Tema 08 –
Gestión de riesgos

Ingeniería del Software

Héctor Gómez Gauchía
Dep. Ingeniería del Software e Inteligencia Artificial
Facultad de Informática
Universidad Complutense Madrid

Trabajando con Rubén Fuentes, Antonio Navarro, Juan Pavón y Pablo Gervás

Contenidos

- Introducción
  - Problemática
- Aspectos de la solución
  - Riesgos y tipología
  - Gestión de riesgos
  - Plan de gestión de riesgos
    - IEEE Std. 1540-2001

Introducción

- Riesgo es todo aquello que pueda afectar negativamente al proyecto de software.
  - *Todo* puede afectar negativamente a nuestro proyecto.
  - Luego debemos preocuparnos por todo.
  - Fin del tema... ¿o no?
- Aunque todo es preocupante, hay unos riesgos más preocupantes que otros.
  - Ej. fallo en la especificación de requisitos vs abducción de la plantilla
- La *gestión de riesgos* se ocupa de la valoración de riesgos y la planificación y ejecución de medidas para eliminarlos, mitigarlos o reaccionar a su aparición.

Tipos de riesgo

- Los riesgos se clasifican atendiendo a distintas dimensiones:
  - Ámbito
    - Dónde pueden surgir y a qué afectan:
      - *Del proyecto*
      - *Técnicos*
      - *Del negocio*
  - Predictibilidad
    - Hasta qué punto se pueden anticipar:
      - *Conocidos* por el personal
      - *Desconocidos* pero potencialmente identificables
      - *Impredecibles*
- Conocer la tipología ayuda a identificar posibles fuentes de problemas.

Tipos de riesgos: del proyecto

- Los *riesgos del proyecto* amenazan al plan del proyecto.
  - Si se hacen reales, aumenta el esfuerzo y/o el coste.
- Identifican problemas potenciales en:
  - Presupuesto
  - Planificación
  - Personal
  - Recursos
  - Participantes
  - Requisitos

Tipos de riesgos: técnicos

- Los *riesgos técnicos* amenazan la calidad del software.
  - Aparecen porque el sistema puede ser más difícil de construir de lo esperado.
- Identifican problemas potenciales en:
  - Requisitos
  - Diseño
  - Implementación
  - Interfaz
  - Verificación
  - Mantenimiento
  - Incertidumbre técnica
  - Tecnologías desconocidas

Tipos de riesgos: del negocio

- Los *riesgos del negocio* amenazan la viabilidad del proyecto.
- Identifican problemas potenciales con:
  - Construir un sistema no necesitado → riesgo de mercado
  - Construir un producto que no encaja en la estrategia de la compañía → riesgo de estrategia
  - Construir un producto difícil de vender → riesgo de ventas
  - Perder el apoyo de los gestores superiores → riesgo administrativo
  - Perder presupuesto o personal asignado → riesgo presupuestario

Estrategias de gestión de riesgos

- Estrategia reactiva → reacción
  - Supervisa el proyecto en previsión de posibles riesgos.
  - Se asignan recursos por si los riesgos se convierten en problemas.
  - El equipo no se preocupa de los riesgos hasta que algo va mal.
  - El equipo intenta sofocar el problema.
  - Cuando se falla, entra en acción la gestión de crisis.
    - El proyecto se encuentra en riesgo real.
- Estrategia proactiva → prevención
  - Comienza antes que los trabajos técnicos.
  - Se identifican riesgos potenciales.
  - Se evalúa la probabilidad y consecuencias de los riesgos.
  - Se priorizan los riesgos.
  - Se produce un *plan de gestión del riesgo*.
  - El objetivo es evitar el riesgo, aunque también se proporcionan *planes de contingencia*.

Gestión de riesgos proactiva

- Varias propuestas:
  - En su artículo de 1991 [Boehm, 1991], Boehm fija las bases para la gestión del riesgo en el software.
  - Otra aproximación es la propuesta por el Instituto de Ingeniería del Software (en inglés, SEI) [*Quality Managers Software Quality Assurance Subcommittee*, DoE, 2000].
    - Se trata de una ampliación de las ideas de Boehm.
- Ambas aproximaciones son muy similares.
  - La aproximación de Boehm es más clara.
  - La aproximación SEI es más actual y está mejor documentada.

