Universidad de las Ciencias Informáticas

Facultad 3

Titulo: Propuesta de procedimiento para el desarrollo y aplicación de la Gestión del Riesgo en proyectos de producción de software.

Trabajo de Diploma para optar por el título de Ingeniero en Ciencias Informáticas.

Autor(es): Delisay Susé Baldají

Tutor(es): Carlos Y. Hidalgo García

Ciudad Habana

Junio, 2007

El camino a transitar será difícil

pero llegar a su final causará gran regocijo.

Agradecimientos

Quiero agradecerle a mi tutor: ***Carlos Y. Hidalgo*** *García por su incondicional ayuda en este trabajo y en mis años de estudiante.*

A mi madre: ***Mercedes Baldají*** *por su eterna paciencia y por apoyarme en cada momento de mi vida.*

A mi hermana y mi padre: ***Anay Susé y Rober Susé*** *por preocuparse siempre por mí aunque la distancia se oponga.*

A mi novio: ***Yosel Velazco*** *por estar siempre a mi lado.*

A mis amigos: ***Yorleidis, Yamilka, Marisbely, Isel, Anni y Lázaro*** *por brindarme su cariño todos estos años y enseñarme el verdadero significado de amistad.*

Y a todos aquellos que hicieron posible este trabajo.

Delisay

Dedicatoria

A mi abuela…

que siempre estará conmigo.

Delisay

Declaración de autoría

Declaro que soy el único autor de este trabajo y autorizo a la facultad 3 de la Universidad de las Ciencias Informáticas a hacer uso del mismo en su beneficio.

Para que así conste firmo la presente a los ____ días del mes de _____ del año _____.

Delisay Susé Baldají

_____

Carlos Y. Hidalgo García

_____

Resumen

La gestión de los riesgos en un proyecto provee de un entorno disciplinado para la toma de decisiones preactivas en base a determinar constantemente que puede ir mal, identificar cuales son los riesgos mas importantes en los cuales enfocarse e implementar estrategias para gestionarlos; esta actividad se inicia en la primera etapa de un proyecto de software y se desarrolla a lo largo de todo su ciclo de vida.

La gestión de riesgos en el ámbito del software procura formalizar el conocimiento orientado a la minimización o prevención de riesgos en proyectos de desarrollo de software, mediante la generación de principios y buenas prácticas de aplicación realista [17]. Hasta el momento se han propuesto y utilizado diferentes enfoques de gestión del riesgo desde que Boehm [3] atrajo a la comunidad de ingeniería del software hacia la gestión del riesgo. Sin embargo, es evidente que pocas organizaciones utilizan todavía de una forma explícita y sistemática métodos específicos para gestionar los riesgos en sus proyectos software.

El procedimiento desarrollado en este trabajo es una herramienta que brinda la posibilidad de efectuar estrategias preactivas de Gestión de Riesgos en los proyectos productivos en la Universidad de Ciencias Informáticas.

Palabras Claves: riesgo, gestión de riesgos, estrategias reactivas y preactivas.

INDICE

ÍNDICE DE FIGURAS

Introducción

La Universidad de Ciencias Informáticas (UCI) fue creada en el año 2002 por el Comandante en Jefe Fidel Castro. Actualmente cuenta con cerca de 10 mil estudiantes insertados en 10 facultades y entre sus objetivos principales se encuentra el de aumentar y fomentar la producción de software en Cuba. Para lograrlo los estudiantes se vinculan a diferentes proyectos productivos en los cuales pueden desarrollar nuevas habilidades y aplicar los conocimientos adquiridos en clases. En el transcurso de 5 años se ha podido comprobar que un aspecto importante en este complejo proceso de creación del software es lograr que éste cumpla con los requerimientos especificados y las necesidades o expectativas del cliente o usuario, que esté en el plazo solicitado y se ajuste al presupuesto asignado; por lo que en la UCI cada facultad posee y prioriza un grupo de trabajo encargado de chequear y mantener la calidad en cada proyecto realizado.

Situación Problémica.

La calidad de un software se ve afectada considerablemente si no se tienen en cuenta los riesgos que puedan afectarlo, ya que si estos se hacen realidad es probable que la planificación temporal del proyecto se retrase, que la implementación pueda llegar a ser difícil, que los costos aumenten, entre otros. A todos estos factores está expuesta la UCI ya que no cuenta con un personal especializado en herramientas y métodos que posibiliten la gestión de riesgos en la producción de software.

Problema Científico.

¿Como aumentar la calidad en los proyectos de producción de software de la UCI mediante el desarrollo de una eficaz gestión de riesgos?

Objeto de Estudio.

Proceso de gestión del riesgo en la producción de software.

Objetivo General.

Elaborar un procedimiento para el desarrollo y aplicación de la gestión de riesgos en proyectos de producción de software en la UCI.

Objetivos Específicos.

1. Identificar los principales riesgos presentes en la producción de software.
2. Analizar el proceso de Gestión del Riesgo en la producción de software.

Campo de Acción.

Proceso de gestión del riesgo en la producción de software en la UCI.

Hipótesis.

Si se desarrolla un procedimiento para la gestión del riesgo en el proceso de producción de software en la UCI esto aumentará la calidad del producto, permitiendo desarrollar e implementar anticipadamente respuestas apropiadas a problemas o dificultades que puedan surgir en el proyecto.

Tareas de investigación.

1. Definir tendencias actuales relacionadas con la gestión del riesgo.
2. Localizar herramientas actuales para la gestión del riesgo.
   2.1. Identificar los riesgos por categoría que se tratan en cada uno.
   2.2. Establecer una valoración sobre estas herramientas.
3. Estudiar metodologías actuales para la gestión del riesgo.
   3.1. Establecer una valoración sobre estas metodologías.
4. Identificar características de la gestión del riesgo en la UCI.
5. Elaborar una propuesta de procedimiento para la gestión del riesgo.

Marco Teórico Conceptual

Definición de términos operacionales.

Cliente: Persona que solicita la creación del software.

Usuario: Persona que utiliza o trabaja con el software.

Producto*:* Algo que se produce para un colaborador, un empresario o un cliente. Desde el punto de vista de un ingeniero de software son los programas, documentos y los datos que configuran el software de computadora. Pero desde el punto de vista de los usuarios el producto obtenido es la información resultante que hace de algún modo el mundo mejor a estos.

Software de computadora: Producto que diseñan y construyen los ingenieros de software. Esto abarca programas que se ejecutan dentro de una computadora, documentos que comprenden formularios virtuales e impresos y datos que combinan números y texto, y también incluyen representaciones de información de audio, video e imágenes.

Riesgo: Probabilidad de un daño.

Proyecto: Normalmente produce un producto. Es un esfuerzo temporal emprendido para crear un producto o un servicio único. [12]

Requerimientos de un software: Requisitos que debe cumplir para satisfacer las demandas o expectativas del cliente.

Calidad: Conjunto de propiedades y de características de un producto o servicio, que le confieren aptitud para satisfacer necesidades explícitas o implícitas (ISO 8402)

Gestión del riesgo: Conjunto de pasos y procesos que tienen como objetivo garantizar que el proceso de desarrollo del software se de en las condiciones óptimas de seguridad posible para la infraestructura y población, y que la atención y acciones desplegadas ante un desastre promuevan el mismo desarrollo.

Marco Metodológico

Métodos Teóricos:

Analítico-Sintético: Son dos procesos que permiten buscar la esencia de los fenómenos, los rasgos que lo caracterizan y distinguen.

Su objetivo en esta investigación es analizar las teorías, documentos, conceptos, etc.; permitiendo la extracción de los elementos más importantes que se relacionan con mi objeto de estudio (Proceso de gestión del riesgo en la de producción de software)

Análisis histórico – lógico: Permite estudiar de forma analítica la trayectoria histórica real de los fenómenos, su evolución y desarrollo.

Su objetivo en esta investigación es la de constatar teóricamente como ha evolucionado el fenómeno de la gestión del riesgo a partir de los años 40

permitiendo determinar cambios en su funcionamiento, aportes relevantes, entre otras características que puedan servirle a la investigación que se lleva a cabo.

Métodos Empíricos:

Observación: Es el registro visual de lo que ocurre en una situación real, en un fenómeno determinado; clasificando y consignando los hechos y acontecimientos pertinentes de acuerdo con algún esquema previsto.

Este método se utilizo en distintos momentos de esta investigación y recoge la información de cada uno de los conceptos o variables definidas en la hipótesis de este trabajo.

Entrevista: Es una conversación planificada para obtener información.

El uso de este método constituye un medio para el conocimiento cualitativo de los fenómenos que se relacionan con la gestión del riesgo, y sobre características personales del entrevistado y la percepción que tiene este sobre la investigación que se lleva a cabo.

Variables de la Investigación.

Variable independiente:

Gestión del riesgo en el proceso de producción de software en la UCI.

Variable dependiente:

Aumento de la calidad del producto permitiendo desarrollar e implementar anticipadamente respuestas apropiadas a problemas o dificultades que puedan surgir en el proyecto.

Capítulo 1

Estado del Arte

1.1. Factores de riesgo más significativos.

A continuación se describen los factores de riesgos más significativos encontrados la literatura consultada de acuerdo a sus autores.

Boehm [5] identifica 10 factores de riesgo en proyectos de desarrollo de software. Estos hacen referencia a riesgos relacionados con el personal, itinerarios, funcionalidad del sistema, gestión de requerimientos, proveedores y el uso y desempeño de los recursos.

Barki [2] presenta 5 factores, los cuales fueron clasificados de la siguiente forma: El factor 1 se le dio el nombre de nueva tecnología; ya que de las cinco variables que lo conforman, cuatro de ellas están relacionadas con tecnología; el factor 2 se le nombró tamaño o alcance de la aplicación, ya que de las cinco variables que lo conforman, cuatro hacen referencia al número de personas en el equipo, diversidad del equipo, número de usuarios futuros, y número de niveles jerárquicos ocupados por los usuarios futuros. En el factor 3, cuatro de las cinco variables se refieren a la experiencia del equipo, nombrando de esta forma al factor. En el factor 4, las variables hacen referencia a la complejidad técnica, y al número de enlaces de la aplicación, nombrando al factor como complejidad de la aplicación. Finalmente al quinto factor se le llamo ambiente organizacional, puesto que esta compuesto por variables relacionadas con la aplicación o con el personal de la organización.

Jones [13] presenta 3 factores de riesgos principalmente incurridos por los administradores del proyecto. El factor 1 hace referencia a los riesgos asociados con la estimación y planificación

inexacta, el factor 2 se refiere a los reportes y estados incorrectos u optimistas y el factor 3 se refiere a las presiones externas.

