Capítulo 5. IAGP 2005/06. Gestión de riesgos en ingeniería del software

Actualizado 2006/06/17

5.1 Introducción

En su libro sobre análisis y gestión del riesgo, Robert Charette presenta la siguiente definición de riesgo:

> En primer lugar, el riesgo afecta a los futuros acontecimientos. El hoy y el ayer están más allá de lo que nos pueda preocupar, pues ya estamos cosechando lo que sembramos previamente con nuestras acciones del pasado. La pregunta es, podemos por tanto, cambiando nuestras acciones actuales, crear una oportunidad para una situación diferente y, con suerte, mejor para nosotros en el futuro. Esto significa, en segundo lugar, que el riesgo implica cambio, que puede venir dado por cambios de opinión, de acciones, de lugares... En tercer lugar, el riesgo implica elección y la incertidumbre que entraña la elección. Por tanto, el riesgo, como la muerte, es una de las pocas cosas inevitables de la vida.

Cuando se considera el riesgo en el contexto de la ingeniería

del software, los tres pilares conceptuales de Charette se hacen continuamente evidentes. El futuro es lo que nos preocupa, ¿qué riesgos podrían hacer que nuestro proyecto fracasara? El cambio es nuestra preocupación ¿cómo afectarán los cambios en los requisitos del cliente, en las tecnologías de desarrollo, en los ordenadores a las que van dirigidas, el proyecto y todas las entidades relacionadas con él, al cumplimiento de la planificación temporal y al éxito en general? Para terminar, nos enfrentamos con elecciones ¿qué métodos y herramientas deberíamos emplear, cuánta gente debería estar implicada, qué importancia hay que darle a la calidad?

Peter Drucker dijo una vez: "Mientras que es inútil intentar eliminar el riesgo y cuestionable el poder minimizarlo, es esencial que los riesgos que se tomen sean los riesgos adecuados". Antes de poder identificar los "riesgos adecuados" que se pueden tomar en un proyecto de software, es importante poder identificar todos los riesgos que sean obvios a jefes de proyectos y profesionales del software.

Estrategias de riesgo reactivas y proactivas

Las estrategias de riesgo reactivas se han denominado humorísticamente "Escuela de gestión del riesgo de Indiana Jones". En las películas, Indiana Jones, cuando se enfrentaba a una dificultad insuperable, siempre decía "¡No te preocupes, pensaré en algo!". Nunca se preocupaba de los problemas hasta que ocurrían, entonces reaccionaba como un héroe.

Como el jefe del proyecto de software normalmente no es Indiana Jones y los miembros de su equipo no son sus fiables colaboradores, la mayoría de los equipos de software confían solamente en las estrategias de riesgo reactivas. En el mejor de los casos, la estrategia reactiva supervisa el proyecto en previsión de posibles riesgos. Los recursos se ponen aparte, en caso de que pudieran convertirse en problemas reales.

Pero lo más frecuente es que el equipo de software no haga nada respecto a los riesgos hasta que algo va mal. Después el equipo vuela para corregir el problema rápidamente. éste es el método denominado a menudo "de bomberos". Cuando falla, "la gestión de crisis" entra en acción y el proyecto se encuentra en peligro real.

Una estrategia considerablemente más inteligente para el control del riesgo es ser proactivo. La estrategia proactiva empieza mucho antes de que comiencen los trabajos técnicos. Se identifican los riesgos potenciales, se valoran su probabilidad y su impacto y se establece una prioridad según su importancia. Después el equipo de software establece un plan para controlar el riesgo. El primer objetivo es evitar el riesgo, poco común no se pueden evitar todos los riesgos. el equipo trabaja para desarrollar un plan de contingencia que le permita responder de una manera eficaz y controlada. A lo largo de lo que queda de este capitulo, estudiamos la estrategia proactiva para el control de riesgos.

5.2 Riesgos del software

Se han producido amplios debates sobre la definición adecuada para riesgo de software, y hay acuerdo común en que el riesgo siempre implica dos características:

- Incertidumbre: El acontecimiento que caracteriza al riesgo puede o no puede ocurrir; por ejemplo, no hay riesgos de un 100 por ciento de probabilidad.

- Pérdida: Si el riesgo se convierte en una realidad, ocurrirán consecuencias no deseadas o pérdidas.

Cuando se analizan los riesgos es importante cuantificar el nivel de incertidumbre y el grado de pérdidas asociado con cada riesgo. Para hacerlo, se consideran diferentes categorías

de riesgos.

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.

Los riesgos del negocio amenazan la viabilidad del software a construir Los riesgos del negocio a menudo ponen en peligro ei 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 ei 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).

Es extremadamente importante recalcar que no siempre funciona una categorización tan sencilla. Algunos riesgos son simplemente imposibles de predecir. Otra categorización general de los riesgos ha sido propuesta por Charette. Los riesgos conocidos son todos aquellos que se pueden descubrir después de una cuidadosa evaluación del plan del proyecto. del entorno técnico y comercial en el que se desarrolla el proyecto y otras fuentes de información fiables (p. ej.: fechas de entrega poco realistas. falta de especificación de requisitos o de ámbito del software. o un entorno pobre de desarrollo), los riesgos predecibles se extrapolan de la experiencia en proyectos anteriores (ej.: cambio de personal, mala comunicación con el cliente. disminución del esfuerzo del personal a medida que atienden peticiones de mantenimiento). Pueden ocurrir pero son extremadamente difíciles de identificar por adelantado.