Gestión de riesgos: pasos

- Valoración del riesgo
  - Identificación del riesgo
  - Análisis del riesgo
  - Priorización del riesgo
- Control del riesgo
  - Planificación de la gestión del riesgo
  - Resolución del riesgo
  - Monitorización del riesgo

Identificación del riesgo

- La *identificación del riesgo* produce listas de elementos de riesgo específicos para el proyecto que comprometan seriamente su éxito.
- Existen varias técnicas de identificación del riesgo:
  - Listas de comprobación de elementos de riesgo
    - La tabla de los *Top 10 Software Risk Items* de Boehm
    - Taxonomía SEI de Riesgos del Software [Carr et al., 1993]
  - Análisis de supuestos (comparación)

10 elementos claves de riesgo para el software

Elemento de riesgo	Técnica de reducción del riesgo
Deficiencias del personal	Contratar gente con talento, asignación de trabajos, construcción de equipos, acuerdos entre personal clave, formación cruzada
Planificaciones y presupuestos poco realistas	Estimación multifuente detallada de costes y planificación, diseñar en función del coste, desarrollo incremental, reutilización del software, *fregado de requisitos*
Desarrollo de las funciones y propiedades erróneas	Análisis de organización, análisis de la misión, revisiones del usuario y participación del usuario, prototipado, manuales de usuario preliminares, formulación de operaciones-concepto, análisis de rendimiento sin nombre, análisis de calidad-factor
Desarrollo erróneo del interfaz de usuario	Prototipado, escenarios, análisis de tareas, participación del usuario
Chapado	*Fregado de requisitos*, prototipado, análisis de costes-beneficios, diseñar en función del coste
Continua corriente de cambios en los requisitos	umbral de cambio alto, ocultación de información, desarrollo incremental
Deficiencias en componentes proporcionados externamente	*Benchmarking*, inspecciones, comprobaciones por referencia, análisis de la compatibilidad
Deficiencias en tareas desarrolladas externamente	Comprobaciones por referencia, auditorias antes de los incentivos, contratos con incentivos, diseño o prototipado competitivo, construcción de equipo
Deficiencias en rendimiento en tiempo real	Simulación, *benchmarking*, modelado, prototipado, instrumentación, ajuste
Exprimir las capacidades informáticas	Análisis técnicos, análisis coste-beneficio, prototipado, compropaciones por referencias.

Análisis de riesgos

- El *análisis de riesgos* determina la probabilidad y consecuencias asignadas a cada riesgo.
  - La *probabilidad* indica las posibilidades de que el riesgo se haga real.
  - Las *consecuencias* indican la gravedad de los efectos si el riesgo se hace real.

Asignación de probabilidades

- Puede estimarse directamente.
- También aplicando técnicas como las descritas en:
  - [AFSC/AFCL, 1993], incluido en [Pressman, 1993]
  - La tabla del SQAS-SEI (*Software Quality Assurance Subcommittee*, SEI)

Probability	Description	Severity	Consequence
Frequent	Not surprised, will occur several times (Frequency per year > 1)	Catastrophic	Greater than 6 month slip in schedule; greater than 10% cost overrun; greater than 10% reduction in product functionality
Probable	Occurs repeatedly/ an event to be expected (Frequency per year $1\text{-}10^{-1)}$	Critical	Less than 6 month slip in schedule; less than 10% cost overrun; less than 10% reduction in product functionality
Occasional	Could occur some time (Frequency per year 10^{-1} - $10^{-2)}$	Serious	Less than 3 month slip in schedule; less than 5% cost overrun; less than 5% reduction in product functionality
Remote	Unlikely though conceivable (Frequence per year 10^{-2} - 10^{-4})	Minor	Less than 1 month slip in schedule; less than 2% cost overrun; less than 2% reduction in product functionality
Improbable	So unlikely that probability is close to zero (Frequency per year 10^{-4} - 10^{-5})	Negligible	Negligible impact on program

Análisis de riesgos: formularios

- En el proceso de análisis del riesgo podemos utilizar *formularios de gestión riesgos*.

E.1 Example 1: Risk Accounting Form

Risk Accounting Form[1]		
Identified by:	**Date:**	
	ID #: *CM Tracking #*	
Statement of Risk (with context):		
	Consequence: (**C**ost , **S**chedule, **P**erformance, **Q**uality)	Risk Magnitude Rm
	Severity: (**C**ritical, **S**erious, **M**oderate, **M**inor)	
	Probability of occurrence? (**H**igh, **M**edium , **L**ow, %)	
	Timeframe of risk? (**N**ear-term, **F**ar-term)	
Mitigation Strategy: Different strategies to mitigate this risk. When it must be mitigated.		
Contingency Action and Trigger:		
Risk Grouping: *Other risks (by ID) that will impact this risk or are impacted by this risk*		

