PGP. Gestión de Riesgos

Introducción

Tipos y fuentes de riesgo

Paradigma de la gestión de riesgos

Fuentes Bibliográficas

PGP. Gestión de Riesgos

¿Por qué van mal los proyectos de software?

- Conocimiento poco adecuado de las necesidades del usuario
- Documentos de requisitos poco elaborados
- Gestión pobre de los requisitos
- Arquitectura/diseño pobre o inexistente
- Codificar primero y plantear las preguntas después
- Comprensión pobre del diseño/código de legado
- Falta de revisiones con colegas para detectar problemas en las etapas iniciales
- Personal sin experiencia o incompetente
- Pruebas poco efectivas que no detectan en defectos serios
- …

PGP. Gestión de Riesgos

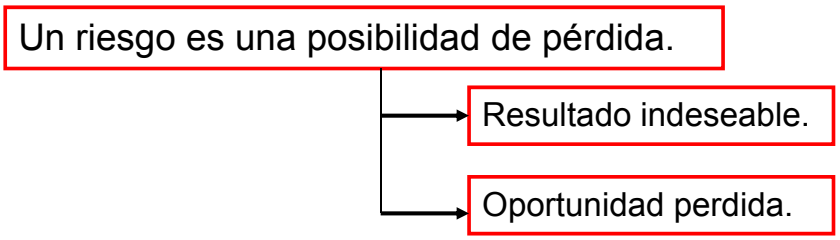
¿Qué es un riesgo?

PRINCE2 lo define como "*casualidad de exposición a las consecuencias adversas de eventos futuros*"

El PM-BOK proporciona la siguiente definición: "*Un riesgo es un evento o una condición inciertos que, si ocurren, tienen un efecto positivo o negativo sobre los objetivos del proyecto*"

Lo riesgos se relacionan con posibles problemas futuros, no con los actuales. Implican, por tanto, una posible causa y su efecto. Por ejemplo, un desarrollador se va -> la tarea se retrasa.

Genéricamente un riesgo es algo que puede ocurrir o no. Un riesgo es una medida de la probabilidad y pérdida de que se produzca un resultado inadecuado que afecte al producto, proceso o proyecto software.



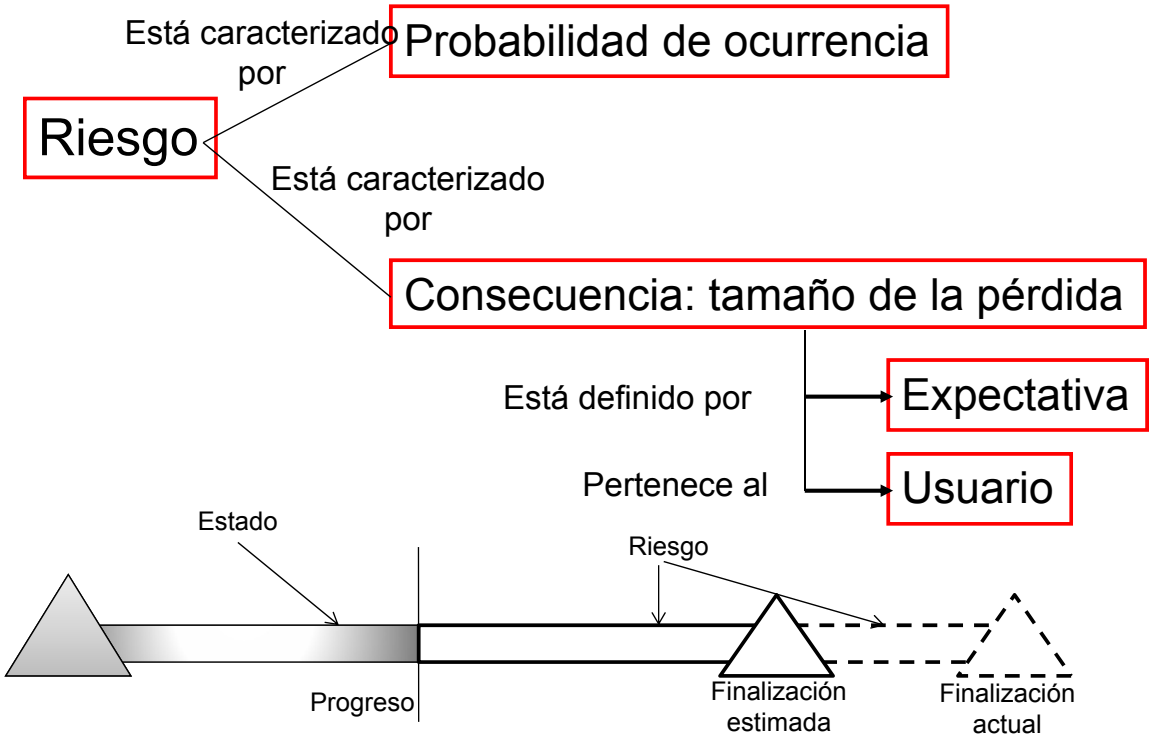
PGP. Gestión de Riesgos

Imprevistos en un viaje en coche

Situación imprevista	***Problema***	***Plan de acción***
Congestión inusual de tráfico	*Podría llegar tarde a una entrevista*	*Escuchar los informes de tráfico por la radio* *Plantear rutas alternativas antes de empezar el viaje*
Pinchazo en un neumático	*Podría no llegar a la entrevista o llegar tarde*	*Asegurarse que el neumático de repuesto está utilizable e inflado*
Rotura del coche o accidente	*Probablemente no llegar a la entrevista*	*No hay plan de acción*

PGP. Gestión de Riesgos

Anatomía de un riesgo



PGP. Gestión de Riesgos

Algo de historia:

- Barry Boehm publica su modelo en espiral y un tutorial sobre gestión de riesgos a finales de los años 80.
- Charette publica libros sobre gestión de riesgos y el modelo hélice de riesgos entre finales de los 80 y comienzos de los 90.
- Métodos de gestión de riesgos del SEI: taxonomía de riesgos y libro guía en los años 90.
- Principios de gestión de riesgos de Elaine Hall en 1998.
- Se incrementa en la industria la conciencia sobre el tema y se mejora la práctica.

PGP. Gestión de Riesgos

Tipos de riesgos

- De proyecto
  - Operativo
  - Organizativo
  - Contractual
- De proceso
  - De gestión
  - Técnico
- De producto

–Conocidos

–Predecibles

–Impredecibles

Hughes and Cotterell (2002) plantean la siguiente clasificación:

- Los debidos a dificultades de estimación.
- Los debidos a suposiciones hechas en el proceso de planificación.
- Los imprevisibles

PGP. Gestión de Riesgos

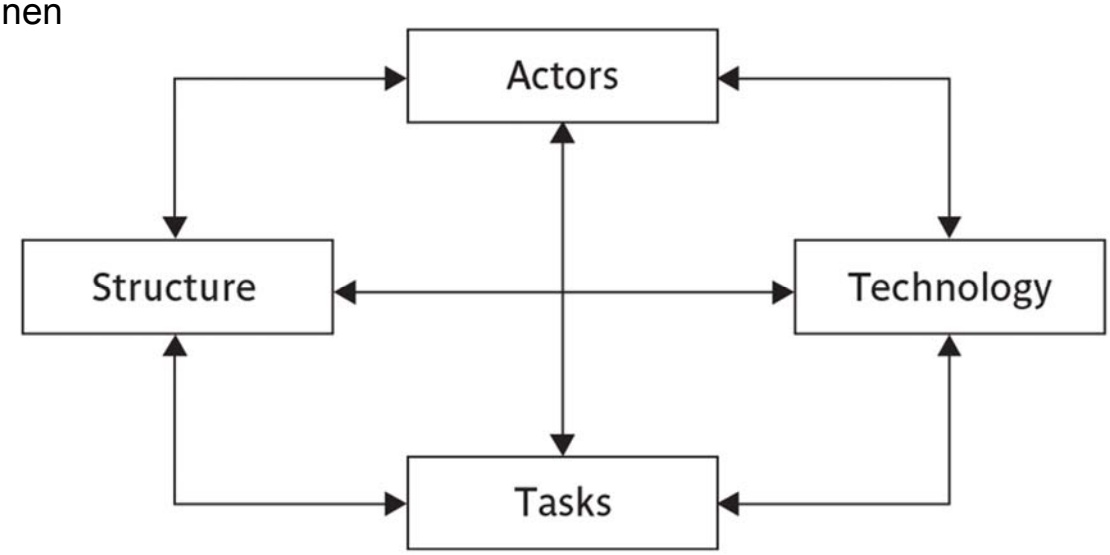
Algunas causas de los riesgos de software

- Riesgos de Proyecto
  - Restricciones de recursos, interfaces externas, relaciones con los proveedores, políticas internas, problemas de coordinación interna del equipo o del grupo, financiación no adecuada.
- Riesgos de Proceso
  - Proceso software no documentado, falta de revisiones efectivas de colegas, no prevención de defectos, proceso de diseño pobre, gestión pobre de requisitos, planificación ineficaz.
- Riesgos de Producto
  - Falta de experiencia en el dominio, diseño complejo, interfaces definidas deficientemente, sistemas de legado poco comprendidos, requisitos vagos o incompletos.

Pueden servir de pauta para considerar posibles riesgos en un proyecto.

PGP. Gestión de Riesgos

Categorías del Riesgo (basadas en el modelo de riesgo socio-técnico de Lytinen



Fuente: Bob Hughes and Mike Cotterell. *Software Project Management* (5e) The McGraw-Hill Companies, 2009

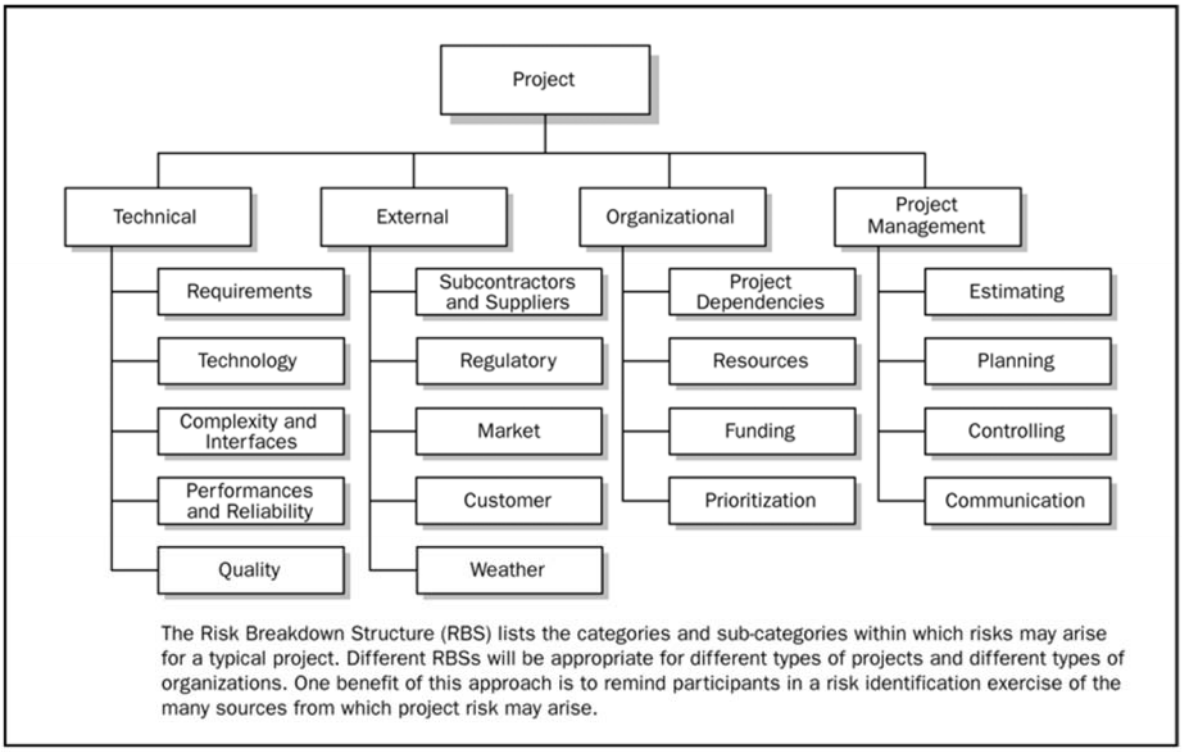
PGP. Gestión de Riesgos

Factores de riesgo:

- Debidos a la aplicación
- Debidos al personal
- Debidos al proyecto
- Métodos del proyecto
- De hardware/software
- Debidos al cambio/relevo del personal
- Debidos a los proveedores
- Debidos al entorno
- Factores ligados a la salud y a la seguridad

La relación no implica que todos vayan a existir en todos los proyectos, pero sí que se deben considerar

PGP. Gestión de Riesgos



The Risk Breakdown Structure (RBS) lists the categories and sub-categories within which risks may arise for a typical project. Different RBSs will be appropriate for different types of projects and different types of organizations. One benefit of this approach is to remind participants in a risk identification exercise of the many sources from which project risk may arise.