5.3 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 presentada en el apartado anterior: 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'?"

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.
- 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.

La lista de comprobación de elementos de riesgo puede organizarse de diferentes maneras. Se pueden responder a

cuestiones relevantes de cada uno de los temas apuntados anteriormente para cada proyecto de software. Las respuestas a estas preguntas permiten al planificador del proyecto estimar el impacto del riesgo. Un formato diferente de lista de comprobación de elementos de riesgo contiene simplemente las características relevantes para cada subcategoría genérica. Finalmente, se lista un conjunto de "componentes y controladores del riesgo" junto con sus probabilidades de aparición. Los controladores del rendimiento, el soporte, el coste y la planificación temporal del proyecto se estudian como respuesta a preguntas posteriores.

5.3.1 Riesgos del tamaño del producto

Pocos gestores experimentados discutirían la siguiente frase: El riesgo del proyecto es directamente proporcional al tamaño del producto. La siguiente lista de comprobación de elementos de riesgo identifica riesgos genéricos asociados con el tamaño del producto (software):

- ¿Tamaño estimado del producto en LDC o FP?
- ¿Grado de seguridad en la estimación del tamaño?
- ¿Tamaño estimado del producto en número de programas, archivos y transacciones?
- ¿Porcentaje de desviación en el tamaño del producto respecto a la medida de productos anteriores?
- ¿Tamaño de la base de datos creada o empleada por el producto?
- ¿Número de usuarios del producto?
- ¿Número de cambios previstos a los requisitos del producto? ¿Antes de la entrega? ¿ Después de la entrega?
- ¿Cantidad de software reutilizado?

En cada caso, la información del producto a desarrollar debe compararse con la experiencia anterior. Si ocurre una gran

desviación del porcentaje o si las magnitudes son similares. pero si los resultados anteriores fueron poco satisfactorios, el riesgo es grande.

5.3.2 Riesgos del impacto en el negocio

Un gestor de ingeniería (algo magufo) de una gran compañía de software colocó una placa con el texto: "¡dios me concedió el cerebro para ser un buen jefe de proyectos y el sentido común para correr como un diablo cuando marketing establece las fechas límite del proyecto!". Al departamento de marketing le guían las consideraciones del negocio, y éstas entran a veces en conflicto directo con las realidades técnicas. La siguiente lista de comprobación de elementos de riesgo identifica riesgos genéricos asociados con el impacto en el negocio:

- ¿Efecto de este producto en los ingresos de la compañía?
- ¿Viabilidad de este producto para los gestores expertos?
- ¿Es razonable la fecha límite de entrega?
- ¿Número de clientes que usarán este producto y la consistencia de sus necesidades relativas al producto?
- ¿Número de otros productos/sistemas con los que este producto debe tener interoperatividad?
- ¿Sofisticación del usuario final?
- ¿Cantidad y calidad de la documentación del producto que debe ser elaborada y entregada al cliente?
- ¿Limitaciones gubernamentales en la construcción del producto?
- ¿Costos asociados por un retraso en la entrega?
- ¿Costos asociados con un producto defectuoso?

Cada respuesta para el producto a desarrollar debe

compararse con la experiencia anterior. Si se obtiene una gran desviación del porcentaje o si las magnitudes son similares, pero los resultados anteriores fueron poco satisfactorios, el riesgo es grande.

5.3.3 Riesgos relacionados con el cliente

No todos los clientes son iguales. Pressman y Herron tratan este aspecto cuando dicen: Los clientes tienen diferentes necesidades. Algunos saben lo que quieren; otros saben lo que no quieren. Algunos están deseando saber todos los detalles, mientras que otros se quedan satisfechos con vagas promesas.

Los clientes tienen diferentes personalidades. Algunos disfrutan siendo clientes (la tensión, la negociación, las recompensas psicológicas de un buen producto).

Otros preferirían no ser clientes en absoluto. Algunos aceptarían felizmente cualquier cosa que se les entregara y le sacarían el mejor provecho a un producto pobre. Otros se quejarán amargamente cuando les falte calidad; algunos darán las gracias cuando la calidad es buena; unos pocos se quejarán por todo.

Los clientes también tienen varios tipos de asociaciones con sus suministradores. Algunos conocen bien a sus proveedores y sus productos; otros no se han visto nunca las caras y se comunican siempre mediante correspondencia escrita y algunas llamadas telefónicas breves.

Los clientes se contradicen a menudo. Quieren todo para ayer y gratis. A menudo, el producto se ve cogido entre las propias contraindicaciones del cliente.

