

Universidad de las Ciencias Informáticas



Título:

**Proceso de Gestión de riesgos para
proyectos de desarrollo de software de Softel.**

**Tesis para optar por el Título Académico de Master en
Gestión de Proyectos Informáticos**

Autor: Ana Silvia Valladares Arenas

Tutor: DrC. Rolando Alfredo Hernández León

Ciudad de la Habana

29 de Junio de 2010

“Si conoces al enemigo y te conoces a ti mismo, no tendrás que temer el resultado de cien batallas”

Sun Tzu, general chino que vivió hace 2.500 años

Para el Jefe de proyectos de software, el enemigo es el riesgo.

Roger S. Pressman

“Identificando y tratando con los riesgos desde el inicio del desarrollo disminuye los costos en términos de tiempo y ayuda a prevenir los desastres del software.”

Boehm

Agradecimientos.

A mi familia por el apoyo permanente que le dan a mi desarrollo profesional, fundamentalmente a mi esposo e hijos. A mi mamá por toda la ayuda brindada sobre todo en los momentos en que más necesitaba concentrarme en mi investigación. A Elena por ayudarme también en muchos momentos.

Agradezco a todos mis compañeros de trabajo, los cuales asumen con entusiasmo y dedicación los retos que nos hemos puesto para lograr la mejora continua de los procesos de gestión que lleva a cabo Softel.

Al Profesor Rolando por haber sembrado en mi un nuevo afán por el mundo de la investigación científica.

A todos los que me rodean y contribuyen a luchar por ser mejor cada día.

Resumen.

En el presente trabajo, a partir de identificar que el proceso que se realiza actualmente en Softel para la gestión de los riesgos en los proyectos de software que se ejecutan no se corresponde con las necesidades reales de la empresa, se traza como objetivo definir dicho proceso. Para ello se hace un estudio del proceso de gestión de riesgos para la ejecución de proyectos de desarrollo de software en diferentes entidades de Ciudad Habana para detectar las principales dificultades que se están enfrentando, su incidencia en la gestión de proyectos y obtener la información suficiente que permita definir un proceso que se ajuste más a las necesidades reales de Softel. Se sigue el procedimiento establecido en la bibliografía consultada para elaborar el cuestionario que se utiliza y seleccionar una muestra representativa de los especialistas vinculados a la gestión de riesgos en proyectos de software y, a partir de la información obtenida, se define un proceso para realizar la gestión de riesgos con mayores posibilidades de éxito. El proceso definido se aplica actualmente en la empresa Softel, donde se ha podido evaluar utilizando un método de experto. Después de terminada la investigación y evaluado el proceso de gestión de riesgos se ha llegado a la conclusión que en la actualidad no existe ningún proceso para gestión de riesgos en proyectos de software que se ajuste a las necesidades de Softel. De las entidades estudiadas, sólo la UCI tiene establecido un proceso para la gestión de riesgos y el resultado obtenido confirma que el proceso definido se corresponde con las necesidades de Softel, por lo que se propone continuar con su aplicación en esta empresa y proponer su generalización al resto de las entidades que tengan condiciones semejantes.

Palabras claves: Riesgos, Gestión de Riesgos, Plan de Mitigación, Plan de Contingencia, Análisis de riesgos, Evaluación de probabilidad e impacto.

ÍNDICE.

Introducción.	7
Capítulo I. Fundamentos teóricos de la gestión de riesgos.....	14
Introducción.....	14
1.1 Riesgo.....	14
1.2 Gestión de Riesgos.....	15
1.3 Estrategias de riesgo reactivas y proactivas.....	17
1.4 Algunos antecedentes sobre los riesgos del software y su gestión.....	17
1.5 Los riesgos en el contexto empresarial.....	20
1.6 Necesidad de gestionar los riesgos.....	23
1.7 Marcos para la gestión de riesgos.....	24
1.7.1 Generaciones.....	24
1.7.2 McFarlan.....	25
1.7.3 Boehm.....	26
1.7.4 Gestión de riesgos de proyectos de PMI.....	26
1.7.5 Programa de gestión de riesgos del SEI.....	27
1.7.6 Modelo de Hall.....	28
1.7.7 Modelo SERIM de Karolak (IEEE).....	29
1.7.8 Modelo de Barki.....	29
1.7.9 Pressman.....	29
1.7.10 IEEE Computer Society.....	30
1.7.11 Richard Fairley (IEEE).....	31
1.7.12 <i>Microsoft Solutions Frameworks (MSF)</i>	31
1.7.13 MAGERIT.....	31
1.7.14 Dirección Nacional de Aduanas de Chile.....	32
1.7.15 Modelo Gestión Riesgos en Proyectos de Desarrollo de Software (MoGeRi).....	33
1.7.16 La Evaluación de Riesgos del Sistema de Control Interno.....	34
1.7.17 Modelos de Calidad.....	35
1.8 Algunas herramientas y técnicas.....	37
1.8.1 Para la identificación de riesgos.....	37
1.8.2 Para el control de las organizaciones: Matriz de Control Interno.....	39
1.9 Experiencia de la Universitat Politècnica de Catalunya (UPC). Proyecto PRISMA.....	39
1.10 Estudios sobre la gestión de riesgos en Cuba.....	40