PMBOK Gráfico 11-4. Ejemplo de una Estructura de Desglose del Riesgo (RBS)

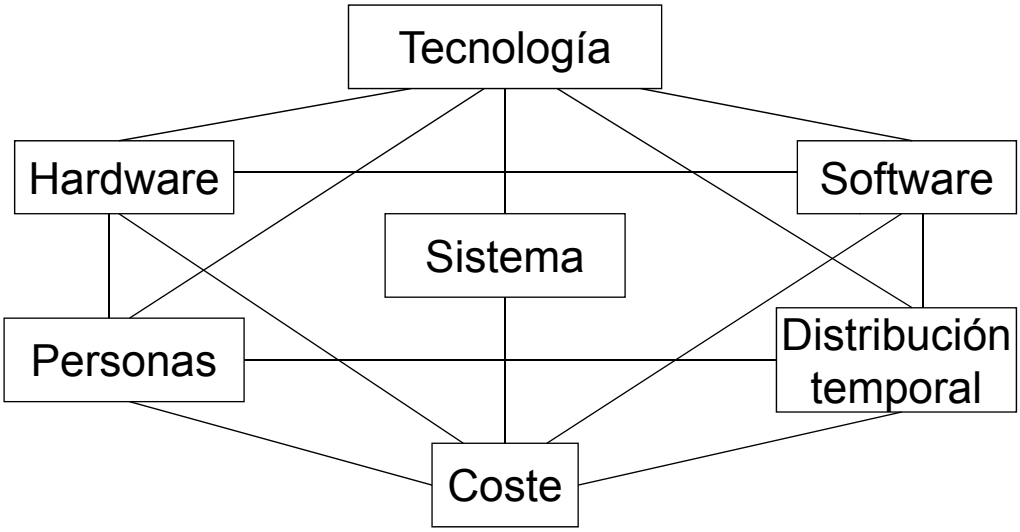
PGP. Gestión de Riesgos

"En el equipo del proyecto no hay nadie con experiencia en Interfaces gráficas de usuario" "Los requisitos son inestables"	Cosas que contribuyen al riesgo. **Factores de riesgo**
"Se puede gastar un tiempo excesivo en el desarrollo de IGU" "Los requisitos pueden cambiar"	Cosas que ocurren **Eventos de riesgo**
"A lo mejor tenemos que reelaborar la IGU" "Se necesita un esfuerzo de desarrollo extra debido a los cambios en los requisitos"	Consecuencias de las cosas que ocurren. **Consecuencias de los riesgos**
"El proyecto puede no cumplir plazos temporales o puede necesitar un presupuesto adicional"	Efectos de que ocurran las cosas **Efectos de los riesgos en los objetivos**
"Hay un 50% de probabilidad de que el responsable de pruebas se vaya antes de que comience la fase de pruebas"	Probabilidades de que ocurran cosas. **Probabilidad de riesgo**
"El uso de la herramienta CASE XXX es un riesgo en el proyecto" "¿Es un riesgo liberar un prototipo demasiado pronto?"	**Acción, persona u objeto asociados con el riesgo**

Factores de riesgos más habituales para diferentes tipos de proyectos de software

Sector del proyecto	Factor de riesgo	% de proyectos con riesgo
MIS	Modificación de los requisitos	80%
	Presión excesiva en el Plan.	65%
	Calidad baja	60%
	Sobrepasar el presupuesto	55%
	Control de configuración no adecuado	50%
Comercial	Documentación del usuario poco adecuada	70%
	Baja satisfacción del usuario	55%
	Tiempo de mercado excesivo	50%
	Acciones competitivas perjudiciales	45%
	Gastos de pleitos	30%

Fuentes de riesgo en desarrollo de software (contexto)



Sacado de [Higuera 1996], "*Software Risk Management*", Technical Report CMU/SEI-96-TR-012, ESC-TR-96-012, 1996

PGP. Gestión de Riesgos

Se llama **gestión de riesgos** a la práctica de valorar y controlar los riesgos que afectan a un producto, proceso o proyecto software. El propósito de la Gestión de Riesgos es identificar problemas potenciales antes de que ocurran. En general, la idea es describir inicialmente los objetivos y después se describen los riesgos en términos de incertidumbre, pérdidas y tiempo.

Los conceptos básicos de la gestión de riesgos son:

- Objetivo
- Incertidumbre
- Pérdidas. A veces se habla también de oportunidad y coste de oportunidad.
- Tiempo
- Elección
- Tomar decisiones inteligentes
- Resolver el riesgo
- Prevenir problemas

La gestión del riesgo es necesaria porque:

- El riesgo del software es inherente en este trabajo.
- El riesgo aumenta a medida que aumenta la complejidad del sistema.
- El riesgo impide conseguir los objetivos si no se considera.

PGP. Gestión de Riesgos

Entre las características de la Gestión de Riesgos se pueden considerar:

1.- Considerar las oportunidades y amenazas.

2.- Analizar la incertidumbre, incluyendo la ambigüedad, en donde esté presente.

3.- Preocuparse de las raíces de la incertidumbre en términos de lo que se conoce como las seis Ws (preguntas) de un proyecto:

- Quién (*who*)
- Porqué (*why*)
- Qué (*what*)
- De qué forma (*whichway*)
- Con qué (*wherewithal*). Con qué recursos.
- Cuando (*when*)

PGP. Gestión de Riesgos

¿Por qué se deben gestionar los riesgos?

•Todos los proyectos tienen riesgos y alguno de ellos ocurrirá.

•La gestión de riesgos es una inversión de futuro:

– Muchas veces es más barato evitar un problema potencial que corregir uno que se ha producido.

– Si se corrigen los problemas a medida que se presentan, el flujo de problemas posibles continuará en el futuro manteniéndote ocupado.

•Es importante conocer donde están los riesgos para enfocar sobre áreas esenciales de riesgos.

•La gestión intuitiva de riesgos rara vez es suficiente en el caso de proyectos grandes, complejos.

•La gestión mejora la predictibilidad y control de los proyectos.

•Para conseguir un conocimiento consistente de los riesgos en toda la organización.

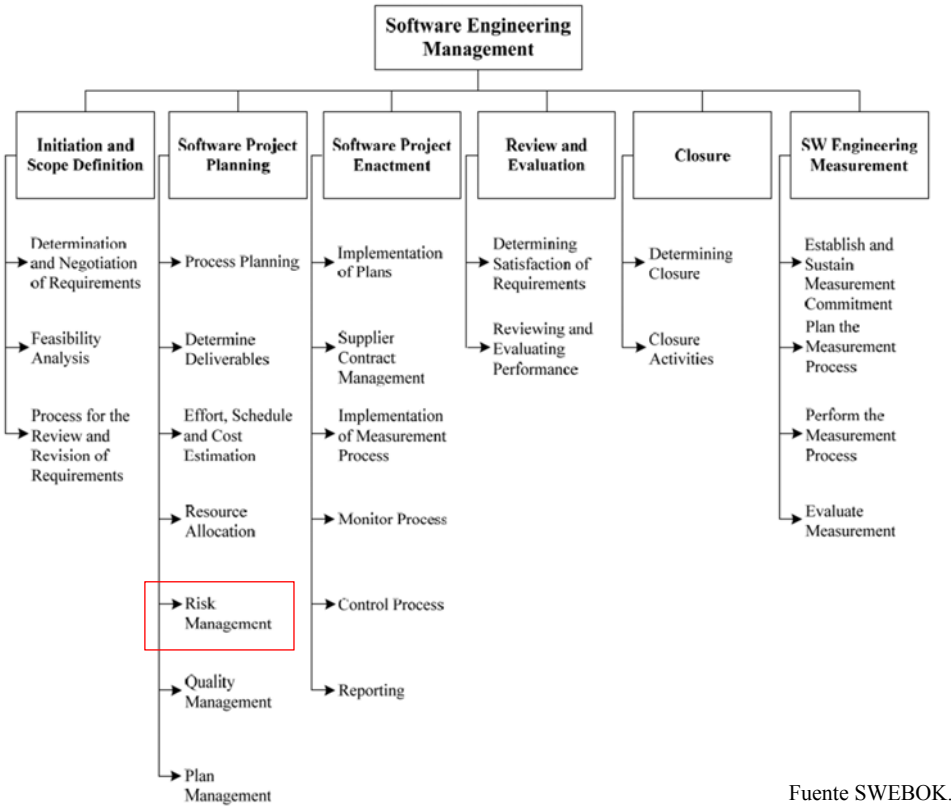
•Para aprender de los riesgos que se han producido.

PGP. Gestión de Riesgos

Es un proceso continuo, orientado hacia el futuro, que es una parte importante de la gestión de proyectos. Si la gestión de riesgos es tan importante ¿por qué casi nadie la realiza?

- Es difícil medir el éxito en gestión de riesgos.
- La gestión de riesgos es nueva, la gente no conoce sus posibilidades.
- El riesgo es un fenómeno abstracto, difícil de entender.
- Algunas organizaciones tienen una cultura interna que admite que pueden existir riesgos y desaconseja una aproximación analítica a los riesgos.
- La mayoría de los gestores de proyectos gestionan riesgos pero no lo consideran un tema importante.
- La mayoría de las organizaciones no consideran la acción de su gestión conjuntamente (proceso caótico).

PGP. Gestión de Riesgos



Fuente SWEBOK. Edición 2004.

PGP. Gestión de Riesgos

Procesos de un Área de Conocimiento	Grupos de Procesos de Dirección de Proyectos				
	Grupo de Procesos de Iniciación	Grupo de Procesos de Planificación	Grupo de Procesos de Ejecución	Grupo de Procesos de Seguimiento y Control	Grupo de Procesos de Cierre
11. Gestión de los Riesgos del Proyecto		Planificación de la Gestión de Riesgos 3.2.2.15 (11.1) Identificación de Riesgos 3.2.2.16 (11.2) Análisis Cualitativo de Riesgos 3.2.2.17 (11.3) Análisis Cuantitativo de Riesgos 3.2.2.18 (11.4) Planificación de la Respuesta a los Riesgos 3.2.2.19 (11.5)		Seguimiento y Control de Riesgos 3.2.4.11 (11.6)	

Correspondencia de los grupos de procesos de dirección de proyectos para la gestión de riesgos

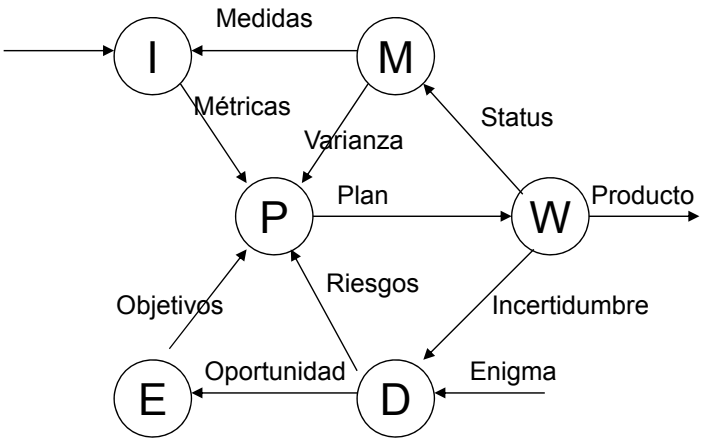
Fuente PMBOK. Edición 2004.

PGP. Gestión de Riesgos

Características de una buena gestión de riesgos

- Proactiva
- Integrada
- Sistemática
- Disciplinada (P^2I^2)
  - Personal
  - Proceso
  - Infraestructura
  - Implementación

PGP. Gestión de Riesgos



El modelo de seis disciplinas, que mejora el modelo de mejora evolutivo de W. Edwards Deming.:

(E) *Envision* (previsión, imaginación).

(P) Planificar el trabajo

(W) Trabajar el plan (work)

(M) Medir el trabajo

(I) Mejorar el proceso (improve)

(D) Descubrir las posibilidades

Adaptado de *Managing Risk: Methods for Software Systems Development.* Elaine M. Hall, Addison-Wesley 1998

PGP. Gestión de Riesgos

Principios de la gestión de riesgos del software (SEI)

Mantenimiento de una perspectiva global.

Tener una visión previsora, pensar en los riesgos que puedan aparecer en el futuro (por ejemplo cambios en el software).

Alentar la comunicación abierta. Si a alguien se le ocurre un riesgo potencial que no lo descarte. Se debe alentar tanto a los usuarios como a los miembros del equipo a sugerir riesgos.

Integración. El proceso de desarrollo de software debe estar integrado con la consideración permanente de los riesgos.

Enfatizar un proceso continuo.

Desarrollar una visión conjunta del producto (mayor implicación de los usuarios).

Alentar el trabajo en equipo.

PGP. Gestión de Riesgos

Paradigma de la gestión de riesgos del software (SEI 92)

Función	Descripción
Identificar	Buscar y localizar riesgos antes que se presenten los problemas
Analizar	Transformar los datos del riesgo en información para la toma de decisiones. Evaluar el impacto, probabilidad y establecer el tiempo, clasificar y priorizar los riesgos.
Planificar	Trasladar la información sobre riesgos en decisiones y acciones de disminución de su efecto (tanto en el presente como en el futuro) e implementar dichas acciones.
Seguir	Monitorizar los indicadores de riesgo y las acciones para mitigar su efecto.
Controlar	Corregir las desviaciones sobre los planes de disminución de su efecto.
Comunicar	Proporcionar información y realimentación interna y externa al proyecto en las actividades de riesgo, riesgos corrientes y riesgos emergentes.

En cualquier caso debe existir la comunicación en todas las funciones de gestión del riesgo.

Todas esas actividades pueden ser concurrentes entre los diferentes riesgos.

PGP. Gestión de Riesgos

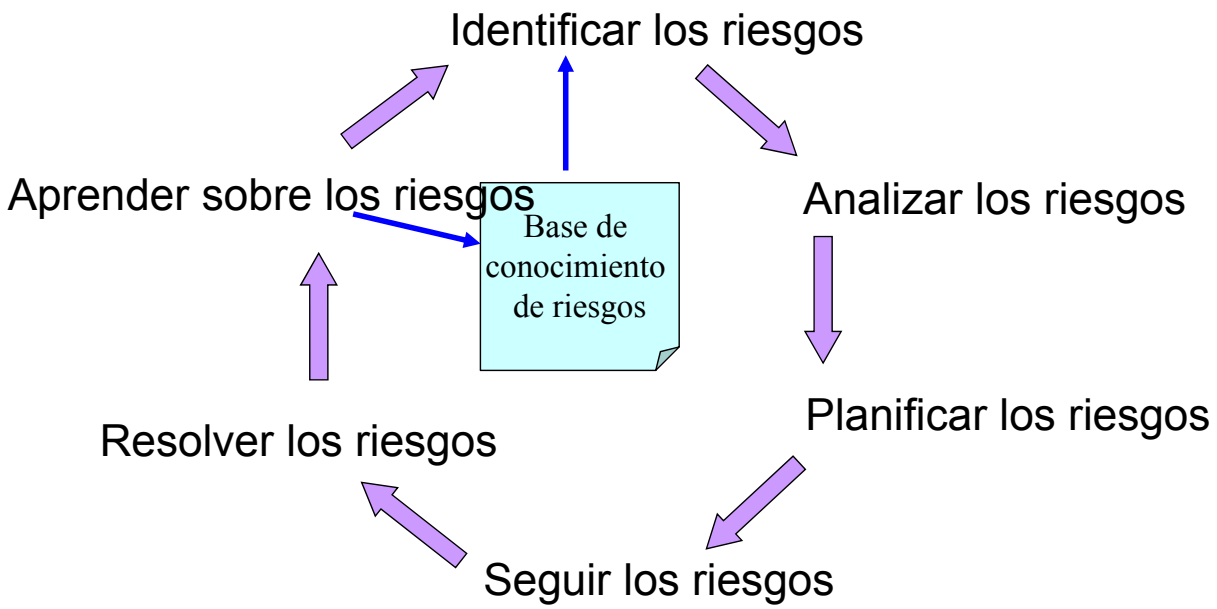
Hughes y Cotterell plantean el siguiente marco de trabajo para riesgos:

- Identificación del riesgo - ¿Qué riesgos puede haber?
- Análisis y priorización de los riesgos – ¿Cuáles son los riesgos mas serios?
- Planificación de los riesgos – ¿Qué haremos si se presentan?
- Monitorización del riesgo – ¿Cuál es el estado actual del riesgo?

