

## CAPÍTULO

# 28

## ADMINISTRACIÓN DEL RIESGO

### CONCEPTOS CLAVE

categorías de riesgo .....	642
estrategias .....	641
proactiva .....	641
reactiva .....	641
exposición al riesgo .....	648
identificación .....	642
lista de verificación de ítem de riesgo .....	643
MMMR .....	651
proyección .....	644
refinamiento .....	649
seguridad y riesgos .....	651
tabla de riesgo .....	645
valoración .....	643

**E**n su libro acerca de administración y análisis de riesgos, Robert Charette [Cha89] presenta una definición conceptual de riesgo:

Primero, el riesgo se preocupa por los acontecimientos futuros. Ayer y hoy están más allá de la preocupación activa, pues ya cosechamos lo que previamente se sembró por nuestras acciones pasadas. La cuestión tiene que ver, por tanto, con si podemos, al cambiar nuestras acciones de hoy, crear una oportunidad para una situación diferente y esperanzadoramente mejor para nosotros en el mañana. Esto significa, segundo, que el riesgo involucra cambio, como en los cambios de mentalidad, de opinión, de acciones o de lugares [...] [Tercero,] el riesgo involucra elección y la incertidumbre que ella conlleva. En consecuencia, paradójicamente, el riesgo, como la muerte y los impuestos, es una de las pocas certezas de la vida.

Cuando se considera el riesgo en el contexto de la ingeniería del software, los tres fundamentos conceptuales de Charette siempre están presentes. El futuro es su preocupación: ¿qué riesgos pueden hacer que el proyecto de software salga defectuoso? El cambio es lo que preocupa: ¿cómo afectan en los cronogramas y en el éxito global los cambios que puede haber en los requisitos del cliente, en las tecnologías de desarrollo, en los entornos meta y en todas las otras entidades conectadas con el proyecto? Por último, se debe lidiar con las opciones: ¿qué métodos y herramientas deben usarse, cuántas personas deben involucrarse, cuánto énfasis es “suficiente” poner en la calidad?

Peter Drucker [Dru75] dijo alguna vez: “aunque sea fútil intentar eliminar el riesgo, y cuestionable intentar minimizarlo, es esencial que los riesgos tomados sean los riesgos correctos”.

### UNA MIRADA RÁPIDA

**¿Qué es?** El análisis y la administración del riesgo son acciones que ayudan al equipo de software a entender y manejar la incertidumbre. Muchos problemas pueden plagar un proyecto de software. Un riesgo es un problema potencial: puede ocurrir, puede no ocurrir. Pero, sin importar el resultado, realmente es una buena idea identificarlo, valorar su probabilidad de ocurrencia, estimar su impacto y establecer un plan de contingencia para el caso de que el problema realmente ocurra.

**¿Quién lo hace?** Todos los involucrados en el proceso de software (gerentes, ingenieros de software y otros interesados) participan en el análisis y la administración del riesgo.

**¿Por qué es importante?** Piense en la consigna de los boy scouts: “estar preparados”. El software es una empresa difícil. Muchas cosas pueden salir mal y, francamente, muchas con frecuencia lo hacen. Por esta razón es que estar preparado, comprender los riesgos y tomar medidas proactivas para evitarlos o manejarlos son elementos clave de una buena administración de proyecto de software.

**¿Cuáles son los pasos?** Reconocer qué puede salir mal es el primer paso, llamado “identificación de riesgos”. A continuación, cada riesgo se analiza para determinar la probabilidad de que ocurra y el daño que causará si ocurre. Una vez establecida esta información se clasifican los riesgos, por probabilidad e impacto. Finalmente, se desarrolla un plan para manejar aquellos que tengan alta probabilidad y alto impacto.

**¿Cuál es el producto final?** Se produce un plan para mitigar, monitorear y manejar el riesgo (MMMR) o un conjunto de hojas de información de riesgo.

**¿Cómo me aseguro de que lo hice bien?** Los riesgos que se analizan y manejan deben inferirse a partir de un estudio del personal, el producto, el proceso y el proyecto. El MMMR debe revisarse conforme avance el proyecto para asegurarse de que los riesgos se mantienen actualizados. Los planes de contingencia para administración del riesgo deben ser realistas.

Antes de poder identificar los “riesgos correctos” que se van a tomar durante un proyecto de software, es importante identificar todos los que son obvios para gerentes y profesionales.

## 28.1 ESTRATEGIAS REACTIVAS DE RIESGO FRENTE

### A ESTRATEGIAS PROACTIVAS DE RIESGO



#### Cita:

**“Si no atacas de manera activa los riesgos, ellos te atacarán de manera activa.”**

Tom Gilb

Las estrategias *reactivas* de riesgo se han llamado irrisoriamente la “escuela de gestión de riesgo de Indiana Jones” [Tho92]. En las películas que llevan su nombre, Indiana Jones, cuando enfrenta una dificultad abrumadora, invariablemente dice: “No te preocupes, ¡pensaré en algo!”. Al nunca preocuparse por los problemas hasta que suceden, Indy reaccionará en alguna forma heroica.

Tristemente, el gerente promedio de proyectos de software no es Indiana Jones y los miembros del equipo del proyecto de software no son sus fieles ayudantes. Sin embargo, la mayoría de los equipos de software se apoyan exclusivamente en estrategias reactivas de riesgo. Cuando mucho, una estrategia reactiva monitorea el proyecto para riesgos probables. Los recursos se hacen a un lado para lidiar con los riesgos, hasta que se convierten en problemas reales. De manera más común, el equipo de software no hace nada acerca de los riesgos hasta que algo sale mal. Entonces el equipo se apresura a entrar en acción con la intención de corregir el problema rápidamente. Con frecuencia esto se llama *modo bombero*. Cuando falla, la “administración de crisis” [Cha92] toma el control y el proyecto está en un peligro real.