E.2 Example 2: Risk Information Sheet

ID:	**Risk Information Sheet**[2]		Identified:
Priority:	Statement of Risk:		
Probability:			
Impact:			
Timeframe:	Origin:	Class:	Assigned To:
Context:			
Mitigation Strategy:			
Contingency Action and Trigger:			
Status:			Status Date:
Approval:	Closing Date:	Closing Rationale:	

Priorización de riesgos

- La *priorización* de riesgos produce una lista ordenada de elementos de riesgo identificados y analizados.
- Posibles técnicas de priorización:
  - Crear una *tabla de riesgo* que ordena los riesgos por probabilidad y consecuencia.
    - Así, sólo los riesgos por encima de la *línea de corte* son considerados.
  - Calcular la *exposición al riesgo*, multiplicando probabilidad por consecuencias.
    - Así, sólo se tratan los riesgos de mayor exposición.
  - Utilizar mecanismos como los descritos en SQAS-SEI para calcular el *nivel de riesgo*.

Niveles de riesgo SQAS-SEI (1/2)

Probability / Severity	Frequent	Probable	Occasional	Remote	Improbable
Catastrophic	IN	IN	IN	H	M
Critical	IN	IN	H	M	L
Serious	H	H	M	L	T
Minor	M	M	L	T	T
Negligible	M	L	T	T	T
LEGEND	T = Tolerable	L = Low	M = Medium	H = High	IN = Intolerable

Niveles de riesgo SQAS-SEI (2/2)

- T: Tolerable
  - Si sucede, no importa.
- L: Bajo
  - Si sucede, los efectos son asumibles.
- M: Medio
  - Si sucede, afecta a los objetivos, costes o planificación.
  - Debería controlarse.
- H: Alto
  - Si sucede tiene una grave trascendencia.
  - Debería controlarse, supervisarse y tener planes de contingencia.
- IN: Intolerable
  - No puede obviarse su gestión bajo ningún concepto.

Gravedad de los riesgos

- Hablaremos de *gravedad* de los riesgos para caracterizar a los riesgos priorizados.
- Así los riesgos más graves serán aquellos:
  - Más altos en la tabla de riesgo
  - De mayor nivel de exposición
  - De nivel de riesgo más alto

Planificación de gestión

- La función *planificar* convierte la información sobre riesgos en decisiones y acciones para el presente y el futuro.
- La planificación incluye:
  - Desarrollar acciones para controlar riesgos individuales.
  - Priorizar las acciones contra los riesgos.
  - Crear un *Plan de Gestión del Riesgo*.

Alternativas de reacción a los riesgos

- Se analiza la lista ordenada de riesgos y se decide cómo se pueden tratar los riesgos:
  - Evitar el riesgo
    - Elegir una alternativa de menor riesgo.
  - Controlar el riesgo
    - Se decide reducir/mitigar el riesgo.
  - Asumir el riesgo
    - Se acepta que el riesgo ocurra.
  - Transferir el riesgo
    - Reducir el riesgo compartiéndolo.

Acciones a incluir en el plan

- Se deben evaluar todas las posibilidades teniendo en cuenta el aumento de costes y tiempo.
- Para aquellos riesgos que se decidan controlar, habrá que especificar qué mecanismos de reducción del riesgo se proponen.
- También deben proponerse planes de contingencia por si los riesgos se hacen reales.

Resolución del riesgo

- Durante la *resolución del riesgo* se llevan a cabo los pasos identificados para reducir y controlar los riesgos.

Monitorización de riesgos

- Durante la monitorización de riesgos:
  - Se comprueba si se están llevando a cabo los pasos de reducción del riesgo.
  - Se comprueba si los riesgos se están haciendo reales.
    - Ej. usando métricas
  - Se llevan a cabo las acciones correctivas necesarias.

PLAN DE RIESGOS

Plan de riesgos

- La información esencial sobre el proceso de gestión del riesgo puede incluirse en un Plan de Reducción, Supervisión y Gestión del Riesgo (RSGR).
  - Durante la reducción se proponen pasos:
    - Evitar que el riesgo se convierta en realidad.
    - Tener soluciones (*back-up*) en el supuesto de que el riesgo se convierta en realidad.
  - Durante la supervisión se:
    - Controla si el riesgo se ha hecho real.
    - Supervisa la efectividad / implementación de los pasos de reducción.
  - En gestión del riesgo, el riesgo se ha hecho real y se aplican las soluciones (planes de contingencia) considerados en reducción del riesgo.
- El RSGR puede ser un documento independiente o parte del plan de proyecto.