Un "mal" cliente puede tener un profundo impacto en la habilidad del equipo de software para completar el proyecto a tiempo y dentro de presupuesto. Un mal cliente representa

una amenaza significativa al plan del proyecto y un sustancial riesgo para el jefe del proyecto. La siguiente lista de comprobación de elementos de riesgo identifica riesgos genéricos asociados con diferentes clientes:

- ¿Ha trabajado con el cliente anteriormente?
- ¿Tiene el cliente una idea formal de lo que se requiere? ¿Se ha molestado en escribirlo?
- ¿Aceptará el cliente gastar su tiempo en reuniones formales de requisitos para identificar el ámbito del proyecto?
- ¿Está dispuesto el cliente a establecer una comunicación fluida con el desarrolador?
- ¿Está dispuesto el cliente a participar en las revisiones?
- ¿Es sofisticado técnicamente el área del producto?
- ¿Está dispuesto el cliente a dejar a su personal hacer el trabajo? Es decir, ¿ resistirá la tentación de mirar por encima del hombro durante el trabajo técnico?
- ¿Entiende el cliente el proceso del software?

Si la respuesta a alguna de estas preguntas es "no", se debería hacer una investigación más profunda para valorar el potencial de riesgo.

5.3.4 Riesgos del proceso

Si el proceso del software no está bien definido; si el análisis, diseño y pruebas se realizan sobre la marcha; si la calidad es un concepto que todo el mundo estima importante, pero por la que nadie actúa de manera tangible para alcanzarla, entonces el proyecto está en peligro. Las siguientes preguntas se han extraído sobre la evaluación de la ingeniería del software desarrollado por R. S. Pressman & Associates. Inc. Las preguntas se han adaptado del cuestionario de evaluación del proceso del software del Instituto de Ingeniería del Software (IIS).

Aspectos del proceso

• ¿Apoyan sus gestores senior unas normas escritas que hagan hincapié en la importancia de un proceso estándar para el desarrollo del software?

• ¿Ha desarrollado su organización una descripción escrita del proceso del software a emplear en este proyecto?

• ¿Están de acuerdo los miembros del personal con el proceso del software tal y como está documentado y estan dispuestos a usarlo?

• ¿Se emplea este proceso del software para otros proyectos?

• ¿Ha desarrollado o adquirido su organización cursos de formación de ingeniería del software para jefes de proyecto y personal técnico?

• ¿Se ha proporcionado una copia de los estándares de ingeniería del software publicados a cada desarrollador y gestor de software?

realizado en un proyecto se ajusta a los estándares de ingeniería del software?

• ¿Se emplea una gestión de configuración para mantener la consistencia entre los requisitos del sistema/software, diseño, código y casos de prueba?

• ¿Hay algún mecanismo de control de cambios de los requisitos del cliente que impacten en el software?

• ¿Hay alguna declaración de trabajo documentada, una especificación de requisitos software y un plan de desarrollo del software para cada subcontratación?

• ¿Se sigue algún procedimiento para hacer un seguimiento y revisar el rendimiento de las subcontraciones?

Aspectos técnicos

• ¿Se emplean técnicas de especificación de aplicaciones para ayudar en la comunicación entre el cliente y el desarrollador?

• ¿Se emplean métodos específicos para el análisis del software?

• ¿Emplea un método específico para el diseño de datos y arquitectónico?

• ¿Está escrito su código en más de un 90 por ciento en lenguaje de alto nivel?

• ¿Se han definido y empleado reglas específicas para la documentación del código?

• ¿Emplea métodos específicos para el diseño de casos de prueba?

• ¿Se emplean herramientas de software para apoyar la planificación y el seguimiento de las actividades?

• ¿Se emplean herramientas de software de gestión de configuración para controlar y seguir los cambios a lo largo de todo el proceso del software?

• ¿Se emplean herramientas de software para apoyar los procesos de análisis y diseño del software?

• ¿Se emplean herramientas para crear prototipos software?

• ¿Se emplean herramientas de software para dar soporte a los procesos de prueba?

• ¿Se emplean herramientas de software para soportar la producción y gestión de la documentación?

• ¿Se han establecido métricas de calidad para todos los proyectos de software?

• ¿Se han establecido métricas de productividad para todos los proyectos de software?

Si la mayoría de las cuestiones anteriores se han respondido negativamente, el proceso del software es débil y el riesgo es alto.

5.3.5 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?

• ¿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?

• ¿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 profundidad para valorar el riesgo potencial.

5.3.6 Riesgos del entorno de desarrollo

Si a un carpintero se le pidiera que construyera un mueble de

calidad con una simple sierra de mano, se dudaría de la calidad del producto final. Las herramientas inapropiadas o ineficaces pueden estropear los esfuerzos de incluso un experimentado profacT EMCos rs cr 5 0 eMC EMC norzos dg

• ¿Existen expertos disponibles para responder todas las preguntas que surjan sobre las herramientas?

• ¿Es adecuada la ayuda en línea y la documentación de las herramientas?

Si se ha contestado negativamente a la mayoría de las preguntas anteriores, el entomo de desarrollo es débil y el riesgo es alto.

5.3.7 Riesgos asociados con el tamaño de la plantilla de personal y su experiencia:

Bohem sugiere las siguientes cuestiones para valorar los riesgos asociados con el tamaño de la plantilla de personal y su experiencia:

• ¿Disponemos de la mejor gente?

