7. Análisis y gestión del riesgo

Índice

- Referencias
- Introducción
- Estrategias de gestión del riesgo
- Tipos de riesgos
- Gestión del riesgo Boehm
  - Pasos.
  - Identificación del riesgo.
  - Análisis del riesgo.
  - Priorización del riesgo.

Índice

  - Planificación de la gestión del riesgo.
  - Resolución del riesgo.
  - Monitorización del riesgo.
- El plan de Reducción Supervisión y Gestión del Riesgo (RSGR)
- IEEE Std. 1540-2001

Índice

- La Regla de Pareto
- Riesgos y peligros para la salud
- Conclusiones

Referencias

- Pressman, R.S. *Ingeniería del Software. Un Enfoque Práctico. Sexta Edición*. McGraw-Hill, 2005
- Sommerville, I. *Ingeniería del Software*. 7ª edición. Addison-Wesley, 2005
- Boehm, B.W. Software Risk Management: Principles and Practices. *IEEE Software*. January, 1991

Referencias

- Software Quality Assurance Subcommittee of the Nuclear Weapons Complex Quality Managers under the United States Department of Energy. SQAS21.01.00-1999
- IEEE Std. 1540-2001, IEEE Standard for Software Life Cycle Processes-Risk Mangement

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?

Introducción

- Aunque *todo* es preocupante, hay unos riesgos más preocupantes que otros

  e.g. fallo en la SRS vs. abducción de la plantilla
- En este tema nos encargaremos de valorar los riesgos más preocupantes y de su gestión

Introducción

- Atributos del riesgo:
  - Afecta a acontecimientos futuros.
  - Implica cambio.
  - Implica elección e incertidumbre.
- ¿Por qué gestionar riesgos?
- Para evitar *desastres* en la gestión de proyectos software

Estrategias de gestión del riesgo

- Dos tipos de estrategias

  - Estrategia reactiva.

  - Estrategia proactiva.

- Estrategia reactiva:

  - Supervisa el proyecto en previsión de posibles riesgos.

  - Se asignan recursos por si los riesgos se convierten en problemas.

Estrategias de gestión del riesgo

- El equipo no se preocupa de los riesgos hasta que algo va mal.
- El equipo intenta *sofocar* el problema (bomberos).
- Cuando se falla, entra en acción la *gestión de crisis*.
- El proyecto se encuentra en riesgo real.

- La estrategia proactiva:
  - Comienza antes que los trabajos técnicos.
  - Se identifican riesgos potenciales.

Estrategias de gestión del riesgo

- Se evalúa probabilidad y consecuencia de los riesgos.
- Se priorizan los riesgos.
- Se produce un plan de gestión del riesgo.
- El objetivo es evitar el riesgo...

... pero también se proporcionan *planes de contingencia*.

- Aplicaremos una estrategia proactiva

Tipos de riesgos

- Los riesgos pueden ser:
  - Del proyecto.
  - Técnicos.
  - Del negocio.
- Los *riesgos del proyecto* amenazan al plan del proyecto.
  - Si se hacen reales, aumenta el esfuerzo y/o el coste.

Tipos de riesgos

- Identifican problemas potenciales en:
  - Presupuesto
  - Planificación
  - Personal
  - Recursos
  - Participantes
  - Requisitos

Tipos de riesgos

- 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

Tipos de riesgos

  - Verificación
  - Mantenimiento
  - Incertidumbre técnica
  - Tecnologías desconocidas
- Los *riesgos del negocio* amenazan la viabilidad del proyecto
  - Identifican problemas potenciales con:
    - Construir un sistema no necesitado (riesgo de mercado).

Tipos de riesgos

- 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)

Tipos de riesgos

- Otra clasificación identifica riesgos:
  - Conocidos
  - Desconocidos
  - Impredecibles
- Los riesgos *conocidos* son aquellos de los que el personal es consciente

Tipos de riesgos

- Los riesgos *desconocidos* son aquellos de los que el personal sería consciente si se siguiera un proceso de identificación.
- Los riesgos *impredecibles* son aquellos que en principio, no eran esperables.

Gestión del riesgo Boehm Introducción

- En su artículo de 1991*, Boehm fija las bases para la gestión del riesgo en el software
- Otra aproximación es la propuesta por el SEI**, ampliación de las ideas de Boehm

*Boehm, B.W. Software Risk Management: Principles and Practices. *IEEE Software*. January, 1991.

**SQAS21.01.00-1999

Gestión del riesgo Boehm Introducción

- A mi juicio, ambas aproximaciones:

  - Son casi equivalentes.

  - La aproximación de Boehm es más clara.

  - La aproximación SEI es más actual, y está mejor documentada. En particular la aproximación SQAS: *Software Quality Assurance Subcommittee of the Nuclear Weapons Complex Quality Managers under the United States Department of Energy* (http://cio.doe.gov/sqas)

Gestión del riesgo Boehm
Pasos

- Gestión del riesgo
  - 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.

Gestión del riesgo Boehm
Identificación del riesgo

- La *identificación del riesgo* produce listas de elementos del riesgo específicos para el proyecto que comprometan seriamente el éxito del proyecto
- Una técnica de identificación del riesgo es el uso de *listas de comprobación* de elementos del riesgo
- Otra es el *análisis de supuestos* (comparación)

Gestión del riesgo Boehm Identificación del riesgo

- La tabla de los *Top 10 Software Risk Items* de Boehm puede ser una lista de comprobación de elementos del riesgo

Gestión del riesgo Boehm
Identificación del riesgo

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.