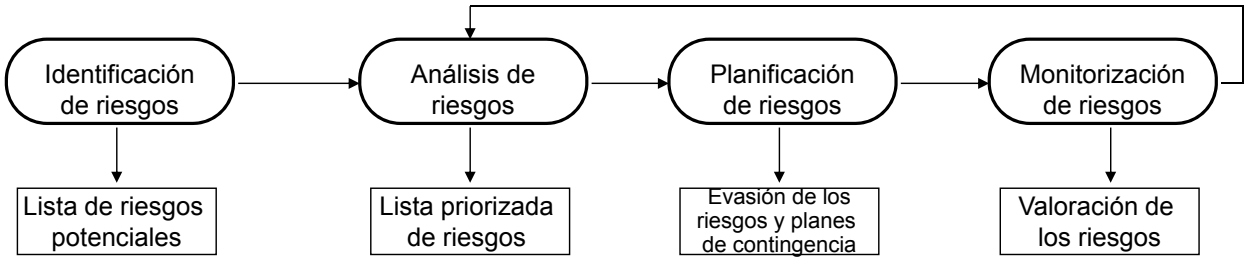
Fuente: Bob Hughes and Mike Cotterell. *Software Project Management* (5e) The McGraw-Hill Companies, 2009

PGP. Gestión de Riesgos

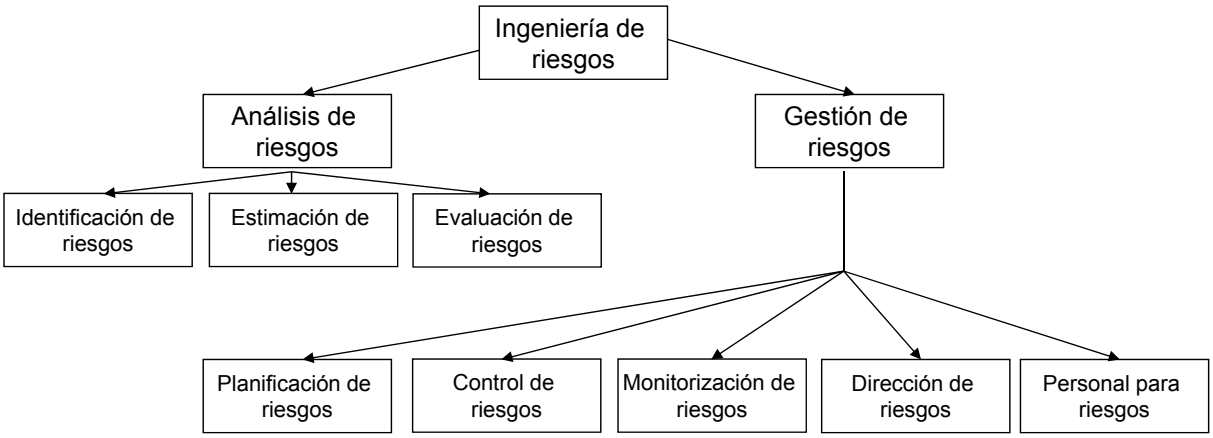
El proceso de Gestión de los Riesgos



PGP. Gestión de Riesgos



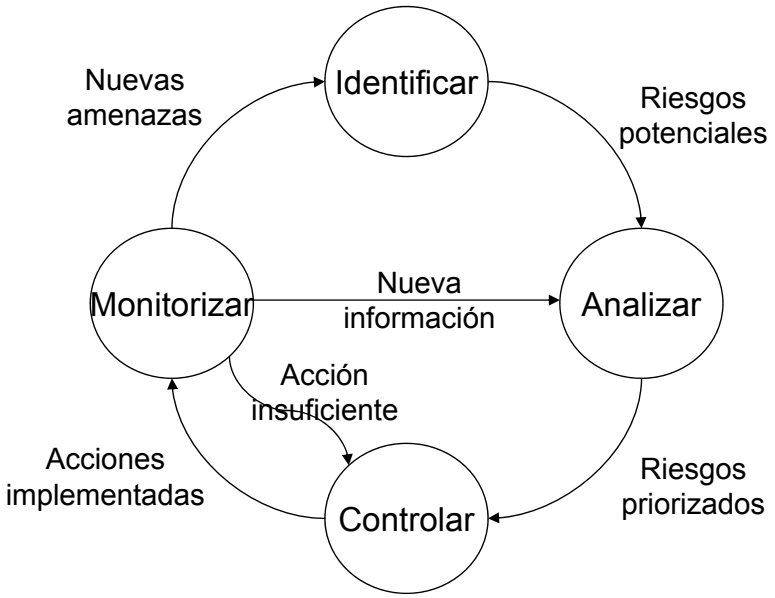
Proceso de gestión del riesgo, según Sommervile



Fuente: **Sommervile**

PGP. Gestión de Riesgos

Casi todos los métodos de gestión de riegos tienen un modelo de proceso genérico muy similar:



Identificación

Tareas relacionadas con la identificación de los riesgos:

- Realizar una valoración de los riesgos. (Formal, entrevistas, citas facilitadas)
- Identificar los riesgos de forma sistemática. (Listas de comprobación)
- Definir los atributos de los riesgos.
- Documentar los riesgos identificados.
- Comunicar los riesgos identificados.

Identificación: Descubrimiento

Tormenta de ideas del equipo

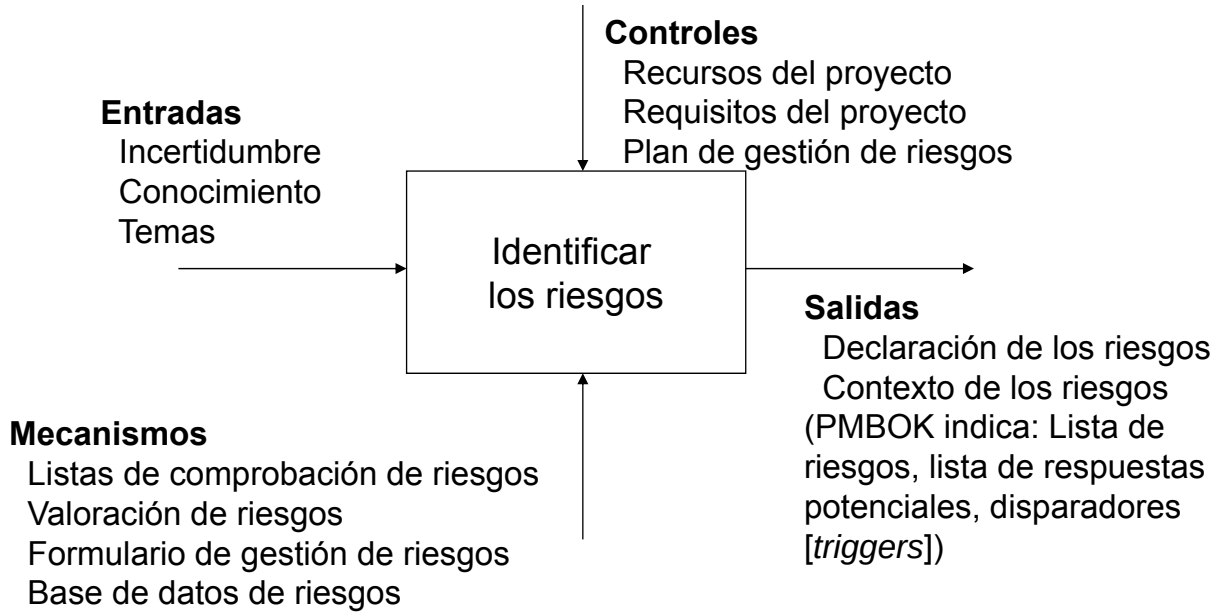
Búsqueda de Riesgos

Walkthroughs

Espúrio

Base de conocimiento de riesgos

PGP. Gestión de Riesgos



Proceso de identificación de los riesgos

PGP. Gestión de Riesgos

Listas de comprobación

Pros:

- Rápido y fácil de utilizar
- Estandariza los resultados
- Cubre un área amplia
- Puede provocar que se piense en nuevos riesgos

Contras:

- Causa fatiga
- No alienta la creatividad
- Puede ser sesgado debido a un dominio diferente
- No alienta que se encuentren riesgos específicos de la situación

Tormenta de ideas

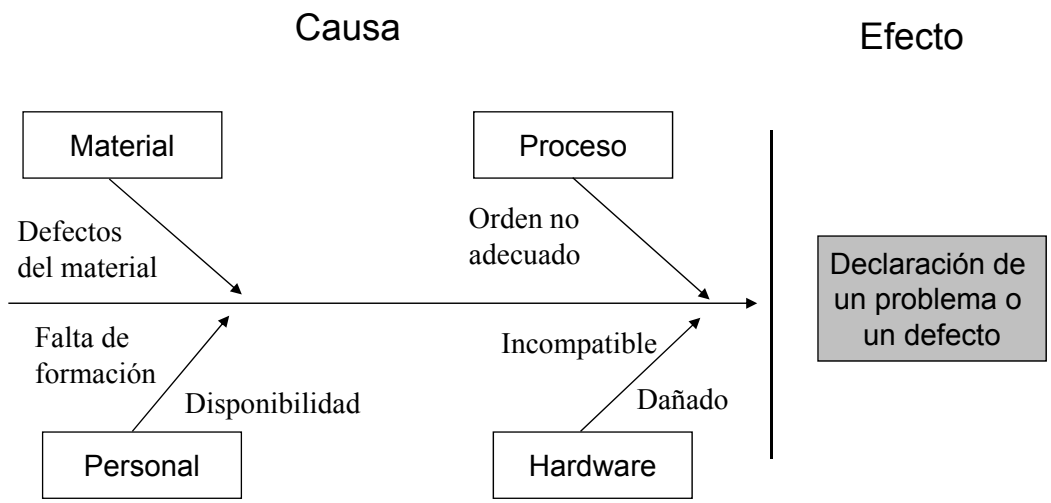
Pros:

- Rápido y fácil de utilizar
- Influencia del conocimiento y perspicacia de las personas
- Mantiene a los participantes activos
- Desarrolla compromisos

Contras:

- Requiere entrenamiento
- La dinámica de la reunión puede sesgar los resultados
- Dependiente de la experiencia de los participantes

PGP. Gestión de Riesgos



Los diagramas causa-efecto muestran la causas de un problema y el efecto que cada solución propuesta tendrá sobre el problema

Fuente: Kim Heldman, Vanina Magano. *PMP exam. Review guide*. Sybex. 2009

PGP. Gestión de Riesgos

Pautas para identificación de los riesgos:

- Comenzar con una tormenta de ideas abierta
  - Permite aprender y utilizar una técnica efectiva
- Realizar una tormenta de ideas focalizada
  - Por área de proyecto, *stakeholder*, objetivo, área técnica, etc.
- Utilizar lista de comprobación para garantizar un recubrimiento suficiente
  - Utilizar los elementos de dicha lista como puntos de discusión
  - Se puede utilizar después de la reunión para obtener una lista de riesgos
  - **¡Utiliza la experiencia para personalizar las listas de comprobación!**

PGP. Gestión de Riesgos

Identificación: Cuantificación

Exposición al riesgo = Probabilidad x Consecuencia

Matriz Impacto/Probabilidad

Impacto/ Probabilidad	Muy alto	Alto	Medio	Bajo	Muy bajo
Catastrófico	Alto	Alto	Moderado	Moderado	Bajo
Crítico	Alto	Alto	Moderado	Bajo	Ninguno
Marginal	Moderado	Moderado	Bajo	Ninguno	Ninguno
Despreciable	Moderado	Bajo	Bajo	Ninguno	Ninguno

Fuente: Pressman

PGP. Gestión de Riesgos

Descriptores cualitativos del impacto en el coste y rango de valores asociados

Impact level	*Range*
High	Greater than 30% above budgeted expenditure
Significant	20 to 29% above budgeted expenditure
Moderate	10 to 19% above budgeted expenditure
Low	Within 10% of budgeted expenditure.

PGP. Gestión de Riesgos

Estimación de los niveles de riesgo según ISO/IEC 27005:2008

	Likelihood of incident scenario	Very Low (Very Unlikely)	Low (Unlikely)	Medium (Possible)	High (Likely)	Very High (Frequent)
Business Impact	Very Low	0	1	2	3	4
	Low	1	2	3	4	5
	Medium	2	3	4	5	6
	High	3	4	5	6	7
	Very High	4	5	6	7	8

We have based the estimation of risk levels on ISO/IEC 27005:2008 (10).

PGP. Gestión de Riesgos

Matriz de Probabilidad e Impacto

Probabilidad	Amenazas					Oportunidades				
0,90	0,05	0,09	0,18	0,36	0,72	0,72	0,36	0,18	0,09	0,05
0,70	0,04	0,07	0,14	0,28	0,56	0,56	0,28	0,14	0,07	0,04
0,50	0,03	0,05	0,10	0,20	0,40	0,40	0,20	0,10	0,05	0,03
0,30	0,02	0,03	0,06	0,12	0,24	0,24	0,12	0,06	0,03	0,02
0,10	0,01	0,01	0,02	0,04	0,08	0,08	0,04	0,02	0,01	0,01
	0,05	0,10	0,20	0,40	0,80	0,80	0,40	0,20	0,10	0,05

Impacto (escala de relación) sobre un objetivo (por ejemplo, coste, tiempo, alcance o calidad)

Cada riesgo es clasificado de acuerdo con su probabilidad de ocurrencia y el impacto sobre un objetivo en caso de que ocurra. Los umbrales de la organización para riesgos bajos, moderados o altos se muestran en la matriz y determinan si el riesgo es calificado como alto, moderado o bajo para ese objetivo.

