Club de Investigación Tecnológica

Administración del Riesgo en Proyectos Informáticos

Ing. Carlos E. Vargas, CSQE

Noviembre 2007

Club de Investigación Tecnológica

Informes publicados

	Informe	Autor	Fecha
1.	Redes de Computadores	Dr. Roberto Sasso	Agosto 1988
2.	Sistemas Expertos	Dr. Claudio Gutiérrez	Enero 1989
3.	Planificación de Sistemas	Dr. René-Pierre Bondu	Abril 1989
4.	Proyectos de Sistemas	Ing. Ignacio Trejos	Setiembre 1989
5.	Bases de Datos	Dr. Carlos González	Diciembre 1989
6.	Escapando de los Sistemas del Ayer	Lic. Pablo Rojas, M.Sc.	Marzo 1990
7.	Aplicaciones Creativas	Dr. Roberto Sasso	Mayo 1990
8.	Calidad de Sistemas	Dr. Ulises Agüero	Octubre 1990
9.	Personal y Organización de Sistemas	KPMG Consultores	Marzo 1991
10.	Sistemas Abiertos	Ing. José Rubinstein, MBA	Octubre 1991
11.	Análisis de la Industria de la TI.	Lic. Roberto Venegas, MBA	Enero 1992
12.	Nuevas Tecnologías de Información	Dr. Roberto Sasso (Editor)	Marzo 1992
13.	Ambientes de Proveedores Múltiples	Lic. Alexis Rodríguez U.	Julio 1992
14.	Planificación y Recuperación de Desastres	Sr. Gerardo Ortuño	Agosto 1992
15.	Diseño de Redes Novell	Ing. David Baruch	Agosto 1993
16.	Minis Vs LANs	Ing. Marvin Campos	Octubre 1993
17.	Intercambio Electrónico de Datos (EDI)	KPMG Consultores	Enero 1995
18.	Sistemas Abiertos de Software	Ing. José Ardón	Abril 1995
19.	Outsourcing de Tecnología de Información	Roxana Murillo, M.Sc.	Julio 1996
20.	Redes Empresariales de Banda Ancha	Ing. Aníbal Mayorga, M.Sc.	Febrero 1997
21.	Comercio Electrónico	Dr. Roberto Sasso Rojas	Abril 1997
22.	Estudio de Opinión Informática	Dr. Freddy Abarca	Julio 1997
23.	Desarrollo de Sistemas Cliente/Servidor	Lic. Édgar Hernández Ing. Luis Martínez	Diciembre 1997

24.	Enfrentando el año 2000. Guía Práctica	Ing. Carlos Gallegos, M.Sc. Dr. Roberto Sasso Ing. Ignacio Trejos, M.Sc.	Mayo 1998
25.	Depósitos de Datos	Beatriz Jiménez, M.Sc. Rafael Avalos, M.Sc.	Noviembre 1998
26	El modelo de objetos: Análisis y Diseño	Ing. Ignacio Trejos, M.Sc. Ing. Antonio Luna	Setiembre 1999
27.	Silicon Valley, 1999	Ing. Mauricio Monge Dr. Roberto Sasso Ing. Ignacio Trejos, M.Sc.	Enero 2000
28.	Calidad de los datos: Un enfoque conceptual	Ing. Lilia Muñoz, M.Sc.	Febrero 2000
29.	El modelo de objetos: Lenguaje de modelaje Unificado (UML)	Ing. Antonio Luna Ing. Ignacio Trejos, M.Sc.	Marzo 2000
30.	Medición de calidad de datos: Un enfoque práctico	Ing. Franco Quirós	Marzo 2000
31.	Seguridad de la información en la era de los negocios digitales	Lic. Édgar Hernández Lic. Marco V. Gámez	Julio 2001
32.	Transformación de aplicaciones legacy	Ing. Declan Good	Agosto 2002
32.	Legacy transformation	Ing. Declan Good	August 2002
33.	Calidad en la especificación de requerimientos	Ing. Javier Rivas	Febrero 2003
34.	Inteligencia de negocios	Lic. José Mayorga	Setiembre 2004
35.	Sistemas colaborativos	Ing. Xinia Robles Lic. Lizette Ramírez, M.Sc.	Octubre 2004
36.	XML: Tecnología y aplicaciones	Dr. José Enrique Araya Ing. Emilia Zeledón	Enero 2005
37.	Procesos de software	Ing. Priscilla Garbanzo, MIS	Setiembre 2005
38.	Patrones de software	Lic. Alan Calderón, M.Sc.	Agosto 2006
39.	Administración del Riesgo en Proyectos Informáticos	Ing. Carlos E. Vargas, CSQE	Noviembre 2007

Editado y publicado por Rho-Sigma, S.A., a nombre del Club de Investigación Tecnológica.

San José, Costa Rica. Noviembre 2007

Resumen Ejecutivo

La conciencia mundial sobre el riesgo se ha agudizado en la presente década, mayormente impulsada por eventos lamentables que han tenido un impacto global en la aceptación y cumplimiento de reglas y procedimientos asociados con la prevención de acciones contrarias al interés y bienestar común de la sociedad y los servicios vitales que marcan la interacción globalizada de los países.

Esta conciencia, aunada a una cada vez más atendida insatisfacción con los resultados de los proyectos informáticos, y la preocupación que genera en los involucrados en su planteamiento, administración y ejecución, ha generado una actitud ante el riesgo que debería promover la inversión oportuna del esfuerzo y la atención focalizada que se requiere para efectuar los procesos de la administración del riesgo presentados y explicados en este informe.

Con base en los lineamientos y recomendaciones de las instituciones de influencia internacional más relevantes en el desarrollo de la administración de proyectos, particularmente en el campo de los proyectos informáticos y atendiendo la actual focalización sobre la administración efectiva del riesgo, se desarrollan en este informe los procesos recomendados en el ciclo de vida de esta administración, buscando una interiorización de su importancia y un conocimiento práctico de los procedimientos por seguir para mejorar las probabilidades de éxito de los proyectos con la mitigación oportuna de los riesgos que todo proyecto enfrenta durante su ejecución.

Esperamos que el estudio del material presentado sea de amplia utilidad para los profesionales involucrados en la ejecución de proyectos informáticos. El Club de Investigación Tecnológica y el autor se declaran en disposición de apoyar al lector en la clarificación del tema y el acceso a los materiales referenciados, en aras de lograr una mejor ejecución de los procesos de administración del riesgo, y, consecuentemente, de la mejora en los índices de éxito de los proyectos informáticos.

Del autor

Carlos E. Vargas Mora es Ingeniero Industrial, con una trayectoria de trabajo profesional en la industria informática que se inició en 1973. Profesor en programas de control del proceso y administración de proyectos, ha desarrollado labores docentes con el Instituto Tecnológico de Costa Rica, la Universidad Nacional, Cenfotec y la Universidad Latina, y desempeñado funciones gerenciales en dirección de proyectos en múltiples firmas de prestación de servicios informáticos en el país e internacionalmente.

Agradecimiento

Profundo y sincero a Ignacio Trejos Zelaya y al Club de Investigación Tecnológica por la oportunidad enriquecedora de desarrollar este informe tras una investigación esclarecedora sobre el tema de administración del riesgo y sus implicaciones para una administración de proyectos efectiva y eficaz.

Nota editorial

Este informe fue revisado por Roberto Sasso e Ignacio Trejos. La edición final estuvo a cargo de Ignacio Trejos.

Administración del riesgo en proyectos informáticos

Tabla de Contenidos

Tabla de Figuras

Administración del riesgo en proyectos informáticos

1 - Introducción

Con el nuevo milenio, tras la tragedia de los atentados terroristas que afectaron el territorio estadounidense el 11 de setiembre de 2001, los habitantes de este planeta hemos redescubierto la realidad y peligrosidad de los riesgos que enfrentamos en el devenir de nuestras acciones de todos los días.

Siete años después, podemos valorar cuánto se ha modificado el comportamiento social como consecuencia de esta **toma de conciencia del riesgo** en el comportamiento de las organizaciones y de los individuos.

Tenemos nuevas reglas, procedimientos y exigencias para abordar el medio de transporte emblemático del siglo XX: la aviación. Qué se puede transportar en un vuelo comercial, en la mano o en el equipaje, las revisiones físicas o por medio de escaneo electrónico de los pasajeros, los chequeos incisivos y minuciosos de la documentación de cada uno, matizados por la influencia de las sospechas posibles según la etnia, procedencia o religión, son sólo una muestra de un cambio de actitud hacia la mitigación del riesgo que cada pasajero representa para sus compañeros de vuelo al abordar una cápsula metálica que de sufrir algún percance en vuelo sellaría la suerte final de todos los ocupantes de la aeronave.

Sobre la misma línea en el mismo ejemplo podemos indagar sobre los nuevos procedimientos de revisión de antecedentes en los empleados de los aeropuertos, las tripulaciones, los proveedores que suplen al aeropuerto de la infinidad de insumos básicos para su funcionamiento, así como las revisiones de ingreso a las personas y a los artículos que llevan consigo o en el vehículo en que hacen su ingreso a las instalaciones aeroportuarias.

Tras un vistazo al ejemplo dado, si tomamos **conciencia** del por qué de las nuevas acciones, reglamentaciones y cuidados, podemos ver claramente que ante la forma en que fue imprevisto el esquema de abordaje y utilización del transporte aéreo en los atentados de la emblemática fecha del 11/9, necesariamente concluiremos que algo distinto debe hacerse, para prever los riesgos asociados a una repetición de los nefastos hechos. Pero si analizamos en más detalle, podemos encontrar que muchas de las "nuevas" reglamentaciones ya estaban en esencia definidas, escritas y vigentes cuando se dieron los lamentables ataques, simplemente no se tomaban "tan en serio" o "al pie de la letra", pues al ignorarlas no se había valorado lo que en la realidad podría suceder al ejercer controles laxos sobre la seguridad de la operación de la industria aeronáutica.

¿A dónde llegamos tras esta reflexión? ¿Qué fue lo que cambió tras los hechos dolorosos? ¿Por qué ahora estamos dispuestos a sacrificar agilidad, tiempo y comodidad individual y colectiva para ajustarnos a un riguroso acatamiento de las reglas de prevención aplicadas?

Lo que cambió fue que individual y colectivamente tomamos conciencia del impacto que los riesgos que enfrentamos en esta operación de transporte tendrían sobre vidas y propiedades, si los dejamos al azar y no actuamos efectiva y eficientemente en su mitigación.

Individual y colectivamente, en cada país, ciudad y aeropuerto, los habitantes del planeta han tomado conciencia de los riesgos involucrados y se han mostrado dispuestos a acatar rigurosamente las reglas que les ayuden a reducir su probabilidad de ocurrencia.

En un principio, consternados, la reacción individual, que al sumar es masiva, fue la de evitar el riesgo: no vuelo. Alternativamente utilizaríamos el tren, el automóvil, la moto...; pero en el mundo de presión por la velocidad de entrega de servicios y presencias, en su mayoría los habitantes del planeta han vuelto a utilizar el medio más ágil, sometiéndose ahora más rigurosamente a las reglas, antiguas y nuevas, que les den la tranquilidad de que lo están haciendo en condiciones "aceptables", bajo niveles de riesgo "razonables".

Ahí tenemos una lección ilustrativa de la teoría básica del riesgo, y de los mecanismos requeridos para ubicar su manejo, o intención de manejo, en niveles aceptables.

Lo señalado ilustra el tema central de esta investigación para darnos una comprensión básica del por qué y el para qué de cada uno de los elementos centrales que se señalan en los lineamientos esenciales de la Administración del Riesgo. Veamos.

Propósito de la investigación

Dada la motivación a la Administración del Riesgo presentada, pretendemos ahora hacer un recorrido de las necesidades, causas y efectos de los riesgos que se enfrentan en el desarrollo de proyectos informáticos, dado que es ya usual, temido y hasta esperado, que los proyectos en esta área presenten un comportamiento sumamente incierto, en el que son frecuentes los atrasos en el cumplimiento de metas en el tiempo, los costos sobrepasados y la insatisfacción de los requerimientos que el proyecto debe obtener, o hay carencias en la calidad y consistencia de los productos logrados. Estos elementos marcan con frecuencia la realidad del desempeño de los proyectos.

La administración de proyectos en general, y de proyectos informáticos en particular, es un ejercicio complejo e incierto que exige una disciplina de atención a las áreas señaladas en los lineamientos del PMI [PMI 2004], lineamientos orientados a mejorar las probabilidades de éxito de los proyectos, que se define como la obtención de los resultados buscados en el tiempo planeado, con la calidad esperada, al costo presupuestado y satisfaciendo cabalmente los requerimientos y expectativas de todos los interesados directa o indirectamente en los resultados del proyecto.

El objetivo de esta investigación es brindar un panorama que responda a las siguientes preguntas, en el marco de los proyectos informáticos:

- ¿Cuál es la concepción básica de riesgo?
- ¿De qué trata la Administración del Riesgo?
- ¿Qué modelos de Administración de Riesgo son aplicables?
- ¿Qué actividades o procesos deben considerarse para una Administración efectiva del Riesgo?
- ¿Cómo lo anterior puede contribuir a mejorar el desempeño de los proyectos informáticos?

Los resultados de la investigación deberán servir como un instrumento de revaloración de la necesidad de efectuar una Administración de Riesgo eficaz en los proyectos informáticos, tanto por parte de los Gerentes de Proyecto como por su equipo de trabajo, dado que la administración proactiva necesaria durante el desarrollo del proyecto requiere la constante atención, detección y respuesta del equipo de trabajo sobre los factores de riesgo que enfrenta el proyecto.

Para la conformación de este informe, se consideran las fuentes definidas en la sección de Referencias, que son mayormente obras de renombre orientadas a explicar y habilitar el esfuerzo gerencial en la Administración de Proyectos Informáticos, dentro de la cual la Administración de Riesgos es un elemento central. El investigador aplica asimismo su experiencia en la dirección de proyectos para enfatizar aquellos elementos que generalmente provocan fallas en los proyectos por la falta de atención rigurosa a los mecanismos y procesos aquí descritos.

2 - Los proyectos informáticos y su realidad de desempeño

Según el Project Management Institute [PMI 2004], "un proyecto es un esfuerzo temporal emprendido para crear un producto, servicio o resultado único". Ampliando esta definición, citamos a Kerzner [Kerzner 2001]: "Un proyecto es un esfuerzo que tiene un objetivo definible, consume recursos, y opera bajo restricciones de tiempo, costo y calidad. Adicionalmente, los proyectos son generalmente considerados como actividades que son únicas para la organización."

