establecidos.
- Determina que los diversos proyectos cuentan con los recursos adecuados en el momento adecuado.
- Realiza un seguimiento del progreso con respecto a los hitos establecidos y asegura que se tomen las medidas correctivas apropiadas, si es necesario. • Informa sobre el estado de implementación a los patrocinadores, la gerencia y la junta.

Se utilizan procesos, procedimientos, técnicas y herramientas apropiados para planificar y organizar el trabajo, y para gestionar la entrega de la solución ERM que obtendrá los beneficios establecidos en el caso de negocio.

El siguiente resumen ilustra cómo el caso de negocios de ERM de la gerencia, la gestión del viaje de ERM

La gestión de planes y programas está interrelacionada:



La oficina del programa también puede funcionar en una capacidad de mejora continua una vez que la solución ERM esté en funcionamiento. Lugar. Cuando surgen brechas en la infraestructura de ERM y en las capacidades para administrar los riesgos prioritarios, los planes de acción deben desarrollarse para implementar las mejoras necesarias. Estos esfuerzos de mejora deben priorizarse e incorporado en el proceso de planificación empresarial. Para brechas serias y otros problemas, la situación debe ser bajo control en el momento oportuno. Los propietarios de procesos y riesgos responsables ejecutan planes de acción en acuerdo con los plazos establecidos. La oficina del programa supervisa la ejecución de estos planes de acción y asegura que las unidades de aseguramiento, como la auditoría interna, estén satisfechas de que los planes de acción se lleven a cabo efectivamente. La oficina del programa informa el estado de implementación a la gerencia ejecutiva y al directorio.

La disciplina de gestión de programas es vital para implementaciones más complejas. ERM puede representar potencialmente un cambio radical en la actitud y el comportamiento de la organización. Como con cualquier cambio significativo, la adopción de ERM es fundamentalmente un proceso de creación de conciencia, desarrollo de compromiso y, en última instancia, impulsar la aceptación de propiedad en toda la organización a los gerentes apropiados. La habilitación del cambio es, por lo tanto, un aspecto significativo de una iniciativa de ERM porque la perspectiva de todos sobre el riesgo puede variar significativamente.

El viaje de ERM es un proceso de crecimiento que lleva a la empresa a mejorar sus capacidades de gestión de riesgos. Como navega su viaje de ERM, la organización se vuelve más sensible a los cambios en el entorno y dentro de sus procesos de negocio. Esta sensibilidad en la cultura es importante porque las oportunidades y los riesgos continúan aflorando y cambiando rápidamente en la economía global. Desarrollando así un sistema eficaz en toda la empresa visión de la gestión de riesgos empresariales siempre será un viaje de aprendizaje y mejora continua.

139. ¿Cómo podemos evaluar cuantitativa y cualitativamente los beneficios de implementar ERM en términos de mejorar el rendimiento?

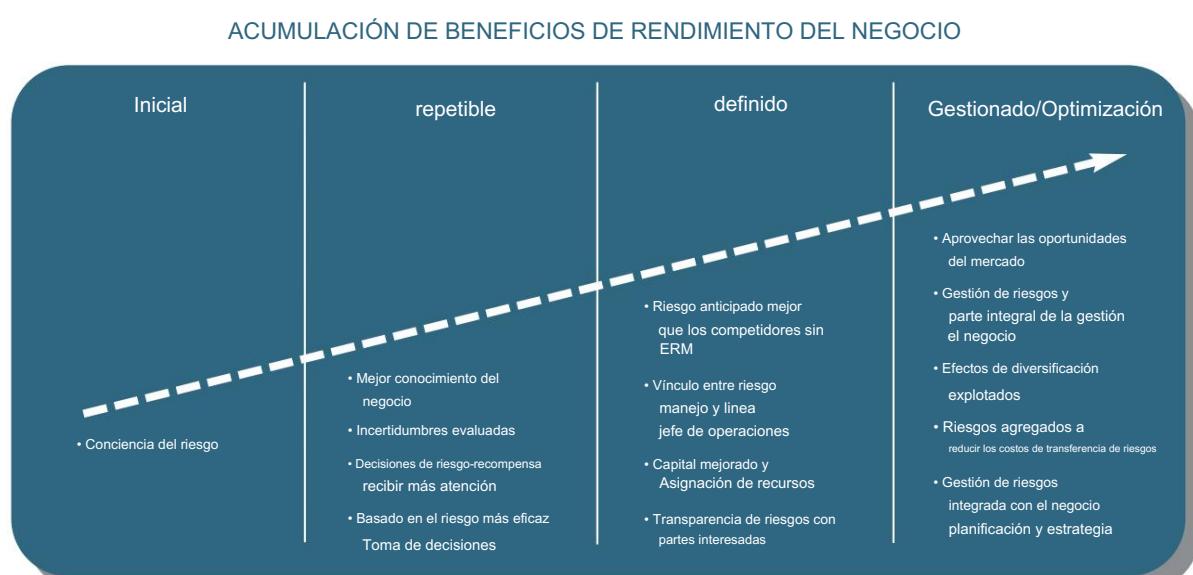
Para aquellos riesgos en los que la gerencia ha optado por alcanzar un estado "gestionado" u "optimizado" en el modelo de madurez de capacidad, hay tres pasos para mejorar las capacidades. Estos pasos son cuantificar el riesgo en toda la empresa, mejorar el rendimiento de la empresa y establecer una ventaja competitiva sostenible. Estos capacidades concluyen la progresión hacia una solución ERM. Las capacidades mejoradas proporcionan información sobre la dirección final del viaje ERM.

El modelo de madurez de la capacidad ilustra cómo mejorar las capacidades de gestión de riesgos requiere la adopción de nuevas prácticas de gestión de riesgos a lo largo del tiempo:



La implementación de una solución ERM no es algo que ocurra de la noche a la mañana. El continuo ilustra la progresión necesaria para mejorar las capacidades de gestión de riesgos a lo largo del tiempo.

Los beneficios de ERM también se acumulan a medida que se mejoran las capacidades de gestión de riesgos, dándose cuenta plenamente del valor propuesta articulada en el caso de negocio:



140. ¿Cómo se gestiona la implementación del ERM?

El patrocinador de ERM debe realizar un seguimiento del progreso a lo largo del tiempo para asegurarse de que el proceso de implementación va por buen camino con Expectativas. Cuatro cosas hacen posible este seguimiento:

- Primero, el patrocinador debe asegurarse de que el proceso de implementación se centre en las cosas correctas mediante el uso de un análisis de brechas en torno a las capacidades para gestionar los riesgos prioritarios de la empresa. Integración de la gestión de riesgos actividades con la ejecución de la estrategia empresarial ayuda a asegurar el enfoque adecuado. Consulte la pregunta 85. • En segundo lugar, el patrocinador debe insistir en tener un plan que describa actividades discretas secuenciadas lógicamente para construir las capacidades deseadas por la gerencia y definir los hitos y puntos de control para monitorear progreso con el tiempo. Consulte las Preguntas 137 y 138. •
- Tercero, el patrocinador debe monitorear la ejecución del plan contra los hitos establecidos y puntos de control Consulte la Pregunta 138. • Finalmente, el patrocinador debe evaluar los beneficios de ERM contra los beneficios esperados articulados en el caso de negocios. Consulte las preguntas 134 y 136.

141. ¿Cómo sabemos cuándo hemos terminado?

La implementación de ERM se completa cuando el plan de implementación se ejecuta por completo y el se realizan los beneficios articulados en el caso de negocio. Como se discutió más adelante en la pregunta 138, el programa La oficina de administración proporciona la supervisión necesaria para llevar el esfuerzo al cierre. El director general y ejecutivo El comité también proporciona supervisión.

142. Dado que tenemos tantas otras cosas en marcha, ¿cómo podemos asumir algo como ERM? ¿implementación?

Este es un problema de priorización que comienza en la parte superior de la organización. En última instancia, el director general y el consejo de administración los directores deben decidir lo que es importante. Como hemos señalado a lo largo de esta publicación, la integración es un tema efectivo al implementar ERM, por ejemplo, integración con planificación comercial, gestión estratégica, Six Sigma, gestión de asignación de capital, gestión de I+D, marketing y desarrollo empresarial, etc. Por lo tanto, en lugar de crear un apéndice, el énfasis está en integrar mejoras en la gestión de riesgos en la estructura y los procesos de gestión existentes.

143. ¿Qué estándares deben usar las empresas para evaluar su enfoque de ERM?

COSO proporcionó criterios amplios para guiar a las organizaciones, públicas y privadas, grandes y pequeñas, con y sin fines de lucro, y evitó un enfoque único para todos. Los "estándares" se encuentran dentro de los objetivos de la organización. y se ven afectados por la aplicación de los componentes del marco COSO. La definición de ERM proporcionada por COSO proporciona puntos clave de enfoque para que las organizaciones los aborden. Es razonable esperar que más explícito Los estándares o ejemplos de "mejores prácticas" pueden surgir dentro de diferentes sectores industriales a medida que se gana experiencia. aplicando el marco COSO.