Una estrategia considerablemente más inteligente para la administración del riesgo es ser proactivo. Una estrategia *proactiva* comienza mucho antes de iniciar el trabajo técnico. Los riesgos potenciales se identifican, su probabilidad e impacto se valoran y se clasifican por importancia. Luego, el equipo de software establece un plan para gestionar el riesgo. El objetivo principal es evitarlo, pero, dado que no todos los riesgos son evitables, el equipo trabaja para desarrollar un plan de contingencia que le permitirá responder en forma controlada y efectiva. A lo largo del resto de este capítulo se estudia una estrategia proactiva de gestión del riesgo.

## 28.2 RIESGOS DE SOFTWARE

Aunque hay un considerable debate acerca de la definición adecuada de riesgo de software, existe un acuerdo general en que los riesgos siempre involucran dos características: *incertidumbre* (el riesgo puede o no ocurrir; es decir, no hay riesgos 100 por ciento probables<sup>1</sup>) y *pérdida* (si el riesgo se vuelve una realidad, ocurrirán consecuencias o pérdidas no deseadas [Hig95]). Cuando se analizan los riesgos es importante cuantificar el nivel de incertidumbre y el grado de pérdidas asociados con cada riesgo. Para lograr esto, se consideran diferentes categorías de riesgos.



**¿Qué tipos de riesgos es probable encontrar conforme se construye el software?**

Los *riesgos del proyecto* amenazan el plan del proyecto, es decir, si los riesgos del proyecto se vuelven reales, es probable que el calendario del proyecto se deslice y que los costos aumenten. Los riesgos del proyecto identifican potenciales problemas de presupuesto, calendario, personal (tanto técnico como en la organización), recursos, participantes y requisitos, así como su impacto sobre un proyecto de software. En el capítulo 26, la complejidad, el tamaño y el grado de incertidumbre estructural del proyecto también se definieron como factores de riesgos para el proyecto (y la estimación).

Los *riesgos técnicos* amenazan la calidad y temporalidad del software que se va a producir. Si un riesgo técnico se vuelve una realidad, la implementación puede volverse difícil o imposible. Los riesgos técnicos identifican potenciales problemas de diseño, implementación, interfaz,

<sup>1</sup> Un riesgo que es 100 por ciento probable es una restricción sobre el proyecto de software.

verificación y mantenimiento. Además, la ambigüedad en la especificación, la incertidumbre técnica, la obsolescencia técnica y la tecnología “de punta” también son factores de riesgo. Los riesgos técnicos ocurren porque el problema es más difícil de resolver de lo que se creía.

Los *riesgos empresariales* amenazan la viabilidad del software que se va a construir y con frecuencia ponen en peligro el proyecto o el producto. Los candidatos para los cinco principales riesgos empresariales son: 1) construir un producto o sistema excelente que realmente no se quiere (riesgo de mercado), 2) construir un producto que ya no encaje en la estrategia empresarial global de la compañía (riesgo estratégico), 3) construir un producto que el equipo de ventas no sabe cómo vender (riesgo de ventas), 4) perder el apoyo de los administradores debido a un cambio en el enfoque o en el personal (riesgo administrativo) y 5) perder apoyo presupuestal o de personal (riesgos presupuestales).

Es extremadamente importante observar que la categorización simple de riesgos no siempre funciona. Algunos de ellos son simplemente impredecibles por adelantado.

Otra categorización general de los riesgos es la propuesta por Charette [Cha89]. Los *riesgos conocidos* son aquellos que pueden descubrirse después de una evaluación cuidadosa del plan del proyecto, del entorno empresarial o técnico donde se desarrolla el proyecto y de otras fuentes de información confiables (por ejemplo, fecha de entrega irreal, falta de requisitos documentados o ámbito de software, pobre entorno de desarrollo). Los *riesgos predecibles* se extrapolan de la experiencia en proyectos anteriores (por ejemplo, rotación de personal, pobre comunicación con el cliente, disolución del esfuerzo del personal conforme se atienden las solicitudes de mantenimiento). Los *riesgos impredecibles* son el comodín en la baraja. Pueden ocurrir y lo hacen, pero son extremadamente difíciles de identificar por adelantado.

### Cita:

**“Los proyectos sin riesgos reales son perdedores. Casi siempre están desprovistos de beneficio; es por esto por lo que no se hicieron años atrás.”**

Tom DeMarco y Tim Lister

### INFORMACIÓN



#### Siete principios de la administración de riesgos

El Software Engineering Institute (SEI) ([www.sei.cmu.edu](http://www.sei.cmu.edu)) identifica siete principios que “ofrecen un marco conceptual para lograr una administración de riesgo efectiva”. Éstos son:

**Mantener una perspectiva global:** ver los riesgos del software dentro del contexto de un sistema donde el riesgo es un componente y el problema empresarial que se pretende resolver.

**Tomar una visión de previsión:** pensar en los riesgos que pueden surgir en el futuro (por ejemplo, debido a cambios en el software); establecer planes de contingencia de modo que los eventos futuros sean manejables.

**Alentar la comunicación abierta:** si alguien enuncia un riesgo potencial, no lo ignore. Si un riesgo se propone de manera informal, considéralo. Aliente a todos los participantes y usuarios a sugerir riesgos en cualquier momento.

**Integrar:** una consideración de riesgo debe integrarse en el proceso del software.

**Enfatizar un proceso continuo:** el equipo debe vigilar a lo largo del proceso de software, modificar los riesgos identificados conforme se conozca más información y agregar unos nuevos conforme se logre mejor comprensión.

**Desarrollar una visión de producto compartida:** si todos los participantes comparten la misma visión del software, es probable que haya mejor identificación y valoración del riesgo.

**Alentar el trabajo en equipo:** los talentos, habilidades y conocimientos de todos los participantes deben reunirse cuando se realicen actividades de administración de riesgos.

### 28.3 IDENTIFICACIÓN DE RIESGOS

La identificación de riesgos es un intento sistemático por especificar amenazas al plan del proyecto (estimaciones, calendario, carga de recursos, etc.). Al identificar los riesgos conocidos y predecibles, el gerente de proyecto da un primer paso para evitarlos cuando es posible y para controlarlos cuando es necesario.

