ADMINISTRACIÓN DE RIESGOS

Es el proceso mediante el cual se identifica, se mide y se controla la exposición al riesgo. Es un elemento esencial para la liquidez y solvencia de cualquier negocio.

La administración de riesgos asegura el cumplimiento de las políticas definidas por los comités de riesgo, refuerza la capacidad de análisis, define metodología de valoración, mide los riesgos y, establece procedimientos y controles homogéneos.

Se refiere al establecimiento de los lineamientos para la adecuada administración de los riesgos de la empresa, de la industria y del entorno e involucrar a toda la organización en su manejo, detectar y aprovechar las oportunidades en los riesgos.

Las funciones principales en la Administración de Riesgos, son:

- Análisis de riesgos y oportunidades incluyendo la globalización, volatilidad económica, riesgos micro y macro económicos.
- Administración de Seguros
- **Administración de riesgos operativos y financieros**.

El futuro de una empresa es lo que puede llegar a **ser** y lo que puede llegar a **hacer**. El futuro es una posibilidad que se construye en el presente con decisiones dirigidas hacia el futuro, tendientes a realizar los objetivos empresariales o bien personales. La construcción del futuro se hace con base a **previsiones** las cuales no son algo concreto y delimitado, sino que se dan con base a la probabilidad de los eventos.

La **probabilidad** es una **medida del grado de credibilidad** de que se presente un evento y el **grado de certeza** de las probabilidades está en función de la calidad y cantidad de la información disponible. Si se conocen las probabilidades asociadas con los eventos convierte los problemas inciertos en problemas con riesgo. De aquí nace el estudio profesional de los Riesgos que ahora se ha convertido en una carrera profesional que posibilita que lo desconocido sea administrable.

¿Qué es la administración de riesgos financieros?

La administración de riesgos financieros es una rama especializada de las finanzas corporativas, que se dedica al manejo o cobertura de los riesgos financieros.

La **incertidumbre** existe siempre que no se sabe con seguridad lo que ocurrirá en el futuro. El riesgo es la incertidumbre que si "importa" porque incide en el bienestar de la gente.

Toda situación riesgosa es incierta, pero piense usted que puede haber incertidumbre sin riesgo".

Por esta razón, un Administrador de Riesgos Financieros se encarga del asesoramiento y manejo de la exposición ante el riesgo de corporativos o empresas a través del uso de instrumentos financieros derivados.

Para tener un panorama más particular sobre la administración de riesgos, podemos apreciar la diferencia entre **objetivos y funciones** de la administración de riesgos financieros.

Cuadro No. 1: **Objetivos y funciones de la administración de riesgos financieros**

OBJETIVOS	FUNCIONES
Identificar los diferentes tipos de riesgo que pueden afectar la operación y/o resultados esperados de una entidad o inversión.	Determinar el nivel de tolerancia o aversión al riesgo.
Medir y controlar el riesgo "no-sistemático", mediante la instrumentación de técnicas y herramientas, políticas e implementación de procesos.	Determinación del capital para cubrir un riesgo.
	Monitoreo y control de riesgos.
	Garantizar rendimientos sobre capital a los accionistas.
	Identificar alternativas para reasignar el capital y mejorar rendimientos.

También es de suma importancia conocer los tipos de riesgos a los que se enfrenta toda empresa, así como, su definición;

¿Cuáles son los tipos de riesgos financieros más comunes?

Cuadro No. 2: **Tipos de riesgos financieros**

TIPO DE RIESGO	DEFINICIÓN
RIESGO DE MERCADO	Se deriva de cambios en los precios de los activos y pasivos financieros (o volatilidades) y se mide a través de los cambios en el valor de las posiciones abiertas.
RIESGO CRÉDITO	Se presenta cuando las contrapartes están imposibilitadas para cumplir sus obligaciones contractuales
RIESGO DE LIQUIDEZ	Se refiere a la incapacidad de conseguir obligaciones de flujos de efectivo necesarios, lo cual puede forzar a una liquidación anticipada, transformando en consecuencia las pérdidas en "papel" en pérdidas realizadas.
RIESGO OPERACIONAL	Se refiere a las pérdidas potenciales resultantes de sistemas inadecuados, fallas administrativas, controles defectuosos, fraude, o error humano
RIESGO LEGAL	Se presenta cuando una contraparte no tiene la autoridad legal o regulatoria para realizar una transacción
RIESGO TRANSACCIÓN	Asociado con la transacción individual fijada en moneda extranjera: importaciones, exportaciones, capital extranjero y préstamos
RIESGO DE CONVERSIÓN Ó TRADUCCIÓN	Surge de la conversión de Estados Financieros en moneda extranjera a la moneda de la empresa matriz para efectos de reportes financieros
RIESGO ECONÓMICO O DE TIPO DE CAMBIO	Asociado con la pérdida de ventaja competitiva debido a movimientos de tipo de cambio