De estas definiciones podemos establecer que los proyectos, cada uno en su momento para la organización que lo requiere, presenta un reto de desarrollo de actividades que no se han ejecutado previamente y pueden no ser repetidas a futuro. Además, se parte de que el proyecto se plantea en un contexto de limitaciones preestablecidas en relación con el tiempo en que debe completarse, el presupuesto asignado, y la calidad esperada en el producto, servicio o resultado que debe producir. En proyectos informáticos, este producto será usualmente una aplicación o artefacto de software con una funcionalidad definida, que satisface los requerimientos establecidos al inicio del proyecto, por lo que su calidad estará directamente relacionada con el cumplimiento funcional del resultado.

En 1995, tras estudios, encuestas y análisis efectuados hasta 1994, un grupo consultor, el Standish Group International, Inc., presentó los resultados de su recopilación exhaustiva de información sobre el comportamiento de lo proyectos informáticos, en su Chaos Report [SGI 1995]. Desde entonces, periódicamente se actualiza el estudio, lo que permite tener una visión panorámica del comportamiento de los proyectos informáticos en el tiempo.

En la actualización del Chaos Report al 2001 [SGI 2001], el desempeño histórico de los proyectos lucía según la siguiente gráfica:

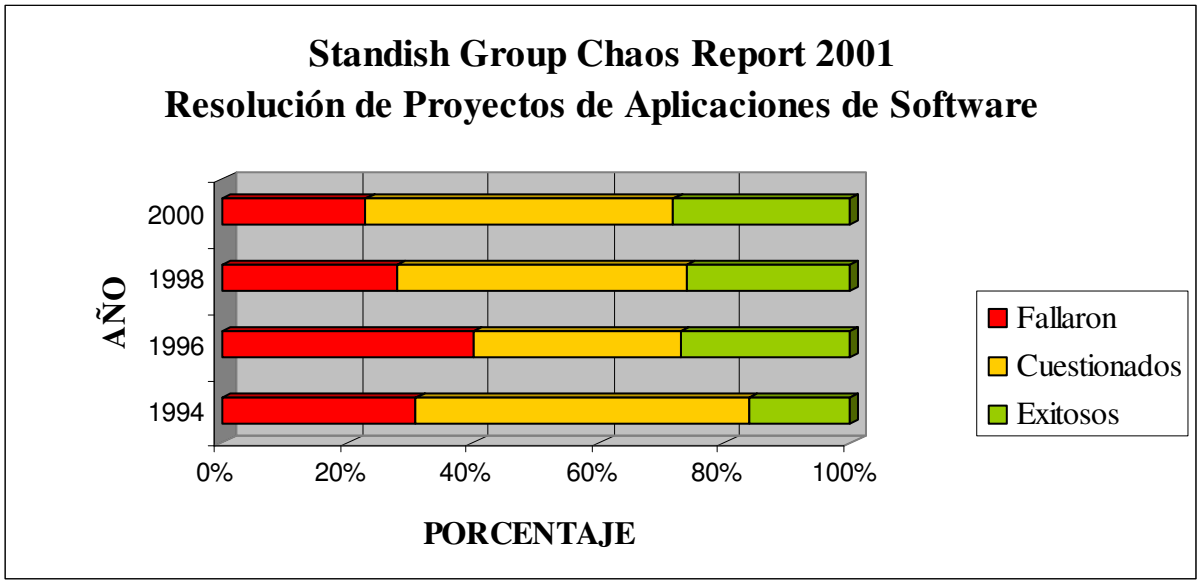


Figura 1 - Resolución de proyectos de aplicaciones de software 2001

Esta gráfica presenta la resolución acumulada de más de treinta mil proyectos de aplicaciones de software en empresas estadounidenses, pequeñas, medianas y grandes en las industrias de los sectores de clasificación general (aeronáutica, banca y finanzas, gobierno, farmacia, etc.), presentados en las actualizaciones bianuales del Chaos Report de 1994 al 2000.

Como se puede apreciar, en ese período la mejora en el porcentaje de proyectos exitosos pasa apenas de un 16% al 28%, en tanto que los proyectos fracasados se redujeron de un 31% a un 23%. Los proyectos "cuestionados" son aquellos que no cumplieron plenamente sus objetivos de tiempo (oportunidad), costo (presupuesto) y/ó calidad (funcionalidad y satisfacción de requerimientos). Estos representaron el 52% en 1994, bajando ligeramente al 49% en el estudio del 2000.

Según la actualización al año 2004 [SGI 2004], la tasa de éxito mejoró hasta el 34%, mejorando los resultados de 1994 en más de un 100%, en tanto que la tasa de fracasos se redujo al 15%. Los proyectos cuestionados representaron un 51% del total.

La gráfica comparativa luce entonces como sigue:

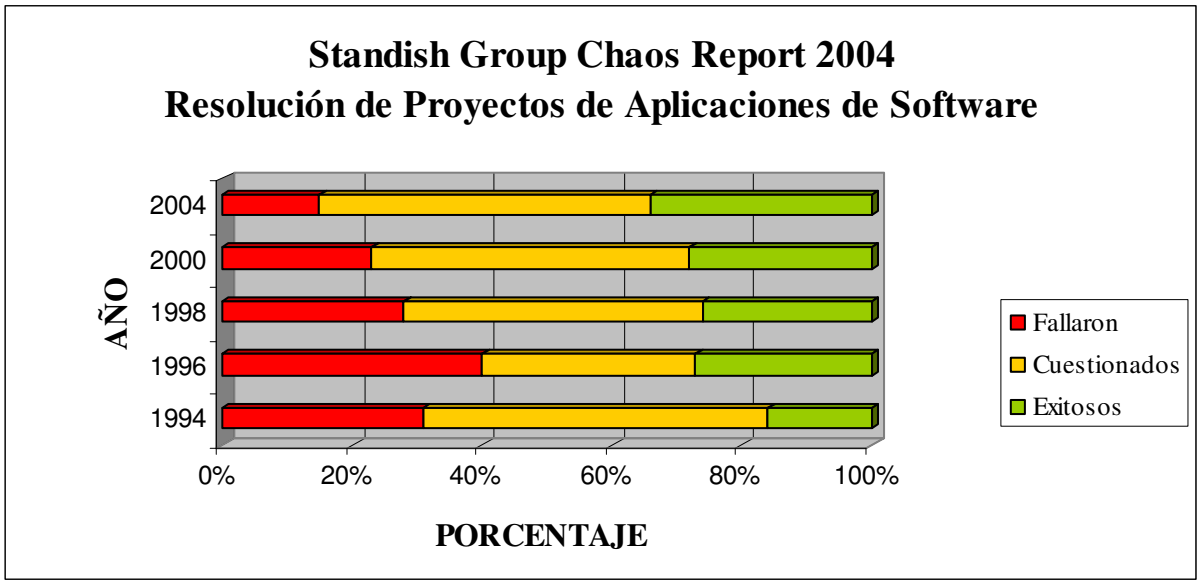


Figura 2 - Resolución de proyectos de aplicaciones de software 2004

Como razones para la mejora en la tasa de proyectos exitosos, el Standish Group señala:

"La razón principal es que los proyectos se han reducido en tamaño. La utilización de desarrollo iterativo, en oposición al método de cascada, que obligaba a la definición inicial de todos los requerimientos del proyecto, ha permitido este importante avance.

*La mayoría de los proyectos 'cuestionados' en la encuesta del 2004 tuvieron excesos de costo del orden del 20%, una mejora de tres veces sobre los resultados de 1994. Los excesos de costo totales, incluyendo proyectos fracasados, se estableció en el 43% en el 2004, versus un exceso del 180% en 1994 (*notar que el 43% mencionado incluye el exceso de costo incurrido por proyectos que al final fueron un fracaso, no solamente 'cuestionados'*).*

En el Chaos Report del 2004 se estimó en $55 mil millones las pérdidas en proyectos, contra un gasto total de $255 mil millones. En 1994, la estimación fue de $140 mil millones en pérdidas,

$80 mil millones de ellos en proyectos fracasados, de un gasto total en proyectos de $250 mil millones."

Siendo optimistas en el análisis de lo presentado, el Standish Group enfatiza la mejora en proyectos exitosos que pasaron en una década del 16% al 34%. Hay reducción de pérdidas, pero, para considerar estos resultados consistentes con la preocupación, mayor conocimiento y esfuerzo por mejorar la administración de los proyectos, los avances son escasos: excederse en 180% sobre el 82% de los proyectos (1994), con $140 mil millones en el 31% de los proyectos clasificados como fracaso, versus un 20% sobre el 15% (2004), es difícilmente un indicador de mejora sustancial para un tema así estudiado y señalado.

Es de notar que el porcentaje de proyectos 'cuestionados' se redujo en esta década del 53% al 51%, lo que difícilmente es motivo de celebración.

Los resultados observados sólo pueden transmitir al observador una inquietud de incertidumbre si está considerando iniciar un proyecto específico de este tipo.

Pero los resultados son consecuencia de la falta de cumplimiento en los proyectos de lo que se denomina "factores críticos de éxito" (FCEs), que el Standish Group determina para cada período de análisis. En 2001, los 10 FCEs principales fueron:

1. Apoyo y compromiso ejecutivo
2. Disponibilidad, participación y compromiso del usuario
3. Experiencia del Gerente de Proyecto
4. Objetivos de Negocio bien definidos
5. Alcance racionalizado
6. Infraestructura de software estandarizada
7. Requerimientos básicos firmes
8. Metodología Formal
9. Estimaciones realistas
10. Otros (puntos de control frecuentes, planeación adecuada, equipo de trabajo competente, sentido de propiedad del proyecto)

Si consideramos los factores señalados, vemos que su cumplimiento, crítico como es para el éxito del proyecto, nos señala que en los proyectos en que no se contó con estos factores, se concretaron riesgos específicos en estos elementos que el equipo de proyecto no logró resolver, enfrentándose a sus consecuencias.

3 - ¿Qué es riesgo?

Antes de considerar los enfoques recomendados para una administración de riesgo efectiva, revisemos los conceptos base del riesgo propiamente.

De acuerdo con el Project Management Institute [PMI 2004], *riesgo* es:

- "un evento o condición incierta que, si ocurre, tiene un efecto positivo o negativo en al menos uno de los objetivos del proyecto, tales como tiempo, costo, alcance o calidad", y
- "La *administración del riesgo del proyecto* incluye los procesos relacionados con llevar a cabo la planeación de la administración de riesgos, su identificación, análisis, respuesta, monitoreo y control en un proyecto. La mayoría de estos procesos se ejecutan durante el desarrollo del proyecto. Los objetivos de la administración de riesgos son maximizar la probabilidad y consecuencias de eventos positivos, y minimizar la probabilidad e impacto de eventos adversos al proyecto"

Todo proyecto, en su carácter de esfuerzo único que enfrenta la organización, tiene elementos de incertidumbre que dan origen a los riesgos particulares del proyecto. Se tienen riesgos conocidos que son aquellos que han sido identificados y analizados, para los que se puede planificar una respuesta según los procesos de la Administración del Riesgo descritos más adelante. Los riesgos desconocidos no se pueden manejar en forma proactiva, por lo que su mitigación adecuada se limitará a una planeación contingente, al igual que sucede con los riesgos conocidos cuya mitigación, por razones de costo o efectividad, no es recomendable desarrollar un plan de respuesta.

Las organizaciones generalmente perciben el riesgo como una amenaza al éxito del proyecto, pero la incertidumbre puede estar asociada a una oportunidad que aumente las probabilidades de éxito. Estas oportunidades, al identificarse, deben asimismo ser atendidas generando un plan de respuesta para aprovecharlas si se presentan.

Tanto las organizaciones como los individuos tienen distintas actitudes ante el riesgo. Al iniciarse un proyecto, deben revisarse estas actitudes, de manera que se defina un ambiente de identificación y valoración del riesgo consistente con los objetivos de la organización ante el proyecto por desarrollar. El entusiasmo y la percepción de logro o éxito anticipado que se puede tener al inicio de un proyecto puede llevar a los involucrados a fallar en la identificación y valoración de los riesgos que enfrentarán, lo que aumenta la amenaza de aquellos riesgos que son menospreciados o ignorados.

La actitud general ante el riesgo debe ser explícita y comunicada en forma abierta y honesta, estableciendo el balance deseado entre aceptación de riesgos y los niveles de inaceptabilidad que determinan qué riesgos no se deben enfrentar, o no se está dispuesto a hacerlo. A partir de esta actitud, la administración del riesgo será asumida con compromiso, proactividad y consistencia durante el desarrollo del proyecto.

Para ilustrar lo anterior, tomemos el caso de un proyecto de desarrollo de un sistema transaccional en Internet, recientemente desarrollado para una organización local. Al inicio del proyecto, sin mayor evaluación, y tras haber concluido el proceso licitatorio necesario para la contratación, el cliente pidió que la aplicación fuese construida con la última versión disponible de la herramienta de desarrollo. Ni el cliente ni la empresa desarrolladora efectuaron un análisis

de los riesgos involucrados: esta última versión estaba recientemente liberada, su proveedor aún no iniciaba los cursos necesarios de familiarización con las diferencias entre esta versión y la anterior, la que estaba siendo "estudiada" por su personal técnico.

El proyecto se inició en este contexto sin mayor consideración al tema, según la planificación de desarrollo inicialmente planteada. Transcurridas las etapas de Definición de Requerimientos y aún de Diseño, se empezó la construcción del sistema con la versión mencionada, para encontrar, como era de temerse, que el equipo de trabajo no tenía el dominio adecuado de las diferencias, que resultaron ser extensas e importantes, tanto que el ambiente de producción requerido exigía la actualización de las otras aplicaciones que poseía el cliente para poder implementar el nuevo sistema.

Peor aún, los equipos de producción de que se disponía no eran adecuados para manejar las exigencias de recursos (memoria, distribución de procesos) de la versión escogida. La falta de experiencia con estos requerimientos fue obvia tanto en el equipo de desarrollo como en la contraparte técnica del cliente, que entraron en la usual devolución de culpas hasta que el proyecto fue cancelado por el cliente, alegando "incumplimiento de contrato".

Un caso claro de una Administración de Riesgos deficiente, por no decir inexistente...