Existen dos tipos distintos de riesgos para cada una de las categorías que se presentaron en la sección 28.2: riesgos genéricos y riesgos específicos del producto. Los *riesgos genéricos* son una amenaza potencial a todo proyecto de software. Los *riesgos específicos del producto* pueden



*Aunque es importante considerar los riesgos genéricos, son los riesgos específicos del producto los que provocan más dolores de cabeza. Asegúrese de emplear tiempo para identificar tantos riesgos específicos del producto como sea posible.*

identificarse solamente por quienes tienen clara comprensión de la tecnología, el personal y el entorno específico del software que se construye. Para identificar los riesgos específicos del producto, examine el plan del proyecto y el enunciado de ámbito del software, y desarrolle una respuesta a la siguiente pregunta: ¿qué características especiales de este producto pueden amenazar el plan del proyecto?

Un método para identificar riesgos es crear una lista de verificación de ítem de riesgo. La lista de verificación puede usarse para identificación del riesgo y así enfocarse sobre algún subconjunto de riesgos conocidos y predecibles en las siguientes subcategorías genéricas:

- *Tamaño del producto*: riesgos asociados con el tamaño global del software que se va a construir o a modificar.
- *Impacto empresarial*: riesgos asociados con restricciones impuestas por la administración o por el mercado.
- *Características de los participantes*: riesgos asociados con la sofisticación de los participantes y con la habilidad de los desarrolladores para comunicarse con los participantes en forma oportuna.
- *Definición del proceso*: riesgos asociados con el grado en el que se definió el proceso de software y la manera como se sigue por parte de la organización desarrolladora.
- *Entorno de desarrollo*: riesgos asociados con la disponibilidad y calidad de las herramientas por usar para construir el producto.
- *Tecnología por construir*: riesgos asociados con la complejidad del sistema que se va a construir y con lo "novedoso" de la tecnología que se incluye en el sistema.
- *Tamaño y experiencia del personal*: riesgos asociados con la experiencia técnica y de proyecto global de los ingenieros de software que harán el trabajo.

La lista de verificación de ítem de riesgo puede organizarse en diferentes formas. Las preguntas relevantes en cada uno de los temas pueden responderse para cada proyecto de software. Las respuestas a dichas preguntas permiten estimar el impacto del riesgo. Un formato diferente de lista de verificación de ítem de riesgo simplemente menciona las características que son relevantes en cada subcategoría genérica. Finalmente, se menciona un conjunto de "componentes y promotores de riesgo" [AFC88] junto con sus probabilidades de ocurrencia. Los promotores de desempeño, apoyo, costo y calendario se analizan en respuesta a las preguntas anteriores.

Algunas listas de verificación exhaustivas para riesgo de proyecto de software están disponibles en la red (por ejemplo, [Baa07], [NAS07], [Wor04]). Puede usar dichas listas de verificación para comprender los riesgos genéricos para proyectos de software.

### 28.3.1 Valoración del riesgo de proyecto global

Las siguientes preguntas se infirieron de los datos de riesgo obtenidos al entrevistar en diferentes partes del mundo a gerentes de proyectos de software experimentados [Kei98]. Las preguntas se ordenan por su importancia relativa para el éxito del proyecto.



**¿El proyecto de software en el que trabaja está en serio peligro?**

1. ¿Los gerentes de software y de cliente se reunieron formalmente para apoyar el proyecto?
2. ¿Los usuarios finales se comprometen de manera entusiasta con el proyecto y con el sistema/producto que se va a construir?
3. ¿El equipo de ingeniería del software y sus clientes entienden por completo los requisitos?
4. ¿Los clientes se involucraron plenamente en la definición de los requisitos?
5. ¿Los usuarios finales tienen expectativas realistas?

6. ¿El ámbito del proyecto es estable?
7. ¿El equipo de ingeniería del software tiene la mezcla correcta de habilidades?
8. ¿Los requisitos del proyecto son estables?
9. ¿El equipo de proyecto tiene experiencia con la tecnología que se va a implementar?
10. ¿El número de personas que hay en el equipo del proyecto es adecuado para hacer el trabajo?
11. ¿Todas las divisiones de cliente/usuario están de acuerdo en la importancia del proyecto y en los requisitos para el sistema/producto que se va a construir?

**WebRef**

*Risk radar* es una base de datos y herramientas que ayudan a los gerentes a identificar, clasificar y comunicar riesgos de proyecto. Puede encontrarse en [www.spmn.com](http://www.spmn.com)

Si alguna de estas preguntas se responde de manera negativa deben establecerse sin falta pasos de mitigación, monitoreo y gestión. El grado en el que el proyecto está en riesgo es directamente proporcional al número de respuestas negativas a dichas preguntas.

### 28.3.2 Componentes y promotores de riesgo

La fuerza aérea estadounidense [AFC88] publicó un escrito que contiene excelentes lineamientos para la identificación y reducción de los riesgos de software. El enfoque de la fuerza aérea requiere que el gerente del proyecto identifique los promotores de riesgo que afectan los componentes de riesgo de software: rendimiento, costo, apoyo y calendario. En el contexto de este análisis, los componentes de riesgo se definen en la forma siguiente:

- *Riesgo de rendimiento*: grado de incertidumbre de que el producto satisfará sus requisitos y se ajustará al uso pretendido.
- *Riesgo de costo*: grado de incertidumbre de que el presupuesto del proyecto se mantendrá.
- *Riesgo de apoyo*: grado de incertidumbre de que el software resultante será fácil de corregir, adaptar y mejorar.
- *Riesgo de calendario*: grado de incertidumbre de que el calendario del proyecto se mantendrá y de que el producto se entregará a tiempo.

**Cita:**

"La administración del riesgo es administración de proyecto para adultos."

Tim Lister

El impacto de cada promotor de riesgo sobre el componente de riesgo se divide en una de cuatro categorías de impacto: despreciable, marginal, crítico o catastrófico. En la figura 28.1 [Boe89] se describe una caracterización de las potenciales consecuencias de errores (hileras con etiqueta 1) o de un fallo para lograr el resultado deseado (hileras con etiqueta 2). La categoría de impacto se elige con base en la caracterización que se ajusta mejor a la descripción en la tabla.

