Proceso software y gestión

Tema 7. Introducción a la gestión de riesgos

ESCUELA TÉCNICA SUPERIOR DE
INGENIERÍA INFORMÁTICA
Departamento de Lenguajes y Sistemas Informáticos

Gestión de riesgos

1. Introducción.
2. Clasificación de los riesgos.
3. Aspectos generales de la gestión de riesgos.
4. Plan de gestión de riesgos.
5. Estrategia de respuestas.
6. Gestión de riesgos ágil.

Gestión de riesgos
Introducción

Gestión de riesgos → Contingencia o proximidad de un daño.

RAE

- Acción y efecto de gestionar. → Hacer diligencias conducentes al logro de un negocio o de un deseo cualquiera.
- Acción y efecto de administrar. → Ordenar, disponer, organizar, en especial la hacienda o los bienes

❑ Los riesgos normalmente son considerados como amenazas para el proyecto, y como tales deben ser minimizados.
❑ Deben buscarse oportunidades para transformar un evento desfavorable en algo positivo.

Otra definición: posibilidad de no cumplimiento de objetivos.

"Risk in itself is not bad; risk is essential to progress, and failure is often a key part of learning. But we must learn to balance **the possible negative consequences of risk against the potential benefits of its associated opportunity."**
[Van Scoy, Roger L. Software Development Risk: Opportunity, Not Problem. Software Engineering Institute, CMU/SEI-92-TR-30, ADA 258743, September 1992]

Gestión de riesgos

Introducción

Conceptos

- **Activo: c**ualquier recurso de SW, HW, datos, administrativo, físico, de personal, de comunicaciones…
- **Vulnerabilidad:** debilidad que puede ser 'activada' de forma accidental o intencionadamente. Es un factor de riesgo interno de un elemento expuesto a una amenaza de ser susceptible a sufrir un daño y de encontrar dificultades en recuperarse posteriormente.
- **Amenaza:** es la posibilidad de que se produzca una determinada vulnerabilidad de forma satisfactoria. Una fuente de amenazas no plantea un riesgo cuando no hay vulnerabilidades que puedan ser 'activadas'. Es una circunstancia o evento con la capacidad de causar daño a un sistema, entendiendo como daño una forma de destrucción, revelación o modificación de datos.
- **Impacto:** es la materialización de un riesgo; una medida del grado de daño o cambio sobre un activo.
- **Suposiciones:** son afirmaciones aceptadas como reales pero sin ningún tipo de prueba que las sustente.

Las suposiciones y los riesgos comparten dos características claves: incertidumbre (probabilidad) y consecuencia (impacto). Las suposiciones con baja probabilidad e impacto alto o muy alto se convierten en riesgo

Gestión de riesgos

Introducción

Riesgo de proyecto

❑ **Riesgo de un proyecto:** es un evento o condición incierta que, si se produce, tendrá un efecto positivo o negativo sobre al menos un objetivo del proyecto, como tiempo, coste, alcance o calidad.

❑ El riesgo del proyecto tiene su origen en la incertidumbre que está presente en todos los proyectos.

❑ El riesgo está compuesto de tres componentes esenciales: un evento definible, probabilidad de ocurrencia y consecuencia de la ocurrencia (impacto).

❑ Características de los riesgos:

- ➢ Son situacionales: varían drásticamente de una situación a otra.
- ➢ Pueden ser interdependientes: los riesgos a menudo están relacionados.
- ➢ Dependen de la magnitud: un determinado riesgo podría ser aceptado por ejemplo, si los beneficios y oportunidades potenciales son mayores.
- ➢ Están basados en valor: el nivel de tolerancia del riesgo varía en función de las personas y las organizaciones.
- ➢ Están basados en tiempo: el riesgo es un fenómeno del futuro causado por acciones actuales. El tiempo además afecta a la percepción del riesgo. Dependiendo de cuándo ocurra el riesgo, la percepción cambia.

Gestión de riesgos
Clasificación de los riesgos

❑**Según su conocimiento:**

➢**Riesgos conocidos:** son aquellos que han sido identificados y analizados, y es posible planificar las acciones a tomar al respecto.

➢**Riesgos desconocidos:** no pueden gestionarse de forma proactiva, y una respuesta prudente del equipo del proyecto puede ser asignar una contingencia general contra dichos riesgos.