Contrastemos lo expuesto con la siguiente recomendación del Software Technology Support Center [STSC 1995]:

- "El desarrollo de software es uno de los desafíos de administración más expuestos al riesgo de esta década. Factores de riesgo están frecuentemente presentes, los que pueden impactar negativamente el proceso de desarrollo y, si se ignoran, pueden llevar a la falla total del proyecto. Para contrarrestar estos factores, los riesgos del software deben ser **activamente** valorados, controlados y mitigados **en forma rutinaria**."

Posterior a la conclusión anotada, el STSC, unidad de la Fuerza Aérea estadounidense creada para apoyar los procesos de adquisición y compra de aplicaciones de software para esta rama militar y asesor del Departamento de Defensa, ha continuado trabajando de cerca con el Software Engineering Institute (SEI), de la Universidad de Carnegie Mellon, una de las instituciones más prestigiadas en el apoyo a la conceptualización y soporte constante al desarrollo de la Ingeniería de Software.

Procedamos ahora a analizar cómo enfrentar la problemática descrita mediante una aplicación efectiva del objetivo de este informe.

4 - Administración del riesgo en proyectos

Una pobre Administración del Riesgo incide en un resultado insuficiente en el proyecto total, que lo coloca en alguna situación comprometida como las descritas anteriormente.

Aunque las distintas disciplinas en las que se aplica la Administración del Riesgo presentan sus facetas, objetivos, herramientas y valoración en forma particular según los elementos que definen su éxito o fracaso, en la Administración de Proyectos, de acuerdo con los lineamientos presentados en el Cuerpo de Conocimiento de Administración de Proyectos (Project Management Body of Knowledge, PMBOK [PMI 2004]), recopilado y difundido por el Project Management Institute (PMI), se establecen los procesos básicos que se deben ejecutar para lograr una Administración de Riesgo efectiva, dentro del proceso de administración y ejecución de un proyecto dado.

Partimos del enfoque genérico del PMI para estructurar los procesos básicos de la Administración del Riesgo. El PMI es una organización multidisciplinaria cuyas publicaciones involucran la participación de profesionales de la mayoría de las industrias representativas del quehacer humano – aeronáutica, defensa, automotriz, e-business, servicios financieros, gobierno, recursos humanos, tecnologías de información, telecomunicaciones, manufactura, energía, farmacia, distribución – nombrando sólo algunos de los más de 30 "Grupos de Interés Específico" ó SIGs por sus siglas en inglés (Specific Interest Group). Afortunadamente, la conceptualización de estos procesos es adecuadamente aplicable al área de sistemas de información, foco de este informe.

De acuerdo con el PMBOK, estos procesos básicos son:

1. Planeación de la administración del riesgo
2. Identificación de riesgos
3. Análisis cualitativo del riesgo
4. Análisis cuantitativo del riesgo
5. Planeación de la respuesta al riesgo
6. Monitoreo y control del riesgo

En nuestra exposición posterior, presentamos los apartados descriptivos de estos procesos agrupando los procesos de Análisis, incluyendo los análisis Cualitativo y Cuantitativo, así como las consideraciones reflejadas en los apartados sobre tolerancia al riesgo y toma de decisiones en condiciones de incertidumbre.

Así, nuestro esquema, que continúa estando apegado a los lineamientos del PMI en contenido y consistencia, se presenta como:

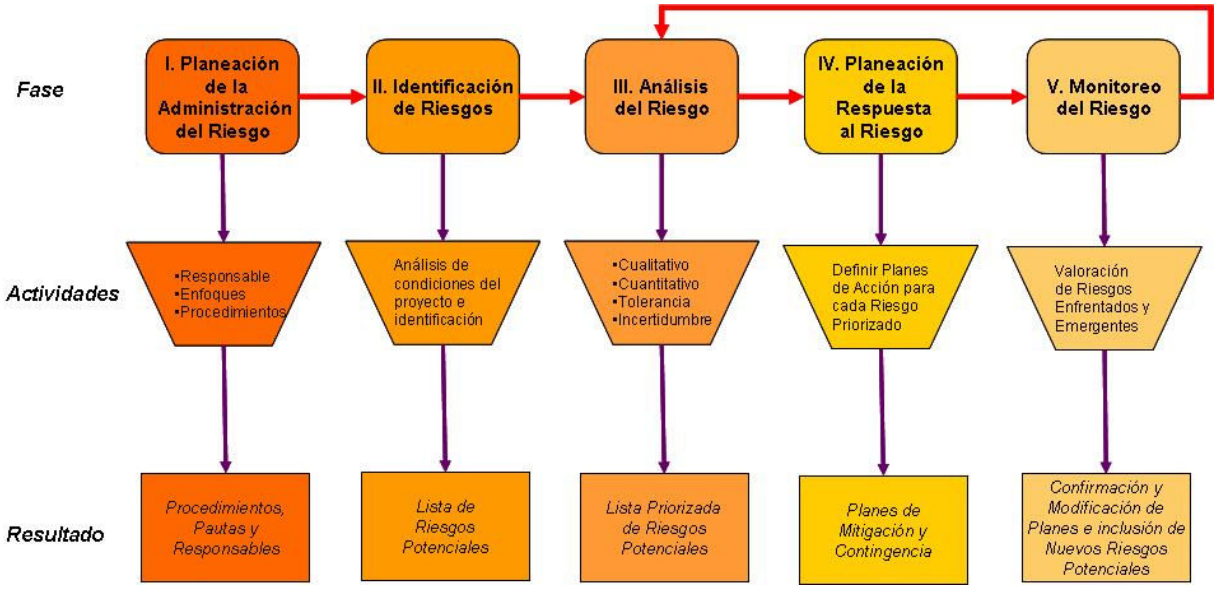


Figura 3 - Ciclo de vida de la administración del riesgo

Adicionalmente, las características de necesidad de un proceso continuo y permanente para la administración del riesgo por toda la duración del proyecto, ha llevado a formular este proceso como un ciclo continuo que se ilustra en la siguiente gráfica:

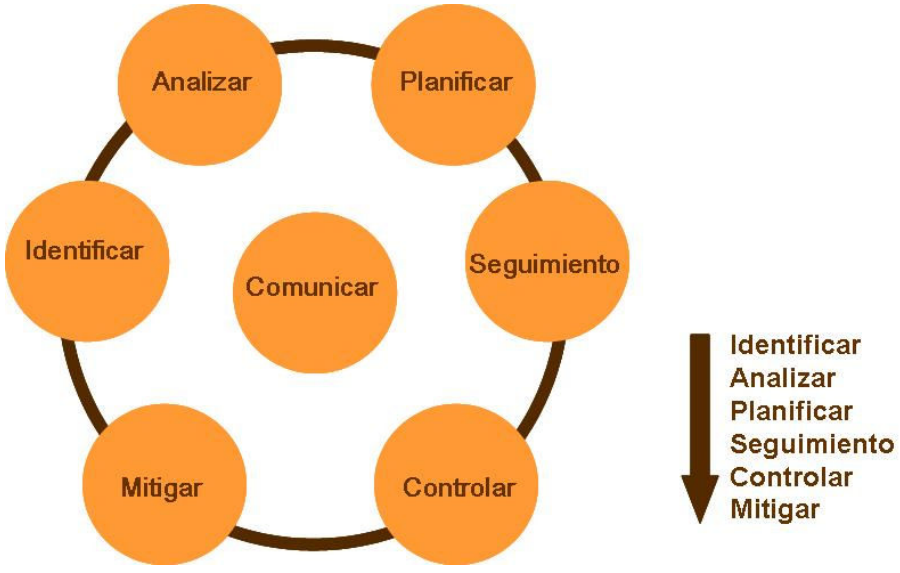


Figura 4 - Ciclo de la administración del riesgo [SEI 1997]

En la literatura disponible sobre el tema se presentan formas variadas de presentar este ciclo, entre ellas la consideración de elementos que se consideran ayudas valiosas para una administración más efectiva, como lo hace el SEI [SEI 1995], al incorporar en esta administración una participación más explícita del equipo de trabajo del proyecto. En el Anexo 1 se incluye la gráfica que ilustra los elementos adicionales por considerar y su descripción.

Podemos encontrar, a manera de corroboración de la validez de los conceptos, enfoques de estructuración de la Administración del Riesgo en publicaciones más específicas en este campo (i.e. [McConnell 1996]), en que los procesos recomendados para esta administración son esencialmente los mismos, al partir del trabajo pionero en ingeniería de software realizado por Barry Boehm [Boehm 1989]. Seguidamente presentamos gráficamente los tres primeros niveles de su modelo de riesgos de proyecto:

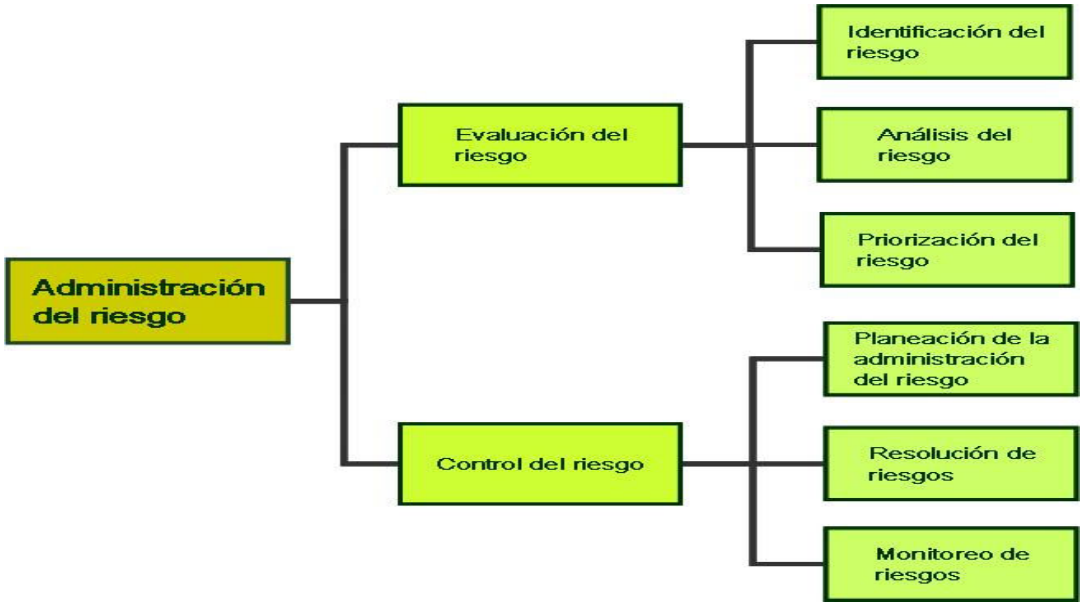


Figura 5 - Modelo de riesgos de proyectos de Boehm [Boehm 1989]

Seguidamente analizamos los procesos propuestos según este esquema:

4.1. - Planeación de la administración del riesgo

El proceso de administración del riesgo se basa en la definición formal y anticipada al inicio del proyecto de cuáles son los enfoques, estrategias, responsabilidades y actividades que formalmente se llevarán a cabo durante el desarrollo del proyecto para minimizar el impacto de los riesgos identificados.

Qué elementos se deben analizar, con qué frecuencia se valorará su evolución, cómo y dónde se decide la aplicación de las medidas definidas en el plan de respuesta de cada riesgo identificado, así como qué indicadores se considerarán en el monitoreo de riesgos, los criterios para determinar

si un riesgo ha sido superado (cuando la situación, acción o evento posible deja de ser un riesgo para el proyecto), y los mecanismos de constante vigilancia para detección de riesgos emergentes.

Esta definición estructural para llevar a cabo una administración de riesgo efectiva conlleva definir claramente, según la situación y envergadura del proyecto en cuestión, quién será el responsable de ejecutar esta administración y cuáles serán sus pautas de acción. Según las características del proyecto y el nivel de experiencia del equipo de trabajo en el desarrollo de proyectos similares, esta responsabilidad puede requerir la designación de un miembro del equipo con un nivel de dedicación significativo a este monitoreo, o puede ser asumida por el líder del proyecto, quien debe establecer claramente en qué momento "se pone el sombrero" de administrador de riesgos para verificar la situación general en este tema.

De experiencias analizadas recientemente (en al ámbito nacional, en una empresa de desarrollo de software), cabe ilustrar el punto con lo sucedido en un proyecto específico que llegó a una situación de fracaso por rechazo del cliente en sus etapas finales. Se detectó que, pese a haberse efectuado una identificación inicial de riesgos (por ejemplo, la posibilidad de carencia, pérdida ó cambio del patrocinador del proyecto), al no haberse definido claramente quién era el responsable de esta administración, se provocó que el equipo entero de proyecto, al enfrentar primero los rumores y luego la materialización de la pérdida del patrocinador del proyecto en el cliente, no reaccionara del todo, esto es, no administrara ni ejecutara plan alguno de mitigación, lo cual llevó al proyecto a una situación de orfandad evidente cuando se presentaron problemas sobre los criterios de aceptación del producto de software desarrollado.

No sólo necesitamos conocer los procesos de administración del riesgo, sino que la definición de quién es responsable de la efectividad de esta administración es tan crítica como la definición de otras responsabilidades específicas en el equipo de trabajo del proyecto, tanto por parte del grupo desarrollador, como por la contraparte del cliente del proyecto.

En resumen, el proceso de planeación de la administración del riesgo consiste en la definición de responsabilidades, pautas de monitoreo y control, y procedimientos de acción ante la variación en las situaciones de riesgo identificadas, además de la definición de los mecanismos de comunicación de la evolución de los riesgos considerados.

4.2. - Identificación de riesgos

Como mencionáramos en la introducción de este informe, lo que más claramente podemos identificar como elemento cambiante sobre la actitud individual y social ante el riesgo en el nuevo siglo, ha sido la toma de conciencia de las consecuencias y costos relacionados con los riesgos que se enfrentan en la mayoría de las actividades humanas.

Por definición, un proyecto es el emprendimiento de un esfuerzo que no se ha llevado a cabo anteriormente y no se repetirá en las mismas condiciones a futuro. El hecho de que las personas, las necesidades, la tecnología, las condiciones sociales y ambientales cambien de un proyecto a otro, lo convierten en un esfuerzo particular y único, y consecuentemente tendremos nuevos riesgos asociados con todas las variables cambiantes, lo que nos llevará a la necesidad de analizar en cada instancia, en el proceso de conceptualización y definición de cada proyecto, qué riesgos particulares enfrentamos.

