**UNIVERSIDAD DE LAS CIENCIAS INFORMÁTICAS**

**Facultad 9**


# GUÍA METODOLÓGICA PARA EL ANÁLISIS DE RIESGOS

**TRABAJO DE DIPLOMA PARA OPTAR POR EL TÍTULO DE INGENIERO EN CIENCIAS INFORMÁTICAS**

**AUTOR:** Jorge Alberto Mora Julián

**TUTORA:** MSc. Yeleny Zulueta Veliz

Ciudad de la Habana, julio de 2008

"Año 50 de la Revolución"

*El futuro pertenece a quienes creen en la belleza de sus sueños.*
*Eleanor Roosevelt*

*A mis padres y mi abuela por lo que representan, a ellos les debo todo lo que soy. A mi hermano Alexander que tanto quiero.*

*A mi abuelo, que siempre está presente...*

*A mi familia, por la confianza que siempre han depositado en mí y el cariño que me han demostrado,*

*A mis amigos, mis compañeros de grupo y a todos los que de una u otra forma me han ayudado a llegar hasta aquí y han tenido que ver conmigo; a toda la gente que quiero y tengo presente,*

*A Isis, por su apoyo en estos meses de tesis,*

*A mi tutora, por su ayuda y conocimientos,*

*A Fidel y la Revolución por esta oportunidad,*

*A todos, mis agradecimientos...*

## DECLARACIÓN DE AUTORÍA

Declaro que soy el único autor de este trabajo y autorizo a 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 _____.

| | |
|---|---|
| Jorge Alberto Mora Julián | MSc. Yeleny Zulueta Veliz |

**Tutora:** Yeleny Zulueta Veliz. Graduada de Ingeniería Informática en 2004. Profesora asistente de la Universidad de las Ciencias Informáticas. Máster en Gestión de Proyectos Informáticos.

Dirección: Universidad de las Ciencias Informáticas (UCI), edificio 29, apto: 29103.

E-mail: yeleny@uci.cu

**Asesora:** Lic. Karolay Rodríguez Alpajón. Graduada en Sociología. Profesora adiestrada de la Universidad de las Ciencias Informáticas.

Dirección: Universidad de las Ciencias Informáticas (UCI), edificio 127, apto 127106.

E-mail: karob@uci.cu

**RESUMEN**

La Gestión de Riesgos ha adquirido una gran importancia en los últimos años por la influencia que tiene en el logro de los objetivos de los proyectos y la calidad de los mismos. El Análisis de Riesgos es una fase indispensable de este proceso, pues sus resultados son necesarios para la creación de planes acertados para su gestión.

En la Universidad de las Ciencias Informáticas (UCI) el Análisis de Riesgos no se realiza con la formalidad necesaria, pues no existe una metodología que homogenice su aplicación en los proyectos productivos.

En este documento se valoran las tendencias actuales en la gestión y el análisis de los riesgos a nivel mundial, tomando como referencia los principales métodos y modelos existentes. Se propone además una guía metodológica para realizar el Análisis de Riesgos en los proyectos de desarrollo de software, definiendo los roles que deben participar en el mismo y las técnicas que se pueden utilizar, descritas y ejemplificadas para su mejor comprensión.

La guía propuesta en esta investigación puede utilizarse como referencia para la realización del Análisis de Riesgos en la UCI y cualquier otra institución dedicada a la producción de software cuyo proceso de desarrollo posea características similares a los de la universidad.

**PALABRAS CLAVES**

Software, riesgo, probabilidad, impacto, priorización, técnicas, Gestión de Riesgos, Análisis de Riesgos.

**ÍNDICE**

## ÍNDICE DE TABLAS



## ÍNDICE DE FIGURAS

## INTRODUCCIÓN

La informática y las comunicaciones se han convertido en factores claves para el desarrollo, hoy día se habla de la sociedad de la información, pues esta da sustento a muchos de los avances científicos de los que somos testigos. La utilización de software se ha extendido a nivel mundial en las más disímiles esferas, actualmente su producción se hace cada vez más compleja, crear productos de alta calidad, en menos tiempo y con menor coste son objetivos perseguidos por los que apuestan a esta empresa, por lo cual se hace necesaria una correcta Gestión de Software.

Parte importante de la Gestión de Software es la Gestión de Riesgos, el desarrollo de software, como muchos procesos de carácter ingenieril, está expuesto a la incidencia de múltiples riesgos: durante el proceso de desarrollo es muy posible que se introduzcan cambios que afecten a este, los cuales generalmente se traducen en riesgos y pueden influir en aspectos de gran importancia como son el coste, la planificación temporal o la calidad del producto.

El concepto de riesgo en el contexto de la gestión de proyectos de software cuenta con múltiples definiciones elaboradas por expertos en el tema. No obstante, la mayoría de ellos convergen en que el riesgo implica dos factores: "Incertidumbre" y "Efecto en los objetivos" (1).

La investigación en Gestión de Riesgos en el software persigue la concepción de principios y buenas prácticas con el fin de evitar o minimizar los riesgos y el efecto que puedan tener en el proceso de desarrollo de software a través de la planificación, identificación, análisis, la respuesta a los riesgos y el seguimiento y control de estos en un proyecto (2).

El Análisis de Riesgos se convierte en una de las fases fundamentales a tener en cuenta cuando se habla de la seguridad del software que se utiliza, el que se construye, y del mismo proceso de desarrollo. La evaluación continua del riesgo a lo largo de todas las fases del proyecto es esencial para lograr los objetivos trazados en el mismo.

La ventaja que proporciona el análisis es principalmente que permite conocer de antemano cuáles de los riesgos identificados son más probables y el impacto que pueden ocasionar estos en el producto, el equipo o el equipamiento. Con este conocimiento se hace mucho más sencillo crear un plan para gestionarlos de forma eficaz y eficiente, pues permite además centrar los esfuerzos y recursos en los riesgos más importantes y de esta forma minimizar sus efectos al máximo.

La Universidad de las Ciencias Informáticas (UCI) es una institución que combina la formación, la producción y la investigación. Surgida en el año 2002 como parte de la Batalla de Ideas que lleva a cabo el pueblo de Cuba desde finales del siglo pasado, la UCI es un centro importante de producción de software, definiéndose de esta forma como estratégico para el futuro económico del país (3).

Debido a la importancia que adquiere la producción de software en la UCI, es necesaria la realización de una correcta gestión de los proyectos y minimizar o eliminar los riesgos que puedan afectar el producto desde cualquier ámbito. La poca experiencia en la Gestión de Riesgos en la universidad y el peculiar modelo de producción que sigue la misma trae consigo que no se realice un análisis de riesgos adecuado en los proyectos productivos, por lo cual puede verse afectada la calidad del producto y en muchos casos se hace difícil cumplir con la planificación temporal realizada.

El análisis, dentro del proceso de la Gestión de Riesgos, no se realiza siguiendo una guía formal en la Universidad de las Ciencias Informáticas debido a la ausencia de un método que se adapte a las particularidades de los proyectos de desarrollo de software en la institución.

Teniendo en cuenta la situación problemática planteada el problema al que se le dará solución en esta investigación es: ¿Cómo garantizar la fiabilidad de los resultados en el análisis de los riesgos en un proyecto de desarrollo de software?

El objeto de estudio de esta investigación es la Gestión de Riesgos en el Proceso de Desarrollo de Software, y el objetivo general que se persigue con ella es establecer una guía metodológica que permita realizar el análisis de los riesgos a través de diferentes técnicas para el cálculo de la probabilidad de ocurrencia, el impacto de estos en los proyectos de desarrollo de software, y su priorización. Los objetivos específicos de la investigación son los siguientes:

1. Caracterizar los métodos utilizados para el análisis de los riesgos.
2. Analizar métodos y técnicas alternativas para la estimación y cálculo de la probabilidad de ocurrencia de los riesgos y su impacto en proyectos de desarrollo de software.
3. Documentar métodos y técnicas alternativas para la estimación y cálculo del impacto y la probabilidad de los riesgos en proyectos de desarrollo de software.

El campo de acción de la investigación es el Análisis de los Riesgos en el Proceso de Desarrollo de Software.

Una vez establecido el problema científico y los objetivos de esta investigación se puede plantear como hipótesis que: como resultado de un correcto estudio de los modelos existentes para el Análisis de los Riesgos en los proyectos de desarrollo de software y las tendencias actuales en este campo, es posible proponer una guía metodológica para el Análisis de Riesgos que se adapte a las necesidades de los proyectos de desarrollo de software que se llevan a cabo en la Universidad de las Ciencias Informáticas.

Al concluir la investigación se obtendrá:

- Un análisis de las tendencias actuales en la gestión de los riesgos en el proceso de desarrollo de software.
- Una guía para la utilización de diferentes métodos para el cálculo del impacto, la probabilidad y realizar la priorización de los riesgos.
- Una representación en lenguaje de modelación de las actividades relacionadas con el análisis de los riesgos.
- Valoraciones para la aplicación de la propuesta.

Para obtener estos resultados es necesario llevar a cabo las siguientes tareas:

- Valorar las tendencias actuales en la Gestión de Riesgos en proyectos de desarrollo de software.
- Analizar los métodos existentes para el análisis de los riesgos.
- Identificar y fundamentar las alternativas para el análisis de los riesgos.
- Analizar la realización del Análisis de Riesgos en la UCI.
- Adaptar técnicas para el análisis de riesgos a las necesidades de los proyectos productivos de la universidad.
- Describir y ejemplificar técnicas para el análisis de riesgos.
- Definir principios y buenas prácticas para el análisis de riesgos.

Definidos los elementos necesarios para encontrar la respuesta al problema que se plantea en la investigación es preciso seleccionar las herramientas de las cuales se va a hacer uso para llevarla a cabo, para esto se trazó una estrategia explicativa, con el fin de variar el problema modificando las causas que lo producen.

Esta investigación se llevó a cabo haciendo uso de métodos científicos tanto teóricos como empíricos. Los métodos teóricos se utilizaron para el estudio de las características de la Gestión y

como parte de esta el Análisis de los Riesgos en el Proceso de Desarrollo de Software que no son directamente observables. Dentro de estos métodos se utilizaron los siguientes:

**Histórico-Lógico:** el uso de este método científico permitió analizar la trayectoria del Análisis de los Riesgos desde sus inicios, permitiendo conocer la lógica interna de su desarrollo.

**Analítico-Sintético:** este método tiene su principal soporte en los procesos de análisis y síntesis, fue utilizado con el objetivo de delimitar los diferentes componentes y las relaciones de los diferentes modelos existentes para realizar el Análisis de los Riesgos en el proceso de desarrollo de software con el fin de facilitar su estudio, y luego establecer la unión de estos componentes para el análisis de las relaciones entre ellas y sus características generales.

**Hipotético-Deductivo:** este método fue utilizado para la verificación de la hipótesis y el surgimiento de nuevo conocimiento a partir de esta y del estudio de metodologías generales existentes para el Análisis de los Riesgos en diversas áreas.

Los métodos empíricos se utilizaron para describir y explicar las características del Análisis de los Riesgos en el proceso de desarrollo de software de la Universidad de las Ciencias Informáticas, comprobando la hipótesis derivada de los métodos teóricos, llevando la investigación a un nivel de mayor elaboración. Para esto se utilizó la observación científica, en este caso la observación externa abierta y no incluida.

Este documento cuenta con 3 capítulos los cuales están estructurados de la siguiente forma:

**Capítulo 1:** Fundamentos Teóricos del Análisis de Riesgos. En este capítulo se analiza la Gestión de Riesgos partiendo de los conceptos básicos relacionados con esta disciplina. Se analizan diferentes modelos utilizados a nivel mundial y cómo estos tratan el Análisis de Riesgos dentro de su proceso de gestión, además se analiza la Gestión de Riesgos en la UCI y las deficiencias en el análisis existentes en la universidad llegando a consideraciones generales sobre los aspectos que deben estar presentes en una metodología de Análisis de Riesgos para la UCI a través de la comparación de los modelos estudiados.

**Capítulo 2:** Técnicas para el Análisis de Riesgos. En este capítulo se valoran las técnicas para el análisis de riesgos propuestas por los diferentes modelos de gestión analizados en el capítulo 1, además de algunas técnicas alternativas.

**Capítulo 3:** Guía Metodológica para el Análisis de Riesgos. En este capítulo se propone una guía metodológica para el análisis de riesgos en los proyectos de desarrollo de software. Se definen los roles involucrados en el análisis y se explican las técnicas para llevarlo a cabo, además se proponen algunos principios a tener en cuenta para un correcto análisis de los riesgos.

# CAPÍTULO 1: FUNDAMENTOS TEÓRICOS DEL ANÁLISIS DE RIESGOS

## 1.1 Introducción

En este capítulo se realiza una descripción detallada de las tendencias de la Gestión de Riesgos en el mundo y se describe la situación problemática existente con el Análisis de Riesgos en la Universidad de las Ciencias Informáticas. Se analizan modelos para la Gestión de Riesgos y todas las tendencias que puedan aportar elementos o dar respuesta al problema científico planteado.

## 1.2 Conceptos asociados a la Gestión de Riesgos

Como parte de la fundamentación teórica de la presente investigación se hace necesario aclarar algunos conceptos profundamente relacionados con la Gestión de Riesgos y cuyo conocimiento es necesario para una mejor comprensión de este trabajo.

**Proyecto informático:**

Independientemente de los diferentes tipos de proyectos, existe un concepto general, utilizado con mucha frecuencia: "Un proyecto es una herramienta o instrumento que busca recopilar, crear, analizar en forma sistemática un conjunto de datos y antecedentes, para la obtención de resultados esperados. Es de gran importancia porque permite organizar el entorno de trabajo".

Un proyecto surge como respuesta a la concepción de una "idea" que busca la solución de un problema o la forma de aprovechar una oportunidad de negocio. Además constituye una ruta para el logro de conocimientos específicos en una determinada área o en una situación en particular, a través de la recolección y el análisis de datos (4).

Es esencialmente un conjunto de actividades interrelacionadas, con un inicio y una finalización definida, que utiliza recursos limitados para lograr un objetivo deseado (5).

Cuando se habla de proyecto informático, tomando las definiciones de proyecto existentes, se puede decir que es un sistema de cursos de acción simultáneos y/o secuenciales que incluye personas, equipamientos de hardware, software y comunicaciones, enfocados en obtener uno o más resultados deseables sobre un sistema de información, el cual tiene un inicio y un fin definidos.

**Riesgo:**

El término riesgo se utiliza en general para situaciones que involucran incertidumbre, en el sentido de que el rango de posibles resultados para una determinada acción es en cierta medida significativo (6).

Según la Guía PMBOK® (Project Management Body of Knowledge) un riesgo es una condición futura o circunstancia que existe por fuera del control del Líder del proyecto y de su equipo, puede tener un impacto negativo (amenaza) o positivo (oportunidad) por lo menos en uno de los objetivos del proyecto: que no son más que los costos(cumplir con los costos planificados al principio del proyecto), el tiempo (obtener cada versión del software en el tiempo acordado) y el alcance del proyecto (cumplir con las características del producto que se acordaron) y calidad (cumplir con los requerimientos de calidad pactados) (2).

Otros plantean que el riesgo es la probabilidad de que una amenaza se convierta en un desastre. Sin embargo los riesgos se pueden reducir o manejar. Si se es cuidadoso en las relaciones con el ambiente, estando conscientes de las debilidades y vulnerabilidades frente a las amenazas existentes, se pueden tomar medidas para asegurarse de que las amenazas no se conviertan en desastres (7).

Un riesgo es cualquier suceso cuya aparición no se puede determinar a priori y que pueda influir negativamente en el devenir del proyecto. Este está asociado a cualquier actividad que se realice en el proyecto y que imponga una decisión entre varias opciones, ya que siempre habrá un riesgo a equivocarse en la decisión tomada. El riesgo por tanto irá acompañado de todo cambio o decisión que se produzca en el proyecto, ya que estas siempre representan un marco de incertidumbre ante lo que puede ocurrir. Además constituye una falta de conocimiento sobre futuros acontecimientos (8).

Un riesgo se relaciona con la probabilidad de que ocurra alguna circunstancia adversa al proyecto. Existen tres clases principales de riesgos:

- Los riesgos de un proyecto afectan a la planificación temporal, el coste y la calidad del proyecto. Estos riesgos identifican problemas potenciales de presupuesto, calendario, personal, recursos, cliente, etc.
- Los riesgos de un producto o técnicos afectan a la calidad y la planificación temporal del software por desarrollarse. Identifican posibles problemas de incertidumbre técnica, ambigüedad, en la especificación, diseño, implementación, interfaz, etc.

- Los riesgos del negocio son los que afectan a la organización que desarrolla el software. Amenazan la viabilidad del software, los principales riesgos del negocio son: el riesgo de mercado, riesgo estratégico, riesgo de ventas, riesgo de presupuesto.

También se pueden calificar los riesgos en función de su facilidad de detección, estas clasificaciones son las siguientes (1):

- Riesgos conocidos: son aquellos que se pueden predecir después de una evaluación del plan de proyecto, del entorno técnico y otras fuentes de información fiables.
- Riesgos predecibles: se extrapolan de la experiencia de proyectos anteriores.
- Riesgos impredecibles: pueden ocurrir, pero es extremadamente difícil identificarlos por adelantado.

Existen riesgos genéricos, los cuales representan una amenaza potencial para todos los proyectos de software y los riesgos específicos del producto, los cuales solo pueden ser identificados por aquellos que tienen una visión de la tecnología, el personal y el entorno específico del proyecto en cuestión (1).

Partiendo de las definiciones de riesgo anteriores se puede definir para esta investigación un riesgo como un suceso cuya aparición no puede ser determinada a priori y que en caso de ocurrir traerá al proyecto consecuencias negativas. El riesgo está estrechamente relacionado con la incertidumbre y acompaña a cada cambio o decisión que se tome en el proyecto. Una vez materializado el suceso deja de ser un riesgo para convertirse en un problema.

**Gestión de Riesgos**

Según la Guía PMBOK ® la Gestión de Riesgos constituye un Proceso social complejo que conduce al planeamiento y aplicación de políticas, estrategias, instrumentos y medidas orientadas a impedir, reducir, prever y controlar los efectos adversos de fenómenos peligrosos sobre la población, los bienes y servicios (2).

La gestión de riesgos es la aplicación sistemática de políticas, procedimientos y prácticas de gestión a las tareas de identificar, analizar, evaluar y controlar los riesgos (7).

Según la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas (MAGERIT) es la selección e implementación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados (9).

La Gestión de Riesgos está conformada por etapas, cada una de las cuales tiene su objetivo en el proceso, una de estas etapas es el Análisis de Riesgos.

**Análisis de Riesgos:**

El Análisis de Riesgos constituye una serie de pasos que ayudan al equipo de software a comprender y a gestionar la incertidumbre (1).

Constituye un proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización (9).

El Análisis de Riesgos se puede clasificar en cualitativo o cuantitativo:

- **Análisis cualitativo de riesgos:** se encarga de priorizar los riesgos para realizar otros análisis o acciones posteriores, evaluando y combinando su probabilidad de ocurrencia y su impacto (2). Para estas evaluaciones se utilizan valores cualitativos, por lo cual este tipo de análisis no arroja resultados numéricos, sino que brinda una clasificación de estos valores de forma subjetiva.
- **Análisis cuantitativo de riesgos:** se encarga de analizar numéricamente el efecto de los riesgos identificados en los objetivos generales del proyecto (2). Para este análisis se utilizan valores numéricos reales del proyecto o la organización y los resultados son más exactos y objetivos, aunque las técnicas utilizadas para realizarlo son más complejas.

**Probabilidad:**

Se define como cálculo de probabilidad al conjunto de reglas que permiten determinar si un determinado fenómeno ha de producirse, fundando la suposición en el cálculo, las estadísticas o la teoría. La probabilidad mide la frecuencia con la que ocurre un resultado en un experimento bajo condiciones suficientemente estables.

En este trabajo es la probabilidad de que un riesgo se materialice o no en un proyecto, no basta con saber que el riesgo existe, sino que para su correcto análisis es preciso determinar cuán inminente es su efecto en el proyecto.