Fuente: PMBOK 2004

Planif. y Gestión de Proyectos de Software *2015-2016*

PGP. Gestión de Riesgos

Condiciones Definidas para Escalas de Impacto de un Riesgo sobre los Principales Objetivos del Proyecto
(Sólo se muestran ejemplos para impactos negativos)

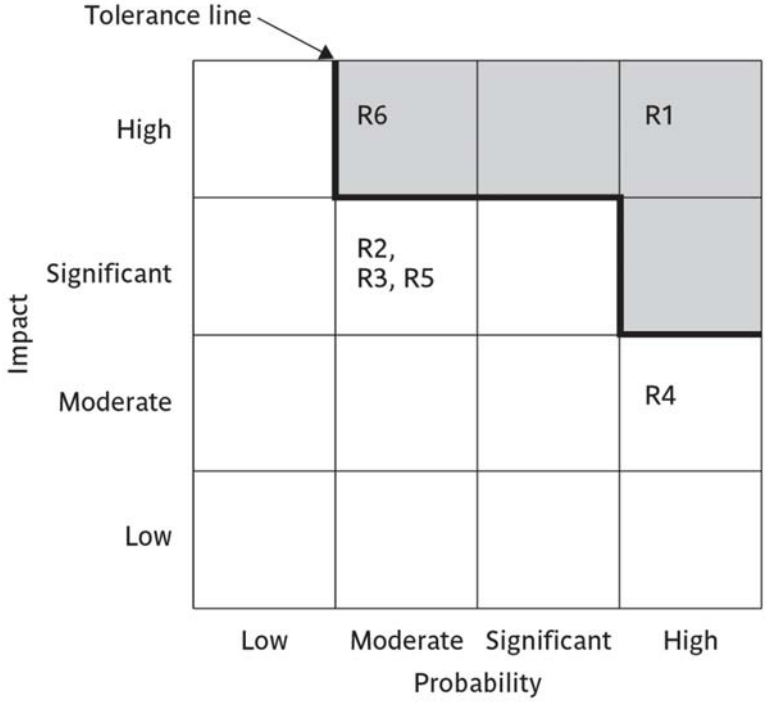
	Se muestran escalas relativas o numéricas				
Objetivo del Proyecto	Muy bajo /0,05	Bajo /0,10	Moderado /0,20	Alto /0,40	Muy alto /0,80
Coste	Aumento de coste insignificante	Aumento del coste <10%	Aumento del coste del 10-20%	Aumento del coste del 20-40%	Aumento del coste >40%
Tiempo	Aumento de tiempo insignificante	Aumento del tiempo <5%	Aumento del tiempo del 5-10%	Aumento del tiempo del 10-20%	Aumento del tiempo >20%
Alcance	Disminución del alcance apenas perceptible	Áreas de alcance secundarias afectadas	Áreas de alcance principales afectadas	Reducción del alcance inaceptable para el patrocinador	El elemento terminado del proyecto es efectivamente inservible
Calidad	Degradación de la calidad apenas perceptible	Sólo las aplicaciones muy exigentes se ven afectadas	La reducción de la calidad requiere la aprobación del patrocinador	Reducción de la calidad inaceptable para el patrocinador	El elemento terminado del proyecto es efectivamente inservible

Esta tabla presenta ejemplos de definiciones del impacto de los riesgos para cuatro objetivos del proyecto diferentes. Estos deben adaptarse al proyecto individual y a los umbrales de riesgo de la organización en el proceso Planificación de la Gestión de Riesgos. Las definiciones del impacto pueden desarrollarse para las oportunidades de forma similar.

Fuente: PMBOK 2004

PGP. Gestión de Riesgos

Ejemplo de aplicación de la matriz probabilidad-impacto



La esquina superior derecha indica que requieren una acción urgente

Fuente: Bob Hughes and Mike Cotterell. *Software Project Management* (5e) The McGraw-Hill Companies, 2009

PGP. Gestión de Riesgos

Ordenación de riesgos

Valores crecientes (de más crítico a menos crítico)

Prioridad	*Criterio*	*Acción*
1	Cualquier riesgo crítico	Tomar una acción inmediata
2	Significativo, probable y próximo en el tiempo	Iniciar procedimientos de la planificación de riesgos
3	Significativo, probable y lejano en el tiempo	Conseguir más información y realizar una revisión en la siguiente reunión
4	Significativo pero poco probable	Conseguir más información sobre la posibilidad y volver a valorar
5	No significativo	Mantener bajo revisión

Las medidas del impacto deben contemplar también costes potenciales:

- Coste de los retrasos sobre las fechas de entrega fijadas
- Exceso en los costes por uso adicional de recursos o uso de otros más caros
- Los costes producidos o implícitos por cualquier alejamiento de la calidad o funcionalidad del sistema.

Adaptado de *Software Project Managment.* Hughes and Cotterell, Mc Graw-Hill 2002

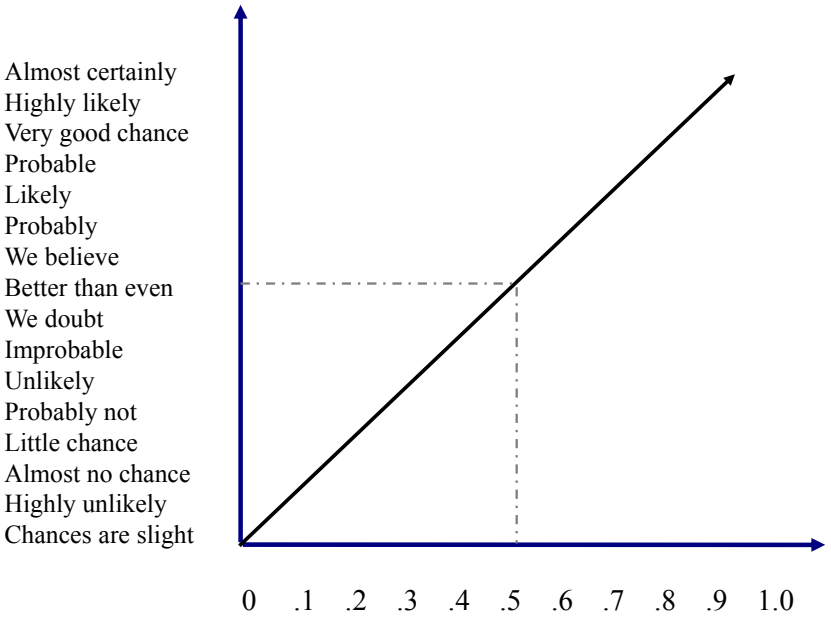
PGP. Gestión de Riesgos

Cálculo de la exposición al riesgo

Factor	**Prob.**	**Consec.**	**Exposición**
Entrega retrasada por el vendedor (ACME) de los componentes COTS	0.25	28 días	7 días
Retraso en la integración del API de ACME	0.6	15 días	9 días
Necesidad de pruebas de unidad adicionales; 3% más clases de las que se estimaron inicialmente	0.9	20 días	18 días
El grupo de pruebas Beta informa que no no pudieron encontrarnos un hueco hasta el 1 de mayo en lugar del 1 de abril	0.5	30 días	15 días
Exposición total al riesgo			49 días

Nota: En este caso para simplificar, todas las consecuencias de los riesgos son retrasos temporales.

Probabilidad percibida



Adapted from *Managing Risk: Methods for Software Systems Development* by Elaine M. Hall, Addison-Wesley 1998

PGP. Gestión de Riesgos

Porqué parece conveniente cuantificar los riesgos

- Permite la evaluación más crítica de las ideas de solución
- Alienta el diseño con la percepción del riesgo
- Facilita la realimentación sobre los riesgos que se han olvidado
- Permite la realimentación sobre el impacto de los riesgos que se han anticipado
- Facilita la reserva de recursos para tratar los riesgos
- Nos permite determinar si un riesgo es aceptable

PGP. Gestión de Riesgos

¿Qué indica el PMBOK sobre cuantificación de riesgos?

La cuantificación implica evaluar los riesgos y las interacciones entre ellos para valorar el rango de posibles consecuencias sobre el proyecto. El objetivo fundamental es determinar qué eventos de riesgo justifican respuesta.

Entradas:

- Tolerancias del cliente al riesgo, por ejemplo una organización puede considerar una probabilidad del 15% de sobrecoste como un riesgo elevado mientras otra puede considerarlo un riesgo bajo.
- Fuentes de riesgo
- Eventos de riesgos potenciales, como el desarrollo de una nueva tecnología.
- Estimaciones de coste
- Estimaciones de la duración de la actividad

PGP. Gestión de Riesgos

PMBOK. Cuantificación de riesgos (2)

Herramientas y técnicas:

- Valor monetario esperado (probabilidad x estimación de la ganancia o pérdida).
- Sumas estadísticas.
- Simulación, por ejemplo usando PERT o CPM
- Árboles de decisión
- Juicio de expertos

Salidas:

- Lista de amenazas a considerar o de oportunidades a seguir
- Lista de amenazas a aceptar y de oportunidades a ignorar.

PMBOK. Cuantificación de riesgos (3). Simulación

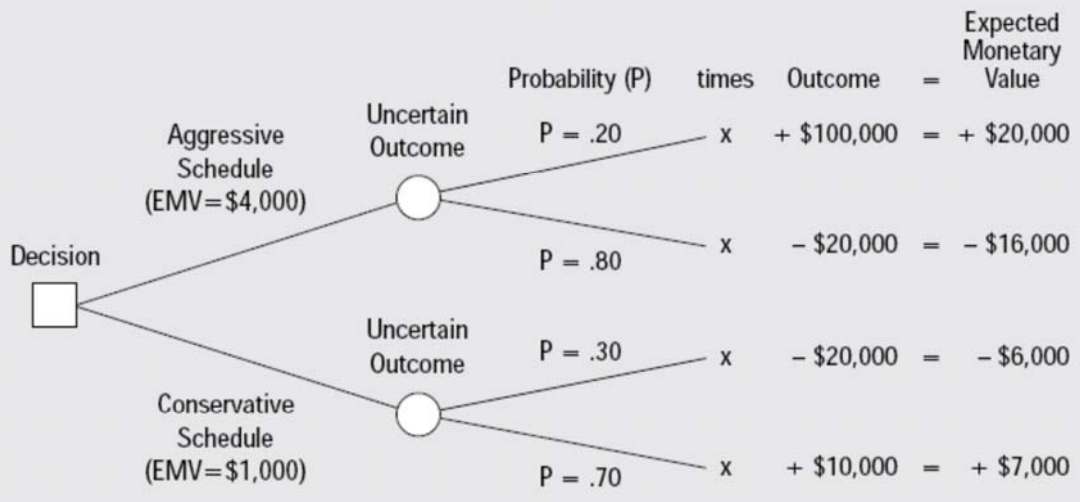
Figure 11–3. Results from a Monte Carlo Simulation of a Project Schedule

This S-curve shows the cumulative probability of project completion by a particular date. For example,the intersection of the dashed lines shows that there is a 50 percent probability that the project will be finished within 145 days of its start. Project completion dates toward the left have higher risk while those toward the right have lower risk.

PGP. Gestión de Riesgos

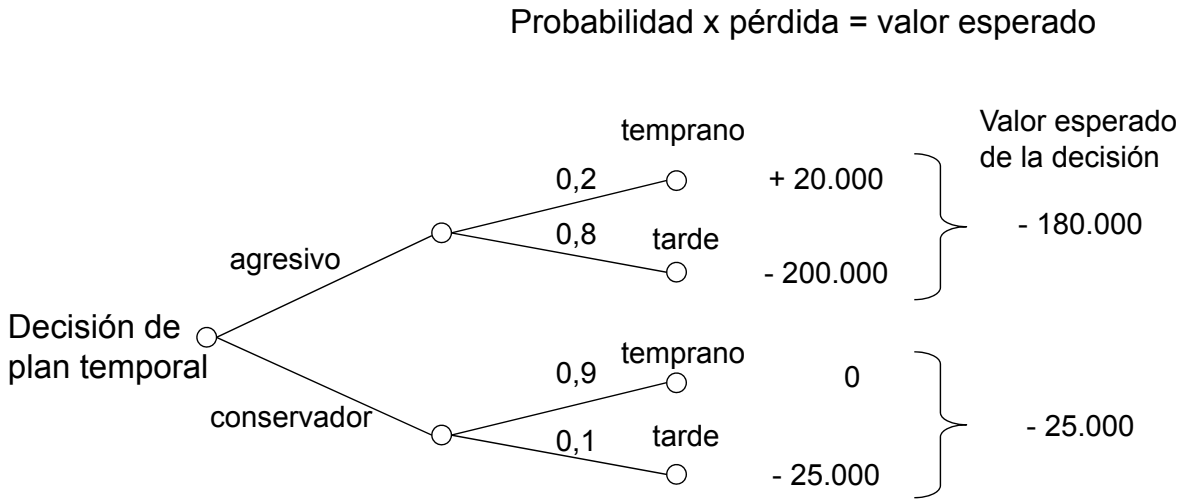
PMBOK. Cuantificación de riesgos (3). Árboles de decisión

Figure 11–5. Decision Tree



- Expected monetary value (EMV) of result = Outcome x Probability of that outcome.
- Expected monetary value of a decision = sum of EMVs of all Outcomes stemming from that decision.
- Aggressive schedule has expected monetary value of $4,000 and is "preferred" over conservative schedule with expected monetary value of $1,000.

PGP. Gestión de Riesgos



Ejemplo de árbol de decisión con datos más parecidos a la realidad

PGP. Gestión de Riesgos

Identificación: Documentación

Cabecera
Valoración
Plan de acción
Seguimiento
Resolución

Proyecto	*Nombre del proyecto*
Fecha	*Fecha de entrada*
Nombre del riesgo	*Nombre del riesgo*
Categoría del riesgo	*Tipo del riesgo*
Probabilidad	*Posibilidad de ocurrencia*
Consecuencias	*Gravedad del impacto*
Creador	*Quién informó este riesgo*
Fase/actividad	*En qué parte del proceso*
Elemento deWBS	*Relación con WBS*

Adaptado de *Managing Risk: Methods for Software Systems Development.*Elaine M. Hall, Addison-Wesley 1998

Identificación: Documentación

Un método para identificar riesgos es crear una ***lista de comprobación de los elementos de riesgo***.

Tamaño del producto: riesgos asociados con el tamaño general del software a construir o modificar.

Impacto en el negocio: riesgos asociados con las limitaciones de gestión o el mercado.

Características del cliente: riesgos asociados con las características de los clientes y la forma de comunicación del desarrollador con el cliente.

Definición del proceso: riesgos asociados con el grado de definición del proceso y su seguimiento por la organización.

Entorno de desarrollo: riesgos asociados con la disponibilidad y calidad de las herramientas que se van a emplear en la construcción del producto.

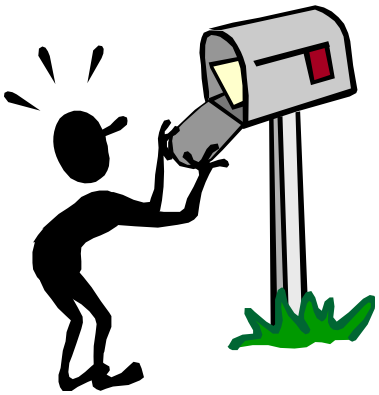
Tecnología a construir: riesgos asociados con la complejidad del sistema a construir y la tecnología que contiene el mismo.

Tamaño y experiencia de la plantilla: riesgos asociados con la experiencia técnica y de proyectos de los ingenieros de software.

PGP. Gestión de Riesgos

Identificación: Comunicación

Notificar a todos los “usuarios” afectados:



- Usuarios
- Responsable del Proyecto/Programa
- Miembros del equipo de gestión
- Departamento de Marketing
- Departamento de Ventas
- Soporte del usuario
- Departamento Financiero
- Garantía de Calidad
- …

Análisis de los riesgos: Preguntas

- ¿Cuán grave es la consecuencia?
- ¿Cuál es la probabilidad de su ocurrencia?
- ¿La exposición al riesgo es aceptable?
- ¿Con cuánta rapidez se debe tratar el riesgo?
- ¿Cuál es la causa del riesgo?
- ¿Existen semejanzas entre los riesgos?
- ¿Hay relaciones de dependencia entre ellos?
- ¿Cuáles son los conductores (*drivers*) del riesgo?