Según la disciplina, podemos ciertamente considerar los riesgos identificados previamente (en otros proyectos), y añadir a la lista de posibilidades aquellos que han tenido un impacto significativo en el desarrollo de esas experiencias. Pero estas consideraciones son de utilidad referencial, y sólo el análisis detallado y actualizado de las condiciones que enfrentará el proyecto en cuestión permitirá identificar qué riesgos probables enfrentaremos en su realización.

Disponemos de un gran número de fuentes, como las mencionadas en las fuentes referenciales de este informe, sobre el tratamiento de riesgos y del análisis de experiencias previas, para definir una lista base de posibles riesgos, pero no se trata de "escoger" de esta lista cuáles riesgos vamos a incluir en el Plan de Administración del Riesgo del proyecto, sino más bien de tomarlos como referencia y analizar profundamente el entorno organizacional, las características tecnológicas, las condiciones operativas, las experiencias previas del cliente y del equipo de desarrollo, etc., que nos lleven a determinar con exactitud y profundidad cuáles son los riesgos que deben ser valorizados y priorizados, y sobre ellos efectuar una definición de plan de respuesta realista y ejecutable para mitigar su aparición en el desarrollo del proyecto.

Los riesgos que enfrentamos en todo proyecto pueden tener causas internas o externas. Las causas internas son las que de alguna manera están dentro del área de influencia del equipo de proyecto, siendo identificables en el esquema estructural del proyecto, y su atención, análisis y toma de decisiones adecuadas minimiza el que se materialicen los riesgos asociados en el proyecto. Las causas externas son aquellas que están totalmente fuera de esta área de influencia y, por lo tanto, aunque se logre identificarlas; posiblemente sea conveniente manejarlas mediante provisiones de contingencia en el plan y en el presupuesto del proyecto.

El proceso de análisis para la identificación de riesgos empezará así con identificar las posibles causas de problemas que el proyecto enfrenta.

Según McConnell [McConnell 1996], los factores principales identificados como asociados a los riesgos que enfrentan los proyectos más frecuentemente se relacionan con tres elementos:

- Cometer alguno de los "errores clásicos" de los proyectos informáticos
- Ignorar los "fundamentos del desarrollo de software"
- Fallar en la administración activa del riesgo como se describe en este informe

Los "errores clásicos" identificados por McConnell se clasifican en:

a) Relacionados con la Gente (i.e.: motivación débil, socavada o inexistente, personal mediocre o insuficiente capacitado para las tareas asignadas, expectativas poco realistas tanto del cliente como del equipo de proyecto, falta de un patrocinador efectivo del proyecto que defina, aclare y defienda oportunamente las acciones propuestas por el equipo de proyecto)

b) Relacionados con el Proceso (i.e.: planificación excesivamente optimista, gestión de riesgos insuficiente, fallas en el contrato, abandono del plan de trabajo al estar bajo presión)

c) Relacionados con el Producto (i.e.: requerimientos excesivos, cambios en funcionalidad durante el desarrollo, negociación constantemente fluctuante)

d) Relacionados con la Tecnología (i.e.: síndrome de la panacea: el proyecto no puede resolver de la noche a la mañana todos los problemas de la organización asociados a

su área de acción, cambio de herramientas en medio proyecto: versiones, herramientas complementarias, plataforma)

Los Fundamentos del Desarrollo del Software se refieren los principios esenciales relacionados con la Administración (estimación, planificación, seguimiento y valoración de métricas), los principios Técnicos (administración de requerimientos, diseño, construcción, administración de la configuración) y los principios del Aseguramiento de la Calidad (pruebas, revisiones técnicas). La no atención de estos principios es más bien una falla de desempeño profesional en el equipo de trabajo, pero el Gerente de Proyecto debe asegurar que el desarrollo propuesto cumple a cabalidad con las mejores prácticas aplicables en estas áreas. Un desarrollo de proyecto que no sigue un método consistente enfrentará múltiples riesgos en cada una de sus etapas que posiblemente den al traste con el propio proyecto.

Por último, la referencia a la Administración Activa del Riesgo enfatiza el objetivo de esta discusión. La Administración del Riesgo no es un elemento opcional, ni se puede "medio llevar" sin que esta actitud tenga serias y posiblemente fatales consecuencias para el proyecto.

Complementariamente, en el desarrollo de la capacidad de identificación de riesgos necesaria para este proceso, podemos considerar la propuesta de clasificación para la identificación de riesgos planteada por Lyytinen [Lyytinen 2000], en la delineación empírica de seis componentes de riesgo en el desarrollo de software obtenida mediante una encuesta, que presentamos con los principales factores de influencia para cada componente:

1. Riesgos de cronogramación y tiempo, referidos a la planeación de actividades y su correspondiente estimación de esfuerzos:
   a. experiencia en métodos de administración de riesgos
   b. uso regular continuo de métodos de administración de riesgos
   c. dimensión del último proyecto realizado
   d. experiencia del líder del proyecto
   e. conocimiento y características de la industria (en nuestro caso, del desarrollo de software)
   f. tipo de la aplicación desarrollada

2. Riesgos de funcionalidad del sistema:
   a. análisis de decisiones clave
   b. nivel de estandarización de los métodos de administración de riesgos
   c. complementariedad y coordinación entre los métodos de administración de riesgos y los métodos de desarrollo
   d. características de la industria
   e. entrenamiento del líder de proyecto
   f. experiencia del líder de proyecto

3. Riesgos de subcontratación:
   a. extensión del entrenamiento en administración de proyectos
   b. experiencia en la administración de proyectos complejos y/o extensos
   c. el tamaño de la organización de software (subcontratista)

4. Riesgos de administración de requerimientos

La administración de requerimientos se fortalece con un compromiso en la aplicación de métodos de administración de riesgos y enfocándose (frecuente, no esporádicamente), en analizar aquellas partes del plan de proyecto o especificaciones que se encuentren débilmente definidas.

a. herramientas de administración de proyectos
b. uso de metodología de desarrollo
c. arquitectura del hardware
d. tipo de aplicación

5. Riesgos de uso y desempeño de los recursos
   a. experiencia con métodos de administración de riesgos
   b. características de la industria
   c. el tamaño de la organización de software

6. Riesgos de administración del personal
   a. extensión de la aplicación de los métodos de administración de riesgos
   b. nivel de estandarización de los métodos de administración de riesgos
   c. características de la industria
   d. educación del líder de proyecto
   e. arquitectura del hardware (dominio, solidez, experiencia)
   f. uso de metodologías de análisis y diseño
   g. tipo de la herramienta de administración de proyectos

Estos componentes y sus factores de influencia, que se repiten en algunos de los componentes, nos permiten, en el momento de analizar el proyecto para identificar sus riesgos, considerar el estado de la realidad que enfrentaremos en su desarrollo según las características específicas del proyecto de interés. Mayor discusión de otras consideraciones podemos encontrarlas en las referencias de [Lyytinen 1996] y [Lyytinen 1998], que presentan un marco de trabajo conceptual para el análisis del proyecto en el proceso de identificación de riesgos.

Una vez que se han identificado las fuentes de posibles riesgos y se ha levantado una lista de las más relevantes para el proyecto en cuestión, es recomendable que el equipo de proyecto (incluyendo la contraparte del cliente), efectúe una sesión de análisis conjunta a fin de valorar la completitud de esta identificación, agregando o desechando elementos según sea requerido.

El objetivo del proceso será tener una lista de los Riesgos más relevantes que debe enfrentar el proyecto.

Como ejemplo, veamos la lista de los 10 Riesgos más comunes según Boehm & Jones [Boehm & Jones]:

1. Incremento no valorado de funcionalidad
2. Perfeccionismo de requerimientos o del desarrollador (“enchapado en oro”)
3. Escatimar en la calidad
4. Planificación excesivamente optimista
5. Diseño inadecuado
6. Síndrome de la solución mágica y rápida (“silver bullet”)
7. Desarrollo orientado a la investigación
8. Personal mediocre
9. Fallas en la contratación
10. Desacuerdos entre desarrolladores y el cliente

Cabe resaltar que en la lista anterior, los riesgos se presentan en su orden de importancia según la incidencia o peligrosidad que tienen para la generalidad de los proyectos según el análisis efectuado por Boehm en la década de 1980, sobre sus experiencias en la industria de defensa de los Estados Unidos. Debemos considerar en nuestro análisis las diferencias que esta identificación

presentaría en una organización gubernamental o una empresa según sus características particulares.

Si analizamos estos riesgos, es probable que detectemos algunos que ya hemos enfrentado en proyectos previos, pero, como se señaló anteriormente, los riesgos que determinemos que deben estar en nuestra lista de riesgos principales son los que hemos seleccionado después de un análisis cuidadoso, bien pensado y referido a las realidades contextuales de nuestro proyecto. Nuestra lista final no necesariamente debe ser ni estar limitada a 10 riesgos. Será de la extensión que la realidad de riesgo de nuestro proyecto indique.

Es en este proceso de identificación de riesgos que debemos asimismo considerar en el análisis los factores críticos de éxito presentados en el capítulo 2 de este informe.

En [McConnell 1996] encontramos una extensa tabla ilustrativa de los riesgos que se presentaron anteriormente (Capítulo 5, Tablas 5.3, traducida e incluida en el Anexo 2 de este informe).

4.3. - Análisis del riesgo

El proceso de análisis del riesgo es vital para determinar la prioridad de atención que se debe dar a los distintos riesgos identificados. En el análisis de los riesgos que enfrenta el proyecto, dependiendo de la experiencia de la organización en los elementos principales del proyecto (alcances, tecnología, requerimientos), podemos utilizar técnicas de tipo:

- Cualitativo
- Cuantitativo
- Valorativo de la incertidumbre de la información o de los datos utilizados, su comprensión y significado, y la tolerancia de la organización y los involucrados.

Con frecuencia, el impacto del riesgo no se puede cuantificar en los términos que se desearían. Por esta razón se utilizan principalmente dos modos de análisis: el análisis cualitativo, en que no se usan números (por su propia inexistencia) y el análisis cuantitativo, que requiere información fidedigna y completa que permita el análisis estadístico del comportamiento esperado en el proyecto según los distintos métodos aplicables.

Para alcanzar el objetivo de una priorización de los riesgos identificados, consideremos que cada riesgo presenta dos componentes primarios para un evento dado:

- Una **probabilidad de ocurrencia** de ese evento (cuán viable es que se llegue a dar el evento identificado)
- El **impacto** de la ocurrencia del evento en cuestión, valorable ya sea mediante una cuantificación de su costo en términos monetarios (costo del trabajo adicional, retrabajo, multas, pérdida de ventas, etc.), o una medición en otros términos (costo de la credibilidad de la organización, posicionamiento de mercado, incapacidad de cumplimiento de objetivos estratégicos u obligaciones contractuales o legales, etc.).

La combinación de estos dos componentes es lo que nos permite tener una valoración relativa de los diferentes riesgos, permitiendo así su priorización.

La diferencia básica entre la decisión de llevar a cabo un análisis cualitativo ó cuantitativo será entonces consecuencia del tipo de información de que dispongamos para dicho análisis. En aquellos casos que no dispongamos de información fidedigna, acumulada y/o histórica sobre el comportamiento organizacional previo, o estadístico del evento analizado, llevaremos a cabo un análisis cualitativo. Si disponemos de información numérica sobre el evento en cuestión, podremos entonces efectuar un análisis cuantitativo.

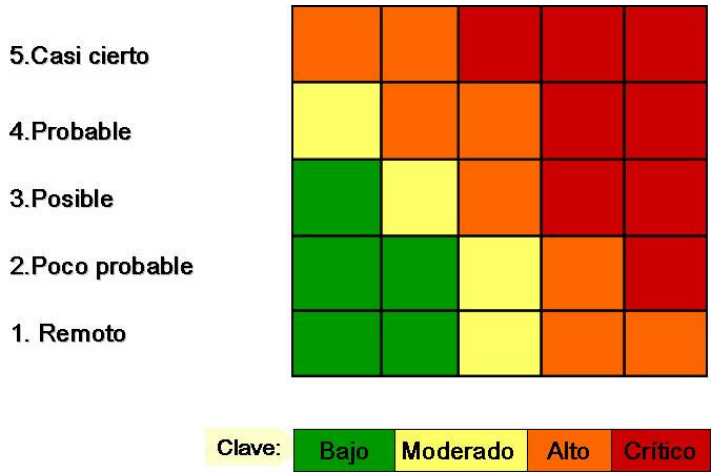
4.3.1. - Análisis cualitativo del riesgo

El análisis cualitativo es así el proceso de valorar el impacto y la probabilidad de ocurrencia de los riesgos identificados, utilizando una calificación apreciativa general tanto para la probabilidad como para el impacto.

Como ilustración de este proceso, desarrollaremos un ejemplo general en el cual construimos una matriz de valoración que nos simplifique la calificación del riesgo considerado en sus dos dimensiones: su probabilidad de ocurrencia y su impacto sobre el proyecto en caso de presentarse.

Para esto, utilizamos una matriz de 5x5, con la probabilidad de ocurrencia en el eje **vertical**, y el impacto en el eje **horizontal.** Veamos cómo se construye la matriz:

1. Para calificar la **probabilidad de ocurrencia**:

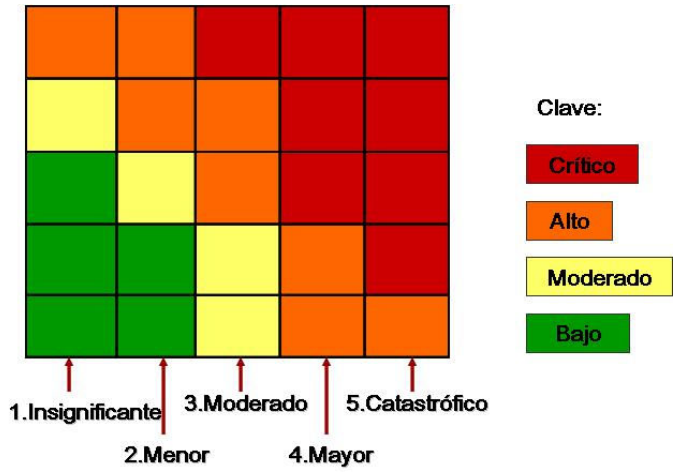


(La **probabilidad de ocurrencia** de un riesgo es evaluada en escala de 1 a 5)

Figura 6 – Construcción de una matriz de valoración de riesgos (Paso 1)

La escala utilizada para valorar la probabilidad de ocurrencia va de 1=Remoto a 5=Casi cierto, y los colores en la gráfica son el resultado de la combinación de esta probabilidad con la valoración del impacto. Debemos considerar que esta valoración es cualitativa por lo que la clave de valor combinado no es el resultado de una fórmula numérica.