• ¿Tiene el personal todos los conocimientos adecuados?

• ¿Tenemos suficiente personal?

• ¿Se ha asignado al personal para toda la duración del proyecto?

• ¿Habrá parte del personal de#EFBB72;l proyecto que trabaje sólo durante parte de él?

• ¿Dispone el personal de las expectativas correctas sobre el trabajo?

• ¿ Ha recibido el personal la formación adecuada?

• ¿Será mínimo el movimiento del personal para permitir la continuidad?

Si la respuesta a alguna de estas preguntas es "no", se debería hacer una investigación más profunda para valorar el potencial de riesgo.

5.3.8 Componentes y controladores del riesgo

Las Fuerzas Aéreas de Estados Unidos han redactado un documento que contiene excelentes directrices para identificar riesgos software y evitarlos. El enfoque de las Fuerzas Aéreas requiere que el gestor del proyecto identifique los controladores del riesgo que afectan a los componentes de riesgo software (rendimiento, coste, soporte y planificación temporal). En el contexto de este estudio, los componentes de riesgo se definen de la siguiente manera:

• Riesgo de rendimiento: el grado de incertidumbre con el que el producto encontrará sus requisitos y se adecue para su empleo pretendido.

• Riesgo de coste: el grado de incertidumbre que mantendrá el presupuesto del proyecto.

• Riesgo de soporte: el grado de incertidumbre de la facilidad del software para corregirse, adaptarse y ser mejorado.

• Riesgo de la planificación temporal: el grado de incertidumbre con que se podrá mantener la planificación temporal y de que el producto se entregue a tiempo.

COMPONENTES / CATEGORÍA		RENDIMIENTO	SOPORTE	COSTE	PLANIFICACIÓN TEMPORAL
CATASTRÓFICO	1	Dejar de cumplir los requisitos provocaría el fracaso de la misión.		Malos resultados en un aumento de costes y retrasos de la planificación temporal con otros que superan los $500K.	
	2	Degradación significativa para no alcanzar el rendimiento técnico.	El software no responde o no admite soporte.	Recortes financieros significativos, presupuestos excedidos.	Fecha de entrega inalcanzable.
CRÍTICA	1	Dejar de cumplir los requisitos degradaría el rendimiento del sistema hasta un punto donde el éxito de la misión es cuestionable.		Malos resultados en retrasos operativos y/o aumento de costo con valor esperado de $100K a $500K.	
	2	Alguna reducción en el rendimiento técnico.	Pequeños retrasos en modificaciones software.	Algunos recortes de los recursos financieros, posibles excesos del presupuesto.	Posibles retrasos de la fecha de entrega.
MARGINAL	1	Dejar de cumplir los requisitos provocaría la degradación de la misión secundaria.		Los costes, impactos y/o retrasos recuperables de la planificación temporal con un valor estimado de $1K a $100K.	
	2	De mínima a pequeña reducción en el rendimiento técnico.	El soporte de software responde.	Recursos financieros suficientes.	Planificación temporal realista, alcanzable.
DESPRECIABLE	1	Dejar de cumplir los requisitos provocaría inconvenientes o impactos no operativos.		Los errores provocan impactos mínimos en el coste y/o planificación temporal con un valor esperado de menos de $1K.	
	2	No hay reducción en el rendimiento técnico.	Software fácil de dar soporte.	Posible superávit de presupuesto.	Fecha de entrega fácilmente alcanzable.

El impacto de cada controlador de riesgo en el componente de riesgo se divide en cuatro categorías de impacto - despreciable, marginal, crítico y catastrófico. La figura indica las consecuencias potenciales de errores (filas etiquetadas con 1) o la imposibilidad de conseguir el producto deseado (filas etiquetadas con 2) La categoría de impacto es elegida basándose en la caracterización que mejor encaja con la descripción de la tabla.