❑**Según sus fuentes:**

➢**Riesgos internos:** tienen sus fuentes dentro de la organización, incluyendo el proyecto. Pueden ser controlados por el equipo de proyecto.

➢**Riesgos externos:** tienen sus fuentes fuera de la organización que lleva a cabo el proyecto.

❑**Diferentes tipos de riesgos:**

➢**Riesgos de planificación/cronograma**: tareas con larga duración sin hitos bien definidos, tareas con múltiples predecesores, tareas estimadas de forma no realista, tareas dependientes de organizaciones externas, …

➢**Riesgos de recursos**: pérdida de contribuidores críticos, trabajo con proveedores no fiables, tareas no asignadas a nadie, formación, …

➢**Riesgos financieros**: desajustes en presupuesto, cambios en el coste de material, …

➢**Riesgos de alcance y calidad**: nueva tecnología no probada (incertidumbre), cambios en los requisitos del cliente, herramientas no disponibles, …

➢**Riesgos generales**: mal entendimiento (requisitos, diseño…), seguridad, pérdida de patrocinio, …

➢**Riesgos del negocio:** de mercado (producto demasiado bueno), estratégico (producto que no encaja), de ventas (producto poco vendible), de presupuesto (producto fuera de presupuesto).

Gestión de riesgos

Aspectos generales de la gestión de riesgos

- Se lleva a cabo:
  - En la elaboración de una propuesta, cuando se planifica el proyecto.
  - A intervalos regulares durante la vida del proyecto: por ejemplo, como parte de los informes de estado del proyecto.
  - Cuando hay un cambio de alcance en el proyecto
- Es un proceso iterativo y recurrente a lo largo de toda la vida del proyecto.
- El propósito es minimizar la probabilidad y consecuencias de los riesgos negativos (o amenazas) y maximizar la probabilidad y consecuencias de los riesgos positivos (u oportunidades).
- Beneficios que se obtienen al llevar a cabo una buena gestión de los riesgos:
  - Se reduce los costes del proyecto.
  - Se mejora la satisfacción del cliente.
  - Se incrementa la capacidad y probabilidades de éxito.
  - Facilita el desarrollo del proyecto.
  - Disminuye drásticamente las sorpresas en los proyectos.
  - Ayuda a la empresa a conseguir los objetivos de negocio y proyecto evitando problemas que podrían causar pérdidas inesperadas y no planificadas.

Gestión de riesgos
Plan de gestión de riesgos (PGR)

- Describe la estrategia que se va a seguir en el proyecto, y cómo las actividades de gestión de riesgos van a ser organizadas y llevadas a cabo durante la vida del proyecto.
- Un plan de riesgos debe describir:
  - Una estrategia de gestión de riesgos.
  - Alcance del esfuerzo en gestión de riesgos .
  - Cómo se piensa llevar a cabo la identificación de riesgos.
  - Cómo se va a llevar a cabo el análisis de riesgos (cualitativo, cuantitativo, priorización).
  - Cómo se va a llevar a cabo el plan de respuesta (no debe contener los propios planes de respuesta ni tratar riesgos concretos).
  - Cómo se va a llevar a cabo la monitorización y control.
  - Presupuesto de gestión de riesgos.
  - Calendario de actividades de gestión de riesgos.
  - Roles y responsabilidades.