144. ¿Hay algún peligro que se deba evitar al implementar un enfoque de ERM?

El escollo principal que se debe evitar es no comprender el propósito de la implementación de ERM. No es inusual para empresas para consultar o incluso proceder con la implementación de ERM sin comprender el problema están tratando de resolver. La falta de clarificación de la propuesta de valor conduce en última instancia a la frustración cuando los costos duros se incurre para obtener beneficios que se perciben como blandos. La falta de aclaración del propósito de ERM conduce a búsquedas interminables de soluciones únicas para todos, actividades de implementación innecesarias y falsos comienzos.

Hay otras trampas que se deben evitar al implementar ERM. A continuación enumeramos diez de ellos:

- Falta de apoyo desde arriba: Establecer la propiedad de ERM (en lugar de hablar de boca para afuera) en el nivel más alto de la organización es fundamental. Sin el apoyo y compromiso del CEO y del directorio, ERM no se puede implementar de manera efectiva. La falta de apoyo se manifiesta en una serie de

maneras, por ejemplo, ERM no se ve como una prioridad, la ausencia de una visión compartida y un caso de negocios convincente, la falta de compromiso por parte del CEO, los esfuerzos serios pero infructuosos de la gerencia de nivel inferior para vender ERM al alza, la falta de presencia de la alta gerencia en reuniones de estado, etc. El compromiso desde arriba es donde todo comienza. Sin ella, se pierde impulso, el proyecto se desenfoca y la iniciativa se estanca. • Falta de apropiación y aceptación por parte de las partes interesadas: la apropiación y el compromiso de las partes interesadas clave son vitales para el éxito de la implementación de ERM. Si no se presta la atención adecuada a la gestión del cambio y a mantener a las personas comprometidas y no hay métricas de rendimiento que impulsen el proceso de implementación, la iniciativa fracasará.

- Falta de integración de ERM con lo que importa: Si hay intentos de implementar ERM sin un comprensión de los generadores de valor y los problemas comerciales en la pantalla del CEO, la implementación de ERM no tendrá éxito. La vinculación con los temas comerciales en la agenda de la dirección ejecutiva es vital para el éxito. Una evaluación de riesgos empresariales con la estrategia comercial como contexto es una excelente manera de comenzar este vínculo. Cuando la evaluación de riesgos de la empresa es seguida por respuestas de riesgo enfocadas que abordan los riesgos prioritarios utilizando la estrategia comercial como contexto, la iniciativa ERM se vincula de manera más efectiva con los generadores de valor del negocio. Este vínculo aumenta el énfasis en mejorar las métricas, las medidas y el seguimiento. A menos que se integre con procesos ya institucionalizados en la organización, la ERM a menudo se considera un apéndice. La gestión estratégica, la planificación empresarial, la gestión del rendimiento, los gastos de capital, la gestión de la calidad, el cumplimiento de Sarbanes-Oxley y otras formas de gestión del cumplimiento son ejemplos de procesos ya existentes que la dirección puede optar por integrar con ERM. • Sumergirse en los detalles: cuando los patrocinadores de ERM permiten que la implementación se deteriore hasta el punto en que las evaluaciones de riesgo se atascan en los procesos de negocios o donde la gerencia debe sortear largas listas de factores de riesgo, el proceso de implementación tiene problemas. COSO afirmó que ERM debe aplicarse en toda la empresa, no a nivel de proceso. COSO también afirmó que ERM debe aplicarse en el establecimiento de estrategias, por lo que el proceso de evaluación debe centrarse en los problemas del "panorama general" para retener la confianza y la capacidad de atención de la gerencia operativa y senior. • Falta de definición de roles y responsabilidades: Clarificar roles y responsabilidades siempre ha sido un desafío en la gestión de riesgos y lo es particularmente con ERM. Debido a que los enfoques actuales de gestión de riesgos están demasiado arraigados en la era de comando y control, a menudo conducen a un comportamiento de silo que genera brechas (ningún propietario de un riesgo) y superposiciones (demasiados propietarios de un riesgo) con el tiempo.
- Falta de consideración de las cuestiones culturales: ERM es un cambio cultural. Los problemas asociados con la cultura y el impacto de la conciencia del riesgo y la sensibilidad al riesgo de la organización en el comportamiento se analizan en nuestra respuesta a la Pregunta 102. Si bien esta área a menudo se considera un "beneficio indirecto", no obstante es importante.
- Falta de equilibrio entre las actividades de creación de mercado y de control: el resultado rara vez es bueno cuando el las actividades empresariales y los mecanismos de control de una organización están desequilibrados. La búsqueda desenfrenada de oportunidades para crear valor empresarial sin establecer límites razonables a través de controles y equilibrios puede tener consecuencias desastrosas. La oscilación del péndulo hasta el comportamiento de aversión al riesgo puede conducir a un desempeño deficiente en relación con los competidores. El objetivo final de la estructura de supervisión es brindar seguridad a la junta directiva y al director general de que las actividades empresariales del negocio y las actividades de control del negocio están razonablemente equilibradas para que se entiendan y gestionen los riesgos inherentes al comportamiento de búsqueda de oportunidades. Consulte nuestra respuesta a la pregunta 53 para obtener más información.
- Fracaso en el manejo de conflictos de intereses: Los conflictos de intereses crean desafíos porque el típico La estructura de control interno se basa en la presunción de que las partes independientes operan en condiciones de plena competencia entre sí. Si eso no sucede, ya sea por la existencia de partes relacionadas o por una renuncia o violación de la política de "conflicto de intereses" de la entidad, pueden surgir problemas significativos. Depende de la junta garantizar que se lleve a cabo un comportamiento empresarial responsable en la organización.
- No aplicar el enfoque ERM de la gerencia en toda la empresa: como lo define COSO, la gerencia no puede implementar ERM a menos que se aplique en toda la empresa (o en una unidad operativa específica). La aplicación desigual generalmente conduce a la transparencia en algunas partes de la organización y la oscuridad en otras partes de la organización. Llámalo como quieras, pero no es ERM como lo define COSO.

- Adelantarse a las capacidades de la empresa: ERM no se trata de implementar las más sofisticadas técnicas. Es un enfoque progresivo para implementar los ocho componentes del marco COSO para abordar los riesgos prioritarios de la organización. Las entidades a menudo se ven tentadas a implementar capacidades mejoradas (como se describe en la Pregunta 125) antes de haber establecido la base adecuada (como se describe en la Pregunta 96) y construido capacidades básicas de gestión de riesgos (como se describe en la Pregunta 103). O empiezan a desarrollar capacidades antes de haber sentado las bases. En otras palabras, se adelantan a sí mismos, a menudo buscando la "solución rápida". A menudo, no funciona y conduce al desperdicio.

---

## RELEVANCIA PARA EL CUMPLIMIENTO DE SARBANES-OXLEY

145. ¿La Ley Sarbanes-Oxley de 2002 (SOA) exige que las empresas adopten ERM? ¿Existen otras leyes y reglamentos que obliguen a ERM?

No, SOA no exige ERM. Hasta donde sabemos, no existen leyes ni reglamentos específicos que exijan ERM. Sin embargo, la implementación de ERM facilitaría el cumplimiento de las leyes y reglamentos aplicables, incluida SOA.

146. ¿Puede ERM ayudar a los funcionarios certificadores con el cumplimiento de sus responsabilidades de certificación de la Sección 302 de la SOA y de evaluación de la Sección 404?

Mucho después de que se completen los proyectos para implementar los requisitos de Sarbanes-Oxley, los funcionarios certificadores deben evitar que el proceso de divulgación se estanque. La gestión de riesgos en toda la empresa sacará a la luz riesgos nuevos y emergentes para una acción y divulgación oportunas. Por lo tanto, ERM ayudará a los funcionarios certificadores con el cumplimiento de sus responsabilidades de certificación trimestral de la Sección 302 de la SOA y de evaluación anual de la Sección 404.

147. ¿Cómo se relaciona ERM con el cumplimiento de SOA?

Si bien los esfuerzos de cumplimiento de SOA son de vital importancia, necesarios y valiosos, ERM es más amplio. Si bien el cumplimiento de SOA se centra en informes financieros y públicos fiables, así como en otros aspectos de la gobernanza para restaurar la confianza de los inversores en los mercados de capitales, ERM aborda el espectro completo de riesgos que enfrenta la organización, incluidos los riesgos asociados con los informes estratégicos, operativos, internos y otros. objetivos de cumplimiento. La mayoría de las empresas públicas en los Estados Unidos utilizan el Marco Integrado de Control Interno para facilitar su cumplimiento con la Sección 404. El Marco Integrado de Gestión de Riesgo Empresarial es más amplio que el marco de control interno y abarca ese marco.