2. Para calificar el **impacto**:



(El **impacto** de un riesgo en el proceso se evalúa en escala de 1 a 5)

Figura 7 – Construcción de una matriz de valoración de riesgos (Paso 2)

Obtenemos así una matriz con probabilidad e impacto, que usaremos para valorar los distintos riesgos:

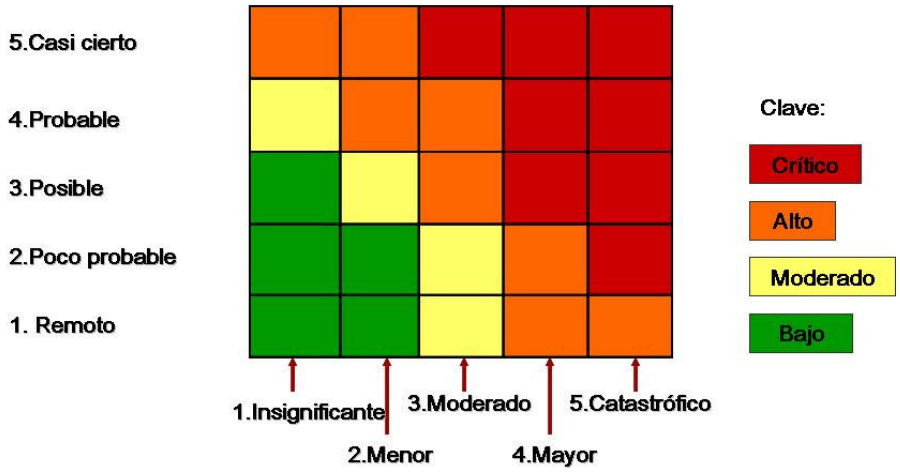


Figura 8 – Construcción de una matriz de valoración de riesgos (Paso 3)

En la gráfica, en que se ha asignado un código de color para la valoración final del riesgo considerado, se utilizan los siguientes criterios:

Bajo

- Impacto mínimo sobre el costo, el tiempo (cronograma) ó técnico. *Una supervisión gerencial normal es suficiente.*

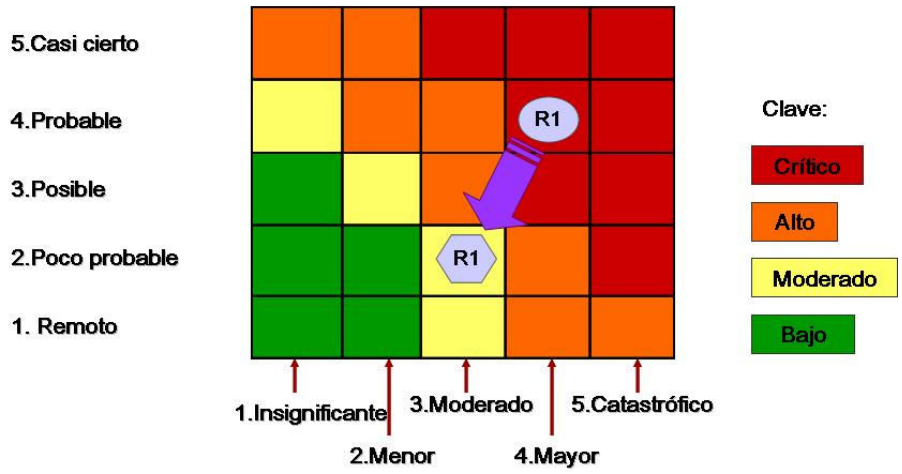
Moderado

- Algún impacto sobre costos, tiempo ó técnico. Puede requerirse de acciones especiales para aliviar el problema. *Una atención gerencial adicional puede ser necesaria.*

Alto / Crítico

- Impacto sustancial sobre el costo, tiempo ó técnico. Acción sustancial requerida para manejar el problema. *Una atención gerencial de alta prioridad es requerida.*

Al calificar un riesgo dado, una vez asignada la probabilidad (i.e. 4, Probable) y el impacto (i.e. 4, Mayor), podemos visualizar la valoración del riesgo (en este caso, Crítico), y analizar hacia dónde nos conviene orientar los esfuerzos de prevención o la estrategia de mitigación (esto es, los esfuerzos de control), para tener una valoración del riesgo que sea aceptable para la organización. En el ejemplo que se presenta seguidamente, se sugiere buscar que la probabilidad sea poco probable y el impacto moderado, ilustrándolo en la Figura 9:



(La porción de riesgo que no es controlada constituye el **riesgo residual)**

Figura 9 – Construcción de una matriz de valoración de riesgos (Ejemplo 1)

La decisión presentada nos llevaría la valoración del riesgo a un área en la matriz donde podríamos considerar aceptable el riesgo. El reto para obtener la calificación buscada es el tema de nuestro proceso de planeación de la respuesta al riesgo (apartado 4.4., adelante), en que definiremos qué hacer para lograrlo.

Ejemplo de aplicación:

Para aclarar nuestra valoración de un riesgo dado, analicemos cómo proceder si determinamos en nuestra identificación de riesgos que nuestro proyecto es susceptible de enfrentar una situación apegada a la definición del riesgo 1 en la lista de Boehm que discutiéramos en el apartado 4.2. (Página 17): "Incremento no valorado de funcionalidad".

En la conceptualización del proyecto, identificamos sus alcances, de acuerdo con los requerimientos que el proyecto debe satisfacer, y consecuentemente efectuamos una planeación de actividades con su estimación de tiempos, para satisfacer el desarrollo de la funcionalidad requerida en el software en cumplimiento cabal de los requerimientos establecidos, lo que efectuamos en un trabajo conjunto con el cliente o usuario "propietario" del proyecto.

Es posible que durante el desarrollo del proyecto, al profundizar con el cliente o usuario respectivo los aspectos detallados del proceso a apoyar por la aplicación en desarrollo para la implementación de la funcionalidad requerida, el cliente puede identificar nuevas funciones, separación o profundización de las ya establecidas, y plantee solicitudes de modificación o ampliación de los alcances funcionales de la aplicación.

Ante esta situación, el líder de proyecto debe analizar cuidadosamente las implicaciones de lo solicitado, a fin de valorar cómo su atención afecta las fases del desarrollo ya cumplidas, tales como el diseño de la aplicación y la arquitectura operativa de la aplicación, así como determinar sus implicaciones en los tiempos establecidos, los recursos planificados y asignados, y el cumplimiento de las fechas límite en que se deben entregar los productos de cada etapa del desarrollo.

Puede determinarse que lo solicitado por el cliente requiere ajustes mínimos en programación, pero no afecta el diseño del sistema ni la arquitectura establecida para su funcionamiento e implementación adecuada, en cuyo caso se puede atender la solicitud e incorporar los ajustes correspondientes en el plan de desarrollo del proyecto, con variaciones en costos, recursos y fechas totalmente aceptados por el cliente porque no inciden significativamente sobre las metas iniciales del proyecto.

Pero también podemos encontrar en la valoración que lo solicitado implica modificaciones al diseño (nuevos módulos, modificación de las estructuras de datos, cambios en la arquitectura: nuevas funcionalidades de plataforma, incremento en la capacidad de almacenamiento y/o proceso, uso de nuevas herramientas o componentes no considerados en la planeación inicial, etc.). En este caso, los resultados del análisis efectuado deben ser discutidos con el cliente y debemos negociar el camino por seguir, ya sea que se acepte modificar el plan de trabajo con aceptación de las variaciones en costo, recursos y tiempo, y se reprogramen las fechas límite para los entregables definidos, o se decida dejar la implementación de las nuevas funcionalidades para ser atendidas en un momento posterior a la conclusión del proyecto de acuerdo con los alcances iniciales.

Es de notar que lo discutido es tan válido para un desarrollo interno en la organización como para un proceso de contratación externa del proyecto.

El escenario discutido es más frecuente de lo que podríamos haber considerado durante la conceptualización y planeación inicial del proyecto, y ha sido la causa de múltiples fracasos de proyectos como discutiéramos en el capítulo 3 (pág. 9).

Si nuestra valoración de esta situación nos señalara que la probabilidad de ocurrencia es “Probable” (considerando la experiencia del cliente, los usuarios y la organización, así como el tipo de aplicación a desarrollar y la intensidad y completitud de la educción y análisis de requerimientos efectuado durante la conceptualización del proyecto), y, tuviésemos una ventana de ejecución del proyecto limitada (por ejemplo, la aplicación debe ser implementada al inicio del próximo ejercicio fiscal), que nos indica que atrasos en la ejecución por situaciones como la discutida tendrían un efecto catastrófico que podría llevar a la cancelación del proyecto o a un atraso en las metas organizacionales con serias consecuencias (i.e. la aplicación por implementar es crítica para el cumplimiento de normativas de la industria correspondiente), la valoración de las dos dimensiones del riesgo las podemos reflejar en nuestra matriz de análisis (Probable/Catastrófico => Riesgo Crítico):

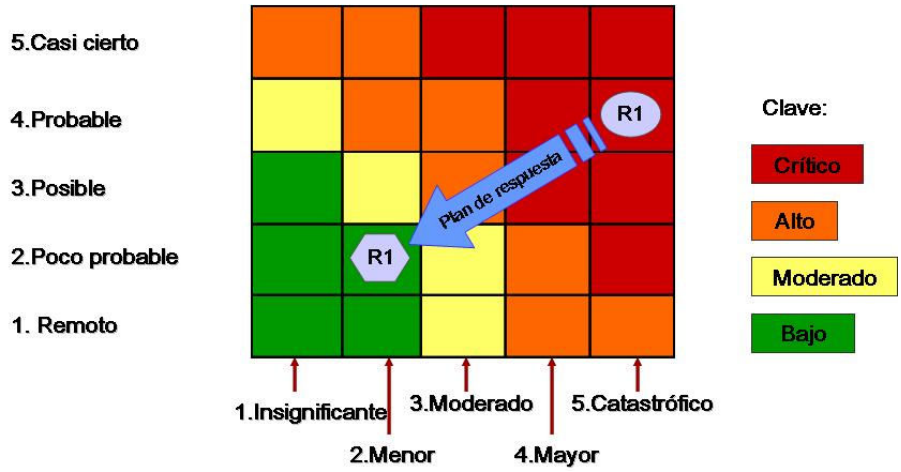


Figura 10 – Construcción de una matriz de valoración de riesgos (Ejemplo 2)

Seguidamente, en el proceso de planeación de la respuesta al riesgo (apartado 4.4.), se define qué hacer para lograr que la valoración de un riesgo, si desarrollamos y ejecutamos su plan de respuesta en forma efectiva, pase a una situación de riesgo residual que consideremos aceptable (i.e. Poco probable/Moderado => Riesgo Bajo).

4.3.2. - Análisis cuantitativo del riesgo

Con el proceso de análisis cuantitativo se busca también valorar el impacto y la probabilidad de ocurrencia de los riesgos, pero utilizando métodos de calificación más elaborados, cuyo resultado depende de la disponibilidad de información precisa y pertinente sobre el proyecto. Con algunos de los métodos se procede a la obtención, análisis y tabulación de información para conseguir un enfoque de valoración adecuado.

Seguidamente se presentan algunos de los métodos utilizados en este tipo de análisis, con una caracterización breve de su procedimiento particular, según lo encontramos en [Futrell 2002]:

- Método Delphi:
  1. Se selecciona un panel de expertos (aislados y desconocidos unos de otros)
  2. Se prepara y circula un cuestionario sobre riesgos
  3. Se solicitan enfoques y opiniones sobre manejo de riesgos
  4. Se comparten todas las respuestas y retroalimentación estadística con todo el grupo
  5. Se repite el ciclo hasta obtener convergencia en un enfoque de consenso
- Análisis de sensibilidad:
  1. Se escogen unas pocas variables con gran impacto en el plan
  2. Se define un rango probable de variación
  3. Se evalúa el efecto de su cambio en los resultados del proyecto

- Análisis de probabilidad:
  1. Se procede en forma similar al análisis de sensibilidad
  2. Se añade una distribución de probabilidad para cada variable, usualmente ajustada para evitar el efecto del optimismo
- Simulación de Monte Carlo:
  1. Se procede en forma similar al análisis de probabilidad
  2. Se asignan valores escogidos al azar para cada variable
  3. Se corre la simulación un número de veces para obtener la distribución de probabilidades del resultado
  4. Produce un rango de probabilidades para el resultado
- Análisis de árbol de decisiones:
  1. Método gráfico
  2. Fuerza las consideraciones de probabilidad para cada resultado
  3. Usualmente aplicado a costo y tiempo

Es conveniente mantener en mente el más crítico aspecto de la cuantificación del riesgo: todos los valores numéricos son derivados de las mejores estimaciones, y como tales su aplicación a un proyecto que aún no se desarrolla tiene todo el peso de la incertidumbre asociada a su aplicabilidad.

Veamos un ejemplo de aplicación del método de análisis de árbol de decisiones:

La cuantificación del riesgo se inicia con el cálculo del factor de exposición al riesgo (FER), según la fórmula siguiente:

FER = [Probabilidad de ocurrencia (P)] x [Cantidad en discusión (C)]

El ejemplo que se presenta es aplicable a la valoración del riesgo asociado a un concurso de contratación en que se establece un premio por entrega anticipada del producto del proyecto ($100,000 bajo un cronograma acelerado o agresivo, cuya probabilidad de cumplimiento real se estima en 0.2), y una multa por entrega tardía bajo el cronograma regular ($250,000), cuya probabilidad de cumplimiento es de 0.9. ¿Se debe presentar un cronograma acelerado o regular?