Estévez y Pastor [7] presentan factores que abarcan primordialmente los riesgos organizacionales y estratégicos de la organización. La perspectiva estratégica trata sobre las competencias claves para lograr los objetivos de la organización a largo plazo, mientras que la perspectiva táctica afecta a las actividades de negocio con objetivos a corto plazo.
La siguiente tabla presenta un resumen de los riesgos encontrados en la literatura:

Factor	**Boehm y Ross (1991) Lista de riesgos desarrollada de acuerdo al punto de vista de los accionistas.**
Factor 1	Falta de personal cualificado.
Factor 2	Itinerario y presupuesto poco realistas.
Factor 3	Desarrollo incorrecto de las funciones del software.
Factor 4	Desarrollo incorrecto de las interfaces del usuario.
Factor 5	Adición de funciones o características innecesarias.
Factor 6	Cambio constante en los requerimientos.
Factor 7	Fallas en los componentes subcontratados.
Factor 8	Pobre calidad de las tareas subcontratadas.
Factor 9	Fallas en Tiempo real de respuesta.
Factor 10	Inhabilidad para implementar soluciones técnicas debido a la pobre capacidad de conocimientos en la ciencia de computación.
Factor	**Barki (1993) Evaluación de riesgos en proyectos de desarrollo de software**
Factor 1	Tecnológico
Factor 2	Tamaño de la aplicación
Factor 3	Falta de experiencia
Factor 4	Complejidad de la aplicación

Factor 5	Ambiente organizacional
Factor	**Jones(1998) Tres factores de riesgo relevantes en el desarrollo de software**
Factor	Estimación y planeación inexacta del itinerario.
Factor	Reporte de status incorrecto y optimistas.
Factor	Presiones externas las cuales dañan los proyectos de software.
Factor	**Estévez y Pastor (2000) Factores estratégicos y organizacionales.**
	Factores estratégicos
Factor 1	Apoyo continuo de la alta dirección.
Factor 2	Gestión efectiva del cambio organizacional.
Factor 3	Buena gestión del ámbito del proyecto.
Factor 4	Composición adecuada del equipo del proyecto.
Factor 5	Rediseño adecuado de los procesos de negocio.
Factor 6	Papel adecuado del líder de proyecto.
Factor 7	Papel adecuado del jefe de proyecto.
Factor 8	Implicación y participación de los usuarios.
Factor 9	Confianza entre actores.
	Factores tácticos
Factor 1	Equipo y consultores dedicados.
Factor 2	Comunicación interna y externa.
Factor 3	Plan formalizado del proyecto
Factor 4	Programa de formación adecuado.
Factor 5	Precisión de problemas inesperados.
Factor 6	Uso adecuado de consultores.
Factor 7	Responsables debidamente autorizados.

1.2. Herramientas actuales utilizadas para la gestión del riesgo.

Existen una gran cantidad de herramientas software de gestión de riesgos disponibles en el mercado y las cuales siguen diferentes metodologías. Las más significativas son las siguientes:

Active Risk Manager (ARM)

Descripción: Herramienta integrada de Gestión de Riesgos que brinda una solución para la Identificación de Riesgos mediante la utilización de la información contenida en la WBS (Web Based System) del proyecto.

Proveedor: Strategic Thought.

Plataforma: Web Based (requiere instalación de servidor).

Sistemas Operativos: Windows 98, ME, NT, 2000, y XP.

Idioma: inglés.

Licenciamiento: Comercial

Características Destacables:

- Gerenciamiento integrado de riesgos basado en estándares predefinidos.
- Alto grado de integración con herramientas estándares del mercado (VISIO, MS Office, Primavera, etc.).
- Generación de reportes.

Se muestra en los Anexos una pantalla correspondiente a la herramienta analizada (véase **Figura 6** - Pantalla Principal de Gestión de Riesgos en ARM).

Technical Risk Identification and Mitigation System (TRIMS)

Descripción: Herramienta integrada de Gestión de Riesgos que emplea ingeniería de conocimientos y se enfoca en la identificación, medición y seguimiento de riesgos técnicos de proyectos.

Proveedor: Navy's Best Manufacturing Practices.

Plataforma: Win32.

Sistemas Operativos: Windows 98, ME, NT, 2000, y XP.

Idioma: inglés.

Licenciamiento: Libre.

Características Destacables:

- Gerenciamiento integrado de riesgos.
- Generación de reportes.
- Orientada a categorías de riesgos predefinidas para sectores específicos.

Se muestran a continuación algunas pantallas correspondientes a la herramienta analizada (véase **Figura 7** - Pantalla Principal de TRIMS, **Figura 8** - Carga de Riesgo en TRIMS y **Figura 9**- Reporte en TRIMS).

RiskTrak

Descripción: Herramienta integrada de Gestión de Riesgos que brinda una solución para la Identificación de Riesgos mediante el empleo de base de datos.

Proveedor: Risk Services & Technology.

Plataforma: Web Based (requiere instalación de servidor).

Sistemas Operativos: Windows 98, ME, NT, 2000, y XP.

Idioma: inglés.

Licenciamiento: Comercial

Características Destacables:

- Generación de reportes.
- Administración centralizada de gerenciamiento de riesgo a nivel organizacional.

Se muestran en los Anexos algunas pantallas correspondientes a la herramienta analizada (véase **Figura 10** - Categorías de Riesgos en RiskTrack y **Figura 11** - Análisis de Riesgos en RiskTrack).

WelcomRisk

Descripción: Herramienta integrada de Gestión de Riesgos que brinda una solución para la Identificación Sistemática de Riesgos mediante la utilización de bibliotecas configurables de categorías de riesgos.

Proveedor: Welcom

Plataforma: Web Based (requiere instalación de servidor).

Sistemas Operativos: Windows 98, ME, NT, 2000, y XP.

Idioma: Inglés.

Licenciamiento: Comercial

Características Destacables:

- Generación de reportes.
- Integración con herramientas estándares del mercado (MS Project, Primavera, etc.).
- Alto grado de seguridad tanto a nivel de sistema como de aplicación.

Se muestran en los Anexos algunas pantallas correspondientes a la herramienta analizada (véase **Figura 12** - Resumen de Riesgos y **Figura 13** - Reporte en WelcomRisk).

@Risk

Descripción: Herramienta de Inteligencia de Negocios, que le muestra todos los resultados posibles de una situación de negocios y le indica la probabilidad de que ocurran.

Proveedor: Palisade

Sistemas Operativos: Windows 98, 2000 y XP

Idioma: Español, inglés, alemán, francés y japonés.

Licenciamiento: Comercial

Características Destacables:

- @RISK funciona en Excel.
- Presenta resultados con gráficos espectaculares.
- Análisis de escenarios identifica las situaciones –o combinaciones que producen un resultado determinado.
- Integración con herramientas estándares del mercado (MS Project)
- Variedad de eficaces funciones analíticas (Búsqueda de Objetivo, Análisis de Tendencia, Análisis Avanzado de Sensibilidad)
- Ofrece un informe estadístico completo de las simulaciones, así como acceso a todos los datos generados.

Se muestran en los Anexos algunas pantallas correspondientes a la herramienta analizada (véase **Figura 14** – Gráfico de selección de distribuciones).

Valoración del autor sobre las herramientas

Ventajas

Las herramientas software de gestión del riesgo caracterizadas anteriormente realizan una efectiva y rápida gestión de riesgo. Presentan los resultados con gráficos que facilitan la compresión y generan detallados reportes, los cuales le permiten al cliente saber que puede o esta yendo mal en su organización.

Algunas están integradas a herramientas estándares del mercado como Microsoft Office, Primavera, Visio, entre otros.

Poseen un alto grado de seguridad y trabajan, la gran mayoría, en los sistemas operativos Windows 98, 200 y XP.

Desventajas

Estas herramientas no son una vía efectiva para gestionar los riesgos en los proyectos productivos de la universidad ya que no se comercializan libremente, se enfocan sólo en una categoría de riesgos (TRIMS – Technical Risk Identification and Mitigation System), están

orientadas a compañías maduras que poseen una amplia base de datos organizacional que les permite generar información de categorías propias de riesgos (RiskTrak y WelcomRisk), o bien emplean un mecanismo que no se orienta al uso de taxonomías[1] (ARM – Active Risk Manager).

1.3. Metodologías actuales utilizadas para la gestión de riesgo.

Actualmente existen en el mercado un gran número de metodologías para la gestión de riesgos, algunas de ellas son:

AUDIRISK

Metodología para la valoración y el análisis de Riesgos. Es consistente con las normas y principios de auditoria generalmente aceptados, comprende la implantación del modelo COBIT, así como con la norma ISO 9000, ISO 17799-1 (Código de Buenas Prácticas para la Gestión de Seguridad de la Información) e ISO 17799-2 (Sistemas de Gestión de Seguridad de la Información). Dispone de herramientas de software y hardware para apoyar el uso de esta metodología.

MARGERIT

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas impulsada originalmente por el Ministerio de Administraciones Publicas (MAP). Es de carácter público, y su utilización no requiere autorización previa del MAP. 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.

[1] La Administración de Riesgos en base a Taxonomías implica el utilizar una estructura agrupadora de los mismos de acuerdo a sus diferentes clases.

Esta metodología considera acertadamente que la gestión del riesgo es el “alma mater “ de toda actuación organizada en materia de seguridad y, por tanto, de la gestión global de la misma.

Se presenta en 7 guías metodológicas: Guía de Aproximación, Guía de Procedimientos, Guía de Técnicas, Guía para Responsables del Dominio protegible, Guía para el Desarrolladores de Aplicaciones, Arquitectura de la información y especificaciones de la interfaz para el intercambio de datos, y Referencia de Normas legales y técnicas.

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

AUDICONTROL

Metodología asistida por computadora para gestión de riesgos en procesos de negocio y sistemas de información, basada en un enfoque proactivo en lugar del tradicional y ya obsoleto enfoque reactivo del control.

La metodología fue desarrollada por AUDISIS (Auditoria Integral y Seguridad en Sistemas de Información), una firma colombiana dedicada a prestar servicios de consultoría en auditoria de sistemas, administración de riesgos y diseño de controles. Es el resultado de experiencias y conocimientos adquiridos a través de 18 años de trayectoria profesional en empresas de diferentes tamaños y grados de sofisticación tecnológica en Colombia y países de Centro y Sur América.

PMI

Con el propósito de plantear una gestión de riesgos eficiente para compañías que utilizan una mezcla de métodos agiles como: Scrum, Rational Unified Process (RUP) y Microsoft Solutions Framework (MSF) de desarrollo de software, se utiliza como base la gestión de riesgos utilizada

por el PMI, unido a la utilización de herramientas de otra organizaciones y a las practicas de gestión ágil de proyectos.

Metodología para la gestión de riesgos desarrollada por PMI (Project Management Institute) la cual consta de cinco procesos. Cada proceso ocurre por lo menos una vez en cada proyecto. Se utiliza como metodología base unido a la utilización de herramientas de otras organizaciones y a las prácticas de gestión ágil de proyectos. Ver Figura 1.

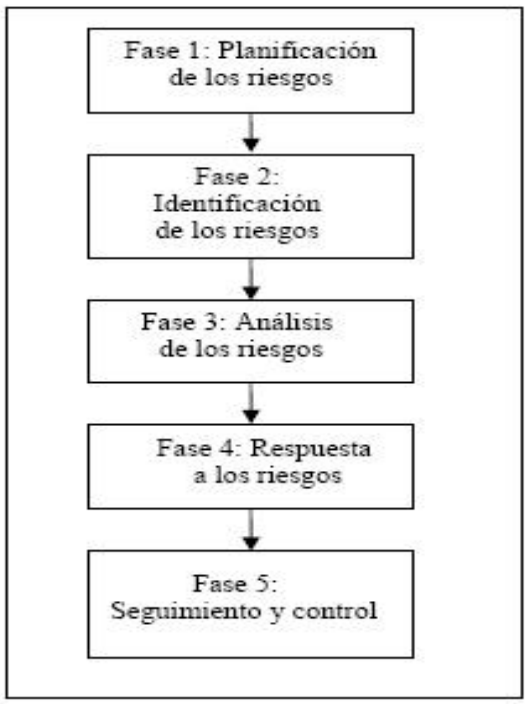

Figura 1 - Diagrama de Flujo de la metodología PMI

AUDAP

Metodología asistida por computador para auditoria centrada en riesgos críticos en procesos de negocio y tecnología de información. Sirve para apoyar a los auditores internos, externos y de sistemas en el desarrollo del enfoque de "Auditoria Centrada en Riesgos Críticos". Presenta

guías y formatos para ejecutar las tres fases de la auditoria en procesos de negocio y servicios automatizados: Planeación, Ejecución y Comunicación de resultados.

La metodología AUDAP y la herramienta de software que la soporta, están alineadas con el enfoque de mejoramiento de procesos y la norma ISO 9000. La propiedad intelectual de esta metodología está registrada a nombre de AUDISIS.

