

# Temario:

## Unidad IV: Gestión del riesgo.

- 4.1 .- Concepto de riesgo.
- 4.2 .- Clasificación de los riesgos.
- 4.3 .- Riesgos del software.
- 4.4 .- Identificación del riesgo.
- 4.5 .- Evaluaciones y proyecciones del riesgo.
- 4.6 .- Reducción, supervisión y gestión del riesgo.
- 4.7 .- Riesgos tecnológicos.
- 4.8 .- Riesgos y peligros para la humanidad.

# Unidad IV: Gestión del riesgo.

## 4.1 .- Concepto de riesgo.

El concepto de riesgo esta íntimamente relacionado al de incertidumbre, o falta de certeza, de algo pueda acontecer y generar una pérdida del mismo. Se conocen diversidad de conceptos sobre el riesgo, entre ellos se pueden señalar los siguientes:

- Riesgo es un conjunto de circunstancias que representan una posibilidad de pérdida.
- Riesgo es la incertidumbre de que ocurra una pérdida económica .
- Riesgo es la posibilidad de que por azar ocurra un hecho que produzca una necesidad patrimonial.
- Riesgo es la eventualidad del suceso cuya realización ha de obligar al asegurador a efectuar la prestación que le corresponde.

Al analizar cada una de estas definiciones se puede constatar que aunque son de diferentes autores, todas coinciden cuando expresan que el riesgo es la incertidumbre asociada con la posibilidad de que se produzca una pérdida económica, por lo cual el patrimonio del asegurado se vería afectado.

## 4.2 .- Clasificación de los riesgos.

Los riesgos se pueden clasificar en:

### **I.- Riesgos Físicos**

- Ruido.
- Presiones.
- Temperatura.
- Iluminación.
- Vibraciones
- Radiación Ionizante y no Ionizante.
- Temperaturas Extremas (Frío, Calor).
- Radiación Infrarroja y Ultravioleta.

## 4.2 .- Clasificación de los riesgos.

### 2.- Riesgos Químicos

- Polvos.
- Vapores.
- Líquidos.
- Disolventes.

### 3. Riesgos Biológicos

- Anquilostomiasis.
- Carbunco.
- La Alergia.
- Muermo.
- Tétanos.
- Espiroquetosis Icterohemorrágica.

## 4.2 .- Clasificación de los riesgos.

### **4. Riesgos Ergonómicos.**

- No existe una definición oficial de la ergonomía. Murrue la definió como "El estudio científico de las relaciones del hombre y su medio de trabajo". Su objetivo es diseñar el entorno de trabajo para que se adapte al hombre y así mejorar el confort en el puesto de trabajo.

### **5. Riesgos Psicosociales: Stress.**

- Los factores de riesgo psicosociales deben ser entendidos como toda condición que experimenta el hombre en cuanto se relaciona con su medio circundante y con la sociedad que le rodea, por lo tanto no se constituye en un riesgo sino hasta el momento en que se convierte en algo nocivo para el bienestar del individuo o cuando desequilibran su relación con el trabajo o con el entorno.

## 4.3 .- Riesgos del software.

**Los riesgos del proyecto** .- amenazan al plan del proyecto. Es decir, si los riesgos del proyecto se hacen realidad, es probable que la planificación temporal del proyecto se retrase y que los costos aumenten. Los riesgos del proyecto identifican los problemas potenciales de presupuesto, planificación temporal, personal (asignación y organización), recursos. cliente y requisitos y su impacto en un proyecto de software.

**Los riesgos técnicos** .- amenazan la calidad y la planificación temporal del software que hay que producir. Si un riesgo técnico se convierte en realidad, la implementación puede llegar a ser difícil o imposible. Los riesgos técnicos identifican problemas potenciales de diseño, implementación, de interfaz. verificación y de mantenimiento. Además. las ambigüedades de especificaciones, incertidumbre técnica, técnicas anticuadas y las "tecnologías punta" son también factores de riesgo. Los riesgos técnicos ocurren porque el problema es más difícil de resolver de lo que pensábamos.

## 4.3 .- Riesgos del software.

**Los riesgos del negocio** .- amenazan la viabilidad del software a construir. Los riesgos del negocio a menudo ponen en peligro el proyecto o el producto. Los candidatos para los cinco principales riesgos del negocio son:

1. Construir un producto o sistema excelente que no quiere nadie en realidad (riesgo de mercado),
2. Construir un producto que no encaja en la estrategia comercial general de la compañía (riesgo estratégico),
3. Construir un producto que el departamento de ventas no sabe cómo vender
4. Perder el apoyo de una gestión experta debido a cambios de enfoque o a cambios de personal (riesgo de dirección)
5. Perder presupuesto o personal asignado (riesgos de presupuesto).