## 28.4 PROYECCIÓN DEL RIESGO

La proyección del riesgo, también llamada *estimación del riesgo*, intenta calificar cada riesgo en dos formas: 1) la posibilidad o probabilidad de que el riesgo sea real y 2) las consecuencias de los problemas asociados con el riesgo, en caso de que ocurra. Usted trabaja junto con otros gerentes y personal técnico para realizar cuatro pasos de proyección de riesgo:

1. Establecer una escala que refleje la probabilidad percibida de un riesgo.
2. Delinear las consecuencias del riesgo.
3. Estimar el impacto del riesgo sobre el proyecto y el producto.
4. Valorar la precisión global de la proyección del riesgo de modo que no habrá malos entendidos.

**FIGURA 28.1**

**Valoración de impacto.**  
Fuente: [Boe89].

Componentes		Rendimiento	Apoyo	Costo	Calendario
Categoría					
<b>Catastrófico</b>	1	La falla para satisfacer el requisito resultaría en fallo en la misión		La falla da como resultado aumento de costos y demoras en el calendario, con valores esperados en exceso de US\$500K	
	2	Degradoación significativa para no lograr el rendimiento técnico	Software que no responde o no puede tener apoyo	Significativos recortes financieros, probable agotamiento de presupuesto	IOC inalcanzable
<b>Crítico</b>	1	Falla para satisfacer el requisito degradaría el rendimiento del sistema hasta un punto donde el éxito de la misión sería cuestionable		La falla da como resultado demoras operativas y/o aumento de costos con valor esperado de US\$100K a US\$500K	
	2	Cierta reducción en rendimiento técnico	Demoras menores en modificaciones de software	Cierto recorte de recursos financieros, posible agotamiento	Possible deterioro en IOC
<b>Marginal</b>	1	Falla para satisfacer los requisitos resultaría en degradación de misión secundaria		Costos, impactos y/o calendario recuperable se deterioran con valor esperado de US\$1K a US\$100K	
	2	Reducción mínima a pequeña en rendimiento técnico	Apoyo de software receptivo	Suficientes recursos financieros	Calendario realista, alcanzable
<b>Despreciable</b>	1	Falla para satisfacer requisitos crearía inconvenientes o impacto no operativo		Error da como resultado costo menor y/o impacto en calendario con valor esperado de menos de US\$1K	
	2	No reducción en rendimiento técnico	Software fácilmente soportable	Possible subejercicio de presupuesto	IOC alcanzable con facilidad

Nota: 1) La consecuencia potencial de errores o fallos de software no detectados.

2) La consecuencia potencial si el resultado deseado no se alcanza.



Piense duro acerca del software que está a punto de construir y pregúntese, ¿qué puede salir mal? Cree su propia lista y pida a otros miembros del equipo que hagan lo mismo.

La intención de estos pasos es considerar los riesgos de manera que conduzcan a una priorización. Ningún equipo de software tiene los recursos para abordar todo riesgo posible con el mismo grado de rigor. Al priorizar los riesgos es posible asignar recursos donde tendrán más impacto.

#### 28.4.1 Elaboración de una tabla de riesgos

Una tabla de riesgos proporciona una técnica simple para proyección de riesgos.<sup>2</sup> Una tabla de muestra de riesgo se ilustra en la figura 28.2.

Comience por elaborar una lista de todos los riesgos (sin importar cuán remotos sean) en la primera columna de la tabla. Esto puede lograrse con la ayuda de las listas de verificación de ítem de riesgo mencionadas en la sección 28.3. Cada riesgo se clasifica en la segunda columna (por ejemplo, TP implica un riesgo de tamaño de proyecto, EMP implica un riesgo empresarial). La probabilidad de ocurrencia de cada riesgo se ingresa en la siguiente columna de la tabla. El valor de probabilidad para cada riesgo puede estimarse individualmente por los miembros del equipo. Una forma de lograr esto es encuestar a todos los miembros del equipo hasta que su valoración colectiva de la probabilidad del riesgo comience a convergir.

A continuación, se valora el impacto de cada riesgo. Cada componente de riesgo se valora usando la caracterización que se presenta en la figura 28.1 y se determina una categoría de

<sup>2</sup> La tabla de riesgos puede implementarse como un modelo de hoja de cálculo. Esto permite fácil manipulación y ordenamiento de las entradas.

**FIGURA 28.2**

Ejemplo de tabla de riesgo previo al ordenamiento

Riesgos	Categoría	Probabilidad	Impacto	RMMR
Estimación de tamaño puede ser significativamente baja	PS	60%	2	
Mayor número de usuarios que el planificado	PS	30%	3	
Menos reuso que el planificado	PS	70%	2	
Usuarios finales que se resisten al sistema	BU	40%	3	
Fecha de entrega será apretada	BU	50%	2	
Pérdida de fondos	CU	40%	1	
Cliente cambiará requisitos	PS	80%	2	
Tecnología no satisfará las expectativas	TE	30%	1	
Falta de capacitación en herramientas	DE	80%	3	
Personal inexperto	ST	30%	2	
Alta rotación de personal	ST	60%	2	
Σ				
Σ				
Σ				

Valores de impacto:

- 1—catastrófico
- 2—crítico
- 3—marginal
- 4—despreciable

impacto. Las categorías para cada uno de los cuatro componentes de riesgo (rendimiento, apoyo, costo y calendario) se promedian<sup>3</sup> para determinar un valor de impacto global.

Una vez completadas las primeras cuatro columnas de la tabla de riesgos, la tabla se ordena por probabilidad y por impacto. Los riesgos de alta probabilidad y alto impacto se ubican en la parte superior de la tabla y los riesgos de baja probabilidad se ubican en el fondo. Esto logra una priorización de riesgo de primer orden.

Es posible estudiar la tabla ordenada resultante y definir una línea de corte. La *línea de corte* (dibujada horizontalmente en algún punto de la tabla) implica que sólo los riesgos que se encuentran por arriba de la línea recibirán mayor atención. Los riesgos que caen por abajo de la línea se vuelven a valorar para lograr una priorización de segundo orden. En la figura 28.3, el impacto y la probabilidad del riesgo tienen una influencia distinta sobre la preocupación de la administración. Un factor de riesgo que tenga un alto impacto pero una muy baja probabilidad de ocurrencia no debe absorber una cantidad significativa de tiempo administrativo. Sin embargo, los riesgos de alto impacto con probabilidad moderada alta y los riesgos de bajo impacto con alta probabilidad deben someterse a los siguientes pasos del análisis de riesgos.