La metodología consta de los siguientes elementos: manual de la metodología; software ejecutable para asistir el uso de la metodología; manual del usuario del software AUDAP; bases de datos con conocimientos y "best practices" (mejores practicas) sobre escenarios de riesgo (tecnología de información del estándar COBIT y 8 de AUDISIS), categorías de riesgos típicos, amenazas o causas de riesgos, controles, técnicas de auditoria y cuestionarios.

Valoración del autor sobre las metodologías

Estas metodologías permiten utilizar estrategias preactivas con el objetivo de realizar un análisis de riesgos de forma temprana, sistemática, formal y profunda, evitando así un menor tiempo de reacción ante la aparición de riesgos impredecibles. Las compañías que las desarrollaron tienen una gran experiencia en este campo y brindan un amplio soporte técnico para la implantación de estas.

Estas metodologías (exceptuando PMI) no son una vía efectiva para gestionar los riesgos en los proyectos productivos de la universidad ya que solo una se comercializa libremente, y no están enfocadas a la gestión de riesgos en el proceso de producción de software. Solo PMI pudiera guiar la gestión de riesgos en el proceso de producción de software en la UCI ya que este modelo tiene como objetivo garantizar que los riesgos del proyecto sean identificados, analizados, documentados, mitigados y controlados correctamente durante todo el ciclo de vida del proyecto.

1.4. Características de la gestión de riesgos en la UCI.

Uno de los principales problemas que siempre ha tenido la industria del software es que a pesar de que hay estándares, metodologías, técnicas y demás herramientas, éstas no se emplean de manera generalizada, haciendo de esta industria algo menos que una artesanía. Sin embargo, se ve que sí es un factor que contribuye al éxito del proyecto. De hecho, se ha comprobado que el 46% de los proyectos finalizados con éxito habían utilizado alguna metodología formal de gestión, en comparación con el 70% del resto de los proyectos (no satisfactorios y con fracaso) que no utilizaron ninguna metodología formal.

Atendiendo a este importante planteamiento se puede decir que en la universidad, donde la gran mayoría de los estudiantes están vinculados a proyectos productivos, sí se realiza la Gestión del Riesgo, pero solo en proyectos de gran magnitud o de alcance nacional e internacional (ej. ONE - Oficina Nacional de Estadísticas) e Identidad) y por módulos, en los cuales se identifican los riesgos que puedan afectar al proyecto y se tratan de mitigar aquellos que aparecen en toda su etapa de vida.

Esto trae consigo que una parte significativa de proyectos no culmine con éxito sus objetivos propuestos (entrega en tiempo, costo, entre otros) o peor aun que fracase completamente.

Algunos ejemplos de riesgos que se han podido identificar en estos proyectos son:

- Se pierde el rol de jefe de equipo, es un programador mas por lo que no cumple con las tareas de jefe de equipo y su prioridad es la programación.
- No debe recaer la responsabilidad de la arquitectura en una única persona, sino en un equipo que se especializa en diferentes partes y aspectos del sistema.
- Falta de una Gestión de Riesgos.
- No se realizan pruebas que detecten fallas en los principios básicos del negocio.

- No existe una estrategia de liberación, el producto que se realiza es muy grande y se pretende liberarlo todo de una sola vez.
- No se incorporan desde el inicio elementos de seguridad.
- No se recogen métricas que permitan ir teniendo una línea base que sirva para próximas estimaciones.

Se ha podido llegar a la conclusión que principalmente en los proyectos productivos de la universidad se tratan de identificar los riesgos que puedan presentarse y se procede a mitigarlos pero no se planifican los recursos, el presupuesto, ni el esfuerzo para reducir las probabilidades y el impacto de los riesgos; por lo que no se realiza una correcta gestión de riesgos y las actividades que conlleva este complejo pero necesario proceso recaen solamente en el líder y el planificador del proyecto.

Capítulo 2

Los Riesgos

El SEI (*Software Engineering Institute*) define al **riesgo** como "*la posibilidad de sufrir una pérdida*" [18] y a la Administración de Riesgos como "*la práctica compuesta de procesos, métodos y herramientas que posibilita la Gestión de los Riesgos en un proyecto y que provee de un entorno disciplinado para la toma de decisiones preactivas en base a determinar constantemente que puede ir mal (riesgos), identificar cuales son los riesgos mas importantes en los cuales enfocarse e implementar estrategias para gestionarlos*"; esta actividad se inicia en la primera etapa de un proyecto de software (durante la exploración de conceptos) y se desarrolla a lo largo de todo su ciclo de vida (hasta la aceptación del producto del proyecto).

Una correcta Gestión de Riesgos posibilita, por tanto, el aprovechamiento óptimo de recursos y provoca, como consecuencia, el aumento de ganancias y la disminución de pérdidas.

La ausencia de una apropiada Gestión de Riesgos conlleva a la imposibilidad de lograr el control efectivo de un proyecto derivando esto en la imposibilidad de realizar una correcta administración del mismo. En base a las consideraciones antes expuestas, la Gestión de Riesgos debe ser enfatizada y considerada como una actividad clave en todo tipo de proyectos y, particularmente, en proyectos de desarrollo de software.

Al realizar la Gestión de Riesgos, es fundamental lograr una clara descripción del riesgo de forma tal de que el mismo pueda ser comprendido y manejado adecuadamente; cuando se lo enuncia, no solo debe considerarse el síntoma sino también sus consecuencias.

2.1. Los riesgos.

"En primer lugar, el riesgo concierne a lo que ocurra en el futuro. El hoy y el ayer no nos conciernen realmente, porque ahora ya estamos recogiendo los frutos de lo que sembramos en el pasado. La cuestión es si podemos, entonces, modificando nuestras acciones en este momento, crear una oportunidad para una situación diferente y más esperanzadora de nuestro mañana. Esto significa, en segundo lugar, que el riesgo implica un cambio, que puede venir dado por cambio de opiniones, acciones o lugares. En tercer lugar, el riesgo implica una elección, y la falta de certeza de que la elección sea correcta. Así, paradójicamente, el riesgo como la muerte o los impuestos, es una de las pocas cosas inevitables de la vida." [6]

El riesgo debe ser descrito por una frase lo suficientemente completa y directa que permita analizar su causa raíz, discutir su impacto y desarrollar un conjunto de respuestas o acciones para prevenirlo o reducir sus consecuencias. Debe evitarse el uso de abreviaciones o acrónimos que resulten difíciles de comprender como de generalizaciones y detalles irrelevantes. Puede ser de utilidad en algunos casos agregar información de contexto aun riesgo para facilitar su entendimiento a personas que puedan no conocer todos los detalles del proyecto (ya sea en la actualidad como en el futuro).

Se han producido amplios debates sobre la definición adecuada para riesgo de software, y hay un acuerdo común en que el riesgo siempre implica dos características [11]:

Incertidumbre: El acontecimiento que caracteriza al riesgo puede o no puede ocurrir: por ejemplo, no hay riesgos de un 100 por ciento de probabilidad. (Un riesgo del 100 por ciento es una limitación del proyecto de software)

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

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 de proyecto; es decir, si los riesgos del proyecto se hacen realidad, es probable que la planificaron 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. También están definidos en esta categoría la complejidad del proyecto, tamaño y el grado de incertidumbre.

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, de verificación y de mantenimiento. Además, las ambigüedades de especificaciones, incertidumbre técnica, técnicas anticuadas y las “tecnologías punta” son tan bien 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 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 como 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.

2.2. Identificación del riesgo.

La identificación del riesgo es un intento sistemático para especificar las amenazas al plan de 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.

Genéricos: Son una amenaza potencial para todos los proyectos de software.

Específicos de producto: Solo los pueden identificar los que tienen una clara visión de la tecnología, el personal y el entorno especifico del proyecto en cuestión. Para identificarlos se examina el plan del proyecto y la declaración del ámbito del software y se desarrolla una respuesta a la siguiente pregunta: ¿Que características especiales de este producto pueden estar amenazadas por nuestro plan de proyecto?

Tanto los riegos genéricos como los específicos del producto se deberían identificar sistemáticamente.

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 de 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" [1] 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.

2.2.1. Riesgos del tamaño del software.

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 (línea de código) o FP (punto de función)
- ¿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 en el tamaño del producto respecto a la medida de productos anteriores?
- ¿Numero de usuarios del producto?
- ¿Numero de cambios previstos a los requisitos del producto? ¿Antes de la entrega? ¿Después de la entrega?
- ¿Cantidad de software utilizado?

En cada caso, la información que se tiene del producto a desarrollar debe compararse con la experiencia adquirida con productos similares. Si ocurre una gran desviación del porcentaje, el riesgo es grande; de la misma forma que si las magnitudes son similares podemos estar en presencia de los mismos riesgos que se encontraron anteriormente.

2.2.2. Riesgos del impacto en el negocio.

Un gestor de ingeniería 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 usaran 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 retrazo en la entrega?
- ¿Costos asociados con un producto defectuoso?

Cada respuesta para el producto a desarrollar debe compararse con la experiencia adquirida con productos similares. Si ocurre una gran desviación del porcentaje, el riesgo es grande; de la misma forma que si las magnitudes son similares podemos estar en presencia de los mismos riesgos que se encontraron anteriormente.

2.2.3. Riesgos relacionados con el cliente.

No todos los clientes son iguales. Pressman[2] 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

[2] Roger S. Pressman. Ingeniero de software, Presidente de R. S. Pressman & Associates, Inc.

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 desarrollador?
- ¿Está dispuesto el cliente a participar en las revisiones?
- ¿Es sofisticado técnicamente el área del producto?
- ¿Está dispuesto el cliente a dejar 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.

2.2.4. 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[3]. 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 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 están dispuestos a usarlo?
- ¿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 están 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?

[3] R. S. Pressman & Associates. Inc., empresa de asesoría especializada en métodos y formación de Ingeniería del Software.

- ¿Se han desarrollado diseños de documentos y ejemplos para todas las entregas definidas como parte del proceso del software?
- ¿Se llevan a cabo regularmente revisiones técnicas formales de las especificaciones de requisitos, diseño y código?
- ¿Se llevan a cabo regularmente: revisiones técnicas de los procedimientos de prueba y de los casos de prueba?
- ¿Se documentan todos los resultados de las revisiones técnicas, incluyendo los errores encontrados y recursos empleados?
- ¿Existe algún mecanismo para asegurarse de que el trabajo 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?

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.

2.2.5. 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. Es extremadamente difícil predecir los riesgos, y mucho menos hacer algún 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 Inteligencia Artificial 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.

2.2.6. Riegos 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 profesional.

El entorno de ingeniería del software soporta al equipo del proyecto, al proceso y al producto. Pero si el entorno es malo puede ser una fuente de riesgos significativa. La siguiente lista de comprobación de elementos de riesgo identifica riesgos genéricos asociados con el entorno de desarrollo:

- ¿Tenemos disponible una herramienta de gestión de proyectos de software?
- ¿Tenemos disponible una herramienta de gestión del proceso del software?
- ¿Existen herramientas de análisis y diseño disponibles?
- ¿Proporcionan las herramientas de análisis y diseño, métodos apropiados para el producto a construir?

- ¿Hay disponible compiladores o generadores de código apropiados para el producto a construir?
- ¿Hay disponibles herramientas de pruebas apropiadas para el producto a construir?
- ¿Tenemos disponibles herramientas de gestión de configuración software?
- ¿Hace uso el entorno de bases de datos o información almacenada?
- ¿Están todas las herramientas de software integradas entre sí?
- ¿Se ha formado a los miembros del equipo del proyecto en todas las herramientas?
- ¿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 entorno de desarrollo es débil y el riesgo es alto.

2.2.7. Riesgos asociados con el tamaño de la plantilla de personal y su experiencia.

Boehm [4]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 del 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?

[4] W. B. Boehm, ingeniero de software, creador del Software Risk Management

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

2.2.8. Evaluación global del riesgo del proyecto.

Las siguientes preguntas provienen de los datos del riesgo obtenidos mediante las encuestas realizadas a gestores de software expertos de diferentes partes del mundo [14]. Las preguntas están ordenadas por su importancia relativa para el éxito de un proyecto.