Debido a que tanto la SEC como la PCAOB han respaldado un enfoque basado en el riesgo para evaluar el control interno sobre los informes financieros de acuerdo con la Sección 404, ERM puede brindar beneficios desde el punto de vista del cumplimiento de SOA. ERM ayuda a las empresas a mantener actualizado su proceso de divulgación a través de una cadena de responsabilidad basada en procesos que involucra a los gerentes de unidad y propietarios de procesos en la comunicación de problemas que requieren acción y posible divulgación. Más importante aún, un enfoque en la eficiencia y eficacia operativa con énfasis en aumentar la calidad, comprimir el tiempo y reducir los costos mientras se controla simultáneamente el riesgo de la información financiera dará como resultado un mayor énfasis en los controles automatizados (frente a los controles manuales ad hoc) y controles preventivos (frente a los costosos "buscar". y arreglar" controles de detección). ERM brinda a los ejecutivos y directores más confianza en que la estructura de control interno es sostenible en tiempos de cambios significativos. Un proceso ERM efectivo también brinda a los ejecutivos y directores una mayor confianza en que sus organizaciones están identificando y administrando todas las oportunidades y riesgos comerciales potencialmente significativos.

148. ¿Debe una decisión de implementar ERM considerar el esfuerzo para cumplir con SOA?

ERM apoya y se basa en los esfuerzos de cumplimiento de Sarbanes-Oxley. Si bien ERM puede mejorar la calidad de los informes internos y externos, la integridad en los informes es un requisito previo, no un resultado de ERM. Un compromiso completo y honesto con la presentación de informes justos y veraces, que es el objetivo principal de SOA, revela los signos vitales del cambio, que la administración debe tener en cuenta al evaluar si las estrategias y los objetivos se mantienen.

orientada al mercado, orientada al cliente y competitiva. Una organización no puede gestionar eficazmente sus riesgos cuando suprime información sobre las realidades empresariales.

ERM se enfoca en el riesgo comercial y los controles internos con el objetivo de preservar y crear valor empresarial. ERM alinea estrategia, personas, procesos, tecnología y conocimiento. El énfasis está en la estrategia. Y la aplicación es para toda la empresa. Al administrar los riesgos estratégicamente en toda la empresa, una organización no solo respalda el cumplimiento de Sarbanes-Oxley, sino que también saca a la luz nuevos riesgos a medida que surgen. La transparencia no es solo el nombre del juego, es vital para mantener el cumplimiento de SOA. Si bien no hay duda de que el proceso de divulgación es fundamental, también lo es el proceso de gestión de otros riesgos comerciales. ERM inculca la disciplina necesaria para mejorar continuamente las capacidades de gestión de riesgos, incluidos los riesgos de información financiera.

149. ¿Debería la administración ampliar el enfoque en el cumplimiento para administrar el riesgo comercial?

La respuesta corta es sí." La gestión del riesgo tiene que ver con la gestión de la empresa. El marco COSO sugiere que la administración debe aprovechar la oportunidad de utilizar el marco ERM para construir sobre la base establecida por el cumplimiento de SOA y evaluar si existen oportunidades para mejorar la gestión de riesgos de la organización. Las siguientes son las razones por las cuales:

- El cumplimiento de Sarbanes-Oxley sienta las bases para implementar una infraestructura de ERM que antes no existía para muchas empresas. Aquellas empresas que han implementado procesos mejorados de divulgación y control interno sobre los informes financieros deben analizar más de cerca cómo pueden expandir estas capacidades para abarcar TODAS las actividades comerciales para que tanto los ejecutivos como los directores puedan tener una mayor confianza en que sus organizaciones están identificando y administrando TODAS las actividades potencialmente importantes oportunidades y riesgos comerciales.
- Las empresas exitosas asumen riesgos cuando buscan nuevas oportunidades. Los riesgos cambian constantemente en el mercado global, ya sea que las organizaciones decidan hacer algo para administrarlos o no. A medida que los ejecutivos examinan los riesgos que enfrentan sus empresas hoy en día, verán un perfil diferente al que existía hace incluso unos años. Y, lo que es más importante, pueden esperar ver incluso riesgos diferentes dentro de unos años. El ritmo del cambio y la creciente complejidad de los negocios elevan continuamente el listón de la gestión de riesgos.
- Un enfoque de toda la empresa implementado de manera efectiva para evaluar y administrar el riesgo hará que los riesgos salgan a la superficie más oportuno para que los tomadores de decisiones consideren acciones alternativas y divulgaciones requeridas. ERM ayudará a la organización a crear y proteger el valor empresarial, así como a equipar mejor a la administración para comunicar en un foro público cuáles son los riesgos de la empresa y con qué eficacia se gestionan.

Los gerentes deben tener una comprensión más completa de los riesgos críticos que enfrentan y, más específicamente, la efectividad de las estrategias y capacidades que sus organizaciones tienen para responder a esos riesgos.

150. Como empresa pública, ¿por qué queríamos asumir ERM inmediatamente después del cumplimiento de la Sección 404?

Hablamos de la propuesta de valor de ERM en nuestra respuesta a la Pregunta 4. ERM ayuda a la gerencia a establecer una ventaja competitiva sostenible, optimizar los costos de gestión de riesgos y mejorar el desempeño comercial. El cumplimiento de la Sección 404 requiere la implementación de un proceso continuo para abordar el riesgo de información financiera. Debido a que la mayoría de las empresas utilizan el Control interno de COSO: marco integrado como criterio para cumplir con la Sección 404, muchos elementos del proceso de cumplimiento de la Sección 404 también se aplican a la implementación de ERM. Por lo tanto, el cumplimiento de la Sección 404 proporciona una base para implementar ERM.

A medida que las empresas implementan procesos de autoevaluación para reducir la responsabilidad a los propietarios de procesos (consulte la Pregunta 151) e integran las actividades de cumplimiento de la Sección 302 y la Sección 404 (consulte la Pregunta 152), el cumplimiento de SOA adopta una apariencia más similar a la de ERM. A medida que las empresas amplían el enfoque de cumplimiento a otras leyes y reglamentaciones aplicables (consulte la Pregunta 153), el resultado es la implementación del marco COSO al objetivo de cumplimiento, uno de los cuatro objetivos del marco. A medida que el enfoque se amplía para mejorar la calidad, comprimir el tiempo y reducir el costo de los procesos que alimentan los informes financieros (consulte la Pregunta 154), el resultado es una expansión a la eficacia y eficiencia operativas, otro objetivo del marco COSO. Por lo tanto, todos estos pasos se construyen lógicamente sobre la base establecida por el cumplimiento de SOA.

Si bien no todas las organizaciones comienzan su evolución hacia ERM con el cumplimiento de la Sección 404, la mayoría de las empresas públicas en los Estados Unidos, de hecho, lo hacen porque (1) la inversión inicial en cumplimiento es significativa y (2) una empresa no puede tener un gobierno corporativo sólido sin transparencia en las finanzas. Por lo tanto, un enfoque en informes financieros confiables es una buena base sobre la cual construir capacidades de ERM. El cumplimiento de SOA sienta las bases, en esencia, proporcionando un marco para gestionar otros riesgos en toda la empresa. Por ejemplo, requiere un lenguaje común, una evaluación de riesgos, una evaluación de la eficacia del diseño de los controles internos existentes, la validación de la eficacia operativa de esos controles, así como un seguimiento eficaz. Estos elementos (lenguaje común, evaluar el riesgo, evaluar el diseño, validar la operación y monitorear) son elementos que se pueden aplicar a otros riesgos. La adición de la autoevaluación, la existencia de un comité de divulgación (de acuerdo con la Sección 302) y la participación de la alta dirección son elementos adicionales.

Ya sea que una organización comience su viaje de ERM con el cumplimiento de SOA, con uno o dos riesgos financieros u operativos prioritarios, o con algún otro riesgo prioritario, el enfoque de la infraestructura de ERM es el mismo, es decir, avanzar en la madurez de las capacidades de gestión de riesgos para la organización. riesgos prioritarios. Cualquiera que sea el punto de partida, existen cinco pasos para que las organizaciones decidan ampliar su enfoque a ERM:

- (a) Llevar a cabo una evaluación de riesgos corporativos para identificar y priorizar los riesgos críticos de la organización. Este paso proporciona un contexto para realizar un análisis de brechas de las capacidades actuales y deseadas en torno a la gestión de los riesgos clave. Consulte las preguntas 69 a 84.
- (b) Articular la visión de la gestión de riesgos (consulte la Pregunta 64) y respaldarla con una propuesta de valor convincente (consulte las Preguntas 4 y 134 a 136) utilizando lagunas en torno a los riesgos prioritarios (consulte la Pregunta 111). Este paso proporciona la justificación económica para seguir adelante.
- (c) Mejorar la capacidad de gestión de riesgos de la organización para uno o dos riesgos críticos, por ejemplo, informes financieros o algún otro riesgo vital. Este paso enfoca a la organización en mejorar su capacidad de gestión de riesgos en un área donde la gerencia sabe que se necesitan mejoras.
- (d) Comprender y evaluar la capacidad de la infraestructura ERM existente y desarrollar una estrategia efectiva para avance. Se espera que el avance de las capacidades en torno a la gestión de uno o dos riesgos críticos requiera cierto nivel de infraestructura, por lo que este paso debe tener en cuenta los avances en la infraestructura de ERM que resultan del paso (3). Los posibles elementos de la infraestructura ERM se ilustran en la Pregunta 37.
- (e) Actualizar la evaluación de los riesgos comerciales de la empresa para el cambio, priorizar los riesgos clave adicionales y desarrollar una estrategia para evaluar y mejorar las capacidades de gestión de riesgos para esos riesgos clave. Este paso comienza con la selección de los riesgos prioritarios y la determinación del estado actual de la capacidad de gestión de riesgos para cada uno de esos riesgos. Una vez que se determina el estado actual para cada uno de los riesgos clave, se evalúa el estado futuro deseado con el objetivo de avanzar en la madurez de las capacidades en torno a la gestión de esos riesgos. Consulte la Pregunta 111 para ver ejemplos que ilustran las capacidades de gestión de riesgos en diferentes etapas de madurez.

