

6.1 Introducción

Como consecuencia del elevado número de proyectos informáticos cancelados o entregados fuera de plazo, presupuestos excedidos, conflictos con los usuarios y clientes, serias dificultades operativas, etc., surge el análisis o gestión de riesgos del software como un factor esencial para el buen desarrollo de un proyecto informático. Así, se podría definir *riesgo* como cualquier elemento potencial que puede provocar resultados insatisfactorios en el desarrollo de un proyecto. En consecuencia, parece lógico pensar que el director de un proyecto necesitará, en todo momento, comprender y controlar el riesgo en aquellas áreas que puedan tener influencia sobre el proyecto, así como conocer los riesgos externos que puedan afectar al mismo.

En este capítulo, se intentará introducir al lector en la difícil tarea de identificar y gestionar eficientemente los riesgos inherentes a un proyecto informático y que fundamentalmente se centran en el software. En primer lugar, se reflexionará sobre la importancia de conocer y controlar estos riesgos con el objetivo de evitar el posible fracaso de un proyecto. A continuación, se presenta una clasificación de los riesgos, lo que puede facilitar su identificación durante la ejecución de un proyecto informático. Finalmente, se expondrán las fases generales que componen la gestión efectiva de los riesgos.

6.2 Riesgo asociado a un proyecto

En primer lugar, hay que centrar el problema del riesgo asociado a un proyecto estableciendo como base de partida una definición genérica que haga referencia al concepto de riesgo. Así, para el *US Air Force Systems Command*, riesgo es la forma de expresar la incertidumbre a lo largo del ciclo de vida, la probabilidad de que en un punto del ciclo de vida no se alcancen los objetivos propuestos con los recursos disponibles. Obviamente, además de esta incertidumbre, también interesarán las circunstancias en las que se producen los riesgos, los factores o causas que

los desencadenan, y los efectos producidos en situaciones en las que no se tuvo en cuenta la existencia de los mismos.

De una manera sumamente simplificada, el riesgo se puede definir como la contingencia o proximidad de un daño. Es obvio que en todo lo referente al tratamiento de riesgos, al objeto de hacer mínimos los posibles daños, resulta necesario el análisis y conocimiento de los factores de riesgo para reducir sus efectos mediante la realización de las acciones pertinentes. Por tanto, el análisis de riesgos equivale al estudio de las incertidumbres. Por su parte, la respuesta de los riesgos es equivalente a la toma de decisiones que hagan mínimos sus efectos.

Con respecto a la incertidumbre, debe considerarse que en sí su existencia no significa que conduzca a resultados buenos o malos. Cuando tal incertidumbre da lugar a realidades favorables, constituye una *oportunidad*; cuando, por el contrario, conduce a daños, la incertidumbre se traduce en riesgos. Por ello, el riesgo puede también definirse como la probabilidad de que suceda un hecho desfavorable.

En el contexto de la Ingeniería del Software, se puede decir que el riesgo de un proyecto hace referencia a tres conceptos fundamentales (Charette, 1989):

1. Afecta al futuro, es decir, ¿cuáles son los riesgos que podrían hacer que el proyecto informático fracasara?
2. Se centra en los cambios, es decir, ¿cómo afectarán al éxito global y a los plazos los cambios en los requisitos del cliente, en las tecnologías de desarrollo, en las máquinas destino y en todas las demás entidades relacionadas con el proyecto?
3. Precisa de una selección entre distintas alternativas, es decir, ¿qué métodos y herramientas deberemos usar, cuánta gente deberá estar involucrada en el proyecto, qué importancia hay que darle a la calidad?

Considerando las tres bases conceptuales de Charette, se tendrá la posibilidad de adoptar diferentes estrategias para controlar el riesgo. En primer lugar, lo que se conoce como *estrategia reactiva* consiste en que el equipo de un proyecto informático no lleva a cabo ninguna acción con respecto a los posibles riesgos hasta que surge algún problema real, momento éste en el que todo el equipo se dedica a intentar corregirlo. En el mejor de los casos, los miembros del equipo tan sólo supervisan el proyecto en previsión de posibles riesgos. Básicamente, las raíces de la estrategia reactiva se encuentran en una idea muy simple: ¿por qué trabajar en algo que actualmente todavía no constituye un problema?