Gestión del riesgo Boehm
Identificación del riesgo

- La *Taxonomía SEI de Riesgos del Software** puede ser considerada como otra forma de listar los riesgos del proyecto
- La taxonomía clasifica las características de desarrollo del software
- Identificando las características problemáticas se pueden identificar los riesgos

*CMU/SEI-93-TR-6

Gestión del riesgo Boehm
Análisis del riesgo

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

Gestión del riesgo Boehm
Análisis del riesgo

- La asignación de probabilidades y consecuencias puede *estimarse* directamente, o mediante técnicas como las descritas en el *AFSC/AFLC pamphlet 800-45* de la USAF*

*Estas técnicas vienen descritas en *Software Engineering: A manager's guide* de Pressman.

Gestión del riesgo Boehm
Análisis del riesgo

- Otra opción es utilizar la tabla SQAS-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-$10^{-1)}$	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

Asignación de probabilidad y consecuencias según SQAS-SEI

Gestión del riesgo Boehm
Análisis del riesgo

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

Gestión del riesgo Boehm
Análisis del riesgo

E.1 Example 1: Risk Accounting Form

Risk Accounting Form[1]	
Identified by:	**Date:**
	ID #: *OM Tracking #*
Statement of Risk (with context):	

	Consequence: (**C**ost , **S**chedule, **P**erformance, **Q**uality)	Risk Magnitude Rm
	Severity: (**C**ritical, **S**erious, Mo**d**erate, **M**inor)	
	Probability of occurrence? (**H**igh, Me**d**ium , **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:		

Ejemplos de formulario de gestión del riesgo

Gestión del riesgo Boehm
Priorización del riesgo

- La *priorización* de riesgos produce una lista ordenada de elementos de riesgo identificados y analizados
- Una técnica de priorización es crear una *tabla de riesgo* que los ordena por 1º probabilidad y 2do consecuencia.
  - Así, solo los riesgos por encima de la *línea de corte* son considerados

Gestión del riesgo Boehm
Priorización del riesgo

- Otra técnica de priorización es calcular la *exposición al riesgo*, multiplicando probabilidad por consecuencias
  - Así, sólo se tratan los riesgos de mayor exposición

Gestión del riesgo Boehm
Priorización del riesgo

- Otra opción es utilizar mecanismos como los descritos en SQAS-SEI para calcular su *nivel de riesgo*

Severity \ Probability	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

Nivel de riesgo según SQAS-SEI

Gestión del riesgo Boehm
Priorización del riesgo

- Los niveles de riesgo son:
  - 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.

Gestión del riesgo Boehm
Priorización del riesgo

- 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

Gestión del riesgo Boehm 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*.

Gestión del riesgo Boehm
Planificación de gestión…

- Se analiza la lista ordenada de riesgos y se decide que 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.

Gestión del riesgo Boehm Planificación de gestión…

- 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 que mecanismos de reducción del riesgo se proponen
- También deben proponerse *planes de contingencia* por si los riesgos (evitados, controlados, asumidos o transferidos) se hacen reales

Gestión del riesgo Boehm
Resolución del riesgo

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

Gestión del riesgo Boehm Monitorización de riesgos

- Finalmente, 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 (e.g. usando métricas).
  - Se llevan a cabo las acciones correctivas necesarias

Plan RSGR

- La información esencial sobre el proceso de gestión del riesgo puede incluirse en un *Plan de Reducción, Supervisión y Gestión del Riesgo* (RSGR)
- Éste puede ser un documento independiente, o ser parte del plan del proyecto del software

Plan RSGR

- Así:
  - Durante la reducción se proponen pasos de reducción para:
    - 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.

Plan RSGR

– En gestión del riesgo, el riesgo se ha hecho real y se aplican las soluciones back-up (planes de contingencia) que hemos considerado en reducción del riesgo.

Plan RSGR

- Una plantilla puede ser:

1. Introducción
2. Priorización de riesgos del proyecto
3. Reducción, supervisión y gestión del riesgo
    - 3.k Riesgo k-ésimo
        - 3.k.1 Reducción.
        - 3.k.2 Supervisión.
        - 3.k.3 Gestión.
4. Planificación temporal
5. Resumen

IEEE Std. 1540-2001

- El *IEEE Standard for Software Life Cycle Processes-Risk Management* (1540-2001) define un proceso de gestión del riesgo continuo
- El proceso está formado por seis actividades:
  - *Planear e implementar la gestión del riesgo*: selecciona el proceso de gestión del riesgo

IEEE Std. 1540-2001

- *Gestionar el perfil de riesgo del proyecto*: identifica riesgos
- *Realizar análisis del riesgo*: asigna probabilidad, consecuencia y prioriza
- *Realizar tratamiento del riesgo*: selecciona 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

- 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

Gestión del riesgo
Principio de Pareto

- Para un proyecto grande (70.000 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”

Gestión del riesgo
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**
- e.g.
  - Control de aviones.
  - Software de centrales nucleares.

Conclusiones

- Riesgo
- No gestión riesgo → desastres
- Estrategia reactiva vs. proactiva
- Estrategia de Boehm
- *Boehm's Top 10 Software Risk Items*
- Plan RSGR
- Principio de Pareto
- Riesgos y peligros para la salud