1. ¿Se han entregado los gestores del software y clientes formalmente para dar soporte al proyecto?
2. ¿Están completamente entusiasmados los usuarios finales con el proyecto y con el sistema/producto a construir?
3. ¿Han comprendido el equipo de ingenieros de software y los clientes todos los requisitos?
4. ¿Han estado los clientes involucrados por completo en la definición de los requisitos?
5. ¿Tienen los usuarios finales expectativas realistas?
6. ¿Es estable el ámbito del proyecto?
7. ¿tiene el ingeniero del software el conjunto adecuado de habilidades?
8. ¿Son estables los requisitos del proyecto?
9. ¿Tiene experiencia el equipo del proyecto con la tecnología a implementar?
10. ¿Es adecuado el número de personas del equipo del proyecto para realizar el trabajo?
11. ¿Están de acuerdo todos los clientes/usuarios en la importancia del proyecto y en los requisitos del sistema/producto a construir?

2.2.9. Componentes y controladores del riesgo.

Las Fuerzas Aéreas de Estados Unidos [1] ha 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.

El impacto de cada controlador del riesgo en el componente de riesgo se divide en cuatro categorías de impacto –despreciable, marginal, crítico y catastrófico-. Como muestra la Tabla 1 [4], se describe una categorización de 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.

Componentes / **Categoría**		**Rendimiento**	**Soporte**	**Coste**	**Planificación Temporal**
	1	Dejar de cumplir los requisitos		Malos resultados en un aumento de costes con	

		provocaría el fallo de la misión.		retraso de la planificación temporal con gastos que superan las $500.000	
Catastrófica	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 donde el éxito de la misión es cuestionable.		Malos resultados en retrasos operativos y/o aumento de coste con un valor esperado de $100.000 a $ 5000.000.	
	2	Alguna reducción en el rendimiento técnico.	Pequeños retrasos en modificaciones de software.	Algunos recortes de los recursos financieros, posibles excesos del presupuesto.	Posibles retrasos en 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 $1.000 a $100.000	
	2	De mínima a pequeña reducción en el rendimiento técnico.	El soporte del 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 $1.000	
	2	No hay reducción en el rendimiento	Software fácil de dar soporte.	Posible superávit de presupuesto.	Fecha de entrega fácilmente alcanzable.

		técnico.			

Nota: (1) Posibles consecuencias de errores o defectos del software no detectados.
(2) Posibles consecuencias si el resultado deseado no se consigue.

Tabla 1 -Evaluación del impacto

2.3. 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.

2.3.1. Desarrollo de una tabla de riesgo.

Una tabla de riesgo le proporciona al jefe del proyecto una sencilla técnica para la proyección del riesgo (La tabla de riesgo debería implementarse como un modelo de hoja de cálculo. Esto permite un fácil manejo y ordenación de las entradas.). En la Tabla 2 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 cambiara los requisitos.	PS	80%	2	
La tecnología no alcanzara las expectativas.	TE	30%	1	
Falta de formación en las herramientas.	DE	80%	3	
Personal sin experiencia.	ST	30%	2	
Habrá muchos cambios de personal.	ST	60%	2	

Valores de impacto: 1- catastrófico 2 - critico

3 – marginal 4 - despreciable

Tabla 2 – Ejemplo de una tabla de riesgo.

Un equipo de proyecto empieza por listar todos los riesgos (no importa lo improbables 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 el Epígrafe 2.2.

Cada riesgo es categorizado en la segunda columna (por ejemplo: **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 Tabla 1, 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 (Puede usarse una media ponderada si un componente de riesgo tiene mas influencia en el proyecto) 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. Como muestra la Figura 2, el impacto del riesgo y la probabilidad tienen diferente influencia en la gestión. 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.

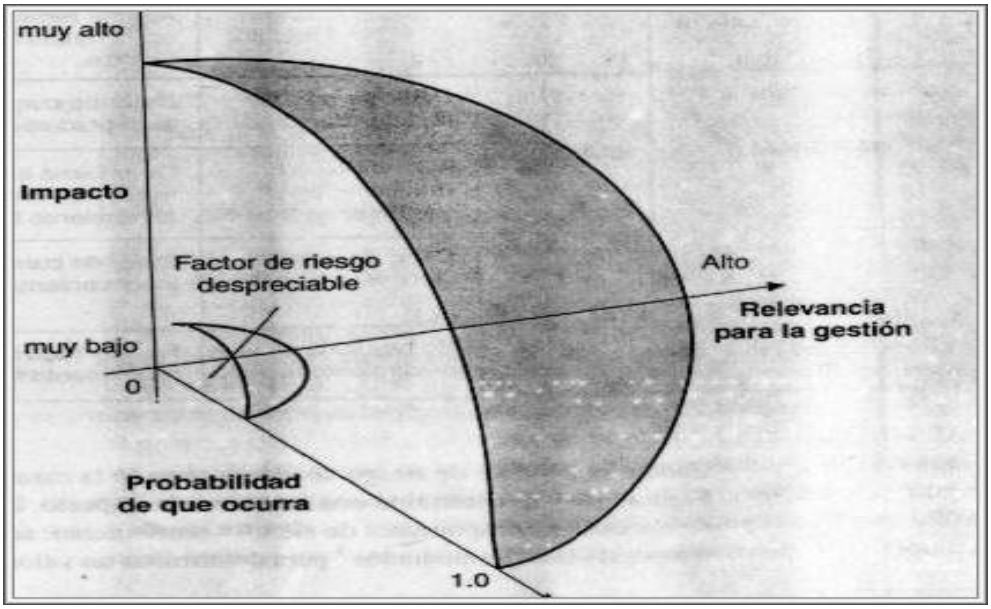

Figura 2 - Riesgos y relevancia para la gestión.

Todos los riesgos que se encuentran por encima de la línea de corte deben ser considerados. La columna etiquetada RSGR (Reducción, Supervisión y Gestión del Riesgo) contiene una referencia que apunta hacia *un Plan de reducción, supervisión y gestión del riesgo,* o alternativamente, a un informe del riesgo desarrollado para todos los que se encuentran por encima de la línea de corte. El plan RSGR y el informe se detalla en el epígrafe 2.7

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 [1]. 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 (por ejemplo: una probabilidad del 0.7 al 1.0 implica un riesgo muy probable).

2.3.2. Evaluación del impacto del riesgo.

Tres factores afectan a las consecuencias probables de un riesgo, si ocurre: su naturaleza, su alcance y cuando ocurre: 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 [1], 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 exposición al riesgo en general, ER, se determina utilizando la siguiente relación [10]:

$$ER = P * C$$

donde *P* es la probabilidad de que ocurra un riesgo, y *C* es el coste del proyecto si el riesgo ocurriera.

Por ejemplo, supongamos que el quipo del proyecto define un riesgo para el proyecto de la siguiente manera:

Identificación del riesgo: Solo el 70 % de los componentes del software planificados para reutilizarlos pueden, de hecho, integrarse en la aplicación. La funcionalidad restante tendrá que ser desarrollada de un modo personalizado.

Probabilidad del riesgo: 80% (probable).

Impacto del riesgo: 60 componentes de software reutilizables fueron planificados. Si solo el 70% pueden usarse, 18 componentes tendrán que desarrollarse improvisadamente (además de otro software personalizado que ha sido planificado para su desarrollo). Puesto que la media por componentes es 100 LDC y los datos locales indican que el coste de la ingeniería del software para cada LDC es de $ 14.000; el coste global (impacto) para el desarrollo de componentes seria 18 * 100 * 14 + $25.200

Exposición al riesgo: ER = 0.80 * 25.200 ~ $20.200

La exposición al riesgo se puede calcular para cada riesgo en la tabla de riesgos, una vez que se ha hecho una estimación del coste del riesgo. La exposición al riesgo total para todos los riegos (sobre la línea de corte en la tabla de riesgos) puede proporcionar un significado para ajustar el coste final estimado para un proyecto. También puede ser usado para predecir el incremento probable de recursos de plantilla necesarios para varios puntos durante la planificación del proyecto.

La proyección del riesgo y las técnicas de análisis descritas en los epígrafes 2.3.1 y 2.3.2 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.

2.3.3. Evaluación de riesgo

En este punto del proceso de gestión del riesgo, hemos establecido un conjunto de ternas de la forma [6]:

$$[r_i , l_i , x_i]$$

donde r_i es el riesgo, l_i es la probabilidad del riesgo y x_i es 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 riegos 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*. [6] 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 3 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.

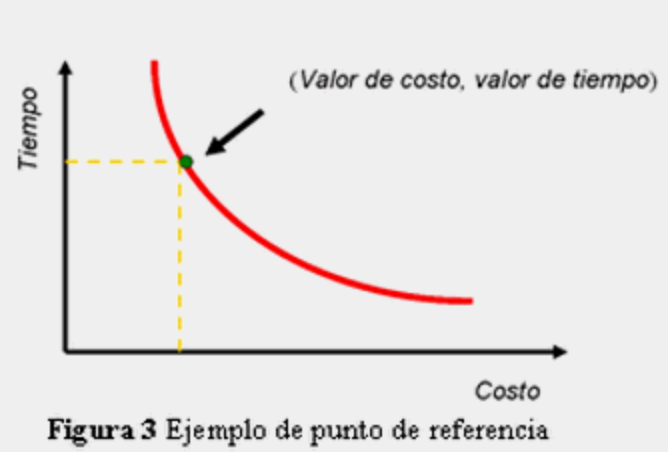

Figura 3 Ejemplo de punto de referencia

Figura 3 – Nivel de referencia de 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, es decir, intentar predecir una decisión de gestión basándose en la combinación de valores de referencia es a menudo imposible. Por lo 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.

2.4. Refinamiento del riesgo

Durante las primeras etapas de la planificación del proyecto, un riesgo puede ser declarado de un modo muy general. Con el paso del tiempo y con el aprendizaje sobre el proyecto y sobre el riesgo, es posible refinar el riesgo en un conjunto de riesgos mas detallados, cada uno algo más fácil, supervisar y gestionar.

Una forma de hacer esto es presentar el riesgo de la forma *condición-transición-consecuencia* (CTC) [9]. Es decir, el riesgo se presenta de la siguiente forma:

Dada esta <condición> entonces existe preocupación por (posiblemente) <consecuencia>.

Utilizando el formato CTC para volver a utilizar el riesgo presentado en el epígrafe 2.5.2, podemos escribir:

Dado que todos los componentes reutilizables del software deben ajustarse a los estándares específicos del diseño y que algunos no lo hacen, es entonces preocupante que (posiblemente) solo el 70% de los módulos planificados para reutilizar puedan realmente integrarse en el sistema que se esta construyendo, teniendo como resultado la necesidad de que el ingeniero tenga que construir el 30% de los componentes restantes.

La condición general que acabamos de destacar puede ser refinada de la siguiente manera:

Subcondición 1: Ciertos componentes reutilizables fueron desarrollados por terceras personas sin el conocimiento de los estándares internos de diseño.

Subcondición 2: El estándar de diseño para interfaces de componentes no ha sido asentado y puede no ajustarse a ciertos componentes reutilizables existentes.

Subcondición 3: Ciertos componentes reutilizables han sido implementados en un lenguaje no soportado por el entorno para el que el sistema ha sido construido.

Las consecuencias relacionadas con estas subcondiciones refinadas siguen siendo las mimas (por ejemplo el 30% de los componentes del software deben ser construidos de un modo personalizado), pero el refinamiento ayuda a aislar los riegos señalados y puede conducir a un análisis y respuesta mas sencilla.