Los pasos anteriores proporcionan una vista simplificada de la tarea de implementar ERM. Se analizan con más detalle en la Pregunta 85. Estos pasos permiten que la gestión proceda de manera práctica.

La implementación de ERM no ocurre de la noche a la mañana y, por cierto, no es fácil de lograr. ERM es un viaje. Las siguientes cuatro preguntas brindan comentarios sobre la evolución del cumplimiento de la Sección 404 a ERM, como se describe anteriormente. Este comentario aborda cuatro fases intermedias que ilustran la evolución desde el cumplimiento de la Sección 404 hasta ERM.

**151. ¿Cómo se basa la autoevaluación en el cumplimiento de la Sección 404? ¿Por qué la autoevaluación contribuye a la evolución hacia ERM?**

Debido a que su aplicación suele ser en toda la empresa, la autoevaluación contribuye al tipo de entorno abierto y comunicaciones ascendentes que facilitan la evolución hacia ERM. Si bien no es obligatorio, la autoevaluación es una mejor práctica reconocida y se ha aplicado a los riesgos y controles durante muchos años. Está sancionado por la Junta de Supervisión Contable de Empresas Públicas (PCAOB, por sus siglas en inglés) como una herramienta para el uso de la gerencia, junto con el monitoreo a nivel de entidad y las pruebas independientes de controles, en el desarrollo del cuerpo de evidencia que respalda una

conclusión en cuanto a la eficacia del control interno sobre la información financiera. Mientras que los auditores externos generalmente no puede depender de los resultados de la autoevaluación a los fines del cumplimiento de la Sección 404, la gerencia sí puede. El personal de la PCAOB explicó esta distinción señalando que, al apoyar una conclusión con respecto a la eficacia del control interno sobre la información financiera, la dirección dispone de procedimientos que el auditor no lo hace. La autoevaluación es un ejemplo de lo que estaba hablando el personal.

Aplicada sistemáticamente en toda la organización a nivel de entidad y de proceso, la autoevaluación es un enfoque predeterminado mediante el cual las personas "informadas" autoevalúan sus riesgos y se autorevisan o autoauditan. Los controles de los que son responsables y comunicar los resultados a la dirección correspondiente. En respuesta a los informes ascendentes de las evaluaciones de los propietarios del proceso, se realiza un seguimiento cuando es necesario. Utilizada en combinación con un proceso de monitoreo efectivo a nivel de entidad y pruebas periódicas de controles, la autoevaluación es un elemento poderoso y flexible de un programa de cumplimiento continuo porque permite que la gerencia reciba una declaración integral de que los controles clave están implementados y funcionando de manera efectiva por parte de las personas que están mejor posicionado para saber. Por ejemplo, como el informe de control interno requerido bajo la Sección 404 de SOA proporciona aseveraciones de los oficiales certificadores, un proceso de autoevaluación reporta aseveraciones relevantes de gerentes y propietarios de procesos con respecto a los controles internos de los que son responsables.

La autoevaluación se puede aplicar a muchas áreas de riesgo, incluidos los riesgos operativos y las áreas de cumplimiento, otras que Sarbanes-Oxley. Se presta muy bien a una cultura ERM, porque fomenta un entorno abierto que facilita la comunicación ascendente de evaluaciones, tanto buenas como malas, dentro de la organización. Este es el tipo de cultura que soporta una evolución hacia ERM.

Cuando se aplica a cualquier proceso o a cualquier área de riesgo, un proceso de autoevaluación efectivo aborda los siguientes principios:

- La autoevaluación es una herramienta de gestión que impulsa el "tono en la parte superior" hacia los propietarios de procesos al reforzando su responsabilidad y rendición de cuentas para el control interno sobre la información financiera.
- Porque los dueños del proceso son los hombres y mujeres más cercanos a los puntos críticos de control dentro del organización, ellos son los que saben lo que funciona y lo que no y cuando los cambios de proceso son ocurriendo Reconocen, a menudo antes que nadie, el impacto de los sistemas, la fuerza laboral y otros cambios generalizados en el rendimiento y la capacidad del proceso.
- El proceso de autoevaluación está alineado con funciones, responsabilidades y autoridades definidas en relación con objetivos de negocio y la gestión de los riesgos que afectan a dichos objetivos.
- Es deseable que las autoevaluaciones se completen para muchos, si no todos, los controles primarios de la empresa, es decir, aquellos controles que son especialmente críticos para la mitigación del riesgo y el logro final de uno o más objetivos comerciales. El proceso subyacente, la evaluación de riesgos y otra documentación de gestión. (por ejemplo, como lo requiere el cumplimiento de la Sección 404) establece la línea de base para la autoevaluación continua. Eso La documentación aborda cuestiones como:
  - ¿Cuáles son los controles clave a nivel de entidad y de proceso?
  - ¿Qué riesgos abordan?
  - ¿Quién es el dueño?
  - ¿Cómo se califican en cuanto a la eficacia del diseño? ¿Son adecuados para mitigar los riesgos que están pretendiendo abordar?
  - ¿Cómo se califican en relación con la eficacia operativa? ¿Los resultados de las pruebas proporcionan evidencia de que Están funcionando según lo previsto?

Los controles primarios seleccionados como los más críticos y significativos a los efectos de lograr el negocio establecido los objetivos deben ser el foco de un programa continuo de autoevaluación.

En resumen, la autoevaluación es un proceso versátil que se puede aplicar a TODOS los tipos de riesgos comerciales. Una vez el proceso de autoevaluación está en marcha, infunde disciplina, refuerza la rendición de cuentas y promueve la transparencia, todos los cuales son bloques de construcción importantes hacia ERM.

152. ¿Qué significa integrar el cumplimiento de los artículos 404 y 302? ¿Cómo tal integración se basa en un proceso de autoevaluación establecido y en el cumplimiento de la Sección 404? ¿Por qué dicha integración contribuye a la evolución de una empresa hacia ERM?

Integrar el cumplimiento de la Sección 404 y la Sección 302 es probablemente un punto de enfoque para la mayoría de las empresas después de presentar su primer informe de control interno, porque tiene sentido comercial hacerlo. Lógicamente se basa en un programa efectivo de autoevaluación (ver Pregunta 151). En el futuro, la gerencia debe pensar en el cumplimiento de las Secciones 302 y 404 como un requisito ÚNICO de informes continuos. Las siguientes razones apoyan este punto de vista:

- La certificación ejecutiva 302 de la compañía cambia después de que se emite el primer informe de control interno para incorporar un reconocimiento más explícito de la responsabilidad de la administración por el control interno sobre la información financiera. Por ejemplo, el nuevo lenguaje establece que la administración es responsable de establecer y mantener el control interno sobre los informes financieros. También establece que la administración ha diseñado el control interno sobre la información financiera, o ha hecho que dicho control interno sobre la información financiera se diseñe bajo su supervisión, para brindar una seguridad razonable con respecto a la confiabilidad de la información financiera y la preparación de estados financieros para propósitos externos de acuerdo con principios contables generalmente aceptados.
- Existe una superposición significativa entre los "controles y procedimientos de divulgación" y el "control interno sobre la información financiera", tal como la SEC define los dos términos. Por lo tanto, dado que la Sección 302 y la Sección 404 abordan, en sustancia, políticas y procedimientos similares, la gerencia debe considerar el proceso de cumplimiento como uno continuo.
- Existen interrelaciones importantes entre las Secciones 302 y 404 con respecto a la notificación oportuna de deficiencias significativas en el control interno sobre la información financiera a los auditores y comités de auditoría y la divulgación oportuna de debilidades materiales a los inversionistas. En la certificación ejecutiva trimestral, los oficiales certificadores deben declarar que "han revelado, con base en su evaluación más reciente del control interno sobre la información financiera, a los auditores y al comité de auditoría, todas las deficiencias significativas y debilidades materiales en el diseño u operación de control interno sobre la información financiera que es razonablemente probable que afecte adversamente la capacidad de la empresa para registrar, procesar, resumir y reportar información financiera". Por lo tanto, cuando el personal de la empresa identifique deficiencias relacionadas con el control interno sobre la información financiera, debe escalar estos asuntos de manera oportuna, a través de un proceso sistemático, para permitir que la gerencia considere rápidamente la gravedad potencial y evalúe si la acción específica y la divulgación son apropiadas.
- La certificación ejecutiva trimestral actual ya aborda las implicaciones del cambio en la control sobre los informes financieros. El lenguaje específico en la certificación es el siguiente:

[Los funcionarios certificadores]...han...revelado en el informe cualquier cambio en el control interno del emisor sobre los informes financieros que haya ocurrido durante el trimestre fiscal más reciente del emisor (el cuarto trimestre fiscal en el caso de un informe anual) que haya afectado materialmente, o es razonablemente probable que afecte materialmente el control interno del emisor sobre la información financiera.