Una vez explicados los fundamentos de objetivos y funciones de la administración de riesgos, así como, los tipos de riesgos financieros, es importante conocer a su vez, el proceso de cómo se administra el riesgo paso a paso, de manera muy general, como se muestra a continuación.

Cuadro No. 3: Proceso de la administración del riesgo

PASO	DEFINICIÓN
IDENTIFICACIÓN DEL RIESGO	Determinar cuáles son las exposiciones más importantes al riesgo en la unidad de análisis (familia, empresa o entidad).
EVALUACIÓN DEL RIESGO	Es la cuantificación de los costos asociados a riesgos que ya han sido identificados.
SELECCIÓN DE MÉTODOS DE LA ADMINISTRACIÓN DEL RIESGO	Depende de la postura que se quiera tomar: Evitar el riesgo (no exponerse a un riesgo determinado); prevención y control de pérdidas (medidas tendientes a disminuir la probabilidad o gravedad de pérdida); retención del riesgo (absorber el riesgo y cubrir las pérdidas con los propios recursos) y finalmente, la transferencia del riesgo (que consiste en trasladar el riesgo a otros, ya sea vendiendo el activo riesgoso o comprando una póliza de seguros).
IMPLEMENTACIÓN	Poner en práctica la decisión tomada.
REPASO	Las decisiones se deben de evaluar y revisar periódicamente.

Es importante recalcar la importancia del método de transferencia del riesgo, ya que hoy en día es el método más utilizado en la administración de riesgos, a su vez, es el método al que se recurre a través de instrumentos derivados.

El método de transferencia del riesgo, cuenta con tres dimensiones, la de protección o cobertura, la de aseguramiento y la de diversificación.

Cuadro No. 4: Dimensiones de la transferencia del riesgo

DIMENSIÓN	DEFINICIÓN
PROTECCIÓN O COBERTURA	Cuando la acción tendiente a reducir la exposición a una pérdida, lo obliga también a renunciar a la posibilidad de una ganancia.
ASEGURAMIENTO	Significa pagar una prima (el precio del seguro) para evitar pérdidas.
DIVERSIFICACIÓN	Significa mantener cantidades similares de muchos activos riesgosos en vez de concentrar toda la inversión en uno solo. (Canasta Financiera Diversificada)

Organización de la información de riesgos

El riesgo implica muchos componentes en activos, amenazas, vulnerabilidades y controles. El responsable de evaluación de riesgos debe poder determinar el componente de riesgo del que se trata sin interferir en el flujo de la conversación. Para el debate, se utiliza una plantilla de discusión de riesgos, con el objeto de facilitar a los asistentes la comprensión de los componentes en riesgo. Esta herramienta también facilita al responsable de registro de evaluación de riesgos la obtención de información de riesgos de forma coherente en las reuniones.

Los datos de la siguiente plantilla se pueden rellenar en cualquier secuencia. Sin embargo, la experiencia demuestra que si se sigue la secuencia según las siguientes preguntas, se facilita a los participantes del debate la comprensión de los componentes de riesgo y revela más información:

Terminología y Categorías de Evaluación de Riesgos

¿Qué activo se va a proteger?

¿Cuál es el valor del activo para la organización?

¿Qué se intenta evitar que le suceda al activo (amenazas conocidas y posibles)?

¿Cómo se puede producir la pérdida o las exposiciones?

¿Cuál es el alcance de la exposición potencial para el activo?

¿Qué se está haciendo actualmente para reducir la probabilidad o el alcance del daño en el activo?

¿Cuáles son las acciones que se pueden adoptar para reducir la probabilidad en el futuro?

Por ejemplo, para el Departamento de Procesamiento de Datos, en lo relacionado a la seguridad de información.

Las preguntas anteriores pueden traducirse en terminología y categorías de evaluación de riesgos específicas que se emplean para asignar prioridades a los riesgos.