2.5. Reducción, supervisión y gestión del riesgo

Todas las actividades de análisis de riesgo investigadas 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
- 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, r_i. Basándose en casos anteriores y en la intuición de gestión, la probabilidad, li, de mucha movilidad se estima en un 0.70 (70%, bastante alto) y el impacto, xi, está previsto en el nivel 2. Esto es, un gran cambio puede tener 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 ejemplo: 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 desarrollar técnicas que aseguren la continuidad cuando se vaya la gente
- Organizar los equipos del proyecto de manera que la información sobre cada actividad de desarrollo esté ampliamente dispersa.
- Definir estándares de documentación y establecer mecanismos para estar seguro de que los documentos se cumplimentan puntualmente.
- Convocar 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 copias de seguridad disponibles, 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 30 ó 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 (por ejemplo: el 80 por ciento de la probabilidad de fracaso del proyecto) se debe solamente al 20 por ciento de los riegos 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 ejemplo, riesgos que conducen a una exposición al riesgo alta).

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).

2.6. 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 menudo 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.

2.7. 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 [16].

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

Algunos equipos de software no desarrollan un documento RSGR formal. Más bien, cada riesgo se documenta utilizando una *hoja de información de riesgo (HIR)* [19]. En la mayoría de los casos, la *HIR* se mantiene utilizando un sistema de base de datos, por lo que la creación y entrada de información, ordenación por prioridad, búsquedas y otros análisis pueden ser realizados con facilidad. El formato de la HIR se muestra en la Tabla 3.

Hoja de información de riesgo			
Id. Riesgo: P02-4-32	Fecha: 5/9/02	Probabilidad: 80%	Impacto: alto

Descripción:

Solo el 70 por 100 de los componentes del software planificados para reutilizar pueden de hecho, integrarse en la aplicación.

La funcionalidad restante tendrá que desarrollarse de un modo personalizado.

Refinamiento/contexto:

Subcondición1: Ciertos componentes reutilizables fueron desarrollados por terceras personas sin el conocimiento de los estándares internos de diseño.

Subcondición 2: El estándar de diseño para interfaces de componentes no ha sido asentado y puede no ajustarse a ciertos componentes reutilizables existentes.

Subcondición 3: Ciertos componentes reutilizables han sido implementados en un lenguaje no soportado por el entorno para el que el sistema ha sido construido.

Reducción/Supervisión:

1. Contactar con terceras personas para determinar la conformidad con los estándares de diseño.
2. Presionar para completar los estándares de la interfaz; considerar la estructura de componentes cuando se decide el protocolo de la interfaz.
3. Comprobación para determinar los componentes en la categoría de subcondición 3; comprobación para determinar si se puede adquirir el soporte del lenguaje.

Gestión/Plan de Contingencia/Acción

Se calcula que la Exposición al Riesgo (ER) es de $20,200. Esta cantidad se coloca

dentro del coste de contingencia del proyecto. La planificación del proyecto revisado asume que se tendrán que construir 18 componentes adicionales; por consiguiente se asignara el personal de acuerdo con las necesidades. Acción: Las fases de reducción se llevaran a cabo a partir de 7/1/02	
Estado actual: 5/10/02: fases de reducción iniciadas.	
Autor: John Gagne	Asignado: B. Laster

Tabla 3 - Hoja de información de riesgo.

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 riesgo(s) ocasionaron tal problema a lo largo de todo el proyecto.

Cuando se pone mucho en juego en un proyecto de software el sentido común nos aconseja realizar un análisis de riesgo. Y sin embargo, la mayoría de los jefes de proyectos lo hacen informal y superficialmente, si es que lo hacen. El tiempo invertido identificando, analizando y gestionando el riesgo merece la pena por muchas razones: menos trastornos durante el proyecto,

una mayor habilidad de seguir y controlar el proyecto y la confianza de planificar estos problemas antes de que ocurran.

El análisis de riesgos puede absorber una cantidad significativa del esfuerzo de planificación del proyecto, pero el esfuerzo merece la pena.

Capítulo 3

Propuesta de procedimiento

De acuerdo con [16], la administración o gestión de riesgos es un proceso iterativo que se aplica durante todo el proyecto y se desarrolla en cuatro etapas; y los resultados de esta deben ser documentados en un plan de administración de riesgos. La Figura 4 refleja el procedimiento.

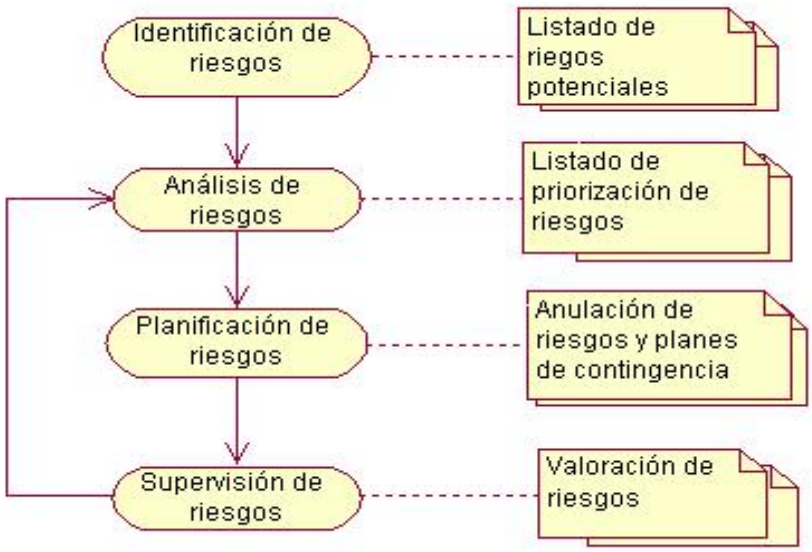

Figura 4- Procedimiento de gestión de riesgo según Pressman.

En [8] se define el paradigma de la gestión del riesgo del SEI, con un proceso de seis actividades, como se observa en la Figura 5, que deben ser desarrolladas de forma continua a lo largo de todo el ciclo de vida del proyecto.

Figura 5 - Procedimiento de gestión de riesgo según Gallagher.

Otra diferencia con el proceso de gestión propuesto en [16], es que en este son incluidas las actividades de vigilancia y comunicación, que mantendrá información y retroalimentación acerca del proceso de gestión de riesgos, del estado de los riesgos atenuados, vigilados y emergentes (nuevos). Considera que las fuentes de información de riesgos pueden ser internas o externas al proyecto.

Como se puede apreciar existen varios modelos de Gestión de Riesgos pero el más aceptado y el que guiará esta investigación consta de cinco pasos (Identificación, Análisis, Planificación, Seguimiento y Control) secuenciales e interactivos, en forma paralela a estos existen dos actividades comunes a ellos: las de documentación y comunicación (véase Figura 6 **-** Modelo de Gestión de Riesgos y Tabla 4 – Descripción del modelo de Gestión del Riesgo).

Este modelo identifica las funciones fundamentales de la gestión de riesgo que deben tenerse en cuenta y emplearse para manejar el riesgo eficazmente: Identificación, Análisis, Planificación, Seguimiento, Control, Documentación y Comunicación. Cada una de estas funciones se definirá con más detalle en el epígrafe 3.1.8

Figura 6 - Modelo de Gestión del Riesgo

Funciones	Descripción
Identificación	Localiza los riesgos antes que estos afecten adversamente el proyecto.
Análisis	Analiza la información que brinda los riesgos.
Planificación	Traduce la información de los riesgos en decisiones y acciones (presentes y futuras) a implementar.
Seguimiento	Monitorea los indicadores de riesgo y las acciones tomadas con cada riesgo.
Control	Corrige desviaciones en las acciones de riesgo planeadas.
Documentación	Proporciona visibilidad y datos de la regeneración externa e

Y Comunicación	interna del programa mientras se va desarrollando y mientras se va saliendo de las actividades de riesgo.

Tabla 4 - Descripción del Modelo de Gestión del Riesgo

3.1. Descripción del procedimiento

3.1.1. Vista General

En la figura 7 se muestra una vista general del procedimiento de gestión de riesgo, la cual indica que el procedimiento se desarrolla de una manera secuencial, aunque existen típicamente iteraciones entre sus pasos. Y en la Figura 5 se muestra el Modelo de Gestión del Riesgo.

3.1.2. Responsabilidades especiales

Las responsabilidades recaen sobre los integrantes de la plantilla del proyecto, de la cual son seleccionados para participar en el Equipo de Evaluación del Riesgo (EER). Este equipo debe tener de uno a 6 integrantes (ingenieros de software), ellos analizan y documentan cualquier riesgo asociado con las tareas que el proyecto debe realizar.

Los siguientes criterios deben tenerse en cuenta a la hora de seleccionar a los integrantes:

- representación de cualquier área funcional considerada como crítica del proyecto.
- mezcla de personas que ocupen diferentes roles en el proyecto (desarrollador, pruebas, etc.)

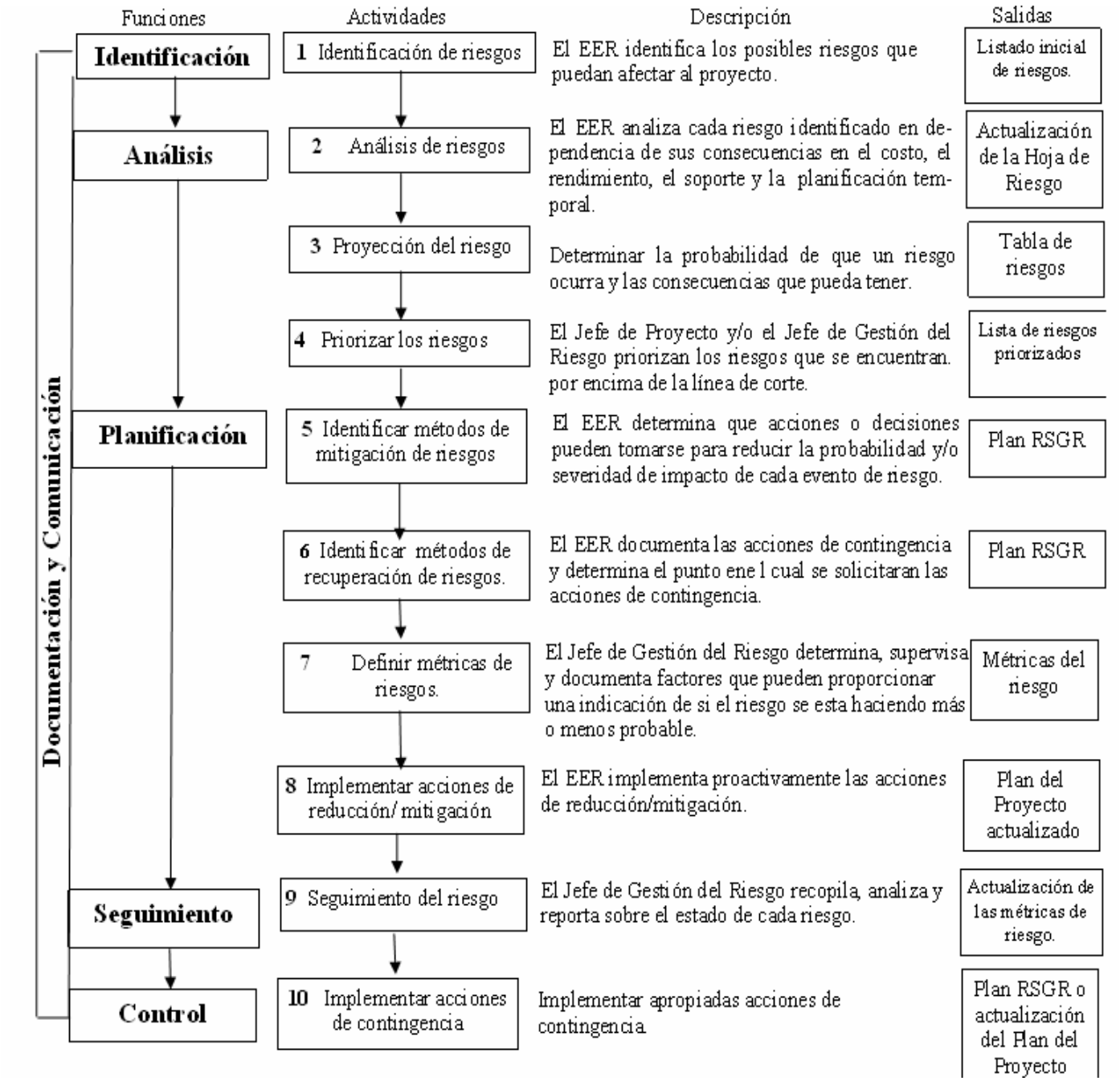

Figura 7– Vista general del procedimiento propuesto

3.1.3. Entradas

Las entradas son elementos que deben estar disponibles para comenzar el procedimiento de gestión de riesgo. Son usadas por los pasos del procedimiento y transformadas en salidas. Ejemplos de entradas son:

a. Hoja de información de riesgos
b. Plan de Proyecto
c. Estándares organizacionales, practicas, líneas de corte relacionadas con el proyecto

3.1.4. Criterios de Entrada

Los criterios de entrada son aquellos elementos que deben completarse antes de comenzar las actividades de la gestión de riesgo para poder lograr un éxito rotundo. Ejemplos de criterios de entrada son:

- la dirección proporcionará recursos adecuados para las actividades de gestión de riesgo (personal, herramientas, etc.)
- se le ha asignado al personal los roles y responsabilidades de la gestión del riesgo, y han sido entrenados para un acercamiento a la gestión del riesgo que se aplicará en el proyecto.