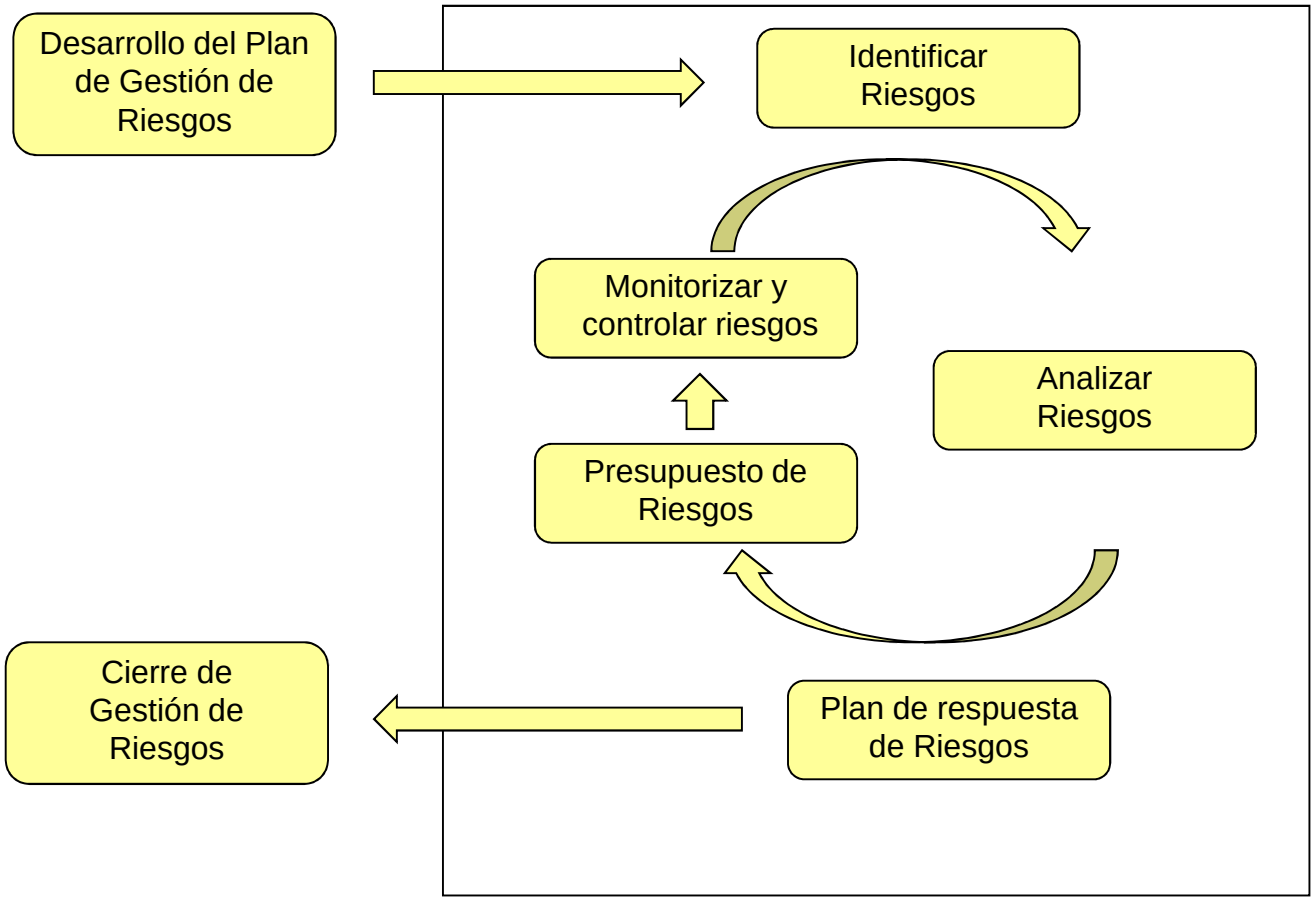
Gestión de riesgos
Plan de gestión de riesgos (PGR)

- Se crea durante la etapa de planificación del proyecto, aunque debe ser revisado a lo largo del mismo.
- Roles y responsabilidades:
  - Jefe de proyecto: genera y mantiene el PGR. Revisa y vigila proactivamente el estado de todos los riesgos del proyecto.
  - Responsables parciales del proyecto: realiza la gestión de los riesgos que le competen, actualiza al jefe de proyecto el registro de riesgos y escala situaciones excepcionales al jefe de proyecto.
  - Equipo de proyecto: ejecuta los planes de respuesta de los que sean responsables e informa al jefe de proyecto de posibles riesgos que detecten.
  - Los gerentes del proyecto: con la ayuda del cliente, deberán revisar los riesgos siempre que por su importancia así se requiera, y también llevarán a cabo aquellos planes de respuesta de los que sean responsables, informando al jefe de proyecto de posibles riesgos que detecten, y colaborando en el proceso de gestión de los mismos cuando se considere necesario.

Gestión de riesgos

Plan de gestión de riesgos (PGR)

Actividades



Ref. **GUÍA AVANZADA DE GESTIÓN DE RIESGOS. INTECO**

Gestión de riesgos

Plan de gestión de riesgos (PGR)

Actividades: desarrollo del PGR

- La planificación de la gestión de riesgos debe completarse en las fases tempranas de la planificación del proyecto.
- Los riesgos definidos y sus correspondientes soluciones, pueden tener un impacto significativo en el coste y planificación del proyecto.
- Tareas: Revisar entradas de riesgo, definir lista de actividades de gestión de riesgos, estimar el esfuerzo de los riesgos, asignar recursos a riesgos, definir herramientas que se van a utilizar, desarrollar planificación y presupuesto de riesgos.