No obstante, es posible que el participante no esté familiarizado con dichos términos y no esté encargado de asignar prioridades a los riesgos. La experiencia demuestra que si se evita terminología de seguridad de información, como amenazas, vulnerabilidades y contramedidas, se mejora la calidad del debate y permite que los participantes sin conocimientos técnicos no se sientan intimidados.

Otra ventaja de utilizar términos funcionales para debatir el riesgo radica en que se reduce la posibilidad de que otros técnicos discutan sutilezas de términos específicos. En este punto del proceso es mucho más importante comprender las áreas de mayor riesgo que debatir definiciones opuestas de amenaza y vulnerabilidad. El responsable de evaluación de riesgos debe esperar hasta el final del debate para resolver dudas acerca de las definiciones y terminología de los riesgos.

Definición de amenazas y vulnerabilidades

La información acerca de las amenazas y vulnerabilidades, proporciona la prueba técnica que se emplea para asignar prioridades a los riesgos en una empresa.

Debido a que muchos participantes sin conocimientos técnicos pueden no estar familiarizados con las exposiciones detalladas que afectan a su empresa, es posible que el responsable de evaluación de riesgos tenga que ofrecer ejemplos que contribuyan a iniciar el debate.

Ésta es un área en la que resulta muy valiosa una investigación previa para ayudar a los responsables de negocios a detectar y comprender el riesgo en sus propios entornos. Como referencia, en el ISO se definen las amenazas como una causa de repercusiones posibles en la organización. Se puede decir que la **amenaza** es un suceso o entidad con posibilidad de dañar el sistema.

Las repercusiones derivadas de una amenaza normalmente se definen con conceptos como confidencialidad, integridad y disponibilidad. Hacer referencia a estándares del sector resulta muy útil al investigar amenazas y vulnerabilidades.

Para el debate de riesgos facilitado puede resultar útil traducir las amenazas y vulnerabilidades en términos conocidos para los participantes sin conocimientos técnicos.

Por ejemplo, ¿qué se intenta evitar? o ¿qué se teme que le suceda al activo?

La mayoría de las repercusiones en la empresa se pueden clasificar en confidencialidad del activo, integridad o disponibilidad del activo para la realización de las actividades. Intente utilizar este enfoque si los participantes tienen dificultades para entender el significado de las amenazas para los activos organizativos.

Un ejemplo habitual de una amenaza para la organización es un ataque a la integridad de los datos financieros. Después de haber articulado lo que intenta evitar, la siguiente tarea consiste en determinar el modo en que las amenazas se producen en la organización.

Una vulnerabilidad es un punto débil de un activo o grupo de activos que una amenaza puede atacar. De un modo simplificado, las vulnerabilidades proporcionan el mecanismo o el *modo* en que se pueden producir las amenazas. Hay quienes definen a la vulnerabilidad como una situación o punto débil en (o la ausencia de) los procedimientos de seguridad, controles técnicos, controles físicos u otros controles que puede aprovechar una amenaza.

Un error habitual al llevar a cabo una evaluación de riesgos es centrarse en vulnerabilidades técnicas. La experiencia ha demostrado que las vulnerabilidades más importantes se suelen producir debido a la ausencia de un proceso definido o un control no adecuado de la seguridad de información.

No deben omitirse los aspectos organizacionales y de liderazgo de la seguridad durante el proceso de recopilación de datos.

Por ejemplo, retomando la vulnerabilidad de actualizaciones de seguridad anterior, la imposibilidad de aplicar actualizaciones en sistemas administrados puede conllevar un ataque a la integridad de la información financiera que se encuentra en dichos sistemas. El control claro y la aplicación de directivas de seguridad de información suelen ser un problema organizacional en muchas empresas.

Es probable que durante el proceso de recopilación de datos se reconozcan a grupos comunes de amenazas y vulnerabilidades. Haga un seguimiento o *follow up* de estos grupos para determinar si con controles similares se puede reducir la probabilidad de varios riesgos.

Estimación de la probabilidad de las amenazas

Después de que los participantes hayan proporcionado las estimaciones de las posibles repercusiones en los activos organizacionales, el responsable de evaluación de riesgos recopila sus opiniones acerca de la probabilidad de que las repercusiones se produzcan.

De este modo se cierra el debate acerca de los riesgos y se permite que el participante comprenda el proceso de identificar los riesgos de seguridad. Recuerde que el grupo de seguridad de información se encarga de la decisión final acerca de la estimación de probabilidad de que se produzcan repercusiones en la organización.