Veamos el árbol de decisión:

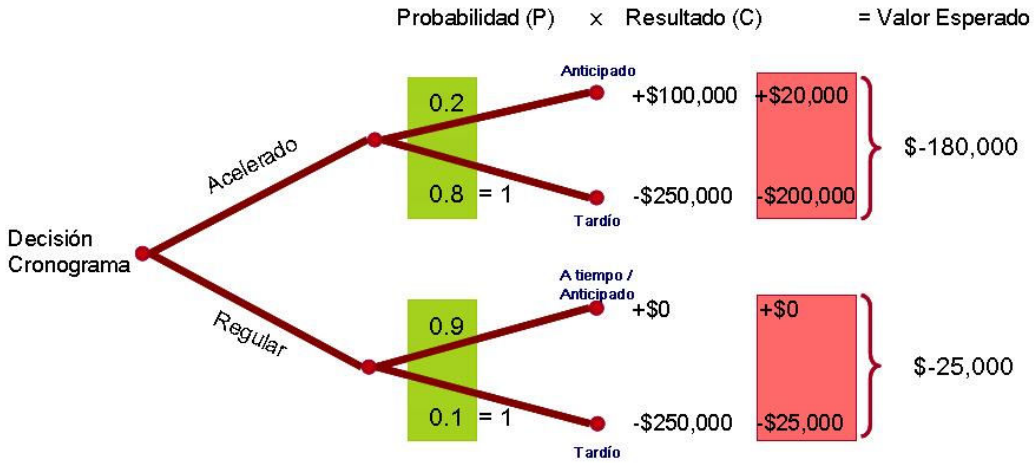


Figura 11 – Análisis de Árbol de Decisiones (Ejemplo 3)

El árbol de decisión presentado nos muestra que escoger un cronograma acelerado implica una pérdida potencial de $180,000, en tanto que un cronograma regular tiene una pérdida potencial de sólo $25,000. El líder de proyecto, seleccionando un cronograma regular, aún tiene la tarea de administrar el riesgo de entrega tardía para reducir este potencial de riesgo, para lo que deberá revisar nuevamente el cronograma y definir un plan de respuesta en el que se planifique seguimiento especial al cumplimiento de todas las actividades que estén en la ruta crítica de la ejecución del proyecto.

Otros métodos identificados como útiles para el análisis cuantitativo son:

- Análisis de costo del ciclo de vida
- Análisis de redes
- Estimación de relaciones
- Escalas de riesgo
- Análisis de tasa de reacción/impacto
- Simulación de EDT (Estructura Desglosada del Trabajo)
- Tendencias tecnológicas de avanzada

En [Kerzner 2001] se presenta un desarrollo detallado del proceso de Monte Carlo con un ejemplo de aplicación en evaluación de colas.

4.3.3. - Tolerancia

La tolerancia al riesgo es lo que permite establecer la medida en la cual la organización está en capacidad de soportar eventos inesperados, de consecuencias inciertas o indeseadas.

Para cada organización se dan niveles de tolerancia, relacionados con la disposición o actitud ante el riesgo, a los que se asocia una capacidad de tolerancia (asimilación de las consecuencias), como por ejemplo, en el ejemplo del apartado anterior, la capacidad de la organización de enfrentar una pérdida de $180,000 al haber escogido proponer llevar el proyecto bajo un cronograma acelerado. Si la organización es financieramente débil, buscar el "premio" propuesto

de los $100,000 y no lograrlo, la puede llevar a una virtual quiebra si no logra alcanzar las metas de desempeño, cumplimiento y entrega propuestas en este cronograma.

Las organizaciones deben estar en capacidad de definir su ámbito de tolerancia, incluyendo el hecho de que este implique tener pérdidas hasta cierto nivel. Este ámbito de tolerancia debe ser real, pues no se puede decir que se está dispuesto a perder mucho cuando en la realidad si se pierde poco, se puede perderlo todo.

El que una organización tome más o menos riesgo, depende de la persona que está a cargo de tomar la decisión. Esta persona es la encargada de generar escenarios para el análisis y decide qué hacer o cuánto está dispuesta a perder. Un buen tomador de decisiones tiene que estar consciente de su realidad y el entorno de la organización, para saber su capacidad de absorción de un impacto negativo de riesgo. Una persona que toma decisiones tiene sus propias limitaciones y actitudes y debe estar consciente de ello también.

Por ejemplo, cuando se hace un análisis de tolerancia para poner un producto en el mercado, se puede pensar en las probabilidades de reacción del mercado con respecto del producto, las cuales podrían ser buenas, mediocres o malas. También se podría decir que el producto puede ser construido utilizando tres métodos diferentes, lo que permitiría ponerlo en el mercado de cierta forma, cada una de las cuales podría significar niveles de riesgo de mayor o menor intensidad.

Veamos la siguiente gráfica, presentada en [Futrell 2002]:

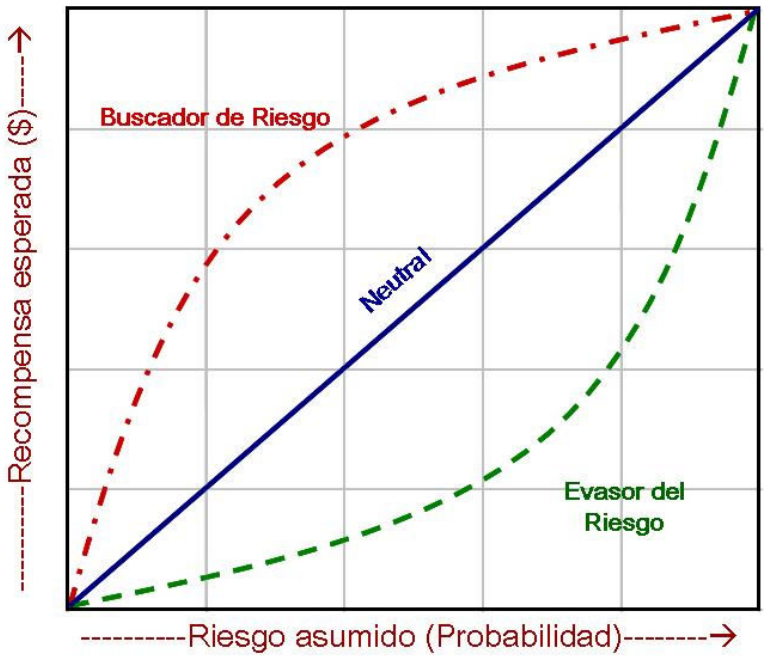


Figura 12 – Variaciones en la Tolerancia al Riesgo [Futrell 2002]

Los líderes de proyecto deben identificar su nivel de tolerancia al riesgo, el que varía según el individuo y la organización. La Figura 12 se obtuvo de respuestas comparativas en decisiones alternativas. La línea central del origen a la esquina derecha superior representa el riesgo neutral, definida por los puntos de equilibrio entre las cantidades en juego ($s), y la probabilidad de ocurrencia del evento de riesgo. Los "buscadores de riesgo" (individuos, equipos de trabajo y organizaciones), siguen la línea superior, aumentando las pérdidas potenciales si el evento de riesgo ocurre. Los "evasores del riesgo", por el contrario, seguirán la línea bajo la línea neutral. Aunque se pueda evadir el riesgo, hay un costo de oportunidad que se incurre bajo la línea neutral, al invertir para evitar riesgos que pueden no presentarse, con lo que se pierden las cantidades invertidas, que podrían haber dado un rendimiento invirtiéndose de otra manera. Estas oportunidades de rendimiento son el costo de oportunidad. Como mínimo, serían los intereses obtenidos en una inversión sin riesgo en bonos estatales.

4.3.4. - Ruido e incertidumbre

La definición básica del riesgo nos dice de: "un evento o condición incierta que, si ocurre, tiene un efecto positivo o negativo en al menos uno de los objetivos del proyecto, tales como tiempo, costo, alcance o calidad". De esta manera, la incertidumbre es inherente al riesgo.

Sin embargo, cuando analizamos las condiciones de un proyecto, esperaríamos que la identificación y el análisis de riesgos fuese un ejercicio que nos lleve a considerar los elementos inciertos más asociados a la ocurrencia de eventos imprevisibles, que a identificar cuáles de estas condiciones están establecidas de manera ligera e incierta, e identificar los "peligros" asociados con esta incertidumbre.

Sabemos que un proyecto se define en el tiempo con un punto de inicio y uno de término, y entre estos dos puntos se planifica el desarrollo de las actividades que permitirán obtener los productos esperados, cumpliendo con la funcionalidad esperada, dentro de los costos establecidos y con la calidad requerida.

Los ejemplos siguientes, sobre el ruido introducido en la definición inicial del proyecto por acciones u omisiones que se presentan muy frecuentemente en el proceso de desarrollo de software, constituyen elementos clave que deben ser analizados en nuestro proceso de identificación de riesgos y ser tomados muy en cuenta en el análisis de los riesgos para obtener una valoración realista que nos lleve a una priorización adecuada de los riesgos que enfrenta el proyecto, y nos permita establecer planes de respuesta consistentes y efectivos para la mitigación de sus efectos:

- Incertidumbre en los requerimientos del producto
    - Usualmente se da inicio al proyecto antes de que todos los requerimientos se conozcan, y estos están sujetos a cambio durante el proceso de desarrollo, por mayor conocimiento del producto y de su ambiente operacional.
- Variabilidad en el desempeño del personal asignado
    - El proyecto se inicia sin que el personal tenga las habilidades o la experiencia requeridas, las que se complementan durante el desarrollo: la productividad del equipo es variable durante el proceso

- Inexactitud de las mediciones base del proyecto
  - Tamaño, costo, esfuerzo requerido, cronograma y mediciones de calidad
  - Interpretación de los estándares por aplicar a la recolección y análisis de datos sobre el desempeño del proyecto
- Variaciones en la interpretación de los datos de desempeño recolectados
  - Esto depende en gran medida de la experiencia y el juicio de los analistas a cargo, y de su conceptualización de los parámetros por aplicar a los modelos de estimación utilizados

Cualquiera de las situaciones presentadas constituye una fuente de riesgos para el proyecto, cuyos efectos debemos anticipar adecuadamente, de manera que podamos definir una estrategia efectiva y desarrollar los planes de mitigación consistentes con su control.

4.4. - Planeación de la respuesta al riesgo

Tras un exhaustivo proceso de identificación y efectuado el análisis de los riesgos del proyecto para definir su criticidad (la valoración dada a cada riesgo según su probabilidad de ocurrencia e impacto), se efectúa su priorización relativa para obtener la lista de los riesgos que serán el foco del esfuerzo de administración de riesgos.

Para los riesgos así priorizados, el proceso de planeación de respuesta se enfoca seguidamente en decidir qué estrategia aplicar al tratamiento posible de cada riesgo, tomando en consideración las características analizadas sobre la tolerancia de la organización y el líder a cargo del proyecto.

Las estrategias disponibles para su aplicación se ilustran en el siguiente gráfico:

Figura 13 – Estrategias aplicables al tratamiento y manejo de cada riesgo

Las estrategias posibles son entonces **evitar** (no enfrentar el riesgo), **transferir** (pasar o compartir el riesgo con una organización externa al equipo de proyecto), **aceptar** (se toma el riesgo como se presenta, aceptando sus consecuencias), o **reducir** (definir un plan de respuesta que mitigue o minimice su probabilidad de ocurrencia e impacto).

En primera instancia, consideramos si hay manera de evitar el riesgo en consideración. Como se ha señalado, al ser el riesgo un evento incierto, evitarlo implica eliminar completamente las condiciones de su posible presentación en la ejecución del proyecto.

Como ejemplificación, para un proyecto de desarrollo de software, tomamos el riesgo octavo de la lista de riesgos más comunes según Boehm (8. Personal mediocre, [Boehm & Jones], citado en apartado 4.2., página 17 de este informe), consideremos que la mediocridad del personal, en términos del proyecto específico analizado, obedece a que el equipo de proyecto no está suficientemente capacitado en las herramientas a utilizar para la construcción de los productos del proyecto.

Si la experiencia de desarrollo de los integrantes del equipo de proyecto ha sido con Visual Basic en una plataforma .net, utilizando una base de datos SQL, y el proyecto está planteado para utilizar Developer con una base de datos Oracle, en ambiente Unix, es de considerar la posibilidad de que el desempeño de este equipo sea "mediocre" en la utilización de las herramientas propuestas. En las condiciones dadas, la valoración cualitativa de este riesgo nos dice que se presentará con una probabilidad de 5. Casi cierto, y un impacto de 5. Catastrófico, lo que lo ubica como un riesgo crítico para el proyecto.

¿Cómo se puede **evitar** este riesgo en este caso? Las posibilidades directas para la aplicación de esta estrategia serían cambiar el ambiente de desarrollo por el que sabemos es dominado adecuadamente por los integrantes del equipo, o en su defecto no desarrollar el proyecto. Si no es factible escoger una de estas opciones, no es posible evitar el riesgo, por lo que se debe considerar una estrategia distinta.

La aplicación de una **estrategia de transferencia** requiere la asignación de un grupo de desarrollo con probado y efectivo dominio de las herramientas a utilizar (un equipo de trabajo distinto al inicialmente considerado, o una organización externa con experiencia en el ambiente especificado, subcontratable con cláusulas de garantía de cumplimiento sobre tiempos, costo, funcionalidad y calidad de los productos obtenidos). Se analizará entonces la disponibilidad de recursos para aplicar una estrategia de transferencia.

Como tercera posibilidad, la **estrategia de aceptación** del riesgo implica ejecutar el proyecto con los recursos disponibles y en las condiciones presentes, asumiendo en su momento los costos asociados al riesgo identificado. Estos costos pueden estar referidos a extensión del tiempo programado y los costos correspondientes (retrabajo, tiempo de trabajo extraordinario, calidad de los productos obtenidos, etc.).

La última estrategia considerada se refiere a **reducir** la probabilidad de ocurrencia y el impacto de la materialización del riesgo bajo análisis.

Es esta estrategia la que conlleva la elaboración de un **plan de respuesta** que nos permita ejecutar todas las actividades que se consideren adecuadas para reducir a un mínimo aceptable la valoración del riesgo. Se procura entonces que, con la aplicación efectiva del plan de respuesta, la valoración del riesgo varíe de la estimación inicial hacia una calificación aceptada por la organización.