3.1.5. Salidas

Las salidas son aquellos elementos que permanecen en los archivos del proyecto después de que el proyecto se ha completado. Ejemplos de salidas son:

a. Plan de Gestión de Riesgos.
b. Tabla de Riesgos.
c. Hoja de información de riesgo o similar.

d. Plan RSGR.
e. Métricas del riesgo.
f. Actualización del Plan del Proyecto

3.1.6. Criterios de Salida

Son revisados los resultados del análisis del riesgo, el Plan de Gestión del Riesgo y el acuerdo general del EER sobre el alcance que tendrán los Riesgos Claves.

Las actividades finales en los eventos de análisis del riesgo son la presentación de los resultados y una reunión con el Jefe de Proyecto. La presentación es generalmente dirigida para todo el personal del proyecto. Todos los participantes deben asistir a la reunión e informarles a estos que sucedió con los riesgos que ellos identificaron. Un ejemplo de una presentación seria:

- Revisar los procesos de valoración del riesgo
- Hacer una revisión completa de la base de datos de riesgos con sus atributos.
- Discutir los Riesgos Claves.
- Identificar los eventos de contingencia y realizar una sinopsis de cada plan asociado a una acción.

3.1.7. Roles y responsabilidades

A continuación se mencionan los roles del EER con sus correspondientes responsabilidades.

1. *Vicedecano de Producción:* Tiene una responsabilidad global sobre varios proyectos y proporciona el apoyo para las actividades de gestión del riesgo pero no forma parte del EER.
2. *Jefe de Proyecto*: Tiene una responsabilidad general sobre el manejo de los riesgos asociados al desarrollo y mantenimiento del sistema; y asegura que la gestión del riesgo se esta realizando de acuerdo al proceso descrito.

3. *Jefe de Gestión del Riesgo*: Puede ser escogido por el Jefe de Proyecto dependiendo del tamaño de la plantilla y la complejidad del proyecto. Es responsable de asegurar la Gestión del Riesgo como se describe en el Plan de Gestión del Riesgo.
4. *Facilitador de la Evaluación del Riesgo*: Es la persona que no tiene un interés marcado en los resultados del proceso y puede llevarlo efectivamente al cierre. Esta persona puede ser un ingeniero calificado en el proyecto
5. *Controlador de la Calidad*: Es el encargado de revisar periódicamente las actividades de la gestión del riesgo para asegurar que los requerimientos de la organización se están siguiendo.

3.1.8. Procedimiento

El procedimiento de gestión de riesgos esta constituido por 10 pasos, los cuales se detallarán más adelante. El desarrollo de las actividades asociadas a cada uno de estos pasos constituye un acercamiento aceptable a la gestión del riesgo y pueden ser incorporadas al Plan de Gestión del Riesgo. El tamaño, visibilidad o consecuencias del proyecto influyen en la complejidad del procedimiento.

Función 1: Identificación

Los riesgos deben ser identificados antes que estos se conviertan en problemas que afecten adversamente el proyecto. Establecer un ambiente ameno, el cual anime a las personas a expresar sus preocupaciones y problemas sobre el proceso en cuestión, y realizar las revisiones de calidad a lo largo de todas las fases del proyecto son técnicas comunes y efectivas para identificar riesgos.

Debe comenzar con el análisis de los riesgos genéricos, que constituyen una amenaza potencial para todos los proyectos de software, que puedan estar presentes en el proyecto en curso. Después se deben identificar los riesgos específicos, que implican un conocimiento profundo del

proyecto, y están relacionados con el entorno de desarrollo, la tecnología, la experiencia y el tamaño del equipo.

Paso 1: Identificación de riesgos

El Facilitador proporcionará una lista de elementos potenciales de riesgos a los integrantes del EER y/o a los clientes. Este documento esta derivado de una lista de posibles riesgos mostrados en la Tabla 5 y detallados cada uno en el Epígrafe 2.2.1

Listado de Riesgos	**Categorías de riesgos**	**Descripción**
Rotación de personal	Plantilla	Personal con experiencia abandona el proyecto antes de que finalice
Subestimación del tamaño	Software	El tamaño del requisito se ha subestimado

Categorías:

1. Riesgos del tamaño del software
2. Riesgos del impacto en el negocio
3. Riesgos relacionados con el cliente
4. Riesgos del proceso
5. Riesgos tecnológicos
6. Riesgos del entorno de desarrollo
7. Riesgos asociados con el tamaño de la plantilla

Tabla 5 – Ejemplo de descripción de riesgos por categoría.

La identificación de riegos es una responsabilidad individual, siendo de vital importancia para el equipo realizar una sesión de identificación de riesgos en la cual cada integrante o cliente expondrá los posibles riesgos que el considere que pueden afectar al proyecto, permitiendo que el listado de riesgos aumente o disminuya en dependencia de la opinión del equipo.

La Hoja de Información de Riesgo, ver ejemplo en la Figura 8, es usada para documentar todos los riesgos potenciales.

<table>
<tr><th colspan="4">Hoja de información de riesgo</th></tr>
<tr><td>Id. Riesgo: P02-4-32</td><td>Fecha: 5/9/02</td><td>Probabilidad: 80%</td><td>Impacto: alto</td></tr>
<tr><td colspan="4">Descripción:

Solo el 70 por 100 de los componentes del software planificados para reutilizar pueden de hecho, integrarse en la aplicación.

La funcionalidad restante tendrá que desarrollarse de un modo personalizado.</td></tr>
<tr><td colspan="4">Refinamiento/contexto:

Subcondición1: Ciertos componentes reutilizables fueron desarrollados por terceras personas sin el conocimiento de los estándares internos de diseño.

Subcondición 2: El estándar de diseño para interfaces de componentes no ha sido asentado y puede no ajustarse a ciertos componentes reutilizables existentes.

Subcondición 3: Ciertos componentes reutilizables han sido implementados en un lenguaje no soportado por el entorno para el que el sistema ha sido construido.</td></tr>
<tr><td colspan="4">Reducción/Supervisión:</td></tr>
</table>

4. Contactar con terceras personas para determinar la conformidad con los estándares de diseño. 5. Presionar para completar los estándares de la interfaz; considerar la estructura de componentes cuando se decide el protocolo de la interfaz. 6. Comprobación para determinar los componentes en la categoría de subcondición 3; comprobación para determinar si se puede adquirir el soporte del lenguaje.
Gestión/Plan de Contingencia/Acción Se calcula que la Exposición al Riesgo (ER) es de $20,200. Esta cantidad se coloca dentro del coste de contingencia del proyecto. La planificación del proyecto revisado asume que se tendrán que construir 18 componentes adicionales; por consiguiente se asignara el personal de acuerdo con las necesidades. Acción: Las fases de reducción se llevaran a cabo a partir de 7/1/02
Estado actual: 5/10/02: fases de reducción iniciadas.

Autor: John Gagne	Asignado: B. Laster

Figura 8 - **Hoja de información de riesgo**

Puede ser beneficioso tener una persona encargada de llevar un control de los riesgos que han sido capturados. Este paso no debe durar más de una semana.

Como la gestión de riesgos es un proceso continuo, la identificación no es un evento que se debe hacer por una sola vez; debe realizarse de forma regular durante toda la vida del proyecto.

Función 2: Análisis

El proceso de Análisis estudia la información que brindan los riesgos. Esto incluye revisarlo, priorizarlo, y seleccionar los riesgos críticos para trabajarlos.

Paso 2: Analizar los riesgo

El equipo debe de realizar una evaluación global del riesgo del proyecto para estimar el nivel de éxito del proyecto. Debe consultarse el epígrafe 2.2.2

El EER analiza cada riesgo identificado en dependencia de las consecuencias que pueda tener en los siguientes componentes de riesgo: costo, rendimiento, soporte y planificación temporal (estos componentes pudiesen incluirse en la Hoja de Información). Un riesgo puede tener impacto en más de una de estas categorías. Por ejemplo, frecuentemente cambian los requerimientos, este riesgo tendrá impacto en las 4. Debe consultarse el Epígrafe 2.2.3. El Facilitador nuevamente puede solicitar al equipo otros riesgos que ellos consideren necesario documentar.

Paso 3: Proyección del riesgo

Este paso consiste en determinar la probabilidad de que un riesgo ocurra y las consecuencias que puede tener.

El jefe de proyecto, conjuntamente con el equipo del proyecto, llena la Tabla de riesgo (véase un ejemplo en la Tabla 2) colocando en ella todos los riesgos identificados en el Paso 1 y determinando su categoría, probabilidad e impacto, dejando para otro paso la columna etiquetada con RSGR. Debe consultarse el Epígrafe 2.3.1 Pudiera colocarse también como otra columna la duración (por cuanto tiempo se manifiesta).

Cada riesgo se considera por separado y se valora en intervalos su probabilidad e impacto:

- probabilidad del riesgo valorada como: *muy bajo* (<10%), *bajo* (10-25%), *moderado* (25-50%), *alto* (50-75%) o *muy alto* (>75%)
- efectos del riesgo valorados como *catastrófico*, *serio*, *tolerable* o *insignificante*.

Paso 4: Priorizar los riesgos

Una vez que se han completado las cuatro primeras columnas de la tabla de riesgo, la tabla es ordenada por probabilidad o 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 y/o el Jefe de Gestión del Riesgo estudian la tabla ordenada resultante y definen una línea de corte*. La línea de corte* 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. Debe consultarse el Epígrafe 2.3.1

Función 3: Planificación

La planificación convierte la información que brinda los riesgos en decisiones y acciones a tomar tanto en el presente como en el futuro, esta envuelve el desarrollo de acciones para dirigir riesgos individuales, la priorización de acciones de riego y la creación de un Plan de Gestión del Riesgo. Un plan para gestionar un riesgo puede ser:

- Mitigar el impacto del riesgo reduciendo el Nivel del Riesgo.
- Desarrollar una estrategia de contingencia en caso de que el riesgo ocurra.

Paso 5: Identificar métodos de mitigación de riesgos

Es necesario que el EER tenga una sesión para determinar que acciones o decisiones pueden tomarse para reducir la probabilidad y/o severidad de impacto de cada evento de riesgo. En caso de que se acepte continuar con el proyecto, el equipo documenta y detalla aquellos que son prácticos y factibles, y los incorpora al Plan de Gestión del Riesgo. Por ejemplo, se determina que existe mucha movilidad en la plantilla del proyecto, algunas acciones serian:

- Reunirse con la plantilla actual y determinar las causas de la movilidad (por ejemplo: malas condiciones de trabajo, salarios bajos, mercado laboral competitivo)
- Una vez que comienza el proyecto, asuma que habrá movilidad y desarrollar técnicas que aseguren la continuidad cuando se vaya la gente.
- Organizar los equipos del proyecto de manera que la información sobre cada actividad de desarrollo esté ampliamente dispersa.