Todos los riesgos que se encuentran por arriba de la línea de corte deben manejarse. La columna marcada MMRM contiene un apuntador al *plan de mitigación, monitoreo y manejo de riesgo* o, alternativamente, en una colección de hojas de información de riesgo desarrolladas para todos los riesgos que se encuentran arriba del corte. El plan MMRM y las hojas de información de riesgo se estudian en las secciones 28.5 y 28.6.

La probabilidad del riesgo puede determinarse al hacer estimaciones individuales y luego desarrollar un solo valor de consenso. Aunque dicho enfoque es factible, se han desarrollado técnicas más sofisticadas para determinar la probabilidad del riesgo [AFC88]. Los promotores de riesgo pueden valorarse sobre una escala de probabilidad cualitativa que tenga los siguientes valores: imposible, improbable, probable y frecuente. Entonces puede asociarse probabilidad

### PUNTO CLAVE

Una tabla de riesgos se ordena por probabilidad e impacto para clasificar riesgos.

#### Cita:

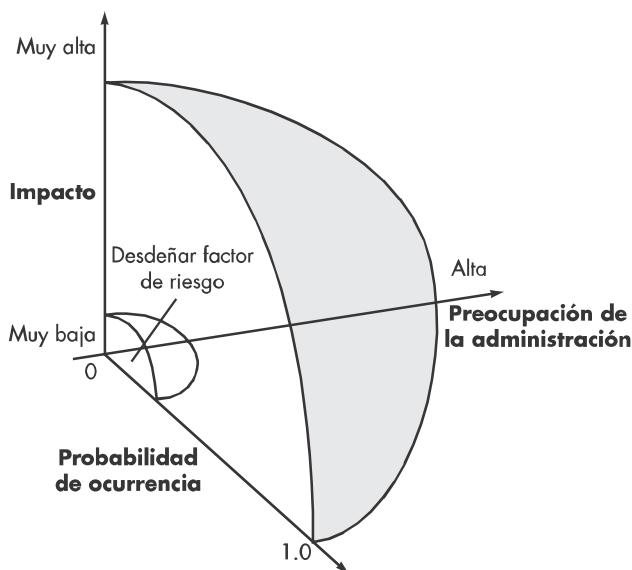
"[Hoy] nadie tiene el lujo de poder conocer una tarea tan bien como para que no contenga sorpresas, y las sorpresas significan riesgo."

Stephen Grey

<sup>3</sup> Puede usar un promedio ponderado si un componente de riesgo tiene más significado para un proyecto.

**FIGURA 28.3**

Riesgo y preocupación de la administración



matemática con cada valor cualitativo (por ejemplo, una probabilidad de 0.7 a 0.99 implica un riesgo enormemente probable).

#### 28.4.2 Valoración de impacto de riesgo

Tres factores afectan las probables consecuencias si ocurre un riesgo: su naturaleza, su ámbito y su temporización. La naturaleza del riesgo indica los problemas probables si ocurre. Por ejemplo, una interfaz externa pobremente definida en el hardware cliente (un riesgo técnico) impedirá el diseño y las pruebas tempranas, y probablemente conducirá más tarde a problemas de integración de sistema en un proyecto. El ámbito de un riesgo combina la severidad (¿cuán serio es?) con su distribución global (¿cuánto del proyecto se afectará o cuántos participantes se dañarán?). Finalmente, la temporización de un riesgo considera cuándo y por cuánto tiempo se sentirá el impacto. En la mayoría de los casos se quiere que las "malas noticias" ocurran tan pronto como sea posible, pero en algunos, mientras más se demoren, mejor.

**?** ¿Cómo se valoran las consecuencias de un riesgo?

Regrese una vez más al enfoque de análisis de riesgos que propuso la fuerza aérea estadounidense [AFC88]; puede aplicar los siguientes pasos para determinar las consecuencias globales de un riesgo: 1) determine la probabilidad promedio del valor de ocurrencia para cada componente de riesgo; 2) con la figura 28.1, determine el impacto para cada componente con base en los criterios mostrados, y 3) complete la tabla de riesgos y analice los resultados como se describe en las secciones anteriores.

La exposición al riesgo global, ER, se determina usando la siguiente relación [Hal98]:

$$ER = P \times C$$

donde  $P$  es la probabilidad de ocurrencia para un riesgo y  $C$  es el costo para el proyecto si ocurre el riesgo.

Por ejemplo, suponga que el equipo de software define un riesgo de proyecto en la forma siguiente:

**Identificación de riesgo.** De hecho, sólo 70 por ciento de los componentes de software calendarizados para reuso se integrarán en la aplicación. La funcionalidad restante tendrá que desarrollarse a la medida.

**Probabilidad del riesgo.** Un 80 por ciento (probable).

**Impacto del riesgo.** Se planificaron 60 componentes de software reutilizables. Si sólo puede usarse 70 por ciento, tendrán que desarrollarse 18 componentes desde cero (además de otro software a la medida que se calendarizó para desarrollo). Dado que el componente promedio es de 100 LOC y que los datos locales indican que el costo de la ingeniería del software para cada LOC es US\$14.00, el costo global (impacto) para desarrollar los componentes sería  $18 \times 100 \times 14 = \text{US\$}25\,200$ .

**Exposición al riesgo.**  $\text{ER} = 0.80 \times 25\,200 \sim \text{US\$}20\,200$ .



Compare la ER para todos los riesgos con la estimación de costo para el proyecto. Si ER es mayor a 50 por ciento del costo del proyecto, debe evaluarse la viabilidad de éste.