Esta representación no solo está en juego para todas las empresas, independientemente de su estado de cumplimiento de la Sección 404, sino que también es una de las principales razones por las que cientos de empresas han revelado problemas relacionados con el control interno durante los meses anteriores a la emisión de su primer informe de control interno.
- Los informes trimestrales son tan importantes como los informes anuales porque las debilidades materiales en el control sobre la información financiera puede surgir de los riesgos de incorrección para ambos. Dado que la administración informa según la Sección 302 trimestralmente y según la Sección 404 anualmente, es importante darse cuenta de que el riesgo de reexpresión se aplica tanto a la información intermedia como a la información anual. Por lo tanto, las empresas deben coordinar su actividad de autoevaluación, monitoreo a nivel de entidad y pruebas de controles independientes con los informes requeridos en las Secciones 302 y 404.

Por lo tanto, en el futuro, muchas empresas deberían pensar en las Secciones 302 y 404 como un proceso de cumplimiento ÚNICO que requiere informes continuos. Este pensamiento da como resultado una "sostenibilidad" mejorada que, desde una SOA

desde el punto de vista del cumplimiento, se refiere a la eficacia continua de dos imperativos de gestión interrelacionados tiempo – (1) la repetibilidad y eficacia de la estructura de control interno, y (2) la rentabilidad de capacidades de cumplimiento SOA de la organización, particularmente con respecto a las Secciones 302 y 404. Simplemente dicho, un enfoque de cumplimiento sostenible es aquel que resistirá el escrutinio a lo largo del tiempo a medida que se produzcan cambios. Mientras el cumplimiento de la Sección 404 durante el primer año es importante; es aún más importante reconocer que la Sección 404 el cumplimiento es continuo. Para muchas empresas, la carga administrativa del año inicial en términos de recursos compromiso y gastos de terceros es inaceptable, por lo que la eficiencia y eficacia está a la orden del día.

Para abordar los problemas interrelacionados de sostenibilidad y eficiencia, muchas empresas abordarán cuatro temas para integrar su cumplimiento con las Secciones 404 y 302 con éxito a lo largo del tiempo:

- Primero, implementar una infraestructura organizacional que facilite el cumplimiento continuo: este tema es discutido en profundidad en el Número 12 del Volumen 1 de The Bulletin de Protiviti , que presenta varias alternativas estructuras para el cumplimiento continuo. Se trata de la transición de “proyecto a proceso” para que el la actividad de cumplimiento es más repetible, claramente definida y mejor gestionada. Se trata de institucionalizar el proceso de cumplimiento a través de:
    - Definir el apoyo de infraestructura del programa en curso y formular un plan a más largo plazo para financiar y presupuestar ese apoyo para que las expectativas y los elementos de acción apropiados se incorporen en el plan de negocios
    - Lograr el compromiso y la aceptación de la gerencia de la unidad, incluida la absorción de los costos del programa en los presupuestos de la unidad
    - Fortalecimiento continuo de los controles a nivel de entidad de la organización, incluido su programa antifraude. y procesos de seguimiento en toda la empresa
    - Remediar las deficiencias de control significativas no resueltas tan pronto como sea posible para que el la infraestructura de cumplimiento se centra en la gestión del cambio en lugar de reparar los problemas de control del año anterior
- Estos pasos requieren una visión empresarial y, por lo tanto, contribuyen a un entorno ERM. • Segundo, establecer la responsabilidad de los propietarios de procesos y otros para el control interno: La Sección 404 la actividad de cumplimiento debe ser impulsada por el propietario del proceso, no por el equipo del proyecto como lo es para la mayoría de las empresas durante el año inicial de cumplimiento. La transición de establecer la rendición de cuentas consiste en impulsar comportamientos deseados a través de:
- Comprensión, aceptación y apropiación de roles y responsabilidades para todos los controles críticos - Definición de metodologías apropiadas e integración en las rutinas comerciales - Articulación de políticas y protocolos de escalamiento, con énfasis en la puntualidad
  - Articular protocolos de remediación y nuevas pruebas, con énfasis en la puntualidad - Desarrollar y brindar orientación, capacitación y apoyo para el propietario del proceso Debido a que aclarar roles y responsabilidades y establecer la rendición de cuentas son vitales para el implementación de ERM, estos pasos contribuyen a la evolución hacia una infraestructura de ERM.
- En tercer lugar, implemente un proceso efectivo de reconocimiento de cambios: para mantener actualizado el proceso de divulgación, los oficiales certificadores necesitan un procedimiento de reconocimiento de cambios que muestre nuevos desarrollos y eventos oportuno para su posterior seguimiento y posible divulgación. Un aspecto importante del reconocimiento del cambio es asegurar que el impacto de los cambios en las políticas, procedimientos y sistemas en la estructura de control interno sea reflejado con precisión en la documentación de los controles para que se puedan realizar actualizaciones en el diseño de los controles evaluación de la eficacia y al plan de pruebas para evaluar la eficacia operativa de los controles. Este tema particular impulsa la transición de la empresa de la documentación inicial en el primer año a un proceso continuo de gestión de documentos. Los pasos que debe tomar la gerencia incluyen:
    - Articular y comunicar responsabilidades para identificar y reportar cambios a tiempo.
    - Establecimiento de protocolos para la actualización de la documentación de controles para el cambio.

- Examinar el desempeño del comité de divulgación frente a los estatutos
- El reconocimiento y la creación de sensibilidad al cambio es de lo que se trata ERM
- Cuarto, identifique y aproveche las oportunidades de mejora adicionales: este tema trata sobre Pasar en un período de tiempo razonable de una dependencia excesiva de los controles manuales y de detección a una combinación adecuada de controles automatizados y preventivos. Incluye la transición de la integral pruebas a pruebas dirigidas como resultado de la mejora del "filtrado" de los controles. Este tema también se trata en gran medida de problemas de alineación y eficiencia, y buscando oportunidades para la transición de los "costos impredecibles" entorno del primer año a un entorno de "costos gestionados" en el futuro. En efecto, este tema es sobre tres cosas: (1) lograr valor agregado al mejorar la calidad, el tiempo y el desempeño de costos de procesos de información financiera, (2) mejorar la sostenibilidad de la estructura de control interno y (3) mejorar la rentabilidad del proceso de cumplimiento haciéndolo basado en el riesgo y de arriba hacia abajo. Este tema incluye, entre otras cosas, lo siguiente:
  - Optimización de los planes de prueba, incluida la selección, el alcance, el tiempo, la remediación, la repetición de la prueba y la prueba de actualización así como la integración efectiva de pruebas de controles independientes con autoevaluación y nivel de entidad y monitoreo a nivel de proceso
  - Decidir una estrategia de depósito de datos a largo plazo, incluida la comprensión y selección de un solución tecnológica de punto o plataforma para lograr eficiencia y eficacia en la documentación, actualización y archivar la documentación de control interno
  - Definición de necesidades y prioridades de mejora y reingeniería de procesos
  - Procesos de evaluación comparativa para mejorar la eficiencia, articular descripciones de trabajo más claras, capacitar de manera efectiva personas, diseñe métricas mejoradas, elimine elementos no esenciales y simplifique, enfoque y automatice el manual actividades
  - Formalizar el proceso para evaluar, clasificar y disponer oportunamente las deficiencias para atender las requisitos de las Secciones 302 y 404
  - Comprender las interdependencias de los controles generales y de aplicación de TI e integrar de manera efectiva ese entendimiento en la Sección 404 controla la documentación y evaluación

A medida que estos pasos amplían el énfasis de la mejora en la calidad, el tiempo y el rendimiento de costos, amplían el enfoque de cumplimiento a la eficacia y eficiencia operativas. Por lo tanto, estos pasos contribuyen a la evolución de ERM.