Este debate se puede considerar de cortesía y un modo de generar buena voluntad en los participantes.

Puede utilizar las siguientes indicaciones para estimar la probabilidad de cada amenaza y vulnerabilidad identificada en el debate:

Alta: muy probable, previsión de uno o varios ataques en un año.
Media: probable, previsión de ataque en dos a tres años.
Baja: no probable, no se prevé ningún ataque en tres años.

Normalmente se incluye la revisión de las incidencias que se han producido recientemente. Según resulte adecuado, debe llevarse a junta estas indicaciones en orden para que los participantes comprendan la importancia de la seguridad y el proceso de administración de riesgos global.

El proceso de administración de riesgos de seguridad de Microsoft asocia un intervalo de un año a la categoría de probabilidad alta porque los controles de seguridad de información normalmente tardan períodos largos en implementarse.

Seleccionar la probabilidad de un año llama la atención del riesgo y anima a tomar una decisión de mitigación en el siguiente ciclo presupuestario.

Una probabilidad alta, combinada con una repercusión alta, demandaría un debate acerca de los riesgos entre los participantes y el equipo de administración de riesgos de seguridad. El grupo de seguridad de información debe tomar conciencia de esta responsabilidad al estimar la probabilidad de las repercusiones.

La siguiente tarea es recopilar las opiniones de los participantes acerca de los posibles controles que puedan reducir la probabilidad de las repercusiones identificadas. Se puede manejar este debate como una sesión de lluvia de ideas y sin criticar o rechazar ninguna idea.

Debemos recordar que el objetivo principal de este debate es demostrar todos los componentes de riesgo para facilitar la comprensión. La selección de mitigación real se produce en la fase de apoyo a la toma de decisiones. Por cada posible control identificado, revise el debate de probabilidad para estimar el nivel de aparición reducida mediante las mismas categorías cualitativas descritas anteriormente. Indique a los participantes que el concepto de reducción de probabilidad del riesgo es la variable principal para administrar el riesgo a un nivel aceptable.

Tareas y componentes principales

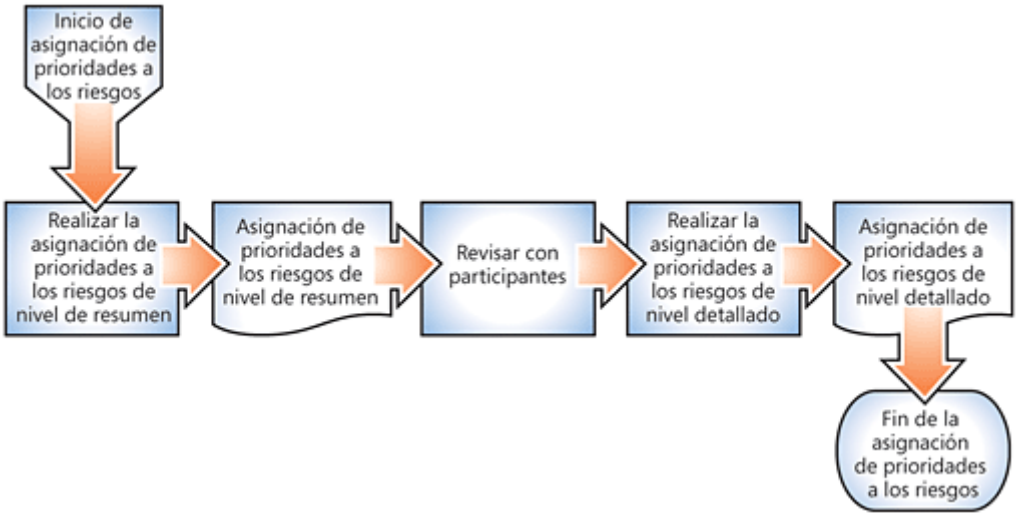
Tarea 1: elaborar la lista de nivel de resumen mediante clasificaciones amplias para estimar la probabilidad de repercusiones para la organización.

Resultado: lista de nivel de resumen para identificar rápidamente la prioridad de los riesgos para la organización.

Tarea 2: revisar la lista de nivel de resumen con los participantes para empezar a alcanzar consenso en la prioridad de los riesgos y seleccionar los riesgos para la lista de nivel detallado.