PGP. Gestión de Riesgos

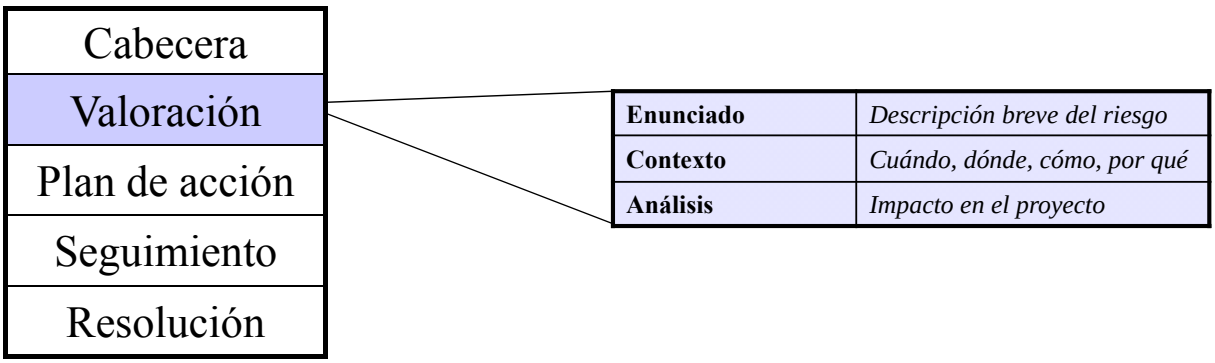
Análisis de los riesgos: Actividades

- **Agrupamiento**
  - Eliminar riesgos redundantes; combinar riesgos relacionados; enlazar riesgos dependientes
- **Determinación de los conductores de los riesgos (risk drivers)**
  - Factores subyacentes que afectan a la gravedad de las consecuencias
  - Pueden afectar a la estimación de la probabilidad, consecuencia y exposición al riesgo
  - Aumentan el conocimiento de cómo se pueden mitigar los efectos de los riesgos
- **Ordenación**
  - Ordenación de la probabilidad, consecuencia, exposición, marco temporal
- **Determinación de las causas raíz (fuentes del riesgo)**
  - Análisis anterior de las causas
  - Identificar causas comunes

Formato de la lista de los Top-n

Riesgo	Prioridad actual	Prioridad anterior	Semanas en Top 10	Estado del Plan de acción	Clasif. del riesgo
Tasa de productividad del Software alta	1	2	2	Captura de los requisitos usando una herramienta de base de datos de requisitos. Garantizando la disponibilidad de los recursos de personal adecuados	Alto
Nivel de Software externo	2	9	2	Incremento del presupuesto de viajes para revisiones “in-situ” adicionales. Habilitar la posibilidad de acceso mediante red.	Alto

Análisis: Documentación



Adaptado de *Managing Risk: Methods for Software Systems Development.*Elaine M. Hall, Addison-Wesley 1998

Planificación: Estrategias de Resolución

- **Evitación del riesgo**
  - Previene la ocurrencia del riesgo, reduce la probabilidad a cero
- **Protección del riesgo**
  - Reduce la probabilidad y/o consecuencia del riesgo antes de que ocurra
- **Reducción del riesgo**
  - Reduce la probabilidad y/o consecuencia del riesgo después de que ocurra
- **Investigar el riesgo**
  - Obtener más información para eliminar o reducir la incertidumbre
- **Reservar el riesgo**
  - Utilizar la planificación reservada previamente o la holgura del presupuesto
- **Transferencia del riesgo**
  - Reorganizar las cosas para desplazar el riesgo a cualquier parte (por ejemplo, a otro grupo)

Hay que considerar además la **aceptación del riesgo** que se produce cuando el coste de la evitación del riesgo puede ser más grande que el coste que puede suponer si se produce

PGP. Gestión de Riesgos

Ventaja de la reducción del riesgo =

$$(RE_{before} - RE_{after}) / (\text{Coste de la reducción del riesgo})$$

RE_{before} es la exposición al riesgo antes de su reducción. Por ejemplo 1% de posibilidad de que un incendio produzca unas pérdidas de 200.000 euros.

RE_{after} es la exposición al riesgo después de su reducción. Por ejemplo, una alarma anti-incendios que cuesta 500 euros reduce la probabilidad de pérdidas por fuego a un 0,5%

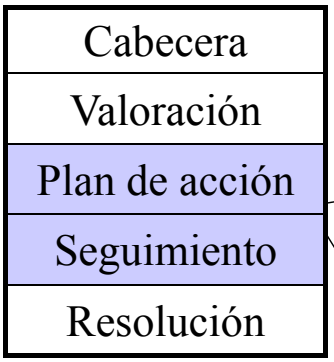
RRL = (1% de 200.000)-(0.5% de 200.000)/500 = 2

RRL > 1.00 por tanto se considera dicho valor

Planificación: Actividades

- **Especificar escenarios**
  - ¿Cómo seríamos capaces de decir qué está ocurriendo?
- **Definir umbrales cuantificados para los avisos iniciales**
  - Qué monitorizar, cuándo consideramos que el riesgo va a ocurrir
- **Desarrollar alternativas de resolución**
  - Formas de eliminar, mitigar o manejar el riesgo
- **Seleccionar la mejor aproximación a la resolución**
  - ¿Cuál es la que tiene mejor devolución de la inversión, ROI (Return Of Investment)?
- **Especificar el plan de acción de riesgos**
  - Documentar las decisiones

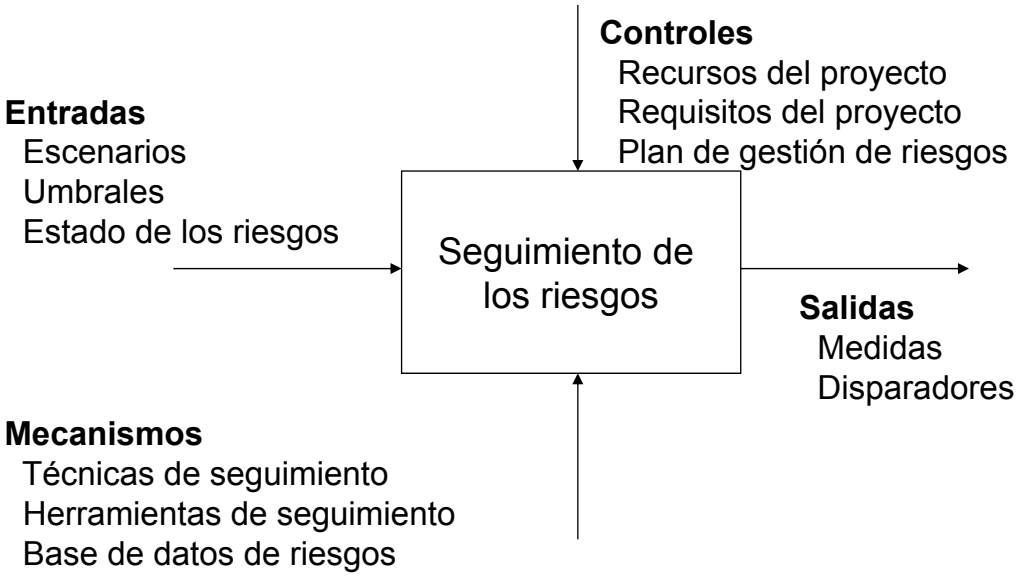
Planificación/seguimiento: Documentación



Escenario	*¿Qué sucedería?*
Indicador	*Métrica a ser seguida*
Condición de disparo	*Valor que indica el escenario del riesgo*
Punto de comprobación	*Cuándo/dónde comprobar la métrica*
Estrategia de resolución	*Cómo se debe manejar el riesgo*
Plan de acción	*Concretar un plan de acción*

Adaptado de *Managing Risk: Methods for Software Systems Development.*Elaine M. Hall, Addison-Wesley 1998

PGP. Gestión de Riesgos



Proceso de Seguimiento de los riesgos

PGP. Gestión de Riesgos

Seguimiento

- **Monitorizar escenarios de riesgo**
  - Vigilar por la aparición de signos de ocurrencia de un escenario del riesgo
- **Comparar los indicadores con las condiciones de disparo**
  - Medidas de indicadores de vigilancia – ¿Satisfacen las condiciones de disparo?
- **Notificar a los usuarios (stakeholders)**
  - Permitir que los usuarios conozcan el riesgo qué está ocurriendo. Ejecutar el plan de acción.
- **Recoger estadísticas**
  - Actualizar la base de datos de riesgos

PGP. Gestión de Riesgos

Por cada item de riesgo se deben preparar las respuestas apropiadas a:

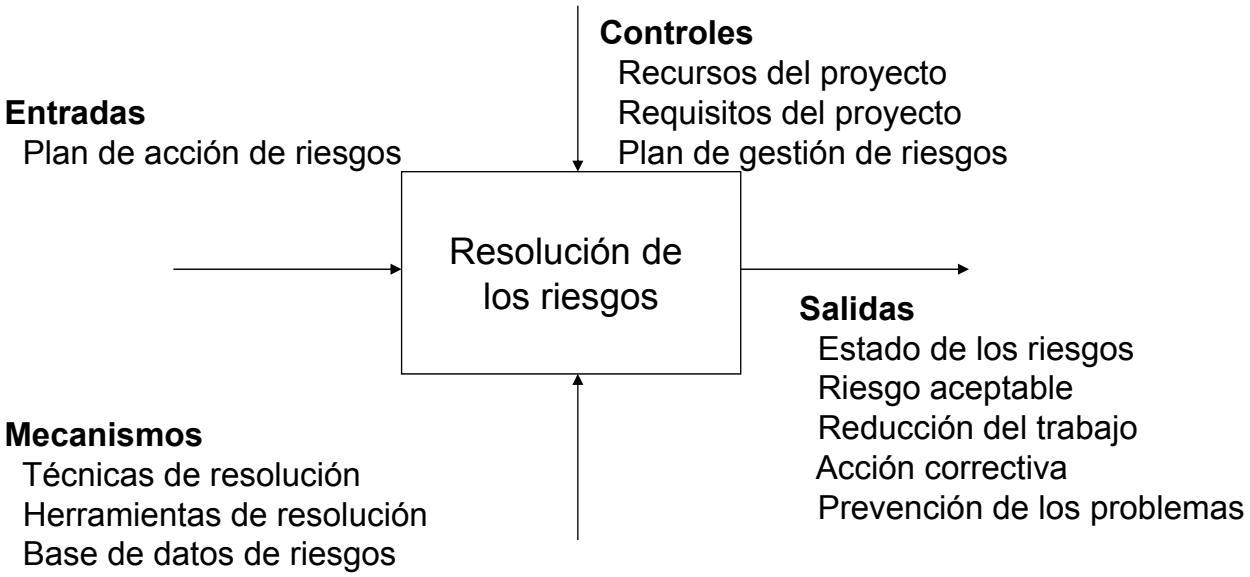
¿Quién es el responsable de la acción?

¿Cuándo se debe realizar la acción?

¿Cuál es la medida a vigilar?

¿Cuál es el valor de disparo de la medida?

PGP. Gestión de Riesgos



Proceso de Resolución de los riesgos

PGP. Gestión de Riesgos

Los objetivos de la resolución de riesgos son (entre otros):

- Asignar responsabilidad y autoridad al nivel de detalle más bajo posible.
- Seguir un plan de acción perfectamente documentado
- Informar del esfuerzo dedicado a la resolución de riesgos
- Tomar acciones correctivas cuando sea necesario
- Estar preparado para adaptarse a circunstancias cambiantes
- Mejorar la comunicación dentro del equipo
- Controlar de forma sistemática los riesgos

PGP. Gestión de Riesgos

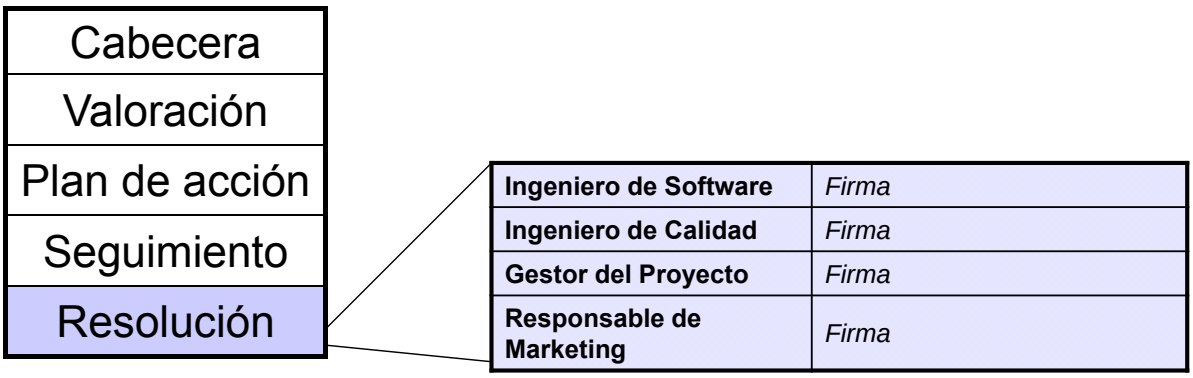
Resolución

- **Reconocimiento con acuse de recibo de la notificación**
  - Permitir a los usuarios conocer que “estás en la onda”
  - Indicar tiempo de respuesta
  - Determinar la responsabilidad/pertenencia
- **Ejecutar el plan de acción**
  - Improvisar, adaptar, superar
  - Buscado: sentido común
- **Proporcionar actualizaciones continuas**
  - Permitir a los usuarios conocer el progreso realizado resolviendo el riesgo
- **Recoger estadísticas**
  - Actualizar la base de datos de riesgos

Criterios de selección

- Escoger una estrategia de coste efectiva
  - Impulso del riesgo (coste-beneficio) = $RE_{(antes)} - RE_{(después)}$ / Coste de resolución
  - ROI = Σ Ahorro/Coste
- Diversificación
  - "*No poner todos los huevos en un cesto*".