Una actitud mucho más inteligente consiste en adoptar una *estrategia proactiva* frente a los riesgos de un proyecto informático. Mediante la estrategia proactiva,

se identificarán los riesgos potenciales, se valorarán su probabilidad y su impacto y se establecerá una prioridad según su relevancia. Posteriormente, el equipo deberá diseñar un *plan de gestión del riesgo* que permita controlarlo. Obviamente, el primer objetivo será evitar el riesgo pero, como no siempre será posible eliminar todos los riesgos, el equipo deberá desarrollar un plan de contingencia que le permita responder de una manera eficaz y controlada ante cualquier problema.

A partir del planteamiento de una estrategia proactiva, la gestión o el análisis del riesgo constará de una serie de actividades genéricas a desarrollar por parte de todo el equipo asignado a un proyecto informático: *identificación, proyección y reducción, supervisión y gestión del riesgo*. En síntesis, por tanto, la gestión de riesgos consistirá en identificar y analizar problemas, y definir y evaluar posibles soluciones. En las siguientes secciones de este capítulo, se abordará en detalle cada una de las tareas o fases en la gestión de riesgos.

6.3 Clasificación de los riesgos del software

Antes de pasar a analizar los «verdaderos riesgos» de un proyecto informático, y que como se comentaba anteriormente se centran en el software, es importante identificar todos los riesgos que puedan resultar obvios, tanto para los gestores como para el personal técnico. Esta tarea de identificación deberá cuantificar las dos características básicas asociadas a los riesgos: el nivel de incertidumbre y el grado de pérdidas o consecuencias no deseadas. Con el objetivo de facilitar este trabajo, resultará muy útil encuadrar los riesgos en diferentes grupos, en función de su naturaleza o, incluso, por razón de su alcance.

6.3.1 Clasificación macroscópica

Aunque cabría clasificar los riesgos de muy diversas maneras, a nivel macroscópico se pueden considerar tres categorías: *riesgos del proyecto*, *riesgos técnicos* y *riesgos del negocio*. Atendiendo a esta primera clasificación, los *riesgos del proyecto* estarían asociados con el plan del proyecto, es decir, si los riesgos del proyecto se hacen realidad, es muy probable que la *planificación* temporal del proyecto se retrase y que los costes aumenten. En otras palabras, estos riesgos identifican potenciales problemas presupuestarios, de agenda, de personal (principalmente, a nivel de organización y de asignación de personal), de recursos, del cliente y de requisitos, así como su impacto en un proyecto informático. Como ejemplo de factores de riesgo para este primer grupo, cabría destacar la complejidad, el tamaño y la estructura del proyecto.

En segundo lugar, los *riesgos técnicos* amenazan la calidad y la **planificación** temporal del software a desarrollar. Si un riesgo técnico se convierte en una realidad, la implementación puede llegar a ser excesivamente difícil o, incluso, puede resultar hasta imposible. Estos riesgos identifican potenciales problemas **de** diseño, implementación, interfaz, verificación y mantenimiento. Los principales factores que pueden influir sobre este grupo hacen referencia a la ambigüedad **de** la especificación, así como a la incertidumbre y la obsolescencia técnica. En general, estos riesgos aparecen cuando la resolución **de** un proyecto resulta más compleja **de** lo que inicialmente se había previsto.

Por último, los *riesgos del negocio* amenazarían la viabilidad del software a elaborar. A menudo llegan a poner en peligro el proyecto o el producto, puesto que pueden llevar al fracaso los resultados **de** los mejores **proyectos informáticos**. Los principales causantes **de** estos riesgos son:

- El desarrollo **de** un producto excelente que en realidad nadie quiere (riesgo **de** mercado).
- El desarrollo **de** un producto que no encaja dentro **de** la estrategia comercial **de** una empresa (riesgo estratégico).
- Los problemas relacionados con la venta del producto o con el precio **de** éste (riesgo comercial).
- La pérdida del apoyo **de** los gestores debido a un cambio **de** enfoque o a un cambio **de** personal (riesgo **de** gestión).
- Las pérdidas presupuestarias o **de** personal asignado a un proyecto (riesgo **de** presupuesto).
- Los sobrecostos en mantenimiento correctivo y preventivo (riesgo **de** mantenimiento).
- Los fallos ocurridos durante la explotación, los cuales pueden causar daños significativos y, eventualmente, pueden ser peligrosos para la vida **de** las personas (riesgos **de** explotación).