Tarea 3: Elaboración de una lista a nivel de detalle, mediante el examen de los atributos pormenorizados del riesgo en el entorno de negocios actual. Esto incluye indicaciones para determinar la estimación cuantitativa de cada riesgo.

Resultado: Elaboración de una lista de nivel detallado que proporciona información exhaustiva de los riesgos principales para la organización.



Preparación para el éxito

La asignación de prioridades a los riesgos para la organización no es una mera propuesta. El equipo de administración de riesgos debe intentar predecir el futuro mediante la estimación de cuándo y cómo las posibles repercusiones pueden afectar a la organización y, a continuación, debe justificar estas predicciones ante los participantes. Un error habitual que cometen muchos equipos es "ocultar" las tareas empleadas para determinar la probabilidad y utilizar cálculos para representar la probabilidad en porcentajes u otras cifras de resultados a las que suponen que los responsables de negocios responderán más rápidamente. Pero la experiencia al desarrollar el proceso de administración de riesgos de seguridad ha demostrado que los participantes son más propensos a aceptar los análisis del equipo de administración de riesgos de seguridad si la lógica es clara durante el proceso de asignación de prioridades. El proceso se centra en la comprensión por parte de los participantes a lo largo del mismo. La lógica de asignación de prioridades debe ser lo más simple posible para lograr el consenso rápidamente y reducir los malentendidos. Por ejemplo, la experiencia en elaboración de evaluaciones de riesgos en el departamento de TI de Microsoft y otras empresas, ha demostrado que las siguientes prácticas resultan útiles para el equipo de administración de riesgos de seguridad durante el proceso de asignación de prioridades:

Analizar los riesgos durante el proceso de recopilación de datos. Debido a que la asignación de prioridades a los riesgos puede ocupar mucho tiempo. Debe intentar anticiparse a los riesgos controvertidos e iniciar el proceso de asignación de prioridades lo más pronto posible. Este método abreviado es posible debido a que el equipo de administración de riesgos de seguridad es el único responsable del proceso de asignación de prioridades.

Es conveniente llevar a cabo una investigación para generar credibilidad para estimar la probabilidad. Deberán utilizarse los informes de auditoría anteriores y tenga en cuenta las tendencias del sector así como las incidencias de seguridad internas según resulte adecuado. Volver a consultar a los participantes según sea necesario para obtener información acerca de los controles actuales y la toma de conciencia de los riesgos específicos en sus entornos.

Programar tiempo suficiente en el proyecto para llevar a cabo investigaciones y realizar análisis de la efectividad y las capacidades del entorno de controles actual.

Recuerde usted a los participantes que el equipo de administración de riesgos de seguridad tiene la responsabilidad de determinar la probabilidad. El patrocinador ejecutivo también debe reconocer esta función y apoyar el análisis del equipo de administración de riesgos de seguridad.

Al comunicar el riesgo en términos de negocios, debe evitar utilizar expresiones relacionadas con el miedo o jerga técnica en el análisis de asignación de prioridades. El equipo de administración de riesgos de seguridad debe comunicar el riesgo en unos términos que la organización comprenda y evitar la tentación de exagerar el nivel de peligro.

Relacionar los nuevos riesgos con los anteriores. Al crear la lista de nivel de resumen, incorpore los riesgos de las evaluaciones anteriores. Esto permite que el equipo de administración de riesgos de seguridad realice un seguimiento de los riesgos en varias evaluaciones y proporcione la ocasión de actualizar los elementos de riesgo anteriores según sea necesario. Por ejemplo, si un riesgo anterior no se ha resuelto debido a los altos costos, revise la probabilidad de que el riesgo se produzca y vuelva a tener en cuenta los cambios en la solución o costos de resolución.

Asignación de prioridades a los riesgos de seguridad

A continuación se explica el proceso de elaboración de las listas de riesgos de nivel de resumen y detallado.

Tarea 1: Determinar el valor de las repercusiones a partir de las declaraciones de repercusiones elaboradas en el proceso de recopilación de datos.

Tarea 2: Estimar la probabilidad de las repercusiones para la lista de nivel de resumen.

Tarea 3: Completar la lista de nivel de resumen mediante la combinación de los valores de repercusiones y de probabilidad por cada declaración de riesgo.

Tarea 1: Determinar el nivel de las repercusiones

La información de clase de activos y de exposición de activo obtenida en el proceso de recopilación de datos se debe resumir en un solo dato para determinar las repercusiones. Recuerde que las repercusiones son la combinación de la clase de activos y el alcance de exposición al activo. Utilice la siguiente figura para seleccionar el nivel por cada declaración de repercusiones.