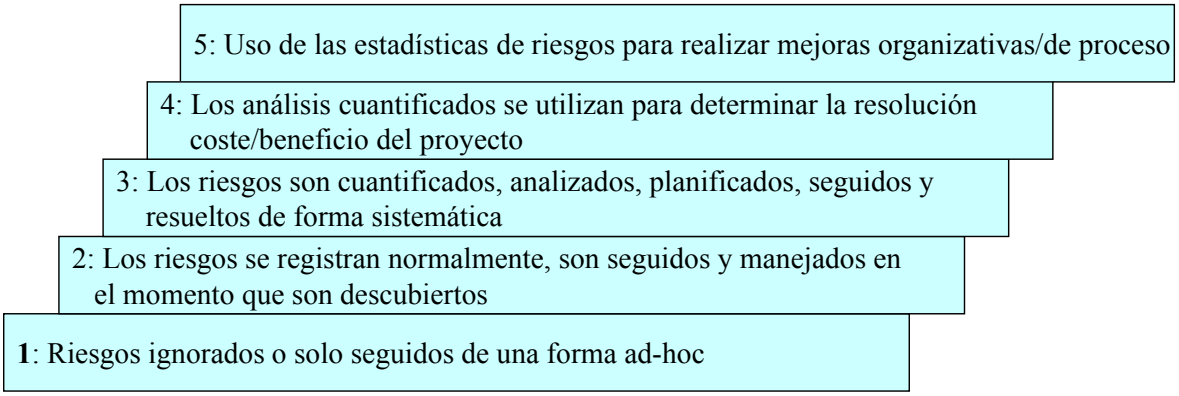
Resolución: Documentación



Adaptado de *Managing Risk: Methods for Software Systems Development*.Elaine M. Hall, Addison-Wesley 1998

PGP. Gestión de Riesgos

Capacidad para la Gestión de Riesgos (modelo CMM del SEI)



PGP. Gestión de Riesgos

Niveles de gestión de riesgos:

Invisible No existe evidencia sobre que se realcen actividades de gestión de riesgos en los proyectos, toda la gestión de riesgos es intuitiva y está incluida implícitamente en la gestión de proyectos.

Ad hoc Los gestores de proyectos realizan de forma ocasional actividades de gestión de riesgos por iniciativa propia.

Sugerida Existen plantillas para documentar los resultados de las actividades de gestión de riesgos, como una sección de gestión de riesgos en el plan de proyecto o una lista de riesgos en el informe de progreso del proyecto. Sin embargo dichas secciones no se requieren en los planes o informes actuales.

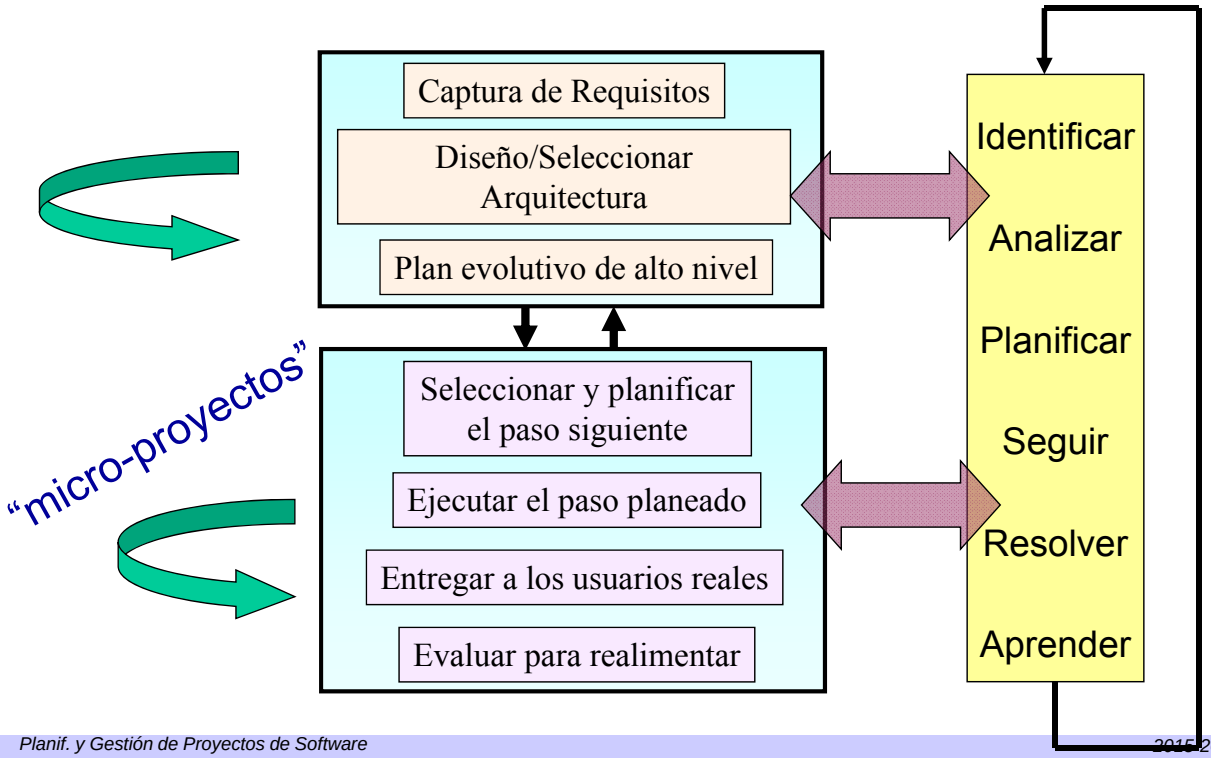
Requerida Los resultados de las actividades de gestión de riesgos son requeridas y comprobadas formalmente en los proyectos, un plan de gestión de riesgos es solicitado y se obtienen, actualizan y analizan las listas de riesgos con frecuencia.

Apoyada Existe un proceso definido para realizar la gestión de riesgos en la organización, incluyendo métodos, herramientas, pautas e infraestructura de apoyo.

Mejorada Existe un proceso sistemático para capturar la experiencia en gestión de riesgos y mejorar las prácticas de dicha gestión basadas en las experiencias anteriores.

PGP. Gestión de Riesgos

Entrega Evolutiva



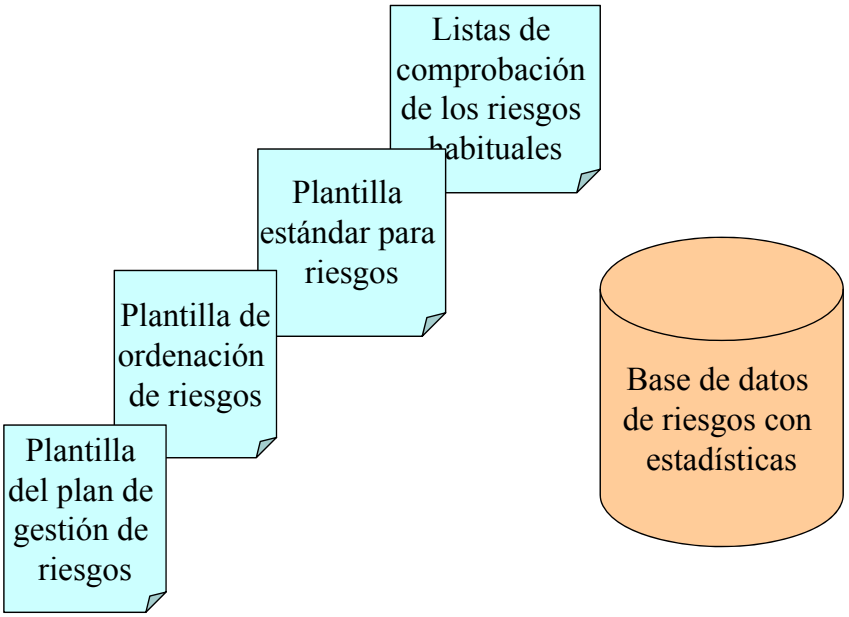
PGP. Gestión de Riesgos

Aprendiendo de los riesgos

- **Post mortem:**
  - ¿Cuáles fueron los riesgos no anticipados?
  - ¿Cuál fue la gravedad actual de la consecuencia?
  - ¿Qué estrategias de resolución funcionaron bien/no tan bien?
  - Qué tipos de riesgos se han podido:
    - ¿Prevenir o transferir?
    - ¿Protegernos de ellos o reducir?
    - ¿Manejar reservando únicamente recursos extra?

- **Acción:**
  - ¿Cuáles son las medidas preventivas que se pueden tomar en el futuro?
  - ¿Existen problemas significativos de prestaciones para el vendedor/partner?
  - ¿Qué podemos compartir con otros equipos de proyecto?

Infraestructura de gestión de riesgos



PGP. Gestión de Riesgos

Gestión de riesgos de proyecto (Resumen)

Incluye los procesos relacionados con la identificación, análisis y control de los riesgos.

- ***Identificación de riesgos***. Determinar los riesgos que probablemente pueden afectar al proyecto y documentar las características de cada uno.
- ***Cuantificación del riesgo***. Evaluar los riesgos y las interacciones entre ellos para valorar los posibles resultados en el proyecto.
- ***Desarrollo de respuesta a los riesgos***. Definir los posibles pasos para responder a las consecuencias de los riesgos.
- ***Control de la respuesta a los riesgos***. responder a los riesgos en el curso del proyecto.

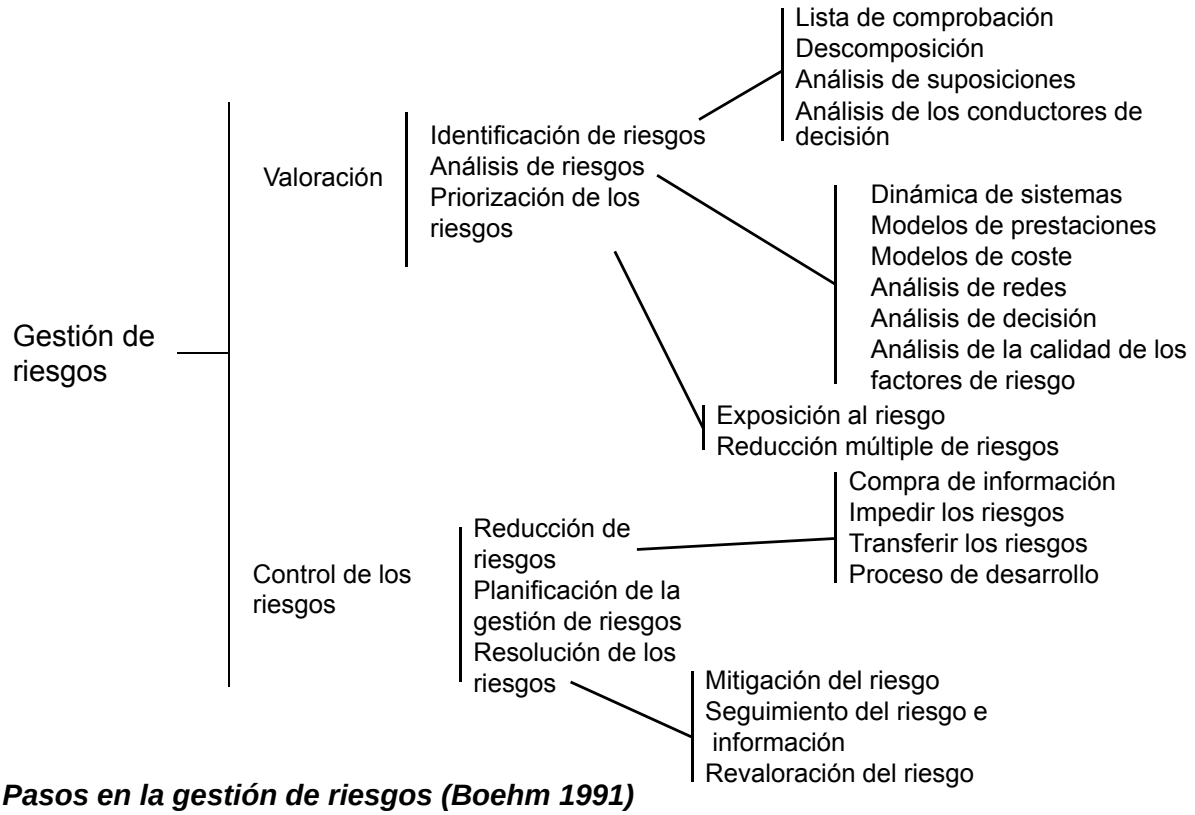
PGP. Gestión de Riesgos

Lista de los 10 riesgos más importantes, según Boehm (1991)

- •Fallos de personal.
- •Planificaciones en tiempo y presupuesto no realistas.
- •Desarrollo de funciones software incorrectas.
- •Desarrollo de interfaces incorrectas.
- •“Chapado en oro”.
- •Secuencia continuada de cambios en los requisitos.
- •Fallos en las tareas realizadas externamente.
- •Fallos en los componentes proporcionados externamente.
- •Fallos en las prestaciones de tiempo real.
- •Capacidades informáticas forzadas

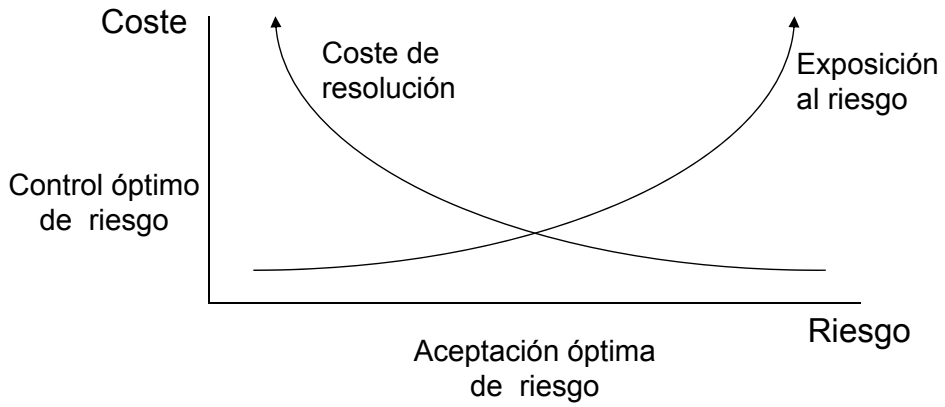
Fuente: Software engineering. Shari Lawrence Pfleeger

PGP. Gestión de Riesgos



Pasos en la gestión de riesgos (Boehm 1991)

PGP. Gestión de Riesgos



Proceso optimizado de gestión del riesgo. Se minimizan el riesgo y el coste total mediante una resolución adecuada del coste-riesgo. Si no hay atención al riesgo se incrementa su exposición al mismo.

PGP. Gestión de Riesgos

Los riesgos son un negocio arriesgado

- Los riesgos son inherentes al desarrollo de cualquier sistema de software grande. Una forma habitual de aproximarse a ellos es ignorarlos.
- Los que eligen minimizar o evitar los riesgos, en oposición a gestionarlos, están realizando un curso para obsolescencia.
- Si no atacas los riesgos activamente, ellos te atacarán activamente a ti.
- Cualquier cosa que pueda ir mal irá mal y en el peor momento posible.
- Si has detectado 4 formas posibles por las que puede fallar tu proyecto, se presentará por sí misma una quinta forma.