La exposición al riesgo puede calcularse para cada riesgo en la tabla de riesgo, una vez hecha la estimación del costo del riesgo. La exposición al riesgo total para todos los riesgos (arriba del corte en la tabla de riesgos) puede proporcionar los medios para ajustar la estimación del costo final para un proyecto. También puede usarse para predecir el aumento probable en recursos de personal requeridos en varios puntos durante el calendario del proyecto.

La proyección del riesgo y las técnicas de análisis descritas en las secciones 28.4.1 y 28.4.2 se aplican de manera iterativa conforme avanza el proyecto de software. El equipo del proyecto debe revisar la tabla de riesgos a intervalos regulares, reevaluar cada riesgo para determinar cuándo nuevas circunstancias cambian su probabilidad e impacto. Como consecuencia de esta actividad, acaso sea necesario agregar nuevos riesgos a la tabla, eliminar algunos riesgos que ya no son relevantes e incluso cambiar las posiciones relativas de otros.

## CASASEGURA



### Análisis de riesgos

**La escena:** Oficina de Doug Miller antes de comenzar el proyecto de software CasaSegura.

**Participantes:** Doug Miller (gerente del equipo de ingeniería del software CasaSegura) y Vinod Raman, Jamie Lazar y otros miembros del equipo de ingeniería de software del producto.

#### La conversación:

**Doug:** Me gustaría usar algo de tiempo en una lluvia de ideas para el proyecto CasaSegura.

**Jamie:** ¿Acerca de qué puede salir mal?

**Doug:** Sí. Aquí hay algunas categorías donde las cosas pueden salir mal. [Muestra a todos las categorías anotadas en la introducción a la sección 28.3.]

**Vinod:** Hmm... quieras que sólo las mencionemos o...

**Doug:** No. Esto es lo que creo que debemos hacer. Todo mundo haga una lista de riesgos... ahora...

[Transcurren diez minutos, todos escriben].

**Doug:** Muy bien, deténganse.

**Jamie:** ¡Pero no he terminado!

**Doug:** Está bien. Revisaremos la lista de nuevo. Ahora, para cada ítem en su lista, asignen un porcentaje de probabilidad de que ocurrirá el riesgo. Luego, asignen un impacto al proyecto sobre una escala de 1 (menor) a 5 (catastrófico).

**Vinod:** Si creo que el riesgo es un volado, específico una probabilidad de 50 por ciento y, si creo que tendrá un impacto de proyecto moderado, específico un 3, ¿cierto?

**Doug:** Exactamente.

[Transcurren cinco minutos, todos escriben].

**Doug:** Muy bien, deténganse. Ahora haremos una lista grupal en el pizarrón. Yo escribiré; cada uno de ustedes dirá una entrada de su lista.

[Transcurren quince minutos; crean la lista].

**Jamie (apunta hacia el pizarrón y ríe):** Vinod, ese riesgo (apunta hacia una entrada en el pizarrón) es ridículo. Hay una mayor probabilidad de que a todos nos caiga un rayo. Debemos removerlo.

**Doug:** No, dejémoslo por ahora. Consideraremos todos los riesgos, sin importar cuán locos parezcan. Más tarde filtraremos la lista.

**Jamie:** Pero ya tenemos más de 40 riesgos... ¿cómo vamos a manejarlos todos?

**Doug:** No podemos. Es por eso por lo que definiremos un corte después de ordenarlos. Yo haré ese corte y nos reuniremos de nuevo mañana. Por ahora, regresen a trabajar... y en su tiempo libre piensen en cualquier riesgo que hayan olvidado.

## 28.5 REFINAMIENTO DEL RIESGO

**?** ¿Cuál es una buena forma de describir un riesgo?

Durante las primeras etapas de la planificación del proyecto, un riesgo puede enunciarse de manera muy general. Conforme pasa el tiempo y se aprende más acerca del proyecto y de los riesgos, es posible refinar el riesgo en un conjunto de riesgos más detallados, cada uno un poco más sencillo de mitigar, monitorear y manejar.

Una forma de hacer esto es representar el riesgo en formato *condición-transición-consecuencia* (CTC) [Glu94]. Es decir, el riesgo se enuncia en la forma siguiente:

Dado que <condición> entonces hay preocupación porque (posiblemente) <consecuencia>.

Al usar el formato CTC para el riesgo de reutilización anotado en la sección 28.4.2, podría escribir:

Dado que todos los componentes de software reutilizables deben apegarse a estándares de diseño específicos y dado que algunos no se apegan, entonces existe preocupación de que (posiblemente) sólo 70 por ciento de los módulos reutilizables planeados puedan realmente integrarse en el sistema que se va a construir, lo que da como resultado la necesidad de ingeniería a la medida del restante 30 por ciento de los componentes.

Esta condición general puede refinarse en la forma siguiente:

**Subcondición 1.** Ciertos componentes reutilizables los desarrolló una tercera persona sin conocimiento de los estándares de diseño internos.

**Subcondición 2.** El estándar de diseño para interfaces de componente todavía no se consolida y puede no apegarse a ciertos componentes reutilizables existentes.

**Subcondición 3.** Ciertos componentes reutilizables se implementaron en un lenguaje que no se soporta en el entorno blanco.

Las consecuencias asociadas con estas subcondiciones refinadas permanecen iguales (es decir, 30 por ciento de componentes de software deben someterse a ingeniería a la medida), pero el refinamiento ayuda a aislar los riesgos subyacentes y puede conducir a análisis y respuestas más sencillos.

## 28.6 MITIGACIÓN, MONITOREO Y MANEJO DE RIESGO

**Cita:**  
"Si tomo muchas precauciones, es porque no dejo nada al azar."  
**Napoleón**

Todas las actividades de análisis de riesgos presentadas hasta el momento tienen una sola meta: auxiliar al equipo del proyecto a desarrollar una estrategia para lidiar con el riesgo. Una estrategia efectiva debe considerar tres temas: 1) evitar el riesgo, 2) monitorear el riesgo y 3) manejar el riesgo y planificar la contingencia.