Gestión de riesgos

Plan de gestión de riesgos (PGR)

Actividades: identificar riesgos

- Es un proceso iterativo a lo largo del proyecto.
- Tareas: identificar riesgos, considerar fuentes de riesgos internos y externos, categorizar los riesgos, identificación de disparadores, consolidación de riesgos en el registro de riesgos.
- Información del registro de riesgos:
  - Identificador del riesgo.
  - Estado del riesgo: identificado, evaluado, planificado, en proceso, cerrado, no ocurrido.
  - Descripción del riesgo, incluye: evento, momento en que ocurrió e impacto.

Gestión de riesgos

Plan de gestión de riesgos (PGR)

Actividades: analizar riesgos

❑ Evalúa los riesgos identificados para determinar la probabilidad de que ocurran, el impacto del riesgo, el impacto acumulativo de múltiples riesgos y la prioridad de cada riesgo.

❑ Tareas:

- ➢ Análisis cualitativo de riesgos: evaluación cualitativa del impacto (muy alto, alto, medio, bajo) y la probabilidad de ocurrencia de los riesgos (baja - <35%, media - <65%, alta - <85%, muy alta).
- ➢ Determinar la categoría y prioridad del riesgo (matriz probabilidad/impacto).
- ➢ Análisis cuantitativo de riesgos: evaluación matemática de la probabilidad de ocurrencia de cada riesgo y sus consecuencias, cálculo del valor esperado.

Valor esperado es un dato estadístico que proporciona significado acerca de las pérdidas o ganancias que se tendrían en caso de que el riesgo ocurriese.

Valor esperado = impacto * probabilidad; impacto: temporal o económica
probabilidad: 0,01 – 0,99

Otra alternativa: impacto total = impacto * probabilidad * factor

Gestión de riesgos

Plan de gestión de riesgos (PGR)

Actividades: planificar respuestas a los riesgos

- Proceso de desarrollar opciones y determinar acciones para mejorar las oportunidades y reducir las amenazas a los objetivos del proyecto.
- Aborda los riesgos en función de su prioridad, introduciendo recursos y actividades en el presupuesto, cronograma y plan de gestión del proyecto, según sea necesario.
- Se integra en la programación (agenda) y el presupuesto del proyecto para la implementación de las respuestas de riesgos.
- Deben ser congruentes con la importancia del riesgo, ser aplicadas a su debido tiempo, ser realistas dentro del contexto del proyecto, estar acordadas por todas las partes implicadas, y a cargo de una persona responsable.
- Tareas: identificar al propietario del riesgo; identificar varias estrategias de respuesta de riesgos para cada riesgo seleccionado, evaluar la efectividad de cada opción y seleccionar la mejor, teniendo en cuenta los posibles nuevos riesgos que se puedan originar; implementar los planes de contingencia para los riesgos identificados, incluyendo los costes (temporales, económicos y de personal) necesarios; determinar riesgos residuales (aquellos que subsisten después de aplicar un plan de respuestas a riesgos); determinar la reserva de riesgos del proyecto.

Gestión de riesgos

Plan de gestión de riesgos (PGR)

Actividades: planificar respuestas a los riesgos

Reserva de riesgos

- "Colchón" presupuestario del proyecto utilizado para reducir el impacto negativo de riesgos (o incrementar los positivos), respetando los márgenes establecidos para el proyecto.
- Incluye una **'reserva de contingencia' y una 'reserva de gestión' cuyo propietario es el jefe del proyecto, que siempre tiene que contar con la aprobación de la empresa.**
- Reserva de contingencia: suma del valor esperado para los riesgos con una estrategia de respuesta de 'aceptación' y el valor esperado para riesgos residuales.
- Reserva de gestión: depende de la incertidumbre de los proyectos (riesgos no conocidos).
- Para tratar los riesgos desconocidos del proyecto se añade una única entrada en el registro de riesgos para todo este conjunto de riesgos desconocidos tratándolos como otro riesgo más, dándoles una descripción, calculando su probabilidad e impacto y desarrollando una estrategia de respuesta de '**aceptación'.**