Para más detalle debe consultarse el epígrafe 2.5

Paso 6: Identificar métodos de recuperación de riesgos

Para cada riesgo que se encuentra por encima de la línea base de la tabla de riesgo, el EER realiza una sesión para validar la naturaleza del evento que traería consigo determinada acción de contingencia. Las acciones de contingencia contra esos riesgos son documentadas en el Plan de Gestión del Riesgo junto con aquellas circunstancias notables o medibles que deben ocurrir para desarrollar la implementación de las acciones de contingencia.

Paso 7: Definir métricas de riesgos

El Jefe de Gestión del Riesgo conjuntamente con el EER determina, supervisa y documenta factores que pueden proporcionar una indicación de si el riesgo se esta haciendo mas o menos probable. En este 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 de Gestión del Riesgo debería supervisar también la efectividad de los pasos de reducción del riesgo. Debe consultarse el epígrafe 2.5

Adicionalmente, el EER define y documenta las medidas del proceso de gestión de riesgos a ser reunidas y analizadas en el propio proceso de riesgo.

Paso 8: Implementar acciones de reducción/ mitigación

Para cada riesgo, el EER conduce las actividades necesarias para implementar las acciones de reducción/mitigación mencionadas anteriormente en el paso 5. Estas actividades están documentadas en el Plan de Gestión de Riesgos para cada escenario de reducción de riesgo. Ejemplos de actividades que dirigirían los niveles de riesgo definidos en el Paso 4 son:

- Riesgo Tolerable (Tolerable Risk): Buenas prácticas de ingeniería de sistemas pueden servir para mitigar cualquier problema de esta magnitud.
- Riesgo Bajo (Low Risk): No se requiere realizar énfasis en un determinado programa en especial, puede emplearse un software normal de ingeniería de grupo, monitoreo y control.
- Riesgo Medio (Medium Risk): Este nivel de riesgo pudiera calificar como un elemento de acción en las reuniones de revisión.
- Riesgo Alto (High Risk): Este nivel de riesgo califica como un elemento de acción en reuniones de revisión.

- Riesgo Intolerable (Intolerable Risk): Este nivel requiere de un control formal y el monitoreo y desarrollo de una acción de contingencia. Cada riesgo en este nivel tiene una definición del evento que debe invocar la acción de contingencia.

Los ejemplos anteriores se basan en la clasificación de riesgos de la siguiente forma:

- Tolerable (**T**olerable): es una condición donde el riesgo se identifica por tener poca o ninguna consecuencia sobre los objetivos del proyecto; la probabilidad de ocurrencia es lo suficientemente baja como para preocuparse poco o no preocuparse.
- Bajo (**L**ow): es una condición donde el riesgo se identifica por tener efectos menores en los objetivos del proyecto; la probabilidad de ocurrencia es lo suficientemente baja como para no preocuparse.
- Medio (**M**edium): es una condición donde el riesgo se identifica como un factor que posiblemente pueda afectar los objetivos del proyecto, el costo o la planificación; la probabilidad de ocurrencia es lo suficientemente alta que requiere controlar de cerca todos los factores contribuyentes.
- Alto (**H**igh): es una condición donde el riesgo se identifica por tener una alta probabilidad de ocurrencia y sus consecuencias podrían afectar los objetivos del proyecto, el costo y la planificación. La probabilidad de ocurrencia es lo suficientemente alta que requiere controlar de cerca todos los factores contribuyentes, el establecimiento de acciones de riesgo, y una aceptable posición de respaldo.
- Intolerable (**IN**tolerable): es una condición donde el riesgo se identifica por tener una alta probabilidad de ocurrencia y sus consecuencias tendrán un impacto significativo en el costo, planificación y/o rendimiento. Estos riesgos constituyen los Riesgos Claves para el proyecto.

Función 4: Seguimiento

Paso 9: Seguimiento del riesgo

El Jefe de Gestión del Riesgo recopila, analiza y reporta sobre el estado de cada riesgo como determina el proceso definido paso 7. El método y el tiempo de reunir y reportar cada métrica son incorporados en el Plan de Gestión del Riesgo. Cada riesgo y su métrica asociada son reportadas de acuerdo al plan implementado

El informe oportuno de medidas asegura que están siguiéndose los procedimientos especificados en el plan, y las métricas derivadas se están computarizando. El Jefe de Gestión del Riesgo recibe y analiza los informes, se asegura que han sido archivados y toma las acciones correctivas requeridas.

Función 5: Control

El control del riesgo es una parte de la gestión del proyecto y cuenta con los procesos de gestión del proyecto para controlar los planes de acción de riesgo, corregir las variaciones de los planes y mejorar el proceso de gestión del riesgo. Las actividades de control del riesgo son documentadas en el Plan de Gestión del Riesgo.

Paso 10: Implementar acciones de contingencia.

Para cada riesgo, si los datos reunidos muestran que los criterios de entrada están disponibles, entonces:

- el Jefe de Proyecto debe implementar las acciones de contingencia, y
- la dirección del proyecto necesita proporcionar y reasignar los recursos requeridos para la ejecución de las acciones de contingencia.

Para desarrollar el Plan RSGR o Plan de Contingencia véase el epígrafe 2.7

Función 6: Documentación y Comunicación

La documentación y la comunicación ocurren a lo largo de todas las funciones de la gestión del riesgo. Son parte integra de todas las actividades de la gestión de riesgo. Sin estas no podría realizarse un acercamiento viable a la gestión del riesgo.

Claramente el personal asociado con el proyecto es el más calificado para identificar riesgos en su trabajo. La gestión del proyecto debe proporcionar un ambiente conducente para que las personas compartan sus preocupaciones con respecto a los riesgos potenciales.

Una efectiva comunicación proporciona visibilidad y datos de la regeneración, tanto interna como externa del programa sobre las actividades actuales.

3.2. Valoración de especialista.

A continuación se presenta una valoración del procedimiento propuesto con el objetivo de validar el resultado de esta investigación. Esta valoración se realizo mediante una entrevista a especialistas conocedores del objeto de estudio.

Nombre: Eugenia G. Muñiz Lodos
Título: MSc. En Sistemas Digitales
Cargos: Profesor Titular Adjunto de la UCI e Investigador Auxiliar del ICID
Centros de trabajo: UCI e ICID

Valoración: El entrevistado en su centro de trabajo ha empleado la gestión de riesgos como método efectivo para mantener la calidad del software que se produce y en su tarea como Profesor titular Adjunto ha identificado riesgos importantes cuando en los proyectos del ICID intervienen estudiantes de la universidad.

Considera que el procedimiento cumple con las etapas fundamentales que caracterizan a una buena Gestión del Riesgo (Identificación, Análisis y Mitigación), y que puede ser una vía efectiva para controlar los riesgos en los proyectos productivos de la universidad, principalmente los de la facultad.

Nombre: Roberto Francia Manzano

Título: Técnico Medio en Computación.

Cargos: Subdirector del Departamento Técnico del Aguas de La Habana.

Centro de trabajo: Aguas de la Habana.

Valoración: El entrevistado ha realizado varias investigaciones sobre la Gestión de Riesgo tanto a nivel tecnológico como enfocada a la producción del software y ha llegado a la conclusión de que este proceso es de vital importancia, ya que permite planificar y prevenir los posibles riesgos, evitando retrasos en los tiempos de entrega, problemas de calidad ene l producto, pobre estimación de los recursos o en el peor de los casos, riesgos que pueden afectar la culminación del proyecto.

Cree que administrar los riesgos por medio de un proceso de desarrollo de software predecible provee un fundamento para desarrollar en forma consistente un mejor software, mas rápidamente y a un menor costo. Empezando con esta base, expresa que se podrán adoptar técnicas y herramientas para lograr que los desarrolladores sean más productivos, para elevar la calidad del software.

Considera que el procedimiento pudiera ser de gran ayuda para la gestión de riesgos en proyectos de producción de software pues explica detalladamente todas aquellas actividades que deben realizarse en cada etapa de este proceso, y que los artefactos que de ellas se generan sirven para ir detallando y controlando todos los riesgos que van surgiendo. Cree relevante la creación de un Equipo de Evaluación del Riesgo que entre sus tareas principales este la de identificar y analizar los riesgos, destacando que este proceso también pudiera ser realizado por el personal encargado de supervisar la calidad del producto.

Conclusiones

El trabajo de Diploma fue desarrollado siguiendo las etapas propuestas por el SEI, y tal como se esperaba las mismas contribuyeron como guía en la ejecución de un eficaz procedimiento para la gestión de riesgos en los proyectos productivos de la UCI que presenta de manera ordenada y detallada las actividades y tareas que corresponden a cada una de esas etapas.

El principal aspecto a destacar lo constituye el hecho de haber alcanzado todos los objetivos propuestos al inicio de la investigación, tanto a nivel metodológico como académico y técnico dentro de los plazos establecidos.

Otro aspecto a mencionar es que el empleo del procedimiento para el desarrollo y aplicación de la Gestión del Riesgo en proyectos de producción de software en la UCI logrará desarrollar e implementar anticipadamente respuestas apropiadas a problemas o dificultades que puedan surgir en los proyectos.

Cabe destacarse además que no solo se desarrolla y detalla este procedimiento sino que se brinda una extensa información sobre los riesgos más frecuentes así como las categorías más relevantes, permitiendo clasificarlos y para luego proceder a su tratamiento.

Finalmente, la continua y progresiva consulta y validación de todas las actividades realizadas, de las conclusiones obtenidas y los documentos generados, ha demostrado que este procedimiento es un efectivo mecanismo de aseguramiento de la calidad del software.

Recomendaciones

Entre las futuras líneas de trabajo para el procedimiento producido se encuentran:

- Creación de una aplicación que posibilite la gestión del riesgo en los proyectos de la universidad (puede estar conectada a una amplia base de datos).
- Realizar una base de datos con la mayor cantidad de riesgos conocidos y sus categorías, donde también se puedan almacenar y documentar las *hojas de información de riesgo.*
- Consultar esta tesis e incluir este procedimiento o parte de el en las actividades que debe desarrollar el planificador y el líder de un proyecto productivo ya que una mala gestión del riesgo puede afectar negativamente la planificación temporal de un proyecto.