Si un equipo de software adopta un enfoque proactivo ante el riesgo, evitarlo siempre es la mejor estrategia. Esto se logra desarrollando un plan para *mitigación del riesgo*. Por ejemplo, suponga que una alta rotación de personal se observa como un riesgo de proyecto  $r_1$ . Con base en la historia y la intuición administrativa, la probabilidad  $I_1$  de alta rotación se estima en 0.70 (70 por ciento, más bien alta) y el impacto  $x_1$  se proyecta como crítico, es decir, la alta rotación tendrá un impacto crítico sobre el costo y el calendario del proyecto.

Para mitigar este riesgo se desarrollará una estrategia a fin de reducir la rotación. Entre los posibles pasos por tomar están:

- Reunirse con el personal actual para determinar las causas de la rotación (por ejemplo, pobres condiciones laborales, salario bajo, mercado laboral competitivo).
- Mitigar aquellas causas que están bajo su control antes de comenzar el proyecto.

**?** ¿Qué puede hacerse para mitigar el riesgo?

- Una vez iniciado el proyecto, suponer que la rotación ocurrirá y desarrollar técnicas para asegurar la continuidad cuando el personal se vaya.
- Organizar equipos de trabajo de modo que la información acerca de cada actividad de desarrollo se disperse ampliamente.
- Definir estándares de producto operativo y establecer mecanismos para asegurar que todos los modelos y documentos se desarrollen en forma oportuna.
- Realizar revisiones de pares de todo el trabajo (de modo que más de una persona “se ponga al día”).
- Asignar un miembro de personal de respaldo para cada técnico crítico.

Conforme avanza el proyecto, comienzan las actividades de *monitoreo de riesgos*. El gerente de proyecto monitorea factores que pueden proporcionar un indicio de si el riesgo se vuelve más o menos probable. En el caso de alta rotación de personal se monitorean: la actitud general de los miembros del equipo con base en presiones del proyecto, el grado en el que el equipo cuaja, relaciones interpersonales entre miembros del equipo, potenciales problemas con la compensación y beneficios, y la disponibilidad de empleos dentro de la compañía y fuera de ella.

Además de monitorear dichos factores, un gerente de proyecto debe dar seguimiento a la efectividad de los pasos de mitigación del riesgo. Por ejemplo, un paso de mitigación del riesgo anotado aquí requiere la definición de estándares de producto operativo y mecanismos para asegurarse de que los productos operativos se desarrollan en forma oportuna. Éste es un mecanismo para asegurar continuidad en caso de que un individuo crucial deje el proyecto. El gerente de proyecto debe monitorear los productos operativos cuidadosamente para asegurarse de que cada uno puede sostenerse por cuenta propia y que imparte información que sería necesaria si un recién llegado fuese forzado a unirse al equipo de software en alguna parte en medio del proyecto.

El *manejo del riesgo* y la *planificación de contingencia* suponen que los esfuerzos de mitigación fracasaron y que el riesgo se convirtió en realidad. Continuando con el ejemplo, el proyecto ya está en marcha y algunas personas anuncian que renunciarán al mismo. Si se siguió la estrategia de mitigación, está disponible el respaldo, la información se documentó y el conocimiento se dispersó a través del equipo. Además, puede cambiar temporalmente el foco de los recursos (y reajustar el calendario del proyecto) hacia aquellas funciones que tengan personal completo, lo que permitirá “ponerse al día” a los recién llegados que deban agregarse al equipo. A los individuos que se retiran se les pide detener todo el trabajo y pasar sus últimas semanas en “modo de transferencia de conocimiento”. Esto puede incluir captura de conocimiento en video, desarrollo de “documentos comentados o wikis” y/o reuniones con otros miembros del equipo que permanecerán en el proyecto.



*Si la ER para un riesgo específico es menor que el costo de mitigación de riesgo, no intente mitigar el riesgo, sino continuar para monitorearlo.*

Es importante anotar que los pasos de mitigación, monitoreo y manejo del riesgo (MMMR) incurren en costos adicionales para el proyecto. Por ejemplo, emplear el tiempo en respaldar a cada técnico crucial cuesta dinero. Por tanto, parte del manejo de riesgos es evaluar cuándo los beneficios acumulativos por los pasos MMMR sobrepasan los costos asociados con su implementación. En esencia, se realiza un análisis clásico costo-beneficio. Si los pasos para evitar el riesgo debido a la alta rotación aumentarán tanto el costo del proyecto como la duración del mismo por un estimado de 15 por ciento, pero el factor de costo predominante es “respaldo”, la administración puede decidir no implementar este paso. Por otra parte, si los pasos para evitar el riesgo se proyectan para aumentar los costos en 5 por ciento y la duración sólo en 3 por ciento, la administración probablemente pondrá todo en su lugar.

Para un proyecto grande pueden identificarse 30 o 40 riesgos. Si para cada uno se identifican entre tres y siete pasos de manejo de riesgo, ¡el manejo del riesgo puede convertirse en un proyecto por sí mismo! Por esta razón, debe adaptar al riesgo de software la regla de Pareto de 80-20. La experiencia indica que 80 por ciento del riesgo de proyecto global (es decir, 80 por

ciento del potencial para falla del proyecto) puede explicarse por sólo 20 por ciento de los riesgos identificados. El trabajo realizado durante los primeros pasos del análisis de riesgos ayudará a determinar cuáles de ellos residen en ese 20 por ciento (por ejemplo, riesgos que conducen a la exposición más alta al riesgo). Por esta razón, algunos de los riesgos identificados, valorados y proyectados pueden no llegar al plan MMMR, no se ubican en el crucial 20 por ciento (los riesgos con prioridad de proyecto más alta).

El riesgo no está limitado al proyecto de software en sí. Pueden ocurrir después de que el software se desarrolló exitosamente y de que se entregó al cliente. Dichos riesgos por lo general se asocian con las consecuencias de falla del software en el campo.

La *seguridad del software* y el *análisis de riesgos* (por ejemplo, [Dun02], [Her00], [Lev95]) son las actividades de aseguramiento de la calidad del software (capítulo 16) que se enfocan en la identificación y valoración de los riesgos potenciales que pueden afectar al software negativamente y hacer que falle todo un sistema. Si los riesgos pueden identificarse tempranamente en el proceso de ingeniería del software, pueden especificarse características de diseño del software que eliminarán o controlarán los riesgos potenciales.