Gestión de riesgos

Plan de gestión de riesgos (PGR)

Actividades: controlar y monitorizar riesgos

- Es un proceso que consiste en controlar los disparadores de riesgos (si ha saltado alguno), gestionar los riesgos identificados, realizar seguimientos sobre los riesgos residuales, descubrir nuevos riesgos, ejecutar planes de respuesta de riesgos y evaluar la efectividad de las acciones de respuesta.
- Se realiza durante la vida del proyecto.
- La monitorización de riesgos determina si: los planes de respuesta de los riesgos han sido implementados de la forma adecuada, los planes de respuesta de los riesgos son efectivos o si es necesario el desarrollo de nuevos planes, las suposiciones de los riesgos continúan siendo válidas, un disparador del riesgo ha ocurrido, se han seguido las políticas de la empresa, han aparecido riesgos no identificados.
- El control de riesgos implica: elegir nuevas estrategias de respuesta, ejecutar planes de contingencia, tomar acciones correctivas o modificar planes del proyecto.
- Tareas: evaluar y actualizar los planes de respuestas; documentar cuándo y cómo se ha llevado a cabo el plan de gestión de riesgos**;** evaluar y actualizar el registro de riesgos.

Gestión de riesgos

Plan de gestión de riesgos (PGR)

Actividades: cierre de la gestión de riesgos

- Compartir lecciones aprendidas.
- Proporcionar entradas al cierre del proyecto.

Gestión de riesgos

Estrategia de respuestas

Estrategia para riesgos negativos o amenazas

- Evitar el riesgo: implica cambiar el plan de gestión del proyecto para eliminar la amenaza que representa un riesgo adverso. Se trata de eliminar un riesgo específico, normalmente eliminando la causa del mismo (cambiando una situación) de tal forma que el riesgo no pueda afectar al proyecto.
- Transferir el riesgo: requiere trasladar el impacto negativo de una amenaza y la responsabilidad del mismo a un tercero para su gestión. No se elimina el riesgo, pero se minimizan las consecuencias para la empresa. Transferir la responsabilidad del riesgo es más efectivo cuando se trata de exposición a riesgos financieros. Transferir el riesgo casi siempre supone el pago de una prima de riesgo a la parte que toma el riesgo.
- Mitigar el riesgo: implica reducir la probabilidad y/o el impacto de un evento de riesgo adverso a un umbral aceptable. Adoptar acciones tempranas para reducir la probabilidad de la ocurrencia de un riesgo y/o su impacto sobre el proyecto a menudo es más efectivo que tratar de reparar el daño después de que ha ocurrido el riesgo.

Gestión de riesgos

Estrategia de respuestas

Estrategia para riesgos positivos u oportunidades

- Explotar: se puede seleccionar esta estrategia para los riesgos con impactos positivos, cuando la organización desea asegurarse de que la oportunidad se haga realidad.
- Compartir: implica asignar la propiedad a un tercero que está mejor capacitado para capturar la oportunidad para beneficio del proyecto.
- Mejorar: modifica el "tamaño" de una oportunidad, aumentando la probabilidad y/o los impactos positivos, e identificando y maximizando las fuerzas impulsoras clave de estos riesgos de impacto positivo. Buscar facilitar o fortalecer la causa de la oportunidad, y dirigirse de forma proactiva a las condiciones que la disparan y reforzarlas, puede aumentar la probabilidad. También puede centrarse en las fuerzas impulsoras del impacto, buscando aumentar la susceptibilidad del proyecto a la oportunidad.

Gestión de riesgos

Gestión de riesgos ágil

- Utilizando las técnicas y prácticas de una gestión de proyectos ágil
  - Entregas frecuentes
  - Maximizar el valor
  - Potencialmente “shipable”
  - Historias de uso
  - Etc.
- Se pueden mitigar algunos riesgos inherentes al desarrollo
  - No aceptación por usuarios finales.
  - Falta de recursos
  - Planificación incorrecta
  - Incertidumbre tecnológica
  - Etc.

Pero aún siguen existiendo riesgos, por lo que es posible una gestión de dichos riesgos desde una perspectiva ágil.

Gestión de riesgos
Gestión de riesgos ágil

- Estrategias
  - Incorporar información de riesgos en las propias historias.
  - Gráfico Risk Burdown
  - Talleres What/Why
  - Gestión de logs de riesgos
  - .