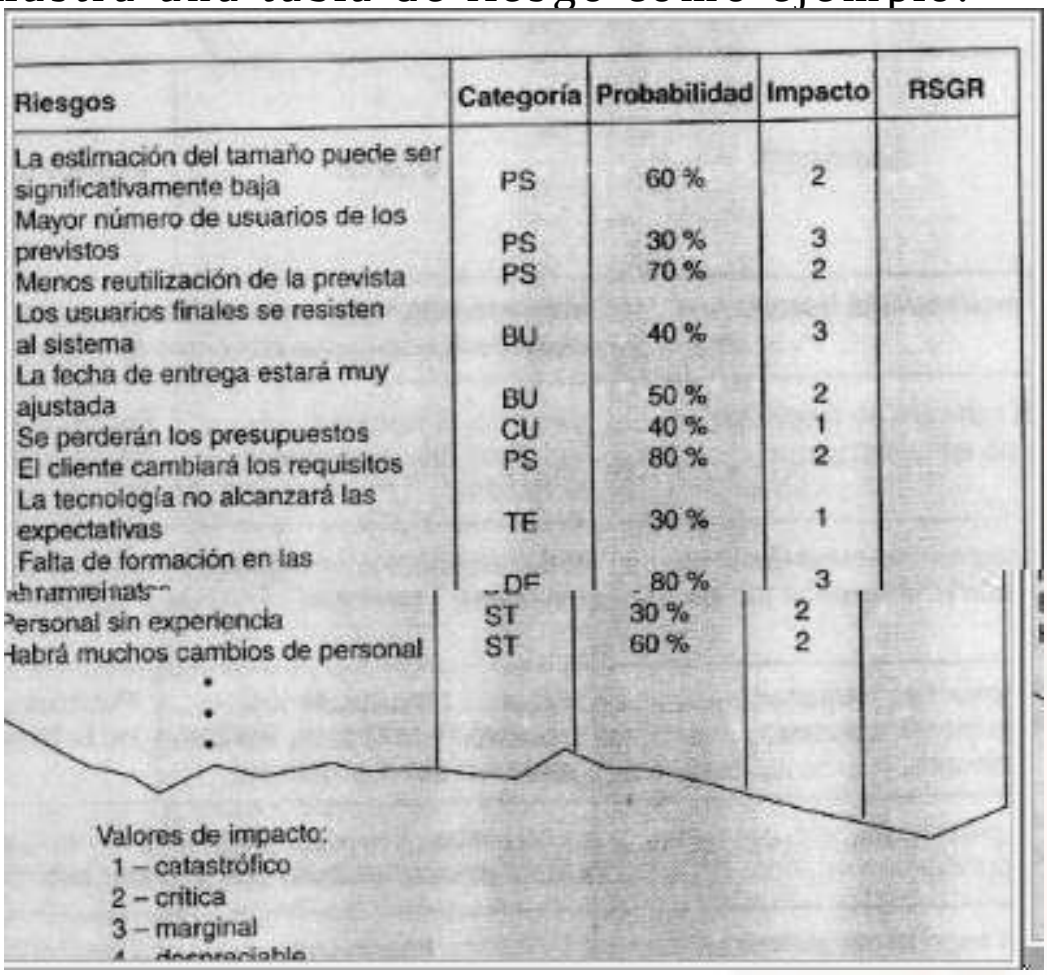
5.4 Proyección del riesgo

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.

5.4.1 Desarrollo de una tabla de riesgo

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.



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 [illegible]	[illegible]DF	80 %	3	
Personal sin experiencia	ST	30 %	2	
Habrá 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 presentada en la Sección 6.3.

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.

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.

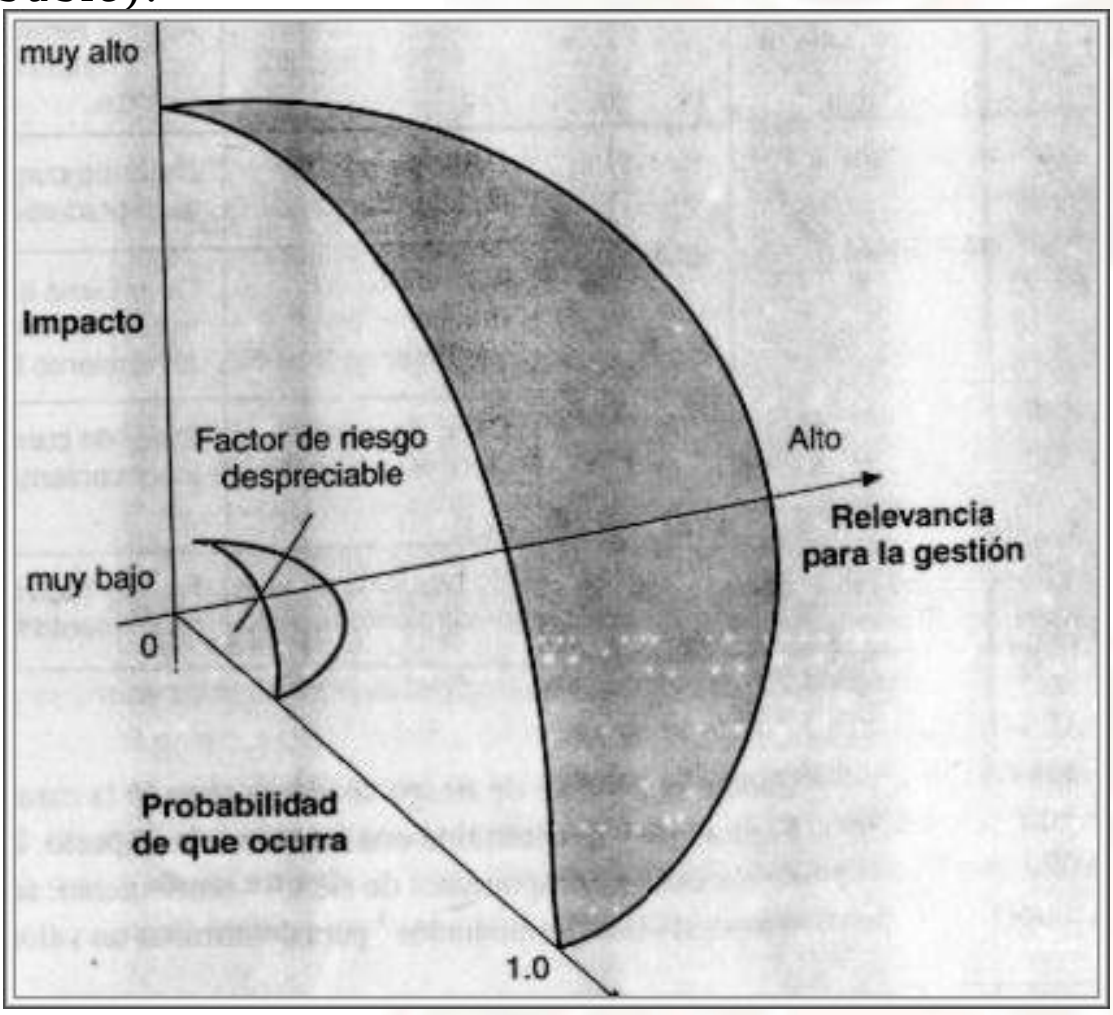
El impacto del riesgo y la probabilidad tienen diferente influencia en la gestión como se ve en la siguiente figura. Un factor de riesgo que tenga un gran impacto pero muy poca probabilidad de que ocurra, no debería absorber una cantidad significativa de tiempo de gestión. Sin embargo, los riesgos de gran impacto con una probabilidad , moderada a alta y los riesgos de poco impacto pero de gran probabilidad deberían tenerse en cuenta en los procedimientos de gestión que se estudian a continuación.