## 28.7 EL PLAN MMMR

En el plan de proyecto del software puede incluirse una estrategia de administración del riesgo, o los pasos de administración del riesgo pueden organizarse en un *plan de mitigación, monitoreo y manejo de riesgo* (MMMR) por separado. El plan MMMR documenta todo el trabajo realizado como parte del análisis de riesgos y el gerente del proyecto lo usa como parte del plan de proyecto global.

Algunos equipos de software no desarrollan un documento MMMR formal. En vez de ello, cada riesgo se documenta individualmente usando una *hoja de información de riesgo* (HIR) [Wil97]. En la mayoría de los casos, la HIR se mantiene con un sistema de base de datos de modo

### HERRAMIENTAS DE SOFTWARE



#### Manejo de riesgo

**Objetivo:** El objetivo de las herramientas de manejo de riesgo es auxiliar de un equipo de proyecto para definir riesgos, valorar su impacto y probabilidad, y monitorear los riesgos a lo largo de un proyecto de software.

**Mecánica:** En general, las herramientas de manejo de riesgo auxilian en la identificación de riesgos genéricos al proporcionar una lista de riesgos empresariales y de proyecto usuales, proporcionar listas de verificación u otras técnicas de "entrevista" que auxilien en la identificación de riesgos específicos del proyecto, asignar probabilidad e impacto a cada riesgo, apoyar las estrategias de mitigación de riesgo y generar muchos reportes diferentes relacionados con el riesgo.

#### Herramientas representativas:<sup>4</sup>

@risk, desarrollada por Palisade Corporation ([www.palisade.com](http://www.palisade.com)), es una herramienta de análisis de riesgo genérico que usa simulación Monte Carlo para impulsar su motor analítico.

Riskman, distribuida por ABS Consulting ([www.absconsulting.com/riskmansoftware/index.html](http://www.absconsulting.com/riskmansoftware/index.html)), es un sistema experto de evaluación de riesgos que identifica riesgos relacionados con proyectos.

Risk Radar, desarrollada por SPMN ([www.spmn.com](http://www.spmn.com)), ayuda a los gerentes de proyecto a identificar y manejar riesgos de proyecto.

Risk+, desarrollada por Deltek ([www.deltek.com](http://www.deltek.com)), se integra con Microsoft Project para cuantificar incertidumbres de costo y calendario.

X:PRIMER, desarrollada por Grafp Technologies ([www.grafp.com](http://www.grafp.com)), es una herramienta genérica web que predice qué puede salir mal en un proyecto e identifica las causas raíz para potenciales fallos y contramedidas efectivas.

<sup>4</sup> Las herramientas que se mencionan aquí no representan un respaldo, sino una muestra de las herramientas que hay en esta categoría. En la mayoría de los casos, los nombres de las herramientas son marcas registradas por sus respectivos desarrolladores.

**FIGURA 28.4**

**Hoja de información de riesgo.**  
Fuente: [Wil97].

Hoja de información de riesgo			
Riesgo ID: P02-4-32	Fecha: 5/9/09	Prob: 80%	Impacto: alto
<b>Descripción:</b> De hecho, sólo 70 por ciento de los componentes de software calendarizados para reuso se integrarán en la aplicación. La funcionalidad restante tendrá que desarrollarse a la medida.			
<b>Refinamiento/contexto:</b> Subcondición 1: Ciertos componentes reutilizables se desarrollaron por una tercera persona sin conocimiento de los estándares de diseño internos. Subcondición 2: El estándar de diseño para interfaces de componente no se consolidó y puede ser que no se apegue a ciertos componentes reutilizables existentes. Subcondición 3: Ciertos componentes reutilizables se implementaron en un lenguaje que no es soportado en el entorno meta.			
<b>Mitigación/monitoreo:</b> 1. Contactar tercera persona para determinar conformidad con los estándares de diseño. 2. Presionar por terminación de estándares de interfaz; considerar estructura de componente cuando se decida acerca de protocolo de interfaz. 3. Comprobar para determinar el número de componentes en la categoría de subcondición 3; comprobar para determinar si se puede adquirir soporte de lenguaje.			
<b>Manejo/plan de contingencia/disparador:</b> <i>ER</i> calculada en US\$20 200. Asignar esta cantidad dentro de los costos de contingencia del proyecto. Desarrollar revisión de calendario y suponer que 18 componentes adicionales tendrán que construirse a la medida; asignar personal en concordancia. Disparador: Pasos de mitigación improductivos al 7/1/09.			
<b>Estado actual:</b> 5/12/09: Pasos de mitigación iniciados.			
Originador: D. Gagne	Asignado: B. Laster		

que la entrada de creación e información, el orden de prioridad, las búsquedas y otros análisis pueden realizarse con facilidad. El formato de la HIR se ilustra en la figura 28.4.

Una vez documentada la MMMR y comenzado el proyecto, inician los pasos de mitigación y monitoreo del riesgo. Como ya se estudió, la mitigación del riesgo es una actividad que busca evitar el problema. El monitoreo del riesgo es una actividad de seguimiento del proyecto con tres objetivos principales: 1) valorar si los riesgos predichos en efecto ocurren, 2) asegurar que los pasos para evitar el riesgo definidos para un riesgo determinado se aplican de manera correcta y 3) recopilar información que pueda usarse para futuros análisis de riesgos. En muchos casos, el problema que ocurre durante un proyecto puede monitorearse en más de un riesgo. Otra actividad del monitoreo de riesgos es intentar asignar orígenes (cuál riesgo causó cuál problema a lo largo del proyecto).

## 28.8 RESUMEN

Siempre que un colectivo cabalga en un proyecto de software, el sentido común dicta análisis de riesgos. E incluso así, la mayoría de los gerentes de proyectos de software lo hacen de manera informal y superficial, si acaso lo hacen. El tiempo que se emplea en identificar, analizar y manejar el riesgo rinde sus frutos en muchas formas: menos agitación durante el proyecto, una mayor capacidad para monitorear y controlar un proyecto, y la confianza que conlleva la planificación de los problemas antes de que se presenten.