Otros aspectos de este tema incluyen:

- Trabajar con el auditor externo para agilizar el proceso de auditoría externa y optimizar el "uso de trabajo de otros"
- Definir el papel continuo de la auditoría interna y alinear los planes y recursos de auditoría con el expectativas de la dirección y del comité de auditoría
- Asegurar que las funciones de cumplimiento normativo y gestión de riesgos se desempeñen de manera efectiva para entidades grandes y complejas
- Alinear el ciclo para las conversiones y actualizaciones de nuevos sistemas con el proceso de cumplimiento de la Sección 404 - Renegociar los arreglos contractuales de subcontratación

Con respecto a la auditoría externa, la mayoría de las empresas han estado en posición de reaccionar ante requerimientos afirmados por sus auditores externos a medida que evolucionan las normas de atestación de control interno. Ahora eso las reglas están sobre la mesa para que todos las vean y la SEC ha emitido una guía para las entidades registradas después de su informe de abril Mesa Redonda de 2005 sobre la Implementación de las Disposiciones de Reporte de Control Interno, la gerencia querrá gestionar la relación de auditoría de manera proactiva y constructiva para que el proceso de auditoría esté más basado en el riesgo y de arriba hacia abajo.

En resumen, la integración del cumplimiento de la Sección 404 y la Sección 302 reconoce que las empresas no pueden cumplir con una sin cumplir también con la otra. Se obtendrá un proceso de cumplimiento más eficiente y efectivo a medida que la administración aborde los cuatro temas anteriores para lograr la sostenibilidad de la estructura de control interno, lograr un valor agregado en los procesos de información financiera y aumentar la rentabilidad del cumplimiento de las Secciones 404 y 302. Cuanto más sostenible el entorno de control, más capaces serán los procesos y controles de la organización para hacer frente al cambio, incluida la rotación significativa, la afluencia de nuevas personas, fusiones y adquisiciones, nuevos sistemas y nuevos procesos. El cumplimiento integrado con las Secciones 302 y 404 también proporciona la "plataforma de lanzamiento" para mejorar los procesos y la estructura de control interno y para mejorar el monitoreo a nivel de entidad y de proceso del proceso de información financiera. Todas estas cosas crean infraestructura y procesos que contribuyen a la evolución de ERM.

153. ¿Cómo se basa el cumplimiento de otras leyes y reglamentos aplicables en el cumplimiento de las Secciones 404 y 302?

¿Por qué dicho cumplimiento contribuye a la evolución hacia ERM?

Integrar el cumplimiento de la Sección 404 y la Sección 302, como se discutió en la Pregunta 152, no es el final del juego. Si bien las Secciones 404 y 302 de SOA son importantes, existen otras leyes y reglamentos que las empresas deben cumplir. De acuerdo con COSO, el cumplimiento de las leyes y reglamentos aplicables es uno de los cuatro grupos de objetivos en el marco integrado de gestión de riesgos empresariales. El incumplimiento de las leyes y reglamentos a nivel internacional, nacional, estatal y local que se aplican a una empresa puede dañar la reputación y la imagen de la marca y provocar la pérdida de mercados, ingresos y ganancias.

Para muchas empresas, existe la oportunidad de aplicar la infraestructura establecida para facilitar el cumplimiento continuo de SOA para abordar el cumplimiento de otras áreas legales y reglamentarias. Cualquier decisión sobre un marco de cumplimiento más amplio debe involucrar al director legal (CLO), o un ejecutivo equivalente, encargado de la responsabilidad de monitorear los cambios en las leyes y regulaciones y las acciones de los reguladores nacionales, estatales o locales, y ayudar al equipo ejecutivo a evaluar el impacto de cambios significativos en las leyes y regulaciones en el negocio. En ausencia de un CLO (o ejecutivo equivalente), el comité ejecutivo debe conferir a alguien o alguna función esta responsabilidad. Un CLO bien conectado (o un ejecutivo equivalente) está idealmente posicionado para reconocer las inefficiencias del comportamiento de los silos y las sinergias potenciales que se pueden obtener de una infraestructura y un marco de cumplimiento comunes. En efecto, un marco e infraestructura de cumplimiento común es un enfoque de toda la empresa para administrar los riesgos de la entidad en torno a las leyes y regulaciones aplicables. Aplica los ocho componentes del marco COSO ERM al objetivo de cumplimiento.

Debido a que la tecnología es un habilitador clave para el cumplimiento de SOA, y hay una amplia gama de herramientas de software disponibles en el mercado, muchas empresas evaluarán si conservar sus "soluciones puntuales" diseñadas específicamente para el cumplimiento de SOA o, alternativamente, adoptar "soluciones de plataforma" más amplias. Las denominadas soluciones de plataforma son infraestructura de software diseñada para otro propósito, como la automatización de procesos comerciales, la gestión de documentos, la gestión financiera o un cumplimiento más amplio, y están adaptadas para el cumplimiento de SOA. Las soluciones puntuales generalmente admiten requisitos de análisis e informes más profundos para el cumplimiento de SOA, mientras que las soluciones de plataforma brindan capacidades extendidas y podrían servir como infraestructura para actividades más amplias de cumplimiento, gobierno y gestión de riesgos a lo largo del tiempo. Las empresas que están adoptando soluciones de plataforma están dando un paso más en el camino hacia ERM porque esas soluciones se pueden aprovechar en otras áreas de cumplimiento.

154. ¿Cómo se construye la eficacia y eficiencia operativa sobre las iniciativas de cumplimiento? ¿Por qué la eficacia y la eficiencia operativas contribuyen a la evolución hacia ERM?

En las Preguntas 152 y 153, analizamos las actividades de gestión de riesgos en torno al cumplimiento. Con el tiempo, las empresas migrarán de un enfoque "impulsado por el cumplimiento" (corto plazo) a un enfoque "impulsado por el valor" (largo plazo) en su iniciativa de cumplimiento de SOA y ampliarán su enfoque a otros riesgos empresariales. ERM ayudará a las empresas a cumplir esta tarea. Según COSO, la eficacia y la eficiencia operativas es uno de los cuatro grupos de objetivos en el marco integrado de gestión de riesgos empresariales.

Los problemas de rendimiento de los procesos se vuelven evidentes a medida que las empresas trabajan para cumplir con SOA. por ejemplo, muchos empresas descubren que deben completar un número incalculable de conciliaciones de cuentas, proceso miles de entradas de diario manuales, examinar cientos de hojas de cálculo, explorar y probar miles de controles e ignorar sin darse cuenta los controles basados en sistemas integrados en las soluciones de gestión financiera que, si se implementa y ejecuta correctamente, apoyaría el cumplimiento. En pocas palabras, para la mayoría de las empresas, el proceso de cumplimiento es difícil y doloroso.

Muchas empresas están respondiendo a este problema haciendo que su proceso de cumplimiento sea más vertical y basado en el riesgo, lo que da como resultado, entre otras cosas, la detección de cuentas de bajo riesgo y la reducción de la cantidad de controles. probado y tal vez implementando un programa de autoevaluación. Si bien estos pasos son apropiados y recomendadas, no abordan la calidad de los controles en sí. Además, sólo conducen a mejoras incrementales que no satisfarán a los ejecutivos conscientes de los costos.

La buena noticia es que SOA solo establece objetivos de cumplimiento. Cuando emitió sus reglas para implementar SOA, el La SEC no prescribió métodos de cumplimiento detallados. Por lo tanto, no hay restricciones sobre "trabajar de manera más inteligente, no más difícil." El proceso de cumplimiento no tiene que ser tan costoso como lo están haciendo muchas empresas, especialmente cuando se reconoce que se produce una gran cantidad de reelaboración en la rutina normal del proceso de información financiera. Por Comprender por qué se requieren tareas que consumen mucho tiempo para ejecutar los procesos de información financiera, identificando causas raíz y mejorando los procesos aguas arriba en la fuente, y eliminando procedimientos no esenciales y simplificando, enfocando y automatizando las actividades manuales, existe una gran oportunidad para aprovechar inversiones del cumplimiento de SOA.

Un punto que a menudo se pasa por alto en esta conversación es que existe un vínculo considerable entre mejorar calidad, tiempo y costo del desempeño del proceso por un lado y la efectividad del control interno sobre informes financieros por otro lado. La gerencia no puede mejorar uno sin mejorar también el otro. El mensaje: Las empresas tienen oportunidades para mejorar el rendimiento de los procesos mediante la incorporación (en lugar de la inspección) de la calidad, la compresión del tiempo y la reducción de costos en sus procesos, y todo esto al mismo tiempo. reducir los riesgos de la información financiera. Por ejemplo:

- A medida que las organizaciones eliminan lo que no es esencial, agudizarán su enfoque en cómo conocen se logran los objetivos y examinar la necesidad de controles redundantes.
- A medida que las empresas simplifiquen, estandaricen y automatizan sus procesos, habrá un mayor énfasis en Controles preventivos (frente a los controles de detección que institucionalizan la reelaboración costosa y sin valor agregado) en procesos) y un mayor énfasis en los controles basados en sistemas (frente a los más costosos controles basados en personas). control S).
- A medida que se realicen esfuerzos para eliminar la repetición del trabajo y generar calidad en los procesos, las empresas reducirán el número de entradas de diario manuales requeridas para cerrar los libros, agilizar la actividad de conciliación de cuentas, implementar controles automatizados disponibles y reduzca el número de hojas de cálculo mediante la transferencia de hojas de cálculo funcionalidad en el sistema ERP de la organización donde pertenece.
- Al mejorar y quitarle tiempo al proceso de información financiera, las organizaciones más grandes facilitarán cumplimiento continuo de los requisitos de presentación acelerada de la SEC.
- A medida que ocurran todos los cambios anteriores, también habrá una mejor combinación de controles preventivos y de detección. a partir de controles automáticos y manuales. El resultado: la estructura de control interno será más sostenible en el tiempo y el proceso de cumplimiento será más rentable.