En el ejemplo discutido, requerimos definir cuál es esta valoración aceptable. De acuerdo con la aplicación de la matriz de valoración del riesgo presentada en el apartado 4.3.1. (página 23 de este informe), si se define como valoración objetivo reducir la probabilidad de ocurrencia a un

nivel de 2. Poco probable, con un impacto de 2. Menor, tendríamos su representación gráfica como sigue:

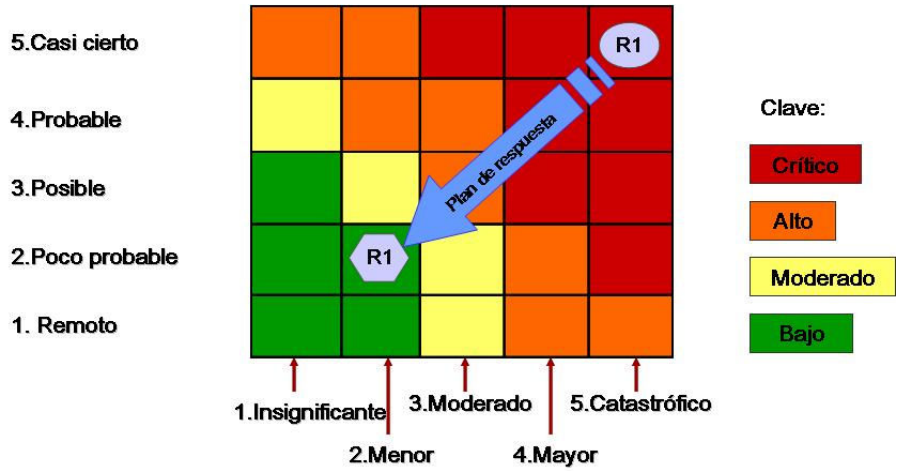


Figura 14 – Matriz de valoración de riesgos (Ejemplo 4)

Así, el plan de respuesta por desarrollar consistirá en identificar y programar la ejecución de las actividades que modifiquen esta valoración hacia el objetivo propuesto. Es importante aclarar que por la naturaleza incierta del riesgo, no buscamos evitarlo, según se discutió anteriormente, sino ubicarlo en un nivel de aceptabilidad. Este riesgo, que sigue presente pero mitigado a un nuevo valor, es el riesgo "residual", remanente siempre presente tras la ejecución efectiva del plan de mitigación definido para su manejo.

Para el riesgo en discusión, podemos identificar las siguientes posibilidades de acción que modifiquen las características "mediocres" del equipo de trabajo:

1. Desarrollo de un plan de capacitación para el equipo de proyecto en las herramientas por utilizar, por ejecutarse previo al inicio de la fase de construcción de los productos del proyecto
2. Validación de la efectividad de la capacitación en un taller guiado y valorado por un experto en la utilización de las herramientas
3. Establecimiento y ejecución de planes de prueba para el aseguramiento de la calidad, rigurosos y oportunos, conducidos por un experto en la utilización de las herramientas, aplicado en puntos de control adecuados a la terminación de productos intermedios y finales de la fase de construcción
4. Monitoreo y control del desempeño del equipo de trabajo, con énfasis en la detección y solución de problemas relacionados con la falta de dominio experto de las herramientas

Cada uno de los elementos presentados debe desglosarse en las actividades específicas que aseguran su ejecución oportuna y rigurosa, sobre la que se centrará el proceso de monitoreo y control del riesgo (apartado siguiente).

Para el primer elemento, las actividades requeridas y su oportunidad en el tiempo pueden ser definidas como sigue:

a. Identificación del proveedor de la capacitación requerida (una semana, ocho semanas antes del inicio de la fase de construcción)
b. Negociación y contratación de la capacitación (si se requiriesen tres semanas para ejecutar la capacitación, la contratación deberá iniciarse seis semanas antes del inicio de la fase de construcción -una semana-)
c. Ejecución de la capacitación (tres semanas, seis semanas antes de la fase de construcción)

Se continuaría con el segundo elemento:

a. Ejecución del taller de validación (una semana, dos semanas antes del inicio de la fase de construcción)
b. Evaluación de resultados y ajustes en el equipo de trabajo de acuerdo con esta evaluación (una semana)

Para los elementos 3 y 4, la definición de actividades se debe desarrollar con un similar nivel de detalle, ubicando cada actividad en el tiempo según la programación de las actividades de la fase de construcción del proyecto, en concordancia con el plan de aseguramiento de calidad integrado a este proceso, y los puntos de control definidos para el monitoreo de la ejecución del plan de proyecto. Para un riesgo como el discutido, el seguimiento de su manejo adecuado se debe programar y efectuar al menos cada semana.

El proceso descrito se aplica cuando reconocemos la posibilidad de mitigar los riesgos identificados. En los casos en que no sea factible su control se deben definir y planificar planes de respuesta contingente, esto es, qué se hace si un riesgo específico se presenta y cómo debe reaccionar la organización para mitigar su impacto, ya que no es posible efectuar actividades para reducir su probabilidad de ocurrencia.

Si consideramos un riesgo de este tipo, por ejemplo, la ocurrencia de un fenómeno natural como un terremoto, sabemos que no hay acciones preventivas posibles para reducir su probabilidad de ocurrencia. Podemos evaluar que según la zona geográfica en que nos encontremos, la probabilidad histórica es mayor o menor (i.e. Cartago o Limón versus San José o San Carlos), pero no hay plan de acción ejecutable para reducir su valoración.

Para un riesgo semejante, se analiza y planea un plan de contingencia. En los centros de proceso de las tecnologías de información que se emplean en una organización, según su criticidad para la operación de la propia organización, esta contingencia se ha enfrentado mediante el diseño e implementación de centros alternos de proceso, que le permitirían a la organización continuar sus operaciones ante la ocurrencia de un evento como el mencionado. La implementación de un centro de contingencia tiene costos elevados (inversión en equipos de proceso de información y comunicaciones, diseño de procedimientos de transferencia de la atención a las operaciones organizacionales, instalaciones y equipos de utilización contingente para la normalización de operaciones, etc.), y puede darse que la organización no esté en capacidad de efectuar estas inversiones, o su valoración del riesgo tenga como respuesta aceptar sus consecuencias sin implementación de medidas de mitigación del impacto. En este último caso, las consecuencias pueden ser la paralización total e incluso la desaparición de la organización.

El desarrollo de planes de contingencia es similar al proceso de planeación de respuesta al riesgo, pero el objetivo de las actividades a desarrollar es la recuperación de la capacidad operativa en el menor tiempo y con el menor impacto permanente que sea factible absorber.

Entre las preguntas clave que debe responder un plan de contingencia podemos citar:

- ¿Quién es responsable de la acción?
- ¿Cuándo debe ejecutarse la acción definida?
- ¿Cuál es la métrica por evaluar en forma periódica para detectar la presentación del evento?
- ¿Cuál es el valor de la métrica es el "disparador" de las acciones contingentes?

En el evento de terremoto mencionado, si monitoreamos el comportamiento de las comunicaciones entre las oficinas centrales de una organización y sus sucursales, podríamos establecer que la métrica a aplicar para proceder a re-enrutar las comunicaciones del centro de proceso principal al alterno sea una interrupción de comunicación con una duración superior a un tiempo establecido (t), y que el valor disparador sea de (t+n). Si t=30 minutos y n=15 minutos, una sucursal incomunicada durante 30 minutos deberá proceder a re-enrutar sus comunicaciones si la situación de interrupción se mantiene 45 minutos después de presentada. En [Futrell 2002] se presenta el desarrollo de una tabla ilustrativa de este procedimiento para los 10 riesgos principales de un proyecto hipotético (Capítulo 18, pp.604-606). Un futuro informe del Club de Investigación Tecnológica abordará precisamente el tema de la administración de los riesgos que se suscitan en las operaciones y servicios de tecnologías de información y comunicación.

4.5. - Monitoreo y control de riesgos

Definidas y programadas las actividades de mitigación para cada uno de los riesgos identificados, el proceso de monitoreo y control de riesgos del proyecto tiene como objetivo asegurar la efectividad de los planes de respuesta definidos.

Las actividades del plan de respuesta de cada riesgo deben ser ubicadas en el tiempo en convergencia con el desarrollo programado de las distintas fases del proyecto y sus actividades (i.e. planeación, diseño, construcción, implementación, etc., según el ciclo de vida por utilizar en el proyecto). La integración en sincronía con las actividades de cada plan de respuesta tienen como objetivo no perder de vista la oportunidad de su ejecución en relación con la planeación del proyecto, y así facilitar su seguimiento y monitoreo.

Como actividad continua y permanente en la administración del proyecto está el monitoreo de la adecuada y oportuna ejecución de estas actividades, así como la valoración periódica de la evolución del riesgo. Como ejemplo, en alusión al caso ilustrado en el apartado 4.3.1. relacionado al riesgo de "Incremento no valorado de funcionalidad", por la naturaleza de este riesgo se puede determinar que su monitoreo será permanente durante toda la fase de construcción e implementación hasta que los productos del proyecto sean aceptados en forma final por el cliente.

En el ejemplo relacionado con el plan de respuesta al riesgo de "Personal mediocre" (apartado 4.4.), el seguimiento del plan cambia de criticidad si al cumplir la actividad 2 (Taller de valoración), se obtiene como resultado una verificación de un nivel adecuado de competencia en el equipo de proyecto, y el aseguramiento de calidad se integra totalmente en las actividades generales del plan de aseguramiento de calidad del proyecto, dentro de las actividades definidas con este fin en los puntos de control correspondientes del proceso de desarrollo.

Otro elemento importante en la administración de los riesgos del proyecto lo constituye la vigilancia constante sobre el ambiente interno y externo a fin de detectar cambios en las condiciones o efectos de los resultados que pudiesen presentar riegos emergentes para su desarrollo, tales como surgimiento de nuevas tecnologías, liberación de nuevas versiones de la plataforma o las herramientas utilizadas, señales de desgaste o pérdida de lealtad en el personal del equipo de trabajo, cambios en el mercado de trabajo, en el mercado del producto en desarrollo o en la industria en que se desenvuelve la organización, surgimiento de nuevas leyes, regulaciones específicas (i.e. en la industria bancaria, nuevas reglamentaciones o exigencias de la autoridad supervisora), etc.

Esta vigilancia constante debe estar enfocada en detectar señales que indiquen que hay posibles nuevos riesgos que analizar y valorar, para eventualmente desarrollar un plan de respuesta para su manejo.

En [Futrell 2002] se presenta un ejemplo de la categorización de riesgos que ilustra el tipo de indicadores que nos pueden ayudar en la identificación de riesgos emergentes (capítulo 18, pp.610-621), así como la elaboración resumida de un reporte de evolución relativa de los riesgos principales de un proyecto para su revisión semanal.

5. Conclusiones y recomendaciones

En el desarrollo de los temas contemplados en este informe, se ha buscado incrementar en el lector la conciencia de la importancia de efectuar en los proyectos informáticos una administración del riesgo comprometida, apoyada por una comprensión profunda de los procedimientos y consideraciones que se deben aplicar en la ejecución de los procesos recomendados por organismos de relevancia internacional sobre el tema, tales como el Project Management Institute, el Software Engineering Institute, el IEEE, la ASQ y múltiples autores que han desarrollado a lo largo de las últimas décadas este tema con acuciosidad e interés en ayudar a los líderes de proyecto y a las organizaciones a efectuar esta administración en forma efectiva y eficiente.

La comprensión de los planteamientos más difundidos sobre el ciclo de vida de esta administración, la explicación de los procedimientos recomendados, y la desmitificación del proceso como un esfuerzo asequible y realizable en todo proyecto para potenciar sus probabilidades de éxito, partiendo de una convicción clara de su importancia, permitirán a los profesionales que enfrentan las distintas responsabilidades en un proyecto y a la administración superior de las organizaciones interesadas, asegurarse y apoyar la disponibilidad oportuna de recursos para la realización de los procesos con conciencia de su importancia y el impacto positivo que su aplicación efectiva tendrá en los resultados del proyecto y en la mejora de los índices de éxito en la ejecución de los proyectos informáticos.

El tema siempre ha sido relevante, y quizá por la toma de conciencia obligada como consecuencia de eventos graves que se han presentado en los años iniciales de este siglo XXI, se ha dado globalmente un impulso a la consideración crítica de procesos como los presentados como una manera de reducir los efectos de la incertidumbre siempre presente en la ejecución de proyectos en las distintas industrias, pero de particular importancia en los proyectos informáticos, dado el cúmulo de resultados insatisfactorios que se ha expuesto y que toda organización y profesional que participa en ellos conoce mediante experiencias cercanas.

La recomendación central sobre la aplicación de lo expuesto es, sucintamente, que en la planeación de los proyectos, el esfuerzo de considerar y aplicar rigurosamente los procesos de la administración del riesgo, redundarán sin duda en una ejecución más fluida del proyecto y una mejora sustancial en sus posibilidades de alcanzar un resultado exitoso, para bien de la organización y mejora de los índices de éxito de la industria.

El Club de Investigación Tecnológica y el autor de este informe instan a los profesionales a aplicar lo planteado, y se ponen a disposición del lector para facilitar el acceso a los materiales referenciados, en la búsqueda de una mejor comprensión de los lineamientos disciplinarios de la administración de proyectos tecnológicos y su aplicación práctica.

Referencias

[ASQ 2002] American Society for Quality. "Certified Software Quality Engineer Primer", Quality Council of Indiana, U.S.A., 2002

[Boehm 1989] Boehm, Barry W. "Tutorial: Software Risk Management", 1989, presentado en "Quality Software Project Management" , pp.596 (Futrell, R.T., Shafer, D.F., Shafer, L.I. "Quality Software Project Management", Software Quality Institute Series, Prentice Hall PTR, U.S.A., 2002)

[Boehm & Jones] Adaptado de "Software Risk Management" (Boehm 1989) y "Assessment and Control of Software Risks" (Jones, 1994). Presentado en [McConnell 1996], pp.86.

[Donaldson 2007] Donaldson, Scott E. & Siegel, Stanley G., "Enriching your project planning: Tying risk assessment to resource estimation", IEEE Computer Society in IT Pro, September-October, 2007

[Futrell 2002] Futrell, R.T., Shafer, D.F., Shafer, L.I. "Quality Software Project Management", Software Quality Institute Series, Prentice Hall PTR, U.S.A., 2002

[Kerzner 1998] Kerzner, Harold. "In Search of Excellence in Project Management, Successful Practices in High Performance Organizations", Van Nostrand Reinhold, U.S.A., 1998

[Kerzner 2001] Kerzner, Harold. "Project Management, A Systems Approach to Planning, Scheduling an Controlling", Seventh Edition, John Wiley & Sons, Inc., U.S.A., 2001

[Laudon 2004] Laudon, Kenneth & Laudon, Jane. "Sistemas de Información Gerencial". Editorial Prentice Hall, Octava Edición, México, 2004

[Lyytinen 1996] Lyytinen, Kalle; Mathiassen, Lars & Ropponen, Janne, "A Framework For Software Risk", Scandinavian Journal of Information Systems, 1996, 8(1):53–68.

[Lyytinen 1998] Lyytinen, Kalle; Keil, Mark; Cule, Paul E. & Schmidt, Roy C., "A Framework For Software Risk", Communications of the ACM, November 1998/Vol. 41, No. 11.