Bibliografía

- Fuente, A. y Cueva, J. (2006). Gestión de Riesgos. Consultado en Enero 24, 2007 en http://www.di.uniovi.es/~aquilino/Asignaturas/ProyectosInformatica/Documentos/Proyectos.v2006.C7.V2.pdf.
- Hernández, R. y Coello, S. (2002). El paradigma cuantitativo de la investigación científica. Ciudad de la Habana: Editorial Universitaria.
- Hernando, S (2005). La gestión del riesgo. HISPASEC Sistemas. Consultado en Abril 5, 2007 en http://www.hispasec.com/.
- Hidalgo Nuchera, A. (2004). Una introducción a la gestión de riesgos tecnológicos. Madrid. Consultado en Abril 5, 2007 en http://www.madrimasd.org/revista/revista23/tribuna/tribuna1.asp
- Humphrey, Watts S. (2005). Introducción al Proceso Software Personal. La Habana: Félix Varela.
- Maniasi, Sebastián (). *Identificación de riesgos de proyectos de software en base a taxonomias*. Consultado en Diciembre 14, 2006 en http://www.itba.edu.ar/capis/webcapis/proyectodetesis
- Pressman, R. (2005). Ingeniria del Software. Un enfoque práctico. La Habana: Félix Varela.
- Pressman, R. (2005). Ingeniería del software. : McGraw - Hill.
- Project Management Institute. (2004). A Guide to the Project Management Body of Knowledge (PMBOK Guide). Newtown Square: Project Management Institute.
- www.buzoneo.info/diccionario_marketing/diccionario_marketing_i.php
- (2007). Risk management. Wikipedia, the free encyclopedia. Consultado en Abril 5, 2007 en http://en.wikipedia.org/wiki/Risk_management.
- http://www.aldion.us/aat.est/esp/deltek-sp.asp

- www.si-web.it/glossario.qualita
- www.buzoneo.info/diccionario_marketing/diccionario_marketing_i.php
- http://www.monografias.com/trabajos41/riesgo-etapa-requisitos/riesgo-etapa-requisitos.shtml

Referencias Bibliográficas

- [1] *Software Risk Abatement*, AFCS/AFLC Pamphlet 800-45, U.S. Air Force, 30 de Septiembre 1988
- [2] Barki, H.A. (1993). Toward an assessment of software development risk. Journal of management Information System risk. Vol. 10, Iss. 2;pg. 203, 23 pgs.
- [3] Boehm, B.: A Spiral Model of Software Development and Enhancement. IEEE Computer. Vol. 21, # 5. 1988.
- [4] Boehm, B., *Software Risk Management*, IEEE Computes Society Press, 1989.
- [5] Boehm, B.W. (1991). Software risk management: principles and practices. IEE Software, pp.32-41.
- [6] Charette, R. N., *Software Engineering Risk Analysis and Management*, Mcgraw-Hill/Intertext, 1989
- [7] Esteves, J., Pastor, J. (2000). Towards the Unification of Critical Success Factors for ERP implementations, 10th Annual BIT conference, Manchester, UK.
- [8] Gallagher, Brian P.: Software Acquisition Risk Management Key Process Area (KPA) — A Guidebook, Version 1.02. Carnegie Mellon University. HANDBOOK CMU/SEI-99-HB-001. 1999.
- [9] Gluch, D.P., <<A Construct for Describing Software Development Risk >>, CMU/SEI-94-TR-14, Software Engineering Institute, 1994.
- [10] Hall, E. M., *Managing Risk: Methods for Software Systems Development*, Addison Wesley, 1998.

- [11] Higuera, R.P, <<Team Risk Management>>, CrossTalk, US Dept. of Defense, Enero 1995, pp. 2-4.
- [12] Humphrey, Watts S. (2005). Introducción al Proceso Software Personal. La Habana: Félix Varela.
- [13] Jones, C. (1998). Minimizing the risks of software development. Cutter IT Journal vol. 11 (6), 13-21.
- [14] Keil, M. et al., <<A Framework for Identifying Software Project Risks>>, CACM, vol 41, No. 11, Noviembre 1998, pp. 76-83.
- [16] Pressman, Roger S. (2005). Ingeniería del Software. Un enfoque Práctico. La Habana: Félix Varela.
- [17] Roppponen, J. and Lyytinen, K.: Components of Software Development Risk: Hot to address Them? IEEE transactions on software engineering, 26(2). 2000.
- [18] *Software Engineering Institute*. Disponible en http://www.sei.cmu.edu/programs/sepm/risk. Página vigente al 24-Jul-2005.
- [19] Williams, R.C., J.A. Walker y A.J. Dorofee, <<Putting Risk Management into Practice>>, *IEEE Software*, Mayo 1997, pp. 75-81.

Glosario de términos

A

- **Actividades:** Es la suma de tareas, normalmente se agrupan en un procedimiento para facilitar su gestión. La secuencia ordenada de actividades da como resultado un subproceso o un proceso. Normalmente se desarrolla en un departamento o función.
- **Aplicaciones:** Programas con los cuales el usuario final interactúa, es decir, son aquellos programas que permiten la interacción entre el usuario y la computadora.
- **Archivos:** Agrupación de información que puede ser manipulada de forma unitaria por el sistema operativo de un ordenador.
- **Artefactos:** Productos tangibles del proyecto que son producidos, modificados y usados por las actividades. Pueden ser modelos, elementos dentro del modelo, código fuente y ejecutables.

B

- **Base de datos:** Una base de datos es un conjunto de datos que pertenecen al mismo contexto, almacenados sistemáticamente para su uso posterior. En este sentido, una biblioteca puede considerarse una base de datos compuesta en su mayoría por documentos y textos impresos en papel e indexados para su consulta.

C

- **Calidad:** Una forma de hacer las cosas en las que, fundamentalmente, predominan la preocupación por satisfacer al cliente y por mejorar, día a día, procesos y resultados. Una forma de gestión que introduce el concepto de mejora continua en cualquier organización y a todos los niveles de la misma, y que afecta a todas las personas y a todos los procesos.
- **Cliente:** Persona que solicita la creación del software.

- **COBIT:** Modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización, es decir, administradores IT, usuarios y por supuesto, los auditores involucrados en el proceso.
- **Computadora:** Dispositivo electrónico compuesto básicamente de un procesador, una memoria y los dispositivos de entrada/salida (E/S).

D

- **Diagrama de flujo:** Los diagramas de flujo representan la forma más tradicional para especificar los detalles algorítmicos de un proceso. Se utilizan principalmente en programación, economía y procesos industriales; estos diagramas utilizan una serie de símbolos con significados especiales.

E

- **Entradas:** Datos que se deben procesar por medio de un sistema de computación.
- **Estándares:** Son acuerdos documentados que contienen especificaciones técnicas u otros criterios específicos para ser usados como referentes, guías o definiciones de características, para asegurar que materiales, productos, procesos y servicios son obtenidos o han sido realizados de acuerdo a sus propósitos.

F

- **Fases:** Cada uno de los estados sucesivos de una algo que cambia o se desarrolla. Una diferencia verdadera de tiempo.
- **Flujo de trabajo:** Secuencia de actividades realizadas por trabajadores y que produce un resultado de valor observable.

G

- **Gestión de proyectos:** Planificación, proyectos, estadísticas, informes. Es la disciplina de organizar y administrar recursos de manera tal que se pueda culminar todo el trabajo requerido en el proyecto dentro del alcance, el tiempo, y coste definidos.

H

- **Hardware:** Es el conjunto de dispositivos electrónicos que proporciona la capacidad de computación y los dispositivos electromecánicos encargados de extraer o suministrar la información en/de los soportes magnéticos.
- **Herramientas:** Instrumento que ayuda a realizar un trabajo, es decir para fabricar artefactos.

I

- **Interfaz:** Parte de un programa informático que permite a éste comunicarse con el usuario o con otras aplicaciones permitiendo el flujo de información.
- **Ingeniería del software:** Enfoque sistemático del desarrollo, operación, mantenimiento y retiro del software. Rama de la ingeniería que aplica los principios de la ciencia de la computación y las matemáticas para lograr soluciones costo-efectivas (eficaces en costo o económicas) a los problemas de desarrollo de software, es decir, permite elaborar consistentemente productos correctos, utilizables y costo-efectivos.
- **ISO 9001:** Es una organización (conjunto de normas de calidad) establecidas por la Organización Internacional para la Estandarización (ISO) que se pueden aplicar en cualquier tipo de organización (empresa de producción, empresa de servicios, administración publica, entre otras.) Su implantación en estas organizaciones, aunque supone un duro trabajo, ofrece una gran cantidad de ventajas para sus empresas.
- **IT (Information Technologies):** Tecnologías de la Información. Una forma de denominar al conjunto de herramientas, habitualmente de naturaleza electrónica, utilizadas para la recolección, almacenamiento, tratamiento, difusión y transmisión de la información.

- **Iterativo:** Dado que los proyectos software son largos es común dividir el trabajo en miniproyectos. Cada miniproyecto es una iteración que resulta en un incremento. Las iteraciones se refieren a pasos en el flujo de trabajo, y los incrementos a un crecimiento en el producto. Para ser más efectivas las iteraciones deben ser controladas, es decir deben ser seleccionadas y llevadas a cabo de una forma planeada, de forma que cada una de las iteraciones constituye un miniproyecto software.

M

- **Metodología:** Manera de cómo se perciben y conocen los objetos y el conjunto de supuestos teóricos que respaldan al método. Ciencia que estudia los métodos utilizados por el ser humano para encontrar soluciones óptimas a problemas teóricos o prácticos. Describe además los métodos, procedimientos e instrumentos que se han utilizado o se utilizarán para lograr los objetivos propuestos.
- **MSF:** Es un marco de desarrollo que define procesos, principios, modelos, disciplinas, conceptos y practicas contrastadoas por Microsoft.

P

- **Plataforma:** En informática, una plataforma es precisamente el basamento, ya sea de hardware o software, sobre el cual un programa puede ejecutarse. Ejemplos típicos incluyen: arquitectura de hardware, sistema operativo, lenguajes de programación y sus librerías de tiempo de ejecución.
- **PMI (Project Mangement Institute):** es la principal Organización Mundial dedicada a la Dirección de Proyectos. Desde su fundación en 1969, ha crecido hasta convertirse en la mayor organización sin fines de lucro que reúne a más de 200.000 profesionales certificados en todo el mundo. **S**u objetivo principal es establecer estándares de Dirección de Proyectos mediante la organización de programas educativos y administrar de forma global el proceso de certificación de profesionales. Tanto sus estándares como su

Certificación Profesional ha sido reconocida por las principales entidades gubernamentales y privadas del mundo.

- **Proceso:** Un proceso se define como un conjunto de tareas, actividades o acciones interrelacionadas entre sí que, a partir de una o varias entradas de información, materiales o de salidas de otros procesos, dan lugar a una o varias salidas también de materiales (productos) o información con un valor añadido.
- **Procedimiento:** Forma específica de llevar a cabo una actividad. En muchos casos los procedimientos se expresan en documentos que contienen el objeto y el campo de aplicación de una actividad; que debe hacerse y quien debe hacerlo; cuando, donde y como se debe llevar a cabo; que materiales, equipos y documentos deben utilizarse; y como debe controlarse y registrarse.
- **Producto:** Es cualquier cosa que puede ser ofrecida al mercado para su compra, para su utilización o para su consideración. Es cualquier bien, servicio o idea capaz de motivar y satisfacer a un comprador.
- **Proyecto:** Esfuerzo temporal, dirigido a crear un producto, servicio o resultado único.

R

- **Recursos:** Son todos aquellos elementos necesarios, tanto tangibles como intangibles, para que una organización cumpla con sus objetivos.
- **Requerimientos:** Una condición o capacidad que debe estar presente en el sistema o componentes del sistema para satisfacer un contrato estándar, especificación u otro documento formal.
- **RUP (Rational Unified Process):** Es un proceso iterativo e incremental para el desarrollo del software creado por Rational Software.
- **Roles:** Papel que ejerce un actor en una actividad o proyecto.

S

- **Salidas:** Resultado del procedimiento.
- **Sistema:** Conjunto de elementos interrelacionados que trabajan juntos para obtener un resultado deseado.
- **Sistemas de información:** Conjunto de ficheros automatizados, programas, soportes y equipos empleados para el almacenamiento y tratamiento de datos de carácter personal.
- **Scrum:** Modelo ágil no centrado en practicas de programación como XP, sino en practicas de gestión.
- **Sistema Operativo:** Conjunto de programas o software destinado a permitir la comunicación del usuario con un computador y gestionar sus recursos de manera cómoda y eficiente. Comienza a trabajar cuando se enciende el computador, y gestiona el hardware de la maquina desde los niveles mas básicos.
- **Software:** Todos los componentes intangibles de una computadora, es decir, al conjunto de programas y procedimientos necesarios para hacer posible la realización de una tarea específica, en contraposición a los componentes físicos del sistema (hardware).

U

- **Usuario:** Individuo que suele llamarse consumidor, usufructuario, beneficiario o cliente que habitualmente utiliza algo ajeno por derecho o por concesión.

1