La visión es clara: Progreso incremental al envolver el proceso de cumplimiento en torno al sistema interno existente. la estructura de control no es suficiente. Las empresas deben mejorar la calidad de sus procesos y controles para maximizar la rentabilidad del proceso de cumplimiento. Este cambio de énfasis de "proyecto a proceso" es donde reside el valor real y amplía el enfoque del cumplimiento a los objetivos operativos. Mientras que el "total" Actualmente no existe una solución para el cumplimiento, la gobernanza y la gestión de riesgos más amplios, es probable que emergen con el tiempo a través de los esfuerzos para integrar varias aplicaciones y plataformas y a medida que las empresas evolucionan hacia ERM.

---

## OTRAS PREGUNTAS

155. ¿La implementación de COSO Enterprise Risk Management – Marco Integrado  
¿prevenir el fraude?

Piense en COSO Enterprise Risk Management – Marco Integrado como una mejora del Control Interno – Marco Integrado. En la medida en que existan elementos de control interno para prevenir, disuadir o detectar el fraude, ERM pretende mejorar el control interno en la gestión de todos los riesgos, incluido el riesgo de fraude. Por ejemplo, los componentes descritos en Enterprise Risk Management – Marco Integrado aumentan el proceso de evaluación de riesgos, haciéndolo más efectivo. La evaluación de riesgos es vital para un programa antifraude. Por supuesto, hay otros aspectos de un programa antifraude que no se abordan explícitamente en el marco de ERM. Consulte las Preguntas 77 a 81 en la Guía de Protiviti sobre la Ley Sarbanes-Oxley: Requisitos de informes de control interno, Preguntas frecuentes sobre la Sección 404, para obtener una discusión de las consideraciones relevantes relacionadas con el fraude. Esa publicación está disponible en [www.protiviti.com](http://www.protiviti.com).

---

156. ¿Ha recibido alguna de las empresas que han divulgado públicamente sus procesos de ERM  
retroalimentación positiva de los analistas?

Dado que COSO lanzó el nuevo marco ERM en septiembre de 2004, es prematuro sacar conclusiones sobre este punto en el momento en que se imprimió esta publicación. Hasta la fecha, si bien hay muchos ejemplos de empresas que divulan prácticas de gestión de riesgos para abordar riesgos específicos, pocas empresas han revelado que han implementado la gestión de riesgos empresariales. Con el tiempo, esperamos que eso cambie.

157. ¿Los analistas y otros dentro de la comunidad inversora o las agencias calificadoras expresaron su  
puntos de vista sobre cómo un enfoque de ERM que funcione de manera efectiva afectaría sus puntos de vista de una empresa?

Desde que se publicó el nuevo marco de ERM en septiembre de 2004, no ha habido tiempo suficiente para que los analistas financieros y las agencias calificadoras interviniieran con un punto de vista sobre ERM, tal como lo define COSO. En el marco, COSO expresó la opinión de que las comunicaciones de una organización a sus partes interesadas, a los reguladores, a los analistas financieros y a otras partes externas brindan información pertinente a sus necesidades, para que puedan comprender fácilmente las circunstancias y los riesgos que enfrenta la entidad. A medida que las entidades brinden dicha divulgación, los analistas financieros y las agencias calificadoras la esperarán.

El diálogo de una entidad con los analistas financieros y las agencias calificadoras de bonos también puede ser iterativo, en el que se pueden obtener conocimientos útiles sobre las percepciones, precisas o inexactas, con respecto a la entidad. Sobre este punto, COSO expresa lo siguiente:

Los analistas financieros y las agencias calificadoras de bonos consideran muchos factores relevantes para el valor de una entidad como inversión. Analizan la estrategia y los objetivos de la administración, los estados financieros históricos y la información financiera prospectiva, las acciones tomadas en respuesta a las condiciones de la economía y el mercado, el potencial de éxito a corto y largo plazo, y el desempeño de la industria y las comparaciones con grupos de pares.  
Los medios impresos y de difusión, en particular los periodistas financieros, también pueden realizar análisis similares.

Las actividades de investigación y seguimiento de estas partes pueden proporcionar información sobre cómo otros perciben el desempeño de la entidad, los riesgos económicos y de la industria que enfrenta la entidad, las estrategias financieras o operativas innovadoras que pueden mejorar el desempeño y las tendencias de la industria. Esta información a veces se proporciona en reuniones cara a cara entre las partes y la gerencia, o indirectamente en análisis para inversionistas, inversionistas potenciales y el público. En cualquier caso, la gerencia debe considerar las observaciones y los conocimientos de los analistas financieros, las agencias calificadoras de bonos y los medios de comunicación que pueden mejorar la gestión de riesgos empresariales.

158. ¿Toda la información sobre riesgos y gestión de riesgos puede clasificarse como información privilegiada entre abogado y cliente y, por lo tanto, no ser detectable?

Si bien esta es una pregunta para el abogado, como regla general, es dudoso que la información sobre riesgos y gestión de riesgos pueda clasificarse como "privilegiada" porque esa información está muy entrelazada con los fundamentos de la gestión del negocio. La gestión de riesgos, como actividad, no suele reducirse a la estrecha

límites de una investigación, pero normalmente es una actividad para integrar con los procesos de la organización. La gestión de un negocio y la gestión del riesgo deben estar inextricablemente unidas entre sí. Dicho esto, las situaciones pueden surgir cuando algunos problemas de riesgo relacionados con asuntos específicos de cumplimiento pueden estar sujetos al privilegio abogado-cliente. Si este es el resultado que desea una empresa, entonces la gerencia debe consultar con un abogado.

159. Dado que se supone que toda esta información es detectable, ¿Genera ERM más litigios riesgo para las empresas?

ERM está diseñado para ayudar a los ejecutivos a administrar mejor el negocio al identificar problemas y riesgos dentro del organización más transparente para la gerencia y la junta. Es cierto que una mayor transparencia es un arma de doble filo que todos, incluida la barra de demandantes, pueden usar para lograr su propósito. pero el verdadero El mensaje con respecto a ERM es que la mayor transparencia que brinda puede ayudar a la administración a mejorar elecciones a lo largo del tiempo. Nada cambiará la exposición de la gerencia a los litigios en caso de que algo salga mal.

160. ¿Existen casos judiciales en los que la dirección de una empresa o su directorio hayan sido considerados deficientes porque no contaban con un sistema adecuado de gestión de riesgos?

Hasta donde sabemos, no tenemos conocimiento de que el tribunal adopte este punto de vista a gran escala. Somos conscientes de casos judiciales en los que se alegaba que el consejo de administración de una empresa no había supervisado adecuadamente la actividades de cobertura de tipos de interés de la organización. La gestión de riesgos ha comenzado recientemente a recibir énfasis como una herramienta para aumentar el proceso de gobernanza. Es prudente que la administración y los directorios analicen cuidadosamente evaluar las capacidades de gestión de riesgos de su organización utilizando COSO Enterprise Risk Management: Marco Integrado. Esto fortalecería su afirmación de que han diseñado e implementado un proceso eficaz de gestión de riesgos.

161. ¿Existen riesgos asociados con la falta de un proceso de ERM y, de ser así, cuáles son?

COSO sugiere que los directores ejecutivos evalúen las capacidades de ERM de su entidad. COSO también afirma que los gerentes dentro de un empresa "debería considerar cómo está llevando a cabo sus responsabilidades a la luz de este marco y discuta con más personal senior ideas para fortalecer la gestión de riesgos empresariales". Además, COSO alienta a los auditores internos a "considerar la amplitud de su enfoque en la gestión de riesgos empresariales". Sin ERM en funcionamiento, la gerencia y los directores enfrentan la perspectiva de no tener suficientes procesos en lugar que les proporcionará una alta confianza de que su organización está identificando y gestionando todos riesgos potencialmente significativos.

162. ¿Es posible vincular un sistema ERM con el desempeño y la compensación de un empleado? ¿Hay alguno? empresas haciendo esto?

Los estándares de recursos humanos son una parte integral del Ambiente Interno, uno de los ocho componentes del marco COSO ERM. Estos estándares abordan, entre muchas otras cosas, el desempeño evaluaciones y programas de compensación. Debido a que ERM requiere una evaluación de la capacidad humana de la entidad estándares de recursos, es apropiado evaluar la efectividad de los procesos de la organización para establecer expectativas de desempeño, monitorear y evaluar el desempeño y alinear la compensación con actuación. Además, al gestionar riesgos específicos, la respuesta al riesgo de una entidad a menudo requerirá la diseño e introducción de medidas de desempeño para ganar más tracción en la implementación de ese riesgo respuesta. Con respecto a los riesgos susceptibles de cuantificación, obviamente es más fácil articular desempeño expectativas que se pueden integrar con el sistema de recompensas. Para otros riesgos, una métrica sustituta (ver La pregunta 112) puede ser apropiada.