		Referencia de clasificación de efecto		
Clase de activo	Alto	Efecto moderado	Efecto alto	Efecto alto
	Medio	Efecto bajo	Efecto moderado	Efecto alto
	Bajo	Efecto bajo	Efecto bajo	Efecto moderado
		Bajo	Medio	Alto
		Nivel de exposición		

Tarea 2: Estimar la probabilidad de nivel de resumen

Utilice las mismas categorías de probabilidad descritas en el proceso de recopilación de datos. Las categorías de probabilidad se incluyen a continuación como referencia:

Alta: muy probable, previsión de uno o varios ataques en un año.

Media: probable, previsión de ataque una vez al menos en dos a tres años.

Baja: no probable, no se prevé ningún ataque en tres años.

Por ejemplo: La asignación de prioridades a riesgos de nivel de resumen es el primer documento formal de la estimación del equipo de administración de riesgos acerca de la probabilidad de riesgo. El equipo de administración de riesgos debe estar preparado para proporcionar pruebas o casos que justifiquen sus estimaciones; por ejemplo, referencias a incidencias anteriores o a la efectividad de los controles actuales.

- Probabilidad de robo por parte de empleados de confianza: baja. Una empresa se puede enorgullecer de contratar a empleados de confianza. El equipo directivo comprueba esta confianza mediante comprobaciones de antecedentes y efectúa auditorías aleatorias de la actividad de los asesores financieros. En el pasado no se han identificado incidencias relacionadas con el abuso por parte los empleados.
- Probabilidad de peligro: media. El departamento de Tecnología de Información, ha formalizado recientemente su proceso de revisiones y configuración de sus sistemas de información, debido a incoherencias en años anteriores. Debido a la naturaleza descentralizada del banco, en ocasiones los sistemas se han identificados como no conformes; no obstante, no se ha informado de incidencias en los últimos meses.
- Probabilidad de peligro de los “hosts” remotos: alta. Los “hosts” remotos normalmente no son compatibles durante largos períodos de tiempo. También se han identificado incidencias recientes relacionadas con infecciones de virus y gusanos en los hosts remotos.

Tarea 3: Completar la lista de nivel de resumen

Después de que el equipo de administración de riesgos de seguridad estime la probabilidad, utilice la siguiente figura para seleccionar la clasificación de riesgo de nivel de resumen.

Nota: Según resulte adecuado para su organización, el nivel de riesgo de una repercusión media combinada con una probabilidad media se puede definir como riesgo alto. Definir los niveles de riesgo independientemente del proceso de evaluación de riesgos proporciona las indicaciones necesarias para tomar esta decisión. Cada organización debe definir lo que significa riesgo alto para su propia empresa.
Ejemplo de Woodgrove: la combinación de las clasificaciones de repercusiones y de probabilidad da como resultado las siguientes clasificaciones de riesgos:

- **Riesgo de robo por parte de empleados de confianza: bajo (repercusión media, probabilidad baja)**
- **Riesgo de peligro de los hosts de la LAN: alto (repercusión alta, probabilidad media)**
- **Riesgo de peligro de los hosts remotos: alto (repercusión alta, probabilidad alta)**

Revisión con los participantes

La siguiente tarea del proceso de asignación de prioridades es la revisión de los resultados de resumen con los participantes. Los objetivos son mantener informados a los participantes acerca del proceso de evaluación de riesgos y solicitar su colaboración para seleccionar los riesgos de los que se realizará un análisis más detallado. Utilice los siguientes criterios al seleccionar los riesgos que se incluirá en el proceso de asignación de prioridades de nivel detallado:

Riesgos de nivel alto: los riesgos clasificados como altos se deben incluir en la lista detallada. Cada riesgo alto debe tener una resolución después del proceso de apoyo a la toma de decisiones; por ejemplo, aceptar el riesgo o desarrollar una solución de mitigación.
Riesgos dudosos: cree el análisis de asignación de prioridades detallado para riesgos moderados que requieren una resolución. En algunas organizaciones se pueden llegar a incluir todos los riesgos moderados en la lista detallada.
Riesgos controvertidos: si un riesgo es nuevo, no se ha comprendido bien o los participantes tienen distintos puntos de vista, cree el análisis detallado para que los participantes tenga un conocimiento más preciso del riesgo.