Veremos algunos ejemplos de algunas técnicas.

Gestión de riesgos
Gestión de riesgos ágil

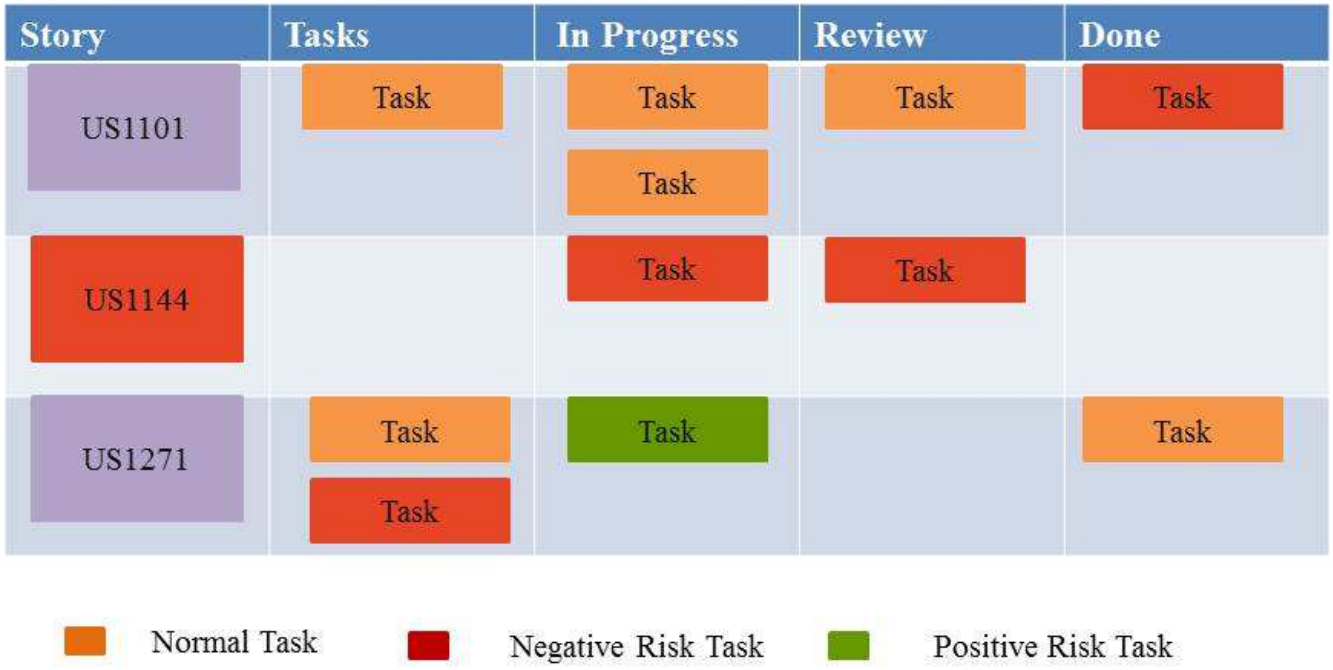
- Talleres What/Why
  - Mediante un brainstorming los miembros del equipo escriben “qué” podría suceder.
  - Una vez completada, se revisará la lista anterior, por ejemplo, eliminando elementos duplicados.
  - Preguntar por qué cada "qué" podría ocurrir. Un enfoque común aquí puede ser anotar cada "qué" como el título en una página en blanco separada.
  - A continuación, pasar las páginas invitando a todos en el equipo a contribuir con sus “por qué” para cada caso.
  - Hay que ser cuidadoso de no enmarcar negativamente la pregunta de "qué" (es decir, lo que podría salir mal) ya que todos en el equipo deben estar abiertos a la posibilidad de que haya oportunidades maduras para la explotación en el proyecto.

Ejemplo: La página "qué" titulada "sitio web no disponible" podría tener las siguientes razones “por qué”: "DNS podría no estar configurado correctamente" o "la configuración del servidor virtual podría diferir de la del servidor físico".