PGP. Gestión de Riesgos

Fuentes Bibliográficas

Parte de las ideas reflejadas en este material se han obtenido de Elaine M. Hall. *Managing Risk*. *Methods for Software Systems Development*. Addison-Wesley, 1998

En los libros de Gestión de proyectos de software, como los reseñados a continuación existe un capítulo dedicado a gestión de riesgos.:

- *A Guide to the Project Management Body* of Knowledge. Project Management Institute, 2004. El capítulo 11 está dedicado a la gestión de riesgos
- Bob Hughes and Mike Cotterell. *Software Project Management*. McGraw Hill, 2002. Dedican el capítulo 7 al tema de Gestión de Riesgos.
- Mary Beth Chrssis y otros. *CMMI para el desarrollo. Guía para la integración de procesos y la mejora de productos*. Ed. Universitaria Ramón Areces, 2012

Libros de Ingeniería de Software:

- Roger S. Pressman. *Ingeniería de Software. Un enfoque práctico*. McGraw-Hill 2002. El capítulo 3 está dedicado a Gestión de Proyectos y el 5 habla de planificación de proyectos. En la última edición el capítulo 25 se dedica completamente a gestión del riesgo.
- Ian Sommerville. *Ingeniería de Software,* Addison-Wesley 2002. El capítulo 4 tiene un punto dedicado a riesgos.

PGP. Gestión de Riesgos

Direcciones interesantes:

http://www.csl.sri.com/users/risko/risks.txt lista de riesgos que aparece en Software Engineering Notes de ACM.

http://www.sei.cmu.edu/risk/main.html página del Instituto de Ingeniería de Software de la CMU dedicada a riesgos.

http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html página de MAGERIT – versión 3. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.

http://www.wikilearning.com/curso_gratis/gestion_de_riesgos_en_ingenieria_del_software-introduccion/3620-1. Página con una lección desarrollada sobre gestión de riesgos. Hay una relación de preguntas a plantearse sobre usuarios, tecnología, etc. con relación a los riesgos.

PGP. Gestión de Riesgos

http://www.iso27000.es/herramientas.html#section7b

http://www.isaca.org/knowledge-center/risk-it-it-risk-management/Pages/Risk-IT1.aspx

http://www.executiveboard.com/blogs/5-it-risks-every-auditor-should-plan-for-in-2013/

http://www.bc.edu/content/bc/offices/audit/tech/itriskscontrols.html

http://www.spaceage.co.za/blog/technical/5-common-it-risks/

http://ist.mit.edu/security/tips

PGP. Gestión de Riesgos — Material adicional

Método de identificación de riesgos del SEI

Se basa en las siguientes suposiciones:

- Los riesgos del desarrollo de software son conocidos normalmente por el personal técnico del proyecto pero se comunican de forma deficiente.
- La gestión de los riesgos, para ser consistente, necesita un método estructurado y repetible de identificación de los mismos.
- La identificación efectiva de los riesgos debe cubrir todas las etapas del desarrollo de software.
- El proceso de identificación se debe fundamentar sobre bases objetivas, no sobre visiones tentativas (“yo creo que...”).
- No se debe plantear un juicio global sobre el éxito o el fracaso de un proyecto basado en el número o naturaleza de los riesgos cubiertos.

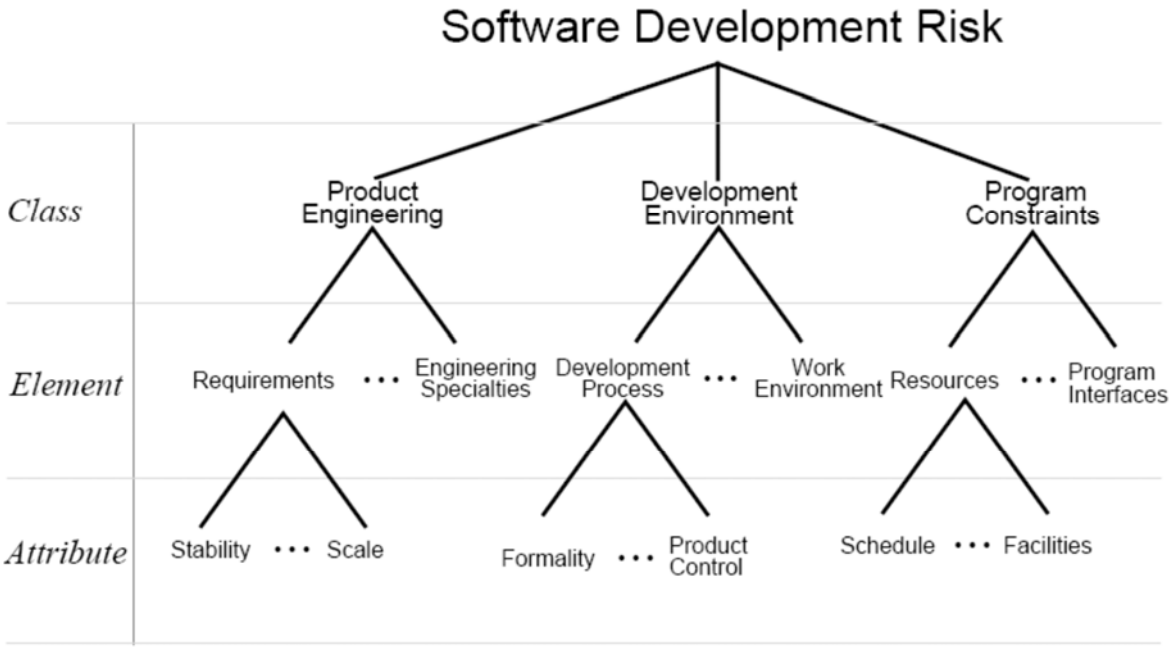
La taxonomía está organizada en tres *clases*:

- Ingeniería del producto. Aspectos técnicos del trabajo a realizar.
- Entorno de desarrollo. Métodos, procedimientos y herramientas utilizadas para producir el producto.
- Restricciones del programa. Factores contractuales, organizativos y operativos con los que se desarrolla el software pero que están fuera del control de la gestión local.

Dichas clases se dividen en *elementos* y cada elemento está caracterizado por sus *atributos*.

Por ejemplo, elementos de la clase de Ingeniería del producto son requisitos, diseño, codificación y pruebas unitarias, integración y pruebas y especialidades de ingeniería como seguridad o fiabilidad.

Estructura de la taxonomía



Desarrollo de la taxonomía

A. Product Engineering

1. Requirements
   a. Stability
   b. Completeness
   c. Clarity
   d. Validity
   e. Feasibility
   f. Precedent
   g. Scale
2. Design
   a. Functionality
   b. Difficulty
   c. Interfaces
   d. Performance
   e. Testability
   f. Hardware Constraints
   g. Non-Developmental Software
3. Code and Unit Test
   a. Feasibility
   b. Testing
   c. Coding/Implementation
4. Integration and Test
   a. Environment
   b. Product
   c. System
5. Engineering Specialties
   a. Maintainability
   b. Reliability
   c. Safety
   d. Security
   e. Human Factors
   f. Specifications

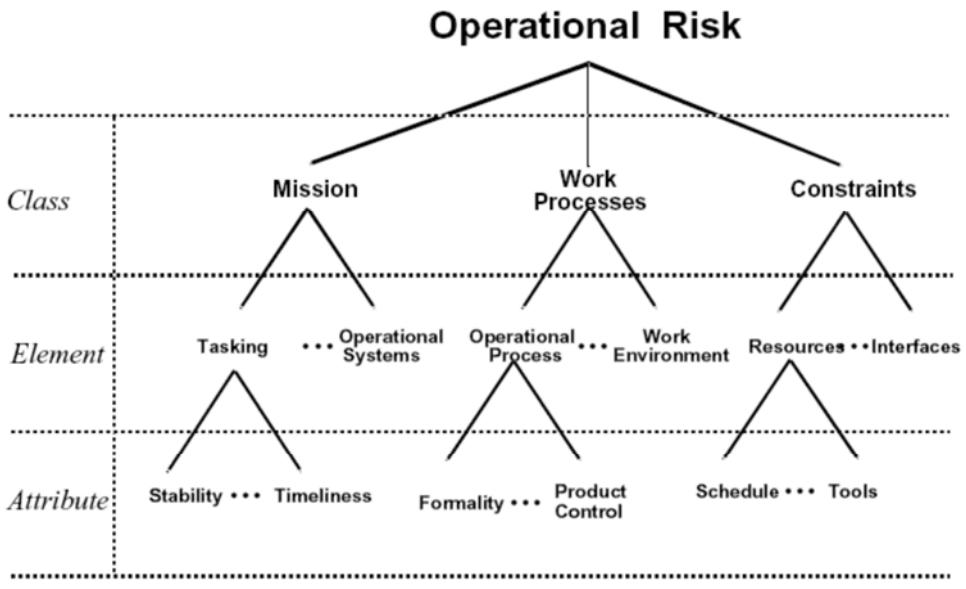
B. Development Environment

1. Development Process
   a. Formality
   b. Suitability
   c. Process Control
   d. Familiarity
   e. Product Control
2. Development System
   a. Capacity
   b. Suitability
   c. Usability
   d. Familiarity
   e. Reliability
   f. System Support
   g. Deliverability
3. Management Process
   a. Planning
   b. Project Organization
   c. Management Experience
   d. Program Interfaces
4. Management Methods
   a. Monitoring
   b. Personnel Management
   c. Quality Assurance
   d. Configuration Management
5. Work Environment
   a. Quality Attitude
   b. Cooperation
   c. Communication
   d. Morale

C. Program Constraints

1. Resources
   a. Schedule
   b. Staff
   c. Budget
   d. Facilities
2. Contract
   a. Type of Contract
   b. Restrictions
   c. Dependencies
3. Program Interfaces
   a. Customer
   b. Associate Contractors
   c. Subcontractors
   d. Prime Contractor
   e. Corporate Management
   f. Vendors
   g. Politics

PGP. Gestión de Riesgos Material adicional



Taxonomy of Operational Risks

A. Mission

1. Tasking, Orders and Plans
   a. Stability
   b. Completeness
   c. Clarity
   d. Validity
   e. Feasibility
   f. Precedent
   g. Timeliness
2. Mission Execution
   a. Efficiency
   b. Effectiveness
   c. Complexity
   d. Timeliness
   e. Safety
3. Product
   a. Usability
   b. Effectiveness
   c. Timeliness
   d. Accuracy
   e. Correctness
4. Operational Systems
   a. Throughput
   b. Suitability
   c. Usability
   d. Familiarity
   e. Reliability
   f. Security
   g. Inventory
   h. Installations
   i. System Support

B. Work Processes

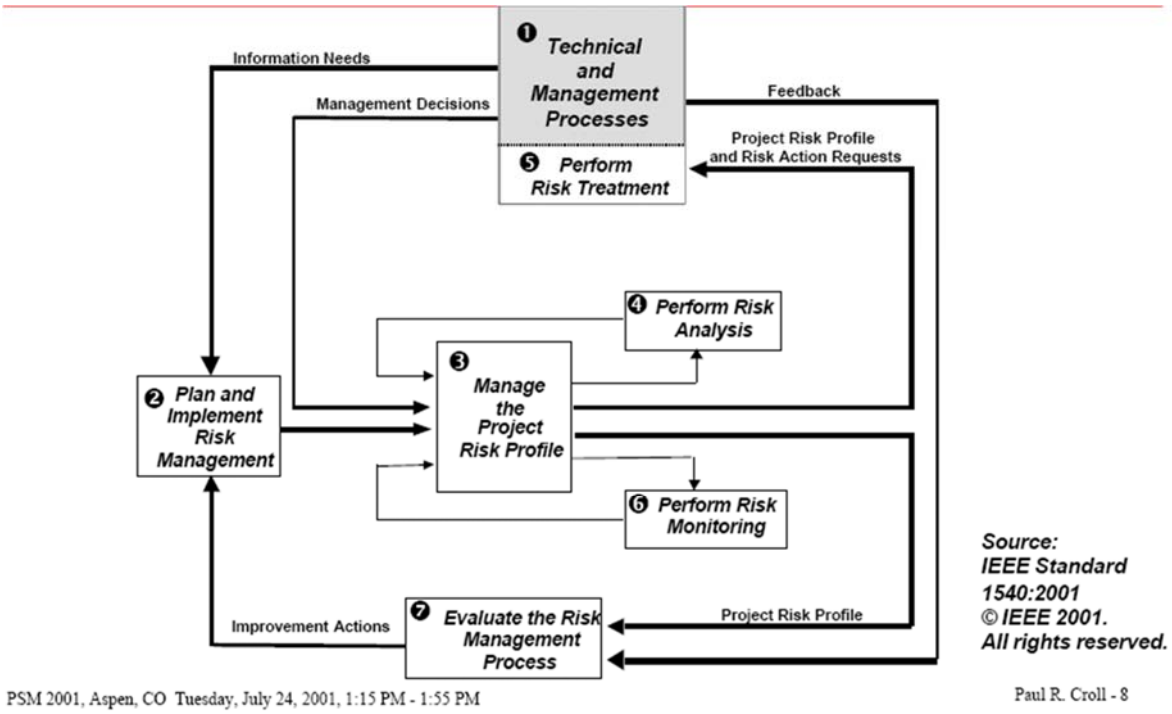
1. Operational Processes
   a. Formality
   b. Suitability
   c. Process Control
   d. Familiarity
   e. Product Quality
2. Maintenance Processes
   a. Formality
   b. Suitability
   c. Process Control
   d. Familiarity
   e. Service Quality
3. Management Process
   a. Planning
   b. Organization
   c. Management Experience
   d. Program Interfaces
4. Management Methods
   a. Monitoring
   b. Personnel Management
   c. Quality Assurance
   d. Configuration Management
5. Work Environment
   a. Quality Attitude
   b. Cooperation
   c. Communication
   d. Morale