163. ¿Existe una certificación, calificación u otro mecanismo de evaluación de terceros para ERM?

En la actualidad, no se ha establecido una certificación, calificación u otro mecanismo de evaluación de terceros establecido para ERM. No esperamos que eso suceda por mucho tiempo.

164. ¿Cómo se relaciona ERM con el Acuerdo de Capital de Basilea que requiere que las instituciones financieras informen sobre  
¿Riesgo operacional?

El Nuevo Acuerdo de Capital de Basilea (Basilea II) del Comité de Supervisión Bancaria de Basilea actualiza el Acuerdo de Basilea de 1988 Acuerdo de Capital (Basilea I) que determina el nivel de capital regulatorio que los bancos internacionales deben mantener para compensar riesgos imprevistos. Este Acuerdo Basilea II, negociado por los supervisores bancarios internacionales, revisa las reglas para asignación de capital para el riesgo de crédito e introduce un nuevo requisito de asignación de capital para el riesgo operativo. El La intención es fomentar requisitos de capital que sean más sensibles al riesgo, para que los bancos tengan mayor flexibilidad para calibrar sus niveles de capital para reflejar con mayor precisión el nivel de riesgo que enfrentan.

El Acuerdo de Capital de Basilea II requiere que las instituciones financieras informen sobre el riesgo operativo. Aunque un ERM proceso facilitaría el cumplimiento de estos requisitos, COSO decidió que comparar el ERM marco para el Nuevo Acuerdo de Capital de Basilea del Comité de Supervisión Bancaria de Basilea estaba más allá del alcance de su proyecto. Hay muchos eventos dentro del alcance de Basilea que están muy sesgados para capturar aquellos riesgos que pueden cuantificarse más fácilmente, principalmente como pérdidas operativas a efectos de información. Esto no es sorprendente dado que los datos subyacentes son críticos para establecer una base estadística para la medición de los requerimientos de capital económico. Sin embargo, existen riesgos que pueden no ser tan susceptibles a tal cuantificación. Debido a que el marco COSO ERM está destinado a abordar todos los eventos que podrían potencialmente tener un efecto adverso significativo en el logro de los objetivos de la entidad, incluyendo los eventos dentro del alcance de Basilea, se prevé que el cumplimiento de Basilea resulte en un paso apropiado hacia la implementación de ERM en las instituciones financieras.

165. ¿Cuál es la diferencia entre ERM y un estándar internacional como ISO?

COSO incluyó la Organización Internacional para la Estandarización, Guía ISO/IEC, en su bibliografía. De este modo, la norma ISO proporcionó una fuente de información para el desarrollo del marco ERM. Sin embargo, COSO decidió que comparar el marco ERM con otros marcos estaba más allá del alcance del proyecto.

166. ¿Cómo se integra COSO Enterprise Risk Management – Marco Integrado con tal marcos como COBIT, ISO 17799, BITS, NIST Special Publication 800-53 e ITIL?

El marco COSO ERM es un marco amplio, que abarca marcos más específicos relacionados con ÉL. Una vez que se identifican los riesgos clave, incluidos los riesgos de TI, la organización puede utilizar los marcos apropiados, mejores prácticas, procesos y medidas que mejor se adapten a la gestión y seguimiento de dichos riesgos. COSO decidió que comparar el marco ERM con otros marcos estaba más allá del alcance del proyecto.

167. ¿Qué está pasando en otros países con respecto a la gestión de riesgos? Son estos desarrollos que impactan positivamente el desempeño de la compañía y el gobierno corporativo?

Las empresas que cotizan en la Bolsa de Valores de Londres y están constituidas en el Reino Unido deben informar a los accionistas sobre un conjunto de principios definidos relacionados con el gobierno corporativo (conocidos como Código, y respaldado con la orientación proporcionada por el "Informe Turnbull", que se actualizó recientemente en el momento en que se imprimió esta publicación). La legislación KonTrag en Alemania exige que las grandes empresas establecer sistemas de supervisión de gestión de riesgos y reportar información de controles a los accionistas. Además, existe legislación relacionada con el control interno y la gestión de riesgos en Australia, Canadá, Francia, Sur África, Japón y otros países. La legislación tipo Sarbanes-Oxley continúa surgiendo en países fuera del Estados Unidos. Si estos desarrollos tienen un impacto positivo en el desempeño de la empresa y queda por probar la gobernabilidad.

168. ¿Existe un formato para comunicar nuestro proceso de gestión de riesgos a nuestros clientes para alinear y cumplir con sus requisitos?

En la industria de servicios financieros, no es inusual encontrar estatutos de comités de riesgo en el sitio web de un banco. Esta la información está disponible para cualquiera que la necesite. Fuera de los servicios financieros, actualmente no hay una Tendencia generalizada de empresas que solicitan información sobre los procesos de gestión de riesgos de otras empresas, ya sean clientes o proveedores. Si surge esa tendencia, será posible rastrear ejemplos de tales informes.

## Acerca de Protiviti Inc.

Protiviti es un proveedor líder de auditoría interna independiente y servicios de consultoría de riesgo empresarial y tecnológico. Ayudamos a los clientes a identificar, evaluar y gestionar los riesgos operativos y relacionados con la tecnología que se encuentran en sus industrias, y asistimos en la implementación de los procesos y controles para permitir su monitoreo continuo. También ofrecemos una gama completa de servicios de auditoría interna enfocados en brindar las habilidades profundas y la experiencia tecnológica para permitir la gestión de riesgos comerciales y la transformación continua de las funciones de auditoría interna.

Protiviti ha sido designado por una firma de investigación independiente como "líder" junto con otras tres firmas consultoras que ofrecen servicios de cumplimiento y ERM. Nuestras ofertas de gestión de riesgos empresariales ayudan a las empresas a alinear sus estrategias, procesos, tecnología y conocimientos con el objetivo de mejorar sus capacidades para evaluar y gestionar, en toda la empresa, las incertidumbres que deben abordar al ejecutar su modelo de negocio. Ofrecemos servicios en evaluaciones de riesgos empresariales y en áreas de riesgo específicas en torno a los problemas que enfrentan las empresas a medida que mejoran la gobernanza y administran los riesgos tecnológicos, operativos, de cumplimiento y financieros. Nuestros servicios de auditoría interna son lo suficientemente flexibles para alinear nuestro trabajo con las capacidades de cumplimiento y ERM que nuestros clientes tienen y eligen implementar.

El enfoque de Protiviti para la implementación de ERM es ofrecer ideas prácticas y comprobadas para comenzar y ayudar a las empresas a desarrollar e implementar su propio enfoque personalizado. Protiviti ve a ERM como un viaje en el que las organizaciones redefinen la propuesta de valor de la gestión de riesgos integrándola con el establecimiento de estrategias. Las ofertas de ERM de Protiviti se centran en evaluar los riesgos en toda la empresa, identificando brechas en las capacidades de gestión de riesgos y cerrando las brechas mejorando las capacidades de gestión de riesgos, formulando respuestas de riesgo efectivas, mejorando la infraestructura de ERM y capacitando al personal interno para garantizar una eficacia continua.

Protiviti tiene más de 40 ubicaciones en América del Norte, Europa, Asia y Australia. La firma es una subsidiaria de propiedad total de Robert Half International Inc. (símbolo NYSE: RHI). Fundada en 1948, Robert Half International es miembro del índice S&P 500.

---

## notas

---

notas

América del norte	América Latina	Europa	Asia-Pacífico		
ESTADOS UNIDOS	MÉXICO +52.9171.1501 +1.888.556.7420 protiviti.com www.protiviti.com.mx	FRANCIA +33.1.42.96.22.77 protiviti.fr	PAÍSES BAJOS +31.20.346.04.00 protiviti.nl	AUSTRALIA +61.3.9948.1200 protiviti.com.au	JAPÓN +81.3.5219.6600 protiviti.jp
CANADÁ +1.416.350.2181 protiviti.ca		ITALIA +39.02.655.06.301 protiviti.it	REINO UNIDO +44.207.930.8808 protiviti.co.uk	CHINA +86.21.63915031 protiviti.cn	SINGAPUR +65.6220.6066 protiviti.com.sg

Protiviti es un proveedor líder de servicios de auditoría interna y consultoría de riesgos. Ayudamos a los clientes a identificar, evaluar y gestionar los riesgos operativos y relacionados con la tecnología que se encuentran en sus industrias, y asistimos en la implementación de los procesos y controles para permitir su monitoreo continuo. También ofrecemos una gama completa de servicios de auditoría interna enfocados en brindar las habilidades profundas y la experiencia tecnológica para permitir la gestión de riesgos comerciales y la transformación continua de las funciones de auditoría interna.

Protiviti no tiene licencia ni está registrada como firma de contadores públicos y no emite opiniones sobre estados financieros ni ofrece servicios de certificación.