Todos los riesgos que se encuentran por encima de la línea de corte deben ser considerados. La columna etiquetada RSGR contiene una referencia que apunta hacia un plan de reducción, supervisión y gestión del riesgo desarrollado para todos los que se encuentran por encima de la línea de corte.

La probabilidad de riesgo puede determinarse haciendo

estimaciones individuales y desarrollando después un único valor de consenso. Aunque este enfoque es factible, se han desarrollado técnicas más sofisticadas para determinar la probabilidad de riesgo.

Los controladores de riesgo pueden valorarse en una escala de probabilidad cualitativa que tiene los siguientes valores: imposible, improbable, probable y frecuente. Después puede asociarse una probabilidad matemática con cada valor cualitativo (p. ej: una probabilidad del 0.7 al 1.0 implica un riesgo muy probable).



5.4.2 Evaluación del impacto del riesgo

Tres factores afectan a las consecuencias probables de un riesgo, si ocurre: su naturaleza, su alcance y cuando ocurre. La naturaleza del riesgo indica los problemas probables que aparecerán si ocurre. Por ejemplo, una interfaz externa mal definida para el hardware del cliente (un riesgo técnico) impedirá un diseño y pruebas tempranas y probablemente lleve a problemas de integración más adelante en el proyecto. El alcance de un riesgo combina la severidad (¿cómo de serio es el problema?) con su distribución general (¿qué proporción del proyecto se verá afectado y cuantos

clientes se verán perjudicados?). Finalmente, la temporización de un riesgo considera cuándo y por cuánto tiempo se dejará sentir el impacto. En la mayoría de los casos, un jefe de proyecto prefiere las "malas noticias" cuanto antes, pero en algunos casos, cuanto más tarden, mejor.

Volviendo una vez más al enfoque del análisis de riesgo propuesto por las Fuerzas Aéreas de Estados Unidos, se recomiendan los siguientes pasos para determinar las consecuencias generales de un riesgo:

1. Determinar la probabilidad media de que ocurra un valor para cada componente de riesgo.

2. Empleando la figura anterior, determinar el impacto de cada componente basándose en los criterios mostrados.

3. Completar la tabla de riesgo y analizar los resultados como se describe en las secciones precedentes.

La proyección del riesgo y las técnicas de análisis descritas en las secciones 5.4.1 y 5.4.2 se aplican reiteradamente a medida que progresa el proyecto de software. El equipo del proyecto debería volver a la tabla de riesgo a intervalos regulares, volver a evaluar cada riesgo para determinar qué nuevas circunstancias hayan podido cambiar su impacto o probabilidad. Como consecuencia de esta actividad, puede ser necesario añadir nuevos riesgos a la tabla, quitar algunos que ya no sean relevantes y cambiar la posición relativa de otros.

5.4.3 Evaluación del riesgo

En este punto del proceso de gestión del riesgo, hemos establecido 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.

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 estudiados anteriormente - 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.

La figura representa esta situación gráficamente. Si una combinación de riesgos lleva a problemas que provocan excesos de coste y retrasos de la planificación temporal, habrá un nivel representado por la curva en la figura que (cuando se exceda) provocará la terminación del proyecto (la región sombreada). En el punto de referencia, las decisiones de seguir o abandonar son igualmente válidas.

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, limitado por una curva o áreas de incertidumbre.

4. Intentar predecir como afectarán las combinaciones compuestas de riesgos a un nivel de referencia.

5.5 Reducción, supervisión y gestión del riesgo

Todas las actividades de análisis de riesgo presentadas hasta ahora 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

• Gestion 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.