## 4.4 .- Identificación del riesgo.

La identificación del riesgo es un intento sistemático para especificar las amenazas al plan del proyecto (estimaciones, planificación temporal, carga de recursos, etc.). Identificando los riesgos conocidos y predecibles, el gestor del proyecto da un paso adelante para evitarlos cuando sea posible y controlarlos cuando sea necesario.

Existen dos tipos diferenciados de riesgos para cada categoría: genéricos y específicos del producto. Los riesgos genéricos son una amenaza potencial para todos los proyectos de software. Los específicos de producto sólo los pueden identificar los que tienen una clara visión de la tecnología, el personal y el entorno específico del proyecto en cuestión. Para identificar los riesgos específicos del producto se examinan el plan del proyecto y la declaración del ámbito del software y se desarrolla una respuesta a la siguiente pregunta: ¿Qué características especiales de este producto pueden estar amenazadas por nuestro plan del proyecto'?"

## 4.4 .- Identificación del riesgo.

Tanto los riesgos genéricos como los específicos del producto se deberían identificar sistemáticamente. Tom Gilb tiene toda la razón cuando dice: "Si no atacas activamente a los riesgos. ellos te atacarán activamente a ti", Un método para identificar riesgos es crear una lista de comprobación de elementos de riesgo. La lista de comprobación se puede utilizar para identificar riesgos y se enfoca en un subconjunto de riesgos conocidos y predecibles en las siguientes subcategorías genéricas:

- **Tamaño del producto:** riesgos asociados con el tamaño general del software a construir o a modificar.
- **Impacto en el negocio:** riesgos asociados con las limitaciones impuestas por la gestión o por el mercado.

## 4.4 .- Identificación del riesgo.

- Características del cliente: riesgos asociados con la sofisticación del cliente y la habilidad del desarrollador para comunicarse con el cliente en los momentos oportunos.
- Definición del proceso: riesgos asociados con el grado de definición del proceso del software y su seguimiento por la organización de desarrollo.
- 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 punta que contiene el sistema.
- Tamaño y experiencia de la plantilla: riesgos asociados con la experiencia técnica y de proyectos de los ingenieros del software que van a realizar el trabajo.

## 4.5 .- Evaluaciones y proyecciones del riesgo.

### **Evaluación del riesgo**

En este punto del proceso de gestión del riesgo, se establece un conjunto de ternas de la forma:

$[r_i, l_i, x_i]$

donde  $r$  es el riesgo,  $l$  la probabilidad del riesgo y  $x$  el impacto del riesgo. Durante la evaluación del riesgo, se sigue examinando la exactitud de las estimaciones que fueron hechas durante la proyección del riesgo, se intenta dar prioridades a los riesgos que no se habían cubierto y se empieza a pensar las maneras de controlar y/o impedir los riesgos que sean más probables que aparezcan.

## 4.5 .- Evaluaciones y proyecciones del riesgo.

Para que sea útil la evaluación, se debe definir un nivel de referencia de riesgo. Para la mayoría de los proyectos, los componentes de riesgo como: - rendimiento, coste, soporte y planificación temporal- también representan niveles de referencia de riesgos. Es decir, hay un nivel para la degradación del rendimiento, exceso de coste, dificultades de soporte o retrasos de la planificación temporal (o cualquier combinación de los cuatro) que provoquen que se termine el proyecto. Si una combinación de riesgos crea problemas de manera que uno o más de estos niveles de referencia se excedan, se parará el trabajo. En el contexto del análisis de riesgos del software, un nivel de referencia de riesgo tiene un solo punto, denominado punto de referencia o punto de ruptura, en el que la decisión de seguir con el proyecto o dejarlo (los problemas son demasiado graves) son igualmente aceptables.

## 4.5 .- Evaluaciones y proyecciones del riesgo.

En realidad, el nivel de referencia puede raramente representarse como una línea nítida en el gráfico. En la mayoría de los casos es una región en la que hay áreas de incertidumbre (ej.: intentar predecir una decisión de gestión basándose en la combinación de valores de referencia es a menudo imposible).