Plan de riesgos: plantilla

- Una plantilla puede ser:
  - Introducción
  - Priorización de riesgos del proyecto
  - Reducción, supervisión y gestión del riesgo
    - 3.k. Riesgo k-ésimo
      - 3.k.1. Reducción
      - 3.k.2. Supervisión
      - 3.k.3. Gestión
  - Planificación temporal
  - Resumen

IEEE Std. 1540-2001

- El estándar IEEE 1540-2001 (*IEEE Standard for Software Life Cycle Processes-Risk Management*) define un proceso de gestión del riesgo continuo.
- El proceso está formado por 6 actividades:
  - Planear e implementar la gestión del riesgo
    - Seleccionar el proceso de gestión del riesgo.
  - Gestionar el perfil de riesgo del proyecto
    - Identificar riesgos.
  - Realizar análisis del riesgo
    - Asignar probabilidades, consecuencias y priorizar.
  - Realizar tratamiento del riesgo
    - Seleccionar riesgos inaceptables y acciones de reducción para ellos.
  - Realizar monitorización del riesgo
    - Seguimiento de riesgos.
  - Evaluar el proceso de gestión del riesgo
    - Evaluación del proceso.

IEEE Std. 1540-2001: índices

- El estándar incluye índices para:
  - Plan de gestión del riesgo
    - Define cómo se van a implementar las actividades de gestión del riesgo durante un proyecto.
  - Petición de acción de riesgo
    - Sirve para capturar información sobre riesgos y comunicarla a los interesados.
  - Plan de tratamiento de riesgo
    - Define cómo van a ser tratados los riesgos inaceptables.

Principio de Pareto en gestión del riesgo

- Para un proyecto grande (70000 LDC) se pueden identificar unos 30 ó 40 riesgos.
- Si se dan entre 3 y 7 pasos de gestión del riesgo para cada uno, la gestión del riesgo se vuelve inviable.
- Por tanto aplicaremos la Regla de Pareto 80-20:
  - "el 80% del riesgo real se debe al 20% de los riesgos identificados".

Riesgos y peligros para la salud

- Si durante el desarrollo u operación del software se pudieran derivar riesgos y/o peligros para la salud, la gestión del riesgo es la actividad prioritaria en el proyecto.
  - Ej. control de aviones y software de centrales nucleares

CONCLUSIONES

Conclusiones

- Los riesgos son amenazas a la realización del proyecto.
  - Factibles, probables y con un impacto no desdeñable
  - Esta calificación es variables según el tipo de aplicación y dominio.
    - Aplicaciones críticas para la salud
- Hay que gestionar los riesgos con el fin de evitar que se conviertan en problemas sin solución.
  - Estrategia reactiva vs proactiva
  - Teniendo en cuenta en principio de Pareto
- La estrategia de gestión de riesgos se plasma en el plan RSGR.

Glosario

- AFSC/AFLC = *Air Force Systems Command / Air Force Logistic Command, USA*
- CMU = *Carnegie Mellon University*
- DoE = *Department of Energy, USA*
- LDC = Líneas de Código
- RSGR = Plan de Reducción, Supervisión y Gestión del Riesgo.
- SEI = *Software Engineering Institute*
- SQAS-SEI = *Software Quality Assurance Subcommitte*, SEI
- SRS = *Software Requirements Specification*
- US = USA = *United States of America*
- USAF = *US Air Force*

Referencias (1/2)

- R. Pressman: Ingeniería del Software. Un enfoque práctico, 7ª edición. McGraw-Hill, 2010.
  - Capítulo 28
- I. Sommerville: Ingeniería del Software, 7ª edición. Addison Wesley, 2007.
  - Capítulo 5.4
- AFSC/AFLC: Software Risk Abatement. AFSC/AFLC pamphlet 800-45, 1998.
- B.W. Boehm: Software Risk Management: Principles and Practices. IEEE Software 8(1), pp. 32-41, 1991.
- M.J. Carr, S.L. Konda, I. Monarch, F.C. Ulrich: Taxonomy-Based Risk Identification. Technical Report CMU/SEI-93-TR-6, 1993.
- Clay F. Walker IEEE: IEEE Std. 1540-2001. IEEE Standard for Software Life Cycle Processes-Risk Management. IEEE, 2001.

Referencias (2/2)

- R.S. Pressman: A manager's guide to software engineering. McGraw-Hill, 1993.
- Quality Managers Software Quality Assurance Subcommittee, DoE, USA: Software Risk Management – A Practical Guide. SQAS21.01.00-1999. Department of Energy of the United States of America, 2000.