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 cumplimenten puntualmente.

• 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.

Además de supervisar los factores apuntados anteriormente, el jefe del proyecto debería supervisar también la efectividad de los pasos de reducción del riesgo. Por ejemplo. un paso de reducción del riesgo apuntado anteriormente instaba a la definición de "estándares de documentación y mecanismos para asegurarse de que los documentos se cumplimenten puntualmente". Este es un mecanismo para asegurarse la continuidad, en caso de que un individuo crítico abandone el proyecto. El jefe del proyecto debería comprobar los documentos cuidadosamente para asegurarse de que son válidos y de que cada uno contiene la información necesaria en caso de que un miembro nuevo se viera obligado a unirse al proyecto.

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.

Es importante advertir que los pasos RSGR 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.

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).

5.6 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 rnenudo superan al riesgo. Hoy en día, se emplean regularmente hardware y software para el control de sistemas de seguridad crítica.

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.

5.7 El plan RSGR

Se puede incluir una estrategia de gestión de riesgo en el plan del proyecto de software o se podrían organizar los pasos de gestión del riesgo en un plan diferente de reducción, supervisión y gestión del riesgo (Plan RSGR). Todos los documentos del plan RSGR se llevan a cabo como parte del análisis de riesgo y son empleados por el jefe del proyecto como parte del Plan del Proyecto general. A continuación se expone un esquema del Plan RSGR.

I. Introducción

1. Alcance y propósito del documento

2. Visión general de los riesgos principales

3. Responsabilidades

a. Gestión
b. Personal técnico

II. Tabla de riesgo del proyecto.

1. Descripción de todos los riesgos por encima de la línea de corte

2. Factores que influyen en la probabilidad e impacto

III. Reducción, supervisión y gestión del riesgo

n. Riesgo # n

a. Reducción

i.Estrategia general.
ii. Pasos específicos.

b. Supervisión

i. Factores a supervisar
ii. Enfoque de supervisión

c. Gestión

i. Plan de contingencia
ii. Consideraciones especiales.

IV. Planificación temporal de revisión del Plan RSGR

V. Resumen

Una vez que se ha desarrollado el plan RSGR y el proyecto ha comenzado, empiezan los procedimientos de reducción y supervisión del riesgo Como ya hemos dicho antes, la reducción del riesgo es una actividad para evitar problemas La supervisión del riesgo es una actividad de seguimiento del proyecto con tres objetivos principales (1) valorar cuando un riesgo previsto ocurre de hecho; (2) asegurarse de que los procedimientos para evitar el riesgo definidos para el riesgo en cuestión se están aplicando apropiadamente; y (3) recoger información que pueda emplearse en el futuro para analizar riesgos. En muchos casos, los problemas que ocurren durante un proyecto pueden afectar a más de un riesgo. Otro trabajo de la supervisión de riesgos es intentar determinar el "origen" (qué riesgos ocasionaron tal problema) a lo largo de todo el proyecto.

5.8 MAGERIT

MAGERIT es el acrónimo de "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas". Es una metodología de carácter público, perteneciente al Ministerio de Administraciones Públicas. Su utilización no requiere autorización previa del MAP.