Gestión de riesgos

Gestión de riesgos ágil

Risk Modified Kanban Board

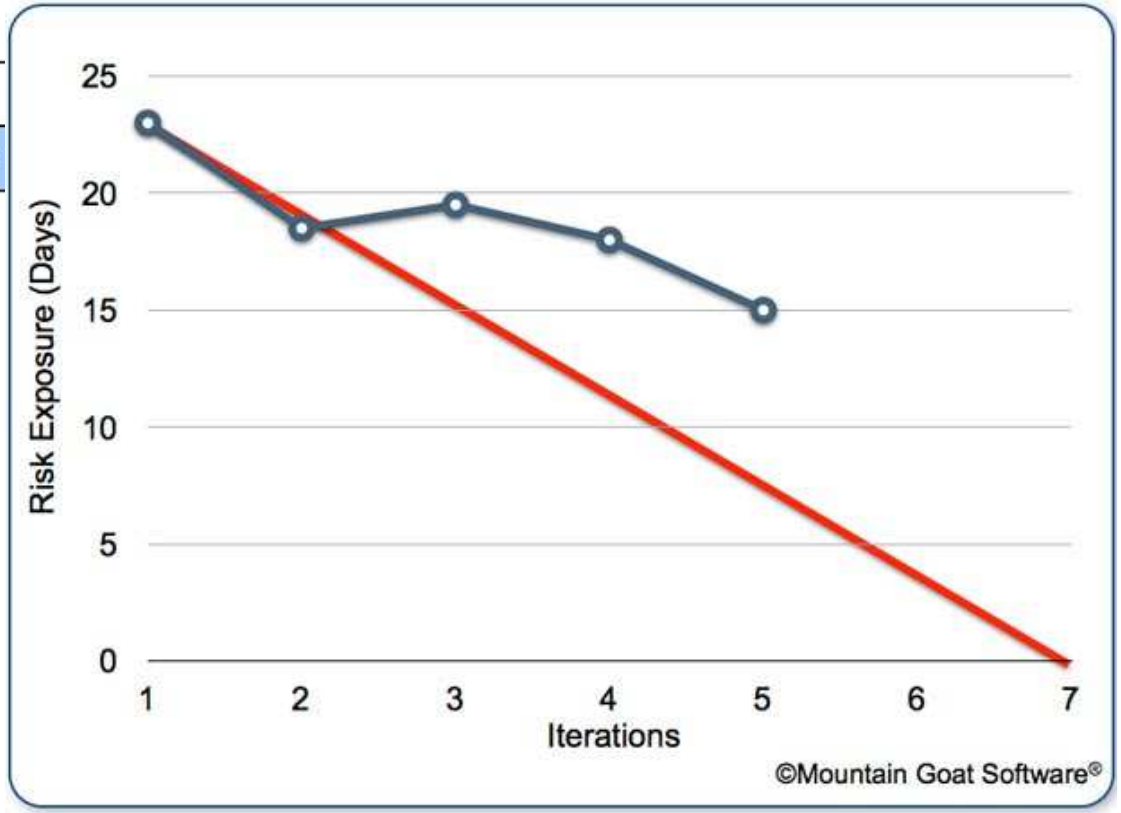


Gestión de riesgos

Gestión de riesgos ágil

Gráfico Risk Burdown

Risk	Probability of Risk	Size of Loss (Days)	Risk Exposure (Days)
Backup and restore may require the inclusion of additional third-party products.	20%	15	3
The lack of scientifically relevant sample data impacts Partner A's ability to validate the product.	35%	20	7
There won't be time for Partner A to provide feedback on the format of Analysis reports, which means they could find the reports unacceptable during validation.	10%	5	0.5
Partner A employees are not available to validate the new features until too late in the process, limiting our ability to make additional releases that address any issues they might uncover.	20%	5	1
There won't be time in the QA process to validate, equally, on all browsers on all operating systems.	40%	5	2
Partner A may require more end-user documentation than has been provided.	25%	20	5
		Exposure:	18.5



Gestión de riesgos

Bibliografía

1. Ingeniería del software. Un enfoque desde la guía SWEBOK. Salvador Sánchez, Miguel Ángel Sicilia, Daniel Rodríguez. IBERGACETA PUBLICACIONES, S.L. 2011
2. Ingeniería del software. Un enfoque práctico. Roger S. Pressman. McGraw-Hill, 2010.
3. Gestión del proceso software. Gonzalo Cuevas Agustín, et al. Centro de estudios Ramón Areces, S.A., 2003.
4. Guía avanzada de gestión de riesgos. INTECO, 2008.
5. Guía práctica de gestión de riesgos. INTECO, 2008.