**Impacto:**

El impacto de un riesgo sobre un proyecto de software es el daño que este puede causar en caso de materializarse desde cualquier punto de vista, el conocimiento del impacto que puede ocasionar un riesgo es necesario para determinar la importancia de este y planificar su gestión.

**Plan de Gestión de Riesgos:**

Se realiza como parte de una fase más de la Gestión de Riesgos, es el plan que se realiza con el fin de tratar los riesgos identificados, normalmente está estrechamente relacionado con el análisis de los riesgos, pues utiliza estos resultados para definir cuáles son las mejores estrategias para enfrentar, minimizar o tratar de eliminar los factores que producen la amenaza.

Es un conjunto coherente y ordenado de estrategias, programas y proyectos, que se formulan para orientar las actividades de reducción de riesgos (9).

## 1.3 La Gestión de Riesgos en el Proceso de Desarrollo de Software

Aunque hace más de una década aparecieron los primeros enfoques de gestión del riesgo, es evidente que su utilización es pobre a nivel mundial en los proyectos de desarrollo de software actuales. La Gestión de Riesgos en proyectos se trata de una disciplina de la Ingeniería del Software que está empezando a adquirir gran importancia, en los últimos años las empresas están dedicándole más tiempo y recursos debido a la aparición de estándares internacionales propuestos para este proceso (8).

En su libro "Ingeniería del Software. Un Enfoque Práctico", Roger Pressman plantea que el análisis y la gestión del riesgo son una serie de pasos que ayudan al equipo de software a comprender y a gestionar la incertidumbre. Plantea que sin tener en cuenta el resultado de un problema es una buena idea identificarlo, evaluar su probabilidad de aparición, estimar su impacto y establecer un plan de contingencia por si ocurre (1).

### 1.3.1 Estrategias frente al riesgo

Existen dos tipos de estrategias frente al riesgo en los proyectos de software: las estrategias reactivas y las proactivas. La mayoría de los equipos de software confían solamente en las estrategias reactivas, estas estrategias se dan cuando se espera a que los riesgos se conviertan en realidad para actuar en consecuencia, estas producen tiempo perdido, retrasos en los proyectos, etc. (8). En el mejor de los casos, se supervisa el proyecto en previsión de posibles riesgos. Los recursos se ponen aparte, en caso de que pudieran convertirse en problemas reales, pero lo más frecuente es que el equipo de software no haga nada respecto a los riesgos hasta que algo va mal. El peligro ante el cuál se pone al proyecto al seguir una estrategia reactiva frente al riesgo no hace aconsejable el uso de estas (1).

Una estrategia más inteligente para controlar el riesgo es ser proactivo. Estas estrategias comienzan antes del trabajo técnico, pasan por la evaluación previa y sistemática de todos los riesgos inherentes al proyecto, evaluando sus consecuencias (8). Una vez identificados los riesgos potenciales se evalúa su probabilidad y su impacto y se establece una prioridad según su importancia, esto produce la creación del Plan de Gestión de Riesgos por parte del equipo de software. Como es probable que no se puedan evitar todos los riesgos el equipo trabaja en la creación de un plan de contingencia para responder de forma eficaz y controlada en caso de que se materialice el riesgo. (1)

### 1.3.2 Evolución de la Gestión de Riesgos

La Gestión de Riesgos constituye un eje transversal e integrador en los diferentes proyectos que tienen por objetivo garantizar que los procesos de desarrollo impulsados en la sociedad se den en las condiciones óptimas de seguridad y que la atención y acciones desplegadas ante consecuencias no deseadas promuevan el mismo desarrollo (10).

Han existido tres generaciones de modelos de riesgos en proyectos informáticos las cuales serán brevemente abordadas a continuación.

**Primera generación G1 (Casuística)**

La primera generación data de principios de los años 80 del siglo pasado y se basa en listas casuísticas de riesgos especiales para proyectos, el modelo de gestión de riesgos casuístico consiste en identificar casos de riesgos y extrapolarlos a otros proyectos, por lo cual no existe una planificación específica. En esta generación se definen los riesgos tecnológicos y listas de comprobación de riesgos, estas listas están basadas en preguntas que determinan factores de riesgos (11).

Durante los años 60 se producen análisis de riesgos cuantitativos para describir el comportamiento de sistemas complejos y análisis cualitativos como los árboles de fallos para sistemas híbridos con la incertidumbre de la intervención humana y la imposibilidad de probar los impactos salvo por la simulación.

En esta generación se obtiene la definición del riesgo como una entidad con dos dimensiones: probabilidad y consecuencias, la cual sigue vigente en la actualidad (8).

**Segunda generación G2 (Taxonómica)**

La segunda generación data de principio de los años 90 del pasado siglo y recibe el nombre de taxonómica, está basada en modelos de procesos y eventos. Estos modelos reciben por parte de algunos autores críticas relacionadas principalmente con su carácter preventivo y reactivo, pues centran su atención en el análisis de los riesgos en el inicio del proyecto y actúan de manera improvisada al surgir algún riesgo durante el avance del mismo (11).

Dentro de esta generación se pueden incluir los siguientes modelos (8):

- Modelo de Boehm.
- Modelo de Hall.
- Modelo de Riesgos del Software Engineering Institute.

**Tercera Generación G3 (Causal)**

La tercera generación es la causal y es la que se encuentra actualmente emergente. Surgió a mediados de los 90 del siglo pasado simultáneamente en Europa y Estados Unidos y aprovecha los métodos de Gestión de Riesgos utilizados en los sistemas. Esta generación se apoya en modelos sistémicos relacionales y proactivos en el aseguramiento de los proyectos (11).

Los principales modelos de GR de esta generación son:

- Modelo MAGERIT de Gestión de Riesgos en Sistemas Adaptados a Proyectos.
- Modelo Eurométodo.
- Modelo Information Services Procurement Library (ISPL).
- Proyectos de investigación europeos como RiskMan, DriveSPI, RiskDriver, Moynihan, Barki, Schmidt e INSEAD.

### 1.3.3 Métodos de resolución de riesgos

Existen 4 métodos generales de resolución de riesgos en función de la actitud que se muestre frente al riesgo, estos métodos son: eliminación, retención, evitación y transferencia (11).

**Eliminación del riesgo:**

Se trata de eliminar los factores que inducen el riesgo y con ello eliminar la posibilidad de exposición de este.

Este tipo de riesgos deben ser no inherentes a la propia actividad realizada, sino riesgos accesorios que no influyen directamente en el logro de los objetivos del proyecto.

**Retención del riesgo:**

La mayor parte de los riesgos que se identifican en un proyecto no son posibles de eliminar por lo que es necesario hacerles otro tipo de tratamiento.

La retención del riesgo es la asunción por parte de los responsables del proyecto de que el riesgo existe, y que es necesario convivir con él.

**Evitación del riesgo:**

El riesgo existe y puede provocar sus efectos negativos, en este caso hay que identificar los factores que provocan el riesgo y mantenerlos bajo control para evitar que este provoque sus efectos.

**Transferencia del riesgo:**

Algunos tipos de riesgo, que son generalmente poco probables pero los de mayor efecto negativo, pueden ser transferidos a terceros mediante la contratación de seguros o haciendo contratos en los que el cliente o los proveedores asumen el riesgo y liberan al equipo de proyecto de su gestión.

Los riesgos propios del proceso de software no pueden ser eliminados, pues siempre estarán presentes, se pueden eliminar solamente riesgos independientes al proceso, la diferencia entre la eliminación y evitación del riesgo es básicamente esa, la diferencia entre los tipos de riesgos que se evitan y los que se eliminan, además de que cuando se evita el riesgo se controlan los factores que lo producen y cuando se elimina es necesario excluir del proceso estos factores.

### 1.3.4 Análisis de los Riesgos

El análisis del riesgo implica cualquier método, ya sea cualitativo o cuantitativo, que dé la posibilidad de evaluar el impacto de un riesgo y la probabilidad de ocurrencia del mismo. Con los resultados del análisis de riesgos se puede determinar cuáles son los más importantes, además de brindar ayuda a la hora de elegir un curso de acción en la toma de decisiones (8).

El impacto y la probabilidad de un riesgo se pueden determinar a través de técnicas y métodos que plantean algunos de los modelos de Gestión de Riesgos existentes en la actualidad.

Como parte del análisis de los riesgos se hace necesario ordenarlos, la asignación de prioridades a los riesgos permite darles tratamiento según su importancia, esta se realiza debido a la frecuente necesidad de tratar solamente a un determinado número de riesgos y no a todos los identificados, para esto se utilizan los valores de probabilidad de ocurrencia e impacto que se obtuvieron al analizar cada uno de los riesgos. Roger Pressman plantea que una vez obtenida la probabilidad de ocurrencia del riesgo y el daño que este pueda causar se priorizan en función de la probabilidad y el impacto (1). El Instituto de Gestión de Proyectos (PMI) establece como una de las salidas del análisis de riesgos la lista priorizada de riesgos, en la cual se incluyen los riesgos que representan una mayor amenaza para el proyecto (2). Por su parte Boehm propone como una de las actividades de la Gestión de Riesgos la Priorización del Riesgo.

Existen diversas técnicas para priorizar los riesgos, entre ellas se encuentra la creación de tablas ordenadas por probabilidad y luego por impacto, el cálculo de exposición al riesgo, obtenido de multiplicar la probabilidad por el impacto(8) y las matrices de probabilidad e impacto.

### 1.4 Modelos existentes para la Gestión de Riesgos

Existen diferentes modelos orientados a la Gestión de Riesgos. En la tabla 1 se muestran algunos de los más ampliamente conocidos y de fácil acceso y la implementación por estos de las funciones básicas para la Gestión de Riesgos.

Como se observa en la tabla 1, la mayoría de los modelos analizados coinciden en la realización de una serie de actividades para el análisis de riesgos las cuales son:

- Identificación de los Riesgos.
- Análisis de Riesgos.
- Planificación de Respuestas.
- Seguimiento y control

El Análisis de Riesgos es una actividad común para todos estos modelos, cada uno de ellos plantea la estimación de la probabilidad de ocurrencia de los riesgos y el impacto de estos además de su priorización utilizando diversas técnicas.

En este epígrafe se abordan algunos de estos modelos, cómo proponen la Gestión de Riesgos y de qué forma enfocan el análisis como actividad clave en este proceso.

| Modelo | DR | P | I | A | R | S-C | C | Métricas |
|---|---|---|---|---|---|---|---|---|
| Boehm | - | | x | x | x | x | | Caracterizar Riesgo |
| SEI | - | | x | x | x | x | x | Caracterizar Riesgo |
| PMI | -+ | x | x | x | x | x | | Caracterizar Riesgo |
| Hall | -+ | | x | x | x | x | | Caracterizar Riesgo |
| McFarlan | - | | x | x | x | x | | Caracterizar Riesgo |
| Capers Jones | - | | x | x | x | x | | Caracterizar Riesgo |
| MAGERIT | - | x | x | x | x | x | | Caracterizar Riesgo (Activo, Amenaza y Riesgo) |
| Eurométodo/ISPL | - | | x | x | x | x | | Caracterizar Riesgo |
| DriveSPI | - | | x | x | x | x | | Caracterizar Riesgo<br>Medir Resultados<br>Mejorar Resultados |

**Tabla 1: Definición de Riesgo (DR), Planificación (P), Identificación (I), Análisis (A), Planificación de Respuestas (R), Seguimiento y Control (S-C), Comunicación (C) y métricas en modelos de Gestión de Riesgos. Fuente: Retos en la Gestión de los Riesgos en**

### 1.4.1 Barry W. Boehm

Uno de los autores más destacados en la Gestión de Riesgos es Barry W. Boehm, el cual realizó diversos trabajos sobre este tema, principalmente su libro "Software Risk Management" y su artículo "Software Risk Management: Principles and Practices". Muchas de las técnicas planteadas por él se utilizan en la actualidad. La Gestión de Riesgos para Boehm tiene dos etapas fundamentales: la Valoración y el control del riesgo, estas etapas se realizan a través de determinados pasos, reflejados en la figura 1.

Estas dos fases propuestas por Boehm plantean que primero es necesario determinar cuáles de las posibles circunstancias adversas puede constituir un riesgo, analizarlos y determinar su importancia relativa con respecto a otros riesgos identificados, concluyéndose de esta forma la Valoración del Riesgo. Como parte del Control hay que determinar cómo se va a afrontar el riesgo, para lo cual es necesario planificar la gestión y el control del riesgo, darle soluciones y determinar su gestión y luego seguirlos y monitorizarlos (8).

Como parte de la Valoración del Riesgo Boehm propone el Análisis de Riesgos, en su modelo las actividades básicas son la evaluación y la clasificación.

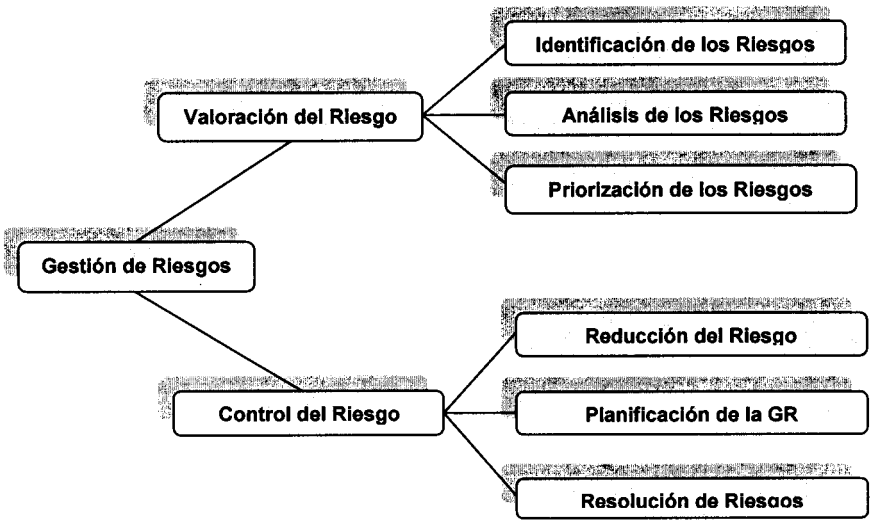


**Figura 1: Gestión de Riesgos según Boehm. Fuente: Mejora y ampliación de gestión de riesgos bajo el framework jrisk para empresa dedicada a realizar proyectos de software (8).**

Durante la evaluación se deben obtener datos cuantificables que permitan la comparación con otros riesgos, para mejorar de esta forma su comprensión y poder realizar una clasificación coherente de estos.

Los principales conceptos que tiene en cuenta Boehm para la clasificación de los riesgos son la consecuencia o impacto de estos, la probabilidad de que ocurran y el período de tiempo en el que es posible mitigarlos (8).

### 1.4.2 Metodología para el Análisis y Gestión de Riesgos de los Sistemas de Información y Administraciones Públicas (MAGERIT)

Uno de los métodos utilizados para el Análisis y Gestión de Riesgos es la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas (MAGERIT). Esta metodología estudia a fondo los riesgos que soporta un sistema de información y el entorno asociado a él, señala los riesgos existentes, identificando las amenazas que asechan al sistema de información, y determina las vulnerabilidades de este.

MAGERIT fue desarrollado por un equipo del Comité Técnico de Seguridad de los Sistemas de Información y Tratamiento Automatizado de Datos Personales, del Consejo Superior de

Informática de España. Fue creado en sus inicios para gestionar los posibles riesgos de seguridad derivados de la utilización de medios electrónicos, informáticos y telemáticos, el cual ha sido adaptado a proyectos posteriormente.

El modelo MAGERIT se divide en 3 submodelos (8):

- Submodelo de procesos.
- Submodelo de entidades.
- Submodelo de eventos.

Dentro del submodelo de procesos MAGERIT define el análisis de riesgos.

Según el método MAGERIT (9) el proyecto se divide en tres grandes procesos los cuales se presentan en la siguiente figura:

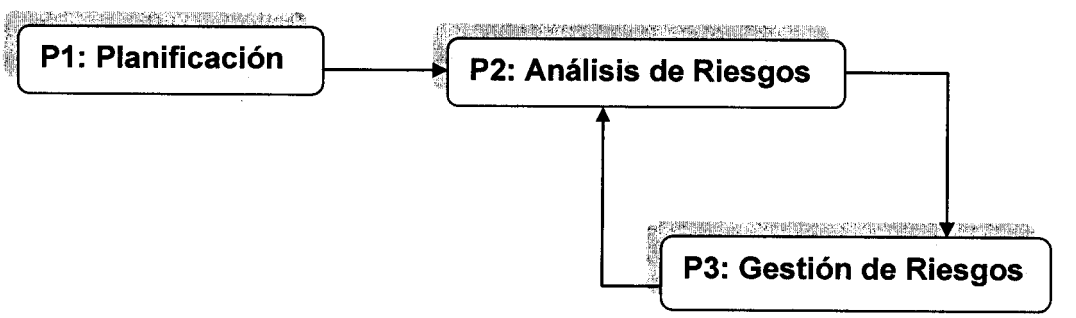


**Figura 2: Modelo de procesos en MAGERIT. Fuente: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Guía de Técnicas (9).**

El Análisis de Riesgos permite determinar qué tiene la organización y estimar lo que podría pasar. Los elementos del análisis de riesgos según MAGERIT son los siguientes (9):

1. Activos, son los elementos del sistema o estrechamente relacionados con este que aportan valor a la organización.
2. Amenazas, son eventos no deseados que pueden ocurrirles a los activos causando un prejuicio a la organización.
3. Salvaguardas, son los elementos de defensa desplegados para las amenazas no causen tanto daño.

Un análisis de riesgos según el modelo MARGERIT es una aproximación metódica para determinar el riesgo, definido como la medida del daño probable sobre un sistema (9).

Propone una serie de guías metodológicas, entre las cuales se encuentran la Guía de Procedimientos, en la que explica la terminología para realizar el Análisis y la Gestión de Riesgos de un sistema de información, y la Guía de Técnicas, que brinda las técnicas necesarias para realizar el Análisis y la Gestión de Riesgos.

Los objetivos de MAGERIT son los siguientes:

1. Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de detenerlos a tiempo.
2. Ofrecer un método sistemático para analizar tales riesgos.
3. Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
4. Apoyar la preparación a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

El Análisis de Riesgos propuesto por MAGERIT es orientado a los activos, que son los recursos del sistema de información o relacionados con este, necesarios para que la Organización funcione correctamente y alcance los objetivos propuestos por su dirección (9), se centra en el valor de los activos de la organización, determinando la vulnerabilidad de estos ante una determinada amenaza, la degradación del valor de los activos causada por esta, el impacto que tendría la materialización de la amenaza sobre el activo, y el riesgo.

### 1.4.3 Eurométodo

Otro de los métodos existentes para la Gestión de Riesgos es el Eurométodo, es utilizado para valorar y determinar los riesgos asociados a un sistema de información y los servicios asociados. Fue desarrollado por la Comisión Europea para la contratación de sistemas y servicios informáticos.

Los objetivos de Eurométodo son los siguientes (13):

1. Ayudar al entendimiento mutuo entre clientes y proveedores de proyectos y servicios de sistemas de información dentro de un mercado internacional abierto, proporcionando

asesoramiento apoyado por un conjunto de conceptos y terminología que se utilizarán en las transacciones.

2. Mejorar la adquisición de sistemas de información y servicios, teniendo presente la situación del problema y los riesgos asociados.
3. Proporcionar un marco para la unificación de la terminología de los métodos.

La Gestión de Riesgos de Eurométodo se compone de tres fases (8):

- Análisis de Riesgos.
- Planificación de la Gestión de Riesgos (estrategia de desarrollo y propuesta de hitos de decisión).
- Supervisión de Riesgos (mide si las salvaguardas tienen éxito).

El Análisis de Riesgos de Eurométodo proporciona orientaciones para evaluar la probabilidad de riesgos, pero no para valorar la magnitud de su impacto negativo (consecuencias adversas), que está fuertemente relacionada con la naturaleza y especificidad de la organización del dominio objetivo. La magnitud del impacto negativo debe valorarse desde una perspectiva de negocio: supervivencia, funcionamiento efectivo y evolución de la organización del dominio objetivo. En algunos casos, la repercusión se puede valorar en términos económicos (13).

El análisis de Riesgos de Eurométodo se sustenta en factores situacionales definidos por este método. La valoración de los factores situacionales es la base para la evaluación de la incertidumbre y la complejidad de la situación. Los riesgos pueden extraerse de los factores situacionales y de la incertidumbre y complejidad generales.

En la figura 3 se muestra el Análisis de Riesgos y el diseño de la estrategia de Gestión de Riesgos en Eurométodo.

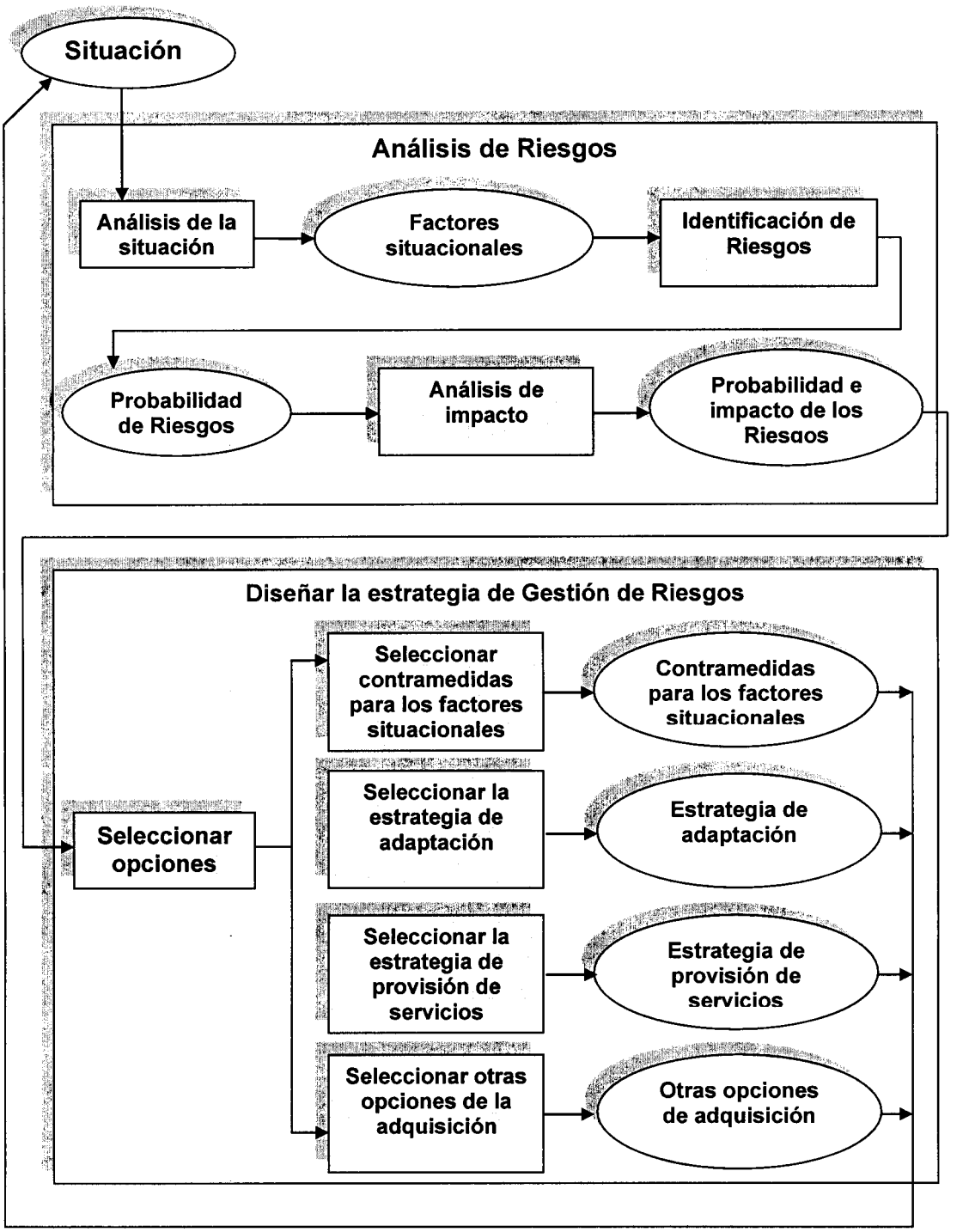


**Figura 3: Análisis de Riesgos y Diseño de la estrategia de Gestión de Riesgos en Eurométodo. Fuente: Eurométodo V1 (13).**

### 1.4.4 Modelo de Gestión de Riesgos del Project Management Institute (PMI)

El Project Management Institute (PMI) es considerado la asociación profesional para la Gestión de Proyectos sin fines de lucro más grande del mundo, entre sus principales objetivos se encuentran la formulación de estándares profesionales, la generación de conocimientos a través de la investigación y la promoción de la Gestión de Proyectos como profesión.

Este instituto plantea una metodología de gestión de proyectos detallada, es la metodología más completa en cuanto a las funciones básicas que deben tenerse en cuenta para realizar una Gestión de Riesgos eficiente antes de que estos constituyan una amenaza para el proyecto (10).

Esta metodología consta de 5 procesos, entre los cuales se encuentra el Análisis de los Riesgos. Según plantea PMI en su guía PMBOK® (2) estos procesos deben llevarse a cabo al menos una vez en cada fase del proyecto. La siguiente figura muestra las fases de la Gestión de Riesgos según PMI (10).

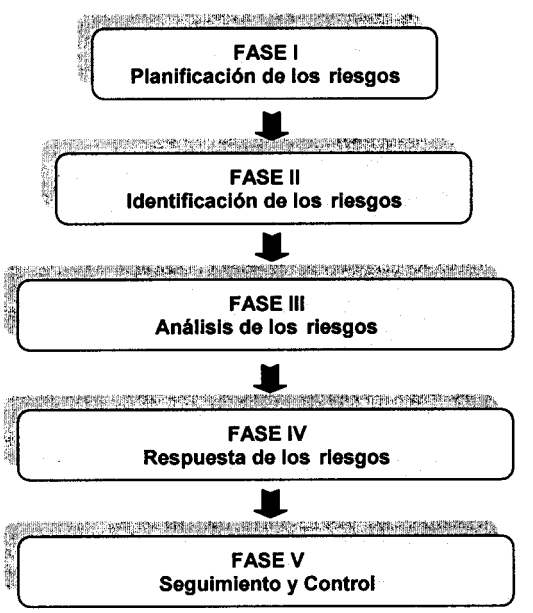


**Figura 4: Procesos para la Gestión de Riesgos de PMI. Fuente: Guía de los Fundamentos de la Dirección de Proyectos. Tercera Edición (Guía del PMBOK®) (10).**

PMI propone la realización del análisis cualitativo y cuantitativo de los riesgos del proyecto. En este modelo el análisis cualitativo da paso al análisis cuantitativo, aunque estos se pueden hacer independientemente también.

Según el PMBOK® (2) el análisis cualitativo de los riesgos es normalmente una forma rápida y rentable de establecer prioridades para la Planificación de la Respuesta a los Riesgos y sienta las bases para el análisis cuantitativo de los riesgos en caso de que sea necesario.

El análisis cuantitativo de riesgos, según PMI se realiza respecto a los riesgos priorizados en el proceso de análisis cualitativo de riesgos por tener un posible impacto significativo sobre las demandas concurrentes del proyecto. Este proceso analiza el efecto de esos riesgos y les asigna una clasificación numérica. También presenta un método cuantitativo para tomar decisiones en caso de incertidumbre (2).

Al igual que MAGERIT, el Análisis de Riesgos propuesto por PMI es orientado a los activos de la organización.

### 1.4.5 Software Engineering Institute – Continuous Risk Management (SEI - CRM)

El Software Engineering Institute es un instituto federal estadounidense de investigación y desarrollo (I+D), fundado en 1984 para desarrollar modelos de evaluación y mejora en el desarrollo de software. Es financiado por el Departamento de Defensa de los Estados Unidos y administrado por la universidad Carnegie Mellon. Es un referente de la Ingeniería de Software desde el desarrollo, en 1991 del Capability Maturity Model for Software (SW-CMM) que fue el punto de arranque del modelo que ha desarrollado sobre el concepto de capacidad y madurez hasta el actual Capability Maturity Model Integration (CMMI).

Uno de los modelos más conocidos para la Gestión de Riesgos es el modelo SEI-CRM (Software Engineering Institute – Continuous Risk Management) es un método en el ámbito de la Ingeniería del Software cuyos conceptos, procesos y herramientas permiten gestionar de manera continua los riesgos de un proyecto, proporcionando un entorno disciplinado para la toma de decisiones a lo largo de todas las fases del proyecto: análisis de los problemas en potencia (riesgos), determinación de los riesgos importantes para elaborar estrategias y planes para gestionarlos. Estos riesgos son controlados hasta que se resuelven o se convierten en problemas menores y son tratados como tales (14).

SEI – CRM define el riesgo como la posibilidad de pérdida y este es en función de la probabilidad de que suceda un evento adverso, y el impacto, manifestado en una combinación de pérdida económica, retraso temporal y pérdida de rendimiento.

Los pasos seguidos por el modelo SEI – CRM son los siguientes (8):

- Identificar: busca y localiza los riesgos antes de que estos se produzcan.
- Analizar: procesa los datos sobre los riesgos para obtener información que ayude a la decisión.
- Planificar: traduce la información de riesgos en decisiones y acciones (ambas presentes y futuras) e implementa dichas acciones.
- Seguir: monitoriza los indicadores y acciones tomadas contra los riesgos.
- Controlar: corrige las acciones planeadas contra los riesgos.
- Comunicar: proporciona visibilidad y datos de retroalimentación internos y externos al programa sobre actividades de riesgo actuales y emergentes.

Estas actividades se gestionan como un ciclo básico a lo largo de todo el ciclo de vida del proyecto (14). En la figura 5 se muestran los pasos del modelo SEI – CRM para la gestión de Riesgos.

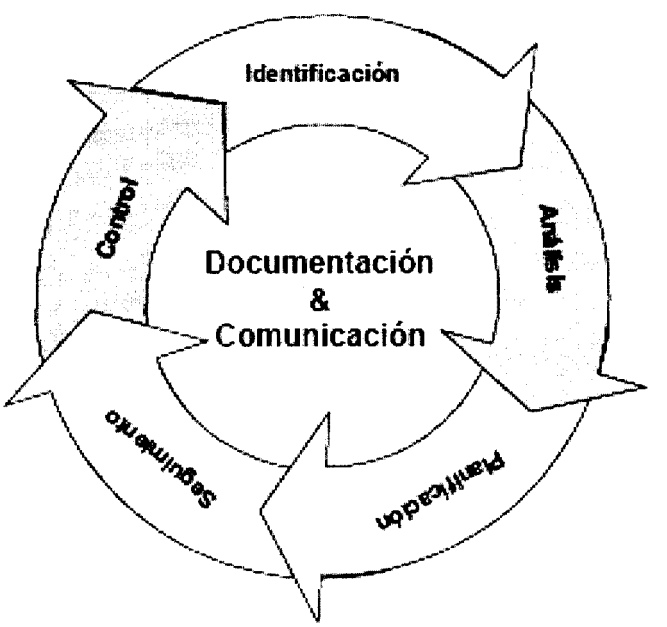


**Figura 5: Paradigma de Gestión de Riesgos del SEI: Fuente: Software Risk Management (15)**

## 1.5 Análisis de Riesgos en la Universidad de las Ciencias Informáticas

La Universidad de las Ciencias Informáticas (UCI) combina la formación académica de sus estudiantes con la preparación práctica de los mismos. La producción de software es uno de los más importantes objetivos que persigue la universidad y a raíz de esto cada una de las facultades que la conforman está dividida en polos productivos en los cuales están vinculados todos sus estudiantes directamente a la producción o la investigación.

En seis años de creada, la UCI ha logrado grandes avances en la producción de software, convirtiéndose en la referencia de la Industria Cubana del Software, a la vez ha ingresado importantes sumas bajo el concepto de exportaciones, lo cual reafirma su importancia desde el punto de vista económico. La producción de software en la universidad también está dirigida a satisfacer las necesidades del país para su informatización.

Cada facultad cuenta con sus proyectos de software, por lo tanto cada proyecto debe buscar alternativas para gestionarse y lograr la calidad del proceso y el producto realizado. Es una realidad que la gestión de proyectos no es siempre efectiva, trayendo como consecuencias, entre otras, incumplimientos de la planificación y que los productos no tengan toda la calidad requerida.

Uno de los puntos claves para lograr un proyecto con calidad y en tiempo es precisamente la Gestión de Riesgos, las acciones que se llevan a cabo en la UCI para el tratamiento de los riesgos no sigue un modelo formal para realizarla.

Encuestas realizadas en la universidad en diferentes ocasiones demuestran el escaso conocimiento sobre la Gestión de Riesgos entre el personal vinculado a los proyectos productivos de la misma. Como parte de un trabajo investigativo sobre la Gestión de Riesgos realizado por la Máster en Gestión de Proyectos Informáticos Yeleny Zulueta Veliz se realizaron entrevistas a personas vinculadas a la producción de software en la universidad y arrojaron como resultados la carencia de conocimientos de la Gestión de Riesgos y su aplicación. El personal vinculado a los proyectos productivos en la UCI tiene conocimiento de los riesgos que pueden afectarlos, sin embargo no se realiza un análisis adecuado de estos para la determinación de su probabilidad de ocurrencia e impacto, por lo que en la mayoría de los casos simplemente se realiza una identificación de los riesgos del proyecto (3).

Estudios llevados a cabo en el año 2008 demuestran que aún continúan los problemas asociados al conocimiento y aplicación de la Gestión de Riesgos en los proyectos de software de la UCI. Los

encuestados para los trabajos de diploma Guía para la gestión de riesgos a través de RUP (16) y Guía de Métricas para la Gestión de Riesgos en Proyectos de Desarrollo de Software de la UCI (17) reflejaron reconocer la importancia de la Gestión de Riesgos, pero que no se realiza el análisis y el tratamiento de los mismos hasta que se presentan. Otro de los resultados obtenidos es el desconocimiento de cómo realizar la Gestión de Riesgos debido entre otras causas a que no cuentan con vías factibles y el desconocimiento de los procesos y modelos para llevarla a cabo.

La Dirección de Calidad de Software de la Universidad de las Ciencias Informáticas creó el Expediente de Proyecto en la UCI con el fin de estandarizar y organizar los artefactos generados durante el proceso de desarrollo de software y contribuir a la calidad de los mismos (18). En el Expediente de Proyecto en la UCI hay un apartado dedicado a los riesgos. En este se pueden encontrar dos plantillas que rigen la Gestión de Riesgos en la universidad, estos son la Lista de Riesgos (Anexo 1) y el Plan de Mitigación de Riesgos (Anexo 2).

En la Lista de Riesgos se recoge la siguiente información:

- Riesgo.
- Tipo de Riesgo.
- Impacto.
- Descripción.
- Probabilidad.
- Efectos.

Luego se desarrolla una estrategia de mitigación en cada proyecto para reducir el impacto del riesgo, además se define un plan de contingencia con las acciones a tomar en caso de que el riesgo se materialice.

El próximo paso se denomina Gestión de Riesgos en el cual se propone la estimación de la probabilidad de ocurrencia de los riesgos, el impacto sobre el proyecto y el ordenamiento del registro de riesgos por probabilidad e impacto. En este proceso se llena otra tabla con los siguientes datos:

- Riesgo.
- Probabilidad de ocurrencia.

- Impacto.
- Mitigación del riesgo.
- Monitoreo del riesgo.
- Administración del riesgo.

Independientemente de que estos documentos intentan organizar la Gestión de Riesgos pueden identificarse algunas deficiencias en los mismos una vez estudiadas las tendencias a nivel mundial, las más notables son las siguientes:

- Las tareas para la Gestión de Riesgos son simplemente planteadas, no se indica cómo llevarlas a cabo.
- El Análisis de Riesgos se orienta, pero no se define como una fase más de la Gestión de Riesgos.
- No se proponen técnicas para la realización del análisis de los riesgos.
- No se propone una metodología a seguir, se indica qué hacer, pero no cómo.

Una vez valorada la Gestión de Riesgos en la UCI y como parte de esta el Análisis de Riesgos se puede apreciar que la ausencia de una metodología para realizar este último se hace evidente. La causa fundamental es que no se cuenta con un modelo que se adapte a las necesidades y particularidades del proceso de producción en la universidad y su Gestión de Riesgos. Las principales causas por las cuales no se aplican los modelos existentes en la universidad es por la falta de madurez de esta como centro de producción de software y por otra parte la poca profundidad de las metodologías que pueden ser utilizadas sin que representen una amenaza para el desarrollo de software en la UCI.

### 1.6 Conclusiones Parciales

Los modelos de Gestión de Riesgos utilizados mundialmente plantean la importancia del Análisis de Riesgos para la correcta gestión de los proyectos y hacen su propuesta de cómo llevarlo a cabo. Contrariamente a lo que muchos desarrolladores de software creen, este debe realizarse en cada una de las fases del proyecto, pues no basta con hacerlo al comenzar el mismo, la dinámica de los proyectos informáticos hace que se realicen cambios continuamente en los mismos y que sea necesaria la toma de decisiones cada vez que uno de estos cambios se vaya a realizar, en estos momentos es necesario hacer nuevamente el Análisis de Riesgos para

determinar qué riesgos pueden traer consigo los cambios que van a tener lugar, y cómo pueden estos afectar a los ya existentes.

La cantidad de riesgos varía de un proyecto a otro, al igual que las amenazas que pueden representar estos, cada proyecto tiene sus propios intereses a la hora de gestionarlos: mientras para un proyecto es importante determinar en términos económicos los efectos de un riesgo (para lo cual es necesario un Análisis de Riesgos orientado a los activos), para otro puede ser de vital importancia analizar los efectos de los riesgos en la planificación temporal obviando el impacto monetario de estos, de igual forma se pueden requerir los resultados del análisis en cifras exactas, para lo cual es necesario realizar un análisis cuantitativo o simplemente con un análisis cualitativo es suficiente; es por eso que una metodología para el Análisis de los Riesgos debe ser flexible a las necesidades del cliente.

Los métodos estudiados para la realización de esta investigación coinciden en la importancia de priorizar los riesgos en función de diferentes factores, generalmente por el impacto que tienen en los proyectos y la probabilidad de ocurrencia de los mismos, para determinar cuáles serán los riesgos a los que el equipo de desarrollo les dará atención inmediata, y no gastar recursos y tiempo gestionando riesgos de materialización poco probable o cuya gestión causaría más pérdidas que las ocasionadas por el mismo riesgo. Una vez que se desarrolla un plan para enfrentar los riesgos se vuelve a realizar el análisis con el objetivo de valorar la efectividad de las medidas propuestas para contrarrestar el efecto de estos o disminuir la probabilidad de ocurrencia.

El enfoque de la GR en los métodos analizados se orienta más a un análisis cualitativo, actualmente es mucho más complejo un análisis cuantitativo de los riesgos, pues cada día es más difícil valorar la información exactamente, o determinar la probabilidad de determinados riesgos.

Es necesario educar a los equipos de desarrollo de software en el Análisis y Gestión de Riesgos. Proporcionar una metodología flexible y las técnicas y herramientas necesarias para el Análisis y la Gestión de Riesgos constituye el primer paso para lograr el análisis sistemático y formal de los riesgos en los proyectos productivos de la universidad.

## CAPÍTULO 2: TÉCNICAS PARA EL ANÁLISIS DE RIESGOS

### 2.1 Introducción

En este capítulo se abordan las técnicas más utilizadas en el mundo aplicadas al análisis tanto cualitativo como cuantitativo de los riesgos. En el capítulo anterior se explicaron algunos de los modelos de Gestión de Riesgos que proponen la realización del análisis. La mayor parte de las técnicas que se abordan en este capítulo son propuestas y utilizadas en estos modelos.

Los modelos de gestión de riesgos estudiados en el capítulo anterior utilizan diversas técnicas para la estimación del impacto, la probabilidad de los riesgos y la priorización de estos.

Si bien es importante contar con una guía para el Análisis de Riesgos en cualquier proyecto, es necesario también disponer de un número de técnicas y herramientas de las cuales se pueda hacer uso a la hora de realizarlo. Estas deben ser diversas para brindar a los gestores del riesgo, la posibilidad de escoger las más adecuadas dependiendo del tipo de análisis que se desee realizar. Cada modelo propone un grupo de técnicas posibles a utilizar en dependencia del análisis de riesgos que definen, algunas de estas son comunes en diferentes modelos.

### 2.2 Métodos Generales para el Análisis de Riesgos

Algunos de los modelos y metodologías estudiadas en el capítulo anterior plantean métodos para realizar el Análisis de Riesgos, estos métodos proponen una serie de pasos a seguir utilizando determinadas herramientas para determinar impacto, probabilidad de ocurrencia y priorizar los riesgos, a continuación se abordan algunos de estos métodos.

#### 2.2.1 Análisis Mediante Tablas

Una de las técnicas para analizar los riesgos es el análisis mediante tablas. Son útiles métodos simples de análisis llevados a cabo por medio de tablas que aciertan en la identificación de la importancia relativa de los diferentes activos sometidos a amenazas (19). El análisis mediante tablas es un análisis matricial en el cual se determina el valor de una determinada variable deseada a través de la intersección en una matriz de dos valores estimados anteriormente.

El análisis mediante tablas propuesto por la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) es orientado a los activos, para realizarlo se determina una escala para calificar el valor de los activos, la magnitud del impacto, y la magnitud del riesgo, estas escalas son determinadas por el equipo encargado de analizar los riesgos.

**Determinación del Impacto:**

Para determinar el impacto de un riesgo en el análisis mediante tablas es necesario determinar la degradación de los activos cuando son expuestos ante los efectos del riesgo, con el valor de cada activo y la degradación de este se determina el impacto mediante tablas sencillas de doble entrada.

El impacto de cada riesgo sobre cada uno de los activos es ubicado en la tabla en dependencia del valor de este y la degradación que pueda causar. Los niveles del impacto (muy bajo, bajo, medio, alto, muy alto), son determinados por la organización o el proyecto que realice el análisis.

**Estimación del Riesgo:**

Tal como se calificó el valor de los activos, se califica la frecuencia del riesgo, y se combinan el impacto y la frecuencia en una tabla para determinar el riesgo. Es necesario recordar que MAGERIT define el riesgo como la medida del daño probable sobre un sistema (19).

En este caso los niveles de riesgo también son determinados por la organización o el proyecto en cuestión.

**Matriz de Probabilidad e Impacto**

La Matriz de Probabilidad e Impacto es también un tipo de análisis mediante tablas, utilizado para la priorización de los riesgos, generalmente estos se priorizan teniendo en cuenta la Exposición al Riesgo, la Matriz de Probabilidad e Impacto además de ordenar los riesgos determina cuáles son más críticos para el proyecto.

Las calificaciones son asignadas a los riesgos basándose en la probabilidad y el impacto evaluados. Esta matriz especifica combinaciones de probabilidad e impacto que llevan a la calificación de los riesgos como de prioridad baja, moderada o alta. Pueden usarse términos descriptivos o valores numéricos, dependiendo de la preferencia de la organización.

La organización debe determinar qué combinaciones de probabilidad e impacto resultan en una clasificación de riesgo, moderado o bajo. Se deben representar estos estados con colores. Normalmente, estas reglas para calificar los riesgos son especificadas por la organización de antemano, antes de comenzar el proyecto. Las reglas para calificar los riesgos pueden adaptarse al proyecto específico en el proceso Planificación de la Gestión de Riesgos.

En el caso de la Matriz de Probabilidad e Impacto se puede calificar un riesgo por separado para cada objetivo (por ejemplo, coste, tiempo y alcance). Además, puede desarrollar maneras de

determinar una calificación general para cada riesgo. Finalmente, las oportunidades y las amenazas pueden manejarse en la misma matriz, usando definiciones de los distintos niveles de impacto apropiados para cada una.

La puntuación del riesgo ayuda a guiar las respuestas a los riesgos. Por ejemplo, los riesgos que, de ocurrir, tienen un impacto negativo sobre los objetivos (amenazas), y que se encuentran en la zona de alto riesgo de la matriz, pueden requerir prioridad de acción y estrategias de respuesta agresivas. Las amenazas de la zona de riesgo bajo pueden no requerir una acción de gestión proactiva, más que ser incluidas en una lista de supervisión o añadidas a una reserva para contingencias.

Lo mismo ocurre con las oportunidades: aquellas que se encuentran en la zona de riesgo alto, que pueden obtenerse con más facilidad y que ofrecen los mayores beneficios deberían, por lo tanto, tener prioridad. Las oportunidades de la zona de riesgo bajo deberían ser supervisadas (2).

### 2.2.2 Análisis Algorítmico

Otro de los métodos brindados por la Metodología para la Gestión de Riesgos de los Sistemas de Información es el análisis algorítmico, en el cual siguiendo una serie de pasos se calculan diversos elementos necesarios para el Análisis de Riesgos desde el impacto de un riesgo, la eficacia de las salvaguardas planeadas contra este como la importancia del mismo en relación al resto de los riesgos.

El análisis algorítmico cuenta con dos enfoques: uno cualitativo y otro cuantitativo. La diferencia fundamental entre estos modelos es la información que brindan. El modelo cualitativo busca la valoración relativa del riesgo que corren los activos, o sea, qué es lo más frecuente y qué es lo menos; el análisis cuantitativo responde cuánto más y cuánto menos, con este último se puede determinar cuánto se puede perder por el impacto de una determinada amenaza, o cuán efectiva puede ser la salvaguarda en términos de reducción del impacto o la frecuencia de aparición de determinada amenaza (19).

El análisis algorítmico brinda información más detallada sobre los riesgos, su aplicación es más compleja pero debe tenerse en cuenta en los proyectos que deseen exactitud a la hora de analizarlos.

**Modelo Cualitativo:**

Este modelo busca saber qué hay sin cuantificarlo con precisión. En este modelo se trabaja sobre una escala discreta de valores, para esto se posicionan los activos en una escala de valor relativo, definiendo un valor como frontera entre los valores que preocupan y los que son despreciables.

Sobre esta escala de valor se mide tanto el valor del activo, como el impacto de una amenaza cuando ocurra y el riesgo al que está expuesto.

El impacto mide el daño sobre el activo, es la medida del coste si se materializa la amenaza, y el riesgo pondera el impacto con la frecuencia estimada de ocurrencia de esta.

Las estimaciones del impacto y riesgo residual incorporan la eficacia de las salvaguardas creadas para enfrentarse a la amenaza, ya sea limitando el impacto o reduciendo la frecuencia de ocurrencia. Con los resultados de estos parámetros se valora qué salvaguardas tomar para contrarrestar el riesgo.

El modelo combina los siguientes parámetros de análisis.

- Calibración del valor del activo.
- Calibración de la degradación que supone una amenaza como porcentaje.
- Calibración de la frecuencia de ocurrencia de la amenaza por medio de una escala discreta.
- Vertebración de un paquete de salvaguardas.
- Calibración de la eficacia de las salvaguardas por medio de un porcentaje.

El primer paso de este modelo es determinar el valor de cada activo, pues, aunque de manera relativa, es necesario valorar los elementos involucrados en el análisis. Para esto se determina una escala de valores simbólicos estableciendo una frontera entre los valores que son despreciables y los que son significativos. Es necesario señalar que las diferentes dimensiones de un análisis son independientes entre sí, por lo que se le da un valor a cada una de las dimensiones del activo en cuestión.

Luego se determina la dependencia entre los activos, la cual puede ser transitiva, y seguido se calculan una serie de elementos que dependen uno de otro.

- **Valor acumulado:** el valor acumulado sobre un activo es el mayor de los valores que soporta, bien propio o de alguno de sus superiores (activos de los cuales depende).

- **Degradación del valor de un activo:** cuando un activo es víctima de una amenaza parte de su valor se pierde, por lo cual se asigna un valor entre 0.0 y 1.0 que representa esta degradación.
- **Impacto acumulado de una amenaza sobre un activo:** es la medida de lo que implica una amenaza; es decir la pérdida del valor acumulado.
- **Impacto repercutido de una amenaza sobre un activo:** si un activo A depende de otro B las amenazas sobre B repercuten sobre A.

Una vez realizados estos cálculos se determina la frecuencia de las amenazas, para lo cual se utiliza también un grupo de valores simbólicos, entre los cuales existe un valor de frecuencia despreciable y otro de frecuencia normal de la amenaza. Tras determinar la frecuencia se calculan los siguientes elementos (19):

- Riesgo: es una función del impacto y la frecuencia.
- Riesgo acumulado: es una función del impacto acumulado de una amenaza sobre un activo y la frecuencia de esta.
- Riesgo repercutido: es una función del impacto repercutido de una amenaza sobre un activo y la frecuencia de esta.
- Paquete de salvaguardas: estas se despliegan frente a una amenaza, tienen una eficacia que se puede descomponer en eficacia frente al impacto y eficacia frente a la frecuencia.
- Degradación residual: degradación del activo luego de reducida la degradación por las salvaguardas.
- Impacto residual: impacto sobre el activo luego de ser reducido este por el paquete de salvaguardas.
- Frecuencia residual: frecuencia de la amenaza luego de haber sido reducida esta por el paquete de salvaguardas.
- Riesgo residual: Se calcula a raíz del impacto y frecuencia residuales.

**Modelo Cuantitativo**

En este modelo se trabaja con valores reales, siempre superiores a cero, se utiliza cuando se desea saber exactamente cuán frecuente puede ser una amenaza o cuánto podría costar exactamente la materialización de esta.

Se modela el grado de dependencia entre activos como un valor continuo entre 0.0 (activos independientes) y 1.0 (activos absolutamente dependientes; lo que ocurre sobre el inferior repercute contundentemente sobre el superior).

Se mide el valor del activo, propio o acumulado, y el impacto de una amenaza cuando ocurra el riesgo que supone. El riesgo pondera el impacto con la frecuencia estimada de ocurrencia de la amenaza, el impacto mide el coste si ocurriera y el riesgo mide la exposición en un período de tiempo.

Si la valoración del activo es económica, el impacto calculado es el coste introducido por la amenaza, y el riesgo calculado es la cantidad que hay que prever como pérdidas anuales. El modelo cuantitativo permite comparar el gasto en salvaguardas con la disminución de pérdidas.

Las estimaciones de impacto y riesgo residual incorporan la eficacia de las salvaguardas para enfrentarse a la amenaza.

El modelo combina los siguientes parámetros de análisis:

- Calibración del valor del activo por medio de una cantidad numérica.
- Calibración de la dependencia entre activos por medio de un porcentaje.
- Calibración de la degradación que supone una amenaza por medio de un porcentaje.
- Calibración de la frecuencia de ocurrencia de la amenaza por medio de una frecuencia.
- Vertebración de un paquete de salvaguardas.
- Calibración de la eficacia de las salvaguardas por medio de un porcentaje.

Este modelo plantea una serie de pasos a seguir para analizar los riesgos. En primer lugar se determina el valor de los activos, el cual es un valor real superior a cero, determinando un valor frontera entre los valores despreciables y los significativos.

Luego se determina la dependencia entre los activos, en este caso se determina el grado en que depende un activo de otro, la dependencia puede ser transitiva, y para cada caso existe una forma de determinarla.

Luego se calculan los siguientes elementos (19).

- Valor acumulado: suma de los valores de los activos superiores (de los que depende) ponderados por el grado de dependencia.
- Degradación del valor de un activo.
- Impacto acumulado de una amenaza sobre un activo.
- Impacto repercutido de una amenaza sobre un activo.
- Frecuencia de una amenaza.
- Riesgo.
- Riesgo acumulado.
- Riesgo repercutido.

### 2.2.3 Entrevistas y Reuniones

Otras de las técnicas recomendadas tanto para la estimación de la probabilidad de ocurrencia como para el impacto de los riesgos son las entrevistas y reuniones.

Los riesgos pueden ser evaluados en entrevistas o reuniones con participantes seleccionados por su familiaridad con las categorías de riesgo del orden del día. Entre ellos se incluyen los miembros del equipo del proyecto y, quizás, expertos ajenos al proyecto. Es necesario el juicio de expertos, ya que es posible que haya poca información sobre los riesgos en la base de datos de la organización de proyectos anteriores. Un facilitador experimentado puede dirigir la discusión, ya que los participantes pueden tener poca experiencia en la evaluación de riesgos.

El nivel de probabilidad de cada riesgo y su impacto sobre cada objetivo se evalúa durante la entrevista o reunión. Los detalles explicativos, incluidas las asunciones que justifican los niveles asignados, también se registran. Las probabilidades y los impactos de los riesgos se califican de acuerdo con las definiciones dadas en el plan de gestión de riesgos. A veces, los riesgos con calificaciones evidentemente bajas en cuanto a probabilidad e impacto no se califican, pero se incluyen en una lista de supervisión para su seguimiento futuro (2).

Estos métodos a pesar de ser subjetivos pueden ser la única solución viable cuando la información que se posee sobre los riesgos no es suficiente o fiable, los valores que se obtendrán

no serán exactos, pero sí lo suficientemente cercanos a la realidad, siempre que se eliminen las fuentes de sesgo, como para realizar un análisis válido de los riesgos.

### 2.2.4 Método Delphi

Para el Análisis de riesgos puede utilizarse el Método Delphi, a través del cual se puede analizar tanto la probabilidad de ocurrencia del riesgo, el impacto que este pueda tener para el proyecto y ayudar a los equipos de software en la toma de decisiones. Este método es una técnica que permite hacer predicciones en situaciones de incertidumbre.

El método Delphi es utilizado como sistema para obtener información sobre el futuro. Fue definido como un método de estructuración de un proceso de comunicación grupal que es efectivo a la hora de permitir a un grupo de individuos, como un todo, tratar un problema complejo (20).

Una de las características más importantes de este método es el anonimato, pues ningún experto conoce la identidad de los otros que componen el grupo, esto impide que sean influenciados por otros, y que se pueda actuar y defender sus argumentos sin el temor de que sepan su identidad en caso de que estos sean erróneos.

Ese método se realiza a través de la selección de un grupo de expertos que evalúan cualquier cuestión referida a acontecimientos futuros, con la utilización de este método se trata de consenso entre los participantes y a la vez que estos mantengan su autonomía. La capacidad de predicción de este método se basa en la utilización sistemática de un juicio intuitivo emitido por un grupo de expertos (21).

Dentro de los métodos de pronóstico se clasifica al Delphi como uno de los más cualitativos.

Este método cuenta con una serie de fases, las cuales son simplemente mencionadas a continuación, pues en el capítulo 3 se explica con más profundidad este método:

1. Formulación del problema.
2. Elección de expertos.
3. Elaboración y lanzamiento de los cuestionarios (esta fase se realiza en paralelo con la fase 2).
4. Desarrollo práctico y explotación de los resultados.

La cantidad óptima de expertos necesarios para llevar a cabo este método no se ha determinado, pero estudios realizados plantean que es necesario un número mínimo de 7 expertos, debido a

que el error disminuye por cada experto que se añade hasta llegar a 7 pero no se recomienda que sea mayor de 30 pues el incremento del coste y trabajo no compensa la mejora que se realiza en la previsión (21).

### 2.3 Técnicas para la Estimación de la Probabilidad de Ocurrencia del Riesgo

La evaluación de probabilidad investiga la probabilidad de ocurrencia de cada riesgo específico. Es necesario evaluar la probabilidad de ocurrencia de cada uno de los riesgos obtenidos en la fase de identificación.

La probabilidad de ocurrencia nunca será un valor exacto, pues es imposible determinar con exactitud la probabilidad de que algo ocurra, simplemente existen técnicas a través de las cuales se puede estimar esta probabilidad de forma tal que sea lo más cercana a la realidad posible, en este epígrafe se abordarán estas técnicas.

#### 2.3.1 Técnicas definitorias

Intentan definir la probabilidad de diferentes maneras con la idea de suministrar un lenguaje sin ambigüedades para describir el término de probabilidad.

La probabilidad existe en una banda, que abarca desde lo imposible hasta la certeza total. Hay muchas maneras de describir este espectro, y las técnicas definitorias para evaluar probabilidad de riesgos ofrecen diferentes maneras de describir la escala, para dar a los evaluadores marcos de referencia con cierto significado, contra los cuales, se pueda estimar la probabilidad de un riesgo dado. Por ejemplo, distintas posiciones del espectro de probabilidad pueden ser definidos, usando calificativos (por ejemplo bajo, medio, alto), frases (improbable, imposible, bastante probable) medidas de posibilidades (1:50, 1:10, 1:3), números (porcentajes o decimales), o rangos (1-10%, 20-50%).

Los métodos definitorios son utilizados más comúnmente por practicantes de riesgos, pero hay varios problemas que afectan su efectividad. Por ejemplo, tanto los calificativos como las frases son ambiguos y pueden ser interpretados con subjetividad.

Los otros métodos por definiciones, tienen también problemas, ya que las fracciones de posibilidades son pocos familiares para muchos. Los porcentajes o valores decimales específicos introducen una falsa aparente precisión, donde la realidad es menos cierta, y los rangos fijos son artificiales y no reflejan la verdadera banda de probabilidad de un riesgo en particular.

Para todos los métodos definitorios los evaluadores enfrentan el desafío de justificar, cual punto en la escala definida debe seleccionar, ya que el cálculo de las probabilidades de riesgo sigue siendo subjetiva (22).

### 2.3.2 Técnicas comparativas

Estas técnicas utilizan varios comparadores contra los cuales la probabilidad de un riesgo dado puede ser comparada.

Una serie de técnicas han sido desarrolladas para asistir en el cálculo de probabilidades de riesgos, que proveen valores contra los cuales, se pueden comparar las posibilidades de ocurrencia de un riesgo, preguntando si la probabilidad del riesgo que está sucediendo, es más, o menos, o tiene el mismo valor que se está presentando. Todas estas técnicas apuntan a ajustar el comparador hasta que el evaluador no puede distinguir una diferencia entre la probabilidad del riesgo y el valor de comparación. Este valor se toma entonces, como el mejor estimado de la probabilidad del riesgo. Hay distintas formas de presentar probabilidades, contra las cuales la probabilidad de un riesgo puede ser comparada. Estas incluyen:

- **Apuestas:** Esta técnica plantea realizar una apuesta y ajustarla hasta que los apostantes estén igual de seguros, luego, calcular la probabilidad de riesgos como la apuesta menor dividida entre la cantidad total en juego.
- **Orientado según su valor:** La probabilidad del riesgo se compara con un evento cuya probabilidad se conoce, por ejemplo, ¿es más, o menos, que la posibilidad de obtener 10 caras en un experimento de lanzamiento de una moneda? Se presentan distintos eventos hasta que el evaluador no distingue una diferencia.
- **Posibilidad relativa:** Similar al método de orientación según su valor, se le pregunta al evaluador, cuánto más posiblemente puede ocurrir un riesgo que algún otro evento cuya probabilidad sea conocida. El proceso puede continuar usando el método "orientado en el valor", hasta que se alcanza la igualdad, o la probabilidad diferencial puede sumarse al valor de comparación para obtener la probabilidad estimada del riesgo que ocurre.

Aunque los métodos de comparación parecen ser fáciles de usar, estos tienen un número de dificultades, que incluyen problemas para entender los comparadores. Adicionalmente, las

evaluaciones que usan técnicas comparativas están particularmente sujetas a sesgos perceptivos y heurísticos (22).

### 2.3.3 Método del Estado Natural

Este método sugiere que la probabilidad está basada en una descripción de varios "estados naturales" dentro del medio ambiente de proyectos.

Una técnica usada con menor frecuencia, ha sido desarrollada para deducir probabilidades de riesgos, a partir de la descripción del estado de una variable relacionada con proyectos (por eso, el método se llama técnica de "estado natural"). Esto incluye la descripción de un rango de situaciones o escenarios alternos, que pudieran ocurrir para una fuente de riesgos dada en un proyecto, donde cada escenario tiene una probabilidad asociada de riesgos relacionados que puedan surgir. El evaluador luego identifica dónde está ubicado el proyecto en la escala de escenarios, y a continuación, el chance de los riesgos con posibilidad de ocurrencia en esa área, es inferido.

Este método tiene la ventaja de ser menos subjetivo que otros, ya que la situación del proyecto se compara con un conjunto de alternativas definido y objetivo, y la evaluación se basa en hechos conocidos del proyecto, más que en la confianza en una opinión subjetiva. Por supuesto ello requiere que, para cada fuente de riesgos, se desarrollen y clasifiquen todos los escenarios, por adelantado.

Esto se puede hacer a un nivel genérico, o bien los escenarios pueden asociarse con riesgos específicos; cuanto mas detalle mejor, pero se requiere un mayor trabajo para desarrollar suficientes escenarios que cubran todos los riesgos.

El método de estado natural también permite la comparación de exposición a riesgos para proyectos relacionados, desde una fuente común dada y facilita el aprendizaje de la experiencia previa, ya que los "estados naturales" pueden construirse a partir de los resultados de proyectos anteriores (22).

## 2.4 Técnicas para la estimación del impacto del riesgo y la toma de decisiones

La evaluación del impacto de los riesgos investiga el posible efecto sobre un objetivo del proyecto, como tiempo, coste, alcance o calidad, incluidos tanto los efectos negativos por las amenazas que implican, como los efectos positivos por las oportunidades que generan (2).

Parte del análisis de riesgos es la toma de decisiones, cuando el equipo de proyecto se encuentra en una situación en la cual debe tomar un camino entre varias opciones es necesario evaluar las ventajas y desventajas de cada una de estas, entre las técnicas para la toma de decisiones se encuentran las que se exponen a continuación.

Para la estimación del impacto del riesgo se pueden utilizar técnicas abordadas anteriormente como las entrevistas y reuniones, el Método Delphi a continuación se abordan algunas técnicas que pueden ser utilizadas para la estimación del impacto de un riesgo y la toma de decisiones.

### 2.4.1 Análisis de Sensibilidad

El análisis de sensibilidad ayuda a determinar qué riesgos tienen el mayor impacto posible sobre el proyecto. Este método examina la medida en que la incertidumbre de cada elemento del proyecto afecta al objetivo que está siendo examinado, cuando todos los demás elementos inciertos se mantienen en sus valores de línea base. Una representación típica del análisis de sensibilidad es el diagrama con forma de tornado, que es útil para comparar la importancia relativa de las variables que tienen un alto grado de incertidumbre con aquellas que son más estables (2).

Es una de las partes más importantes en la programación lineal, muy útil en la toma de decisiones, pues permite determinar cuándo una solución sigue siendo óptima. Permite determinar qué tan sensible es la respuesta óptima del método Simplex, al cambio de datos como las ganancias o disponibilidad de recursos.

### 2.4.2 Valor Monetario Esperado.

El análisis del valor monetario esperado es un concepto estadístico que calcula el resultado promedio cuando el futuro incluye escenarios que pueden ocurrir o no (es decir, análisis con incertidumbre). El valor monetario esperado de las oportunidades generalmente se expresará con valores positivos, mientras que el de los riesgos será negativo. Este se calcula multiplicando el valor de cada posible resultado por su probabilidad de ocurrencia, y sumando los resultados. Este tipo de análisis se usa comúnmente en el análisis mediante árbol de decisiones. Se recomienda el uso del modelado y la simulación para el análisis de los riesgos de costes y del cronograma, porque son más efectivos y están menos sujetos a errores de aplicación que el análisis del valor monetario esperado (2).

### 2.4.3 Árbol de Decisiones.

El análisis mediante árbol de decisiones normalmente se estructura usando un diagrama de árbol de decisiones que describe una situación que se está considerando, y las implicaciones de cada una de las opciones disponibles y los posibles escenarios. Incorpora el coste de cada opción disponible, las probabilidades de cada escenario posible y las recompensas de cada camino lógico alternativo. Al resolver el árbol de decisiones se obtiene el valor monetario esperado (u otra medida de interés para la organización) correspondiente a cada alternativa, cuando todas las recompensas y las decisiones subsiguientes son cuantificadas, este análisis puede realizarse tanto para la toma de decisiones como para la estimación del impacto del riesgo (2).

La mayor limitación del árbol de decisiones viene dada al analizar un número pequeño de opciones, además, se requiere que todos los factores se presenten cuantitativamente. A pesar de estas limitaciones constituye una técnica cuantitativa poderosa para calcular el futuro posible.

### 2.4.4 Modelado y simulación

Una simulación de proyecto usa un modelo que traduce las incertidumbres especificadas a un nivel detallado del proyecto en su impacto posible sobre los objetivos del proyecto. Las simulaciones normalmente se realizan usando la técnica Monte Carlo. En una simulación, el modelo del proyecto se calcula muchas veces (iteradas), utilizando valores de entrada seleccionados al azar de una función de distribución de probabilidad (por ejemplo, coste de los elementos del proyecto o duración de las actividades del cronograma) que se elige para cada iteración de las distribuciones de probabilidad de cada variable. Se calcula una distribución de probabilidad (por ejemplo, coste total o fecha de conclusión) (2).

## 2.5 Conclusiones Parciales

Las técnicas utilizadas para el Análisis de Riesgos pueden ser muy subjetivas, sobre todo las relacionadas con la estimación de la probabilidad de ocurrencia de los riesgos, por lo que es necesario contar para poder utilizar con éxito muchas de las técnicas expuestas en este capítulo con una base de datos en el proyecto con información sobre los riesgos en proyectos similares y personal con experiencia en la Gestión de Riesgos.

Una de las técnicas más completas para el análisis son las propuestas por la Metodología de Análisis y Gestión de Riesgos para los Sistemas de Información (MAGERIT), sin embargo, no se adaptan a las particularidades de los proyectos de desarrollo de software debido a que estas están dirigidas principalmente a los sistemas de información y trabajan con parámetros como la

frecuencia de ocurrencia de una amenaza que no existen en los proyectos de desarrollo de software.

Otro aspecto necesario es eliminar todas las fuentes posibles de sesgo a la hora de realizar estas estimaciones dentro del Análisis de Riesgos, eliminándolas se podrán obtener resultados más precisos en este proceso de la Gestión de Riesgos.

De los métodos y técnicas analizados en este capítulo no se utilizarán todos en la solución e esta investigación. El Análisis Mediante Tablas y el Algorítmico en sus dos variantes deben ser adaptados a las necesidades de los proyectos de desarrollo de software, utilizando los parámetros del Análisis de Riesgos correspondientes. Las Entrevistas y Reuniones, el Método Delphi, la Matriz de Probabilidad e Impacto y el Árbol de Decisiones pueden ser utilizados sin necesidad de adaptaciones ni cambios, sin embargo, otros métodos como el Modelado y Simulación deben ser estudiados más a fondo debido a su complejidad, en el caso del análisis de sensibilidad, su aplicación al Análisis de Riesgos en los proyectos de software requiere de estudios posteriores.

Las técnicas de priorización analizadas realizan esta actividad a través del cálculo de la Exposición al Riesgo, determinada en función de la probabilidad de ocurrencia de cada riesgo y su impacto en el proyecto.

La subjetividad de las técnicas comparativas y definitorias hacen que su uso requiera de experiencia en el campo de los riesgos, en caso de no ser así podrían arrojar resultados erróneos, teniendo en cuenta la poca madurez de los proyectos de software en la Universidad no se tendrán en cuenta estas técnicas en los resultados de esta investigación.

# CAPÍTULO 3: GUÍA METODOLÓGICA PARA EL ANÁLISIS DE RIESGOS

## 3.1 Introducción

En este capítulo se brinda una Guía Metodológica dirigida a los proyectos de software con el fin de orientar a los equipos de desarrollo en su Análisis de Riesgos de una manera organizada y eficiente para lograr la homogenización de este proceso en la Universidad de las Ciencias Informáticas.

La principal característica de esta guía es la flexibilidad y adaptación para cualquier tipo de análisis que se quiera realizar, brindando para cada momento las técnicas adecuadas, con cuya utilización el equipo logrará los resultados esperados.

En este capítulo se brinda también la descripción y ejemplificación de las técnicas propuestas en cada momento y su adaptación en muchos casos al proceso de Gestión de Riesgos de la UCI. La guía no cuenta con una serie de pasos consecutivos a seguir, sino que permite al cliente escoger entre las posibles variantes que esta brinda.

## 3.2 Objetivos de la Guía Metodológica para el Análisis de Riesgos.

Los objetivos de la presente Guía Metodológica son los siguientes:

- Lograr una vía formal para la realización del Análisis de Riesgos en la Universidad de las Ciencias informáticas.
- Ofrecer un método formal para analizar los riesgos identificados por el equipo de Gestión de Riesgos que se adapte a las particularidades de los proyectos de software que se llevan a cabo en la Universidad de las Ciencias informáticas basado en las tendencias existentes en el mundo.
- Lograr que la información necesaria para la realización del Plan de Mitigación sea más fiable y su obtención se estandarice en los proyectos de software de la UCI.

## 3.3 Propuesta de Guía Metodológica para el Análisis de Riesgos.

En este epígrafe se expone conceptualmente en qué consiste el Análisis de Riesgos propuesto en esta Guía Metodológica. Partiendo del estudio del Análisis de Riesgos en la UCI y su realización a nivel mundial se evidencia la necesidad de contar con un método para el Análisis de Riesgos para los proyectos de software. La diferencia en los intereses de cada proyecto en

particular hace que esta actividad no pueda ser rígida y que se brinde opciones al equipo de desarrollo en cuanto al tipo de análisis que desee realizar.

Inicialmente se impone la necesidad de conocer la probabilidad de ocurrencia de cada riesgo, el impacto que este puede ocasionar en caso de materializarse y su importancia con respecto al resto de los riesgos identificados para su posterior tratamiento.

Cada riesgo puede afectar de manera diferente a un proyecto, incluso un mismo riesgo puede impactar de diversas formas. El impacto puede verse reflejado en varias componentes del proyecto, principalmente en el coste, planificación temporal, la calidad del mismo y el alcance (2), esta guía divide en Análisis de Riesgos principalmente en el análisis orientado a los activos y no orientado a activos. La diferencia fundamental radica en que el primero se realiza a partir del valor de los activos y su aplicación es fundamentalmente para analizar los riesgos en cuanto a coste.

Otra de las decisiones que el equipo de Gestión de Riesgos es la correspondiente a realizar análisis cualitativo, cuantitativo o ambos, la guía permite la realización de cada uno de estos análisis por separado, el cuantitativo a continuación del cualitativo e incluso escoger uno de estos sin necesidad de realizar el otro.

Luego de determinar la probabilidad y el impacto de los riesgos la guía propone la priorización de los mismos independientemente del análisis realizado y las técnicas que se pueden utilizar para su realización.

### 3.4 Roles del Análisis de Riesgos:

Como todo proceso dentro de la Gestión de Proyectos, el análisis de riesgos debe ser realizado por personas capacitadas para cada una de las actividades que se requieran realizar. Por esto se hace necesario definir los roles que participan en el análisis y especificar los requisitos que deben cumplir y sus responsabilidades dentro del proceso.

Los roles responsables de realizar las tareas del Análisis de Riesgos son el Equipo de Gestión de Riesgos (EGR) y el Líder o Gestor de Riesgos (GR). En la tabla 2 se encuentra cada rol, con las funciones que debe cumplir y las habilidades requeridas por cada uno.

| Rol | Funciones | Habilidades |
|---|---|---|
| Equipo de GR | Recopilar información sobre los riesgos y su impacto en el proyecto.<br>Analizar la probabilidad de ocurrencia y el impacto de los riesgos.<br>Priorizar los riesgos.<br>Actualizar el Registro de Riesgos con los datos arrojados en el análisis. | Dominar técnicas de recopilación de información.<br>Dominar técnicas de estimación de probabilidad de los riesgos.<br>Dominar técnicas de estimación de impacto de los riesgos.<br>Dominar técnicas de priorización de los riesgos.<br>Poseer conocimientos sobre probabilidades y matemática aplicada. |
| Gestor de Riesgos | Dirigir y guiar las actividades del Análisis de Riesgos.<br>Supervisar el cumplimiento de las actividades relacionadas con el Análisis de Riesgos.<br>Planificar y realizar la Priorización de los Riesgos<br>Mantener al equipo informado y lograr la comunicación entre sus miembros. | Dominar técnicas de recopilación de información.<br>Dominar técnicas de estimación de probabilidad de los riesgos.<br>Dominar técnicas de estimación de impacto de los riesgos.<br>Dominar técnicas de priorización de los riesgos.<br>Poseer conocimientos sobre probabilidades y matemática aplicada<br>Dominar técnicas de dirección de equipos |

**Tabla 2: Roles involucrados en el Análisis de Riesgos con sus funciones y habilidades**

### 3.5 Estructura del Análisis de Riesgos

En la figura 6 se muestra la estructura del Análisis de Riesgos en el modelo propuesto, a continuación se abordan las entradas y salidas de este proceso, las técnicas y herramientas no se analizan a continuación pues en este capítulo se dedica un epígrafe para su explicación y ejemplificación para mejor comprensión del equipo de Gestión de Riesgos.

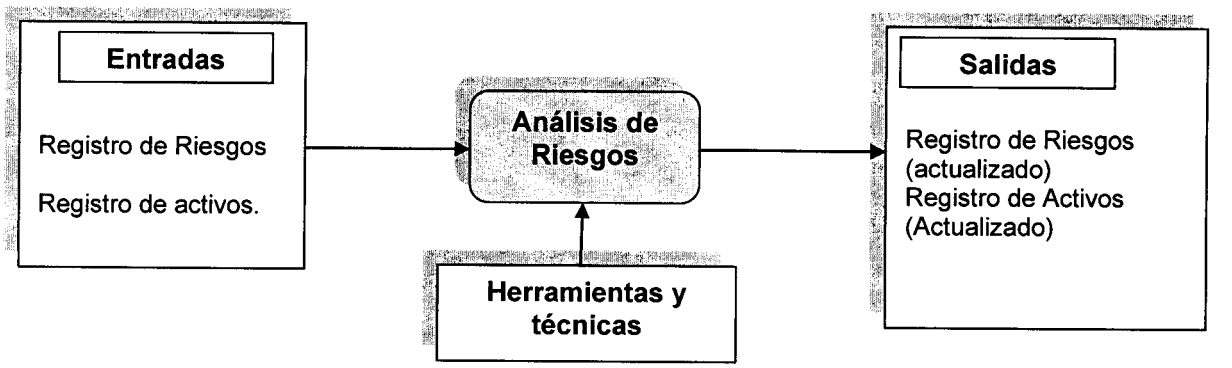


**Figura 6: Análisis de Riesgos en el modelo propuesto.**

### 3.5.1 Entradas

Para el Análisis de Riesgos debe contar con las siguientes entradas:

Registro de Riesgos (Anexo 3): constituye el artefacto más importante del Análisis de Riesgos, pues se utiliza desde la identificación de los riesgos y es el que se actualiza a lo largo de todo el análisis incluyéndole la probabilidad del riesgo, el impacto y en este registro es donde se realiza la priorización, para esto se cuenta con una plantilla que se puede observar en el Anexo 3.

En caso de que se vaya a realizar un análisis orientado a los activos es necesario también contar con el Registro de Activos (Anexo 4), el cual es un documento con el listado de todos los activos con los que se cuenta, desde programas, información hasta equipamiento.

### 3.5.2 Salidas

Como salida del Análisis de Riesgos se encuentra el Registro de Riesgos actualizado con los datos de la probabilidad de ocurrencia, el impacto en el proyecto y ordenado por la prioridad de los riesgos.

En caso de haberse realizado el análisis orientado a los activos también se obtiene como salida el Registro de Activos actualizado con el valor de cada activo.

En cada una de las actividades se actualizará el registro de riesgos.

## 3.6 Actividades para el Análisis de Riesgos

Las actividades para el Análisis de Riesgos son básicamente las mismas sin importar el tipo de análisis seleccionado por el equipo de Gestión de Riesgos, sin embargo, existen diferencias en las técnicas y los artefactos relacionados.

La primera actividad del Análisis de Riesgos debe ser una reunión del Equipo de Gestión de Riesgos para determinar si el análisis que van a realizar será orientado o no a los activos, esta reunión define por completo el resto de las actividades, pues las técnicas a utilizar son completamente diferentes. Una vez determinado si el análisis será o no orientado a los activos se decide si se realizará un análisis cualitativo, cuantitativo o ambos, esta es la próxima decisión del Análisis de Riesgos.

### 3.6.1 Análisis Orientado a los Activos

A continuación se explican las actividades de Análisis de Riesgos correspondientes al análisis orientado a los activos, estas actividades son comunes para el análisis cualitativo y cuantitativo, en cada técnica se especifica para cuál de estos dos análisis se puede utilizar. Como entradas para este análisis se requieren el Registro de Riesgos y el Registro de Activos. La figura 7 muestra las actividades para el análisis orientado a los activos.

**Actividad: Identificar Activos:**

El objetivo de esta actividad es determinar los activos del proyecto, en esta se crea el Registro de Activos y la ejecuta el Equipo de Gestión de Riesgos.

**Actividad: Valorar activos.**

El objetivo de esta actividad es determinar el valor de cada activo del proyecto para la realización del análisis. Tiene como entrada el Registro de Activos y la salida es este mismo registro actualizado con el valor de los activos. Los responsables de esta actividad son los miembros del equipo de Gestión de Riesgos.

**Actividad: Estimación de la Probabilidad del Riesgo.**

El objetivo de esta actividad es estimar la probabilidad de los riesgos, se tiene como entrada el Registro de Riesgos, el cual es actualizado con la probabilidad de ocurrencia de cada uno de estos. Para la estimación de la probabilidad de los riesgos se pueden utilizar las siguientes técnicas:

- Entrevistas y reuniones (cualitativo).
- Método Delphi (cualitativo y cuantitativo).

**Actividad: Estimación del Impacto del Riesgo.**

Esta actividad tiene como objetivo estimar el impacto de los riesgos, como entrada de esta actividad se cuenta con el Registro de Riesgos y el Registro de Activos, el cual se actualiza con el impacto de los riesgos, el rol responsable de esta actividad es el Equipo de Gestión de Riesgos y se pueden utilizar las siguientes técnicas:

- Análisis Mediante Tablas (cualitativo).
- Análisis Algorítmico (cualitativo y cuantitativo).

**Actividad: Priorizar Riesgos.**

Esta actividad tiene como objetivo priorizar los riesgos para su posterior tratamiento, como entrada de esta actividad se tiene el Registro de Riesgos, el cual se ordena según la prioridad determinada para cada riesgo, los roles responsables de esta actividad son el Gestor de Riesgos y el Equipo de Gestión de Riesgos. Las técnicas que se pueden utilizar para esta actividad son:

- Análisis Mediante Tablas (cualitativo).
- Análisis Algorítmico (cualitativo y cuantitativo).

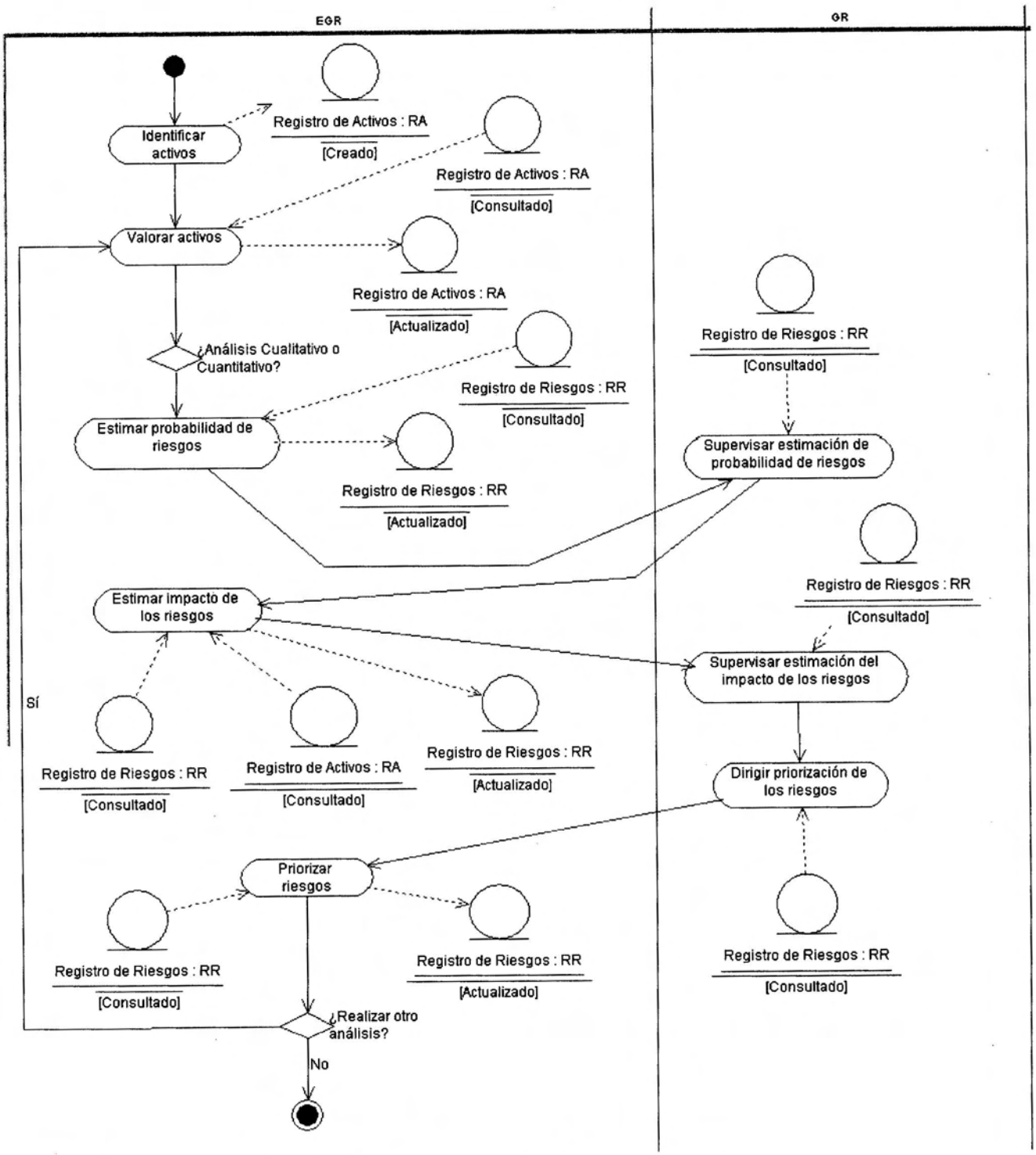


**Figura 7: Actividades del Análisis de Riesgos orientado a los activos**

### 3.6.2 Análisis no Orientado a los Activos.

El análisis no orientado a activos sigue básicamente las mismas actividades que el orientado a activos, aunque las técnicas son diferentes, la figura 8 muestra las actividades de este análisis. La entrada es el Registro de Riesgos. A continuación se describen las actividades de este análisis, con los roles responsables de realizarlas y las técnicas a utilizar, en cada técnica se especifica para qué tipo de análisis (cualitativo o cuantitativo) se recomienda.

**Actividad: Estimación de la Probabilidad del Riesgo.**

El objetivo de esta actividad es estimar la probabilidad de los riesgos, se tiene como entrada el Registro de Riesgos, el cual es actualizado con la probabilidad de ocurrencia de cada uno de estos. Para la estimación de la probabilidad de los riesgos se pueden utilizar las siguientes técnicas:

- Entrevistas y reuniones (cualitativo).
- Método Delphi (cualitativo y cuantitativo).

**Actividad: Estimación del Impacto del Riesgo.**

Esta actividad tiene como objetivo estimar el impacto de los riesgos, como entrada de esta actividad se cuenta con el Registro de Activos, este se actualiza con el impacto de los riesgos, el rol responsable de esta actividad es el Equipo de Gestión de Riesgos y se pueden utilizar las siguientes técnicas:

- Método Delphi (cualitativo y cuantitativo).
- Entrevistas y reuniones (cualitativo).
- Árboles de decisión (cuantitativo).

**Actividad: Priorizar Riesgos.**

Esta actividad tiene como objetivo priorizar los riesgos para su posterior tratamiento, como entrada de esta actividad se tiene el Registro de Riesgos, el cual se ordena según la prioridad determinada para cada riesgo, los roles responsables de esta actividad son el Gestor de Riesgos y el Equipo de Gestión de Riesgos. Las técnicas que se pueden utilizar para esta actividad son:

- Matriz de Probabilidad e Impacto (cualitativo).
- Reuniones y Entrevistas (cualitativo y cuantitativo).

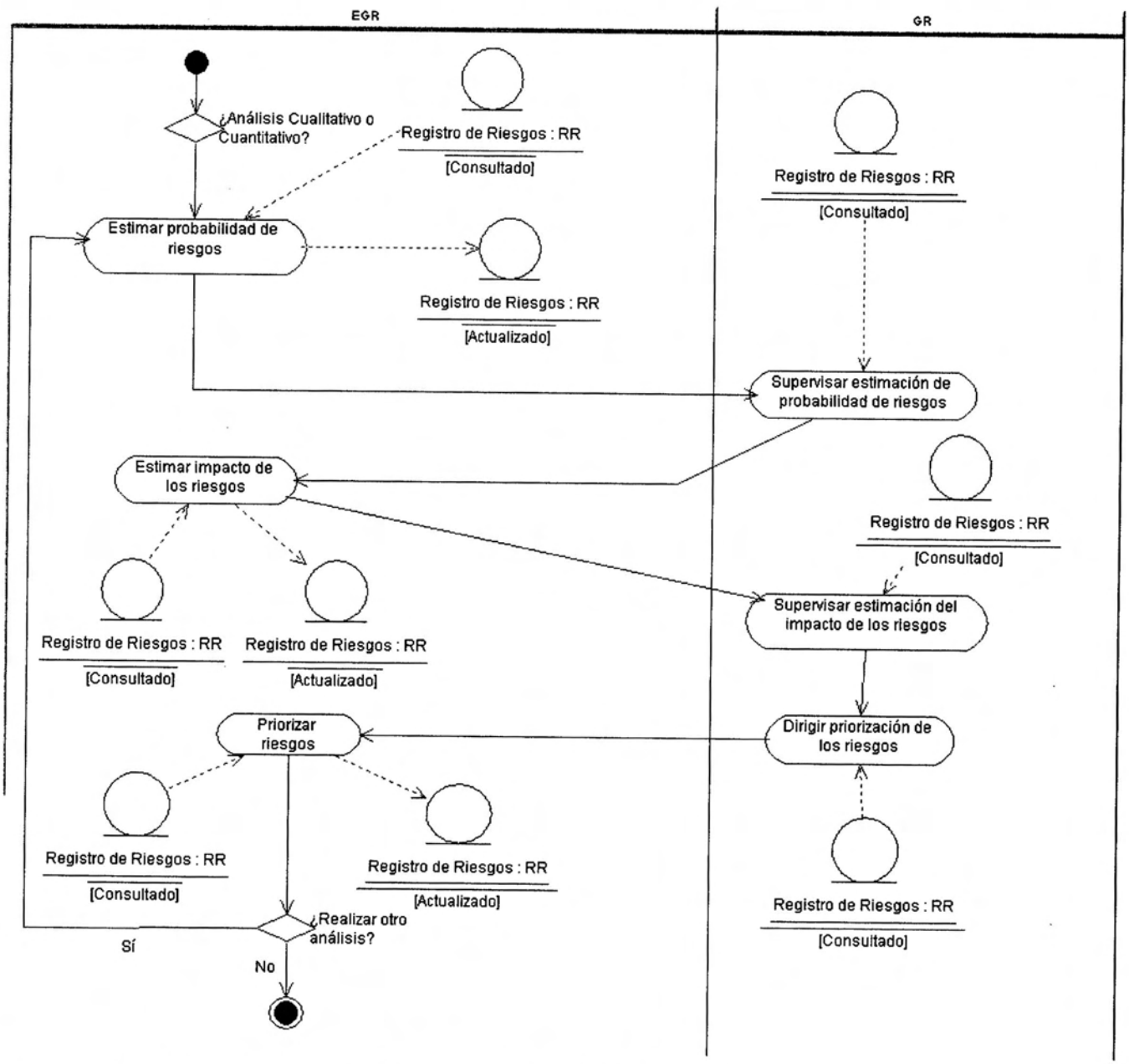


**Figura 8: Actividades del Análisis de Riesgos no orientado a activos**

### 3.7 Técnicas a utilizar para el Análisis de los Riesgos.

En este epígrafe se detallan las técnicas para realizar el análisis de riesgos según el modelo propuesto, Cada técnica está explicada y se especifica en qué actividad del análisis es utilizada.

### 3.7.1 Análisis mediante tablas

El análisis mediante tablas es una técnica simple para realizar el análisis de los riesgos, se propone para el análisis orientado a los activos y trabaja sobre el valor de los mismos, el impacto que causa el riesgo sobre estos y la probabilidad de ocurrencia de los mismos, para lo cual se utilizan escalas de degradación, impacto y probabilidad determinadas por el proyecto.

Para realizar el análisis mediante tablas es necesario disponer de técnicas generales que permitan la determinación de la probabilidad e impacto del riesgo las cuales serán abordadas más adelante en este epígrafe.

El primer paso es determinar el valor de los activos del proyecto, luego se determina para cada riesgo la degradación que causa sobre cada uno de los activos. Haciendo uso de una tabla y con los datos del valor del activo y su degradación frente a la acción de cada uno de los riesgos que se analizan, se ubica en la tabla el impacto del riesgo para cada activo, con estos impactos se determina el impacto general del riesgo.

Para estimar la degradación del activo frente al riesgo se debe hacer uso de técnicas de expertos para una correcta estimación.

La determinación del impacto del riesgo se realiza a través de la asignación de valores a cada uno de los niveles de impacto y se promedian esto, utilizando una escala definida por el equipo del proyecto.

La próxima tarea para el análisis es la determinación de la probabilidad de ocurrencia del riesgo haciendo uso de métodos para la estimación del impacto. Con la probabilidad de ocurrencia se ubica en otra tabla con entradas impacto y probabilidad de ocurrencia para determinar la prioridad del riesgo. Este análisis puede hacerse también cuantitativamente, utilizando valores reales en lugar de las escalas propuestas.

Los valores de las tablas son determinados por el proyecto de antemano, a continuación se ejemplifica el análisis mediante tablas.

La escala a utilizar en el ejemplo es la siguiente:

**Escala:**

**MB:** Muy bajo

**B:** Bajo

**M:** Medio

**A:** Alto

**MA:** Muy alto

El Equipo de Gestión de Riesgos es el encargado de definir la escala que utilizará, para eso debe determinar qué representa un valor muy bajo, bajo, medio, alto y muy alto, o cualesquiera que sean los valores a utilizar en la escala, estableciendo los límites entre uno y otro.

En este ejemplo se analizarán 3 activos del proyecto, estos son los siguientes:

Activo A, valor bajo (B).

Activo B, valor muy alto (MA).

Activo C, valor medio (M).

Se analizará en este caso un riesgo X. Luego de analizar el riesgo en profundidad y su acción sobre cada activo se determina que la degradación de cada uno de los activos una vez expuestos al riesgo, para esto se utiliza una escala de degradación, en este caso con 3 niveles, baja (B), media (M) y alta (A). La degradación de cada uno de los activos sería la siguiente:

Degradación de A: Alta.

Degradación de B: Media.

Degradación de C: Baja.

Utilizando la siguiente tabla se determinará el impacto del riesgo sobre cada uno de los activos, para esto se utiliza una combinación de valor (filas) contra degradación (columnas) que resulta en el impacto del riesgo sobre el activo. La tabla a utilizar puede ser definida por el Equipo de Gestión de Riesgos en conjunto con el Gestor de Riesgos, sin embargo se propone la siguiente a partir de la Guía de Técnicas de la Metodología para el Análisis y la Gestión de Riesgos de los Sistemas de Información (MAGERIT).

Tras la ubicación de cada activo en la tabla se determina que el impacto de X para cada uno de estos es el siguiente:

Impacto sobre A: bajo (B)

Impacto sobre B: Alto (A)

Impacto sobre C: Muy bajo (MB)

Luego se determina el impacto del riesgo sobre el proyecto en general, para esto se da valores a los niveles de impacto y se promedian, se define una correspondencia entre los niveles de impacto y valores reales, en este caso de 1(muy bajo), hasta 5 (muy alto):

**MB:** muy bajo = 1

**B:** bajo = 2

**M:** medio = 3

**A:** alto = 4

**MA:** Muy alto = 5

| Impacto | | Degradación | | |
|---|---|---|---|---|
| | | Baja | Media | Alta |
| Valor | MA | M | A | |
| | A | B | M | A |
| | M | MB | B | M |
| | B | MB | MB | B |
| | MB | MB | MB | MB |

**Tabla 3: Impacto del riesgo sobre un activo.**

**Fuente: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Guía de Técnicas (19).**

De esta forma se calcularía el impacto del riesgo sobre el proyecto:

Impacto $_X$ = [Impacto $_A$ (B)+ Impacto $_B$ (A)+ Impacto $_C$ (MB)]/3

Impacto $_X$ = (2+4+1)/3 = 2

Llevando este resultado a la escala anterior se obtiene que el impacto de X sobre el proyecto es Bajo (B).

Una vez determinado el impacto del riesgo se determina la probabilidad de ocurrencia de este a través de técnicas para la estimación de la probabilidad de ocurrencia del riesgo, En este caso se propone la siguiente escala de probabilidades:

**B:** Baja

**Media:** M

**Alta:** A

**Muy Alta:** MA

Luego se ubica el riesgo en una tabla por su impacto y probabilidad, los valores de la tabla son igualmente determinados con antelación por el equipo de Gestión de Riesgos en conjunto con el Gestor de Riesgos:

| prioridad | | Probabilidad de ocurrencia | | | |
|---|---|---|---|---|---|
| | | Baja | Media | Alta | Muy Alta |
| impacto | MA | A | | | |
| | A | M | A | | |
| | M | B | M | A | |
| | B | MB | B | M | A |
| | MB | MB | MB | B | M |

**Tabla 4: Prioridad del riesgo.**

**Fuente: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Guía de Técnicas (19).**

En este caso el riesgo X tiene probabilidad de ocurrencia Muy alta (MA), por lo que la Prioridad del riesgo sería Alta.

Este análisis se debe realizar para cada uno de los riesgos identificados en el Registro de Riesgos.

### 3.7.2 Análisis Algorítmico (modelo cualitativo)

El análisis algorítmico es propuesto por la Metodología para el Análisis y la Gestión de Riesgos de los Sistemas de Información (MAGERIT) en su guía de técnicas (19) , sin embargo ha sido modificado para su adaptación a esta guía de Análisis de Riesgos.

Como el análisis mediante tablas el análisis algorítmico es orientado a los activos, el primer paso para su realización es dar valor a los activos a través de una escala de valores simbólicos $V_i$ que cumpla con la propiedad de que para toda i, $V_1 < V_{i+1}$.

Luego se determina la dependencia entre los activos, como un valor booleano, teniendo en cuenta que la dependencia puede ser transitiva e incluso dibujar figuras de diamantes como se muestra en la figura 9.

En este caso A depende directamente de B1 y B2, B1 y B2 dependen de C, por lo que A depende de C indirectamente. (19)

Una vez obtenido el valor de los activos se determina a través de técnicas generales la degradación de cada activo en caso de materializarse el riesgo que se está analizando, es

necesario tener en cuenta que los activos que dependen (directa o indirectamente) de un activo afectado por un riesgo, son víctimas de la misma degradación que el activo del cual dependen.

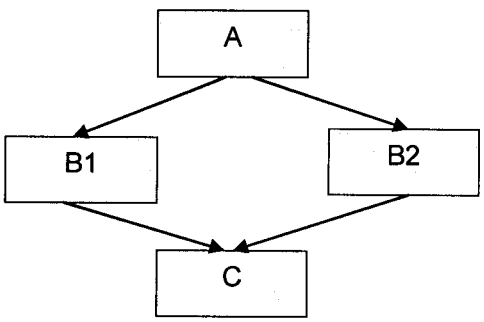


**Figura 9: Dependencia entre activos. Análisis Algorítmico Cualitativo (19)**

Una vez determinada la degradación de cada activo se calcula el impacto del riesgo en estos como la multiplicación del valor del activo por la degradación causada por el riesgo para todos los activos afectados directa o indirectamente por el riesgo.

$Impacto_x = valor_x * degradación_x$

Una vez determinado el impacto del riesgo sobre cada activo se promedian estos y se determina el impacto del riesgo sobre el proyecto.

La próxima tarea que debe llevar a cabo el Equipo de Gestión de Riesgos es estimar la probabilidad de ocurrencia del riesgo, para lo cual se utiliza una escala de valores simbólicos. La probabilidad de ocurrencia del riesgo se multiplica por el impacto del mismo obteniendo de esta forma la exposición al riesgo del proyecto con el fin de priorizarlo tomando como referencia este valor.

A continuación se desarrolla un ejemplo de la adaptación de esta técnica para esta guía metodológica.

Se cuenta con el activo A, el activo B y el activo C, los cuales tienen su valor en la escala de valores ($V_1 - V_{10}$):

Activo A= V3

Activo B = V9

Activo C= V5

A continuación se determina la dependencia entre activos, en este caso A depende de B.

Se supone un riesgo X, el cual afecta directamente al activo B, en este caso se determina la degradación que causaría X a este activo en caso de materializarse. Se estima el porcentaje de degradación del activo, en este caso la degradación de B es del 90 % en caso de materializarse el riesgo X.

El impacto de X sobre los activos en caso de materializarse es el siguiente:

Impacto sobre B = 9 (valor de B) * 0.9 (degradación del activo) = 8.1

En la escala el impacto tendría un valor $V_8$.

También se calcula el impacto sobre los activos que dependen de B:

Como A depende de B entonces X tendría indirectamente un impacto sobre A, esto se calcula de igual forma, el valor de A es $V_3$, el valor de B no es importante, X degrada a B un 90 %, entonces el impacto de X sobre A sería:

Impacto sobre A = 3 (valor de A)*0.9 (degradación causada) = 2.7

En la escala el impacto sobre A tendría un valor $V_3$.

Seguido a esto se promedian los impactos del riesgo en cada uno de los activos para determinar el impacto sobre el proyecto, una vez determinado este se estima la probabilidad de ocurrencia del riesgo y se le da un valor en la escala ($P_1 - P_9$)

El riesgo X tiene una probabilidad $P_7$, con esta probabilidad y el impacto del riesgo en el proyecto se calcula la Exposición al Riesgo, valor por el cual se priorizará el mismo en el Registro de Riesgos.

Impacto sobre el proyecto = 8 + 3 / 2 = 5.5

ER = 5.5 * 7 = 38.5

Una vez realizado esto para cada uno de los riesgos, entonces se priorizan los riesgos por la exposición al riesgo del proyecto.

### 3.7.3 Análisis Algorítmico (Modelo Cuantitativo)

Este modelo se aplica para el análisis cuantitativo de los riesgos, al igual que el modelo cualitativo es orientado a los activos. La diferencia fundamental de este modelo respecto al cualitativo es que se trabaja con valores reales.

Como primera actividad se determina el valor de los activos, el valor de estos activos es un valor real superior a cero.

Luego se determina la dependencia entre estos, a diferencia del modelo cualitativo, en este caso se determina además el grado en que un activo depende del otro. El grado de dependencia de un activo respecto a otro se modela como un número continuo entre 0.0 (activos independientes) y 1.0 (activos totalmente dependientes, lo que ocurre sobre el inferior repercute totalmente sobre el superior).

Al igual que en el modelo cualitativo la dependencia puede ser transitiva y se pueden dibujar figuras de diamantes.

El grado de dependencia de un activo que dependa indirectamente de otro se calcula de la siguiente forma:

grado(A=>C) = $\Sigma_i$ (grado(A=>B) * grado($B_i$ ->C))

Las sumas se realizan de la siguiente forma:

A+b= 1- (1 - a) * (1 - b)

Satisfaciendo de esta forma las propiedades conmutativa y asociativa, además de que se acota el resultado al rango [0;1] si los sumandos están en este rango.

En el siguiente ejemplo se refleja cómo se determina el grado de dependencia entre dos activos:

El activo A depende en un 50 % de B y en un 50 % de C, B a su vez depende en un 50 % de C (figura 10), el grado en que A depende de C se calcula de la siguiente forma:

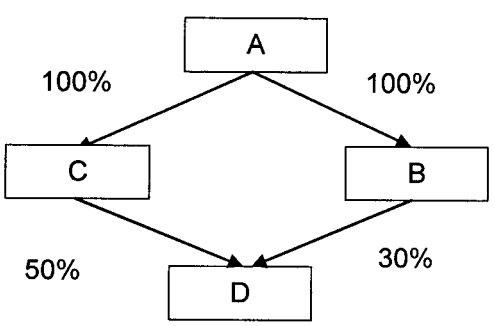


**Figura 10: Grado de dependencia entre activos en el modelo cuantitativo del análisis algorítmico (19)**

grado(A=>C) = $\Sigma_i$ (grado(A=>B) * grado($B_i$ ->C))

Grado(A=>B)=1

Grado (B=>D) = 0.3

Grado en que A depende de D por B= 1*0.3 = 0.3 (a)

Grado(A=>C)=1

Grado (C=>D) = 0.5

Grado en que A depende de D por B= 1*0.5 = 0.5 (b)

Efectuando la suma:

a+b = 1-(1-a)*(1-b)

= 1-(1-0.3)*(1-0.5)

= 1-(0.7)*(0.5)=1 - 0.35 = 0.65 = 65%

La próxima tarea es analizar la degradación del valor del activo en caso de materializarse el riesgo a través de técnicas de expertos o por medio de registros históricos con los que se cuente. Esta degradación es un valor real entre 0.0 (0 %) y 1.0 (degradación 100 %).

Una vez determinada la degradación del valor de los activos se da paso al cálculo del impacto del riesgo en cada uno de los activos, esto se realiza a través de la multiplicación del valor del activo por su degradación. En el caso de los activos que no son afectados directamente por el riesgo, pero que dependen de algún activo afectado entonces se calcula el impacto a través de la multiplicación de su valor por el grado de dependencia por la degradación del activo del cual dependen (valor * grado de dependencia * degradación del activo del cual depende).

Una vez obtenido el impacto del riesgo para cada uno de los activos estos se suman, debido a que se está trabajando con valores reales, para determinar el impacto del riesgo sobre el proyecto.

Luego, haciendo uso de alguna técnica para la estimación de probabilidades se determina la probabilidad de ocurrencia del riesgo. Una vez obtenido este dato se calcula la Exposición al Riesgo (ER) del proyecto multiplicando la probabilidad de ocurrencia por el impacto, y con este valor se prioriza en el Registro de Riesgos.

Este procedimiento se realiza para cada uno de los riesgos que se analizan en el proyecto.

Debido a la similitud de este modelo con el cualitativo no se desarrolla un ejemplo.

### 3.7.4 Entrevistas y Reuniones

Plantea la evaluación de la probabilidad e impacto de los riesgos a través de reuniones y entrevistas con participantes seleccionados por su familiaridad con las categorías de riesgo que se debatirán. Entre estos participantes se incluyen miembros del equipo del proyecto y expertos ajenos a este. La participación de expertos es necesaria, pues es posible que exista poca información sobre los riesgos en proyectos anteriores. La discusión debe ser dirigida por un facilitador experimentado.

En esta reunión, donde se evalúa el nivel de probabilidad del riesgo y su impacto sobre cada objetivo se registran todos los detalles explicativos.

La probabilidad del riesgo se puede determinar a través de una escala que pueda ir desde muy improbable hasta casi certeza, o probabilidades numéricas desde 0.1 hasta 0.9.

| | **Impacto** | | | | |
|---|---|---|---|---|---|
| **Objetivos del proyecto** | Muy bajo | Bajo | Moderado | Alto | Muy alto |
| Coste | Aumento de coste insignificante | Aumento del coste < 10 % | Aumento del coste 10 -20 % | Aumento del coste 20 – 40 % | Aumento del coste > 40 % |
| Tiempo | Aumento de tiempo insignificante | Aumento de tiempo < 5 % | Aumento de tiempo 5 -10 % | Aumento de tiempo 10 - 20 % | Aumento de tiempo > 20 % |

**Tabla 5: Ejemplo de definiciones del impacto de los riesgos para cuatro objetivos del proyecto. Fuente: Guía de los Fundamentos de la Dirección de Proyectos Tercera Edición (Guía del PMBOK) (2)**

El impacto es específico de cada proyecto, y del objetivo que puede verse impactado, para el impacto se determinan escalas relativas con descriptores ordenados por rango, muy bajo, bajo moderado, alto y muy alto; también pueden ser escalas numéricas lineales o no lineales. El impacto se determina anteriormente para cada objetivo del proyecto, se puede realizar mediante una tabla, para que una vez determinado el efecto del riesgo sobre estos objetivos se pueda determinar el impacto (tabla 5). Una vez determinado el posible efecto del riesgo este se ubica en la tabla y se determina el impacto.

Una vez determinada la probabilidad y el impacto del riesgo se puede determinar a través del uso de tablas o matrices de probabilidad e impacto la exposición al riesgo del proyecto para luego priorizarlos (2).

### 3.7.5 Método Delphi

El método Delphi de valoración de expertos puede ser utilizado tanto para la estimación de la probabilidad del riesgo como el impacto.

Para llevar a cabo el método Delphi es necesario realizar un grupo de tareas previas las cuales son listadas a continuación:

- Delimitar el contexto y el horizonte temporal en el que se desea realizar la previsión sobre el tema de estudio.
- Seleccionar el panel de expertos y conseguir un compromiso de colaboración. Las personas escogidas deben tener vastos conocimientos del tema que se abordará y deben evitar la aparición de sesgos en la información disponible en el panel.
- Explicar a los expertos en qué consiste el método, de esta forma los participantes conocen en todo momento cuál es el objetivo de cada uno de los procesos que se realizan.

Se siguen los siguientes pasos:

Paso 1: Formulación del problema: es un punto muy importante, pues es imprescindible definir con precisión el campo de investigación, es importante asegurar que los expertos deben entender el problema de la misma forma.

Paso 2: en este paso se seleccionan las características que deben cumplir el grupo de expertos. Para esto se deben determinar parámetros medibles de acuerdo al tema que se vaya a analizar.

Paso 3: en este paso se calcula la cantidad de expertos o tamaño de la muestra. Para esto se determinan los siguientes parámetros:

- Proporción de error deseado al realizar la inferencia de los n expertos (p).
- Nivel de precisión (i)
- Nivel de confianza (k)

Luego se calcula el tamaño de la muestra a través de la siguiente fórmula:

$N= p(1-p)k / i^2$

Paso 4: reunión de preparación y explicación a los expertos.

Paso 5: Se definen las características según el criterio de expertos.

Paso 6: se establece el nivel de importancia mediante el método. En este paso se dan puntuaciones según la prioridad, en una escala fijada, ejemplo: 1(característica establecida más importante) a n (la menos importante, igual a la cantidad de características). Con estos datos se conforma una matriz con las características establecidas por los expertos en las filas y el criterio de los expertos por las columnas.

Paso 7: Análisis de la concordancia en la valoración de los criterios de los expertos.

Se debe probar el nivel de acuerdo entre los expertos, es necesario comprobar el grado de coincidencia de las valoraciones realizadas. Se puede utilizar para esto el Coeficiente de Concordancia de Kendall (W). Para esto se construye una tabla de aspectos a evaluar contra expertos, donde se asientan los rangos de valoración asignados a cada aspecto evaluado contra cada uno de los expertos, siempre tomando los datos a partir de la tabla que se usó en el método Delphi.

Paso 8: en este paso se seleccionan las características establecidas por los expertos.

### 3.7.6 Matriz de probabilidad e impacto

Esta es una técnica para priorizar los riesgos en dependencia de la exposición al riesgo, en esta se ubican las probabilidades y el impacto, el interior de la matriz se llena con la exposición al riesgo (resultado de multiplicar la probabilidad por el impacto), en dependencia de la zona de la matriz donde se encuentren los riesgos se determina la prioridad de estos para ser tratados.

El equipo de proyecto debe determinar los umbrales para riesgos altos, moderados o bajos, para delimitarlos en la matriz. Luego se ubica cada riesgo dentro de la matriz, En la tabla 6 se muestra una matriz de probabilidad e impacto con los se muestra una matriz de probabilidad e impacto, los colores determinan las prioridades que deben tener los riesgos en dependencia de la Exposición al Riesgo del Proyecto. En este caso la prioridad del riesgo es baja hasta una exposición de 0.05, desde 0.06 hasta 0.14 es media y desde 0.18 en adelante es alta (2).

Se puede clasificar cada riesgo por separado para cada objetivo (coste, tiempo, alcance, etc), además se pueden desarrollar formas de determinar una clasificación general para cada riesgo.

| Probabilidad | Impacto | | | | |
|---|---|---|---|---|---|
| 0.90 | **0.05** | **0.09** | | | |
| 0.70 | **0.04** | **0.07** | **0.14** | | |
| 0.50 | **0.03** | **0.05** | **0.10** | | |
| 0.30 | **0.02** | **0.03** | **0.06** | **0.12** | |
| 0.10 | **0.01** | **0.01** | **0.02** | **0.04** | **0.08** |
| | 0.05 | 0.10 | 0.20 | 0.40 | 0.80 |

**Tabla 6: Matriz de Probabilidad e Impacto. Fuente: Guía de los Fundamentos de la Dirección de Proyectos Tercera Edición (Guía del PMBOK®) (2)**

Para la estimación de la probabilidad de ocurrencia de los riesgos también se pueden utilizar las técnicas definitorias y comparativas expuestas en el capítulo 2 de esta investigación.

### 3.7.7 Árbol de Decisiones

Esta es una técnica para la toma de decisiones, sin embargo se puede utilizar para la determinación impacto del riesgo. El método del árbol de decisión considera dos parámetros, estos son costo y consecuencias.

El primer paso para construir el árbol de decisión es la identificación de las opciones que se presentan ante el problema analizado. Estas elecciones forman las ramas del árbol, cada una de estas decisiones llevan a diferentes resultados. Se incluye en el árbol el costo de cada decisión o situación que se analice y su probabilidad, además se refleja en el árbol la incertidumbre, pues al no conocer un resultado exacto para el problema que se analiza se deben reflejar todas las opciones. El resultado de este árbol son las consecuencias, determinadas por cada uno de los caminos posibles del mismo.

Para determinar los resultados se recorre cada camino del árbol y se acumulan los costos y las consecuencias asociados a cada uno, luego se recorre desde las ramas a la raíz y se calcula el valor esperado de cada elección o situación que se presenta, siguiendo las consecuencias más probables en las ramas. Cuando se está tomando decisiones la rama con el mayor valor esperado es la opción de decisión recomendada.

A continuación se ejemplifica el uso del árbol para la toma de decisiones (1).

La figura 11 representa un árbol de decisión para un sistema X basado en software, en este caso se puede (1) construir el sistema desde el principio, (2) reutilizar los componentes existentes, (3) comprar un producto disponible y modificarlo, (4) contratar el desarrollo del software.

Si se va a construir el sistema desde el principio la probabilidad de que el trabajo sea difícil es del 70 % %, un esfuerzo de desarrollo difícil costará $450 000, un esfuerzo de desarrollo simple se estima que cueste $ 380 000. El valor esperado de construcción, calculado a lo largo de la rama del árbol es:

Coste esperado= $\sum$(probabilidad del camino)$_i$ * (coste estimado del camino)$_i$, donde i es el camino del árbol de decisión.

Entonces:

Coste esperado $_{construcción}$ = 0.30 (380 000) + 0.70 (450 000) = 429 000

Coste esperado $_{compra}$ = 0.70 (275 000) + 0.30 (400 000) = 267 000

Coste esperado $_{contrato}$ = 0.60 (350 000) + 0.40 (500 000) = 410 000

Según la probabilidad y los costes proyectados en la figura 11 el coste más bajo esperado es la opción de compra.

Se deben considerar para este análisis no solo el coste, todos los criterios posibles a evaluar deben estar presentes en este árbol para hacer más reales sus resultados. En este caso pudieran estar presentes factores como la experiencia del desarrollador, la conformidad con los requisitos, etc.

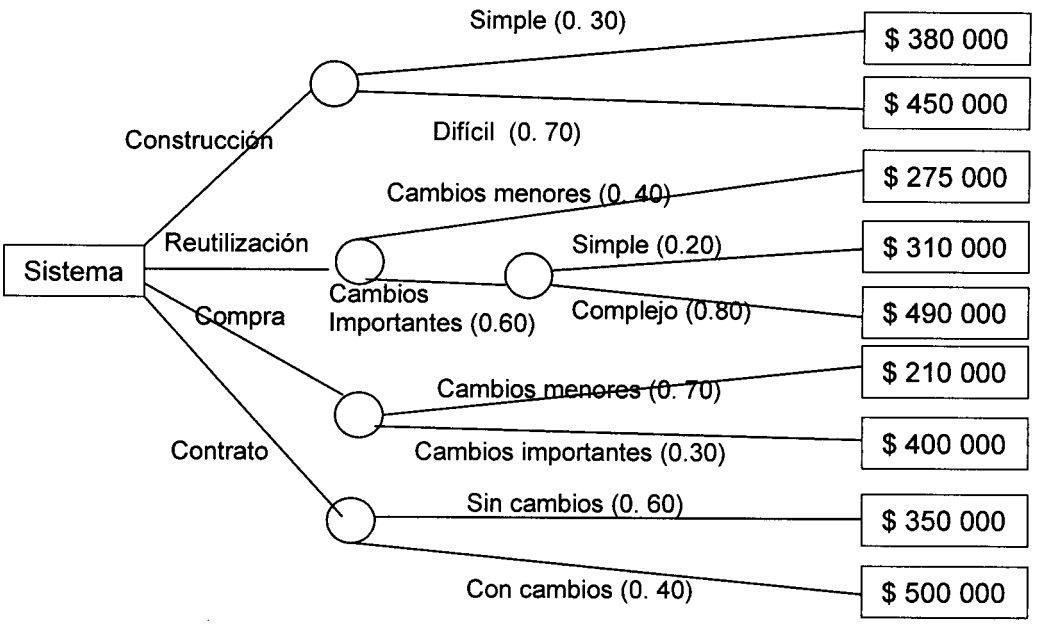


**Figura 11: Árbol de decisiones. Fuente: Ingeniería del Software. Un enfoque práctico (1).**

### 3.8 Conclusiones Parciales

Es aconsejable tanto para la estimación de la probabilidad del riesgo como el impacto del mismo disponer de las personas que más familiarizada esté con el sistema. Es importante también el uso de técnicas de consenso en grupo, en este caso el método Delphi, para la estimación de los riesgos, sobre todo la probabilidad de los mismos, que tiende a ser más subjetiva, con este método se puede hacer converger las diferentes opiniones acerca de la estimación que se esté realizando.

Son muy útiles las técnicas comparativas y definitorias en caso de la estimación de la probabilidad de ocurrencia de los riesgos, pues brindan una forma sencilla de estimarla.

Siguiendo las actividades planteadas en esta guía metodológica y con el uso de las técnicas propuestas se puede lograr un correcto análisis de riesgos, las técnicas propuestas en este capítulo son adaptadas a las necesidades del análisis de riesgos que se plantea, independientemente de su descripción dependen en gran medida del proyecto que realice el análisis los resultados que se obtengan. Es importante a la hora de la toma de decisiones y la estimación de parámetros del análisis eliminar todo el sesgo que pueda existir para lograr resultados más fiables.

Este proceso de Análisis de Riesgos debe realizarse siempre que surjan nuevos riesgos o se desee tomar una decisión. Los resultados del mismo serán tan fiables como el Equipo de Gestión de Riesgos sea capaz de hacerlo.

Para lograr la efectividad del Análisis de Riesgos independientemente del tipo de análisis que se realice es necesario que el Equipo de Gestión de Riesgos conozca y aplique una serie de principios y prácticas que les ayudarán a alcanzar sus objetivos, a continuación se exponen estos principios.

- **Adaptación:** La utilización de un proceso conocido por el equipo, estructurado y repetible es de suma importancia para lograr correctamente los objetivos de la Gestión de Riesgos, para logarlo es necesario adaptar los métodos de análisis a la infraestructura y necesidades del proyecto.
- **Análisis Continuo:** el análisis continuo de los riesgos se hace necesario debido a los cambios que frecuentemente se producen en el mismo. El equipo de Gestión de Riesgos debe analizar ininterrumpidamente proactivamente los riesgos durante todas las fases del ciclo de vida del proyecto. Para lograr el análisis continuo de los riesgos es necesario hacer de este una parte vital de la Gestión de Riesgos a través de la vigilancia continua y la identificación rutinaria de riesgos a lo largo de todas las fases del proyecto.
- **Comunicación Abierta:** Se debe mantener una comunicación abierta entre los miembros del Equipo de Gestión de Riesgos en todos los sentidos con el objetivo de contar con toda la información posible para realizar el análisis de los mismos para esto es necesario que cada miembro del equipo sea capaz de expresar sus opiniones con libertas. Esto requiere del flujo libre de información entre todos los niveles, habilitar la comunicación formal, informal e improvisada, utilizar procesos de conceso que evalúen los criterios individuales, los cuales pueden brindar conocimiento único y dar una visión para el análisis de riesgos.
- **Visión Común:** Todos los miembros del equipo deben comprender el riesgo de la misma forma, antes de realizar el análisis es necesario que cada cual conozca el riesgo, sus causas y la relación de este con los problemas que pueden surgir de igual manera.
- **Aprendizaje Constante:** Es importante aprender de los resultados de otros proyectos, el análisis de los resultados de proyectos anteriores fomenta el aprendizaje dentro del equipo mediante el intercambio de opiniones entre sus miembros.

- **Participación Activa:** La participación activa en el Análisis de Riesgos es responsabilidad de todos los integrantes del equipo. Los miembros del equipo deben tener asignadas tareas específicas para analizar los riesgos y cada uno de ellos se responsabiliza de llevarlas a cabo.
- **Trabajo en Equipo:** El trabajo en equipo es fundamental, una sola persona no es capaz de llevar a cabo el análisis de cada uno de los riesgos, es necesario trabajar en forma cooperativa para lograr un acuerdo común y unir y aprovechar el talento, las habilidades y el conocimiento de cada miembro del equipo.

## CONCLUSIONES

En el transcurso de esta investigación a través de las encuestas analizadas y la observación realizada a los proyectos productivos de la universidad se pudo determinar que:

- No se le da la importancia necesaria a la Gestión y el Análisis de los Riesgos en los proyectos productivos de la Universidad de las Ciencias informáticas, en la mayoría de los casos estos procesos se desarrollan sin la calidad requerida, también contribuye a esto la falta de una guía para analizarlos formalmente.
- La falta de personal capacitado y la poca madurez en el Análisis de Riesgos hace que este no se desarrolle con la calidad requerida, exponiendo a los proyectos de software al impacto de riesgos que pudieron ser minimizados o evitados.

En esta investigación se llevó a cabo el análisis de diferentes modelos de Gestión de Riesgos reconocidos mundialmente y se valoró el análisis de estos en los proyectos productivos de la Universidad de las Ciencias Informáticas, a partir de lo cual se obtuvo la caracterización de los métodos y modelos utilizados para la realización de la Gestión de Riesgos.

Como resultado general de esta investigación y dando cumplimiento al objetivo principal de la misma se obtuvo una Guía Metodológica para el Análisis de los Riesgos con la descripción de las técnicas a utilizar para realizar las diversas actividades planteadas. Se obtuvieron además un grupo de valoraciones y principios para la realización de este análisis en los proyectos de software.

La solución propuesta en esta investigación, a pesar de haber surgido a raíz del análisis de diversos modelos de Gestión de Riesgos, no es una copia de ninguno de estos, sino que toma de cada uno los elementos más importantes y necesarios y los agrupa llevándolos al contexto de la Gestión de Riesgos de la UCI. Entre las ventajas que brinda la guía metodológica es necesario destacar que posibilita fomentar el control de los recursos del proyecto, pues permite el análisis orientado a los activos.

Con su aplicación en los proyectos de software de la universidad se mejorará el Análisis de Riesgos en los mismos de forma notable, se facilitará su realización a los EGR y la comprensión por estos de esta fase. El proceso de Gestión de Riesgos se verá beneficiado al contar con datos más fiables para el tratamiento de los riesgos, y como consecuencia mejorará la calidad del proceso de desarrollo de software en la UCI.

## RECOMENDACIONES

Después de valorar el Análisis de Riesgos en la UCI, los problemas que enfrenta y analizar modelos de Gestión de Riesgos aplicados en el mundo se hace necesario hacer un grupo de recomendaciones para mejorar el Análisis de Riesgos en la institución:

- Incluir en el expediente del proyecto cómo llevar a cabo el Análisis de Riesgos haciendo uso de la metodología propuesta en este trabajo y las técnicas descritas.
- Auditar la realización del Análisis de Riesgos en la Universidad de las Ciencias Informáticas, velando por el cumplimiento del mismo y los resultados de la aplicación de la guía propuesta.
- Brindar una capacitación más profunda a los Gestores y Equipos de Gestión de Riesgos de la universidad con el fin de ganar en la preparación de los mismos y concientizarlos acerca de la importancia del Análisis de Riesgos para la calidad del producto y la salud del proyecto.
- Continuar profundizando en técnicas como el Análisis de Sensibilidad y Modelado y Simulación por su importancia en el Análisis de Riesgos.

## REFERENCIAS BIBLIOGRÁFICAS


1. PRESSMAN, R. S. *Ingeniería del Software. Un enfoque práctico.* Quinta ed. 2001. vol. 1,

2. INSTITUTE, P. M. *Guía de los Fundamentos de la Dirección de Proyectos Tercera Edición (Guía del PMBOK).* 2004,

3. YELENY ZULUETA VÉLIZ, E. D. H. *Modelo de Gestión de Riesgos en Proyectos de Desarrollo de Software.* Universidad de las Ciencias Informáticas, 2007,

4. THOMPSON, J. M. *Concepto de Proyecto* Disponible en: http://www.promonegocios.net/proyecto/concepto-proyecto.html

5. ACKOFF, R. *Proyecto* Disponible en: http://www.cyta.com.ar/biblioteca/bddoc/bdlibros/proyectoinformatico/libro/c1/c1.htm.

6. FIORITO, F. *La Simulación como herramienta para el manejo de la incertidumbre.* 2006,

7. FRIGO, P. E. Disponible en: http://www.eird.org/fulltext/riesgolandia/booklet-spa/.

8. GARCÍA, N. A. *Mejora y ampliación de la aplicación de gestión de riesgos bajo el framework jrisk para empresa dedicada a realizar proyectos de software.* ESCUELA UNIVERSITARIA DE INGENIERÍA TÉCNICA EN INFORMÁTICA DE OVIEDO,

9. PÚBLICAS, M. D. A. *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Método.* Madrid: 2006.

10. CÉSPEDES, Y. F. *Análisis y Gestión de Riesgo para el desarrollo de las aplicaciones del proyecto Atención Primaria de Salud (APS).* Universidad de las Ciencias Informáticas, 2007.

11. *Gestión de Riesgos.*

12. YELENY ZULUETA VELIZ, A. H. G. *Retos en la Gestión de los Riesgos en Proyectos de Software.* Universidad de las Ciencias Informáticas, 2008,

13. EUROMÉTODO, P. *Consejo Superior de Informática. Eurométodo V1.* Madrid: 1997

14. J.ESTEVES, J. A. P., N. RODRÍGUEZ, R. ROY. *Implementación y Mejora del Método de Gestión de Riesgos del SEI en un proyecto universitario de desarrollo de software.* 2001, Disponible en: http://www.ewh.ieee.org/reg/9/etrans/vol3issue1March2005/3TLA1_13Esteves.pdf.

15. RONALD P. HIGUERA, Y. Y. H. *Software Risk Management.* SEI. 1996

16. YAILIÉN HERNÁNDEZ ALBA, L. D. F. *Guía para la Gestión de Riesgos a través de RUP.* Facultad 9. Universidad de las Ciencias Informáticas, 2008.

17. ARIADNA MATOS BORGES, Y. S. G. *Guía de Métricas para la Gestión de Riesgos en Proyectos de Desarrollo de Software de la UCI.* Facultad 9. Universidad de las Ciencias Informáticas, 2008.

18. MARTÍNEZ, R. D. *Expediente de Proyecto en la UCI.*

19. PÚBLICAS, M. D. A. *Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Guía de Técnicas.* Madrid: 2005.

20. H LINSTONE, M. T. *The Delphi Method. Techniques and Applications.* 1975.

21. ASTIGARRAGA, E. *El Método Dephi.*

22. DR DAVID HILLSON, D. D. T. H. Calculando probabilidades de riesgos: Métodos alternativos. En 2004,

## BIBLIOGRAFÍA


- Bohem, BW. (1991).Software risk management: Principles and Practices.
- Moores, T. C, R, E. (1996). A METHODOLOGY FOR MEASURING THE RISK ASSOCIATED WITH A SOFTWARE REQUIREMENTS SPECIFICATION, VOL 4, $N_O$. 1
- Maniasi S. (2005) Un Modelo para la Identificacion de Riesgos en Base a Taxonomías
- Higuera R, P. (1994) An introduction to Team Risk Management (Version 1.0)
- Hillson D. (2005) Decisiones, Decisiones
- Stoneburner G. G, A. F, A. (2002) Risk Management Guide for Information Technology Systems. Recommendations of the National Institute of Standards and Technology.
- Jones, C. (1998).Minimizing the risk of software development. Cutter IT Journal.

**Anexo 1: Lista de Riesgos del Expediente del Proyecto en la UCI**

# Lista de riesgos

Interno

## <Nombre del Proyecto>

<Nombre del producto>

**<Versión >**

**Control de versiones**

| Fecha | Versión | Descripción | Autor |
|---|---|---|---|
| <dd/mmm/yy> | <x.x> | <detalles> | <nombre> |

**Reglas de Confidencialidad**
**Clasificación:** <<Clasificación>>

Este documento contiene información propietaria de ALBET Ingeniería y Sistemas y/o "<<Empresa Cliente>>" , y es emitido confidencialmente para un propósito específico.

El que recibe el documento asume la custodia y control, comprometiéndose a no reproducir, divulgar, difundir o de cualquier manera hacer de conocimientos público su contenido, excepto para cumplir el propósito para el cual se ha generado.

## 1. Introducción

### 1.1 Propósito

*[Definir términos Generales establecidos pro la Dirección de Calidad y Normas de la UCI para los proyectos Productivos]*

### 1.2 Alcance

*[Todos los proyectos de la UCI]*

### 1.3 Referencias

*[Lista de documentos a los que se hace referencia en el Plan]*

| Código | Título |
|---|---|
| [1] | Documento 1 |
| [2] | Documento 2 |
| [3] | Modelo de Diseño - Módulo de Administración v0.0 |

### 1.4 Glosario

*[En el glosario aparecen un grupo de términos básicos para los proyectos productivos de la UCI]*

## 2. Riesgos

| Riesgo | Tipo de Riesgo | Impacto | Descripción | Probabilidad | Efectos |
|---|---|---|---|---|---|
| | *[Los tipos de riesgos pueden ser:*<br>*Tecnológico*<br>*Personal*<br>*Organización*<br>*Herramientas*<br>*Requerimientos*<br>*Estimación]* | *[Lista de impactos en el proyecto o producto.]* | | *[La probabilidad puede ser:*<br>*Alta*<br>*Media*<br>*Baja*<br>*Muy alta*<br>*]* | *[Los efectos pueden ser:*<br>*Catastrófico*<br>*Serias*<br>*Tolerable*<br>*Insignificante*<br>*]* |

**2.1 <Identificador de riesgo—un nombre o número descriptivo>**

**2.1.1 Indicadores**

*[Describe como monitorear o detectar que el riesgo ha ocurrido o está próximo. Incluye cosas como métricas y umbrales, resultados de prueba, eventos específicos, y así sucesivamente.]*

**2.1.2 Estrategia de Mitigación**

*[Describe que se hace actualmente en el proyecto para reducir el impacto del riesgo.]*

**2.1.3 Plan de Contingencia**

*[Describe que curso seguirán las acciones si el riesgo se materializa: solución alternativa, reducción de su efecto, y así sucesivamente.]*

**2.2 <Identificador de riesgo—un nombre o número descriptivo >**

## 3. Gestión de Riesgos

- *Estimar la probabilidad de ocurrencia*
- *Estimar el impacto sobre el proyecto en una escala del 1 al 5, donde*
  - *1 = bajo impacto sobre el éxito del proyecto*
  - *5= impacto catastrófico sobre el éxito del proyecto*
- *ordenar la tabla por probabilidad e impacto*

| Riesgo | Probabilidad | Impacto | Mitigación del riesgo | Monitoreo del riesgo | Administrador del riesgo |
|---|---|---|---|---|---|
| | | | | | |

**Nota:**

***Mitigación***

- *¿Cómo se puede evitar el riesgo?*

***Monitoreo***

- *¿Qué factores podemos vigilar que nos permitan ser capaces de determinar si el riesgo es más o menos probable?*

***Administración***

- *¿Con qué planes de contingencia contamos si el riesgo se vuelve realidad?*

**Anexo 2: Plan de Mitigación de Riesgos del Expediente del Proyecto en la UCI**

# Plan de Mitigación de Riesgos

Interno

## <Nombre del Proyecto>

<Nombre del producto>

<Versión>

**Control de versiones**

| Fecha | Versión | Descripción | Autor |
|---|---|---|---|
| <dd/mmm/yy> | <x.x> | <detalles> | <nombre> |

**Reglas de Confidencialidad**

**Clasificación:** <<Clasificación>>

Este documento contiene información propietaria de ALBET Ingeniería y Sistemas y/o "<<Empresa Cliente>>" , y es emitido confidencialmente para un propósito específico.

El que recibe el documento asume la custodia y control, comprometiéndose a no reproducir, divulgar, difundir o de cualquier manera hacer de conocimientos público su contenido, excepto para cumplir el propósito para el cual se ha generado.

## 1 Introducción

### 1.1 Alcance

*[Proyectos con los que se involucra el Plan]*

### 1.2 Definiciones, acrónimos y abreviaturas

### 1.3 Referencias

*[Lista de documentos a los que se hace referencia en el Plan]*

| Código | Título |
|---|---|
| [1] | Documento 1 |
| [2] | Documento 2 |
| [3] | Modelo de Diseño - Módulo de Administración v0.0 |

**2. Riesgos**

| Riesgo | Tipo de Riesgo | Impacto | Descripción | Probabilidad | Efectos |
|---|---|---|---|---|---|
| | *[Los tipos de riesgos pueden ser:*<br>*Tecnológico*<br>*Personal*<br>*Organización*<br>*Herramientas*<br>*Requerimientos*<br>*Estimación]* | *[Lista de impactos en el proyecto o producto. ]* | | *[La probabilidad puede ser:*<br>*Alta*<br>*Media*<br>*Baja*<br>*Muy alta ]* | *[Los efectos pueden ser:*<br>*Catastrófico*<br>*Serias*<br>*Tolerable*<br>*Insignificante*<br>*]* |

**2.1 <Identificador de riesgo — un nombre o número descriptivo>**

**2.1.1 Indicadores**

*[Describe como monitorear o detectar que el riesgo ha ocurrido o está próximo. Incluye cosas como métricas y umbrales, resultados de prueba, eventos específicos, y así sucesivamente.]*

### 2.1.2 Estrategia de Mitigación

*[Describe que se hace actualmente en el proyecto para reducir el impacto del riesgo.]*

### 2.1.3 Plan de Contingencia

*[Describe que curso seguirán las acciones si el riesgo se materializa: solución alternativa, reducción de su efecto, y así sucesivamente.]*

**<Próximo Identificador de riesgo—un nombre o número descriptivo >**

## 3. Gestión de Riesgos

*[*

- *Estimar la probabilidad de ocurrencia*
- *Estimar el impacto sobre el proyecto en una escala del 1 al 5, donde*
  - *1 = bajo impacto sobre el éxito del proyecto*
  - *5= impacto catastrófico sobre el éxito del proyecto*
- *ordenar la tabla por probabilidad e impacto*

| Riesgo | Probabilidad | Impacto | Mitigación del riesgo | Monitoreo del riesgo | Administración del riesgo |
|---|---|---|---|---|---|
| | | | | | |

*]*

*Nota:*

- *Mitigación*
  *¿Cómo se puede evitar el riesgo?*
- *Monitoreo*
  *¿Qué factores podemos vigilar que nos permitan ser capaces de determinar si el riesgo es más o menos probable?*

- *Administración*
  *¿Con qué planes de contingencia contamos si el riesgo se vuelve realidad?*

**4. Tareas para la Gestión de Riesgos**

*[Breve descripción de las tareas de gestión durante el proyecto. Se debe describir lo siguiente:*

- *La estrategia a utilizar para identificar el riesgo y cómo serán analizados y priorizados.*
- *Estrategias para la mitigación, evasión, y/o prevención para los riesgos más importantes (máximo 10 riesgos)*
- *Como se van a dar seguimiento al estado de cada riesgo significativo y las actividades de mitigación*
- *Cronograma de revisión y reporte de los riesgos. LA revisión de los riesgos debe formar parte de cada revisión de iteración y de aceptación de fases*

**5. Organización y Responsabilidades**

*[Lista de los grupos o personas involucradas en la gestión de los riesgos y la descripción de sus responsabilidades.]*

**6. Presupuesto**

*[Presupuesto disponible para la Gestión de los Riesgos]*

**7. Herramientas y Técnicas**

*[Lista de las herramientas y/o técnicas que serán utilizadas para almacenar lo riesgos, evaluar el riesgo, seguir el riesgo, o generar reportes del control de los riesgos]*

**8. Elementos de Riesgos a Gestionar**

*[Lista de los elementos de riesgo más importantes. Una buena práctica en la industria es publicar y hacer visible los 10 riesgos más significativos.]*

**Anexo 3: Registro de Riesgos del Expediente del Proyecto de la UCI**

| Riesgo | Tipo de Riesgo | Impacto | Descripción | Probabilidad | Efectos |
|---|---|---|---|---|---|
| | *[Los tipos de riesgos pueden ser:*<br>*Tecnológico*<br>*Personal*<br>*Organización*<br>*Herramientas*<br>*Requerimientos*<br>*Estimación]* | *[Lista de impactos en el proyecto o producto.]* | | *[La probabilidad puede ser:*<br>*Alta*<br>*Media*<br>*Baja*<br>*Muy alta*<br>*]* | *[Los efectos pueden ser:*<br>*Catastrófico*<br>*Serias*<br>*Tolerable*<br>*Insignificante*<br>*]* |

**Anexo 4: Registro de Activos del Proyecto**

| Activo | Valor | Riesgos que lo afectan | Activos que dependen |
|---|---|---|---|
| | *[se especifica el valor determinado del activo]* | *[se especifican los riesgos que afectan al activo ]* | *[Activos que dependen directa o indirectamente (en caso de haberlo determinado se incluye el grado de dependencia) ]* |

## GLOSARIO DE TÉRMINOS

**Activo:** Elemento del sistema o estrechamente relacionado con este que aporta valor a la organización

**Calidad del software:** Cumplir sistemáticamente con los requerimientos, para satisfacer las necesidades y expectativas de los clientes o usuarios.

**CMMI:** Capability Maturity Model Integration. Es un modelo para la mejora de procesos que proporciona a las organizaciones los elementos esenciales para procesos eficaces.

**Estándares:** Normas de desempeño definidas para una actividad, un proceso, un producto o un servicio.

**Fase:** Período de tiempo entre dos hitos principales de un proceso de desarrollo.

**Incertidumbre:** expresión del grado de desconocimiento de una condición futura, puede derivarse de la falta de información o incluso porque exista desacuerdo sobre lo que se sabe o lo que podría saberse.

**Ingeniería del Software:** designa el conjunto de técnicas designadas a la producción de un programa de computadora, más allá de la sola actividad de programación.

**Metodología:** Se refiere a los métodos de investigación que se siguen para alcanzar una gama de objetivos en una ciencia.

**PMBOK®:** Project Management Body of Knowledge, es un estándar en la Gestión de Proyectos desarrollado por el Project Management Institute. Es una colección de procesos y áreas de conocimientos generalmente aceptadas como las mejores prácticas dentro de la Gestión de Proyectos.

**PMI:** Project Management Institute, es considerado la asociación profesional para la Gestión de Proyectos sin fines de lucro más grande del mundo. Entre sus principales objetivos se encuentran

formular estándares profesionales, generar conocimiento a través de la investigación, y promover la Gestión de Proyectos como profesión a través de sus programas de certificación.

**Proceso de Software:** Conjunto de pasos ordenados y relacionados entre sí a través de los cuales se convierten los insumos en productos o resultados. Marco de trabajo de las tareas que se requieren para construir software de alta calidad. Proporciona una interacción entre los usuarios y los diseñadores, entre los usuarios y las herramientas de desarrollo, y entre los diseñadores y las herramientas de desarrollo.

**Producto:** Software de computadora que diseñan y construyen los ingenieros del software. Esto abarca programas que se ejecutan dentro de una computadora de cualquier tamaño y arquitectura, documentos que comprenden formularios virtuales e impresos y datos que combinan números y texto y también incluyen presentaciones de audio y vídeo e imágenes.

**SEI:** instituto federal estadounidense de investigación y desarrollo, fundado por el Congreso de los Estados Unidos en 1984 para desarrollar modelos de evaluación y mejora en el desarrollo de software. Es un referente en Ingeniería de Software.

**Sesgo:** un error que aparece en los resultados de un estudio debido a factores que dependen de la recogida, análisis, interpretación, publicación o revisión de los datos que pueden conducir a conclusiones que son sistemáticamente diferentes de la verdad o incorrectas acerca de los objetivos de una investigación.

**Simulación:** es el proceso de diseñar un modelo de un sistema real y llevar a término experiencias con él, con la finalidad de comprender el comportamiento del sistema o evaluar nuevas estrategias (dentro de los límites impuestos por un cierto criterio o un conjunto de ellos) para el funcionamiento del sistema.

**Software:** Conjunto de programas, instrucciones y reglas informáticas para ejecutar ciertas tareas en una computadora. Es un transformador de información, produciendo, gestionando, modificando, adquiriendo, mostrando o transmitiendo información que puede ser tan simple como un bit, o tan complejo como una presentación de multimedia. Como vehículo utilizado para desarrollar el producto, el software actúa como la base del control de la computadora (sistemas operativos), la comunicación de información (redes), y la creación y control de otros programas (herramientas de software y entornos).

**SW – CMM:** Capability Maturity Model for Software. Es un modelo de procesos para el desarrollo y mantenimiento de sistemas de software, diseñado sobre los criterios:

- La calidad de un producto o sistema es consecuencia directa de los procesos empleados en su desarrollo.
- Las organizaciones que desarrollan software presentan un atributo denominado madurez, cuya medida es proporcional a los niveles de capacidad e institucionalización de los procesos que emplean en su trabajo.

**Técnica:** procedimiento o grupo de procedimientos que tienen el fin de obtener un resultado específico sin importar el campo en donde se esté desenvolviendo

**UML:** Unified Modeling Language (Lenguaje Unificado de Modelado): lenguaje creado en el año 1960 con el objetivo de crear un lenguaje de programación universal que pudiera ser usado en cualquier ordenador.