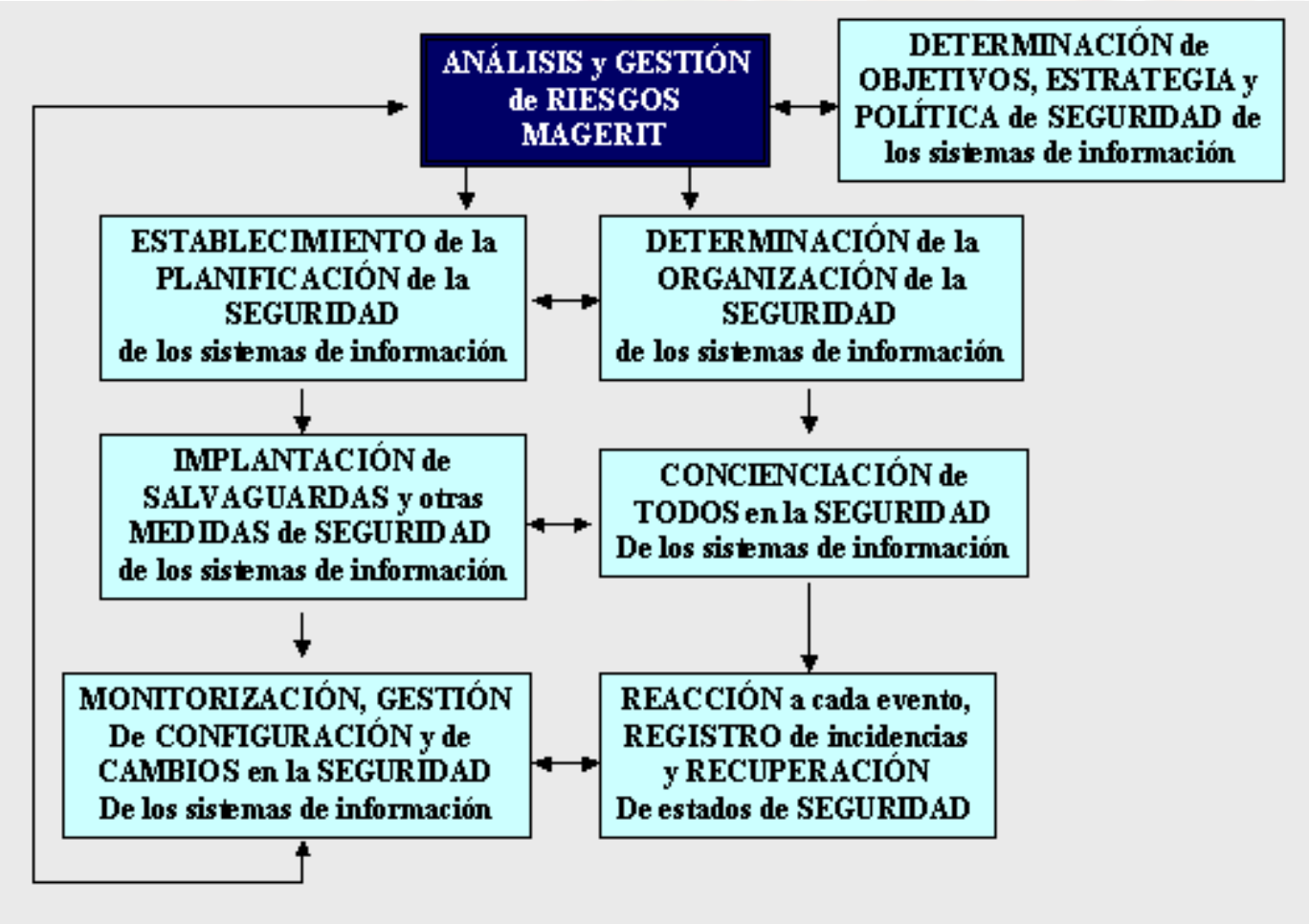
La generalización del uso de las tecnologías de la información y de las comunicaciones es potencialmente beneficiosa para los ciudadanos, las empresas y la propia Administración Pública, pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza en su utilización.

No es posible una aplicación racional de medidas de seguridad sin antes analizar los riesgos para, así implantar las medidas proporcionadas a estos riesgos, al estado de la tecnología y a los costes (tanto de la ausencia de seguridad como de las salvaguardas).

La Metodología de Análisis y GEstión de Riesgos de los sistemas de Información de las AdminisTraciones públicas, MAGERIT, es un método formal para investigar los riesgos que soportan los sistemas de información, y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

MAGERIT ha sido elaborada por un equipo interdisciplinar del Comité Técnico de Seguridad de los Sistemas de Información y Tratamiento Automatizado de Datos Personales, SSITAD, del Consejo Superior de Informática.

La



versión 1.0 de MAGERIT se presenta en siete guías metodológicas:

Guía de Aproximación. Presenta los conceptos básicos de seguridad de los sistemas de información, con la finalidad de facilitar su comprensión por personal no especialista y ofrece una introducción al núcleo básico de MAGERIT, constituido por las Guías de Procedimientos y de Técnicas.

Guía de Procedimientos. Representa el núcleo del método, que se completa con la Guía de Técnicas. Ambas constituyen un conjunto autosuficiente, puesto que basta su contenido para comprender la terminología y para realizar el Análisis y Gestión de Riesgos de cualquier sistema de información.

Guía de Técnicas. Proporciona las claves para comprender y seleccionar las técnicas más adecuadas para los procedimientos de análisis y gestión de riesgos de seguridad de los sistemas de información.

Guía para Responsables del Dominio protegible. Explica la participación de los directivos "responsables de un dominio" en la realización del análisis y gestión de riesgos de aquellos sistemas de información relacionados con los activos cuya gestión y seguridad les están encomendados.

Guía para Desarrolladores de Aplicaciones. Está diseñada para ser utilizada por los desarrolladores de aplicaciones, y está íntimamente ligada con la Metodología de Planificación y Desarrollo de Sistemas de Información, Métrica v2.1.

Arquitectura de la información y especificaciones de la interfaz para el intercambio de datos. La interfaz para intercambio de datos posibilita que un usuario de MAGERIT establezca la comunicación con otras aplicaciones y sistemas facilitando la incorporación de sus productos a la herramienta MAGERIT y viceversa.

Referencia de Normas legales y técnicas. Lista de normas en materia de seguridad a fecha 31 de Diciembre de 1996.

Enlaces de ampliación:

- **Ingeniería del Software III. Universidad Islas Baleares**
- **MAGERIT versión 1.0 (Documentación)**
- **Ministerio Administraciones Públicas. MAGERIT**
- **Seguridad en redes telemáticas. MAGERIT**
- **Riesgo e incertidumbre en la gestión de proyectos informáticos. Juan Izquierdo.**
- **Riesgo deseado?. Gerald J.S. Wilde**
- **Una introducción a la gestión de riesgos tecnológicos. Madridmasd Nº. 23, mayo 2004**