[Lyytinen 2000] Lyytinen, Kalle & Ropponen, Janne, "Components of Software Development Risk: How to Address Them?, A Project Manager Survey", IEEE Transactions on software engineering, vol. 26, no. 2, February 2000.

[McConnell 1996] McConnell, Steve. "Rapid Development, Taming Wild Software Schedules", Microsoft Press, U.S.A., 1996 ("Chapter 5: Risk Management", pp.81-106)

[McFarlan 1981] McFarlan, F. Warren, "Portfolio Approach to Information Systems", Harvard Business Review, September-October, 1981

[NASA 2001] The NASA Academy of Program & Project Leadership, "Foundations of Project Management, Module 8: Risk Management", National Aeronautics & Space Administration, U.S.A., 2001

[PMI 2004] Project Management Institute, "A guide to the Project Management Body of Knowledge – PMBOK", Third Edition, 2004

[SEI 1995] Software Engineering Institute, Risk Management Program, "Team Risk Management", Higuer, Ronald P. January, 1995.

[SEI 1997] Software Engineering Institute, Risk Management Program, "Risk Management in Practice", Audrey J. Dorofee, Julie A. Walker, and Ray C. Williams, Carnegie Mellon University, 1997.

[SGI 1995] The Standish Group International, Inc. "Chaos Report", 1995

[SGI 2001] The Standish Group International, Inc. "Extreme Chaos Report", 2001 update.

[SGI 2004] SoftwareMag.com, "Standish: Project Success Rates Improved Over 10 Years", 15 de Enero de 2004.

[STSC 1995] Software Technology Support Center, Ogden Air Logistics Center, Hill AFB, US Air Force, http://www.stsc.hill.af.mil/crosstalk/2000/02/risk.html

Anexo 1

Participación del equipo de trabajo en el ciclo de administración del riesgo del proyecto:

El SEI ha generado una visión del proceso basada en su propuesta de Administración del Riesgo por el Equipo de Trabajo del Proyecto, que incorpora elementos importantes, cuya descripción se presenta en la tabla A1.1., según se presenta en la referencia [SEI 1995], y que se ilustra con la siguiente gráfica:

FIGURA A1.1. Ciclo de administración del riesgo con participación del equipo de trabajo del proyecto

Los elementos presentados se describen en la siguiente tabla:

Principio	La administración efectiva del riesgo requiere
Vision compartida del producto	Ø Compartir una visión de producto basada en un propósito común, propiedad compartida y compromiso colectivo
	Ø Focalización en los resultados
Trabajo de equipo	Ø Trabajar cooperativamente para alcanzar una meta común
	Ø Unir el talento, las habilidades y el conocimiento
Perspectiva global	Ø Visualizar el desarrollo de software dentro del contexto de la definición, diseño y desarrollo de sistemas mayores
	Ø Reconocer tanto el valor potencial de la oportunidad como el impacto potencial de los efectos adversos
Perspectiva hacia adelante	Ø Pensar hacia el mañana, identificando eventos inciertos y anticipando los resultados potenciales
	Ø Administrar los recursos y las actividades del proyecto en tanto se anticipan eventos inciertos
Comunicación abierta	Ø Estimular el flujo libre de información en y entre todos los niveles del proyecto
	Ø Habilitar la comunicación formal, informal y casual
	Ø Utilización de procesos basados en el consenso que valoren la voz individual (obteniendo conocimientos y visión únicos para la identificación y manejo de riesgos)
Administracion integrada	Ø Convirtiendo la administración de riesgos en una parte integral y vital de la administración de proyectos
	Ø Adaptando los métodos y herramientas de la administración de riesgos a la infraestructura y la cultura del proyecto
Proceso continuo	Ø Manteniendo vigilancia constante
	Ø Identificando y administrando los riesgos rutinariamente a través de todas las fases del ciclo de vida del proyecto

Tabla A1.1. Principios de la administración del riesgo en el equipo de trabajo

Es de notar que la definición utilizada en este planteamiento para el equipo de trabajo del proyecto involucra a todos los participantes en la ejecución del proyecto, incluyendo no sólo los miembros del equipo, sino también la administración de la organización, usuarios e incluso subcontratistas y proveedores. En la experiencia de aplicación del enfoque se señalan las siguientes ventajas:

- Mejora en las comunicaciones
- Aprovechamiento de perspectivas múltiples
- Base de conocimiento experto más amplia
- Compromiso más difundido
- Consolidación de riesgos

Anexo 2

Tabla A2.1. Riesgos potenciales de cronogramación [McConnell 1996]

Creación del cronograma
El cronograma, los recursos, y la definición de producto han sido establecidos por el cliente o la administración superior y no están balanceados
El cronograma omite actividades y tareas necesarias
No se puede construir un producto de las dimensiones especificadas en el tiempo asignado
El producto sobrepasa el tamaño estimado (líneas de código, puntos de función, módulos, etc.)
El esfuerzo es mayor al estimado (en líneas de código, puntos de función, módulos, etc.)
La re-estimación en respuesta a atrasos en el cronograma es excesivamente optimista e ignora la experiencia histórica del proyecto
La presión excesiva del cronograma reduce la productividad
La fecha meta se adelanta sin los ajustes correspondientes al alcance del producto o los recursos disponibles
Un atraso en una tarea causa atrasos en cascada en las tareas relacionadas
El diseño e implementación de áreas no conocidas del producto toman más tiempo del esperado
Organización y administración
El proyecto carece de un patrocinador de alto nivel efectivo
El proyecto se retrasa en exceso en un "front end" difuso
Despidos y recortes reducen la capacidad del equipo
La administración o mercadeo insisten en decisiones técnicas que extienden el cronograma
Una estructura de equipo ineficiente reduce la productividad
El ciclo de revisión/decisión de la administración es más lento de lo esperado
Recortes de presupuesto desordenan los planes del proyecto
La administración toma decisiones que reducen la motivación del equipo de desarrollo
Tareas no técnicas de terceros toman más tiempo del esperado (aprobación de presupuesto, aprobación de compra de equipos, revisiones legales, autorizaciones de seguridad, etc.)
El planeamiento es muy escaso para apoyar la velocidad de desarrollo deseada
Los planes del proyecto se abandonan bajo presión, resultando en un desarrollo caótico e ineficiente
La administración pone más énfasis en "heroísmo" que en un reporte de situación exacto, lo que disminuye su habilidad para detectar y corregir problemas
Ambiente de desarrollo
Las instalaciones no están disponibles a tiempo
Las instalaciones están disponibles pero son inadecuadas (no hay teléfonos, cableado de red, muebles, suministros de oficina, etc.)
Las instalaciones están atestadas, son ruidosas o disruptivas
La herramientas de desarrollo no son instaladas para el momento deseado
La herramientas de desarrollo no funcionan según lo esperado; los desarrolladores necesitan tiempo para crear caminos alternos o cambiarse a nuevas herramientas
La herramientas de desarrollo no son escogidas con base a su mérito técnico y no brindan la productividad planeada
La curva de aprendizaje para las nuevas herramientas de desarrollo es más larga o ardua de lo esperado
Usuarios finales
El usuario final insiste en nuevos requerimientos
El usuario finalmente encuentra el producto insatisfactorio, requiriéndose rediseño y retrabajo
El usuario final no se involucra en el proyecto y consecuentemente no brinda el soporte necesario
No se solicita la información necesaria del usuario final, de manera que el producto finalmente falla en cumplir las expectativas del usuario y debe ser retrabajado
Cliente

El cliente insiste en nuevos requerimientos
El ciclo de revisión/decisión del cliente para planes, prototipos y especificaciones es más lento de lo esperado
El cliente no participará en los ciclos de revisión de planes, prototipos y especificaciones o no está capacitado para hacerlo, resultando en requerimientos inestables y cambios, con alto consumo de tiempo
El tiempo de comunicación del cliente (i.e. tiempo para responder a solicitudes de clarificación de requerimientos), es más lento de lo esperado
El cliente insiste en decisiones técnicas que atrasan el cronograma
El cliente micro-administra el proceso de desarrollo, resultando en un avance más lento de lo planeado
Componentes suministrados por el cliente comparan pobremente con el producto en desarrollo, resultando en diseño y trabajo de integración extra
Componentes suministrados por el cliente son de calidad pobre, resultando en pruebas, diseño y trabajo de integración extra, y esfuerzo extraordinario de la administración de la relación con el cliente
La herramientas de soporte y ambiente exigidas por el cliente son incompatibles, tienen un desempeño insuficiente o funcionalidad inadecuada, resultando en productividad reducida
El cliente no acepta la entrega del software como se terminó, aunque cumple todas las especificaciones
El cliente tiene expectativas de velocidad de desarrollo que los desarrolladores no pueden alcanzar
Contratistas
El contratista no entrega los componentes cuando se prometieron
El contratista entrega componentes con inaceptable baja calidad, y debe invertirse tiempo en mejorar esta calidad
El contratista no se compromete con el proyecto y consecuentemente no provee el nivel de desempeño necesitado
Requerimientos
Los requerimientos se han formalizado pero continúan cambiando
Los requerimientos están pobremente definidos, y su definición adicional extienden el alcance del proyecto
Se añaden requerimientos adicionales
Áreas de producto vagamente especificadas consumen más tiempo del esperado
Producto
Módulos propensos a error requieren más pruebas, diseño y trabajo de implementación de lo esperado
Calidad inaceptablemente baja requiere más pruebas, diseño y trabajo de implementación en correcciones de lo esperado
Expandir los límites del estado del arte en ciencias computacionales en una o más áreas extiende el cronograma impredeciblemente
El desarrollo de funciones erróneas del software requiere rediseño e implementación
El desarrollo de una interfaz de usuario errónea resulta en rediseño e implementación
El desarrollo de funciones extra del software que no son requeridas (“gold plating”), extienden el cronograma
Alcanzar las restricciones de tamaño y velocidad del producto requiere más tiempo del esperado, incluyendo tiempo para rediseño y reimplementación
Requerimientos estrictos de compatibilidad con los sistemas existentes requiere más pruebas, diseño e implementación de lo esperado
Requerimientos de interfaz con otros sistemas, otros sistemas complejos u otros sistemas fuera del control del equipo producen diseño, implementación y pruebas imprevistas
Requerimientos de operación bajo múltiples sistemas operativos toma más tiempo satisfacer de lo esperado
La operación en una plataforma de software desconocida o no probada causa problemas imprevistos
La operación en una plataforma de hardware desconocida o no probada causa problemas imprevistos
Desarrollo de un tipo de componente que es completamente nuevo para la organización toma más tiempo de lo esperado
La dependencia de una tecnología que aún está en desarrollo extiende el cronograma

Ambiente externo
El producto depende de regulación gubernamental, que cambia inesperadamente
El producto depende de estándares técnicos en borrador, los que cambian inesperadamente

Personal
La contratación toma más tiempo del esperado
Los prerrequisitos de las actividades (i.e. entrenamiento, terminación de otros proyectos, adquisición de permisos de trabajo) no se pueden completar a tiempo
Relaciones deficientes entre los desarrolladores y la administración atrasan la toma de decisiones y el seguimiento
Los miembros del equipo no se comprometen con el proyecto y consecuentemente no proveen el nivel de desempeño necesario
Baja motivación y moral reducen la productividad
La falta de especialización necesaria aumenta los defectos y el retrabajo
El personal necesita tiempo adicional para aprender sobre herramientas de software o ambiente desconocidas
El personal necesita tiempo adicional para aprender sobre ambiente de hardware desconocido
El personal necesita tiempo adicional para aprender sobre lenguaje de programación desconocido
Personal bajo contrato se marcha antes de que el proyecto esté completo
Personal permanente se marcha antes de que el proyecto esté completo
Nuevo personal de desarrollo se añade tarde en el proyecto, y el "overhead" adicional de entrenamiento y comunicaciones reduce la efectividad de los miembros existentes del equipo
Los miembros del equipo no trabajan juntos eficientemente
Conflictos entre miembros del equipo producen comunicaciones pobres, diseños pobres, errores de interfaces y retrabajo extra
Miembros problemáticos no se sacan del equipo, dañando la motivación general
El personal más calificado para trabajar en el proyecto no está disponible
El personal más calificado para trabajar en el proyecto está disponible pero no se asigna por razones políticas u otras
No se encuentra personal con habilidades críticas necesarias para el proyecto
Personal clave está disponible sólo parcialmente
No hay suficiente personal disponible para el proyecto
Las asignaciones de la gente no corresponde a sus fortalezas
El personal trabaja más lentamente de lo esperado
El sabotaje en la administración del proyecto resulta en cronogramación y planeamiento ineficientes
El sabotaje por personal técnico resulta en trabajo perdido o baja calidad, y requiere retrabajo

Diseño e implementación
Diseño sobresimplificado falla en señalar asuntos importantes y produce rediseño y reimplementación
Diseño sobrecomplicado requiere esfuerzo innecesario e improductivo en implementación
Diseño pobre lleva a rediseño y reimplementación
Uso de metodología desconocida resulta en tiempo de entrenamiento extra y en retrabajo para corregir malos usos primerizos de la metodología
El producto se implementa en un lenguaje de bajo nivel (i.e. assembler), y la productividad es menor a lo esperado
La funcionalidad necesaria no se puede implementar utilizando las bibliotecas seleccionadas de código o clases; los desarrolladores deben cambiar a nuevas bibliotecas o construir a la medida la funcionalidad necesaria
Las bibliotecas de código o clases son de baja calidad, provocando pruebas adicionales, corrección de defectos y retrabajo
Las reducciones esperadas en el cronograma por herramientas de mejora de la productividad están sobreestimadas
Componentes desarrollados separadamente no se pueden integrar fácilmente, requiriendo rediseño y retrabajo

Proceso
La cantidad de papeleo produce avance más lento de lo esperado
El seguimiento inexacto del avance resulta en desconocimiento que el proyecto está atrasado hasta tarde en el proyecto
Actividades iniciales de aseguramiento de calidad se subejecutan, resultando en retrabajo extenso al final
El seguimiento inexacto de los resultados de calidad resulta en desconocimiento de problemas de calidad que afectan el cronograma hasta tarde en el proyecto
Poca formalidad (falta de apego a las políticas y estándares del software) resulta en comunicaciones equivocadas, problemas de calidad y retrabajo
Demasiada formalidad (apego burocrático a las políticas y estándares del software) resulta en "overhead" excesivo
El reporte del avance a la administración toma más tiempo de los desarrolladores de lo esperado
Una administración a medias del riesgo falla en detectar los principales riesgos del software
La administración del riesgo del proyecto de software toma más tiempo del esperado