Por tanto, durante la evaluación del riesgo, se realizan los siguientes pasos:

1. Definir los niveles de referencia de riesgo para el proyecto.
2. Intentar desarrollar una relación entre cada  $[r_i, l_i, x_i]$  y cada uno de los niveles de referencia.
3. Predecir el conjunto de puntos de referencia que definan la región de abandono.
4. Intentar predecir como afectarán las combinaciones compuestas de riesgos a un nivel de referencia.

## 4.5 .- Evaluaciones y proyecciones del riesgo.

### **Proyección del riesgo**

La proyección del riesgo, también denominada estimación del riesgo, intenta medir cada riesgo de dos maneras -la probabilidad de que el riesgo sea real y las consecuencias de los problemas asociados con el riesgo, si ocurriera. El jefe del proyecto, junto con otros gestores y personal técnico, realiza cuatro actividades de proyección del riesgo: (1) establecer una escala que refleje la probabilidad percibida del riesgo; (2) definir las consecuencias del riesgo; (3) estimar el impacto del riesgo en el proyecto y en el producto; y (4) apuntar la exactitud general de la proyección del riesgo de manera que no haya confusiones.

Una tabla de riesgo le proporciona al jefe del proyecto una sencilla técnica para la proyección del riesgo'. En la Figura se ilustra una tabla de riesgo como ejemplo.

## 4.5 .- Evaluaciones y proyecciones del riesgo.

Riesgos	Categoría	Probabilidad	Impacto	RSGR
La estimación del tamaño puede ser significativamente baja	PS	60 %	2	
Mayor número de usuarios de los previstos	PS	30 %	3	
Menos reutilización de la prevista	PS	70 %	2	
Los usuarios finales se resisten al sistema	BU	40 %	3	
La fecha de entrega estará muy ajustada	BU	50 %	2	
Se perderán los presupuestos	CU	40 %	1	
El cliente cambiará los requisitos	PS	80 %	2	
La tecnología no alcanzará las expectativas	TE	30 %	1	
Falta de formación en las herramientas	DE	80 %	3	
Personal sin experiencia	ST	30 %	2	
Habrà muchos cambios de personal	ST	60 %	2	
•				
•				
•				

Valores de impacto:  
1 - catastrófico  
2 - crítica  
3 - marginal  
4 - despreciable

Un equipo de proyecto empieza por listar todos los riesgos (no importa lo remotos que sean) en la primera columna de la tabla. Se puede hacer con la ayuda de la lista de comprobación de elementos de riesgo.

## 4.5 .- Evaluaciones y proyecciones del riesgo.

Cada riesgo es categorizado en la segunda columna (p. ej.: **PS** implica un riesgo del tamaño del proyecto. **BU** implica un riesgo de negocio). La probabilidad de aparición de cada riesgo se introduce en la siguiente columna de la tabla. El valor de la probabilidad de cada riesgo puede estimarse por cada miembro del equipo individualmente. De los valores individuales se obtiene la media para obtener una probabilidad consensuada. A continuación se valora el impacto de cada riesgo.

Cada componente de riesgo se valora usando la caracterización presentada en la primera figura, y se determina una categoría de impacto. Las categorías para cada uno de los cuatro componentes de riesgo - rendimiento, soporte, coste y planificación temporal- son promediados para determinar un valor general de impacto.

## 4.5 .- Evaluaciones y proyecciones del riesgo.

Una vez que se han completado las cuatro primeras columnas de la tabla de riesgo, la tabla es ordenada por probabilidad y por impacto. Los riesgos de alta probabilidad y de alto impacto pasan a lo alto de la tabla, y los riesgos de baja probabilidad caen a la parte de abajo. Esto consigue una priorización del riesgo de primer orden.

El jefe del proyecto estudia la tabla ordenada resultante y define una línea de corte. La línea de corte (dibujada horizontalmente) implica que sólo a los riesgos que quedan por encima de la línea se les prestará atención en adelante. Los riesgos que caen por debajo de la línea son reevaluados para conseguir una priorización de segundo orden.

## 4.6 .- Reducción, supervisión y gestión del riesgo.

Todas las actividades de análisis de riesgo tienen un objetivo único: ayudar al equipo del proyecto a desarrollar una estrategia para tratar los riesgos. Una estrategia eficaz debe considerar tres aspectos:

- Evitar el riesgo
- Supervisar el riesgo
- Gestión del riesgo y planes de contingencia

Si un equipo de software adopta un enfoque proactivo frente al riesgo, evitarlo es siempre la mejor estrategia. Esto se consigue desarrollando un plan de reducción del riesgo. Por ejemplo, asuma que se ha detectado mucha movilidad de la plantilla como un riesgo del proyecto,  $n$ . Basándose en casos anteriores y en la intuición de gestión, la probabilidad,  $li$ , de mucha movilidad se estima en un 0.70 (70 por ciento, bastante alto) y el impacto, si está previsto que tenga un impacto crítico en el coste y planificación temporal del proyecto.

## 4.6 .- Reducción, supervisión y gestión del riesgo.

Para reducir el riesgo, la gestión del proyecto debe desarrollar una estrategia para reducir la movilidad. Entre los pasos que se pueden tomar están estos:

- Reunirse con la plantilla actual y determinar las causas de la movilidad (por ej.: malas condiciones de trabajo, salarios bajos, mercado laboral competitivo).
- Actuar para reducir esas causas que estén al alcance del control de gestión antes de que comience el proyecto.
- Una vez que comienza el proyecto, asuma que habrá movilidad y desarrolle técnicas para asegurarse la continuidad cuando se vaya la gente.
- Organice los equipos del proyecto de manera que la información sobre cada actividad de desarrollo esté ampliamente dispersa.
- Defina estándares de documentación y establezca mecanismos para asegurarse de que los documentos se cumplan puntualmente.

## 4.6 .- Reducción, supervisión y gestión del riesgo.

- Convoque reuniones de revisión de todo el trabajo de manera que más de una persona a la vez esté familiarizada con el trabajo.
- Defina un miembro de la plantilla como reserva para cada técnico crítico.

A medida que progresa el proyecto comienzan las actividades de supervisión del riesgo. El jefe del proyecto supervisa factores que pueden proporcionar una indicación de si el riesgo se está haciendo más o menos probable. En el caso de gran movilidad del personal, se pueden supervisar los siguientes factores:

- Actitud general de los miembros del equipo basándose en las presiones del proyecto.
- El grado de compenetración del equipo.
- Relaciones interpersonales entre los miembros del equipo.
- La disponibilidad de empleo dentro y fuera de la compañía.

## 4.6 .- Reducción, supervisión y gestión del riesgo.

La gestión del riesgo y los planes de contingencia asumen que los esfuerzos de reducción han fracasado y que el riesgo se ha convertido en una realidad. Continuando con el ejemplo, suponga que el proyecto va muy retrasado y un número de personas anuncia que se va. Si se ha seguido la estrategia de reducción, tendremos reservas, la información está documentada y el conocimiento del proyecto se ha dispersado por todo el equipo. Además, el jefe del proyecto puede temporalmente volver a reasignar los recursos (y reajustar la planificación temporal del proyecto) desde las funciones que tienen todo su personal, permitiendo a los recién llegados que deben unirse al equipo que vayan "cogiendo el ritmo". A los individuos que se van se les pide que dejen lo que estén haciendo y dediquen sus últimas semanas a "transferir sus conocimientos". Esto podría incluir la adquisición de conocimientos por medio de vídeos, el desarrollo de "documentos con comentarios" y/o reuniones con otros miembros del equipo que permanezcan en el proyecto.

## 4.6 .- Reducción, supervisión y gestión del riesgo.

Es importante advertir que los pasos RSGR (reducción, supervisión y gestión de riesgos) provocan aumentos del coste del proyecto. Por ejemplo, emplear tiempo en conseguir una reserva de cada técnico crítico cuesta dinero. Parte de la gestión de riesgos es evaluar cuando los beneficios obtenidos por los pasos RSGR superan los costes asociados con su implementación. En esencia, quien planifique el proyecto realiza el clásico análisis coste/beneficio. Si los procedimientos para evitar el riesgo de gran movilidad aumentan el coste y duración del proyecto aproximadamente en un 15 por ciento, pero el factor coste principal es la copia de seguridad (backup), el gestor puede decidir no implementar este paso. Por otra parte si los pasos para evitar el riesgo llevan a una proyección de un aumento de costes del 5 por ciento y de la duración en un 3 por ciento, la gestión probablemente lo haga.

## 4.6 .- Reducción, supervisión y gestión del riesgo.

Para un proyecto grande se pueden identificar hasta unos 40 riesgos. Si se pueden identificar entre tres y siete pasos de gestión de riesgo para cada uno, la gestión del riesgo puede convertirse en un proyecto por sí misma. Por este motivo, adaptamos la regla de Pareto 80-20 al riesgo del software. La experiencia dice que el 80 por ciento del riesgo total de un proyecto (p. ej.: el 80 por ciento del potencial de fracaso del proyecto) se debe solamente al 20 por ciento de los riesgos identificados. El trabajo realizado durante procesos de análisis de riesgo anteriores ayudará al jefe de proyecto a determinar qué riesgos pertenecen a ese 20 por ciento. Por este motivo, algunos de los riesgos identificados, valorados y previstos pueden no pasar por el plan RSGR -no pertenecen al 20 por ciento crítico (los riesgos con la mayor prioridad del proyecto).

## 4.7 .- Riesgos tecnológicos.

Alcanzar los límites de la tecnología es un reto excitante. Es el sueño de casi todos los técnicos, porque fuerza al profesional a emplear su talento al máximo. Pero también es muy arriesgado. La ley de Murphy parece mantener su imperio en esta parte del universo del desarrollo, haciendo extremadamente difícil predecir los riesgos, y mucho menos hacer ningún plan sobre ellos. La siguiente lista de comprobación de elementos de riesgo identifica riesgos genéricos asociados con la técnica a construir.

- ¿Es nueva para su organización la tecnología a construir?
- ¿Demandan los requisitos del cliente la creación de nuevos algoritmos o tecnología de entrada o salida?
- ¿El software interactúa con hardware nuevo o no probado?

## 4.7 .- Riesgos tecnológicos.

- ¿Interactúa el software a construir con productos software suministrados por el vendedor que no se hayan probado?
- ¿Interactúa el software a construir con un sistema de base de datos cuyo funcionamiento y rendimiento no se han comprobado en esta área de aplicación?
- ¿Demandan los requisitos del producto una interfaz de usuario especial?
- ¿Demandan los requisitos del producto la creación de componentes de programación distintos de; los que su organización haya desarrollado hasta ahora?
- ¿Demandan los requisitos el empleo de nuevos métodos de análisis, diseño o pruebas?

## 4.7 .- Riesgos tecnológicos.

- ¿Demandan los requisitos el empleo de métodos de desarrollo del software no convencionales, tales como los métodos formales, enfoques basados ... en IA y redes neuronales?
- ¿Imponen excesivas restricciones de rendimiento los requisitos del producto?
- ¿No está seguro el cliente de que la funcionalidad pedida sea factible?

Si la respuesta a alguna de estas preguntas es afirmativa, se debería realizar una investigación más profunda para valorar el riesgo potencial.

## 4.7 .- Riesgos y peligros para la seguridad.

El riesgo no se limita al proyecto de software solamente. Pueden aparecer riesgos después de haber desarrollado con éxito el software y de haberlo entregado al cliente. Estos riesgos están típicamente asociados con las consecuencias del fallo del software una vez en el mercado.

Aunque la probabilidad de fallo de un sistema de alta ingeniería es pequeña, un defecto no detectado en un sistema de control y supervisión basados en ordenador podría provocar unas pérdidas económicas enormes, o peor, daños físicos significativos o pérdida de vidas humanas. Pero el coste y beneficios funcionales del control y supervisión basados en computadora a menudo superan al riesgo. Hoy en día, se emplean regularmente hardware y software para el control de sistemas de seguridad crítica.

## 4.7 .- Riesgos y peligros para la seguridad.

Cuando se emplea software como parte del sistema de control, la complejidad puede aumentar del orden de una magnitud o más. Sutiles defectos de diseño inducidos por error humano -algo que puede descubrirse y eliminarse con controles convencionales basados en hardware- se convierten en mucho más difíciles de descubrir cuando se emplea software.

La seguridad del software y el análisis del peligro son actividades para garantizar la calidad del software que se centra en la identificación y evaluación de peligros potenciales que pueden impactar al software negativamente y provocar que falle el sistema entero. Si se pueden identificar los peligros al principio del proceso de ingeniería del software, se pueden especificar características de diseño software que eliminen o controlen esos peligros potenciales.

# Cybergrafia.

<http://www.worldlingo.com>

<http://www.monografias.com>

<http://www.mitecnologico.com>

<http://sistemas.itlp.edu.mx>

<http://www.qualitrain.com.mx>

<http://www.eumed.net>

<http://www.calidaddelsoftware.com>

<http://es.wikipedia.org>

<http://www.um.es>