6.3.2 Otra clasificación

Otra posible clasificación genérica **de** los riesgos **de** un proyecto informático es la propuesta por Charette. En este caso, se distingue entre *riesgos conocidos*, *riesgos predecibles* y *riesgos impredecibles* (Charette, 1989). Así, los *riesgos conocidos* son todos aquellos que se pueden descubrir después **de** una minuciosa evaluación del plan del proyecto, del entorno técnico y comercial en el que se desarrolla el

- *Tamaño del producto*: riesgos asociados con el tamaño general del software a construir o a modificar.
- *Impacto en el negocio*: riesgos asociados con las limitaciones impuestas por la gestión o por el mercado.
- *Características del cliente*: riesgos asociados con la sofisticación del cliente y la habilidad del equipo de desarrollo para comunicarse con el cliente en los momentos oportunos.
- *Definición del proceso*: riesgos asociados con el grado de definición del proceso de desarrollo de software y su seguimiento por la empresa de desarrollo.
- *Entorno de desarrollo*: riesgos asociados con la disponibilidad y calidad de las herramientas que se van a emplear en el desarrollo del producto.
- *Tecnología a construir*: riesgos asociados con la complejidad del sistema a construir y la tecnología que contiene el sistema.
- *Tamaño y experiencia de la plantilla*: riesgos asociados con la experiencia técnica y de proyectos de los ingenieros del software que van a realizar el trabajo.

Esta lista de comprobación de elementos de riesgo podrá recoger información muy variada y organizarse de diversas maneras. No obstante, la técnica más sencilla consiste en responder a una serie de cuestiones relevantes para cada una de las categorías que se acaban de indicar, lo que permitirá al responsable o jefe del proyecto estimar la probabilidad y el impacto del riesgo (segunda etapa en la gestión de riesgos). En cada caso, la información del producto a desarrollar deberá compararse con la experiencia anterior, es decir, comprobar si existen importantes desviaciones o si, por el contrario, las estimaciones son suficientemente similares.

A modo de ejemplo, se podría mencionar algunas de las preguntas que permitirían facilitar la identificación de los riesgos asociados con el tamaño del producto:

- ¿Cuál es el tamaño estimado del producto en LDC (o cualquier otra medida)?
- ¿Cuál es el grado de seguridad en la estimación del tamaño del producto?
- ¿Cuál es el tamaño del producto en número de programas y archivos?
- ¿Cuál es el porcentaje de desviación en el tamaño del producto respecto a la medida de productos anteriores?
- ¿Cuál es el número de usuarios del producto?

- ¿Cuál es el número de cambios previstos sobre los requisitos del producto?
- ¿Qué cantidad de software podrá ser reutilizado?
- ¿Cuál es el tamaño de la base de datos creada o empleada por el producto?

En el caso de los riesgos relacionados con el tamaño y la experiencia del equipo asignado a un proyecto informático, Bohem (Bohem, 1989) sugiere las siguientes cuestiones para valorarlos:

- ¿Disponemos de la mejor gente?
- ¿Tiene el personal los conocimientos adecuados?
- ¿Tenemos suficiente personal?
- ¿Se ha asignado al personal para toda la duración del proyecto?
- ¿Ha recibido el personal la formación necesaria?
- ¿Será mínimo la movilidad del personal para permitir la continuidad?
- ¿Dispone el personal de las expectativas correctas sobre el trabajo a realizar?

6.5 Proyección del riesgo

La segunda de las tareas propias de la gestión de riesgos de un proyecto se refiere a la *proyección del riesgo*. La proyección del riesgo, también denominada *estimación del riesgo*, intenta medir cada uno de los riesgos identificados en la lista de comprobación de elementos de riesgo desde dos perspectivas complementarias: la *probabilidad* de que el riesgo sea real y las *consecuencias* o el *impacto* de los problemas asociados con el riesgo, suponiendo que éste ocurre. Por tanto, se trata de dar respuesta a una serie de cuestiones fundamentales, tales como:

- ¿Constituye esto realmente un riesgo o no?
- ¿Cuál es la importancia real del riesgo?
- ¿Cuáles podrían ser sus consecuencias?
- ¿Cuál es la probabilidad de que ocurra el riesgo?

Atendiendo a estos objetivos, el jefe del proyecto informático, junto con otro personal técnico, deberá llevar a cabo cuatro actividades básicas durante esta fase de gestión de riesgos: