

Universidad de las Ciencias Informáticas

Facultad 3



Propuesta de modelo para la
Gestión de Riesgos en los
proyectos de producción de software.

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

Autor: Eduardo García Hernández.

Tutor: Dr.C Pedro Y. Piñero Pérez.

Ciudad de la Habana, Junio 2008.

DECLARACIÓN DE AUTORÍA

Declaramos ser autores de la presente tesis y reconocemos a la Universidad de las Ciencias Informáticas los derechos patrimoniales de la misma, con carácter exclusivo.

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

Eduardo García Hernández

DrC. Pedro Y. Piñero Pérez

Firma del Autor

Firma del Tutor

Dedicatoria

*A mi familia,
por sus siempre sabias palabras,
por indicar el camino correcto,
por sus rezos y sus desvelos,
por su ejemplo, por su sacrificio,
por su confianza y su amor, por todo.*

Agradecimientos

*Agradezco a todos los que han contribuido en mi formación
y en la realización de este trabajo, especialmente:*

A Mamá y Papá, por todo lo que se puede agradecer en una vida, por su corazón.

A Papi y Mami, por su amor, sus consejos, su guía, su apoyo, por estar ahí.

A Linet, por todo su cariño y tenerme siempre presente.

Abuela y Tía, por su preocupación siempre.

A tío, por ser más que tío.

A Isa, Abuela y Eliet, por todos los momentos.

A Eduardo, por su cariño con todos.

*A Lidy, por tantas cosas... por todo el tiempo bueno y malo compartido,
su comprensión y amor.*

A toda mi familia vecina.

*A todos los sherpas, por la grandeza de estar juntos siempre,
a los que están cerca y los que no.*

A mi tutor, Pedro, por su ayuda en este trabajo, las valiosas ideas y el tiempo dedicado.

A Jesie y Henry, por los comentarios sobre este trabajo.

A mis compañeros de aula, por su apoyo, y a mis profesores.

Al viejo.

A mis amigos, A Abbie.

A la Revolución y la Universidad, por darnos a todos una oportunidad.

Resumen

En este trabajo se propone un modelo de Gestión de Riesgos con alcance en el desarrollo de proyectos de producción de software. Para ello se realizó un estudio del estado del arte de diferentes modelos para la Gestión de Riesgos analizándose las ventajas y desventajas de cada uno de ellos. El que se propone mejora las deficiencias de los modelos anteriores y constituye un modelo ajustado para la Gestión de Riesgos en proyectos de software desarrollados en entornos similares al de la Universidad de las Ciencias Informáticas. Se define en el mismo una nueva e intuitiva representación de los riesgos y de los procesos necesarios para su gestión. Se adaptan técnicas y métodos a las condiciones de la universidad y se proponen algunas nuevas, junto con actividades y métricas explicadas todas en función de brindar guía objetiva y práctica en su utilización. Se definen los roles y artefactos que se generan en cada proceso y su uso como entrada o salida. Se propone un mecanismo de evaluación y aprendizaje del proceso general que ayuda a mantener un enfoque en la mejora continua y se definen puntos de extensibilidad para futuros trabajos sobre el modelo.

Palabras Claves: Modelo de Gestión de Riesgos, Gestión de Riesgos, Riesgo, Gestión de Proyectos.

Abstract

This work proposes a risk management model with scope in software development projects. For this, a study of the state of the art was made analyzing advantages and disadvantages of different risk management models. The proposed model improves the deficiencies in previous models and constitutes an adjusted model for risk management in development software projects in environment like those in the Universidad de las Ciencias Informáticas. The model defines a new and intuitive representation of the risks itself and the processes involved in risk management. It adapts techniques and methods to local conditions and proposes new activities, techniques and metrics, all of them explained with the intention to offer an objective and practical guide in its utilization. The model defines the roles and artifacts generated in each process of the risk management and its use as an input or output. It proposes a mechanism to evaluate and learn from the risk management process that helps to maintain focus on continuous improvement. The model defines extensibility points that will help in its extension with further work.

Keywords: Risk Management Model, Risk Management, Risk, Project Management.

Índice de Contenidos

Índice de Tablas	VIII
Índice de Figuras	VIII
Introducción	1
La naturaleza incierta de los riesgos	2
Los riesgos en el mundo de los negocios	2
Los riesgos en el mundo del software	2
La Gestión de Riesgos	3
Caracterización de la Gestión de Riesgos en la Universidad de las Ciencias Informáticas	5
Problema Científico	6
Objeto de estudio	6
Campo de acción	6
Hipótesis	6
Objetivos	6
Objetivo general	6
Objetivos específicos	6
Posibles resultados	7
Métodos y técnicas a utilizar	7
Estructura del trabajo	7
Capítulo 1: Estudio del estado del Arte sobre Gestión de Riesgos en proyectos de software	8
Centros de Pensamiento	9
Sociedad para el Análisis de Riesgos (SRA)	9
Project Management Institute (PMI)	9
Software Engineering Institute (SEI)	10
Microsoft Corporation	10
Risk World	10
Evolución de la Gestión de Riesgos	10
El Modelo de Boehm	11
Continuous Risk Management (CRM)	13
Taxonomy-Based Risk Identification	17
Software Risk Evaluation (SRE)	19
El Modelo de Hall	22
PMBOK®	22

Microsoft Solutions Framework – Risk Management Discipline.	26
Estándares, Normas y Certificaciones	32
Gestión de Riesgos en la Universidad de las Ciencias Informáticas.	32
Conclusiones del Estudio del Estado del Arte	34
Capítulo 2: Identificación y Análisis	36
Alcance del Modelo.....	36
Principios.....	37
Premisas para su aplicación.	38
Representación del modelo.....	39
Representación de los riesgos.....	40
Primer Grupo de Procesos.....	42
Planeación.....	42
Identificación.....	46
Análisis Cualitativo.....	55
Análisis Cuantitativo.....	64
Conclusiones Parciales.....	66
Capítulo 3: Medición y Control	67
Segundo Grupo de Procesos	67
Planeación de la Respuesta.	67
Monitoreo y Control.....	72
Evaluación y Aprendizaje.....	79
Roles y sus Responsabilidades	82
Artefactos.....	83
Resumen	84
Grado de terminación.....	86
Ventajas y desventajas respecto a otros modelos.....	86
Evolución del modelo	88
Extensión del modelo.....	89
Conclusiones Parciales.....	89
Conclusiones	90
Recomendaciones	91
Bibliografía.....	92
Anexo1 – Plan de Gestión de Riesgos.....	98
Anexo2 – Taxonomía del Desarrollo de Software	99
Anexo3 – Cuestionarios para la Identificación.....	100

Anexo4 – Modelo para documentar el riesgo.....	106
Anexo5 – Lista de Riesgos Comunes	107
Anexo6 – Lecciones Aprendidas.....	112
Anexo7 – Plan de Respuesta de Riesgo.....	113
Anexo8 – Respuestas Comunes a Riesgos.....	114

Índice de Tablas

Tabla 1. Ejemplo de planificación guiada por hitos.....	45
Tabla 2. Probabilidades de los riesgos.....	56
Tabla 3. Impacto respecto al costo.	58
Tabla 4. Impacto respecto al tiempo.	58
Tabla 5. Impactos consolidados.....	59
Tabla 6. Impacto respecto al costo.	59
Tabla 7. Grados de certidumbre.....	60
Tabla 8. Matriz de probabilidad e impacto.....	61
Tabla 9. Grado de importancia de cada objetivo.	63
Tabla 10. Valores numéricos de impactos de cada categoría.	63
Tabla 11. Marcos de tiempo.....	71
Tabla 12. Métricas sobre la Gestión de Riesgos.	77
Tabla 13. Roles y responsabilidades.	82
Tabla 14. Artefactos del modelo.....	83
Tabla 15. Resumen del modelo.	84

Índice de Figuras

Figura 1. Elementos de Construcción de una Profesión. Adaptado de (28).	8
Figura 2. Evolución de la Gestión de Riesgos.....	11
Figura 3. Pasos de la Gestión de Riesgos. Modelo de Boehm. Tomado de (48).....	12
Figura 4. Paradigma de Gestión de Riesgos del SEI. Imagen tomada de (37).....	13
Figura 5. Taxonomía del desarrollo de software. Imagen tomada de (39).....	18

Figura 6. Procesos de la Gestión de Riesgos de MSF. Imagen tomada de (22).	27
Figura 7. Definición del riesgo de MSF. Imagen tomada de (22).	28
Figura 8. Probabilidad de ocurrencia de los riesgos. Tomado de (22).	28
Figura 9. Impacto esperado en el costo. Tomado de(22).	29
Figura 10. Matriz de probabilidad e impacto. Tomado de (22).	29
Figura 11. Fórmula para calcular la exposición. Tomado de (22).	30
Figura 12. Representación del riesgo. Tomado de (22).	30
Figura 13. Principios del Modelo.	37
Figura 14. Premisas del Modelo.	38
Figura 15. Flujo de ejecución más común de los procesos de la Gestión de Riesgos.	39
Figura 16. Actividad de la Gestión de Riesgos en cada fase del proyecto.	40
Figura 17. Representación del riesgo.	41
Figura 18. Flujo de trabajo de Planeación.	43
Figura 19. Técnica de Entrevista.	49
Figura 20. Procedimiento para realizar las entrevistas.	50
Figura 21. Técnica Tormenta de Ideas.	51
Figura 22. Desarrollo de las ideas.	52
Figura 23. Técnica basada en el conocimiento.	54
Figura 24. Flujo de trabajo de Análisis Cualitativo.	55
Figura 25. Priorización utilizando técnicas estadísticas.	62
Figura 26. Flujo de trabajo de Análisis Cuantitativo.	64
Figura 27. Flujo de trabajo de Planeación de la Respuesta.	67
Figura 28. Proceso para asistir en la determinación de la estrategia a seguir.	69
Figura 29. Flujo de trabajo de Monitoreo y Control.	73
Figura 30. Ejemplo de reporte de riesgos cerrados (izquierda) y riesgos de alta prioridad (derecha)...	78
Figura 31. Ejemplo de gráfico para observar las variaciones respecto a los datos anteriores.	78
Figura 32. Flujo de trabajo de Evaluación y Aprendizaje.	79
Figura 33. Evolución futura del modelo.	89

Introducción

Los riesgos están presentes siempre en todo tipo de actividad que ha hecho el hombre, pues cada una tiene presente elementos que atentan en alguna medida contra su desarrollo satisfactorio o están propensas a que algunos eventos sucedan y causen efectos similares.

De seguro el hombre primitivo conocía que las ataduras de la punta de su lanza al mango podían romperse o el viento cambiar y estropear la cacería. Romperse la atadura o que cambie el viento son eventos que pueden ocurrir durante la actividad y de hacerlo trae efectos negativos para ella.

De esta forma en todos los aspectos de la vida diaria tenemos riesgos presentes: la grasa en las comidas puede que nos aumente el colesterol, los tornillos en las llantas de los autos pueden deteriorarse y quebrarse y tener un accidente, en fin.

De seguro también el hombre primitivo reforzaba la atadura de la lanza y observaba el comportamiento del viento para decidirse a cazar; igualmente evaluamos si nos aumentamos la grasa en las comidas y si es hora de llevar el auto a revisión. Es decir, como proceso del pensamiento lógico, nos cuestionamos estos elementos y eventos y tomamos medidas para que los efectos de su ocurrencia sean lo menos negativo posible.

También el hombre primitivo tenía una manzana en la bolsa para si el viento cambiara utilizarla como comida ese día; también tenemos pastillas guardadas para bajar el colesterol y dispositivos en el auto para si se poncha. O sea que haciendo uso de nuestra capacidad previsoras nos preparamos para que cuando aquellos elementos o eventos que no podemos asegurar del todo ocurran, minimizar los efectos negativos que nos puedan causar.

Se ha visto hasta aquí como se pueden desencadenar eventos que nos preocupan y la forma inherente en que día a día el hombre “gestiona” esos eventos en las actividades cotidianas, pero de forma muy parecida este proceso se aplica a todas las actividades ingenieriles que ha participado el hombre en todas las eras industriales.

A este proceso donde se identifican los riesgos, se toman medidas para minimizar los efectos y otras para prepararse en caso que ocurran y se monitorean se denomina precisamente “Gestión de Riesgos”.

La Gestión de Riesgos ha evolucionado pasando por un proceso inherente como se observó anteriormente, a un proceso consciente, a un proceso lógico, sistemático y explícito como tenemos hoy en día (1), apoyado por las matemáticas y metodologías desarrolladas en este sentido.

Se gestionan los riesgos para la salud, la seguridad nacional, los cambios climáticos, el medio ambiente, la construcción, el transporte.

La naturaleza incierta de los riesgos.

Como se observó en varios ejemplos, los riesgos son por naturaleza inciertos (2), es decir, una vez que identificamos un riesgo este tiene determinada probabilidad de ocurrir, y los esfuerzos siempre se concentran en encontrar la probabilidad con la mayor certidumbre posible para poder prepararse mejor para su ocurrencia.

Los riesgos en el mundo de los negocios.

En el mundo de los negocios se comienza a formalizar la Gestión de Riesgos como un mecanismo de protección y control para los proyectos, para minimizar los eventos negativos así como sus efectos, para conocer el grado de certidumbre o la probabilidad de que fracase el proyecto, o tener la seguridad que se está preparado para situaciones emergentes. También dada la necesidad de una medición constante de los indicadores claves para el éxito del proyecto, de un análisis de los resultados y control periódico, para tener un panorama en tiempo real (o lo más real posible) del estado del proyecto y así tomar las decisiones correctas en el momento adecuado. (3).

El sector financiero aplica con más rigor la Gestión de Riesgos para asegurar y evaluar las inversiones y obtener valor de mercado, pero en general muchos sectores y entidades privadas y estatales, reconocen la importancia de su aplicación y surgen nuevos métodos para aplicar los procesos definidos en la Gestión de Riesgos específicos a cada área así como nuevos tipos o categorías de riesgos a tener en cuenta. En general todas las empresas necesitan controlar los riesgos de una forma u otra, y nuevos riesgos surgen en la medida que evolucionan las industrias y aparecen nuevas necesidades y desafíos que enfrentar (4), (5).

Los riesgos en el mundo del software.

El software requiere que se comprenda el fenómeno y que además se modele (6): la situación de la vida real que un software modela o intenta resolver, tiene una complejidad que generalmente es alta, modelarla para que sea solucionable por un sistema informático es complejo, además de los requerimientos del software en sí (funcionales o no), se unen muchos otros que aumentan la complejidad: flexibilidad, encapsulamiento, alta cohesión, bajo acoplamiento, reusabilidad; la comunicación entre desarrolladores y clientes.

Unido a esto, durante el desarrollo del proyecto existen muchos riesgos de diferentes categorías (operacionales, funcionales, del entorno) que atentan contra sus objetivos.

Las empresas dedicadas a la producción de software aumentan y el índice de fracaso de los proyectos de software tiende a aumentar y empeorar (7). Al tener la Gestión de Riesgos la intención de minimizar o reducir el impacto de los riesgos en los objetivos del proyecto, ésta se impone como una práctica necesaria en la gestión de proyectos de software y es un componente fundamental en la gestión integrada de proyectos.

Un proyecto de software puede ser considerado exitoso si cumple con los requerimientos, es entregado en tiempo y dentro del presupuesto (8), por lo que todo elemento o evento que atente contra estos objetivos fundamentales, debe manejarse con cuidado y para esto la Gestión de Riesgos ofrece un mecanismo, guía y elementos que ayudan a los gerentes de proyectos a identificar, controlar y prepararse para los riesgos.

Frecuentemente en los proyectos de software no son bien entendidos los requerimientos, o las planificaciones y presupuestos son irrealistas o se subestima la complejidad del software, en fin, que existen o surgen situaciones que afectan al proyecto y todos estos factores constituyen riesgos que están presentes en el proyecto, y trae implicaciones catastróficas ignorarlos o no tomar medidas para ello.

Las estadísticas indican que una parte significativa de los proyectos de software que fracasan, no tuvieron, o tuvieron una pobre Gestión de Riesgos, y los problemas que enfrentaron hubieran sido eliminados, o su impacto reducido, si hubieran tenido una Gestión de Riesgos formal (9). No quiere decir que solamente aplicando esta disciplina en la gestión de proyectos se llegue al éxito, pero sí es una práctica importante.

Hoy día aumenta el uso del software en actividades críticas para los negocios, los gobiernos; varían las tecnologías y es necesaria una respuesta rápida a los clientes para aprovechar la oportunidad de negocio; las técnicas tradicionales de planeación necesitan de disciplinas de soportes más fuertes para que la gestión de proyectos responda a las necesidades actuales, y en este sentido la Gestión de Riesgos se alza e incluso hay tendencias a dirigir el desarrollo del proyecto guiado por los riesgos.

La Gestión de Riesgos.

En la Gestión de Riesgos se identifican varias etapas o procesos fundamentales que varían según la tendencia o el autor pero en general se consideran: planeación, identificación, análisis, mitigación, control y seguimiento (10).

En la etapa de planificación, es donde se decide qué estrategia se utilizará para la Gestión de Riesgos. En esta etapa los directivos del proyecto deciden cómo afrontar y guiar la Gestión de Riesgos respetando las políticas o disposiciones de la empresa, utilizando una guía para la Gestión de Riesgos. Aquí definen qué elementos considerarán de cada riesgo, cómo se van a medir, qué criterios se utilizarán, con qué documentos se trabajará y qué formato y consideraciones deben tener.

Este proceso se realiza en una etapa muy inicial del proyecto y generalmente se realiza similar a proyectos con características comunes: recursos humanos que participan, situaciones sociales o políticas etc. es decir, con el tiempo los gerentes de proyectos se hacen marcos de trabajo para planificar la Gestión de Riesgos y se tiende a utilizarlos en futuros proyectos.

Una vez que el equipo de proyecto establece las disposiciones sobre cómo se debe manejar la Gestión de Riesgos, y durante el proyecto y en varias iteraciones se hará una identificación de los riesgos. Este es un proceso donde se descubren los riesgos involucrados en el proyecto, y se documentan. Es una

etapa importante en la Gestión de Riesgos y requiere de mucha honestidad por parte de los implicados para reconocer riesgos de cualquier índole que puedan afectar al proyecto.

Elementos que influyen en esta etapa son: la capacidad de los implicados de detectar un riesgo¹, la experiencia en Gestión de Riesgos o en gestión de proyectos en general, pues algunos gerentes de proyectos experimentados crean su propia lista de “riesgos siempre presentes” que resulta útil en esta etapa, la claridad y el grado de definición en los procesos de Gestión de Riesgos, el nivel de concientización con su utilidad para el desarrollo satisfactorio del proyecto.

Con todos los riesgos “más visibles” identificados y documentados se realiza un análisis de los mismos (el nivel de profundidad del análisis y los elementos a analizar así como la estrategia para hacerlo fue establecido en la etapa de planificación).

El análisis de los riesgos se puede hacer cualitativo y cuantitativo. El análisis cualitativo es el proceso de medir el impacto de los riesgos identificados (10) de manera no exacta. Los riesgos se analizan de acuerdo a su probabilidad de ocurrencia y el impacto que traerá para el proyecto, pueden clasificarse alto, medio o bajo. Estos valores o niveles (alto, medio, bajo) son definidos en el proceso de planeación e indican cierto grado de relevancia o diferencia respecto a los otros riesgos.

Durante el análisis cualitativo se clasifican los riesgos en categorías. Estas varían de acuerdo al tipo de proyecto y al tipo de especialista que identificó el riesgo: financieros, operacionales, tecnológicos.

Esta etapa de análisis cualitativo captura las opiniones de los especialistas y de igual forma la experiencia y apreciación correcta es un factor decisivo en la calidad de la Gestión de Riesgos.

El análisis cuantitativo de los riesgos se refiere en cambio a una estimación numérica de la probabilidad de ocurrencia de cada riesgo. Y utilizando técnicas y métodos estadísticos y de simulación, se calcula la probabilidad de alcanzar los objetivos del proyecto.

Este es un elemento importante cuando se desea obtener un valor numérico de la certeza de éxito de un proyecto y una vez más su acercamiento a la realidad depende de cuan cerca a lo real estén los valores de probabilidad de ocurrencia.

Teniendo claridad sobre la probabilidad de ocurrencia de un riesgo, y los impactos que traería, se pueden tomar mejores decisiones sobre qué acciones tomar o qué estrategia seguir para eliminar las amenazas a los objetivos del proyecto que los altos riesgos ofrecen, si aceptar el riesgo, mitigarlo, transferirlo o no tomarlo.

Durante esta etapa de mitigación, se elaboran planes de contingencias para los riesgos que se decidan afrontar (1).

En todo el ciclo de vida del proyecto se monitorea el estado de los riesgos, y se identifican nuevos comenzando el proceso otra vez, o se desechan algunos que ya no constituyen riesgos, se mantienen actualizados los documentos de la Gestión de Riesgos y se reevalúan. En fin, se mantiene un control

¹ Algunas personas detectan riesgos mejor que otras.

periódico sobre el estado de los riesgos sirviendo así como un indicador actualizado de la “salud” del proyecto.

Caracterización de la Gestión de Riesgos en la Universidad de las Ciencias Informáticas

Según entrevistas realizadas, con frecuencia los proyectos productivos sufren afectaciones en su cronograma, en la calidad del producto, en el presupuesto, en la formación de los estudiantes (11). Una variable significativa en la Gestión de Proyectos es la Gestión de Riesgos (12), al punto que en la Facultad 3 por ejemplo se considera que el nivel de calidad de los proyectos depende de la minimización del número de riesgos al que se enfrenta el mismo (12).

Varios estudios estadísticos realizados en la UCI (11 tesis basadas principalmente en encuestas realizadas a líderes de proyecto, estudiantes y directivos) concluyen que en la generalidad de los proyectos productivos no se definen los riesgos con claridad (13), la Gestión de Riesgos es inadecuada y carece de utilización de herramientas para su aplicación (14), generalmente en los proyectos productivos de software los riesgos se gestionan deficientemente (15) y en muchos de ellos no se gestionan (16) (17) y tienen un marco informal (18).

Los documentos oficiales que la institución especifica están descritos en el expediente de proyecto respondiendo al Manual de Procedimientos para el Diagnóstico de Riesgos (19) que implementa la Resolución 297/03 del MFP (estos documentos se discuten en el Capítulo 1 *ver página 32*). Estos documentos tributan a una Gestión de Riesgos “primitiva” que se limita a una lista de riesgos con un análisis cualitativo que se actualiza periódicamente, además este proceso no es bien concientizado, no se tiene como una cultura y una práctica necesaria y responsable.

Existen varios modelos para la Gestión de Riesgos, por ejemplo se pudiera utilizar la guía básica del PMBOK® (10), otros modelos propuestos por el SEI (20), adaptar metodologías como CRAMM (21) o Microsoft Solutions Framework (22) o utilizar otros modelos, métodos y procedimientos propuestos como Keshlaf (23), Yacoub (24), AORDD Framework (25) y muchos otros. Además, existen experiencias en varios proyectos productivos que aplican la Gestión de Riesgos utilizando sus propios métodos y adaptaciones como los proyectos “Conocimiento Geológico” (26), “Atención Primaria a la Salud” (18), y métodos de Gestión de Riesgos adaptadas a RUP (27).

Independientemente a estos modelos y soluciones muy locales, la Gestión de Riesgos es insuficiente y como conclusión en este sentido se llega a que es producto de las insuficiencias en estos modelos para aplicarse a nuestro entorno, para orientar una Gestión de Riesgos efectiva y objetiva para nuestro proceso productivo, donde especifiquen las funciones y los procedimientos de los involucrados en el proyecto y específicamente en la Gestión de Riesgos en cada etapa del proyecto, se especifiquen plantillas para estos procesos, donde se describa la taxonomía de los riesgos característicos y más frecuentes.

Problema Científico

Las insuficiencias en los modelos existentes de Gestión de Riesgos para ser aplicados a proyectos de software desarrollados en entornos productivos similares al de la Universidad de las Ciencias Informáticas están afectando el desarrollo exitoso de los proyectos respecto al cumplimiento de los plazos, la recuperación ante contingencias y mitigación de los factores que pueden provocar el fracaso.

Objeto de estudio

Gestión de Proyectos de Software.

Campo de acción

Gestión de Riesgos en proyectos de software.

Hipótesis

Si se desarrolla un modelo para la Gestión de Riesgos en proyectos de software desarrollados en entornos productivos similares al de la Universidad de las Ciencias Informáticas, contribuiría a mejorar el desarrollo de los proyectos respecto al cumplimiento de los plazos, la recuperación ante contingencias y mitigación de los factores que pueden provocar el fracaso.

Objetivos

Objetivo general

Desarrollar un modelo para la Gestión de Riesgos que contribuya al desarrollo exitoso de proyectos de software en entornos productivos similares al de la Universidad de las Ciencias Informáticas.

Objetivos específicos

- Realizar un estudio del estado del arte acerca de los diferentes enfoques para la Gestión de Riesgos en los procesos de desarrollo de software.
- Desarrollar un modelo para la Gestión de Riesgos en proyectos de desarrollo de software.

- Realizar una evaluación crítica del modelo a partir de la comparación con otros modelos analizados atendiendo a ventajas y desventajas respecto a su contribución al cumplimiento de los plazos de los proyectos, la recuperación ante contingencias y mitigación de los factores que pueden provocar el fracaso.

Posibles resultados

Diseño de un modelo para la Gestión de Riesgos en los proyectos de desarrollo de software desarrollados en entornos productivos similares al de la Universidad de Ciencias Informáticas.

Métodos y técnicas a utilizar

Se utilizó como estrategia de investigación la explicativa. Basados en investigaciones anteriores se determinan las causas del fenómeno y se genera un entendimiento.

Se utilizaron métodos teóricos: Histórico lógico, Hipotético deductivo, Sistémico. Se planteó el problema como un todo donde los elementos del modelo que lo soluciona se comportan como un sistema sostenible e integral. Se enfocó el estudio de la Gestión de Riesgos desde un enfoque histórico lógico, en el capítulo 1 se realiza un estudio del estado del arte sobre la evolución de la Gestión de Riesgos y las principales tendencias actuales. Se siguió un método hipotético deductivo porque a partir del problema se plantearon objetivos específicos y una hipótesis que con el transcurso de la investigación es resuelta.

Estructura del trabajo

Este trabajo consta de tres capítulos donde se describe un estudio del estado del arte sobre el tema en el capítulo 1, analizando los principales centros de pensamiento y la evolución de la Gestión de Riesgos en el mundo del software así como su estado en la universidad. El capítulo 2 describe el modelo propuesto para la Gestión de Riesgos explicando su alcance, representación gráfica y la instrumentación de los procesos de identificación y análisis. El capítulo 3 describe la instrumentación de los procesos de monitoreo y control; además de un resumen con los roles y responsabilidades de los implicados en la Gestión de Riesgos, de los artefactos y de todos los procesos, actividades y técnicas en general. El capítulo finaliza mencionando el grado de terminación del modelo y sus ventajas y desventajas respecto a otros modelos analizados.

Capítulo 1: Estudio del estado del Arte sobre Gestión de Riesgos en proyectos de software

Este capítulo explora los diferentes centros de pensamiento en este sentido, sus publicaciones más importantes, los principales repositorios de materiales de Gestión de Riesgos, los trabajos más relevantes vinculados a la Gestión de Riesgos analizando los procesos definidos, la representación de los riesgos y técnicas o métodos propuestos para llevar a cabo los procesos. Se seleccionaron trabajos de todos los elementos de construcción de la profesión Gerencia de Proyectos: Investigaciones, cuerpo de conocimiento, estándares, educación y certificación como ilustra la Figura 1.

De cada modelo seleccionado se evaluarán con especial atención lo siguientes aspectos:

- Procesos que define el modelo, su comparación con los procesos Planeación, Identificación, Análisis, Planeación de la Respuesta, Control y Seguimiento, Evaluación, Aprendizaje.
- Fortaleza y claridad de las técnicas para cada proceso en especial las técnicas para definir la prioridad de los riesgos y la integridad de los datos de entrada.
- Explicación de la asignación de roles.
- Definición clara de los datos o propiedades de los riesgos.
- Explicación y definición de la documentación o artefactos que se generan.
- Inclusión de elementos para gestionar las oportunidades.
- Inclusión de sugerencias para la respuesta a los riesgos en especial reserva para contingencias.
- Inclusión de las memorias finales de la Gestión de Riesgos.
- Existencia de documentación pública o soporte adecuado para el modelo.

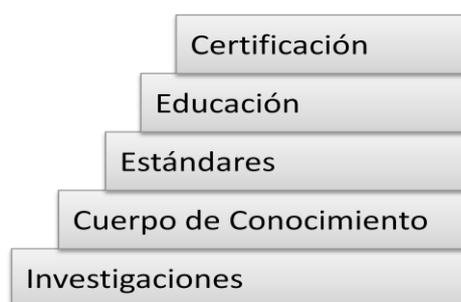


Figura 1. Elementos de Construcción de una Profesión. Adaptado de (28).

Centros de Pensamiento

Los centros de pensamiento más importantes en materia de riesgos identificados son la Sociedad para el Análisis de Riesgos (29) (*Society for Risk Analysis*, SRA por sus siglas en inglés); el Project Management Institute (PMI) (30); Software Engineering Institute (SEI) (31); “Institute of Electrical and Electronics Engineers”(IEEE) (32); Microsoft Corporation (33); International Standard Organization (ISO) (34).

Las secciones siguientes describen brevemente cada uno de estos centros destacando el por qué de su importancia en materia de Gestión de Riesgos.

Sociedad para el Análisis de Riesgos (SRA).

La Sociedad para el Análisis de Riesgos fundada en 1981 ofrece un área de colaboración para profesionales de varias disciplinas vinculados al tema, es la organización líder en la investigación académica en este campo.

Aunque tratan aspectos de riesgos en general rara vez vinculados a la Gestión de Riesgos en proyectos de software, proveen un fórum para el desarrollo de nuevos aspectos teóricos o prácticos en los procesos del análisis de riesgos y estado del arte sobre las más recientes investigaciones y tendencias en materia de riesgos.

Esta sociedad se estructura en 3 divisiones: EE.UU, Europa y Japón.

Su publicación más importante es “Risk analysis, an International Journal” (35), tiene un factor de impacto de 1.938 (36), está clasificada entre las 10 publicaciones más importantes en el “ISI Journal Citation Reports” dentro de las categorías ciencias sociales y métodos matemáticos. Otra publicación importante es el “Journal of Risk Research” lanzado en 1997 como la publicación oficial de SRA-Europa.

Project Management Institute (PMI).

El Project Management Institute (PMI), fundada en 1969 es la asociación líder mundial en dirección de proyectos, defiende y promueve la profesión de Gerente de Proyecto. Durante casi 40 años, el PMI les ha proporcionado a sus miembros la oportunidad de compartir teorías, mejores prácticas y experiencias relacionadas con la dirección de proyectos. Posee estándares en gestión de proyectos como el “Project Management Body of Knowledge” (PMBOK®) (10) y el Organizational Project Management Maturity Model (OPM3®). Tiene programas de certificación como la certificación de directores de proyecto Professional Project Manager (PMP®) y Certified Assistant in Project Management (CAPM®). Sus publicaciones más importantes son el PM Network, PMI Today, y PM Journal.

Software Engineering Institute (SEI).

El (SEI) fundado en 1984, es una unidad de la Carnegie Mellon University dedicada al desarrollo de la ingeniería de software. Comienza a principios de los 90 a desarrollar trabajos en la Gestión de Riesgos, uno de los primeros es el “Continuous Risk Management (CRM²)” (37) (38), un método de Gestión de Riesgos que incluye los principios básicos que concuerdan en gran medida con el modelo de Boehm; “Taxonomy-based Risk Identification” (39), un método para facilitar el proceso de identificación de los riesgos; “Software Risk Evaluation (SRE)” (40) que define un proceso para la identificación, análisis y desarrollo de estrategias de mitigación; “Team Risk Management (TRM)” (41) define la estructura y operaciones a realizar para gestionar los riesgos en una organización por un equipo; una línea de tiempo de estos trabajos y sus principales variantes o tendencias se puede observar en (42) que además mencionan otros trabajos interesantes (43).

Microsoft Corporation.

Microsoft Corporation fundada en 1975, corporación multinacional productora de software líder en el mundo, hacia la década del 2000 promueve “*Microsoft Solutions Framework*”, un conjunto de guías, prácticas, procedimientos y herramientas para el desarrollo de aplicaciones, que incluye una disciplina para la Gestión de Riesgos: Microsoft Solutions Framework – Risk Management Discipline (22).

Risk World.

Uno de los principales repositorios de materiales de riesgos es Risk World (44); reúne una gran variedad referencias a noticias, publicaciones internacionales, libros, bases de datos de riesgos (45) con riesgos de diferentes sectores (no solamente del mundo del software), softwares como herramientas para ayudar en la Gestión de Riesgos; asociaciones o institutos en el mundo con objetivos o misión vinculados a la enfocados a la Gestión de Riesgos, grupos de discusión, artículos entre otros (46). Durante algunos años fue el publicador del “Risk analysis, an International Journal” de la SRA.

Evolución de la Gestión de Riesgos

La Gestión de Riesgos en los proyectos de software comienza a formalizarse a finales de los 80 principios de los 90, con trabajos del “Institute of Electrical and Electronics Engineers” (IEEE) y el “Software Engineering Institute” (SEI). Estos autores sientan las bases de los procesos y principios involucrados en la Gestión de Riesgos. Surgen varios métodos, herramientas y frameworks complementarios a estos modelos o a sus variantes. En el 2000 surge el PMBOK®, cuerpo de conocimiento de la Gestión de Proyectos que incluye prácticas de Gestión de Riesgos. La Figura 2 muestra el orden de los principales trabajos en este sentido.

² CRM, Continuous Risk Management, no Customer Relationship Management.

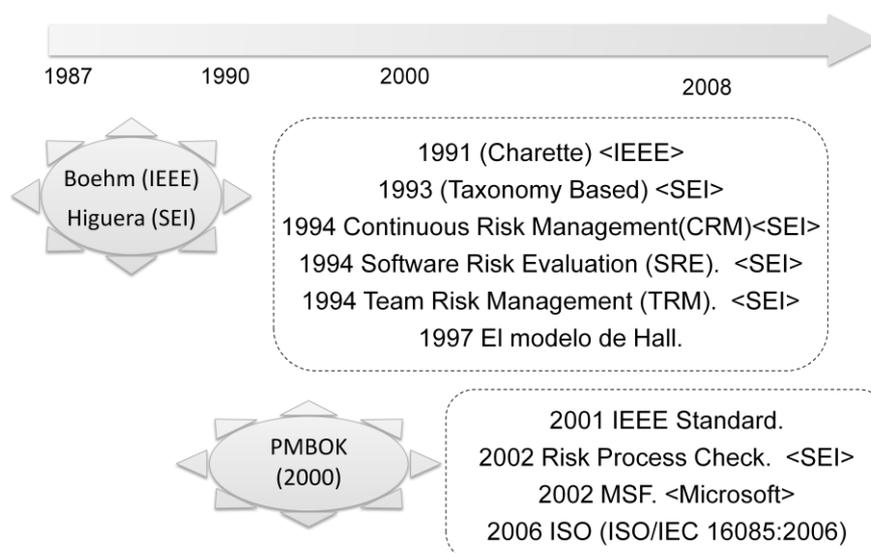


Figura 2. Evolución de la Gestión de Riesgos.

El Modelo de Boehm.

La IEEE fue una de las primeras instituciones en formalizar la Gestión de Riesgos con el modelo propuesto por Boehm en 1989 (47), (9) que ha evolucionado incorporando técnicas y elementos para lograr un modelo más efectivo pero en esencia se mantienen las bases iniciales.

El modelo de Boehm propone procesos y técnicas divididas en 2 partes principales: medición de los riesgos y control de los riesgos. Dentro de la medición incluye procesos como Identificación, Análisis y Priorización. Estos procesos están bien ubicados en esta categoría de acuerdo a su intención, sin embargo la priorización de los riesgos debe considerarse como un proceso dentro del análisis, como una función del análisis que utilizando los datos generados organiza los riesgos y no como un proceso al mismo nivel del resto.

Durante la identificación propone el uso de varias técnicas que ayudarán en esta etapa como listas de chequeo, análisis guiado por decisiones, descomposición etc. Aunque se justifica su importancia de uso para este proceso, estas técnicas se describen de manera abstracta y carecen de claridad para ser usadas.

Para el proceso de análisis propone modelos de rendimiento, modelos de costo, análisis de redes, análisis del factor de calidad. Este proceso se considera importante y con el objetivo de extraer o descubrir la mayor cantidad de datos posibles de los riesgos y el uso de estas técnicas contribuye en este sentido, sin embargo, la descripción precisa y objetiva del uso de estas técnicas se comporta como en el proceso anterior.

Durante el proceso de priorización propone analizar la exposición del riesgo, su influencia y una reducción compacta de los riesgos, pero no se explica con exactitud los criterios para obtener los riesgos priorizados y no son criterios precisos o cuantitativos.

En el control de los riesgos define los procesos de Planeación, Resolución y Monitoreo. La planeación propone la definición de criterios para técnicas o estrategias para manejar los riesgos (Evitar, Transferir, Reducir), el modelo no incluye sugerencias en este sentido. El modelo incluye artefactos como la Planeación de los Elementos y el Plan de la Iteración. De estos artefactos se mencionan sus principios básicos y su descripción general, no se muestran ejemplos o se define claramente su estructura o formato.

Como técnica para la resolución de los riesgos propone prototipos, simulaciones, análisis, reuniones. Estas técnicas se describen pero al igual que en procesos anteriores, no se define claramente cómo utilizarlas en la Gestión de Riesgos.

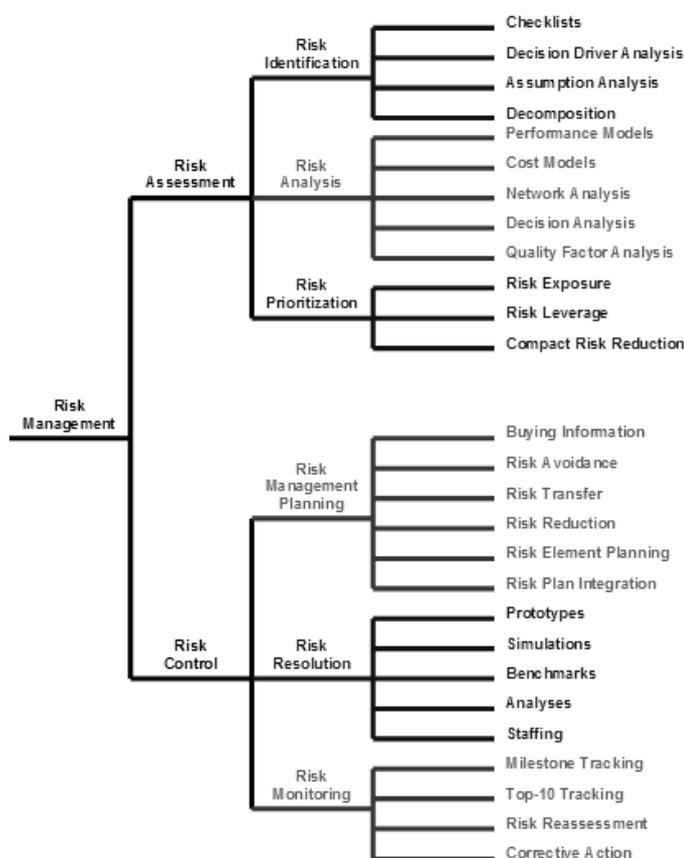


Figura 3. Pasos de la Gestión de Riesgos. Modelo de Boehm. Tomado de (48).

Definen estrategias para el monitoreo: basadas en hitos, los 10 más importantes y medición de los riesgos. De estas estrategias se describe su esencia y su justificación, en el caso de la medición de los riesgos no se explica en profundidad mecanismos, técnicas e indicadores claves para utilizar en su

ejecución; la estrategia de los 10 más importantes no define un criterio cuantitativo o matemático que justifique su elección y se considera no-determinante.

La Figura 3 resume los procesos y técnicas descritos por Boehm.

Este modelo describe la estructura básica de los procesos, métodos y artefactos a desarrollar durante la Gestión de Riesgos, así como una clasificación de acuerdo a la naturaleza de los procesos (medición y control), pero no el orden en el que estos se ejecutan o concurren.

El modelo no incluye la gestión de las oportunidades ni define procesos de aprendizaje de la Gestión de Riesgos, ni el resumen o memorias finales.

El modelo de Boehm sentó las bases sobre los procesos y técnicas a utilizar para el resto de los modelos que surgieron posteriormente. La IEEE adoptó este modelo, que se continuó desarrollando. En su versión de 2001 incluyen procesos de evaluación de la Gestión de Riesgos, este último modelo carece de documentación pública.

Continuous Risk Management (CRM).

“The Software Assurance Technology Center” (TSATC) de NASA desarrolló en conjunto con el SEI “Continuous Risk Management CRM” (37) (38) a principios de los 90, un método de Gestión de Riesgos extendido a la comunidad de desarrollo de NASA. El método reconoce la importancia de la Gestión de Riesgos como una práctica necesaria. Define 6 principios o funciones para la Gestión de Riesgos los cuales ilustra de esta forma:

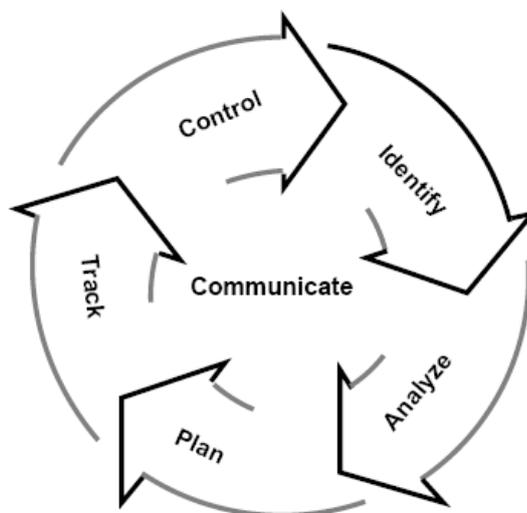


Figura 4. Paradigma de Gestión de Riesgos del SEI. Imagen tomada de (37).

En este método estos procesos ocurren continua e iterativamente, pueden ocurrir simultáneamente, es decir, los riesgos son a la vez controlados mientras se están identificando nuevos riesgos o se está ejecutando el plan de mitigación para otro riesgo. No obstante no queda claro en este modelo cómo ocurre dicha simultaneidad y cómo es la comunicación durante la simultaneidad o durante su flujo secuencial.

Identificación.

Este proceso tiene el objetivo de “considerar los riesgos antes que se vuelvan problemas³”, destaca que cualquiera en el proyecto puede identificar riesgos pues cada cual tiene un conocimiento específico de partes individuales importante.

Hacen énfasis en la forma en que se deben escribir los riesgos: una primera parte definiendo al riesgo, y una segunda opcional definiendo las consecuencias de manera contextual.

La definición del riesgo debe ser clara y precisa. Su forma general de describir un riesgo cumple con la siguiente expresión:

Dado <condición> hay una posibilidad de que <consecuencia> ocurra.

La “Condición” se centra en qué está causando preocupación y es un hecho conocido y certero. La consecuencia no es más que el impacto del riesgo.

De esta forma explican cómo se debe describir un riesgo, este es un elemento importante que ayuda a la documentación objetiva de los riesgos, a su uniformidad y claridad.

Este diagrama ayuda a comprender la estructura para identificar y documentar un riesgo, sin embargo, aunque los elementos son comprensibles, no se detallan sus propiedades y relaciones.

Al igual que muchos autores, reconocen que para este proceso son cruciales las comunicaciones abiertas, la vista futurista y el trabajo en equipo, elementos que constituyen los principios del modelo.

Su definición de la representación de un riesgo es la expresión anterior que forma la definición del riesgo donde brinda un resumen y concreción del riesgo.

Análisis.

Definen este proceso con el objetivo de proveer datos para posteriormente tomar decisiones, es el proceso de examinar cada riesgo en detalle, cómo se relacionan unos con otros y cuáles son los más importantes. A su vez tiene 3 subprocesos: evaluar, clasificar y priorizar.

³ Esta frase textual, ayuda a comprender el significado de Riesgo.

Durante la evaluación se analiza cada riesgo y se deciden valores para los 3 atributos que definieron: impacto (perdidas o efecto en los objetivos del proyecto), probabilidad (probabilidad de ocurrencia), timeframe (periodo en el que se deben tomar medidas al respecto).

Esta última propiedad del riesgo es introducida en este modelo. Se establecen valores cualitativos para cada atributo y los criterios para decidirse por un valor u otro, por ejemplo para el timeframe: Corto Plazo (1 mes), Mediano Plazo (3 meses), Largo Plazo (6 meses).

En la clasificación no definen un árbol de categorías sin embargo destacan bien la importancia de este proceso: entender mejor la naturaleza o la fuente de los riesgos, eliminar riesgos duplicados o combinar los equivalentes.

En la priorización no definen un criterio o algún método, solo destacan que se usa el sentido de “los pocos vitales”⁴ para decidir el Rank de los riesgos, que es usado posteriormente para asignar recursos al proyecto para mitigarlos, pues las condiciones y las prioridades cambian constantemente en el proyecto. Esta técnica de priorización carece de argumentos objetivos, pues no se puede juzgar cuáles riesgos serán más importantes simplemente por un criterio arbitrario.

Planeación

Esta función la definen para decidir qué se hará con los riesgos y planificar las acciones a tomar para los riesgos que se decidan asumir. Proponen los siguientes enfoques para riesgo y el plan asociado para su tratamiento:

Investigar – Plan de investigación. Establecer un plan para investigar el riesgo o los fenómenos asociados. Esta estrategia se menciona pero no ofrecen recomendaciones.

Aceptar – Justificación de la aceptación. En los casos que se decide aceptar un riesgo se debe justificar el por qué.

Observar – Requerimientos de observación. Se refiere a documentar las métricas que se usaran para monitorear las condiciones o los factores del riesgo, no obstante no definen métricas a utilizar como ejemplo o recomendaciones.

Mitigar – Plan de mitigación. Contiene las tareas concretas a llevar a cabo para mitigar el riesgo. En esta estrategia no definen un formato o estructura para el plan.

En esta función (planeación) describen brevemente los posibles enfoques a tener en cuenta y qué elementos hay que generar para cada enfoque en particular sin detallarlos.

Seguimiento.

⁴ Del inglés “Vital Few”, término usado por Joseph M. Juran para describir su uso del principio de Pareto: conocido como “la regla de 80-20”, “la regla de los pocos vitales”, “el principio del factor de esparcimiento”; en la mayoría de los casos el 80% de las salidas se deben a un 20% de las entradas.

Lo define como un proceso donde se chequean constantemente (o cada un tiempo definido) los atributos de los riesgos que se decidieron “Observar” o “Mitigar” en busca de efectividad de los planes de mitigación o de conocer el estatus de los riesgos para medir su salud. Solamente se capturan datos de los riesgos y se reportan.

Este proceso solamente se describe de modo abstracto, quienes implementen este método deben definir una forma de reporte y mecanismos o técnicas para capturar los datos pues no proponen ninguna.

Control.

Esta función tiene como propósito tomar decisiones basadas en los cambios de los valores de los atributos de los riesgos y en la efectividad de los planes de mitigación, por lo que es crucial para su buen funcionamiento que la función de seguimiento sea lo más precisa posible. Aunque hacen énfasis en la necesidad de alguna métrica para estos fines no proponen ninguna.

Como enfoques a tomar con cada riesgo durante esta función está:

Re-planear - modificar el plan o construir uno nuevo cuando se observe que el plan no está ayudando a mejorar los valores de los atributos del riesgo.

Cerrar el riesgo – se refiere a que el riesgo no existe para el proyecto.

Ejecutar un plan de contingencias – en este caso se detectan valores “dañinos” en los atributos de los riesgos y se procede a ejecutar un plan de contingencias para ese riesgo.

Continuar monitoreando – es un enfoque tomado cuando el riesgo se mantiene como se esperaba.

En este proceso tanto como en los anteriores, se mantienen la importancia de las comunicaciones abiertas entre los miembros del equipo.

Comunicación y Documentación.

Este proceso tiene como objetivo que todos los involucrados en el proyecto entiendan las alternativas de mitigación así como los datos de los riesgos. En cada función hay elementos que tienen que ser comunicados y para la efectividad de la Gestión de Riesgos las comunicaciones abiertas en la entidad son muy importantes.

Aunque recalcan con mucho énfasis la necesidad de este proceso, no queda claro la forma o “buenas prácticas” para comunicar los riesgos a través de los procesos, o cómo los procesos mismos promueven la comunicación.

Este modelo en su etapa es muy completo, el SEI imparte un curso para crear habilidades en la Gestión de Riesgos, y ofrecer guía sobre su implementación. CRM carece de especificaciones para los artefactos que se manejan en la Gestión de Riesgos, para los roles que intervienen y para las técnicas

a utilizar para realizar los procesos en especial las técnicas de priorización. CRM tiene falta de documentación pública, el “handbook” se compra al igual que el curso.

Este modelo no gestiona las oportunidades, no las concibe como un elemento manejable en la Gestión de Riesgos y que trae beneficios al proyecto y tampoco define un proceso de resumen de la Gestión de Riesgos donde se recojan las memorias finales y posteriormente se aprenda de los errores y éxitos.

Taxonomy-Based Risk Identification.

Este método fue desarrollado en junio de 1993, como un método de identificación para el primer paso de “Continuous Risk Management”. El método se centra en aquellos riesgos que son conocidos, se hayan comunicado o no; asume que los riesgos son generalmente conocidos por el personal técnico pero no son bien comunicados, que un proceso de identificación continuo es crucial para una Gestión de Riesgos eficiente, la identificación debe cubrir todas las áreas de desarrollo y soporte claves, debe crear un ambiente donde no se emitan juicios u opiniones para observar diferentes puntos de vista, no se debe juzgar el éxito del proyecto por el número de riesgos encontrados.

Proponen un cuestionario: “Taxonomy-Based Questionary” (TBQ) para realizar el proceso de identificación, con una lista de preguntas para de manera intuitiva provocar una tormenta de ideas “organizada”.

La taxonomía del desarrollo de software provee una estructura que ayuda a organizar y la identificación de los riesgos y otras áreas dentro de la Gestión de Riesgos. Este método define la taxonomía del desarrollo de software en 3 partes: **clases, elementos y atributos**.

Identifican 3 clases principales: **Ingeniería del producto** (los aspectos técnicos), **ambiente de desarrollo** (los métodos, procedimientos y herramientas para llevar a cabo el trabajo), **restricciones del programa** (elementos contractuales, operacionales y organizacionales que generalmente están fuera del control directo de los gerentes).

La Figura 6 describe la estructura de la taxonomía.

De esta forma definen cada elemento y cada atributo explicando a qué se refieren cada en el ámbito de un proyecto de desarrollo de software.

El cuestionario se realiza a nivel de Atributo, contiene una serie de preguntas, que puede que no sean relevantes para algún tipo de proyecto, o para alguna etapa del proyecto en específica, o para algún tipo de software en específico, por lo que para alguna de estas combinaciones específicas se pueden crear cuestionarios nuevos o adaptar el cuestionario.

Las preguntas parten tratando de identificar un problema y las acciones que se están tomando para ese problema, de acuerdo a las respuestas se identifican o no riesgos para el proyecto, por ejemplo:

Rendimiento

[¿Existen requerimientos de tiempo de respuesta o “Throughput”?]

[22] ¿Hay algún problema con el rendimiento?

- “Throughput”.
- Programación de eventos en tiempo real asíncronos.
- Respuesta en tiempo real.
- Tiempo de respuesta.
- Respuesta de la base de datos.

[23] ¿Se ha hecho análisis del rendimiento?

(SI) (23.a) ¿Cuál es el nivel de confianza en el análisis de rendimiento?

(SI) (23.b) ¿Se tienen un modelo para trazar el rendimiento desde el diseño a la implementación?

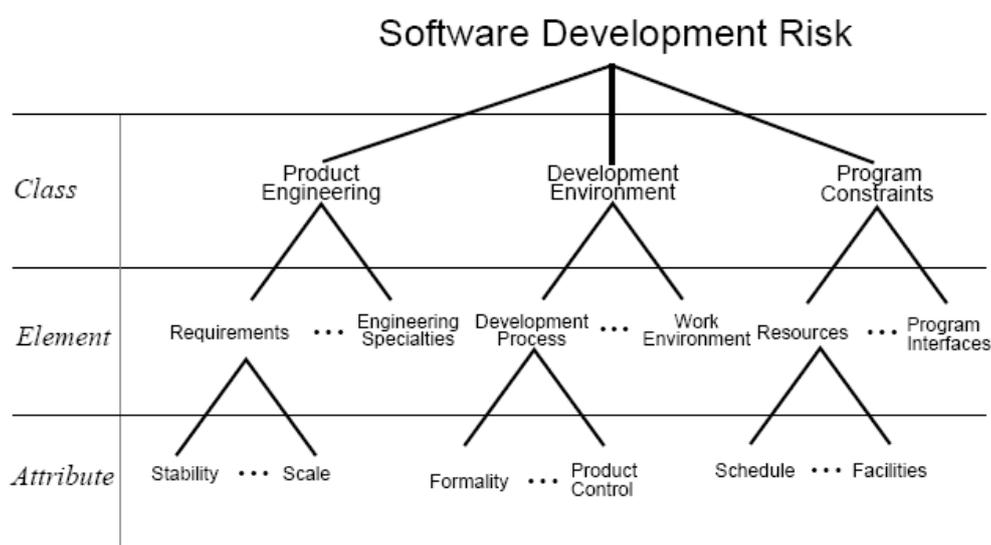


Figura 5. Taxonomía del desarrollo de software. Imagen tomada de (39).

Para la realización de las preguntas se debe escoger a quiénes realizarla. El método propone una forma de realizarlas con la intención de lograr un balance entre calidad de la identificación y tiempo empleado para ello. Se necesita personal que cubra el proyecto horizontal y verticalmente⁵ y en general describen cómo se debe realizar este proceso. Este es un elemento importante dentro del

⁵ Verticalmente se refiere a la organización estructural del proyecto; horizontalmente se refiere a los grupos funcionales del proyecto.

método y para cada implementación debería ajustarse la descripción del proceso a las características propias de la implementación.

Este método de identificación está probado ser efectivo, en todo modelo de Gestión de Riesgos es importante contar con técnicas y métodos para llevar a cabo los procesos, y este propone una taxonomía bastante completa, no obstante es necesario personalizar a las necesidades propias de la universidad, agregando las clases, elementos o atributos propios para el modelo de producción nuestro; y el cuestionario para esos nuevos elementos confeccionarse de acuerdo a la experiencia en el desarrollo de proyectos de este tipo así como personalizar los cuestionarios existentes.

La técnica de cuestionario ayuda a los encargados de la identificación de los riesgos al proveerlos de una “idea por donde comenzar”, sin embargo puede que la identificación se limite a estas áreas o a estas preguntas y otros riesgos importantes (que la taxonomía debe incluir) no sean documentados y por tanto no controlados. No obstante Taxonomy-Method ha demostrado ser eficiente para el SEI (39) y puede personalizarse a las necesidades locales de una empresa para utilizarse como una herramienta útil en la identificación de los riesgos.

Software Risk Evaluation (SRE).

Es un método para identificar, analizar, evaluar y desarrollar estrategias de mitigación para los riesgos; es una herramienta de diagnóstico para crear una línea base de riesgos para un proyecto. El SEI lo propone como método a utilizar en conjunto con CRM y TRM, es más efectivo utilizarlo como el iniciador de CRM.

Se concibe como un servicio a prestar a otras empresas, es implementado en 5 fases: *Contratación* (actividades necesarias para identificar los objetivos del proyecto, acordar elementos sobre el método y coordinar los recursos), *Identificación y Análisis de los Riesgos* (los riesgos son licitados de acuerdo a un procedimiento bien definido y documentado, son analizados y priorizados según lo define el método, y son entregados al gerente de proyecto), *Reporte Interino* (las áreas de riesgos se analizan y se preparan recomendaciones para las que se analizarán en la fase siguiente), *Planeación de la Estrategia de Mitigación* (un plan de mitigación de alcance global es realizado) y *Reporte Final* (contiene todos los datos relevantes recogidos durante el proceso y son el resultado del método).

El método describe cómo tiene que estar estructurado el *equipo de SRE* para aplicarlo. Describe cada fase definiendo su objetivo, los elementos que maneja (entradas, salidas), las personas involucradas, las herramientas a utilizar, las tareas a realizar y el tiempo promedio necesario para realizarlas:

Contratación.

Es la fase más importante para el método pues se definen las expectativas de todos los implicados. SRE considera muy necesario definir explícitamente los retos y expectativas del gerente de proyecto

con el proyecto en sí y con la aplicación de SRE, y el de los interesados. El patrocinio del método por parte del gerente de proyecto es fundamental así como la definición de sus responsabilidades y su involucración activa en todas las actividades del método según se definen.

Durante esta fase se define un acuerdo de trabajo: “working agreement” para formalizar y asegurar responsabilidades mutuas durante la aplicación del método. El acuerdo de trabajo contiene una definición del alcance de la actividad del método, sus objetivos, su rol, los artefactos que se entregarán y los miembros del equipo que aplicará el método, los roles del equipo (un líder y de 3 a 5 miembros del proveedor de SRE y de 2 a 7 de la organización donde se va a aplicar) y las características que deben tener (años de experiencia, habilidades etc.) , el cronograma de trabajo detallando cuanto tiempo se necesita para cada actividad y un acuerdo de confidencialidad sobre el uso de los datos recogidos de los riesgos. El método propone guías para determinar el criterio de éxito del proyecto, lo que ayudará a dirigir la identificación de los riesgos.

En esta fase se definen los criterios para la exposición de los riesgos, el método propone unos criterios para el impacto y la probabilidad del riesgo, y su exposición se calcula de acuerdo a una matriz definida, pero deja abierto a la personalización y lo considera necesario pues ajusta los criterios al ambiente local del proyecto y el gerente se involucra más en esta actividad y lo siente más suyo al definir sus propios criterios.

Los elementos que se desarrollan en esta fase están bien documentados.

Identificación y Análisis de los Riesgos.

Durante esta fase se licitan e identifican los riesgos mediante entrevistas a los miembros del proyecto, luego se analizan y categorizan en áreas. La fase define 8 actividades: Conducir Resumen del Proyecto (donde el equipo conoce datos del proyecto), Conducir el Resumen de Inicio (donde los miembros del equipo entienden los objetivos del método y las actividades que se estarán realizando), Preparar el Equipo (donde se imparte un pequeño entrenamiento a los miembros del equipo no experimentados en la aplicación de SRE), Conducir Entrevistas (donde se identifican los riesgos), Evaluación de los Participantes, Analizar la Sesión, Consolidación, Resumen de Confirmación de Datos.

El método define un grupo de sesiones de 3 horas de duración donde se identifican definiciones de riesgos documentados de la forma condición-consecuencia.

Para estas entrevistas se aplica el cuestionario del SEI TQB (analizado en la sección anterior de este documento), para las entrevistas se define y describe en detalle un protocolo y el método es estricto en su cumplimiento para lograr mayor efectividad. Se definen roles durante la entrevista y sus actividades (Entrevistador, Entrevistado, Documentador de Riesgos, Documentador de Sesión, Compilador de Datos) así como las estrategias que deben seguir durante la entrevista basados en la cantidad de riesgos encontrados, en las áreas cubiertas y en la calidad de las definiciones.

Luego de que el riesgo sea definido por el entrevistado, este debe evaluarlo y revisarlo hasta que el equipo observe que el entrevistado sienta el riesgo como que él lo creó. Este aspecto humanístico es importante para crear una cultura hacia la Gestión de Riesgos y en especial hacia este método.

Los riesgos son priorizados de acuerdo a su exposición y al criterio de los entrevistados, en este sentido el método no define técnicas “fuertes” para la priorización. Como resultado de esta priorización se obtiene un documento con la lista de riesgos que es entregado al gerente de proyecto.

En la consolidación se reorganizan los riesgos en áreas, se revisan los contextos y se reconcilia la exposición. Este proceso consiste en determinar un promedio entre los criterios de impacto y probabilidad definidos para el riesgo según cada miembro. Esta técnica puede ser efectiva aunque se pudieran utilizar técnicas más precisas por ejemplo una suma ponderada donde se exprese la importancia de un objetivo sobre otro.

En el resumen de confirmación de datos se presentan los datos recogidos a los participantes y los resultados del análisis hecho. El método describe los elementos que debe incluir dicha presentación.

Reporte Interino.

En esta fase se analizan las interrelaciones entre las áreas de riesgos detectadas en la fase anterior. Se realiza un dígrafo de relaciones, se prepara el reporte y se organiza la preparación para la Planeación de la Mitigación.

El dígrafo de relaciones debe ilustrar la magnitud de la dependencia (fuerte, media, débil) y se debe organizar jerárquicamente para determinar las áreas que causan o guían los riesgos y las que como consecuencias de otras se ven afectadas. Este proceso es realizado manualmente por los miembros del equipo.

Luego se prepara el reporte parcial donde se incluye el análisis del dígrafo de relaciones y los elementos realizados hasta el momento.

Planeación de la Estrategia de Mitigación.

Durante esta fase se comienza a desarrollar estrategias de mitigación para los riesgos más importantes definidos. Se prepara el equipo para que tenga las habilidades necesarias para esta fase, y luego se comienzan sesiones para planificar las estrategias de mitigación, el método describe brevemente las actividades a realizar en cada sesión, el tiempo que se debe emplear y los participantes; se deben definir métricas para determinar el progreso de las estrategias de mitigación, el método reconoce la falta de métricas y no propone ninguna a utilizar; durante esta actividad se ofrecen guías para su ejecución.

Una sesión llamada “Cross-Area Strategy” identifica conflictos entre las estrategias para diferentes riesgos que pueden ocurrir cuando las sesiones para planificar las estrategias de mitigación ocurren en paralelo por equipos diferentes.

Luego se hace una presentación formal de los resultados obtenidos, esta presentación muestra al proyecto cómo sus esfuerzos contribuyen al resultado del plan de mitigación en general.

Reporte Final.

En esta fase se realiza una consolidación de todas las fases anteriores. Es una compilación y edición de los datos obtenidos y presentados en forma de reporte. Durante esta fase el método propone la creación de una base de datos con los riesgos obtenidos durante su aplicación, sin embargo no proponen ningún formato o especificación y destacan que la empresa debe decidir cuál base de datos y en qué formato deben guardarse los riesgos.

Este es el principal elemento débil en este método ya para implementar una Gestión de Riesgos continua es importante contar con una base de datos bien estructurada y con riesgos bien definidos y categorizados para un posterior análisis o ayuda en la toma de decisiones.

El Modelo de Hall.

Creado en 1997, el modelo de Hall (49), se ajusta a los procesos definidos por Boehm y el de la IEEE en general. Es un análisis detallado de los procesos involucrados en la Gestión de Riesgos incluye el descubrimiento de la Gestión de Riesgos, los procesos involucrados, la infraestructura necesaria para la Gestión de Riesgos, su implementación, y casos de estudios; detalla el proceso de Gestión de Riesgos desde el punto de vista humanístico principalmente, y hace mucho énfasis en las características de las personas, los procesos la infraestructura y la implementación de la Gestión de Riesgos. Este modelo tiene muy poca documentación pública.

PMBOK®.

El PMBOK®, un cuerpo de conocimiento para la gestión de proyectos y estándar nacional para los Estados Unidos desde 2001 (ANSI/PMI 99-001-2000) propone una guía genérica básica para la gestión de los riesgos que analizaremos a continuación.

Define la Gestión de Riesgos como: el proceso sistemático de identificar, analizar y responder a los riesgos del proyecto, incluye maximizar la probabilidad y consecuencias positivas y minimizar las negativas; y define un riesgo como: un evento o condición que si ocurre, tiene una consecuencia positiva o negativa en los objetivos del proyecto.

Propone una serie de procesos involucrados en la Gestión de Riesgos, con sus entradas y salidas. Es una breve descripción de los mismos donde de manera abstracta se resume sus principales características.

- Planeación de la Gestión de Riesgos.
- Identificación de los riesgos.
- Análisis cualitativo.
- Análisis cuantitativo.
- Planeación de la respuesta a los riesgos.
- Monitoreo y control.

Estos procesos serán analizados en la próxima sección.

Esta edición incluye algunos elementos nuevos respecto a la edición anterior que la hacen más integral:

- Estrategias de respuesta a las oportunidades de los riesgos (explotar, mejorar, aceptar, compartir).
El PMBOK® menciona que los riesgos no son siempre negativos, los riesgos son eventos que pueden o no ocurrir, y de hacerlo tienen un impacto positivo o negativo. Es importante identificarlos todos para poder tomar los riesgos que pueden traer beneficios si se está claro también del impacto negativo que puede provocar y por supuesto, tomar las medidas pertinentes para los negativos. Existen varios trabajos sobre la “oportunidad” de los riesgos positivos como “Software Development Risk: Opportunity, Not Problem” (50).
- Algunas de las relaciones de los procesos de la Gestión de Riesgos con otros procesos de la gestión de proyectos (como el Control Integrado de Cambios), otros elementos (como los factores ambientales de la empresa, bases de datos comerciales, políticas y procedimientos, base de conocimientos), y otras tareas que detalla un poco más.
- Categorización de los riesgos.

A continuación se analizan los procesos definidos por el PMBOK® para la Gestión de Riesgos:

Planeación de la Gestión de Riesgos.

Destaca la importancia de este proceso pues es necesario para que el resto se desarrollen con claridad. Menciona que se deben utilizar los factores ambientales de la empresa (actitudes respecto a los riesgos, tolerancia), las categorías de los riesgos, bases de datos comerciales y de aquí se genera el “plan de Gestión de Riesgos” que incluye la metodología (métodos, herramientas y base de conocimientos) para realizar la Gestión de Riesgos, los roles y las responsabilidades, presupuesto, periodicidad, categorías de los riesgos, matriz de probabilidad e impacto, tolerancia, formato de reporte y seguimiento.

Los elementos más explicados son las categorías de riesgos (a la que se dedica una sección posteriormente en este documento) y la matriz de probabilidad e impacto.

Categorías de riesgos.

La definen como un sistema de desglose de riesgos (Risk Breakdown Structure: RBS, por sus siglas en inglés) que funciona como una estructura que garantiza un proceso uniforme para la identificación de los riesgos y sugiere áreas o fuentes posibles donde identificar riesgos posteriormente. Estas categorías son propias de cada organización y deben revisarse con periodicidad.

Matriz de probabilidad e impacto

Primero se establece una escala para evaluar la probabilidad de ocurrencia de un riesgo y otra para el impacto del mismo. Sugiere utilizar probabilidades numéricas que pueden estar asociadas a descripciones relativas (muy improbable → poco probable → probable → casi certeza, etc.). La escala de impacto refleja su importancia, ya sea negativa o positiva (amenazas u oportunidades respectivamente). También se sugiere utilizar una escala relativa con valores numéricos asociados que pueden ser lineales o no de acuerdo al deseo de evitar o no las amenazas de alto impacto.

Propone una matriz de probabilidad e impacto para priorizar los riesgos de acuerdo a su probabilidad e impacto. Esta matriz se utilizará en el análisis cualitativo de los riesgos. Para cada objetivo del proyecto se establecen rangos de criterios para incluir un valor dado en la escala definida anteriormente.

Identificación de los riesgos.

La identificación es el proceso donde se descubren y documentan las características de los riesgos que influyen en el proyecto.

Se proponen varias técnicas que se pueden usar en este proceso: técnicas de recopilación de información (revisión de documentación, tormenta de ideas, técnica Delphi, entrevistas, identificación de la causa, análisis DAFO), técnicas de diagramación (causa efecto, flujo, influencias).

En este proceso se construye lo que denominan “registro de riesgos” que contiene la lista de los riesgos identificados, posibles respuestas, sus causas y las categorías de riesgos actualizadas.

No definen una estructura para la representación de los riesgos, se deja para la interpretación y posterior implementación de una metodología. Estas técnicas de identificación se describen brevemente, quienes la utilicen deben estudiarlas y elaborar mecanismos para su aplicación.

Análisis cualitativo.

Tiene como objetivo priorizar los riesgos para realizar otras acciones como el Análisis Cuantitativo o Planeación de la Respuesta a los Riesgos. Se evalúan la probabilidad e impacto de cada riesgo con

cada objetivo del proyecto utilizando las escalas definidas anteriormente, también se utiliza una matriz de probabilidad e impacto para ayudar a obtener los riesgos más urgentes (aquellos cuya combinación de probabilidad e impacto sea considerada crítica).

Como resultado de este proceso se actualiza el registro de riesgos.

Proponen una lista diferente y simple para los riesgos de muy poca probabilidad e impacto para tenerlos “a la vista”. Las técnicas más fuertes que se describen es la matriz de probabilidad e impacto con valores y mencionan la necesidad de evaluar la calidad de los datos de los riesgos sin profundizar y proponer alguna técnica o mecanismo.

Análisis cuantitativo.

Este análisis se realiza a los riesgos priorizados en el proceso anterior, analiza el efecto de estos riesgos y les asigna una calificación numérica. Proponen técnicas para cuantificar los posibles resultados del proyecto y sus probabilidades (por concepto de los riesgos identificados), evaluar la probabilidad de cumplir un objetivo, cuantificar el riesgo general del proyecto, identificar objetivos viables por concepto de riesgos.

Denotan que este proceso se hace solo si se considera necesario, también puede omitirse el proceso anterior y pasarse a él directamente, debe repetirse después de la Planeación de la Respuesta a los Riesgos.

Se utiliza la técnica de entrevista para cuantificar la probabilidad y el impacto, distribución de probabilidades, análisis del valor monetario esperado, árbol de decisiones, modelado y simulación. En general estas técnicas pueden ser muy efectivas, el PMBOK® las menciona y aunque en muchos casos se ejemplifican aplicadas a la Gestión de Riesgos no queda claro cómo utilizarlas durante todo el proceso.

Planeación de la respuesta a los riesgos.

Es el proceso donde se planifican acciones a tomar para reducir las amenazas y mejorar las oportunidades. Para los riesgos negativos o las amenazas, proponen las siguientes estrategias para enfrentarlos: evitar, transferir, mitigar; y para los positivos o las oportunidades explotar, compartir, mejorar; también se puede “aceptar” un riesgo o una oportunidad; pero no describen las estrategias en detalles o cómo proceder una vez seleccionada una estrategia en particular. Se diseñan planes de contingencia para en caso que ocurran algunos riesgos, es importante identificar disparadores para ese plan de contingencias y seguirlos de cerca. Tampoco ofrecen guías para confeccionar estos disparadores.

Monitoreo y control.

Es el proceso donde se chequean y controlan los riesgos identificados, se buscan variaciones en su estado y se re-calcula el riesgo general, se asegura que se está actuando de acuerdo a lo planificado en la etapa de Planeación de la Respuesta a los Riesgos, se realizan auditorias a los riesgos, se analizan las variaciones y las tendencias. Sin embargo no define qué atributos monitorear, o qué valores indicarían un estado alterado y qué métricas en general utilizar.

El PMBOK®, como cuerpo de conocimiento al fin, ofrece una guía con los principios básicos para la gestión de riesgo, técnicas genéricas y fundamentos de lo que debe incluir los artefactos generados en cada proceso. Para una entidad hacer Gestión de Riesgos debe elaborar una implementación utilizando los principios y fundamentos delineados.

No detalla los roles que intervienen en la Gestión de Riesgos y sus responsabilidades ni un proceso donde se recojan las memorias finales para un posterior análisis y aprendizaje.

Microsoft Solutions Framework – Risk Management Discipline.

Microsoft Solutions Framework es un marco de trabajo propuesto por Microsoft que cubre el ciclo de vida del proyecto y propone métodos y herramientas para el desarrollo del mismo. Dentro de sus disciplinas proponen “Risk management discipline” (22), como un mecanismo para enfrentar la incertidumbre en los proyectos, proponen un enfoque proactivo donde continuamente se evalúen los riesgos.

Se basa en los principios fundamentales de MSF en general y además la Gestión de Riesgos específicamente, hace énfasis en el principio de “mantenerse ágil, esperar el cambio”: este principio no contradice el mantenerse proactivo, se refiere a que cuando se espera que las cosas pueden cambiar, se está más abierto a identificar elementos que pueden hacer que las cosas cambien, y actuar antes de que ocurran.

El principio de las comunicaciones abiertas, es fundamental y al igual que otros modelos, MSF⁶ enfatiza la necesidad de que participen tanto el equipo de desarrollo como los interesados claves en un ambiente sincero de comunicación.

El principio de “aprender de todas las experiencias” ofrece un punto de retroalimentación a su disciplina; consiste en aumentar el conocimiento a través de un análisis para en futuros proyectos disminuir la incertidumbre sobre algunas situaciones y contribuir a la toma de mejores decisiones en general.

⁶ En lo adelante MSF hace referencia a “MSF Risk Management Discipline”, cuando los términos estén juntos sí se diferenciarán.

El último principio es la “responsabilidad compartida”, a diferencia de otros modelos o tendencias (51) MSF propone que nadie es dueño de un riesgo. Todos en el equipo son responsables por activamente participar en la Gestión de Riesgos (no quiere esto decir que alguien modere y controle este proceso).

Planeación.

Esta etapa tiene el mismo objetivo que lo definido en otros modelos, MSF propone una serie de preguntas que ayudan a determinar qué debe incluir el plan de Gestión de Riesgos.

No proponen un formato o una herramienta (como acostumbra Microsoft). Conciben este proceso como fuera del ciclo, es decir, de aquí en adelante comienzan cíclicamente los otros procesos de gestión de riesgo.

MSF define 6 procesos para la Gestión de Riesgos:

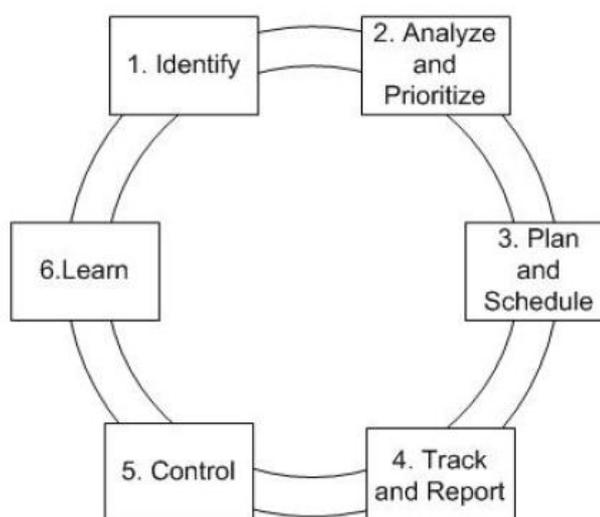


Figura 6. Procesos de la Gestión de Riesgos de MSF. Imagen tomada de (22).

Identificación.

El objetivo de este proceso es la identificación de los riesgos que el equipo presenta y la obtención de una lista de riesgos, bien definidos, concisos; este proceso se nutre del conocimiento que se tenga sobre riesgos anteriores ya que ayuda en la detección de riesgos, en determinar sus propiedades. Proponen que se utilicen métodos que ayuden a la identificación como el Taxonomy-Based del SEI (39) o listas de chequeo como (52).

Para la realización de este proceso proponen como actividad fundamental encuentros estilo taller donde se obtenga la definición de los riesgos. Destacan que muchos grupos de trabajo realizan esta actividad satisfactoriamente una sola vez, y la calidad de la Gestión de Riesgos depende en gran medida de la sistematicidad de este proceso, dicha sistematicidad debe definirse y proponen 3

enfoques para ello: guiado por tiempo (diario, semanal, mensual), guiado por hitos (asociado a algún hito planificado del proyecto) o guiado por eventos (eventos que indicarán la necesidad de realizar una identificación de los riesgos).

Para MSF es muy importante la clasificación de los riesgos pues provee un mecanismo para su estandarización a través de la empresa y para su inclusión en bases de conocimiento que pueden ayudar a la industria a indexar nuevas contribuciones.

MSF propone una taxonomía o categorías de riesgos, aunque se puede utilizar otras conocidas como (39).

Como salida a este proceso se tiene una lista de definiciones de los riesgos. Su forma de representarlos es mediante una descripción textual que incluya los siguientes elementos:

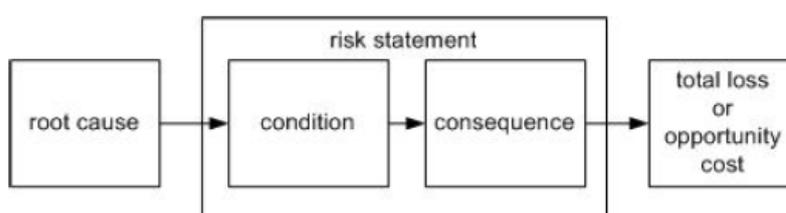


Figura 7. Definición del riesgo de MSF. Imagen tomada de (22).

Esta es una representación conceptual y general del riesgo que define su estructura y sirve de guía a la hora de escribir la definición del riesgo. Como forma de representación del riesgo es suficiente en esta etapa, pero se pudieran incorporar más elementos que se descubren durante esta etapa.

Análisis y priorización.

La intención de este proceso es convertir los datos del riesgo en un formulario utilizable en la toma de decisiones, y priorizar los riesgos obteniendo un ranking para centrarse posteriormente en los más altos riesgos.

Durante esta etapa se analiza la probabilidad del riesgo, para ello MSF define una escala con valores probabilísticos, verbales y numéricos para utilizar:

Probability range	Probability value used for calculations	Natural language expression	Numeric score
1% through 33%	17%	Low	1
34% through 67%	50%	Medium	2
68% through 99%	84%	High	3

Figura 8. Probabilidad de ocurrencia de los riesgos. Tomado de (22).

En la tabla anterior se ofrecen 3 posibilidades pero también proponen uno de 7. En este proceso de análisis, la determinación más correcta posible de la probabilidad de ocurrencia dará al traste con una Gestión de Riesgos “efectiva”.

La asignación de valores numéricos es un aspecto importante pues calculan la exposición del riesgo a partir de estos valores como se verá posteriormente. Respecto a otros modelos, la asignación de valores numéricos es un aspecto positivo en MSF.

También en este proceso se determina el impacto del riesgo, es decir la magnitud de la pérdida o la ganancia para determinados objetivos. MSF también propone una escala de valores para identificar la magnitud en cuanto a costo y tiempo.

Score	Monetary Loss
1	Under \$100
2	\$100-\$1000
3	\$1000-\$10,000
4	\$10,000-\$100,000
5	\$100,000-\$1,000,000
6	\$1,000,000-\$10 million
7	\$10 million-\$100 million
8	\$100 million - \$1 billion
9	\$1 billion - \$10 billion
10	Over \$10 billion

Figura 9. Impacto esperado en el costo. Tomado de (22).

A cada valor de la escala se le asignan valores numéricos lineales, no utilizan ninguna otra “función” lo que indicaría el grado de aceptación de los valores y puede resultar interesante en el análisis de los riesgos.

MSF incluye un elemento interesante: la exposición del riesgo.

La exposición de un riesgo es una medida de su amenaza. Y se define una función para calcular la exposición dependiendo del grado de aceptación de la entidad. MSF propone una forma de calcularla y destaca que la utilización de una matriz (probabilidad x impacto) ayuda a los “decision-makers” pues se puede hacer una escala de colores para ilustrar las exposiciones altas o bajas.

Probability impact	Low = 1	Medium = 2	High = 3
High = 3	3	6	9
Medium = 2	2	4	6
Low = 1	1	2	3

Low exposure = 1 or 2 Medium exposure = 3 or 4 High exposure = 6 or 9

Figura 10. Matriz de probabilidad e impacto. Tomado de (22).

Los riesgos se deben ordenar por la exposición, y adicionalmente plantean una fórmula para que determinadas propiedades de los riesgos influyan en su posición del Rank en mayor o menor medida:

$$\text{Ranking value} = 0.5(\text{probability} \times \text{impact}) - 0.2(\text{when needed}) + 0.3 (\text{control cost} \times \text{probability control will work}).$$

Figura 11. Fórmula para calcular la exposición. Tomado de (22).

Como resultado de este proceso se obtiene la lista que contiene los riesgos con los atributos primarios identificados y evaluados. Adicionalmente definen otros métodos y otra representación de los riesgos en esta etapa como muestra la Figura 12.

Item	Purpose	Status
Risk Statement	Clearly articulate a risk	Required
Probability	Quantify likelihood of occurrence	Required
Impact	Quantify severity of loss or magnitude of opportunity cost	Required
Ranking criterion	Single measure of importance	Required
Priority (rank)	Prioritize actions	Required
Owner	Ensure follow through on risk action plans	Required
Mitigation Plan	Describe preventative measures	Required
Contingency plan and triggers	Describe corrective measures	Required
Root cause	Guide effective intervention planning	Optional
Downstream effect	Ensure appropriate impact estimates	Optional
Context	Document background information to capture intent of team in surfacing risk	Optional
Time to implementation	Capture importance that risk controls be implemented within a certain timeframe	Optional

Figura 12. Representación del riesgo. Tomado de (22).

Esta representación de los riesgos es una de las más completas encontradas ya que recoge varios atributos de los riesgos en una estructura única y entendible.

Adicionalmente proponen que se mantenga una lista pequeña con los riesgos más altos, la intención de esta lista no es otra que mantener un registro de las altas amenazas.

Aunque no lo describen en su representación del riesgo, MSF define un estado que puede tener (desactivado) que son aquellos riesgos que se decide que su gestión no merita la pena, no se define ningún criterio o métrica para esta decisión.

Planeación de la respuesta a los riesgos.

Durante este proceso se toman los riesgos priorizados y se deciden planes de actividades a realizar. Proponen varias estrategias a seguir para un riesgo: Investigar, Aceptar, Evitar, Transferir, Mitigar, Contingencia. En este sentido el modelo tiene algunas variaciones respecto a otros al incluir la contingencia como una estrategia alternativa a diferencia de un atributo siempre presente en el riesgo. El modelo no ofrece estrategias para las oportunidades durante este proceso.

Durante esta fase también definen la forma de controlar las actividades de planeación, estas actividades son incluidas en los elementos de control del proyecto (plan de actividades del proyecto por ejemplo) y además se recogen en un formulario que contiene la identificación del riesgo, y todas las propiedades de planeación: (estrategia de mitigación, métricas, contingencia, disparadores, responsable). En cuanto a las métricas, el modelo no define ninguna, estas deben ser implementadas por el equipo de desarrollo que implemente el plan, es el elemento más débil en los modelos en general.

Seguimiento y Reporte.

El objetivo del seguimiento y reporte es recoger información sobre los riesgos existentes utilizando las métricas definidas monitoreando así el estado del riesgo. Se debe recoger un estado del riesgo y confeccionar un reporte cuyo formato es un estándar para el proyecto u organización. El modelo no define un reporte formal sin embargo menciona los elementos que debe tener (sin considerar las métricas como se observó anteriormente).

MSF concibe el seguimiento y reporte como un proceso al mismo nivel de los anteriores dado la claridad de su objetivo y las salidas que proporciona. Es un proceso que puede tener algún rol o responsabilidad específica asignada y que se ejecuta independientemente del resto de los procesos.

Control.

Para MSF el control de los riesgos consiste en las actividades llevadas a cabo por el equipo al alcanzar algún disparador en un riesgo determinado, es decir, ejecutar los planes de contingencia para un riesgo.

Este proceso está poco definido, debido en parte a la naturaleza de su definición de “control”.

Aprendizaje.

MSF define un proceso importante en la Gestión de Riesgos: el aprendizaje. Destacan la necesidad de contar con una base de datos de riesgos, y al concluir cada proyecto se actualice con los nuevos riesgos identificados o las nuevas categorías (fuentes de riesgos), y los comportamientos en los riesgos, su frecuencia de aparición, pero no definen un formato o estructura que debe tener.

Conciben como un elemento importante a aprender y documentar, las lecciones aprendidas que generalmente son los planes de mitigación exitosos. Estos elementos deben documentarse y guardarse en la entidad para futuros proyectos.

Adicionalmente de este proceso surgen recomendaciones para cambiar la política de Gestión de Riesgos, este es un elemento de análisis y retroalimentación importante y que pocos modelos incluyen.

En general la concepción de este proceso es útil para la Gestión de Riesgos en general, no obstante falta definición y estructura de los elementos a generar y almacenar.

Estándares, Normas y Certificaciones

Para la Gestión de Riesgos existen estándares, al incluir el PMBOK® la Gestión de Riesgos como una de sus áreas, y ser el PMBOK® estándar ANSI, su guía para la Gestión de Riesgos se convierte en un estándar. Varios países definen sus estándares para la Gestión de Riesgos como el estándar australiano (53) y otros.

La IEEE definió un estándar para la Gestión de Riesgos: 1540-2001 (54), y también ISO posee un estándar: (55), las especificaciones de ambos estándares se compran directamente del sitio de estas dos entidades.

Las certificaciones en materia de Gestión de Riesgos se encuentran embebidas dentro de otras certificaciones de gestión de proyectos como PMP.

Gestión de Riesgos en la Universidad de las Ciencias Informáticas.

La Gestión de Riesgos en la Universidad de las Ciencias Informáticas (UCI) tiene documentos oficiales para algunos de sus elementos: el “Manual de Procedimientos para el Diagnóstico de Riesgos” (19).

En este manual se implementa la Resolución 297/03 del MFP, definiendo los pasos, roles y responsabilidades para elaborar un “diagnostico de riesgos”; este es el término que representaría la Gestión de Riesgos.

El procedimiento se centra en el diagnóstico de riesgos para áreas en la universidad que pueden traer un impacto negativo para los objetivos de dichas áreas; no se tienen en cuenta los riesgos que traen impactos positivos (las oportunidades).

Define 3 atributos para los riesgos solamente: frecuencia, impacto, acciones administrativas. Para la frecuencia e impacto no se definen técnicas para su identificación o cálculo, en cambio se propone el uso de las técnicas definidas en el Programa de Preparación Económica para los Cuadros en materia de Control Interno. Se define una clasificación para el riesgo (interno o externo) pero no se tienen otras categorías o taxonomía donde se oriente en las fuentes de riesgos.

El método define: el orden de los pasos lógicos a seguir para realizar el diagnóstico, donde explican a gran escala los involucrados y sus responsabilidades, pero no detallan cómo proceder; y los 3 modelos a emplear: “Evaluación de los Riesgos”, “Anexo para Evidenciar las Acciones Administrativas” y el “Plan de Prevención para el Control Interno”. De estos documentos se define el formato, alcance y responsable de confeccionarlo.

El procedimiento no se ajusta a proyectos productivos de software donde se requiere un mayor nivel de detalle y clasificación en los riesgos, así como técnicas objetivas y precisas para su análisis y posterior mitigación, y el uso de las oportunidades para lograr más valor en el proyecto, la gestión del conocimiento adquirido de los riesgos. Para dichos proyectos dentro de los documentos definidos en el expediente de proyecto se destinan 2 a la Gestión de Riesgos: “Lista de Riesgos” y “Plan de Mitigación”.

El plan de mitigación recoge una lista de riesgos especificando su tipo (Tecnológico, Personal, Organización, Herramientas, Requerimientos, Estimación), una descripción del propio riesgo y de su impacto, la probabilidad de ocurrencia (Alta, Media, Baja, Muy alta) y los efectos (Catastrófico, Serias, Tolerable, Insignificante), no se asocian valores a estas clasificaciones o guías para ayudar en su determinación.

Para cada riesgo se debe describir cómo monitorearlo, la estrategia de mitigación a seguir y el plan de contingencias. Esta descripción textual contiene elementos principales de los riesgos, sin embargo se carece de explicación o guía en este.

El documento recoge en una tabla los identificadores de los riesgos, probabilidad, impacto, mitigación, monitoreo y administración; dicha tabla se ordena por probabilidad e impacto y luego se debe describir las tareas que se llevarán a cabo para gestionarlos: qué estrategia se utilizará para identificarlo y cómo será analizado y priorizado. Estos elementos deben ser herramientas con que cuentan quienes implementen la Gestión de Riesgos. Se deben describir las estrategias a seguir para máximo 10 riesgos (mitigación, evasión, y/o prevención), en este sentido la cantidad de riesgos a decidir su estrategia es arbitraria, cuestión que atenta contra la eficacia de la Gestión de Riesgos, las posibles estrategias no contemplan la explotación de una oportunidad.

Se deben describir otras tareas: cómo se hará el seguimiento a cada riesgo, las actividades de mitigación, el cronograma de revisión y reporte de los riesgos, este último elemento es significativo ya que contribuye a la periodicidad formal de la Gestión de Riesgos sin embargo no concibe formalmente una identificación periódica de los riesgos.

En el plan de mitigación se recoge además las personas responsables involucradas en la Gestión de Riesgos, el presupuesto, las herramientas y técnicas a utilizar.

En sentido general estos documentos contienen los principales elementos de la Gestión de Riesgos, sin embargo es difícil su objetiva utilización por falta de guías y no quedan concretos o están ausentes elementos como categorías de los riesgos, métricas a utilizar en su monitorización y gestión del conocimiento obtenido durante la Gestión de Riesgos.

Conclusiones del Estudio del Estado del Arte

La Gestión de Riesgos tiene varios elementos que cubren casi toda la pirámide de la profesión gestión de proyectos. Generalmente los modelos giran en torno a un conjunto de principios básicos que guían las actividades de la Gestión de Riesgos y en muchos casos estos principios se centran en elementos humanísticos.

Los modelos están basados en los procesos definidos al inicio de la Gestión de Riesgos para los proyectos de software: Planeación, Identificación, Análisis, Planeación de la Respuesta, Control y Seguimiento⁷; y sobre esta línea se han incluido nuevos procesos como el aprendizaje o se ha dividido el análisis en análisis cuantitativo y análisis cualitativo. Los modelos tienen deficiencias para ser aplicados a la universidad al definir la comunicación entre los procesos de acuerdo a su secuencia, simultaneidad y roles involucrados. La descripción de los procesos es generalmente aceptable pero necesita ser personalizada a las condiciones locales de quienes utilicen los modelos detallando las características locales evitando ambigüedad y confusión.

Las técnicas propuestas por los diferentes modelos son generalmente descripciones generales y aunque muchas tienen buen soporte matemático o científico, carecen de explicación objetiva de cómo utilizarlas y cómo sus resultados se integran con la Gestión de Riesgos en general. Algunas técnicas como el Taxonomy Based tienen muy bien detallada su fundamentación y el proceso de aplicación y evaluación aunque necesita personalización y extensión para ser aplicable en nuestro entorno.

La generalidad de los modelos definen roles muy genéricos o no lo definen, el trabajo que más define roles, sus responsabilidades y actividades es Software Risk Evaluation Method.

Los modelos tienen una representación textual del riesgo. Las propiedades de los riesgos varían de un modelo a otro pero siempre definen impacto y probabilidad; no todos los modelos categorizan los riesgos de acuerdo a un sistema de categorías bien estructurado ni se establecen valores objetivos para sus propiedades o la forma de personalizar y extender estos valores. La representación de los riesgos en general es una de las deficiencias principales de los modelos pues no permite un aprovechamiento de dicha representación para lograr un control íntegro del riesgo y conocimiento de su estado en todo momento.

En general se mencionan genéricamente los artefactos que se generan y utilizan en la Gestión de Riesgos, pocos modelos proponen formato y descripción a estos artefactos.

Las oportunidades son gestionadas en pocos modelos y no se define bien un mecanismo donde quede claro que se podrá obtener valor de ellas, o se controle su evolución y se detecten áreas de posibles ingresos.

Los modelos carecen de una definición de un proceso de resumen de la Gestión de Riesgos, donde se analice el proceso, se evalúe, se obtengan métricas y de un proceso de aprendizaje, donde las salidas

⁷ Estos procesos se generalizan de varios modelos de acuerdo a su intención y objetivo, en cada modelo en particular puede que tengan nombres diferentes.

de este resumen, se archiven y tengan un formato tal, que pueda ser objetivamente utilizable en futuros proyectos.

Todos los modelos tienen deficiencias en las métricas para el control y seguimiento de los riesgos para ser aplicados a nuestro entorno.

La documentación pública de los modelos varía de acuerdo a su intención y fabricante: los modelos del SEI, PMI, Microsoft tienen documentación pública utilizable al contrario del resto de los modelos y en especial las normas y certificaciones.

Por todo lo anterior se concluye que los modelos existentes tienen deficiencias para aplicarse en nuestro sistema productivo, que existen varios métodos y técnicas positivas que necesitan adaptación para su uso adecuado. Por lo que proponemos el siguiente modelo como integración, extensión, personalización y ampliación de varios de los modelos existentes para ser aplicado en los proyectos productivos de la universidad.

Capítulo 2: Identificación y Análisis

El siguiente modelo se basa en trabajos analizados en el Capítulo 1, especialmente PMBOK®, “Taxonomy Based Risk Identification”, “Software Risk Evaluation” y “Microsoft Solution Framework – Risk Management Discipline”. Tiene en cuenta la situación actual de la UCI, problemática existente y experiencias en la Gestión de Riesgos. Define prescriptivamente varios criterios basados en la experiencia de algunos expertos.

El modelo propone los procesos, actividades y técnicas a realizar. Durante la descripción de los procesos se mantiene una estructura coherente comenzando con una representación de los roles que intervienen, sus entradas y salidas. Posteriormente se muestra el flujo de trabajo del proceso explicando su contenido y representándolo con un diagrama de actividades UML. Para cada actividad se representa el tiempo aproximado de ejecución, y si es relevante, los participantes, entradas y salidas. Cada actividad tiene posibles técnicas para su ejecución que se explican de forma tal que oriente al interesado para su aplicación.

El modelo se divide en dos grupos de procesos fundamentales, aquellos destinados al descubrimiento y evaluación de los riesgos, y aquellos destinados al control. El primer grupo se compone de los procesos de Identificación, Análisis Cualitativo y Análisis Cuantitativo y el segundo de los procesos planeación de la respuesta, monitoreo y control, evaluación y aprendizaje. El proceso de planificación queda fuera de estos grupos, es un proceso organizativo al inicio del proyecto. A continuación se aborda la descripción de los procesos del primer grupo y en el siguiente capítulo los del segundo grupo.

Alcance del Modelo

Este modelo es aplicable a proyectos de producción de software desarrollados en la Universidad de Ciencias Informáticas que deseen implementar una Gestión de Riesgos periódica con el objetivo de identificar y estudiar los riesgos, de disminuir las amenazas y aumentar las oportunidades.

El modelo ofrece descripción y guía objetiva para la realización de los procesos involucrados en la Gestión de Riesgos: Planeación, Identificación, Análisis Cualitativo, Análisis Cuantitativo, Planeación de la Respuesta, Monitoreo y Control, Evaluación y Aprendizaje especificando sus entradas, salidas, participantes, descripción del flujo de trabajo y las actividades que se realizan durante su ejecución. Define métodos y técnicas a aplicar para dicha realización, describe y da formato a los documentos utilizados en la Gestión de Riesgos. Cubre los procesos de gestión durante todo el ciclo de vida del proyecto. Es utilizado por todo el personal involucrado.

Principios.

El modelo se basa en 4 principios fundamentales para garantizar su adecuado funcionamiento, principios que se refuerzan a través del modelo y a los que tributan todos los procesos y actividades a lo largo de la Gestión de Riesgos de una forma u otra:

Todo el personal involucrado en la Gestión de Riesgos: el modelo concibe a todo el personal involucrado en la Gestión de Riesgos, todos son responsables por su correcta aplicación. Existen roles dentro de la Gestión de Riesgos, equipos encargados de una u otras tareas pero todos en el proyecto son responsables de ejecutar, completar y reportar las actividades asignadas, hacerlo de manera consciente, efectiva y en tiempo. Para que la Gestión de Riesgos sea efectiva no puede ser tarea de unos pocos dentro del equipo, es el proceso cooperativo y sincero de todos los involucrados en el desarrollo del producto.

Enfoque a la mejora continua: el modelo orienta sus actividades con una perspectiva de mejorar continuamente su aplicación, sus procesos y técnicas. El principal elemento que contribuye a la mejora es el aprendizaje. El modelo asume que un aprendizaje continuo, que cubra todas sus áreas y trascienda de proyecto a proyecto. Este es un factor importante para la mejora continua de la Gestión de Riesgos, su aplicación efectiva y el éxito en general para la universidad.

Alto compromiso de la dirección del proyecto: el modelo destaca el compromiso de los directivos del proyecto con la Gestión de Riesgos en el sentido de lograr apoyo y soporte en todas sus actividades; entendimiento pleno de su necesidad, sus beneficios e importancia; para de esta forma lograr una representación en la dirección del proyecto y su ánimo de reforzar, controlar, y velar por estas actividades para que la Gestión de Riesgos fluya en todas las dimensiones del proyecto. La dirección del proyecto debe entender que el principal beneficiado de este proceso serán ellos mismos.

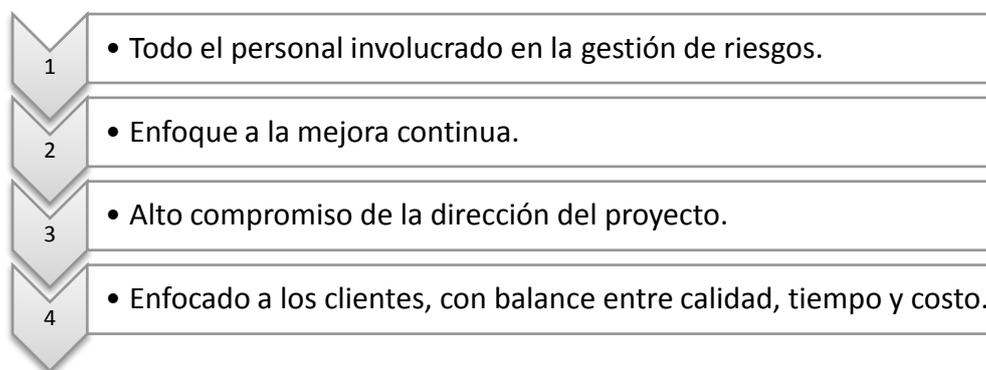


Figura 13. Principios del Modelo.

Enfocado a los clientes, con balance entre calidad, tiempo y costo: con su aplicación, el modelo se centra en obtener beneficio visible para los clientes (quienes deben participar activamente en la

Gestión de Riesgos en cumplimiento al principio 1) para lograr su mayor involucración en este proceso y la intención de realizar las actividades que le correspondan con la mayor exactitud. A la vez, mantienen un equilibrio con la calidad, tiempo y costo para lograr un efecto similar en todas las partes involucradas en el proyecto.

Estos principios sientan las bases del modelo definiendo en cierta forma sus objetivos. El modelo vela por el ajuste y cumplimiento de estos principios en sus elementos.

Premisas para su aplicación.

Las siguientes premisas son cruciales para una aplicación efectiva del modelo:

Recursos humanos con la responsabilidad asignada a la Gestión de Riesgos: para la correcta aplicación de este modelo el proyecto debe asignar explícitamente responsabilidades a los recursos humanos con la Gestión de Riesgos independientemente que todos tengan responsabilidad hacia la Gestión de Riesgos, y dicha responsabilidad se comparta; pues es crucial para lograr un compromiso mayor y organizado hacia el cumplimiento de las actividades.

Justificación de la involucración de la dirección del proyecto en la Gestión de Riesgos al tomar la decisión de incluir el plan de Gestión de Riesgos en el plan de proyecto: el elemento más significativo que denota la involucración activa de la dirección del proyecto con la Gestión de Riesgos es la inclusión del plan de Gestión de Riesgos en el plan de proyecto, así como las tareas generadas durante la Gestión de Riesgos en los planes y mecanismos de planificación y control del proyecto. Esta inclusión asegura una vinculación con el resto de los procesos de organizativos, de control y de desarrollo del proyecto.

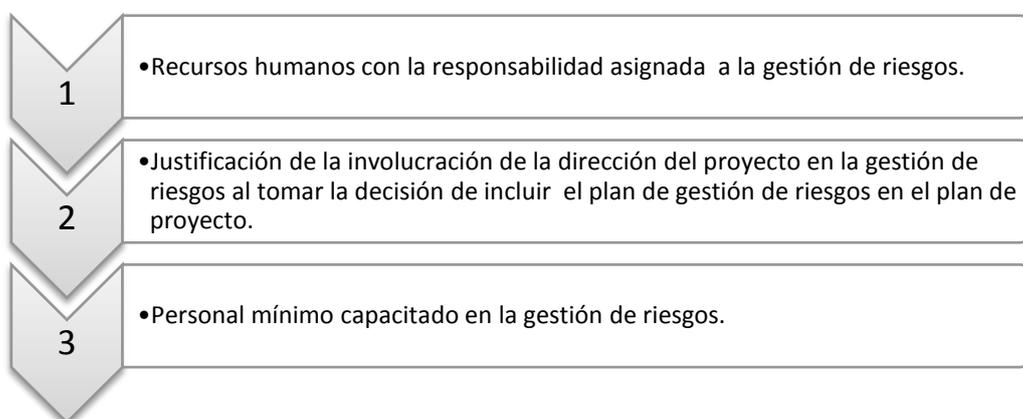


Figura 14. Premisas del Modelo.

Personal mínimo capacitado en la Gestión de Riesgos: es necesario 2 niveles de capacitación en materia de Gestión de Riesgos. Nivel 1: todo el personal del proyecto debe entender los principios de la Gestión de Riesgos, conocer en general los procesos de Gestión de Riesgos y el papel que jugará cada cual. Nivel 2: el grupo de Gestión de Riesgos debe conocer en detalle y profundidad el modelo de Gestión de Riesgos, debe utilizarse para ello un curso de capacitación como se recomienda en la sección Recomendaciones. La preparación del personal en la Gestión de Riesgos ayudará significativamente a su correcta y rápida aplicación.

Representación del modelo

Para la realización de la Gestión de Riesgos, el modelo propone los procesos de Planeación, Identificación, Análisis Cualitativo, Análisis Cuantitativo, Planeación de la Respuesta, Monitoreo y Control, Evaluación y Aprendizaje. Durante la instrumentación de cada proceso se describe su objetivo, fundamentos, actividades principales y las técnicas para desarrollarlas. El modelo propone un conjunto de artefactos y roles encargados de la ejecución de los procesos que se documenta en la instrumentación de cada proceso.

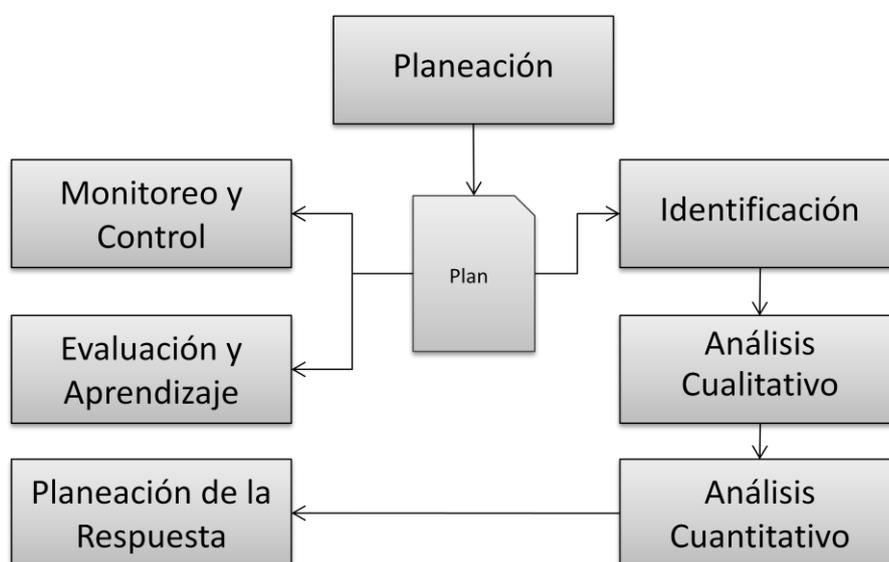


Figura 15. Flujo de ejecución más común de los procesos de la Gestión de Riesgos.

La Figura 15 representa el flujo de ejecución más común de los procesos propuestos para la Gestión de Riesgos y los elementos que disparan su ejecución. Esta figura se puede utilizar para representar gráficamente al modelo ya que contiene los procesos definidos, su flujo principal y el elemento rector de la Gestión de Riesgos: el plan de gestión de riesgos. Durante la planeación se genera el plan de Gestión de Riesgos que define los puntos de ejecución de la Identificación, el Monitoreo y Control y la Evaluación y Aprendizaje. Siempre posterior a la Identificación se realiza el Análisis Cualitativo y

posterior a este el Análisis Cuantitativo. Generalmente se realiza una Planeación de la Respuesta posterior al Análisis Cuantitativo.

El resto de los artefactos generados durante los procesos no se muestran en esta figura, se describen a lo largo del documento y se resumen en la sección Artefactos (*ver página 83*).

La Figura 16 muestra el grado de actividad de los procesos de la Gestión de Riesgos durante el ciclo de vida del proyecto. Esta representación integrada de los procesos con la gestión de proyectos en general es útil para decidir cuándo iniciar cada proceso. Los datos utilizados para la elaboración de la imagen no son empíricos, se basan en las apreciaciones de experiencias en la Gestión de Riesgos.

El proceso de Planificación tiene actividad durante el inicio del proyecto. El proceso de Identificación tiene gran actividad en los inicios, y posteriormente disminuye y se estabiliza, generalmente se realiza la identificación después de cada hito significativo del proyecto. El Análisis Cualitativo se comporta similar a la identificación puesto que la sigue en orden lógico. En Análisis Cuantitativo sigue al cualitativo pero en ocasiones se realiza para evaluar el estado de los riesgos. La Planificación de la Respuesta se ejecuta generalmente después del Análisis Cuantitativo. El Monitoreo y Control es una actividad constante durante las etapas medias del proyecto. La Evaluación y Aprendizaje se realiza al concluir el proyecto.

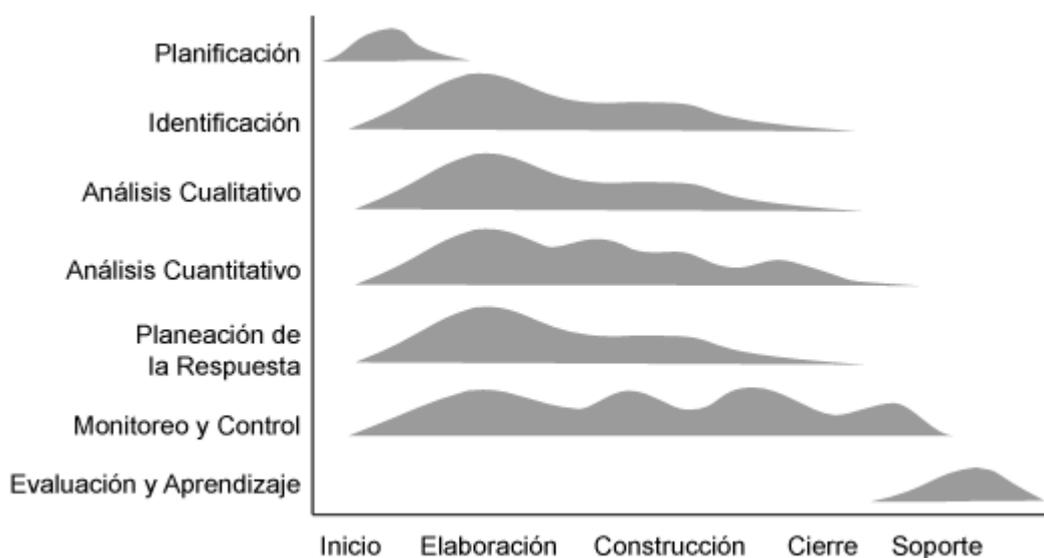


Figura 16. Actividad de la Gestión de Riesgos en cada fase del proyecto.

Representación de los riesgos.

La comunicación de los riesgos a través de los procesos debe ser efectiva, los riesgos deben estar representados de tal forma que dicha representación sea entendible, usable, y práctica, para contribuir a su efectividad y conocer más datos sobre el riesgo.

Antes de describir los procesos y actividades es importante proponer una representación de los riesgos, la siguiente es definida por los autores basándose en trabajos analizados en el capítulo 1 (ver página 8) y “Common Elements of Risk” (56), “A Construct for Describing Software Development Risks” (57), “Nine Best Practices. *The Software Management Framework*” (58).

Proponemos una representación vectorial del riesgo que incluye propiedades claves para su uso adecuado por todos los procesos de la Gestión de Riesgos, y que sea fácil de representar computacionalmente, contribuya al análisis y las búsquedas.



Figura 17. Representación del riesgo.

Las propiedades del vector se describen a continuación.

ID: identificador único del riesgo, debe ser único dentro de la universidad, debe ser una cadena de caracteres donde los dos primeros identifiquen la entidad⁸, los tres siguientes el proyecto, y luego enteros consecutivos, por ejemplo: 03COE15. Los riesgos siempre presentes, o riesgos comunes deben tener los primeros indicadores y cuando un riesgo se decida incluir como riesgo siempre presente, debe cambiarse el indicador del proyecto por GLB, para indicar que es un riesgo global.

Etapa: etapa del proyecto donde se manifiesta el riesgo. (Inicio, Elaboración, Construcción, Cierre, Soporte).

Estado: uno de estos valores: identificado, analizado, activo, cerrado, reabierto.

Prioridad: orden de prioridad para atender este riesgo. Es un valor numérico diferente para cada riesgo indicando su prioridad, 0 muy priorizado, > 0 menos priorizado.

Categoría: identificador de la categoría (una de las definidas por el modelo, ver Anexo2 – Taxonomía del Desarrollo de Software Página 99).

Entrevistado: persona que identificó el riesgo.

Evento: descripción textual del suceso incierto que causa preocupación. No debe ser ambiguo, debe ser corto pero no debe limitarse su descripción por acortarlo. El evento es descrito en futuro.

Consecuencia: descripción textual de las consecuencias que trae la ocurrencia del evento. Debe expresar claramente el impacto sobre los objetivos del proyecto, no tiene por qué ser sobre todos los objetivos, en otra propiedad del riesgo se cuantificará y valorará este impacto.

Nota: estas dos propiedades: evento y consecuencia, al leerlas debe tener sentido, el riesgo será enunciado utilizando estas palabras.

⁸ Puede ser facultad, polo productivo, etc.

Causa: descripción textual de la causa que origina el riesgo. Es importante que sea precisa, descriptiva y objetiva. Es escrito en presente.

Probabilidad: valor numérico indicando la probabilidad de ocurrencia. Este valor es uno de los definidos en el plan de Gestión de Riesgos.

Impacto: valor de impacto para cada objetivo de proyecto, de acuerdo a lo definido en plan de Gestión de Riesgos.

Frecuencia: el factor de aparición del riesgo en el tiempo de proyecto. Expresa un valor porcentual respecto al tiempo total del proyecto indicando con qué frecuencia aparece este riesgo.

Certidumbre de la Información: valor que indica cuán seguro se está de la información obtenida sobre el riesgo.

Marco de tiempo: tiempo mínimo en el que debe ejecutarse los planes de contingencia o explotación para este riesgo, debe expresarse en la unidad de medida acordada en el plan de Gestión de Riesgos.

Estrategia de respuesta: estrategia utilizada para mitigar el riesgo.

Riesgos Relacionados: una lista de otros riesgos relacionados cuya causa o evento esté muy influenciada por este riesgo.

Observaciones: notas importantes sobre el riesgo, su historial.

Primer Grupo de Procesos.

Planeación.



- Líder de Proyecto.
- Asesor de calidad.
- Encargado de recursos humanos.
- Económico.
- Planificador.



- Plan de Gestión de Riesgos
(ver página 98).

Flujo de Trabajo.

Comienza durante la etapa de inicio del proyecto, decide su comienzo el líder de proyecto. Este proceso se ejecuta una sola vez durante el ciclo de vida del proyecto. Durante el proceso de planeación se deciden los elementos que guiarán la Gestión de Riesgos durante toda su aplicación. Recoge las técnicas y notaciones a utilizar y rige sus rangos de valores. El plan de riesgo se incluye en

el plan de proyecto y el líder de proyecto es encargado de controlar su correcto uso. Este proceso genera el Plan de Gestión de Riesgos, el cual es actualizable durante el proyecto.

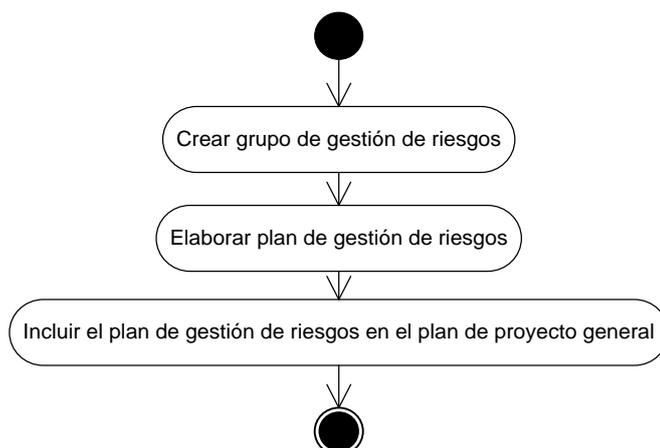


Figura 18. Flujo de trabajo de Planeación.

Actividades.

1 - Creación del grupo de Gestión de Riesgos.



15 minutos



- Líder de proyecto.
- Encargado de recursos humanos

Esta es la primera actividad durante la planeación. Aquí se conforma el grupo de personas que organizarán y ejecutarán las actividades principales de la Gestión de Riesgos. Siempre debe denominarse “grupo de Gestión de Riesgos” y no “equipo”; es importante destacar que la Gestión de Riesgos es responsabilidad de todo el personal, por tanto, denotándolo como equipo daría un grado de aislamiento del resto del equipo de proyecto. El proyecto tiene que verse como un equipo, el grupo de Gestión de Riesgos es un conjunto de personas que sesionan juntas para determinadas actividades en función del equipo de proyecto.

El grupo de Gestión de Riesgos tiene 7 o 9 miembros además del organizador, se organizan en pequeños grupos de acuerdo a la naturaleza de las actividades a realizar. Un miembro puede pertenecer a varios grupos.

Organizador: 1 persona. Encargado de liderar los procesos y actividades⁹. Debe tener habilidades de moderación y liderazgo.

⁹ Más adelante se describen las responsabilidades y tareas de cada rol en cada actividad.

Grupo de Identificación: 5 o 7 personas. Encargados de ejecutar las actividades del proceso de identificación. Deben tener habilidades de facilitación y comunicación.

Grupo de análisis: 7 o 9 personas. Encargados de ejecutar las actividades de los procesos Análisis Cualitativo, Análisis Cuantitativo y Evaluación y Aprendizaje.

Grupo de Monitoreo y Control: 3 o 5 personas. Encargados de las actividades del proceso Monitoreo y Control.

Operaciones: 1 persona. Encargada de las tareas de soporte y aseguramiento de las actividades de la Gestión de Riesgos. Sus responsabilidades varían de acuerdo a las necesidades específicas durante la ejecución de las actividades.

El grupo de Gestión de Riesgos se documenta en el “Plan de Gestión de Riesgos” del proyecto, (ver página 98) en la sección “Grupo de Gestión de Riesgos”.

2 – Elaboración del plan de Gestión de Riesgos.



2 sesiones de 45 minutos.



- Líder de Proyecto.
- Grupo de Gestión de Riesgos.
- Encargado de calidad.



Plan de Gestión de Riesgos.

Durante esta actividad, se confecciona el plan de Gestión de Riesgos, documento rector de la Gestión de Riesgos durante el ciclo de vida del proyecto, contiene los elementos que guiarán la Gestión de Riesgos: su periodicidad, cronograma, valores y criterios a utilizar. A continuación se describen las secciones del plan de Gestión de Riesgos:

Planificación

En esta sección se documenta cuándo y con qué periodicidad se ejecutarán los procesos de la Gestión de Riesgos. El planificador juega un papel importante en este momento. Existen 2 tendencias fundamentales para la definición de la planificación: guiada por hitos, guiada por tiempo.

Si se desea una planificación guiada por hitos, debe documentarse los hitos del proyecto y para cada hito cuáles procesos de la Gestión de Riesgos se iniciarán y observaciones donde se puede especificar alguna recurrencia o cualquier otra indicación, ver un ejemplo en la Tabla 1.

Tabla 1. Ejemplo de planificación guiada por hitos.

Hito	Procesos a Realizar	Observaciones
Inicio Beta2	Identificación. Monitoreo y Control	Realizar monitoreo durante la iteración.

Si se desea una planificación guiada por fechas deben documentarse las fechas en que se realizarán los procesos y en las observaciones especificar recursiones o cualquier otra consideración.

Adicionalmente en la sección “Otras Indicaciones de Planificación” se deben documentar las restricciones e indicaciones que se acordaron durante esta etapa y que operarán sobre la ejecución de los procesos. Por ejemplo: “Realizar identificación 1 semana después del comienzo de cada iteración”.

A continuación se enumeran algunos consejos para la definición de las planificaciones.

- Realizar Identificación al inicio del proyecto y si se considera necesario repetirla en cada hito significativo de proyecto.
- Realizar Monitoreo y Control en cada hito significativo del proyecto.
- Realizar Análisis Cualitativo después de cada hito significativo de proyecto.
- Realizar Evaluación y Aprendizaje en la fase de cierre del proyecto.

Nota: estas sugerencias no limitan la periodicidad de los procesos.

Presupuesto

En esta sección se documenta el presupuesto disponible para las actividades de Gestión de Riesgos y para la ejecución de los planes de respuesta. Debe documentarse el monto del presupuesto para ambos fines. El económico del proyecto es necesario en este momento.

Técnicas a utilizar

En esta sección se documentan las técnicas a utilizar en cada proceso según las técnicas definidas en este documento. Para cada técnica a emplear se documentan los elementos necesarios que son definidos en la etapa de planificación, en la descripción de cada técnica se destacan estos elementos y se explica cómo elaborarlos. El asesor de calidad vela por este proceso para dentro de sus funciones velar por su correcta ejecución, y aporta comentarios valiosos sobre la efectividad de las técnicas seleccionadas. Todos los participantes deben discutir en conjunto los valores y criterios a personalizar en las técnicas.

Actividades de aseguramiento para el plan.

En esta sección se enumeran las actividades que realizará el proyecto en función del aseguramiento del plan, es decir de la Gestión de Riesgos en general. Estas actividades están enfocadas a mejorar la planificación, ejecución y control de los procesos de la Gestión de Riesgos, la investigación, en fin, son actividades para garantizar el correcto funcionamiento del modelo.

3 – Inclusión del plan de Gestión de Riesgos en el plan de proyecto general.



45 minutos.



- Líder de Proyecto.
- Planificador.

Durante esta actividad el líder de proyecto en conjunto con el planificador, analizan el plan de Gestión de Riesgos generado y realizan los ajustes pertinentes en el proyecto para incluir las actividades generadas en los mecanismos de gestión del proyecto. En esta etapa se deben definir políticas para el proyecto destacando la necesidad de que las futuras actividades generadas durante la Gestión de Riesgos sean también incluidas en estos mecanismos. El líder de proyecto debe tener comprometimiento pleno con la Gestión de Riesgos.

Identificación.



- Grupo de identificación.
- Líder de proyecto.
- Organizador de la Gestión de Riesgos.

- Todos los involucrados en la Gestión de Riesgos



- Plan de Gestión de Riesgos.
- Objetivos del proyecto.
- Criterio de éxito del proyecto.
- Lista de Riesgos Comunes.



- Conjunto de definiciones de riesgos.

Flujo de Trabajo.

La identificación comienza según lo planeado en el plan de Gestión de Riesgos en cada una de sus ejecuciones.

Durante este proceso se identifican los riesgos presentes en el proyecto mediante la utilización de alguna de las técnicas descritas en esta sección. Este proceso tiene actividad durante todo el ciclo de vida del proyecto, dicha actividad se comporta como describe la Figura 16 un proceso con una actividad creciente durante los inicios del proyecto, y con el punto máximo cerca del inicio, esta actividad tiende a estabilizarse y disminuir a lo largo del proyecto. Durante este proceso se realizan las actividades de Inicio de Identificación, Realización de la Identificación y Cierre de la identificación como se describe en la Figura 19. Como salida de este proceso se obtiene un conjunto de definiciones riesgos, estas definiciones, documentadas como se explica en la sección Representación de los

riesgos. (ver página 40), constituyen el activo fundamental de la Gestión de Riesgos, los siguientes procesos lo usarán como elemento fundamental sobre el que operan.

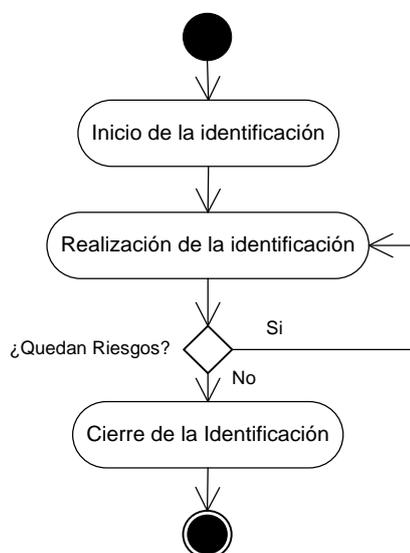


Figura 19. Flujo de trabajo de Identificación.

Es importante que los implicados en la Gestión de Riesgos reconozcan que estas representaciones no son riesgos, los riesgos son los eventos de la vida real que pueden o no ocurrir, las representaciones son una compilación de datos sobre el riesgo. Esta distinción ayuda a mantener el enfoque sobre el riesgo real, y no adoptar una actitud pasiva al considerar que el riesgo está bajo control al estar documentado.

Actividades.

1 – Inicio de la identificación.



15 minutos.



- Líder de Proyecto.
- Organizador de la Gestión de Riesgos.
- Involucrados en la identificación.

Al comenzar la identificación es necesario un encuentro donde participen todos los involucrados en la identificación de riesgos, este encuentro es conducido por el líder de proyecto y el organizador de la

Gestión de Riesgos. Tiene como misión recalcar los objetivos del proyecto y el criterio de éxito para que el proceso de identificación esté orientado en este sentido; ofrecer un panorama de las técnicas que se utilizarán, y el beneficio que se obtendrá de este proceso para aumentar la colaboración de los participantes. En el plan de Gestión de Riesgos se especifican cuales técnicas se van a utilizar y los datos necesarios para su aplicación.

Posterior al inicio, se continúa con la técnica o técnicas que se decidieron utilizar, de acuerdo a como se describe en este documento.

2 – Realización de la identificación.

Para la realización de la identificación se deben aplicar una o varias de las técnicas definidas que se hayan especificado en el plan de Gestión de Riesgos. Su tiempo estimado, participantes etc., depende de las técnicas que se utilicen. A continuación se describen posibles técnicas de identificación.



Punto de extensibilidad: Se pueden incluir otras técnicas para ejecutar esta actividad.

Algunas Consideraciones: La identificación, independientemente de la técnica que se utilice, está guiada por el Criterio de Éxito del Proyecto. Este criterio se elabora en conjunto con los clientes, y principalmente es el cliente quien define el criterio de éxito del proyecto. Dicho criterio es una frase que afirma (de ser posible cuantitativamente) qué hace que se considere el proyecto como satisfactorio. Por ejemplo:

“Versión 1.0 estable, desplegada en el 50 de las instalaciones principales para noviembre 2008 con 90% de las funcionalidades importantes, después de un mes de procesamiento el sistema comportándose estable, manejando 200 usuarios finales, 10 usuarios concurrentes”.

Contar con un criterio de éxito bien definido, garantiza su visibilidad en todas las actividades de la Gestión de Riesgos, y ayuda principalmente en la identificación. Durante este proceso debe mantenerse el enfoque sobre este criterio, los riesgos identificados deben estar orientados a la satisfacción de este criterio, a descubrir elementos que mejoren o atenten contra este criterio.

Sugerencias: para la determinación del criterio de éxito son útiles preguntas como: ¿qué lo hace un suceso: el producto de su área con más calidad en el mercado, el primero en salir, el más seguro? También es importante conocer cuándo será ese suceso ¿dentro de un año? ¿dentro de 1 mes? y qué características relevantes tendrá.

Un efecto similar tienen los objetivos del proyecto. Estos objetivos se enumeran claramente y deben cubrir como mínimo las siguientes categorías: Tiempo, Presupuesto, Calidad. Deben escribirse cuantitativamente siempre que sea posible. Los objetivos del proyecto definidos ayudarán a no perder la perspectiva durante la Gestión de Riesgos, a enfocar todas las actividades en su función para alcanzarlos mejor.

Es útil escribir cada objetivo como afirmación, no como negación, por ejemplo: “*No demorarse más de 3 meses*” puede constituir un objetivo, sin embargo al estar escrito como negación, no ofrece un camino a lo que se quiere, ofrece una restricción de dicho camino; escrito como “Concluir en junio de 2008...” ofrece un mejor panorama del objetivo, un enfoque más directo (aunque signifique lo mismo) y ayuda a la Gestión de Riesgos a ser objetiva. Es importante destacar que no es siempre así, y en ocasiones el líder de proyecto prefiere escribirlo negativamente para denotar su preocupación con la restricción que el objetivo impone, entonces es útil escribirlo como negación cuando sea muy importante destacar dicha restricción.

Sugerencias: aunque los objetivos del proyecto deben estar claros en los participantes, son útiles las siguientes preguntas para su identificación: ¿Cuándo tiene que terminar el proyecto? ¿Cuánto es el presupuesto del proyecto? ¿Cuánto nos podemos exceder del presupuesto?

2 – 1. Técnica de Entrevistas.



1 hora (cada sesión).



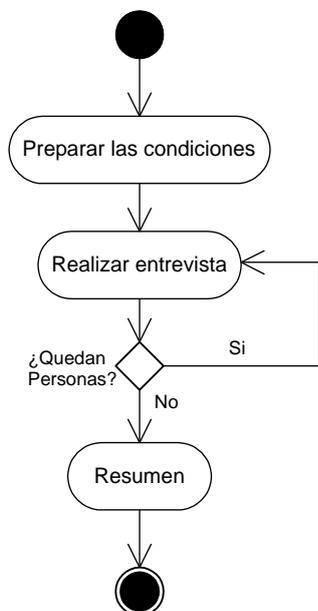
- Grupo de identificación.
- Involucrados en la Gestión de Riesgos.



- Plan de Gestión de Riesgos.
- Criterio de Éxito del Proyecto



- Conjunto de riesgos identificados.
- Contexto de la sesión de identificación.



(Este método es adaptado de “Taxonomy-Based Risk Identification” (39) y “Software Risks Evaluation SRE” (40)). El proceso de identificación se basa fundamentalmente en realizar entrevistas a los involucrados en la Gestión de Riesgos aplicando una serie de preguntas elaboradas (ver Anexo3 – Cuestionarios para la Identificación página 100) y que cubren todos los aspectos del proyecto de acuerdo a una taxonomía del proceso de desarrollo de software (ver Anexo2 – Taxonomía del Desarrollo de Software página 99), para posteriormente obtener definiciones de riesgos que luego serán analizadas. El grupo de identificación puede dividirse y realizar entrevistas simultáneamente.

A continuación se describe el procedimiento para aplicar la técnica:

- 1 – Preparar las condiciones para la realización de las entrevistas:

Figura 20. Técnica de Entrevista.

Se lleva a cabo por el encargado de operaciones y el organizador de la Gestión de Riesgos. Consiste en asegurar un local donde se realizara la entrevista, elaborar un poster o mostrar en un lugar visible la taxonomía completa, imprimir los cuestionarios a aplicar.

2 – Realizar entrevista:

Se lleva a cabo por dos miembros del grupo de identificación: un entrevistador y alguien que documentará el contexto de las entrevistas, para varias sesiones de entrevistas simultaneas, este miembro puede moverse de entrevista a entrevista para documentar un contexto general, no tiene por qué permanecer todo el tiempo de la sesión con el mismo entrevistador.

1- **Inicio.** El entrevistador recibe al entrevistado.

2- **Aplicar Pregunta:** Aplica la primera pregunta del cuestionario, ante la respuesta del entrevistado el entrevistador debe realizar otras preguntas para ayudar al entrevistado a identificar el riesgo (es importante hacerle destacar al entrevistado que es él quien identifica realmente el riesgo).

3- **Documentar el riesgo:** Una vez que el entrevistado comunica el riesgo, el entrevistador captura el riesgo y lo documenta en el modelo especificado en el Anexo4 – Modelo para documentar el riesgo (ver página 106), se documentas las propiedades ID, causa, evento, consecuencia, estado (identificado), y opcionalmente impacto y probabilidad como valores tentativos, quien identificó el riesgo se documenta como responsable, este valor es temporal, durante el análisis se decidirá quiénes son los responsables del riesgo.

4- **Mostrar el riesgo:** el entrevistador muestra el riesgo escrito en el modelo al entrevistado y de ser necesario lo reescriben hasta que el entrevistado quede satisfecho con el riesgo que él ha comunicado.

5- **Fin.**

El proceso se repite con todas las preguntas del cuestionario como se muestra en la Figura 21. El entrevistador no puede interrumpir un riesgo que espontáneamente brote del entrevistado, debe pasar al paso 3, documentarlo y discutirlo posteriormente, sin embargo debe ajustarse al cuestionario.

Como resultado de esta actividad se obtienen varios riesgos identificados y una descripción del contexto de la sesión de identificación.

3 – Resumen:

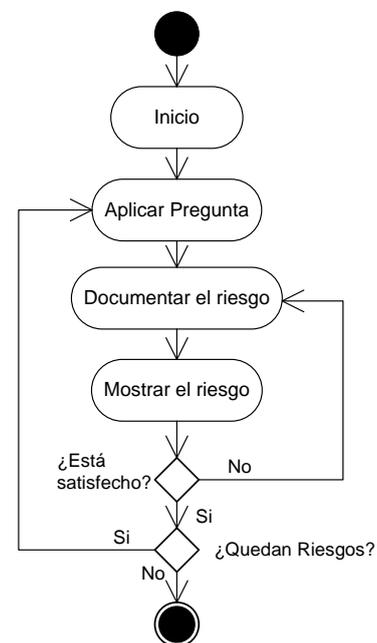


Figura 21. Procedimiento para realizar las entrevistas.

Al concluir la sesión de entrevistas para la identificación, el grupo de identificación se reúne si ha estado aplicando entrevistas separadamente y compila los riesgos obtenidos: todos los riesgos deben ser analizados en busca de riesgos repetidos (duplicados), el contexto debe ser analizado y enriquecido con las propias palabras de los entrevistadores y puede que se identifiquen riesgos del análisis de este contexto que en tal caso deben ser documentados.

Todo el personal que participó en la identificación (los entrevistados), deben ser notificados del resultado: informarles cuántos riesgos se han identificados y las cantidades por categoría, destacando su papel durante la identificación.

A todos los riesgos identificados se documenta la propiedad Etapa con el valor de la etapa actual del proyecto, si el riesgo identificado es un riesgo reincidente, se documenta la nueva etapa sin perder las anteriores para preservar la información del riesgo.

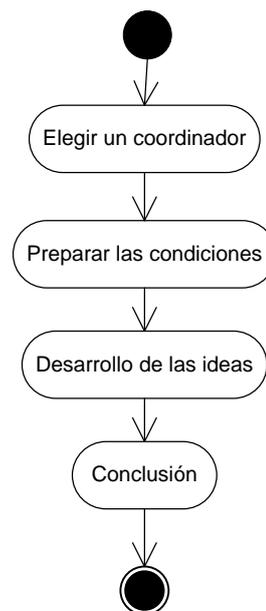


Figura 22. Técnica Tormenta de Ideas.

2 – 2. Técnica de Trabajo en Grupo: Tormenta de Ideas.



Sesiones de 45.
Se recomiendan 2 sesiones



- Grupo de identificación.
- Personal del proyecto (no más de 8 personas).



- Conjunto de riesgos identificados.

(Esta técnica es adaptada de Fundibeq (59)). Esta técnica de trabajo en grupo generalmente potencia la participación y creatividad en sus participantes. Se basa en la elección de un tema de discusión, y en un ambiente propicio para el tema, realizar rondas donde en cada una se proponga una idea, al final se analizan y se discuten.

A continuación se describe el procedimiento para aplicar la técnica:

1 – Elegir un coordinador:

Dentro del grupo de identificación se elige un coordinador para la tormenta de ideas, debe ser alguien con habilidades de liderazgo y moderación, es recomendable que sea el organizador de la Gestión de Riesgos. El coordinador debe ser efectivo en el control y organización del flujo de las ideas, debe evitar que se violen las reglas de la Tormenta de Ideas.

2 – Preparar las condiciones para su aplicación.

Participa el coordinador de la tormenta de ideas, el organizador de la Gestión de Riesgos y el encargado de operaciones.

Se necesitan 2 tipos de condiciones para su aplicación: materiales y psicológicas.

Materiales: el coordinador con ayuda del encargado de operaciones deben garantizar un local para que sesione la tormenta de ideas, material para escribir las ideas, preferentemente una pizarra en lugar visible a todos los involucrados.

Psicológicas: el personal involucrado debe estar en un ambiente que propicie la creatividad, el coordinador debe explicar las reglas de las tormentas de ideas:

- Pensamiento creativo.
- No se admiten críticas ni comentarios en ningún sentido sobre las ideas emitidas.
- Se anotarán todas las ideas.

Se puede simular una tormenta de idea con un tema atractivo, divertido, y diferente del proyecto o la Gestión de Riesgos que no dure más de 10 minutos, con el objetivo de preparar las condiciones psicológicas.

El coordinador debe escribir los riesgos de forma no tabular, es preferible circular y contrarias a las manecillas del reloj para fomentar la creatividad (60).

3 – Desarrollo de las ideas:

El tema central de la tormenta de ideas siempre será la identificación de riesgos. La tormenta de ideas puede estar enmarcada a un área u objetivo específico, en tal caso debe escribirse en un lugar visible durante toda la sesión el tema de la identificación, dicho tema debe ser conciso de forma que defina el alcance de la identificación.

El moderador debe establecer un turno a cada cuál para expresar las ideas sobre posibles riesgos, se expresa 1 riesgo en cada turno, los participantes deben escribirlos para no olvidarlos de turno a turno. Si en un turno alguien no tiene propuesta, puede pasar y se incorpora en el próximo turno. Este proceso debe ser continuo y organizado.

Cuando el moderador considere un número significativo de riesgos, estos deben analizarse: los duplicados se deben fusionar en uno solo que los defina a los dos, deben ordenarse y categorizarse de acuerdo a las categorías de la taxonomía del desarrollo de software.

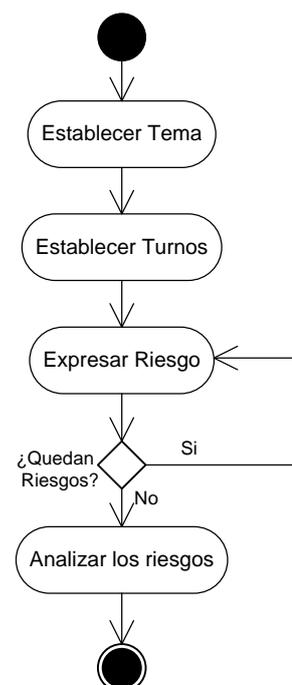


Figura 23. Desarrollo de las ideas.

Se deben mostrar las categorías en las cuales no se hayan identificado riesgos y hacer nuevas rondas para tratar de descubrir riesgos en esas áreas.

Posterior a la organización de los riesgos identificados, estos deben documentarse de acuerdo al modelo especificado en el Anexo4 – Modelo para documentar el riesgo (*ver página 106*), se documentan las propiedades ID, causa, evento, consecuencia, estado (identificado), y opcionalmente impacto y probabilidad como valores tentativos.

El moderador debe decidir cuándo terminar la tormenta y pasar a la conclusión.

4 – Conclusión de la tormenta de ideas:

La tormenta de ideas debe concluir cuando los participantes agotaron sus ideas y no tiene nuevos riesgos que proponer. Debe reflexionarse brevemente sobre los riesgos identificados, deben leerse todos y acordar que están bien categorizados. Deben explicarse dudas sobre los riesgos de surgir alguna.

Salidas:

- Conjunto de riesgos identificados.

2 – 3. Técnicas basadas en el conocimiento (Revisión de los riesgos conocidos).



Sesiones de 45 minutos.



- Grupo de identificación



- Plan de Gestión de Riesgos.
- Lista de riesgos conocidos.
(*ver página 107*).



- Conjunto de riesgos identificados

Generalmente en los proyectos productivos se presentan riesgos repetidos de proyecto a proyecto, es útil contar con una lista de riesgos comunes o frecuentes y durante la etapa de identificación analizarlos y evaluar si están presentes en este proyecto también.

Para aplicar esta técnica debe reunirse el grupo de identificación en sesiones de trabajo donde el organizador lea cada uno de los riesgos presentes en la lista, y el grupo analice si está presente o no en este proyecto, en caso de estar presente el riesgo se documenta y adiciona a la lista de definiciones de riesgos identificados. El proceso se repite con todos los riesgos de la lista de riesgos conocidos.

Esta lista se mantiene en el documento “Lista de riesgos Comunes” (ver página 107). Si se decide que un riesgo de la lista es un riesgo presente se documenta en el formulario correspondiente.

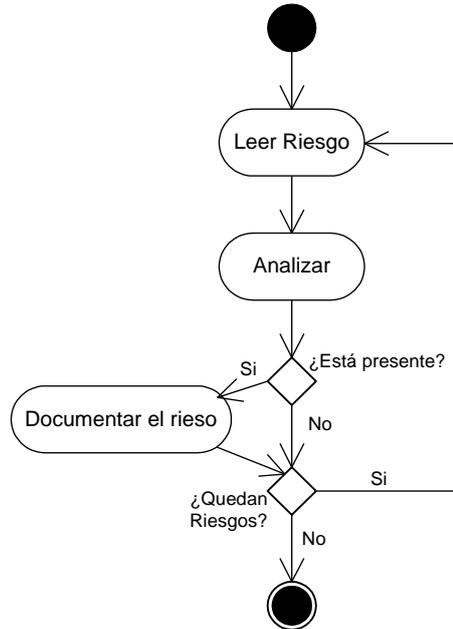


Figura 24. Técnica basada en el conocimiento.

3 – Cierre de la Identificación.



20 – 30 minutos



- Líder de proyecto.
- Grupo de Gestión de Riesgos.

Al concluir la identificación tras aplicar una o varias técnicas de las definidas en este documento, todas las definiciones de riesgos documentadas deben ser analizadas, organizadas y categorizadas de acuerdo a la taxonomía del desarrollo de software. En un encuentro con el líder del proyecto se revisan todos los riesgos identificados, un proceso meramente informativo, no se comentan datos sobre los riesgos o se hace otra actividad, este proceso es necesario para tener un panorama de los riesgos identificados para prepararse para el análisis. Si alguna técnica define un proceso parecido a este (por ejemplo la técnica de entrevistas ver página 49) y es la última técnica a aplicar, puede omitirse este paso.

Análisis Cualitativo.



- Grupo de análisis.
- Líder de proyecto.



- Conjunto de definiciones de riesgos.
- Plan de Gestión de Riesgos.



- Conjunto de definiciones de riesgos (actualizadas).

Flujo de Trabajo.

El análisis cualitativo comienza al concluir la identificación, tiene como objetivo priorizar los riesgos. Durante este proceso se evaluarán cualitativamente las propiedades de los riesgos y se priorizarán utilizando un conjunto de técnicas definidas en cada caso. El flujo de trabajo de esta actividad se describe en la Figura 25. Como salida de este proceso se obtiene el conjunto de riesgos de entrada pero actualizados y priorizados, listos para un posterior análisis más profundo. Al concluir este proceso, los riesgos analizados tienen el estado: analizado.

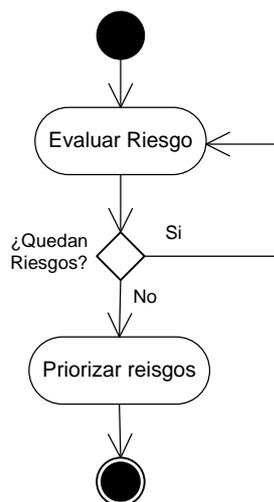


Figura 25. Flujo de trabajo de Análisis Cualitativo.

Actividades.

1 – Evaluación del Riesgo.



2 sesiones de 45 minutos¹⁰.



- Líder de Proyecto
- Grupo de Análisis.

La evaluación de un riesgo consiste en determinar cualitativamente los valores de probabilidad impacto, frecuencia y certidumbre de la información usando las técnicas definidas en el plan de Gestión de Riesgos para posteriormente ordenar los riesgos y obtener su prioridad. A continuación se describen las técnicas aplicables en esta actividad. Los valores de ejemplo en estas técnicas pueden ser utilizados, dichos valores han sido obtenidos prescriptivamente de acuerdo al criterio de algunos expertos.



Punto de extensibilidad: Se pueden incluir otras técnicas para ejecutar esta actividad.

Técnicas para evaluar la probabilidad:

1 – 1. Tabla Fija de Probabilidades.

Esta técnica se basa en la lógica discreta. Para su aplicación se reúne el grupo de análisis, el líder de proyecto, y se puede invitar a otro personal de proyecto que se considere puede aportar comentarios valiosos sobre la probabilidad de ocurrencia de determinados riesgos, pueden invitarse expertos que aporten comentarios similares. En dicha reunión debe existir un ambiente colaborativo, para el éxito de la técnica es importante expresar con la mayor realidad posible la probabilidad del riesgo, no debe existir temor a la expresión o algún tipo de represión.

Se toma cada definición de riesgo, se analiza la probabilidad de ocurrencia que tenga guiado por una tabla similar a la Tabla 2 y luego se documenta el valor de probabilidad en la definición del riesgo.

Tabla 2. Probabilidades de los riesgos.

Probabilidad	Categoría
1% - 33%	Baja
33% - 66%	Media
66% - 99%	Alta

¹⁰ Depende de la técnica a utilizar y la cantidad de riesgos que se evalúen. Se recomienda dedicar todas las sesiones necesarias.

 **Elemento del Plan de Gestión de Riesgos.** Dicha tabla con valores, debe estar reflejada en el plan de Gestión de Riesgos. Deben ajustarse los valores de probabilidad en caso que se considere necesario. La tabla de probabilidades puede tener más definiciones si se desea aumentar las categorías, por ejemplo (muy baja, baja, media, alta, muy alta), en tal caso deben ajustarse los valores de probabilidad para cada categoría.

Técnicas para evaluar la frecuencia:

1 – 3. Métrica de Frecuencia

Se reúne en sesiones de trabajo el grupo de análisis, el líder de proyecto, y se puede invitar a otro personal de proyecto que se considere puede aportar comentarios valiosos, pueden invitarse expertos que aporten comentarios similares.

La técnica se basa determinar la frecuencia de aparición (f) estimando la cantidad de veces que aparecerá el riesgo (n) en una unidad de tiempo para determinar su frecuencia a lo largo del proyecto dividiéndolo por la cantidad total de unidades de tiempo en el proyecto (T).

$$f = \frac{t}{T}$$

Ecuación 1. Métrica de la Frecuencia.

Unidad de tiempo (T): Para proyectos de alrededor de 3 meses, utilizar unidad de medida “semanas” para proyectos de alrededor de 1 año, utilizar unidad de medidas “mes”, para proyectos mayores se recomienda dividirlos en periodos de 1 año y utilizar “mes”.

La frecuencia se puede interpretar, por ejemplo, que un valor de frecuencia 0.3 indicará que ese riesgo aparece el 30% del tiempo en el proyecto.

El valor de frecuencia obtenido para cada riesgo se documenta en la definición de riesgo.

El proceso se repite con todas las definiciones de riesgos.

 **Elemento del Plan de Gestión de Riesgos:** la unidad de tiempo debe estar reflejada en el plan de Gestión de Riesgos.

Técnicas para evaluar el impacto:

1 – 4. Tabla Fija de Impactos.

Se reúne en sesiones de trabajo el grupo de análisis, el líder de proyecto, y se puede invitar a otro personal de proyecto que se considere puede aportar comentarios valiosos, pueden invitarse expertos que aporten comentarios similares.

Se toma cada definición de riesgo, y para cada objetivo del proyecto, se analiza el impacto que ese riesgo puede provocar sobre dicho objetivo utilizando las tablas de impacto como se muestra a

continuación, luego se documenta el impacto del riesgo sobre cada objetivo en la definición del riesgo, se continua con el proceso con todas las definiciones de riesgos.

Para cada objetivo se construye una tabla similar a las siguientes que se documenta en el plan de Gestión de Riesgos:

Tabla 3. Impacto respecto al costo.

Rango del impacto esperado	Expresión
0% - 4%	Bajo
5% - 9%	Medio
> 10%	Alto
-1% - -4%	Bajo
-5% - -9%	Medio
< -10%	Alto

Sugerencia: el criterio para considerar el impacto alto, puede determinarse de acuerdo al presupuesto destinado para reserva.

Tabla 4. Impacto respecto al tiempo.

Rango del impacto esperado	Expresión
0 a 7 días	Bajo
2 a 4 semanas	Medio
> 4 semanas	Alto
< 1 semana	Bajo
< 2 semanas	Medio
< 4 semanas	Alto

Nótese que para cada objetivo se asocian 3 posibles impactos, si se considera necesario se puede extender la cantidad de expresiones (muy bajo, bajo, medio, alto, muy alto) y ajustar los valores de dichas expresiones. Si sobre todos los objetivos existe la misma cantidad de expresiones, estas tablas se pueden consolidar en una sola como muestra la Tabla 5.

Tabla 5. Impactos consolidados.

	Bajo	Medio	Alto	Bajo	Medio	Alto
Tiempo	0 a 7 días	2 a 4 sem.	> 4 sem.	< 1 sem.	< 2 sem.	< 4 sem.
Costo	0% - 4%	5% - 9%	> 10%	-1% - -4%	-5% - -9%	> -10%

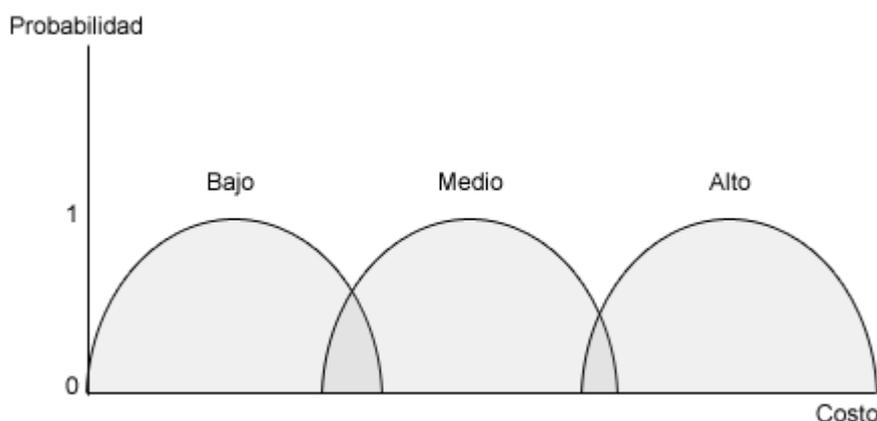
Elemento del Plan de Gestión de Riesgos: las tablas 4, 5 o 6 se documentan en el plan de Gestión de Riesgos con los valores acordados. Durante la Gestión de Riesgos estos criterios pueden cambiar, en tal caso deben actualizarse en el plan.

1 – 5. Tabla Fuzzi de Impactos.

Reunirse en sesiones de trabajo el grupo de análisis, el líder de proyecto, y se puede invitar a otro personal de proyecto que se considere puede aportar comentarios valiosos, deben invitarse expertos que construyan las tablas de impactos.

Se toma cada definición de riesgo, y para cada objetivo del proyecto, se analiza el impacto que ese riesgo puede provocar sobre dicho objetivo, utilizando las tablas de impacto como se muestra a continuación. Luego se documenta el impacto del riesgo sobre cada objetivo en la definición del riesgo, se continúa con el proceso con todas las definiciones de riesgos.

Tabla 6. Impacto respecto al costo.



Elemento del Plan de Gestión de Riesgos: Estas tablas son construidas por expertos, se incluyen en el plan de Gestión de Riesgos.

Técnicas para evaluar la incertidumbre:

1 – 6. Incertidumbre de la información del riesgo.

Esta técnica analiza la certidumbre sobre la información del riesgo para ayudar en la priorización de los mismos posteriormente. El grupo de identificación se reúne en sesiones de trabajo y para cada riesgo determina un valor que describa el grado de certeza que se tiene sobre la veracidad de la información sobre el riesgo. Si bien tener una información certera sobre el riesgo es útil para el éxito de la Gestión de Riesgos, evaluar su certidumbre es igual de importante y se corre tanto riesgo al tener una información no certera que al valorar incorrectamente su certeza, es necesario un equilibrio entre estas dos variables.

El grado de incertidumbre se expresa en valores porcentuales, y deben asociarse criterios verbales como se muestra en la Tabla 7.

Tabla 7. Grados de certidumbre.

Categoría	Valor
Muy Seguro	99%
Seguro	50%
Inseguro	10%

Si se desean aumentar la cantidad de categorías que expresen la seguridad sobre la información del riesgo, debe modificarse esta tabla y actualizarse los valores.

 **Elemento del Plan de Gestión de Riesgos:** la Tabla 7 se especifican en el plan de Gestión de Riesgos.

2 – Priorización de los riesgos.



2 sesiones de 45 minutos.



- Líder de Proyecto.
- Grupo de análisis.

Sugerencia: Depende de la técnica a utilizar y la cantidad de riesgos que se evalúen. Se recomienda dedicar todas las sesiones necesarias.

La priorización de los riesgos consiste decidir cuáles riesgos son más importantes que otros con la aplicación de algunas de las técnicas definidas a continuación, y obtener la lista de riesgos priorizados para posteriormente analizar cuantitativamente los riesgos más importantes. Una vez aplicada alguna de las siguientes técnicas de obtención de prioridad del riesgo, se debe actualizar este valor en la propiedad del riesgo llamada Prioridad.

 Punto de extensibilidad: Se pueden incluir otras técnicas para ejecutar esta actividad.

Técnicas de Priorización:

2 – 1. Matriz de Probabilidad e Impacto.

Esta técnica calcula la prioridad del riesgo basándose en una combinación de probabilidad e impacto, asumiendo que los riesgos con alta probabilidad y alto impacto son más priorizados, es aplicable tanto a las amenazas como a las oportunidades.

El grupo de análisis se reúne en sesiones de trabajo y para cada riesgo analizan su probabilidad e impacto sobre cada objetivo y observan en qué región de la matriz aparece el riesgo, de esta forma se obtiene su grado de prioridad para cada objetivo. Este proceso se aplica a todas las definiciones de riesgos.

Las combinaciones de probabilidad e impacto se reflejan en la siguiente tabla o matriz elaborada por los expertos quienes definen los criterios para decidir si una combinación de probabilidad e impacto determinada es alta prioridad, media o baja.

Tabla 8. Matriz de probabilidad e impacto.

P	I	Bajo	Medio	Alto
Alta		Media	Alta	Alta
Media		Baja	Media	Alta
Baja		Baja	Baja	Media

En caso que las categorías de probabilidad o impacto hayan sido más de 3, se debe actualizar la matriz incluyendo las nuevas categorías y los criterios para las nuevas combinaciones.

Elemento del Plan de Gestión de Riesgos: la matriz de probabilidad e impacto se incluye en el plan de Gestión de Riesgos.

2 – 2. Técnicas Estadísticas.

El uso de técnicas estadísticas es una técnica parecida a la Matriz de Probabilidad e Impacto en principio, consiste en obtener la prioridad del riesgo de acuerdo a sus valores de probabilidad e impacto.

El grupo de análisis se reúne en sesiones de trabajo para calcular la prioridad del riesgo. Los posibles valores de probabilidad e impacto están ubicados en un sistema coordenado. La priorización entonces se realiza ubicando el riesgo actual de acuerdo a sus valores en el sistema coordenado y obteniendo

un punto en dicho sistema. Todos los riesgos son ubicados en este sistema y posteriormente se puede identificar cuáles son los riesgos (puntos) más priorizados de acuerdo a su posición en el sistema coordinado.

Los criterios para determinar cuáles riesgos son más priorizados que otros se representan en este sistema, puede ser mediante regiones o textos descriptivos como la Figura 26, donde los puntos cerca de las regiones o textos serán considerados de acuerdo al criterio establecido para dichas regiones.

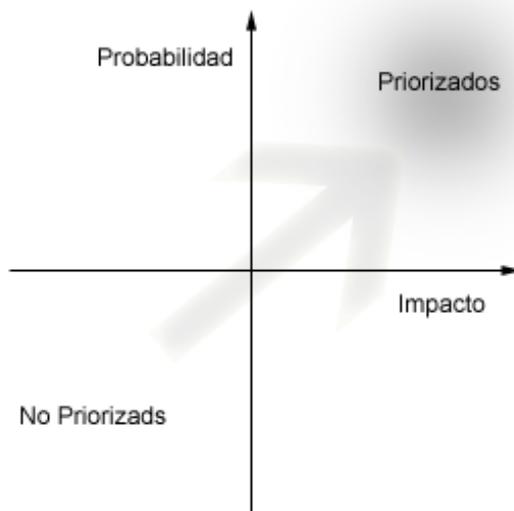


Figura 26. Priorización utilizando técnicas estadísticas.

Elemento del Plan de Gestión de Riesgos: el sistema coordinado y los criterios se incluyen en el plan de Gestión de Riesgos.

2 – 3. Suma Ponderada.

Esta técnica “normaliza” los impactos sobre cada objetivo en un único valor reflejando el impacto total del riesgo.

Para cada objetivo del proyecto (0) se le asignan grados de importancia (i), expresados porcentualmente como muestra la Tabla 9.

Tabla 9. Grado de importancia de cada objetivo.

Objetivo	Importancia
Tiempo	40%
Costo	60%

Tabla 10. Valores numéricos de impactos de cada categoría.

Categoría	Valor
Alto	3
Medio	2
Bajo	1

A cada categoría de impacto se le asocia un valor numérico (v) para “normalizar” sus valores como muestra la Tabla 10. Para calcular el impacto total del riesgo (I) se realiza una sumatoria por cada objetivo multiplicando la importancia de ese objetivo por su valor concreto en ese riesgo. Matemáticamente se puede expresar como la Ecuación 2.

$$I = \sum_{k=0}^n i_k * v_k$$

Ecuación 2. Suma Ponderada.

El impacto total del riesgo (I) es un valor numérico que no debe mezclarse con los impactos sobre cada objetivo en específico siempre que estos estén expresados en valores de su dominio. Por ejemplo, un impacto de \$4000 sobre el costo, o del 30% sobre el costo, no debe compararse con un impacto total de valor 50.

Elemento del Plan de Gestión de Riesgos: la Tabla 9 y Tabla 10 se documentan en el plan de Gestión de Riesgos.

2 – 4. Incertidumbre de la información del riesgo.

Esta técnica de priorización se aplica en conjunto con las técnicas anteriores (preferentemente Suma Ponderada) y si durante la actividad de evaluación se analizó la incertidumbre de la información de cada riesgo.

El grupo de análisis se reúne en sesión de trabajo, con el objetivo de calcular un indicador de priorización para cada riesgo y ordenarlos por dicho indicador. El grupo analiza cada riesgo. Se multiplica el grado de incertidumbre (c) por el impacto total (I) obteniendo un indicador de priorización (p).

$$p = c * I$$

Ecuación 3. Indicador de priorización.

Análisis Cuantitativo.



- Grupo de análisis.
- Líder de proyecto.



- Conjunto de definiciones de riesgos.
- Plan de Gestión de Riesgos.



- Conjunto de definiciones de riesgos (actualizadas).

Flujo de Trabajo.

El análisis cuantitativo se ejecuta después del análisis cualitativo o cuando se considere necesario reevaluar algún o todos los riesgos. Durante este proceso se escoge un conjunto de riesgos más priorizados y se cuantifica numéricamente su impacto sobre los objetivos del proyecto. La cuantificación se realiza con el empleo de algunas técnicas descritas en este documento y siempre es un valor numérico. Generalmente se les realiza análisis cuantitativo solo a los riesgos más priorizados. Los valores numéricos son difíciles de calcular y dependen mucho de las condiciones propias del proyecto y del riesgo, es difícil establecer procedimientos paso a paso para su empleo. El grupo de análisis debe utilizar técnicas que conozcan como diagrama de tornado, árboles de decisiones, valor monetario esperado, simulaciones etc.

A continuación se describen las técnicas más triviales de análisis cuantitativo.

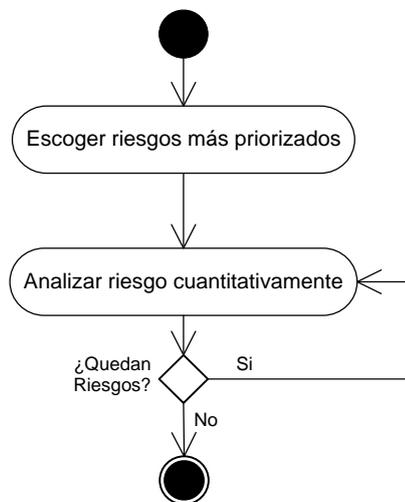


Figura 27. Flujo de trabajo de Análisis Cuantitativo.

Actividades.

1 – Escoger riesgos más priorizados.



15 minutos.

- Líder de Proyecto.
- Grupo de análisis.

El grupo de análisis se reúne en sesión de trabajo y analizan el conjunto de riesgos identificados con el fin de escoger un grupo de los riesgos más priorizados, según la prioridad definida en el proceso anterior, para realizarles el análisis cuantitativo. La elección de la cantidad de estos riesgos depende de las características del proyecto, es difícil establecer un criterio para decidir a cuáles riesgos realizarles este análisis o no, sin embargo debe tenerse en cuenta:

- No violar la prioridad calculada durante el análisis cualitativo.
- Valorar si el riesgo seleccionado para el análisis cuantitativo es adecuado atendiendo a lograr un balance entre el tiempo y recursos que se emplearán para ello, y el valor de haber analizado el riesgo cuantitativamente.

2 – Analizar riesgo cuantitativamente.



Sesiones de 45 minutos¹¹.



- Líder de Proyecto.
- Grupo de análisis.

El grupo de análisis y el líder de proyecto se reúnen en sesión de trabajo y analizan cada uno de los riesgos seleccionados para el análisis cuantitativo con la aplicación de una o varias de las técnicas que se describen a continuación. Tiene el objetivo de determinar valores numéricos de probabilidad e impacto para cada riesgo.



Punto de extensibilidad: Se pueden incluir otras técnicas para ejecutar esta actividad.

3 – 5. Entrevistas.



Sesiones de 45 minutos.



- Líder de Proyecto.
- Grupo de análisis.
- Entrevistados.

El grupo de análisis realiza entrevistas con el fin de determinar el valor numérico más exacto posible de probabilidad e impacto para los riesgos. Las entrevistas son aplicables a individuos con experiencia

¹¹ La duración de esta actividad depende de las características de cada riesgo, del proyecto y las circunstancias en general.

en el dominio del riesgo, personal con mucha experiencia miembro del proyecto o no. Se pueden aplicar métodos de entrevista individual o el método Delphi, siempre con el objetivo de extraer de los expertos el valor más exacto posible de probabilidad e impacto.

3 – 6. Juicio de expertos.



Sesiones de 45 minutos.



- Líder de Proyecto.
- Grupo de análisis.
- Expertos.

Los participantes se reúnen en sesión de trabajo y analizan cada riesgo. Los valores de impacto son determinados de acuerdo al juicio de expertos en la materia. Pueden ser internos o externos a la organización. El criterio de expertos es un elemento de alto valor en la determinación cuantitativa del impacto de un riesgo pues generalmente cuentan con vasta experiencia y han vivido situaciones similares.

La aplicación de esta técnica es útil en combinación con otras, y es recomendable utilizarla siempre con los riesgos más altos independientemente de que estos hayan sido analizados con muchas otras técnicas. Contar con el juicio de expertos es invaluable.

Su éxito depende de las características de los expertos y la correcta información en el riesgo.

Conclusiones Parciales

En este capítulo se da cumplimiento al segundo objetivo relacionado con la confección del modelo. Se define el alcance del mismo y las premisas y principios para su aplicación, elementos que garantizan el funcionamiento del modelo. Se define una representación del modelo y de los riesgos, y se describe el primer grupo de procesos: planeación, identificación, análisis cualitativo y análisis cuantitativo. Se adaptan técnicas como Taxonomy Based Risk Identification y Tormenta de Ideas y se proponen técnicas basadas en el conocimiento para la identificación de los riesgos. Para el análisis cualitativo se adaptan técnicas de evaluación y priorización como matriz de probabilidad e impacto, tabla de probabilidades, técnicas estadísticas; y se proponen técnicas como tabla fuzzy de impacto, métrica de la frecuencia, incertidumbre de la información y suma ponderada. Para el análisis cuantitativo se adaptan técnicas de entrevista y juicio de expertos.

Capítulo 3: Medición y Control

Segundo Grupo de Procesos

Planeación de la Respuesta.



- Líder de Proyecto.
- Grupo de análisis.



- Plan de Gestión de Riesgos.
- Conjunto de riesgos identificados.
- Lecciones aprendidas.
- Respuestas comunes a riesgos.



- Conjunto de planes de respuesta a los riesgos.

Flujo de Trabajo.

Este proceso se ejecuta seguidamente del análisis cualitativo, tiene el objetivo de elaborar estrategias y planes de respuesta (de mitigación o explotación) a los riesgos. Durante este proceso se analiza el conocimiento histórico en busca de guías y recomendaciones para las decisiones que se tomarán. Al concluir este proceso se obtiene el conjunto de planes de respuesta a los riesgos. A los riesgos que se han analizado y definido alguna estrategia de respuesta se les modifica el estado a: Activo.

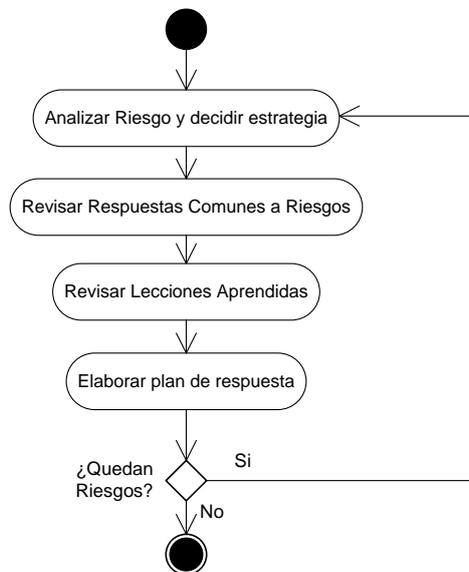


Figura 28. Flujo de trabajo de Planeación de la Respuesta.

Actividades.

1 – Analizar Riesgo y decidir estrategia.



No más de 20 minutos¹².



- Líder de Proyecto.
- Grupo de análisis.

El grupo de análisis se reúne en sesiones de trabajo conjuntamente con el líder de proyecto y analizan cada riesgo, el grupo debe decidir qué estrategia adoptar para el riesgo, las estrategias se describen a continuación:

Estrategias para amenazas:

Evitar: esta estrategia consiste en cambiar el plan de proyecto ampliando el cronograma, o reduciendo el alcance, es decir, relajando el objetivo que está en peligro o tomando otras acciones en virtud de no enfrentar el riesgo.

Transferir: esta estrategia transfiere el impacto negativo del riesgo y su respuesta a un tercero que asuma su gestión, generalmente esta estrategia se toma ante riesgos financieros o requerimientos importantes.

Mitigar: esta estrategia trata de reducir el impacto o la probabilidad del riesgo hasta valores aceptables, estos valores aceptables son definidos por el líder de proyecto respetando las políticas y direcciones de la universidad.

Estrategias para oportunidades:

Explotar: esta estrategia se toma cuando se desee concretar la oportunidad, es decir, reducir su incertidumbre hasta convertirla en un hecho que traerá beneficios.

Compartir: esta estrategia consiste en asignarlo a un tercero que tiene mejores condiciones o posibilidades para explotarlo en beneficio del proyecto. Generalmente se construyen equipos en conjunto.

Mejorar: esta estrategia aumenta la probabilidad, impacto, o la causa del riesgo para acercarla a condiciones de explotación.

Estrategias Comunes:

Aceptar: esta estrategia se utiliza cuando no se desea o no se puede hacer nada con el riesgo, es una estrategia sensible y cuando se adopte debe documentarse el por qué de su elección.

¹² Depende de cada riesgo.

Investigar: esta estrategia se adopta cuando no se tiene suficiente información o los impactos son muy grandes y la certidumbre de la información es poca. Se adopta con el objetivo de aumentar el conocimiento sobre el riesgo y tomar mejores decisiones.

La estrategia seleccionada se documenta en el riesgo. Para su selección es útil seguir un proceso como el que se describe en la Figura 26 (este proceso es adaptado de “Software Acquisition Risk Management Key Process Area (KPA)” (61)):

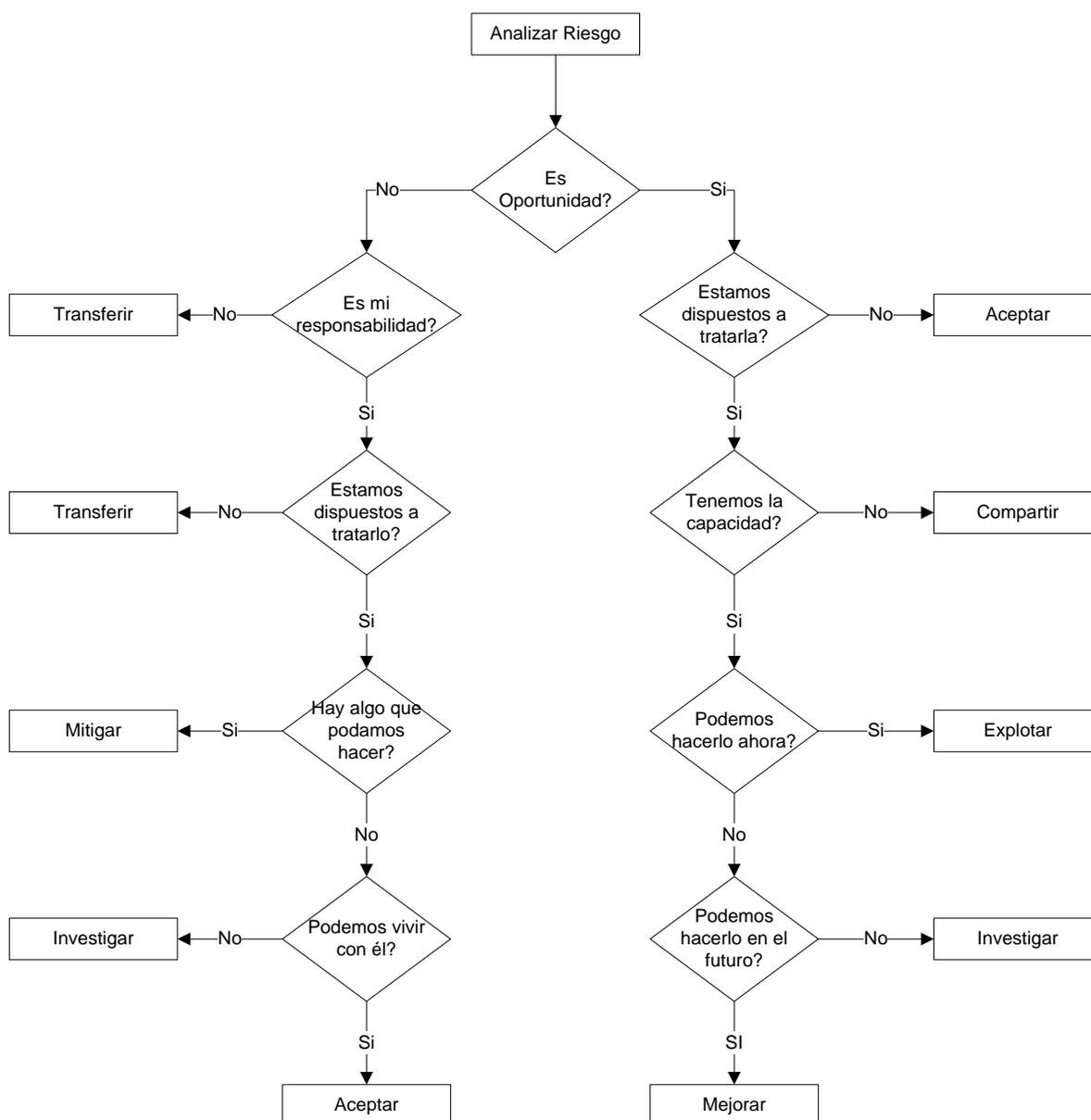


Figura 29. Proceso para asistir en la determinación de la estrategia a seguir.

Este proceso es una ayuda con los pasos lógicos a realizar para la determinación de la estrategia a utilizar. No obliga la selección de la estrategia, pues existen muchos otros factores complejos y diversos a tener en cuenta muy propios de cada proyecto y de las características del riesgo, pero sí es útil como una herramienta para ayudar en la toma de una decisión.

2 – Revisar Respuestas Comunes a Riesgos.



No más de 45 minutos¹³.



- Líder de Proyecto.
- Grupo de análisis.

Una vez propuesta una estrategia a seguir con el riesgo, debe revisarse las respuestas comunes a riesgos (*ver Anexo8 – Respuestas Comunes a Riesgos página 114*) con el objetivo de identificar algunas respuestas conocidas para el riesgo en cuestión.

Deben buscarse riesgos con características similares y observar estrategias y acciones pasadas que se adoptaron para ese riesgo y fueron efectivas, debe compararse si la estrategia seleccionada para el riesgo se corresponde con las estrategias antiguas, en tal caso se tiene un indicio sobre si será efectiva o no sobre el riesgo. No obstante deben evaluarse las condiciones actuales en las que aparece el riesgo, pero contar con el conocimiento anterior de estas estrategias ayuda en la certeza de su elección como un camino viable para el riesgo.

3 – Revisar Lecciones Aprendidas.



No más de 20 minutos.¹⁴



- Líder de Proyecto.
- Grupo de análisis.

Deben revisarse las lecciones aprendidas de la Gestión de Riesgos (*ver Anexo6 – Lecciones Aprendidas Página 112*) especialmente los planes de respuesta que funcionaron y no funcionaron, para riesgos similares, con el objetivo de ganar conocimiento para elaborar un plan de respuesta preciso y efectivo para el riesgo. Es útil que el grupo de análisis discuta sobre las posibilidades de reutilizar un plan de respuesta, y adaptarlo a las nuevas necesidades. Deben anotarse las consideraciones y conclusiones que se acuerden para posteriormente elaborar el plan de respuesta.

¹³ Depende de cada riesgo y la cantidad de respuestas comunes.

¹⁴ Depende de cada riesgo y la cantidad de lecciones.

4 – Elaborar plan de respuesta.



Sesiones de 45 minutos.



- Líder de Proyecto.
- Grupo de análisis.

Una vez tomada una decisión sobre la estrategia a seguir con el riesgo, y habiendo revisado las respuestas comunes a riesgos similares y las lecciones aprendidas en busca de planes que funcionaron o no, se debe elaborar un plan de respuesta para el riesgo utilizando el modelo descrito en el Anexo7 – Plan de Respuesta de Riesgo (ver página 113).

El plan tiene un identificador único, describe a qué riesgos o tipo de riesgos es aplicable, define claramente desde qué tiempo es efectivo y hasta cuándo, puede ser con fechas concretas o tiempos relativos al proyecto. Describe en qué momento se inicia el plan y cuáles son las condiciones para su inicio. Luego se describen las actividades o tareas concretas que componen el plan destacando el responsable de ejecutarla (describiendo su rol) y alguna referencia a la actividad asociada en el plan de actividades general del proyecto. Es importante que las actividades de respuesta al riesgo sean incluidas en los mecanismos de ejecución y control del proyecto logrando un comprometimiento máximo de todos sus miembros en función en su ejecución. Finalmente se deben describir qué criterios se utilizarán para la evaluación de la efectividad del plan, de ser posible deben ser cuantitativos, objetivos y prácticos para el proyecto.

Durante esta actividad también se analiza y se decide un valor para la propiedad del riesgo: marco de tiempo. El valor de dicha propiedad es uno de los definidos en una tabla similar a la Tabla 11.

Tabla 11. Marcos de tiempo.

Marco de Tiempo.	Categoría
Dentro de 1 mes	Corto Plazo
Dentro de 6 meses	Mediano Plazo
Dentro de 1 año	Largo Plazo



Elemento del Plan de Gestión de Riesgos: la Tabla 11 se documenta en el plan de Gestión de Riesgos.

La unidad de tiempo de los valores seleccionados para el marco de tiempo debe estar en concordancia con la unidad seleccionada para la estimación del impacto de los riesgos sobre el tiempo de duración del proyecto.

Los planes de respuesta tienen prioridad. Este es un valor numérico donde 0 es muy priorizado > 0 menos priorizado, con el fin de establecer un orden de importancia entre todos los planes de respuesta que sirve como orden de ejecución aunque no es obligatorio.

Para la determinación de la prioridad debe tenerse en cuenta sobre todo la prioridad del riesgo y su marco de tiempo. La prioridad de un plan (P) está dada por la prioridad del riesgo no cerrado más priorizado (p) de la lista de riesgos a los que este plan es aplicable, y el 20% del marco de tiempo de ese riesgo donde Corto Plazo = 1, Mediano Plazo = 2, Largo Plazo = 3, y el inverso del total de riesgos no cerrados a los que este plan es aplicable:

$$P = p + 0.2 t + \frac{1}{n}$$

Ecuación 4. Prioridad del plan de respuesta.

En base a la naturaleza del plan y la estrategia que representa, se documenta la propiedad: Tipo de Plan, con uno de los siguientes valores: (Mitigación, Contingencia, Explotación, Investigación, transferencia, compartimiento).

Monitoreo y Control.



- Grupo de monitoreo y control.



- Plan de Gestión de Riesgos.
- Conjunto de riesgos identificados.
- Conjunto de planes de respuesta.



- Conjunto de planes de respuesta a los riesgos (actualizados).
- Conjunto de riesgos identificados (actualizados).
- Resumen evaluativo.

Flujo de Trabajo.

El monitoreo y control comienza según lo definido en el plan de Gestión de Riesgos. Tiene como objetivo evaluar el estado de los riesgos identificados y los planes de respuesta. Durante este proceso se identificarán condiciones para iniciar planes de respuesta y se emitirán criterios valorativos sobre el estado de los riesgos en el proyecto. Al concluir este proceso se obtienen los planes de respuesta actualizados y un resumen evaluativo con las impresiones de la Gestión de Riesgos hasta el momento.

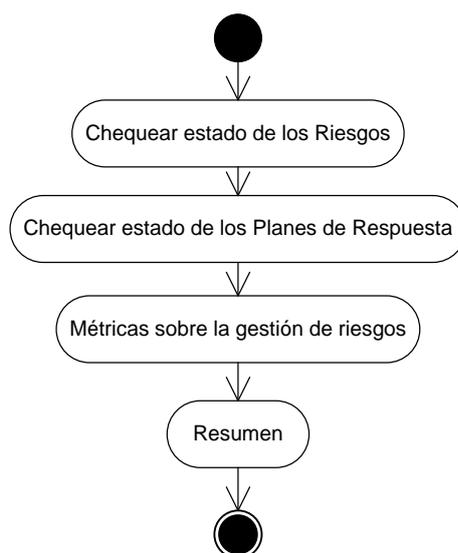


Figura 30. Flujo de trabajo de Monitoreo y Control.

Actividades.

1 – Chequear estado de los Riesgos.



Depende de la cantidad de riesgos y habilidades del grupo de monitoreo y control.



- Grupo de monitoreo y control.

La primera actividad que se realiza es un chequeo del estado de los riesgos existentes. Este chequeo consiste en revisar la lista de riesgos identificados, y en orden de prioridad, el grupo de monitoreo y control debe realizar las investigaciones pertinentes para descubrir si los valores de los atributos de cada riesgo han cambiado y en cuánto lo han hecho. Si se desea puede ejecutarse el proceso de identificación (ver página 46) donde se actualizarán los valores de los riesgos existentes y además se identificarán nuevos riesgos. El grupo de monitoreo puede utilizar técnicas como las que se describen a continuación:

1 – 1. Entrevistas



Sesiones de 45 minutos¹⁵.



- Grupo de monitoreo y control.
- Responsables de los riesgos.

¹⁵ La duración de cada entrevista individual varía de acuerdo al riesgo y a las discusiones.

El grupo de monitoreo comienza revisando los riesgos más priorizados. Para cada riesgo se entrevista con los responsables de ese riesgo y durante una sesión analizan en conjunto su estado actual. Los valores de sus propiedades se documentan en el formulario del riesgo junto con un resumen con las opiniones sobre las variaciones en la sección “Observaciones” del formulario del riesgo. El grupo adicionalmente se entrevista con otras personas que puedan aportar datos relevantes sobre el riesgo. Durante la entrevista son útiles preguntas como: ¿Cree que todavía está presente el riesgo?; ¿Ha variado su probabilidad de ocurrencia?, ¿cuánto?; ¿Ha variado su impacto?, ¿cuánto?

Al concluir la entrevista el grupo debe tener concreción sobre los cambios en los valores del riesgo. Todos los cambios se documentan y se mantienen los valores anteriores para el posterior análisis.

El proceso se repite para todos los riesgos.

2 – Chequear estado de los Planes de Respuesta.



Sesiones de 45 minutos.



- Grupo de monitoreo y control.

El grupo de monitoreo se reúne en sesiones de trabajo y analizan los planes de respuesta asociados a riesgos, teniendo en cuenta la prioridad de los mismos. Para cada plan, si este no estaba en ejecución, se observará si los tiempos y las condiciones de inicio son correctos para su ejecución, en tal caso se procederá con la ejecución del plan. El grupo de monitoreo y control solo es responsable de comunicar al líder de proyecto la necesidad de la ejecución del plan. Si el plan en análisis está siendo ejecutado, el grupo debe evaluar el estado de su ejecución con el uso de algunas de las técnicas propuestas (se recomiendan todas):

2 – 1. Evaluación de la efectividad del plan.

El grupo de monitoreo y control se reúne en sesiones de trabajo y analiza la efectividad del plan de respuesta. Nota: no se le calcula la efectividad a los planes de respuesta que no se hayan iniciado, o que estén concluidos y ya se les haya analizado su efectividad.

La efectividad de un plan es un elemento subjetivo a la dirección del proyecto, sin embargo sugerimos algunos criterios aplicables para la determinación de la efectividad del plan.

Criterio Cualitativo: Considerar un plan efectivo si modificó las probabilidades e impactos de los riesgos en valores notables y beneficiosos. Puede establecerse este criterio en el plan de Gestión de Riesgos, el criterio depende mucho de la dificultad de modificar los valores, y el significado del valor en sí, por ejemplo, puede que resulte muy difícil disminuir la probabilidad de ocurrencia de un riesgo, sin

embargo el plan lo redujo, mínimamente pero lo redujo entonces el plan fue efectivo; o puede que un plan redujo el impacto sobre el costo en un 1%, resultando \$100000 y por tanto se considere significativo.

Criterio Cuantitativo: se considera efectivo un plan de respuesta a amenazas (riesgos negativos) si al calcular el valor de efectividad (E) según lo descrito a continuación, se observan buenos criterios sobre este valor. **Aclaración:** La técnica asume que un plan efectivo es aquel que disminuye el impacto en un valor superior al costo de la disminución. Si se desea emplear este criterio debe tenerse en cuenta esta aclaración. Este criterio es aplicable al objetivo “Costo”, debe evaluarse si es efectivo para otros objetivos.

El grupo calcula la efectividad del plan sobre cada objetivo del proyecto evaluando la siguiente fórmula:

$$Efectividad = \frac{Impacto anterior - Impacto actual}{Costo de la respuesta}$$

Ecuación 5. Efectividad del plan de respuesta.

El “impacto anterior” refleja el valor numérico (antes de realizar el chequeo) asociado al impacto sobre el objetivo sobre el que se está analizando la efectividad del plan, “impacto actual” refleja el valor posterior al chequeo, el valor se documenta tal cual es, aunque sea igual. El “costo de la respuesta” indica, en la misma unidad y notación del impacto, cuánto ha costado hasta el momento la implementación de la respuesta. Por ejemplo si se evalúa la efectividad respecto al costo debe indicar el monto monetario hasta el momento.

Criterios sobre el valor de efectividad:

- Efectividad = 0 indica que el plan no ha causado efecto sobre el objetivo, el costo de la respuesta ha sido en vano.
- Efectividad < 0 indica que el plan no está siendo efectivo, pues no se ha logrado reducir el impacto o se ha reducido a un costo mayor que la reducción del impacto. Cuando esta condición se detecte debe documentarse notablemente para que se tomen las acciones pertinentes.
- Efectividad > 0 indica que el plan está siendo efectivo en alguna medida, pues ha logrado disminuir el impacto y en un costo menor al monto de la disminución.
- Efectividades mayores que las de chequeos anteriores indican que el plan continúa siendo efectivo.

El valor de efectividad calculado por uno u otro criterio se documenta en el plan analizado.

2 – 2. Reunión de estado de situación.

El grupo de monitoreo y la dirección del proyecto se reúne en sesión de trabajo (puede ser tratado en un punto en alguna reunión que tenga la dirección del proyecto y no convocar una reunión solamente para este tema), analizan el estado actual del proyecto y discuten sobre el estado de los planes de respuesta, las impresiones sobre los planes deben ser documentadas en cada uno y si se generan otras actividades para la respuesta a los riesgos sobre los que el plan es aplicable, debe documentarse en la sección adecuada del plan. Si se generan otras actividades de aseguramiento o control para ese plan, deben ser documentadas en los mecanismos de gestión del proyecto pero deben ser referenciadas en las observaciones del propio plan.

2 – 3. Análisis de la reserva.

El grupo de monitoreo y la dirección del proyecto se reúne en sesión de trabajo (puede ser tratado un punto en alguna reunión que tenga la dirección del proyecto y no convocar una reunión solamente para este tema) y analizan el impacto de los planes de respuesta sobre las reservas de tiempo y dinero destinadas a la respuesta a los riesgos. Se debe evaluar de los planes en ejecución si la utilización de estos recursos ha sido efectiva y eficiente, y en caso que se considere necesario se debe ajustar el uso de estos recursos en las actividades del plan para que se ajuste a lo destinado, o modificar la cantidad de los recursos disponibles. En ese caso debe actualizarse el plan de Gestión de Riesgos con los presupuestos y reservas acordados. Para los planes no en ejecución debe analizarse estos valores de acuerdo a la tendencia en los planes que están en ejecución y realizar los mismos ajustes pertinentes.

3 – Métricas sobre la Gestión de Riesgos.



Sesiones de 45 minutos¹⁶.



- Grupo de monitoreo y control.

El grupo de monitoreo analiza los nuevos datos de los riesgos identificados y los planes de respuesta analizados con el objetivo de determinar algunas métricas sobre el estado de la Gestión de Riesgos para su posterior análisis. El equipo se centra en determinar los siguientes elementos:

¹⁶ La duración de cada entrevista individual varía de acuerdo al riesgo y a las discusiones.

Tabla 12. Métricas sobre la Gestión de Riesgos.

Métrica	Valor
Número de riesgos identificados	
Número de riesgos no cerrados	
Numero de riesgos con prioridad Alta	
Efectividad promedio de los planes de respuesta para los riesgos de alta prioridad.	
Efectividad promedio de todos los planes de respuesta	

Nota: la descripción de estos elementos es trivial.

4 – Resumen.



Sesiones de 45 minutos.



- Grupo de monitoreo y control.

Al concluir el proceso el grupo de monitoreo y control se reúne en sesión de trabajo para elaborar un resumen con el estado de los riesgos y planes de respuesta.

Si durante el análisis se detectaron consideraciones de riesgos que ya no están presentes, debe analizarse y en caso que se considere ya no están presentes realmente, se marcan como Cerrado. A los planes asociados a los riesgos cerrados debe actualizárseles su prioridad.

En el resumen se incluyen las métricas calculadas y es muy útil confeccionar gráficos utilizando los datos antiguos que muestren las diferencias respecto a chequeos anteriores. Se recomiendan gráficos para los datos actuales y para observar las variaciones.

Para los gráficos de datos actuales se recomienda un gráfico de pastel para “Número de riesgos no cerrados” y “Número de riesgos con prioridad Alta” respecto al total de riesgos como muestra la Figura 31



Figura 31. Ejemplo de reporte de riesgos cerrados (izquierda) y riesgos de alta prioridad (derecha).

Para observar las variaciones de los elementos: “Número de riesgos identificados”, “Efectividad promedio de los planes de respuesta para los riesgos de alta prioridad” y “Efectividad promedio de todos los planes de respuesta” se recomienda el uso de gráficos de líneas que muestren el estado respecto a los datos anteriores como muestra la Figura 32

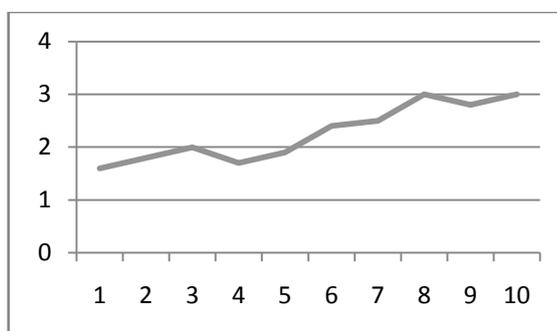


Figura 32. Ejemplo de gráfico para observar las variaciones respecto a los datos anteriores.

En el resumen se incluye una valoración sobre el estado de la Gestión de Riesgos donde se describe las impresiones sobre la efectividad de los planes, la eficacia del trabajo en la Gestión de Riesgos y recomendaciones sobre cambios en el proceso actual. Durante cada ejecución de este proceso a lo largo del proyecto se obtendrán estos resúmenes que se archivan junto con el resto de la documentación y se analizan concluir el proyecto.

El resumen se muestra al gerente de proyecto y si se considera se debe informar a todo el proyecto sobre el estado actual de la Gestión de Riesgos.

Evaluación y Aprendizaje.



- Grupo de Gestión de Riesgos.
- Líder de proyecto.



- Plan de Gestión de Riesgos.
- Conjunto de riesgos identificados.
- Planes de respuesta.
- Lista de riesgos comunes.
- Respuestas comunes a riesgos.
- Conjunto de planes de respuesta.
- Lecciones aprendidas.
- Resúmenes parciales del proceso Monitoreo y Control.



- Lista de riesgos comunes.
- Respuestas comunes a riesgos.
- Lecciones aprendidas.
- Resumen de la Gestión de Riesgos.

Flujo de Trabajo.

Este proceso comienza al concluir el proyecto, tiene como objetivo analizar la Gestión de Riesgos y extraer el conocimiento adquirido, las experiencias y documentarlo para su uso satisfactorio en otros proyectos y futuras ediciones de la Gestión de Riesgos.

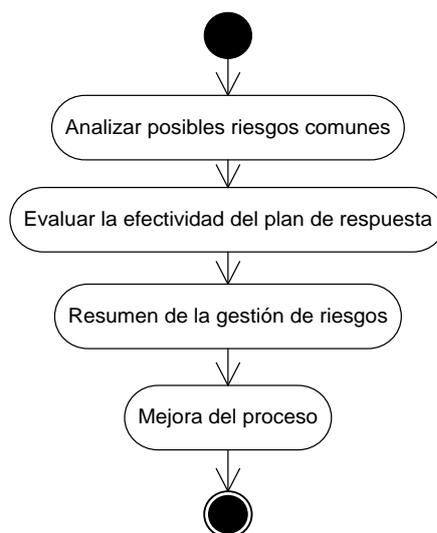


Figura 33. Flujo de trabajo de Evaluación y Aprendizaje.

Actividades.

1 – Analizar posibles riesgos comunes.



Sesiones de 45 minutos.

El grupo de Gestión de Riesgos se reúne en sesiones de trabajo y analizan los riesgos identificados en este proyecto, si los son riesgos comunes se actualiza en el documento Lista de Riesgos Comunes (ver Anexo5 – Lista de Riesgos Comunes Ver página 107) la frecuencia de aparición del riesgo. Esta frecuencia indica en cuántos proyectos ha aparecido este riesgo respecto al total de proyectos realizados. No es la frecuencia del riesgo en sí dentro del proyecto.

Si el riesgo no existía en el documento, este se adiciona y se especifica la frecuencia y etapa del proyecto en que generalmente aparece este riesgo.

El posterior análisis de este documento ayudará en la identificación de los riesgos y en la elaboración de planes de respuesta más efectivos.

2 – Evaluar la efectividad del plan de respuesta.



Sesiones de 45 minutos.

El grupo de Gestión de Riesgos se reúne en sesiones de trabajo y analizan a todos los planes de respuesta evaluando su efectividad. Para el cálculo de la efectividad se debe utilizar la técnica “Evaluación de la efectividad del plan” descrita en la página 74.

Los planes analizados deben referenciarse en el documento “Lecciones Aprendidas” (ver Anexo6 – Lecciones Aprendidas Página 112) junto con la efectividad y comentarios útiles para el futuro uso de esta información. Debe actualizarse su frecuencia de efectividad. Este valor de frecuencia indica cuántas veces este plan ha sido efectivo del total de veces que ha sido aplicado.

3 – Resumen de la Gestión de Riesgos.



Sesiones de 45 minutos.

El resumen de la Gestión de Riesgos tiene 3 momentos:

1 – **Elaboración del resumen:** (60 minutos) El grupo de Gestión de Riesgos se reúnen en una sesión de trabajo y realizan un resumen preliminar de la Gestión de Riesgos que se documenta en “Lecciones Aprendidas”, este resumen es una descripción textual de las experiencias positivas o negativas muy notables de este proyecto en cuanto a Gestión de Riesgos. Debe ser una descripción que ayude a futuros proyectos, deben ser enunciados cortos y precisos sobre la idea que se desee transmitir. La principal fuente para este resumen son los resúmenes elaborados en cada ejecución del proceso Monitoreo y Control.

2 – **Preparación de la reunión:** (20 minutos) el equipo se prepara para una reunión con todo el proyecto. Para esta reunión el grupo debe llevar una presentación donde se refleje: cantidad de riesgos identificados, categorías con más riesgos, efectividad de los planes de Gestión de Riesgos; además se incluyen los elementos significativos que se incluyeron preliminarmente en el resumen.

3 – **Reunión con el proyecto:** (45 minutos) El proyecto se reúne y se comenta lo analizado durante la elaboración del resumen preliminar, las opiniones del resto del proyecto contribuyen al resumen, deben analizarse las proposiciones de todos los involucrados en el proyecto, el conductor de esta reunión debe guiar la discusión en el siguiente sentido:

- Mostrar los resultados de la Gestión de Riesgos:
- Mostrar el resumen preliminar.
- Recoger los comentarios de todo el proyecto. Son útiles preguntas como:
 - o ¿Nos ayudó la Gestión de Riesgos?
 - o ¿Fluyeron bien los procesos?
 - o ¿Dónde tenemos debilidades?

4 – **Elaboración del resumen final:** (20 minutos) el grupo de Gestión de Riesgos se reúne y analizan los comentarios emitidos por el personal del proyecto y las impresiones del encuentro. Finalmente se elabora el resumen de la Gestión de Riesgos con las mismas características descritas en el paso 1.

4 – Mejora del Proceso.



20 minutos.

El grupo de Gestión de Riesgos se reúne en sesión de trabajo y analiza el resumen de la Gestión de Riesgos, las impresiones de la reunión y discuten formas de mejorar los procesos de la Gestión de Riesgos.

La mejora incluye acciones organizativas, operativas, externas a la Gestión de Riesgos o modificaciones a los procesos, actividades y técnicas de la Gestión de Riesgos. En estos casos se debe actualizar el modelo, haciendo las modificaciones pertinentes, consultar la sección Extensión del modelo (*ver página 89*) que contiene las políticas de modificación del modelo.

Roles y sus Responsabilidades

La siguiente tabla resume las responsabilidades de los roles ajenos a la Gestión de Riesgos, léase roles de la gestión de proyectos.

Tabla 13. Roles y responsabilidades.

Rol	Responsabilidades más importantes.
Líder de Proyecto	Elaborar el plan de Gestión de Riesgos. Incorporar los recursos, tiempo y presupuesto requerido para ejecutar el plan de Gestión de Riesgos en el plan de proyecto general. Incorporar las actividades generadas durante la Gestión de Riesgos en el plan de actividades general del proyecto y controlar su ejecución. Decidir las políticas y valores de los elementos de las técnicas a utilizar y decidir en las estrategias y planes de respuesta a riesgos. Participar en los análisis pertinentes.
Planificador	Incluir las actividades generadas en la Gestión de Riesgos en los mecanismos de planificación del proyecto.
Clientes	Definir criterio de éxito del proyecto y participar en la definición de los objetivos del proyecto. Participar en la identificación de los riesgos.
Económico	Colaborar en la definición del presupuesto para la Gestión de Riesgos y para las actividades de respuesta a riesgos. Participar en el análisis del impacto de los riesgos.
Aseguramiento de la calidad	Participar en la creación del plan de Gestión de Riesgos Velar por el ajuste al modelo durante su aplicación.
Recursos Humanos	Confecionar grupo de Gestión de Riesgos.
Resto del proyecto	Participar activamente en la Gestión de Riesgos especialmente en los procesos de identificación y monitoreo.

Artefactos

La siguiente tabla resume los artefactos utilizados durante la Gestión de Riesgos ilustrando su función en cada proceso (entrada, o salida).

Tabla 14. Artefactos del modelo.

Artefactos	Planeación	Identificación	Análisis Cualitativo	Análisis Cuantitativo	Planeación de la Respuesta	Monitoreo y Control	Evaluación y Aprendizaje
Plan de Gestión de Riesgos	S	E	E	E	E	E	E
Objetivos del proyecto		E					
Criterio de éxito del proyecto		E					
Lista de Riesgos Comunes		E					E S*
Conjunto de riesgos identificados		S	E S*	E S*	E	E S*	E
Lecciones Aprendidas					E		E S*
Respuestas comunes a riesgos					E		E S*
Conjunto de planes de respuesta					S	E S*	E
Resumen evaluativo						S	E S*

E = Entrada, **S** = Salida, **S*** = Salida Actualizada.

Resumen

La siguiente tabla describe un resumen de la Gestión de Riesgos recogiendo de cada proceso sus entradas, participantes, actividades y técnicas asociadas y las salidas generadas.

Tabla 15. Resumen del modelo.

Proceso	Entradas	Participantes	Actividades	Técnicas	Salidas
Planeación.		Líder de proyecto. Asesor de calidad. Encargado de recursos humanos. Económico. Planificador.	Creación del grupo de Gestión de Riesgos. Elaboración del plan de Gestión de Riesgos. Inclusión del plan de Gestión de Riesgos en el plan de proyecto general.		Plan de Gestión de Riesgos.
Identificación.	Plan de Gestión de Riesgos. Objetivos del proyecto. Criterio de éxito del proyecto. Lista de Riesgos Comunes.	Grupo de identificación. Líder de proyecto. Todos los involucrados en la Gestión de Riesgos. Organizador de la Gestión de Riesgos	Inicio de la identificación.		Conjunto de riesgos identificados.
			Realización de la identificación.	Técnica de Entrevistas. Técnica de Trabajo en Grupo: Tormenta de Ideas. Técnicas basadas en el conocimiento (Revisión de los riesgos conocidos).	
			Cierre de la Identificación.		
Análisis Cualitativo.	Conjunto de riesgos identificados. Plan de Gestión de Riesgos.	Grupo de análisis. Líder de proyecto.	Evaluación del Riesgo.	Tabla Fija de Probabilidades. Métrica de Frecuencia. Tabla Fija de Impactos. Tabla Fuzzi de Impactos. Incertidumbre de la información del	Conjunto de Riesgos identificados (Actualizados).

				riesgo.	
			Priorización de los riesgos.	Matriz de Probabilidad e Impacto. Técnicas Estadísticas. Suma Ponderada. Incertidumbre de la información del riesgo.	
Análisis Cuantitativo.	Conjunto de riesgos identificados. Plan de Gestión de Riesgos.	Grupo de análisis. Líder de proyecto	Escoger riesgos más priorizados Analizar riesgo cuantitativamente	Entrevistas Juicio de expertos	Conjunto de riesgos identificados (actualizados)
Planeación de la Respuesta.	Plan de Gestión de Riesgos. Conjunto de riesgos identificados. Lecciones aprendidas. Respuestas comunes a riesgos.	Grupo de análisis. Líder de proyecto.	Analizar Riesgo y decidir estrategia.	Evitar, Transferir, Mitigar. Explotar, Compartir, Mejorar.	Conjunto de Planes de respuesta. Conjunto de riesgos identificados (actualizados)
			Revisar Respuestas Comunes a Riesgos Revisar Lecciones Aprendidas Elaborar plan de respuesta		
Monitoreo y Control.	Plan de Gestión de Riesgos. Conjunto de riesgos identificados. Conjunto de planes de respuesta.	Grupo de monitoreo y control.	Chequear estado de los Riesgos.	Entrevistas.	Planes de Respuesta Actualizados. Resumen Evaluativo.
			Chequear estado de los Planes de Respuesta.	Evaluación de la efectividad del plan. Reunión de estado de situación. Análisis de la reserva.	
			Resumen.		
Evaluación y Aprendizaje.	Plan de Gestión de Riesgos. Conjunto de	Grupo de Gestión de Riesgos.	Analizar posibles riesgos comunes. Evaluar la		Lista de riesgos comunes.

	riesgos identificados. Planes de respuesta. Lista de riesgos comunes. Respuestas comunes a riesgos. Conjunto de planes de respuesta. Lecciones aprendidas. Resúmenes parciales.	Líder de proyecto.	efectividad del plan de respuesta. Resumen de la Gestión de Riesgos. Mejora del proceso.		Respuestas comunes a riesgos. Lecciones aprendidas. Resumen de la Gestión de Riesgos
--	---	--------------------	--	--	--

Grado de terminación

El grado de terminación del modelo le permite ser aplicable a proyectos productivos de software en la universidad. El modelo describe todos los procesos y actividades necesarias durante la Gestión de Riesgos cubriendo todo el ciclo de vida del proyecto, y explica las técnicas aplicables en cada actividad. Esta información, unida a la explicación de qué roles realizan las actividades, en qué momento del proyecto y qué artefactos se utilizan y generan, es suficiente para su aplicación por lo que se puede considerar que el modelo está bastante completo.

No obstante quedan muchos elementos por concluir y ampliar por ejemplo: mejor presentación gráfica de los artefactos, elaboración de perfiles de acuerdo al tipo de proyecto que recojan: ajustes en los tiempos de las actividades, configuraciones de las técnicas a utilizar, conjunto de riesgos preliminares etc. Más detalles de los elementos por concluir se pueden encontrar en la sección de Recomendaciones (*ver página 91*).

Ventajas y desventajas respecto a otros modelos

A continuación se describen ventajas y desventajas de este modelo para ser aplicado en la UCI respecto a otros como: PMBOK®, el modelo de Boehm, el modelo de Hall, Continuous Risk Management, Microsoft Solutions Framework, y otros métodos y técnicas como Software Risk Evaluation, y Taxonomy Based Risk Identification.

Claridad: este modelo está descrito con el objetivo de guiar a sus usuarios en su aplicación. Cada descripción de proceso, actividad o técnica está orientada a proveer un camino de la forma más práctica posible hacia una aplicación satisfactoria. El modelo describe claramente cuáles artefactos se

utilizan, cómo interactuar con ellos, cómo se confeccionan, cómo realizar los procesos, cómo ejecutar las actividades, cuánto tiempo estimado se empleará para ello, qué elementos son configurables y extensibles, cómo extenderlo. El modelo está descrito utilizando una estructura jerárquica simple para no perder al lector. Contiene elementos gráficos para ayudar en su claridad. En este sentido la mayoría de los modelos y técnicas carecen de explicación clara. Los trabajos del SEI tienen un enfoque diferente, aunque inferior a este modelo, excepto Software Risk Evaluation que presenta su información de una forma muy coherente, clara y organizada.

Complejidad: la generalidad de los modelos estudiados, al igual que el propuesto, no presentan alta complejidad en cuanto a su fundamento, la estructura de los procesos involucrados etc. sin embargo se aprecia un cierto nivel de complejidad de un modelo a otro, dado principalmente por su forma descriptiva y la complejidad propia de las técnicas que define. La forma descriptiva de este modelo, aunque tributa a la complejidad, se comenta en el enunciado anterior, la complejidad de las técnicas del modelo propuesto respecto a otros modelos, métodos y técnicas en sí, es un aspecto importante a comparar.

El modelo propuesto define un conjunto de técnicas aplicables a las actividades de cada proceso, adaptadas de otros autores o propuestas por los autores de este modelo. A las técnicas se les reduce la complejidad al detallar cómo aplicarla y cómo se integra con el resto de los elementos de la Gestión de Riesgos. En este sentido los otros modelos estudiados, al no describirlas de esta forma, y en muchos casos hacerlo muy abstracto como el PMBOK®, aumenta la complejidad de las técnicas.

Cubrimiento de todas las etapas del proyecto: el modelo se concibe para aplicarse durante todas las etapas del proyecto, describe cuándo comienza cada proceso y ofrece sugerencias sobre el nivel de actividad durante el ciclo de vida del proyecto, para guiar a los organizadores de la Gestión de Riesgos en su aplicación. En este sentido los otros modelos estudiados no especifican la relación que guarda la Gestión de Riesgos con las etapas del proyecto, no ofrecen sugerencias o recomendaciones sobre en qué etapa de proyecto deben ejecutarse los procesos.

Descripción de los roles: el modelo propuesto describe en cada proceso y actividad los roles participantes, roles de la Gestión de Riesgos y de la gestión de proyectos como: líder de proyecto, económico, planificador, encargado de recursos humanos. Se describen las tareas que realizan cada uno de estos roles y las responsabilidades que tienen dentro de la Gestión de Riesgos. Los modelos estudiados no definen roles concretos y con responsabilidades asignadas para la ejecución de la Gestión de Riesgos. Sin embargo el método SRE sí incluye esta característica, destacando la participación y responsabilidades de cada miembro definido con una admirable precisión y descripción.

Descripción de los artefactos: el modelo propuesto describe los artefactos generados e incluye plantillas de ejemplo usables en los anexos, por ejemplo: Plan de Gestión de Riesgos, taxonomía del desarrollo de software, cuestionario para la identificación, plan de respuesta de riesgo, modelo para documentar el riesgo. Durante la descripción de los procesos se referencia cuáles documentos se usan como entrada, como salida, qué elemento del documento se escribe, cuándo se hace y por quién se

hace. En este sentido el modelo tiene un aspecto positivo a diferencia del resto de los modelos que mencionan conceptualmente los artefactos generados sin ejemplificar o aportar valores utilizables. Los modelos existentes no cubren este aspecto.

Aplicabilidad: el modelo propuesto es aplicable solamente a proyectos productivos de software como se describe en la sección Alcance del Modelo (*ver página 36*) pues propone categorías de riesgos, métodos de identificación y otros elementos solamente aplicables a la industria del software y más específicamente a proyectos de la universidad. El modelo tiene como objetivo ayudar en la Gestión de Riesgos para la universidad. Una extensión del modelo para que sea aplicable a otros entornos conllevará a una pérdida de personalización y ayuda en la Gestión de Riesgos. El resto de los modelos analizados, al ser genéricos, son aplicables a otros tipos proyectos desarrollados en otros entornos, léase construcción, educación, finanzas etc. El modelo propuesto especifica con la mayor claridad posible su alcance para evitar confusiones en este sentido.

Otros criterios sobre el modelo: el modelo orienta los procesos de Gestión de Riesgos, sus actividades y técnicas hacia la mejora de las oportunidades y la mitigación de los factores que pueden provocar fracaso. Centra la explicación de sus técnicas (de identificación, análisis, medición y control) en los objetivos de tiempo y costo principalmente sirviendo como una herramienta para asegurarlos en alguna medida. El modelo concibe una serie de estrategias en respuesta a los riesgos donde se contempla la contingencia, la mitigación etc. El elemento más débil del modelo propuesto son las técnicas de análisis cuantitativo, ya que para explicar objetivamente las técnicas para determinar el impacto real de los riesgos sobre los objetivos del proyecto, de forma tal que sirva como guía es necesario el conocimiento de muchos factores muy propios del proyecto y del riesgo en sí.

Evolución del modelo

Se espera que el modelo se comporte como describe la Figura 34. Primeramente una consciente aplicación y mejora continua en varios proyectos productivos donde se enriquezca la base de conocimientos, se adquiera experiencia en su uso, se descubran mejores técnicas o mecanismos para realizar los procesos. Luego cuando el modelo se establezca y su uso sea una tarea cotidiana, se espera la elaboración de un sistema informático como se recomienda posteriormente. Y con el paso del tiempo es necesaria la definición de niveles de madurez de aplicación del modelo, donde se definan los criterios para considerar si un proyecto o la universidad están realizando una Gestión de Riesgos inconsciente (donde los riesgos sean ignorados o se resuelvan según aparecen), intuitiva (donde primitivamente se recoja la lista de riesgos pero no se aplique un proceso de gestión adecuado), planificada (donde con la utilización de un modelo con guías y procedimientos gestionen los riesgos), objetiva (donde una práctica consciente de la gestión de riesgo traiga valor observable para los proyectos) y óptima (donde los resultados de la Gestión de Riesgos se utilicen para realizar cambios organizacionales y estructurales).

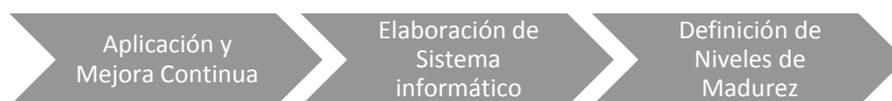


Figura 34. Evolución futura del modelo.

Extensión del modelo

El modelo incluye varios puntos de extensibilidad destinados principalmente a la inclusión de nuevas técnicas para la realización de las actividades. Este modelo propone un conjunto de técnicas explicando cómo utilizarlas y cómo se relacionan con el proceso general de Gestión de Riesgos. Existen muchas otras técnicas que se pueden aplicar.

En caso que se desee incluir técnicas al modelo, debe respetarse el *look-and-feel* de este documento, especificando tiempo estimado de duración de la aplicación de la técnica, quiénes participan, qué artefactos utiliza y cuáles genera, cómo se comunica con el resto de las actividades, qué elementos hay que incluir en el plan de Gestión de Riesgos. Los anexos de las técnicas que lo requieran deben incluirse en la sección adecuada. Los ejemplos utilizados deben tener datos con sentido y usables en el mejor de los casos.

Conclusiones Parciales

En este capítulo se continúa dando cumplimiento al segundo objetivo relacionado con la confección del modelo explicando el segundo grupo de procesos: Planeación de la Respuesta, Monitoreo y Control, Evaluación y Aprendizaje donde se adaptan técnicas como entrevistas, reunión del estado de situación, análisis de la reserva, y se proponen técnicas como la evaluación de la efectividad del plan y métricas para el Monitoreo y Control. Se resumen los roles y responsabilidades, los artefactos generados y el modelo en general. En cumplimiento al tercer objetivo se emite una valoración crítica del modelo atendiendo a semejanzas y diferencias respecto a otros modelos analizados.

Conclusiones

Se realizó un estudio del estado del arte acerca de los diferentes enfoques para la Gestión de Riesgos en los procesos de desarrollo de software en cumplimiento al primer objetivo trazado y se arriba a las siguientes conclusiones:

- La generalidad de los modelos analizados reconocen como procesos definidos en la Gestión de Riesgos los siguientes: Planeación, Identificación, Análisis, Planeación de la Respuesta, Control y Seguimiento pero tienen deficiencias para su aplicación en la UCI al definir la comunicación entre los procesos de acuerdo a su secuencia, simultaneidad y roles involucrados.
- Los modelos analizados con frecuencia constituyen guías abstractas que necesitan ser adaptadas para su aplicación a entornos específicos, y en la mayoría de los casos las técnicas que proponen en los casos analizados son genéricas y aparecen insuficientemente descritas en este sentido.
- Se identifica la representación de los riesgos como una de las deficiencias principales para su aplicación en la UCI, dificultando ello lograr un control íntegro del riesgo y conocimiento de su estado en todo momento.
- Las oportunidades no son adecuadamente gestionadas y la mayoría de los modelos analizados tienen deficiencias en las métricas para el control y seguimiento de los riesgos.

Se desarrolló un modelo para la Gestión de Riesgos, aplicable a los proyectos de desarrollo de software desarrollados en entornos productivos similares al de la Universidad de las Ciencias Informáticas, que mejora las insuficiencias de los modelos existentes para ser aplicados en dichos entornos, dando cumplimiento al segundo objetivo propuesto y se realizó una evaluación crítica del modelo a partir de la comparación con otros modelos analizados. Finalmente se concluye:

- La complejidad del modelo propuesto es similar a la del resto de los modelos analizados durante el estudio del estado del arte.
- El modelo propuesto en la tesis incluye nuevos procesos como el aprendizaje y la etapa de análisis se presenta con una clara definición de análisis cualitativo y análisis cuantitativo.
- Respecto a la claridad el modelo propuesto se explica con mayor claridad que los modelos analizados a diferencia de SRE que presenta una claridad similar al modelo propuesto.
- La propuesta desarrollada cubre completamente todas las etapas del proyecto y define roles y artefactos objetivamente a diferencia de los modelos.
- Este modelo está ajustado para el caso de desarrollo de proyectos de software pero de forma general el flujo de trabajo del mismo y algunas de las técnicas que relaciona son aplicables a otros tipos de proyectos.
- El modelo mantiene un enfoque en los objetivos de tiempo, costo y contempla la recuperación ante contingencias y mitigación de los factores que pueden provocar el fracaso.

Recomendaciones

1. Aplicar continuamente el modelo en varios proyectos productivos de software para valorar su desempeño y ajuste a las necesidades individuales.
2. Mejorar la usabilidad del modelo confeccionando versión electrónica de los artefactos propuestos, describiendo en detalle las técnicas y actividades.
3. Elaborar curso de capacitación de 2 niveles, Nivel 1: curso introductorio donde todo el personal del proyecto entienda los principios y conceptos de la Gestión de Riesgos, entiendan cuál será su papel dentro del proceso, su importancia, y actividades que se realizarán. Nivel 2: (incluye Nivel 1) curso en profundidad donde se enseñe a utilizar este modelo, el grupo de Gestión de Riesgos debe conocerlo en detalle y profundidad.
4. Elaborar sistema informático que ayude en la generación de los artefactos a partir del perfil de proyecto con valores predefinidos basados en el proceso de aprendizaje, asista en la configuración de las técnicas seleccionadas y proponga riesgos durante la identificación.

Bibliografía

1. **Lovejoy, Kristin Gallina.** The Evolution of Operational Risk Management. *Sarbanes-Oxley : Technology / Risk Managemen.* [En línea] 31 de Marzo de 2005. [Citado el: 13 de Enero de 2008.] <http://www.s-ox.com/Feature/detail.cfm?ArticleID=733>.
2. **Perminova, Olga, Gustafsson, Magnus y Wilkström, Kim.** Defining uncertainty in projects – a new perspective. *Science Direct - International Journal of Project Management* 26 (2008) 73-79. [En línea] 30 de Julio de 2007. [Citado el: 13 de Enero de 2008.] http://www.sciencedirect.com/science?_ob=MIimg&_imagekey=B6V9V-4PTN90M-1-1&_cdi=5908&_user=2342189&_orig=browse&_coverDate=01%2F31%2F2008&_sk=999739998&view=c&wchp=dGLzVlz-zSkWA&md5=a067a926e674f20ce70fdc928a7e2574&ie=/sdarticle.pdf.
3. **Söderholm, Anders.** Project management of unexpected events. *Science Direct - International Journal of Project Management* 26 (2008) 73-79. [En línea] 31 de Julio de 2007. [Citado el: 13 de Enero de 2008.] http://www.sciencedirect.com/science?_ob=MIimg&_imagekey=B6V9V-4R05JCV-1-1&_cdi=5908&_user=2342189&_orig=browse&_coverDate=01%2F31%2F2008&_sk=999739998&view=c&wchp=dGLzVlz-zSkWA&md5=607ff88974a6348aa8e593e282f21418&ie=/sdarticle.pdf.
4. **Nocco, Brian W. and Stulz, Rene M.** *Enterprise Risk Management: Theory and Practice.* Julio 2006.
5. **Fredriksen, Veronica.** Do companies need Risk Management? . *Developer Eye.* [En línea] 25 de Marzo de 2005. [Citado el: 13 de Enero de 2008.] http://www.developereye.com/info_view.aspx?id=37492.
6. **Boch, Grady.** *Object Oriented Programming, analisis and design with applications.* s.l. : Adison Wesley, 1996.
7. **Addison, Tom y Vallabh, Seema.** *Controlling Software Project Risks – an Empirical Study of Methods.* s.l. : University of the Witwatersrand y KPMG, 2002.
8. *Risk Management for Information Systems Development.* **Powell, P.L. y J.H., Klein.** 309-319, s.l. : Journal of Information Technolog, 1996, Vol. 11.
9. **Boehm, B.W.** *Software Risk Management: Principles and Practices.* s.l. : IEEE Software, 1991.
10. **Project Management Institute.** *A Guide to the Project Management Body of Knowledge (PMBOK).* Pennsylvania : Project Management Institute, 2000. ISBN: 1-880410-23-0.
11. **DrC. Pinero Perez, Pedro Y.** *Estado de los Proyectos Productivos.* Universidad de las Ciencias Informaticas, 16 de Enero de 2008.
12. **Guevara Delgado, Berenice, Ronda Pupo, Guillermo y Roque del Toro, Ana Josefa.** *Control de Gestión de Software de la Facultad Tres de la UCI. Diagnóstico de la Situación Actual.* La Habana : Universidad de las Ciencias Informáticas, 2007. TD-0285-07.

13. **López Pérez, Yusnay, Bauta Pacheco, Yuraimy y Delgado Martínez, Ramsés.** *Propuesta para aplicar el Modelo CMMI*. Ciudad de la Habana : Universidad de las Ciencias Informáticas, 2007. TD-0306-07.
14. **Aguiar Roque, Yainielys y García Armenteros, Aracelys.** *Caracterización de la Norma Internacional de Certificación de Productos ISO y valoración de su posible aplicación a los productos Informáticos de la UCI*. Ciudad de la Habana : Universidad de las Ciencias Informáticas, 2007. TD-0330-07.
15. **Pelaez Aguiar, Hanillilian, y otros.** *Procedimiento para el control y aseguramiento de la calidad en la Gestión de Proyectos*. Ciudad de la Habana : Universidad de las Ciencias Informáticas, 2007. TD-0376-07.
16. **Tabasco Reyes, Perla Mailen, Marrero Machín, Yadira y Cruz Águila, Lucy.** *Procedimiento para el control y aseguramiento de la calidad en los flujos trabajo Modelación del Negocio y Requerimientos de los proyectos de software de la Facultad 2 de la Universidad de las Ciencias Informáticas*. Ciudad de la Habana : Universidad de las Ciencias Informáticas, 2007. TD-0394-07.
17. **Macias Rojas, Onel y Flores López, Mariano.** *Propuesta para la Gestión de Proyectos durante el proceso de desarrollo de software en proyectos productivos de gestión en la UCI*. Ciudad de la Habana : Universidad de las Ciencias Informáticas, 2007. TD-0418-07.
18. **Figueredo Céspedes, Yelaine, y otros.** *Análisis y Gestión de Riesgo para el desarrollo de las aplicaciones del proyecto Atención Primaria de Salud (APS)*. Ciudad de la Habana : Universidad de las Ciencias Informáticas, 2007. TD-0687-07.
19. **Universidad de las Ciencias Informáticas.** *Procedimiento para diagnóstico de riesgos. Dirección de Producción1*. [En línea] 20 de Marzo de 2007. [Citado el: 20 de Febrero de 2008.] <http://dirproduccion1.uci.cu/polos-productivos/procedimientos-e-instrucciones/Procedimiento%20para%20el%20Diagnostico%20de%20Riesgos.doc/view>.
20. **Higuera, Ronald P. y Haimes, Yacov Y.** *Software Risk Management. Software Engineering Institute*. [En línea] Junio de 1996. [Citado el: 21 de Febrero de 2008.] <http://www.sei.cmu.edu/pub/documents/96.reports/pdf/tr012.96.pdf>. CMU/SEI-96-TR-012 ESC-TR-96-012.
21. **Central Computer and Telecommunications Agency.** *CRAM. CCTA Risk Analysis and Management Methodology*. [En línea] 2005. [Citado el: 19 de Febrero de 2008.] <http://www.cramm.com/overview/howitworks.htm>.
22. **Microsoft.** *MSF Risk Management Discipline. Microsoft Solution Framework*. [En línea] Junio de 2002. [Citado el: 10 de Febrero de 2008.] 602-i401a.
23. *A model and prototype tool to manage software projects risks.* **Keshlaf, A.A. y Hashim, K.** s.l. : Proceedings of First Asia–Pacific Conference. pp. 297–305.

24. **Yacoub, S.M. y Ammar, H.H.** *A methodology for architecture level reliability risk analysis*. s.l. : IEEE Transactions on Software, 2002. 28 (6), 529–547..
25. **Houmb, Siv Hilde y Georg, Geri.** The Aspect-Oriented Risk-Driven Development (AORDD) Framework. *Department of Computer and Information Science NTNU*. [En línea] 2005. [Citado el: 19 de Febrero de 2007.] <http://www.idi.ntnu.no/grupper/su/publ/siv/swde-2005-houmb.pdf>.
26. **Cuza García, Betsy, y otros.** *Gestión de Riesgos en el Proyecto de Informatización del Conocimiento Geológico en Cuba*. Ciudad de La Habana : Universidad de las Ciencias Informáticas., 2007. TD-0846-07.
27. **López Cabrera, Yanisleidy, Alvarez Lamas, Tailys y Fernández Pérez, Yamilis.** *Propuesta para la Gestión de Riesgo en los proyectos productivos de la UCI*. Ciudad de la Habana : Universidad de las Ciencias Informáticas, 2007. TD-0466-07.
28. **Crawford, Lynn.** From Global Standards to Global Communities of Practice. *PMFORUM*. [En línea] [Citado el: 10 de Febrero de 2007.] www.pmforum.org/gpmf/08/GPMF8_Crawford_Presentation.pdf.
29. **Society for Risk Analysis.** *SRA*. [En línea] 2000. [Citado el: 12 de Diciembre de 2007.] <http://www.sra.org>.
30. **Project Management Institute, inc.** Project Management Institute. [En línea] [Citado el: 19 de Febrero de 2008.] <http://www.pmi.org>.
31. **Carnegie Mellon University.** Software Engineering Institute. [En línea] [Citado el: 10 de Febrero de 2008.] <http://www.sei.cmu.edu>.
32. **Institute of Electrical and Electronics Engineers.** IEEE. [En línea] [Citado el: 20 de Febrero de 2008.] <http://www.ieee.org>.
33. **Microsoft Corporation.** Microsoft. [En línea] [Citado el: 19 de Febrero de 2008.] <http://www.microsoft.com>.
34. **International Standard Organization.** ISO. [En línea] [Citado el: 20 de Febrero de 2008.] <http://www.iso.org>.
35. **Society for Risk Analysis.** *SRA Journals*. *SRA*. [En línea] 2000. [Citado el: 12 de Diciembre de 2007.] <http://www.sra.org/journal.php>.
36. **Blackwell Publishing.** Risk Analysis: An International Journal - Journal Information. *Blackwell Publishing*. [En línea] 2006. [Citado el: 12 de Diciembre de 2007.] <http://www.blackwellpublishing.com/journal.asp?ref=0272-4332>.
37. **Rosenberg, Dr. Linda H., Hammer, Theodore y Gallo, Albert.** Continuous Risk Management. *NASA Software Assurance Technology Center*. [En línea] [Citado el: 22 de Febrero de 2008.] http://satc.gsfc.nasa.gov/support/ASM_FEB99/crm_at_nasa.html.

38. **Murphy, Richard L., y otros.** Continuous Risk Management Guidebook. *Software Engineering Institute*. [En línea] [Citado el: 20 de Febrero de 2008.] <http://www.sei.cmu.edu/publications/books/other-books/crm.guidebk.html>.
39. **Carr, Marvin J., y otros.** Taxonomy-Based Risk Identification. *Software Engineering Institute*. [En línea] 1993. [Citado el: 20 de Febrero de 2008.] <http://www.sei.cmu.edu/pub/documents/93.reports/pdf/tr06.93.pdf>.
40. **Williams, Ray C., y otros.** Software Risks Evaluation SRE. *Software Engineering Institute*. [En línea] Diciembre de 1999. [Citado el: 29 de Febrero de 2008.] <http://www.sei.cmu.edu/pub/documents/99.reports/pdf/99tr029-app.pdf> -. CMU/SEI-99-TR-029.
41. **Higuera, Ronald P., y otros.** An Introduction to Team Risk Management. *Software Engineering Institute*. [En línea] Mayo de 1994. [Citado el: 29 de Febrero de 2008.] <http://www.sei.cmu.edu/pub/documents/94.reports/pdf/sr01.94.pdf>. CMU/SEI-94-SR-1.
42. **Williams, Ray C.** New Directions in Risk Management at the SEI. *Software Engineering Institute*. [En línea] 2003. [Citado el: 5 de Marzo de 2008.] <http://www.sei.cmu.edu/risk/new-directions.pdf> .
43. **Higuera, R.P., y otros.** *An introduction to Team Risk Management*. s.l. : Software Engineering Institute, 1994. CMU/SEI-94-SR-1.
44. **Risk World.** Risk World. [En línea] [Citado el: 12 de Diciembre de 2007.] <http://www.riskworld.com>.
45. —. Risk Databases: a listing of databases regarding risk assessment, analysis, and management. *Risk World*. [En línea] [Citado el: 12 de Diciembre de 2007.] <http://www.riskworld.com/websites/webfiles/ws6aa003.htm>.
46. —. Risk Associations and Societies: profiles of a broad spectrum of risk-related organizations. *Risk World*. [En línea] [Citado el: 12 de Diciembre de 2007.] <http://www.riskworld.com/Organizations/Associations/risk.HTM>.
47. **Boehm, B.W.** *Software Risk Management*. s.l. : IEEE Computer Society Press, 1989. ISBN 0818689064.
48. **Data and Analysis Center for Software.** Formal Risk Management. *SOFTWARE ACQUISITION GOLD PRACTICE*. [En línea] [Citado el: 20 de Febrero de 2008.] <https://www.goldpractices.com/practices/frm/>.
49. **Hall, E.M.** *Managing Risk – Methods for Software Systems Development*. s.l. : Addison Wesley, 1997. ISBN 0201255928.
50. **Scoy, Van y L., Roger.** Software Development Risk: Opportunity, Not Problem. *Software Engineering Institute*. [En línea] Septiembre de 1992. [Citado el: 10 de febrero de 2008.] <http://www.sei.cmu.edu/publications/documents/92.reports/92.tr.030.html>.. CMU/SEI-92-TR-030.

51. **Committee for Oversight and Assessment of U.S. Department of Energy Project Management.** *The Owner's Role in Project Risk Management.* s.l. : The National Academies Press, 2005. ISBN: 0-309-54754-7.
52. **McConnell's, Steve.** *Software Project Survival Guide.* Redmond : Microsoft Press, 1998. ISBN: 1-57231-621-7.
53. **AS/NZS.** Risk Management. *Standards Australia.* Strathfield : s.n., 1999. AS/NZS 4360:1999.
54. **IEEE.** IEEE Std 1540-2001 IEEE Standard for Software Life Cycle Processes—Risk Management - Description. *IEEE Standards Association.* [En línea] IEEE. [Citado el: 20 de Febrero de 2008.] http://standards.ieee.org/reading/ieee/std_public/description/se/1540-2001_desc.html. 1540-2001.
55. **International Standard Organization.** ISO/IEC 16085:2006. *ISO.* [En línea] [Citado el: 20 de Febrero de 2008.] http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=40723. ISO/IEC 16085:2006.
56. **Alberts, Christopher J.** Common Elements of Risk. *SEI.* [En línea] 2006. [Citado el: 21 de Febrero de 2008.] <http://www.sei.cmu.edu/publications/documents/06.reports/06tn014.html>. CMU/SEI-2006-TN-014.
57. **Gluch, David P.** A Construct for Describing Software Development Risks. [En línea] Julio de 1994. [Citado el: 6 de Febrero de 2008.] <http://www.sei.cmu.edu/pub/documents/94.reports/pdf/tr14.94.pdf>. CMU/SEI-94-TR-14.
58. **Niwot Ridge Consulting.** Nine Best Practices. *The Software Management Framework.* [En línea] 3 de Junio de 1999. [Citado el: 12 de Febrero de 2008.] <http://www.niwotridge.com>. 720.406.9164.
59. **Fundibeq ANDES.** *CumbreB. Tormenta de Ideas.*
60. *Creativity for Operational Researchers.* **Vidal, Valqui y Victor, Rene.** Denmark : Technical University of Denmark, 2005.
61. **Gallagher, B.P., Alberts, C.J. y Barbour, R.E.** Software Acquisition Risk Management Key Process Area (KPA) – A Guidebook. [En línea] Agosto de 1997. [Citado el: 20 de Febrero de 2008.] <http://www.sei.cmu.edu/pub/documents/97.reports/pdf/97hb002.pdf>. CMU/SEI-97-HB-002.
62. **Walsh, K.R. y Schneider, H.** The Role of Motivation and Risk behaviour in Software Development Success. *Information Research.* [En línea] 2002. [Citado el: 12 de Diciembre de 2007.] <http://InformationR.net/ir/7-3/paper129.html>.
63. **Nieminen, Anu y Lehtonen, Mikko.** Organisational control in programme teams: An empirical study in change programme context. *Science Direct - International Journal of Project Management.* [En línea] 25 de Julio de 2007. [Citado el: 12 de Diciembre de 2007.]
64. **Kwak, Y.H. y Stoddardb, J.** Project risk management: lessons learned from software development environment. *Science Direct.* [En línea] 26 de Marzo de 2003. [Citado el: 13 de Enero de 2007.]

- http://www.sciencedirect.com/science?_ob=ArticleURL&_udi=B6V8B-487656Y-1&_user=2342189&_rdoc=1&_fmt=&_orig=search&_sort=d&view=c&_acct=C000056883&_version=1&_urlVersion=0&_userid=2342189&md5=701854b8c84c020ae10ff834b0ab64eb.
65. **Teague, By Paul E.** Best practices in risk management. *Purchasing*. [En línea] 14 de Julio de 2007. [Citado el: 13 de Enero de 2007.] <http://www.purchasing.com/article/CA6458520.html>.
66. **Universal Risk Project.** Universal Risk Project – Final Report. [En línea] [Citado el: 12 de Diciembre de 2007.] <http://opim-sun.wharton.upenn.edu/~carpen/316/PMI%20Risk%20Management%20SIG%20Project%20Report.pdf>.
67. **Piñero Pérez, Pedro Y.** *Afectaciones en los proyectos productivos*. Universidad de las Ciencias Informáticas, 20 de Enero de 2008.
68. **Risk Management, Software Technical Support Center (STSC).** Guidelines for Successful Acquisition and Management of Software-Intensive Systems (GSAM), Version 3.0, Capítulo 6. 2000.
69. **Meyers, B. Craig.** Risk Management Considerations for Interoperable Acquisition. *SEI*. [En línea] Agosto de 2006. [Citado el: 21 de Febrero de 2008.] <http://www.sei.cmu.edu/pub/documents/06.reports/pdf/06tn032.pdf>. CMU/SEI-2006-TN-032.
70. **CSO.** Risk Analysis Research Center - CSO Research Centers. *CSO Online*. [En línea] CXO Media Inc., 13 de Febrero de 2006. [Citado el: 12 de Diciembre de 2007.] <http://www.csoonline.com/research/risk/index.html>.
71. **Carbone, Thomas A.** Project Risk Management Using the Project Risk FMEA. *All Business*. [En línea] 1 de Diciembre de 2004. [Citado el: 12 de Febrero de 2007.] <http://www.allbusiness.com/management/886375-1.html>.
72. **Caltrans.** *Project Risks Management Handbook*. California : Office of Statewide Project Management Improvement (OSPMI), 2007.

Anexo1 – Plan de Gestión de Riesgos

Grupo de Gestión de Riesgos

Nombre	Organizador	G. Ident.	G. Analisis	G. Monit.	Operaciones

* Marcar con una X los roles a los que pertenece cada persona.

Planificación de las actividades

Planificación Guiada por Hitos:

Hito	Procesos a Realizar	Observaciones

Planificación Guiada por Tiempo:

Fecha	Procesos a Realizar	Observaciones

Otras Indicaciones de Planificación:

--

Presupuesto

Técnicas a utilizar

Actividades de aseguramiento para el plan.

Anexo2 – Taxonomía del Desarrollo de Software

- Ingeniería.
 - Requerimientos.
 - Estabilidad.
 - Completamiento.
 - Claridad.
 - Validez.
 - Factibilidad.
 - Precedentes.
 - Escala.
 - Diseño.
 - Funcionalidad.
 - Dificultad.
 - Interfaces.
 - Rendimiento.
 - Capacidad de probarse.
 - Restricciones de hardware.
 - Software de 3ras partes.
 - Código y Unidades de Prueba.
 - Factibilidad.
 - Pruebas de unidad.
 - Implementación.
 - Integración y Pruebas.
 - Ambiente.
 - Producto.
 - Sistema.
 - Especialidades.
 - Mantenimiento.
 - Fiabilidad.
 - Seguridad.
 - Factores humanos.
 - Especificaciones.
- Ambiente de Desarrollo.
 - Procesos de desarrollo.
 - Formalidad.
 - Adecuación.
 - Control.
 - Familiaridad.
 - Sistema de desarrollo.
 - Capacidad.
- Adecuación.
- Usabilidad.
- Familiaridad.
- Fiabilidad.
- Soporte.
- Entregas.
- Procesos de gestión.
 - Planeación.
 - Organización del proyecto.
 - Experiencia en la gestión.
 - Interfaces del programa.
- Métodos de gestión.
 - Monitoreo.
 - Gestión del personal.
 - Aseguramiento de la calidad.
 - Gestión de la configuración.
- Ambiente de Trabajo.
 - Actitud ante la calidad.
 - Cooperación.
 - Comunicación.
 - Moral.
 - Entusiasmo.
- Restricciones.
 - Recursos.
 - Cronograma.
 - Personal.
 - Presupuesto.
 - Facilidades.
 - Contrato.
 - Tipo de contrato.
 - Restricciones.
 - Dependencias.
 - Interfaces del programa.
 - Cliente.
 - Contratista.
 - Subcontratistas.
 - Contratista principal.
 - Vendedores.
 - Política.

Anexo3 – Cuestionarios para la Identificación

El siguiente cuestionario es utilizado para la identificación de riesgos. Por problemas de espacio se incluyen las preguntas hasta (Procesos de Gestión\Organización del proyecto). El resto de las preguntas se entregan en soporte electrónico.

A. Ingeniería

1. Requerimientos

a. Estabilidad

¿Mientras se desarrolla el producto hay requerimientos cambiantes?

¿Son estables los requerimientos?

(No) (1.a) ¿Cual es el efecto que provoca en el sistema los requerimientos cambiantes?

- Calidad
- Funcionalidad
- Planificación
- Integración
- Diseño
- Pruebas

[2] ¿Están cambiando las interfaces externas?

b. Completamiento.

[¿Hay requerimientos faltantes o están incompletas las especificaciones?]

[3] ¿En las especificaciones quedan elementos por ser definidos?

[4] ¿Conoce algunos requerimientos que deben estar en las especificaciones y no están?

(Si) (4.a) ¿Es posible realizar estos requerimientos en el sistema?

[5] ¿El cliente tiene requerimientos o expectativas que no han sido documentadas?

(Si) (5.a) ¿Hay alguna forma de capturar esos requerimientos?

[6] ¿Las interfaces externas están completamente definidas?

c. Claridad

[¿Existen requerimientos no claros o que necesitan interpretación?]

[7] ¿Eres capaz de entender los requerimientos que están escritos?

(No) (7.a) ¿Las ambigüedades están siendo resueltas satisfactoriamente?

(Si) (7.b) ¿Hay problemas de interpretación o ambigüedad en ellos?

d. Validez

[¿Los requerimientos conducirán al producto que el cliente tiene en mente?]

[8] ¿Existen requerimientos que tal vez no especifiquen lo que el cliente realmente quiere?

(Si) (8.a) ¿Cómo estás resolviendo esto?

[9] ¿Ambas partes están entendiendo lo mismo de los requerimientos?

(Si) (9.a) ¿Tienen un proceso para determinarlo?

[10] ¿Cómo se validan los requerimientos?

- Prototipado
- Analisis
- Simulaciones

e. Factibilidad

[¿Los requerimientos no son factibles desde un punto de vista analítico?]

[11] ¿Hay requerimientos difíciles de implementar técnicamente?

(Si) (11.a) ¿Cuán difícil?

(Si) (11.b) ¿Por qué son difíciles de implementar?

(No) (11.c) ¿Se hizo algún estudio de factibilidad con los requerimientos?

(Si) (11.c.1) ¿Cuan seguro estas de dicho estudio?

f. Precedentes

[¿Los requerimientos especifican algo que no se haya hecho anteriormente, o que la Universidad no haya hecho anteriormente?]

[12] ¿Hay algún estado del arte hecho de los requerimientos?

- Tecnologías
- Métodos
- Lenguajes
- Hardware

(No) (12.a) ¿Algunos son nuevos?

(Si) (12.b) ¿El programa tiene suficiente conocimiento en estas áreas?
 (No) (12.b.1) ¿Existe algún plan para adquirir conocimiento en estas áreas?

g. Escala

[Los requerimientos especifican un producto más grande o más complejo o requiere una organización mayor de lo que está acostumbrada la universidad]
 [13] ¿El tamaño y complejidad del sistema es una preocupación?
 (No) (13.a) ¿Se ha hecho algo antes de este tamaño y complejidad?
 [14] ¿El tamaño del sistema requiere una organización más grande que la acostumbrada?

2. Diseño

a. Funcionalidad

[¿Los problemas potenciales que se discuten son requerimientos funcionales?]
 [15] ¿Hay algún algoritmo especificado que tal vez no cumpla con los requerimientos?
 (No) (15.a) ¿Los algoritmos y diseño son marginales a los requerimientos?
 [16] ¿Cómo determinan la factibilidad de los algoritmos y diseño?
 • Prototipando
 • Modelando
 • Analizando
 • Simulando

b. Dificultad

[¿Es difícil de implementar el diseño?]
 [17] ¿Algo en el diseño depende de suposiciones irrealistas o optimistas?
 [18] ¿Hay algún requerimiento o funcionalidad que es difícil de diseñar?
 (No) (18.a) ¿Tienen soluciones para todos los requerimientos?
 (Si) (18.b) ¿Cuáles son los requerimientos difíciles de diseñar?
 • ¿Por qué son difíciles de diseñar?

c. Interfaces

[¿Las interfaces externas están bien diseñadas y controladas?]
 [19] ¿Las interfaces internas están bien diseñadas?
 • Software--software
 • Software-hardware
 [20] ¿Hay algún proceso para definir las interfaces internas?
 (Si) (20.a) ¿Hay algún proceso de control de cambios para las interfaces internas?
 [21] ¿Hay algún hardware siendo desarrollado paralelamente con el software?
 (Si) (21.a) ¿Las especificaciones del hardware están cambiando?
 (Si) (21.b) ¿Todas las interfaces hacia el software han sido diseñadas?
 (Si) (21.c) ¿Hay algún modelo ingenieril de diseño que puede ser usado para probar el software?

d. Rendimiento

[¿Hay requerimientos rigurosos de tiempo de respuesta o "throughput"?]
 [22] ¿Hay problemas con el rendimiento?
 • "Throughput".
 • Programación de eventos en tiempo real asíncronos.
 • Respuesta en tiempo real.
 • Línea de tiempo de recuperación.
 • Tiempo de respuesta.
 • Tiempo de respuesta de la base de datos, contención o acceso.
 [23] ¿Se ha realizado algún análisis de rendimiento?
 (Si) (23.a) ¿Cuál es tu nivel de confianza con ese análisis?
 (Si) (23.b) ¿Tienen un modelo para trazar el rendimiento desde el diseño hasta la implementación?

e. Capacidad de Probarse

[¿Es el producto difícil o imposible de probar?]
 [24] ¿El software será fácil de probar?
 [25] ¿El diseño incluye elementos que ayuden a probar el sistema?
 [26] ¿El personal de pruebas estuvo involucrado en el análisis de los requerimientos?

f. Restricciones de Hardware.

[¿Hay restricciones ajustadas en el hardware de destino?]

[27] ¿El hardware limita la habilidad de alcanzar algún requerimiento?

- Arquitectura
- Capacidad de memoria
- “Throughput”
- Respuesta en tiempo real
- Líneas de tiempo de recuperación.
- Rendimiento de las bases de datos
- Funcionalidad
- Fiabilidad
- Disponibilidad

g. Software de terceras partes.

[¿Hay algún software siendo usado que no es desarrollado por el equipo?]

Si existe software reutilizado.

[28] ¿Está siendo reutilizado algún software no desarrollado por el equipo?

(Si) (28.a) ¿Se prevé algún problema?

- Documentación
- Rendimiento
- Funcionalidad
- Entrega en tiempo
- Personalización

Si se usa algún software COTS.

[29] ¿Hay algún problema usando el software COTS.

Insuficiente documentación para determinar interfaces, tamaño y rendimiento.

- Bajo rendimiento
- Requiere mucha memoria o espacio de almacenamiento.
- Difícil de unir con el software.
- No suficientemente probado
- Tiene bugs
- No está adecuadamente mantenido.
- Baja respuesta del vendedor

[30] ¿Se prevé algún problema interactuando con las actualizaciones y revisiones del COTS?

3. Código y Unidades de Prueba

a. Factibilidad

[¿La implementación del diseño es difícil o imposible?]

[31] ¿Alguna parte de la implementación no está completamente definida por el diseño especificado?

[32] ¿Los algoritmos y diseño seleccionado son fáciles de implementar?

b. Pruebas

[Los niveles y tiempo asignados a las pruebas de unidad son adecuados?]

[33] ¿Se comenzaron las pruebas de unidad antes de verificar el código respecto al diseño?

[34] ¿Hay suficientes unidades de pruebas especificadas?

[35] ¿Hay tiempo suficiente para realizar todas las unidades de pruebas que se consideran deben realizarse?

[36] ¿Los compromisos se harán respecto a las unidades de prueba si hay problemas con el cronograma?

c. Implementación

[¿Hay algún problema con la implementación?]

[37] ¿Las especificaciones del diseño son suficientemente detalladas para escribir el código?

[38] ¿El diseño está cambiando mientras se codifica?

[39] ¿Hay restricciones del sistema que hacen el código difícil de escribir?

- Tiempo
- Memoria
- Almacenamiento externo

[40] ¿El lenguaje de programación es apropiado para producir el software?

[41] ¿Se están utilizando múltiples lenguajes de programación?

[42] ¿La computadora de desarrollo tiene características de software similares a la de destino? (No) (42.a) ¿Hay diferencias de compilador entre las dos?

4. Integración y pruebas.

a. Ambiente

[¿El ambiente de integración y pruebas es adecuado?]

[45] ¿Hay hardware suficiente para realizar pruebas de integración adecuadas?

[46] ¿Hay algún problema desarrollando escenarios realistas y datos de pruebas para demostrar algún requerimiento?

- Tráfico de datos específicos
- Respuesta en tiempo real

- Manejo de eventos asíncronos.
- Actividad multiusuario.

[47] ¿Es posible verificar el rendimiento desde sus instalaciones?

[48] ¿La instrumentación de hardware y software facilitara las pruebas?

(Si) (48.a) ¿Es suficiente para todas las pruebas?

b. Producto

[¿No son adecuadas las definiciones de las interfaces, las instalaciones o el tiempo?]

[49] ¿El hardware de destino estará disponible cuando se necesite?

[50] ¿Se ha acordado un criterio de aceptación para todos los requerimientos?

(Si) (50.a) ¿Hay algún acuerdo formal?

[51] ¿Las interfaces externas están definidas y documentadas?

[52] ¿Algunos requerimientos son difíciles de probar?

[53] ¿Se ha especificado suficiente la integración del producto?

[54] ¿Se ha destinado un tiempo adecuado para la integración y pruebas?

Si COTS

[55] ¿Serán aceptados los datos del vendedor en la verificación de los requerimientos asignados a los COTS?

(Si) (55.a) ¿Está en el contrato?

c. Sistema

[¿Descoordinada integración del sistema, pobre definición de interfaces o instalaciones inadecuadas?]

[56] ¿Se ha especificado suficientemente la integración del sistema?

[57] ¿Se ha asignado un tiempo adecuado para la integración del sistema y las pruebas?

[58] ¿Todos los contratistas forman parte del equipo de integración?

[59] ¿El producto será integrado en un sistema existente?

(No) (59.a.1) ¿Cómo se está garantizando que el producto funcionara correctamente en el sistema existente cuando sea integrado?

[60] ¿La integración del sistema ocurrirá en la parte cliente¹⁷?

¹⁷ No confundir "cliente" con el termino de arquitectura cliente-servidor, se refiere al cliente del proyecto.

5. Especialidades ingenieriles

a. Mantenimiento

[¿La implementación será difícil de entender o mantener?]

[61] ¿La arquitectura, diseño o código crean dificultades para el mantenimiento?

[62] ¿El personal de mantenimiento estuvo involucrado en el diseño?

[63] ¿La documentación del producto es adecuada para que el producto sea mantenido por alguien diferente a quienes lo construyeron?

b. Fiabilidad

[¿La fiabilidad o disponibilidad son requerimientos difíciles de alcanzar?]

[64] ¿Los requerimientos de fiabilidad están asignados en el software?

[65] ¿Los requerimientos de disponibilidad están asignados al software?

(Si) (65.a) ¿Hay algún problema con los tiempos de respuesta?

c. Seguridad

[¿Hay requerimientos de seguridad no factibles o no demostrables?]

[66] ¿Hay requerimientos de seguridad asociados al software?

(Si) (66.a) ¿Hay alguna dificultad en alcanzar esos requerimientos?

[67] ¿Será difícil de verificar la satisfacción de los requerimientos de seguridad?

[¿Los requerimientos de seguridad son más rigurosos que los acostumbrados?]

[68] ¿Hay requerimientos de seguridad sin precedentes?

[69] ¿Es un sistema "Orange Book"?

[70] ¿Se ha implementado este nivel de seguridad anteriormente?

e. Factores Humanos

[¿El sistema será difícil de utilizar debido a una pobre definición de interfaz humana?]

[71] ¿Hay alguna dificultad en alcanzar los requerimientos de factores humanos?

(No) (71.a) ¿Cómo se está asegurando que se lograrán dichos requerimientos?

Si Prototipado:

(Si) (71.a.1) ¿El prototipo morirá?

(No) (71.a.1a) ¿Se está haciendo un desarrollo evolutivo?

(Si) (71.a.1a.1) ¿Se está experimentado con este tipo de desarrollo?

(Si) (71.a.1a.2) ¿Las versiones interinas son entregables?

(Yes) (71.a.1a.3) ¿Esto complica el control de cambios?

f. Especificaciones

[¿La documentación es adecuada para diseñar, implementar y probar el sistema?]

[72] ¿Las especificación de requerimientos es adecuada para diseñar el sistema?

[73] ¿Las especificaciones de hardware son adecuadas para diseñar e implementar el software?

[74] ¿Los requerimientos de interfaces externas están bien especificados?

[75] ¿Las especificaciones de pruebas son adecuadas para probar totalmente el sistema?

Si se está en la fase de implementación o posterior.

[76] ¿Las especificaciones de diseño son adecuadas para implementar el sistema?

B. Ambiente de Desarrollo

1. Procesos de desarrollo

a. Formalidad

[¿La implementación será difícil de entender y mantener?]

[77] ¿Se está usando más de un modelo de desarrollo?

- Espiral
- Cascada
- Incremental

(Si) (77.a) ¿La coordinación entre ellos está siendo un problema?

[78] ¿Hay planes controlados y formales para todas las actividades de desarrollo?

- Análisis de requerimientos.
- Diseño
- Codificación
- Integración y pruebas.
- Instalación
- Aseguramiento de la calidad
- Gestión de la configuración

(Si) (78.a) ¿Los planes especifican bien el proceso?

(Si) (78.b) ¿Los desarrolladores están familiarizados con los planes?

b. Adecuación

[¿El proceso es adecuado para el modelo de desarrollo?]

[79] ¿El proceso de desarrollo es adecuado para este producto?

[80] ¿El proceso de desarrollo es soportado por procedimientos, métodos y herramientas compatibles?

c. Control

[¿El proceso de desarrollo es controlado y monitoreado usando métricas? ¿Los sitios de desarrollo distribuidos están coordinados?]

[81] ¿Todos siguen el proceso de desarrollo?

(Si) (81.a) ¿Cómo esto es asegurado?

[82] ¿Se puede medir si el desarrollo está alcanzando los objetivos de productividad y calidad? Si hay sitios de desarrollo distribuidos.

[83] ¿Hay adecuada coordinación entre los sitios de desarrollo distribuidos?

d. Familiaridad

[¿Los miembros del proyecto están experimentados en el uso de los procesos de desarrollo? ¿Estos son entendidos por todos?]

[84] ¿Las personas se sienten cómodas con los procesos de desarrollo?

e. Control del Producto

[¿Hay mecanismos para controlar los cambios en el producto?]

[85] ¿Hay alguna trazabilidad de los requerimientos desde el código hasta los casos de prueba?

[86] ¿El mecanismo de trazabilidad es utilizado para evaluar el impacto de los cambios en los requerimientos?

[87] ¿Hay algún proceso de cambio formal?

(Si) (87.a) ¿Cubre toda la línea base de los requerimientos, diseño, código y documentación?

[88] ¿Los cambios de cualquier nivel son mapeados desde el sistema hasta las pruebas?

[89] ¿Hay algún análisis adecuado cuando un Nuevo requerimiento entra al sistema?

[90] ¿Hay alguna forma de tracear las interfaces?

[91] ¿Los procedimientos y planes de pruebas son actualizados con los cambios en los procesos?

2. Sistema de desarrollo

a. Capacidad

[¿El poder de las estaciones de trabajo es suficiente (memoria, capacidad de procesamiento o almacenamiento)?]

[92] ¿Hay suficientes estaciones de trabajo y la capacidad de procesamiento que cada cual necesita para todo el personal?

[93] ¿Hay capacidad suficiente para solapar las fases como implementación, integración y pruebas?

b. Adecuación

[¿El sistema de desarrollo soporta todas las fases, actividades y funciones?]

[94] ¿El sistema de desarrollo soporta todas las fases del programa?

- Análisis de los requerimientos.
- Análisis de rendimiento.
- Diseño
- Implementación
- Pruebas
- Documentación
- Gestión de la configuración
- Gestión de proyecto
- Traceabilidad de los requerimientos

c. Usabilidad

[¿Es fácil de usar el sistema de desarrollo?]

[95] ¿Las personas encuentran el sistema de desarrollo fácil de usar?

[96] ¿Hay Buena documentación sobre el sistema de desarrollo?

d. Familiaridad

[¿Hay poca experiencia con el sistema de desarrollo?]

[97] ¿Se han usado anteriormente estas herramientas y métodos?

e. Fiabilidad

[¿El sistema tiene de errores, se reinicia o tiene problemas?]

[98] ¿El sistema es considerado fiable?

- Compilador
- Herramientas de desarrollo
- Hardware

f. Soporte

[¿Hay algún soporte de expertos o del vendedor?]

[99] ¿Las personas están capacitadas en utilizar las herramientas de desarrollo?

[100] ¿Usted tiene acceso a los expertos en utilizar el sistema?

[101] ¿Los vendedores responden a los problemas rápidamente?

g. Entregas

[¿Hay requerimientos de aceptación definidos para entregar el sistema de desarrollo?]

[102] ¿usted es el responsable de entregar el sistema de desarrollo a los clientes?

(Si) (102.a) ¿Existe un presupuesto y planificación adecuado para esta tarea?

3. Procesos de Gestión

a. Planificación

[¿La planificación es oportuna, los temas técnicos están incluidos y la contingencia analizada?]

[103] ¿El programa está siendo dirigido de acuerdo al plan?

(Si) (103.a) ¿Frecuentemente se realizan “maratones” para cumplir los planes?

[104] ¿Se replanifica cuando ocurren interrupciones?

[105] ¿Las personas de todos los niveles son incluidas en la planificación de su propio trabajo?

[106] ¿Hay planes de contingencia para los riesgos conocidos?

(Si) (106.a) ¿Cómo determinas cuándo activar esos planes?

[107] ¿Los términos a largo plazo son tratados adecuadamente?

b. Organización del Proyecto.

[¿Las relaciones entre los roles están claras?]

[108] ¿La organización es efectiva?

[109] ¿Las personas entienden su rol y el de los otros?

[110] ¿Las personas conocen quien tiene autoridad para qué?

Anexo4 – Modelo para documentar el riesgo

ID:	Etapa:	Estado:	Prioridad:
Categoría:		Entrevistado:	
Definición del riesgo: (evento): (consecuencia):			
Causas:			
Posible Probabilidad (opcional):		Posible Impacto (opcional):	

Probabilidad:	Impacto:
Frecuencia:	Certidumbre:
Marco de tiempo:	Estrategia de respuesta:
Responsables:	
Riesgos Relacionados:	
Observaciones:	

Anexo5 – Lista de Riesgos Comunes

Las siguientes definiciones de riesgos fueron elaboradas de acuerdo al criterio de algunos expertos, la experiencia en el desarrollo de proyectos productivos de los autores, y el análisis de trabajos de varios autores como Addison (7), Risk World (45), Niwot Ridge Consulting (58), Walsh (62), Nieminen (63), Kwak (64), Teague (65), Uniersal Risk Project (66), Piñero (67), STSC (68), Meyers (69), CSO (70), Carbone (71). Estas definiciones no incluyen la consecuencia o impacto, pueden considerarse como factores de riesgos, tienen la intención de ilustrar problemas conocidos que han ocurrido anteriormente y que son frecuentes, para la identificación de riesgos utilizando esta lista de riesgos comunes, deben escribirse en la forma especificada de acuerdo a la técnica.

ID	Riesgo	Frecuencia	Etapa
	Alcance u objetivos no claros o malentendidos.		
	Presupuesto y cronograma irrealista.		
	Planificaciones demasiado optimistas		
	Falta de compromiso de la alta dirección.		
	Falta de involucración del usuario.		
	Conocimiento o habilidades inadecuadas.		
	Personal mediocre.		
	Falta de una metodología de gestión de proyectos efectiva.		
	Líder de proyecto involucrado activamente en el desarrollo.		
	Decisiones arquitectónicas no basadas en criterios tecnológicamente correctos y viables si no influenciadas por otros factores.		
	Requerimientos malentendidos.		
	Meticulosidad en requerimientos o de los desarrolladores.		
	“Gold plating”.		
	Síndrome de la panacea (“esta herramienta ahorrará la mitad del trabajo”)		
	Continuos cambios en los requerimientos.		
	Desarrollo de las funciones incorrectas en el software.		
	Diseño inadecuado.		
	Subcontratación.		
	Errores en la contratación (contrato muy flexible).		
	Uso y rendimiento de los recursos inadecuado.		
	Introducción de una nueva tecnología.		
	Desarrollo orientado a la investigación.		
	Escatimar en la calidad.		
	Desvinculación del grupo de calidad con el proyecto.		
	Incapacidad de manejar las expectativas del usuario final.		
	Diferencias con los clientes.		
	Usuario final no quiere el software.		
	“Maratones” de desarrollo.		

	Ritmo de trabajo extremo.		
	Suspensión de las clases de los estudiantes.		

A continuación se muestran un conjunto de riesgos identificados por la universidad como riesgos frecuentes.

A. Elaboración de la Planificación

- A.1. Las definiciones de la planificación, de los recursos y del producto han sido impuestas por el cliente o un directivo superior, y no están equilibradas.
- A.2. Planificación optimista, «mejor caso» (en lugar de realista, «caso esperado»).
- A.3. La planificación no incluye tareas necesarias.
- A.4. La planificación se ha basado en la utilización de personas específicas de un equipo, pero estas personas no están disponibles.
- A.5. No se puede construir un producto de tal envergadura en el tiempo asignado.
- A.6. El producto es más grande que el estimado (en líneas de código, en el número de puntos función, o en relación con el tamaño del proyecto anterior).
- A.7. El esfuerzo es mayor que el estimado (por líneas de código, número de puntos función, módulos, etc.).
- A.8. La reestimación debida a un retraso en la planificación es demasiado optimista o ignora la historia del proyecto.
- A.9. La presión excesiva en la planificación reduce la productividad.
- A.10. La fecha final ha cambiado sin ajustarse al ámbito del producto o a los recursos disponibles.
- A.11. Un retraso en una tarea produce retrasos en cascada en las tareas dependientes.
- A.12. Las áreas desconocidas del producto llevan más tiempo del esperado en el diseño y en la implementación.

B. Organización y Gestión

- B.1. El proyecto carece de un promotor efectivo en los superiores.
- B.2. El proyecto languidece demasiado en el inicio difuso.
- B.3. Los despidos y las reducciones de la plantilla reducen la capacidad del equipo.
- B.4. Dirección o marketing insisten en tomar decisiones técnicas que alargan la planificación.
- B.5. La estructura inadecuada de un equipo reduce la productividad.
- B.6. El ciclo de revisión/decisión de la directiva es más lento de lo esperado.
- B.7. El presupuesto varía el plan del proyecto.
- B.8. La dirección toma decisiones que reducen la motivación del equipo de desarrollo.
- B.9. Las tareas no técnicas encargadas a terceros necesitan más tiempo del esperado (aprobación del presupuesto, aprobación de la adquisición de material, revisiones legales, seguridad, etc.).
- B.10. La planificación es demasiado mala para ajustarse a la velocidad de desarrollo deseada.
- B.11. Los planes del proyecto se abandonan por la presión, llevando al caos y a un desarrollo ineficiente.
- B.12. La dirección pone más énfasis en las heroicidades que en informarse exactamente del estado, lo que reduce su habilidad para detectar y corregir problemas.

C. Ambiente/Infraestructura de Desarrollo

- C.1. Los espacios no están disponibles en el momento necesario.
- C.2. Los espacios están disponibles pero no son adecuados (por ejemplo, falta de teléfonos, cableado de la red, mobiliario, material de oficina, etc.).
- C.3. Los espacios están sobreutilizados, son ruidosos o distraen.
- C.4. Las herramientas de desarrollo no están disponibles en el momento deseado.
- C.5. Las herramientas de desarrollo no funcionan como se esperaba; el personal de desarrollo necesita tiempo para resolverlo o adaptarse a las nuevas herramientas.
- C.6. Las herramientas de desarrollo no se han elegido en función de sus características técnicas, y no proporcionan las prestaciones previstas.
- C.7. La curva de aprendizaje para la nueva herramienta de desarrollo es más larga de lo esperado.

D. Usuarios Finales

- D.1. Los usuarios finales insisten en nuevos requisitos.

- D.2. En el último momento, a los usuarios finales no les gusta el producto, por lo que hay que volver a diseñarlo y a construirlo.
- D.3. Los usuarios no han realizado la compra del material necesario para el proyecto y, por tanto, no tienen la infraestructura necesaria.
- D.4. No se ha solicitado información al usuario, por lo que el producto al final no se ajusta a las necesidades del usuario, y hay que volver a crear el producto.
- E. Cliente
 - E.1. El cliente insiste en nuevos requisitos.
 - E.2. Los ciclos de revisión/decisión del cliente para los planes, prototipos y especificaciones son más lentos de lo esperado.
 - E.3. El cliente no participa en los ciclos de revisión de los planes, prototipos y especificaciones, o es incapaz de hacerlo, resultando unos requisitos inestables y la necesidad de realizar unos cambios que consumen tiempo.
 - E.4. El tiempo de comunicación del cliente (por ejemplo, tiempo para responder a las preguntas para aclarar los requisitos) es más lento del esperado.
 - E.5. El cliente insiste en las decisiones técnicas que alargan la planificación.
 - E.6. El cliente intenta controlar el proceso de desarrollo, con lo que el progreso es más lento de lo esperado.
 - E.7. Los componentes suministrados por el cliente no son adecuados para el producto que se está desarrollando, por lo que se tiene que hacer un trabajo extra de diseño e integración.
 - E.8. Los componentes suministrados por el cliente tienen poca calidad, por lo que tienen que hacerse trabajos extra de comprobación, diseño e integración.
 - E.9. Las herramientas de soporte y entornos impuestos por el cliente son incompatibles, tienen un bajo rendimiento o no funcionan de forma adecuada, con lo que se reduce la productividad.
 - E.10. El cliente no acepta el software entregado, incluso aunque cumpla todas sus especificaciones.
 - E.11. El cliente piensa en una velocidad de desarrollo que el personal de desarrollo no puede alcanzar.
- F. Personal Contratado
 - F.1. El personal contratado no suministra los componentes en el período establecido.
 - F.2. El personal contratado proporciona material de una calidad inaceptable, por lo que hay que añadir un tiempo extra para mejorar la calidad.
 - F.3. Los proveedores no se integran en el proyecto, con lo que no se alcanza el nivel de rendimiento que se necesita.
- G. Requisitos
 - G.1. Los requisitos se han adaptado, pero continúan cambiando.
 - G.2. Los requisitos no se han definido correctamente. y su redefinición aumenta el ámbito del proyecto.
 - G.3. Se añaden requisitos extra.
 - G.4. Las partes del proyecto que se no se han especificado claramente consumen más tiempo del esperado.
- H. Producto
 - H.1. Los módulos propensos a tener errores necesitan más trabajo de comprobación, diseño e implementación.
 - H.2. Una calidad no aceptable requiere de un trabajo de comprobación, diseño e implementación superior al esperado.
 - H.3. Utilizar lo último en informática alarga la planificación de forma impredecible.
 - H.4. El desarrollo de funciones software erróneas requiere volver a diseñarlas y a implementarlas.
 - H.5. El desarrollo de una interfaz de usuario inadecuada requiere volver a diseñarla y a implementarla.
 - H.6. El desarrollo de funciones software innecesarias alarga la planificación.
 - H.7. Alcanzar el ámbito del producto o las restricciones de velocidad requiere más tiempo del esperado, incluyendo el tiempo para volver a diseñar e implementar.
 - H.8. Unos requisitos rígidos de compatibilidad con el sistema existente necesitan un trabajo extra de comprobación, diseño e implementación.
 - H.9. Los requisitos para crear interfaces con otros sistemas, otros sistemas complejos, u otros sistemas que no están bajo el control del equipo de desarrollo suponen un diseño, implementación y prueba no previstos.
 - H.10. El requisito de trabajar con varios sistemas operativos necesita más tiempo del esperado.
 - H.11. El trabajo con un entorno software desconocido causa problemas no previstos.
 - H.12. El trabajo con un entorno hardware desconocido causa problemas imprevistos.
 - H.13. El desarrollo de un tipo de componente nuevo para la organización consume más tiempo del esperado.
 - H.14. Depender de una tecnología que aún está en fase de desarrollo alarga la planificación.
- I. Fuerzas mayores
 - I.1. El producto depende de las normativas del gobierno, que pueden cambiar de forma inesperada.

I.2. El producto depende de estándares técnicos provisionales, que pueden cambiar de forma inesperada.

J. Personal

J.1. La contratación tarda más de lo esperado.

J.2. Las tareas preliminares (por ejemplo, formación, finalización de otros proyectos, adquisición de licencias) no se han completado a tiempo.

J.3. La falta de relaciones entre la dirección y el equipo de desarrollo ralentiza la toma de decisiones.

J.4. Los miembros del equipo no se implican en el proyecto, y por lo tanto no alcanzan el nivel de rendimiento deseado.

J.5. La falta de motivación y de moral reduce la productividad.

J.6. La falta de la especialización necesaria aumenta los defectos y la necesidad de repetir el trabajo.

J.7. El personal necesita un tiempo extra para acostumbrarse a trabajar con herramientas o entornos nuevos.

J.8. El personal necesita un tiempo extra para acostumbrarse a trabajar con hardware nuevo.

J.9. El personal necesita un tiempo extra para aprender un lenguaje de programación nuevo.

J.10. El personal contratado abandona el proyecto antes de su finalización.

J.11. Alguien de la plantilla abandona el proyecto antes de su finalización.

J.12. La incorporación de nuevo personal de desarrollo al proyecto ya avanzado, y el aprendizaje y comunicaciones extra imprevistas reducen la eficiencia de los miembros del equipo existentes.

J.13. Los miembros del equipo no trabajan bien juntos.

J.14. Los conflictos entre los miembros del equipo conducen a problemas en la comunicación y en el diseño, errores en la interfaz y tener que repetir algunos trabajos.

J.15. Los miembros problemáticos de un equipo no son apartados, influyendo negativamente en la motivación del resto del equipo.

J.16. Las personas más apropiadas para trabajar en el proyecto no están disponibles.

J.17. Las personas más apropiadas para trabajar en el proyecto están disponibles, pero no se pueden incorporar por razones políticas o de otro tipo.

J.18. Se necesitan personas para el proyecto con habilidades muy específicas y no se encuentran.

J.19. Las personas clave sólo están disponibles una parte del tiempo.

J.20. No hay suficiente personal disponible para el proyecto.

J.21. Las tareas asignadas al personal no se ajustan a sus posibilidades.

J.22. El personal trabaja más lento de lo esperado.

J.23. El sabotaje por parte de la dirección del proyecto deriva en una planificación ineficiente e inefectiva.

J.24. El sabotaje por parte del personal técnico deriva en una pérdida de trabajo o en un trabajo de poca calidad, por lo que hay que repetir algunos trabajos.

K. Diseño e Implementación

K.1. Un diseño demasiado sencillo no cubre las cuestiones principales, con lo que hay que volver a diseñar e implementar.

K.2. Un diseño demasiado complejo exige tener en cuenta complicaciones innecesarias e improductivas en la implementación.

K.3. Un mal diseño implica volver a diseñar e implementar.

K.4. La utilización de metodologías desconocidas deriva en un periodo extra de formación y tener que volver atrás para corregir los errores iniciales cometidos en la metodología.

K.5. El producto está implementado en un lenguaje de bajo nivel (por ejemplo, ensamblador) y la productividad es menor de la esperada.

K.6. No se puede implementar la funcionalidad deseada con el lenguaje o bibliotecas utilizados: el personal de desarrollo tiene que utilizar otras bibliotecas, o crearlas él mismo para conseguir la funcionalidad deseada.

K.7. Las bibliotecas de código o clases tienen poca calidad, y generan una comprobación extra, corrección de errores y la repetición de algunos trabajos.

K.8. Se ha sobreestimado el ahorro en la planificación derivado del uso de herramientas para mejorar la productividad.

K.9. Los componentes desarrollados por separado no se pueden integrar de forma sencilla, teniendo que volver a diseñar y repetir algunos trabajos.

L. Proceso

L.1. La burocracia produce un progreso más lento del esperado.

L.2. La falta de un seguimiento exacto del progreso hace que se desconozca que el proyecto esté retrasado hasta que está muy avanzado.

L.3. Las actividades iniciales de control de calidad son recortadas, haciendo que se tenga que repetir el trabajo.

- L.4. Un control de calidad inadecuado hace que los problemas de calidad que afectan a la planificación se conozcan tarde.
- L.5. La falta de rigor (ignorar los fundamentos y estándares del desarrollo de software) conduce a fallos de comunicación, problemas de calidad y repetición del trabajo. Un consumo de tiempo innecesario.
- L.6. El exceso de rigor (aferramiento burocrático a las políticas y estándares de software) lleva a gastar más tiempo en gestión del necesario.
- L.7. La creación de informes de estado a nivel de directiva lleva más tiempo al desarrollador de lo esperado.
- L.8. La falta de entusiasmo en la Gestión de Riesgos impide detectar los riesgos más importantes del proyecto.
- L.9. La Gestión de Riesgos del proyecto software consume más tiempo del esperado.

Anexo6 – Lecciones Aprendidas

Efectividad de los planes de respuesta:

Plan	Efectividad	Frecuencia	Observaciones

Comentarios.

Anexo7 – Plan de Respuesta de Riesgo

ID:	Tipo de Plan:	Prioridad:
Aplicable a los riesgos:		
Efectivo Desde:	Hasta:	Iniciar:
Condiciones para el inicio:		
Costo de la ejecución:		
Actividades:		
Evaluación de la efectividad:		

Anexo8 – Respuestas Comunes a Riesgos

En este documento se describen las respuestas comunes a riesgos. Estas respuestas se obtienen con la aplicación continua del modelo luego de analizar las tendencias de proyecto a proyecto.