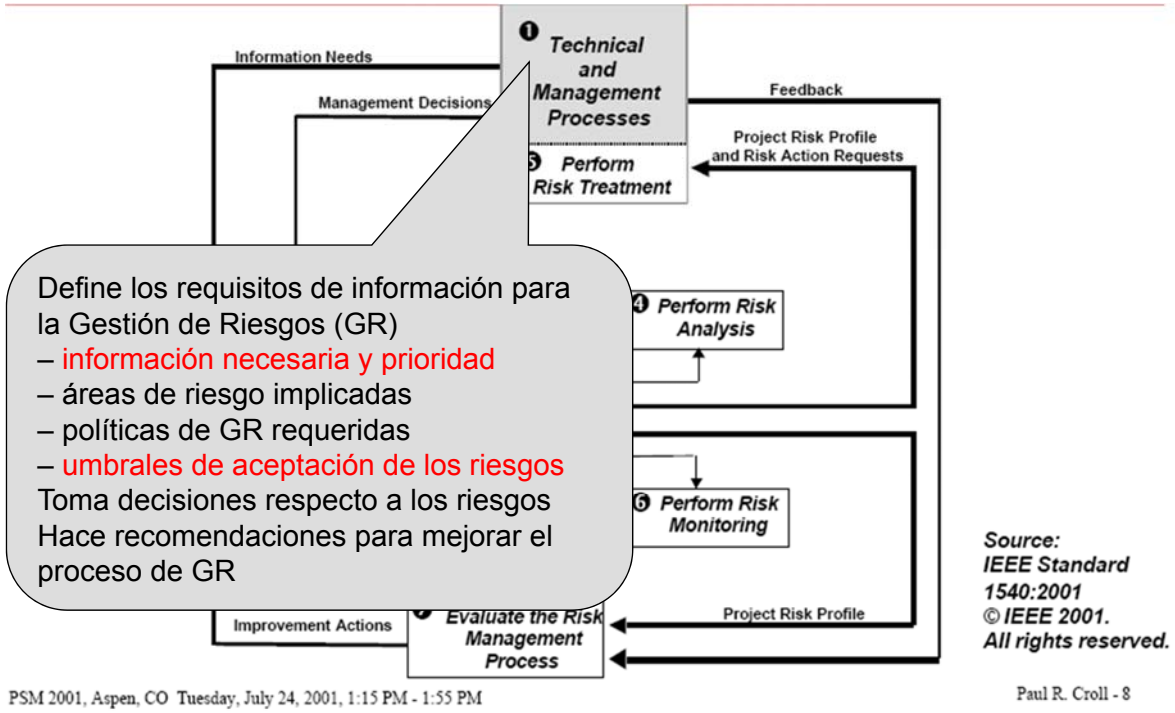
C. Constraints

1. Resources
   a. Schedule
   b. Staff
   c. Budget
   d. Facilities
   e. Tools
2. Policies
   a. Laws and Regulations
   b. Restrictions
   c. Contractual Constraints
3. Program Interfaces
   a. Customers/User Community
   b. Associate Agencies
   c. Contractors
   d. Senior Leadership
   e. Vendors
   f. Politics

http://www.sei.cmu.edu/publications/documents/05.reports/05tn036.html

PGP. Gestión de Riesgos Material adicional

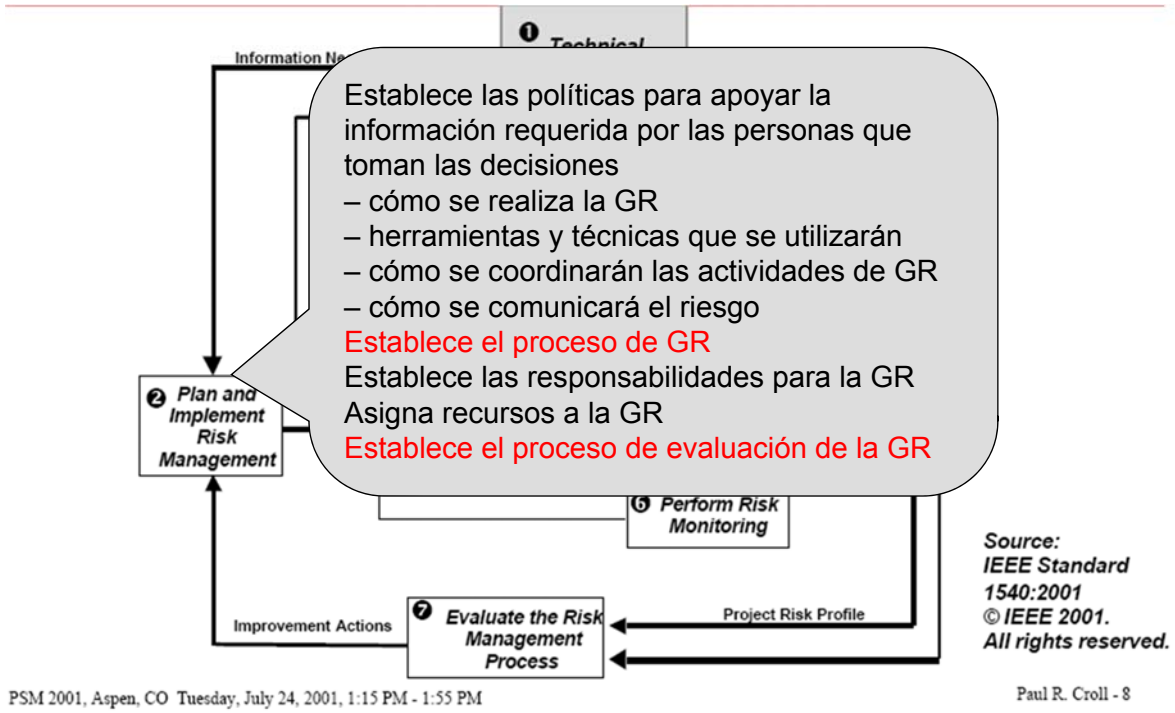




Define los requisitos de información para la Gestión de Riesgos (GR)
– información necesaria y prioridad
– áreas de riesgo implicadas
– políticas de GR requeridas
– umbrales de aceptación de los riesgos
Toma decisiones respecto a los riesgos
Hace recomendaciones para mejorar el proceso de GR

Foco en las medidas

PGP. Gestión de Riesgos Material adicional



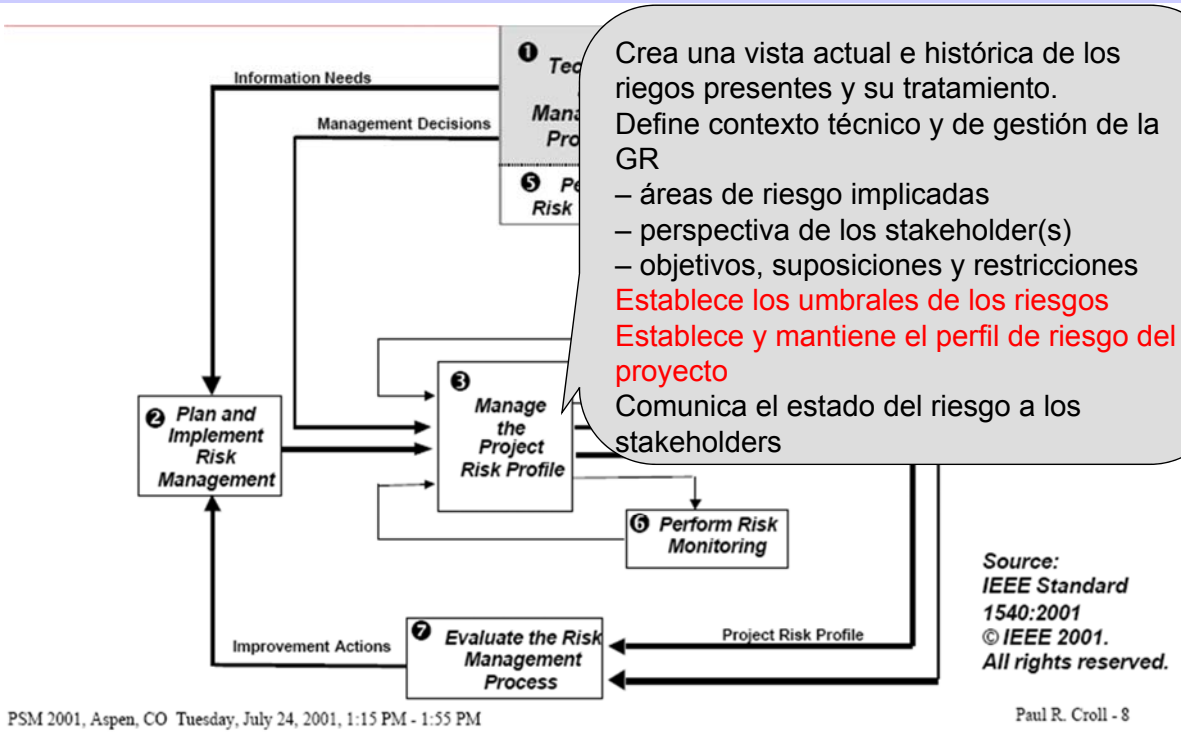
Establece las políticas para apoyar la información requerida por las personas que toman las decisiones
– cómo se realiza la GR
– herramientas y técnicas que se utilizarán
– cómo se coordinarán las actividades de GR
– cómo se comunicará el riesgo
Establece el proceso de GR
Establece las responsabilidades para la GR
Asigna recursos a la GR
Establece el proceso de evaluación de la GR

Foco en las medidas

Planif. y Gestión de Proyectos de Software 2015-2016

PGP. Gestión de Riesgos

Material adicional



Crea una vista actual e histórica de los riegos presentes y su tratamiento.
Define contexto técnico y de gestión de la GR
– áreas de riesgo implicadas
– perspectiva de los stakeholder(s)
– objetivos, suposiciones y restricciones
Establece los umbrales de los riesgos
Establece y mantiene el perfil de riesgo del proyecto
Comunica el estado del riesgo a los stakeholders

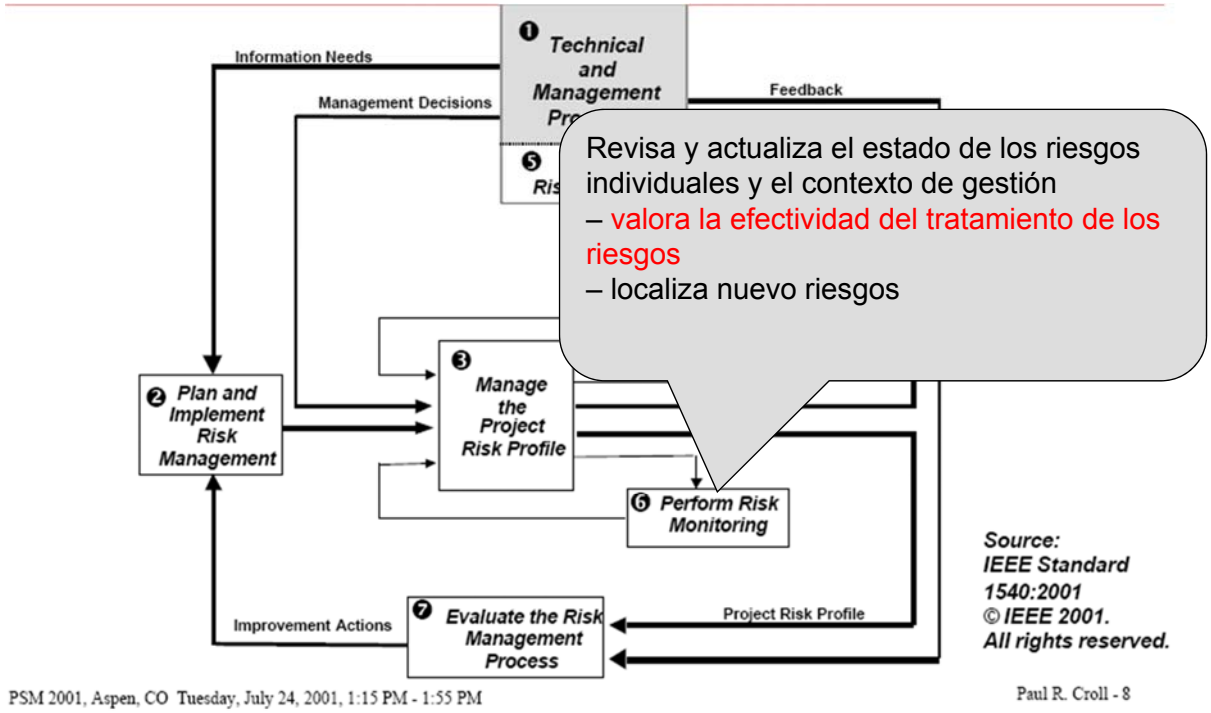
Foco en las medidas

PGP. Gestión de Riesgos

Material adicional

Identifica los riesgos definidos en el contexto de GR
Estima la probabilidad y las consecuencias del riesgo
Evalúa y prioriza los riesgos y sus interacciones frente a los umbrales
Recomienda el tratamiento del riesgo donde sea aplicable
Documenta las solicitudes de acción
– medidas de efectividad del tratamiento
– planes de contingencia

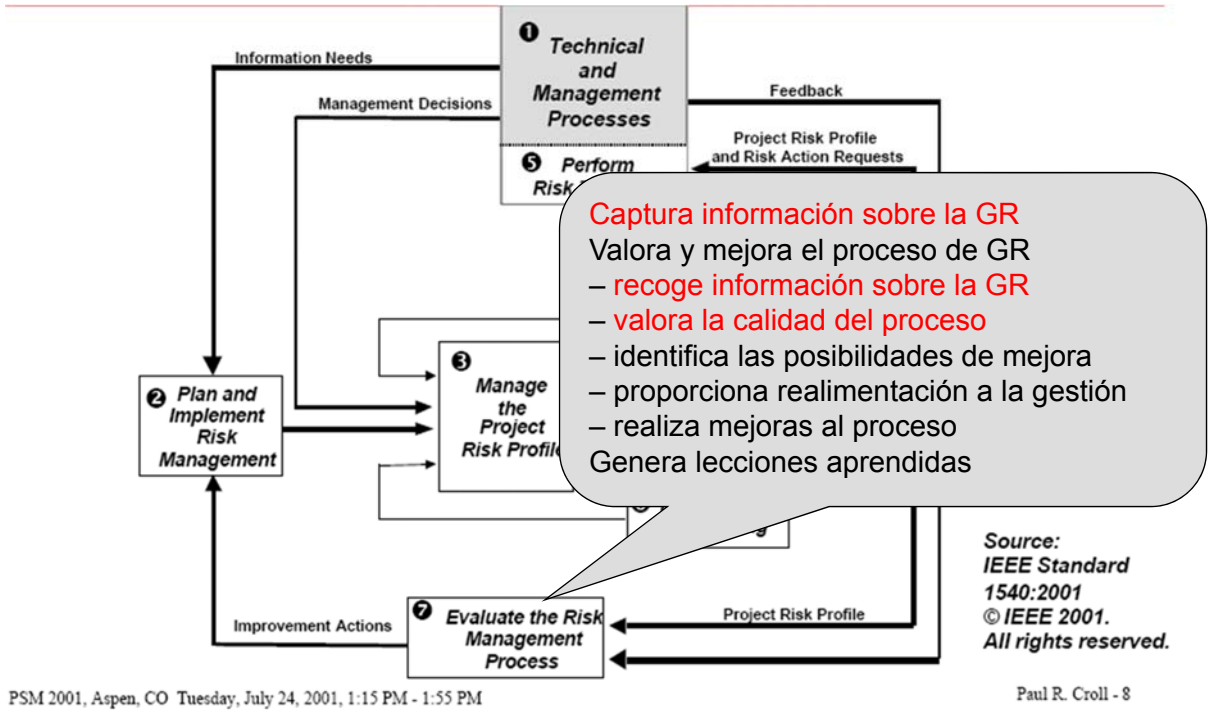
Foco en las medidas



Revisa y actualiza el estado de los riesgos individuales y el contexto de gestión
– valora la efectividad del tratamiento de los riesgos
– localiza nuevo riesgos

Foco en las medidas

PGP. Gestión de Riesgos Material adicional



Captura información sobre la GR
Valora y mejora el proceso de GR
– recoge información sobre la GR
– valora la calidad del proceso
– identifica las posibilidades de mejora
– proporciona realimentación a la gestión
– realiza mejoras al proceso
Genera lecciones aprendidas

Foco en las medidas