Conclusiones parciales.....	41
Capítulo II. Diagnóstico del estado actual.....	42
Introducción.....	42
2.1 Métodos Científicos de Investigación.	42
2.2 Estado actual de la gestión de riesgos en entidades cubanas.....	45
2.2.1 Encuestas.....	45
2.3 Estado actual de la gestión de riesgos en los proyectos de desarrollo de software de Softel.....	49
2.3.1 Caracterización de la Factoría de Software de Softel.	51
2.3.2 Entrevistas.....	53
Conclusiones parciales.....	59
Capítulo III. Definición del Proceso para la gestión de riesgos y evaluación del proceso.	61
Introducción.....	61
3.1 Proceso de gestión de riesgos para los proyectos de desarrollo de software de Softel. ...	61
3.1.1. Elementos tenidos en cuenta para la obtención del proceso.	61
3.1.2. Proceso de Gestión de Riesgos.	66
3.2 Preparación para la introducción del proceso propuesto.	79
3.3 Análisis de los resultados de la evaluación del proceso de gestión de riesgos definido...	81
3.4 Otros resultados alcanzados.	85
Conclusiones parciales.....	86
Conclusiones.	87
Recomendaciones.	88
Referencia Bibliográfica.	89
Glosario de Términos y Acrónimos.....	94
Anexos.....	99
Anexo 1. Encuesta sobre gestión de riesgos.....	99
Anexo 2. Componentes claves de la Entrevista Apreciativa.	101
Anexo 3. Entrevista Apreciativa.....	102
Anexo 4. Plantilla del Plan de Gestión de Riesgos (DG-32.01).	104
Anexo 5. Plantilla del Registro de Riesgos (DG-32.02).	109
Anexo 6. Cuestionario para asignación de peso a los criterios.....	113
Anexo 7. Cuestionario para la evaluación cuantitativa y cualitativa del proceso definido.....	114

Introducción.

La gran mayoría de las empresas pequeñas son muy optimistas al planear sus proyectos. En estas empresas es común suponer que las actividades se realizarán conforme al plan y sin imprevistos. Las empresas pequeñas que intentan llevar a cabo actividades de gestión de riesgos, identifican sólo algunos riesgos altamente visibles al principio del proyecto. Es poco frecuente que estas empresas monitoreen los riesgos identificados o busquen encontrar nuevos riesgos durante la ejecución o finalización del proyecto. El proceso de gestión de riesgos es un proceso iterativo y como tal debe seguirse para lograr los resultados esperados, refinando dichos resultados en cada iteración (Pérez, 2007). A pesar de ser un proceso que se puede explicar relativamente fácil a los ingenieros y profesionales del software, con sólo estudiar la teoría descrita en la literatura, existen grandes imperfecciones en su gestión y los ingenieros de software sienten temor a este vocablo y a la ardua tarea de gestión permanente que el mismo conlleva, donde la constancia y la disciplina son factores decisivos.

Aunque se reconocen avances en el estudio de la gestión de riesgos, es importante destacar que ningún proyecto es exactamente igual a otro y ninguna institución es exactamente igual a otra, así que los resultados, herramientas y experiencias de algunos no pueden convertirse, necesariamente, en recetas para otros. La gestión de riesgos es un proceso inherente a cada proyecto e institución, aunque si se desarrolla en la empresa la capacidad de aprender de otros y adaptar rápidamente a la realidad del proyecto de la empresa, se estará acortando el camino para alcanzar el éxito.

En Cuba existen características propias que generan riesgos a los proyectos, aunque algunas de ellas pueden estar presentes en muchos países de América Latina y en otros subdesarrollados. Cuba ha tenido que hacer ingentes esfuerzos para lograr los escasos, aunque en ascenso, niveles de informatización del país, debido a los pocos recursos materiales y tecnológicos que posee y lo difícil que se hace, muchas veces, el acceso a las tecnologías de la información y las comunicaciones, vitales para desarrollar la industria del software y preparar a las instituciones estatales para recibir la informatización. Se lucha constantemente por evitar la dependencia tecnológica que genera la transferencia de tecnología proveniente del exterior, de la cual Cuba es consumidora por necesidad. El bloqueo económico es un factor que impone la necesidad permanente de buscar soluciones propias sostenibles con los recursos con los que cuenta el país. Esta situación trae necesariamente riesgos a los proyectos, los cuales exigen una concepción integral: recursos humanos y materiales para el desarrollo, implantación y

soporte del software, preparación de las instituciones para recibir la informatización, establecimiento de las comunicaciones necesarias para la transferencia bidireccional de información entre las instituciones y sus niveles de dirección a nivel de municipio, provincia y país.

En el año 2003 el Ministerio de Salud Pública (MINSAP), como organismo rector del Sistema Nacional de Salud (SNS), define como una prioridad su informatización, para esto, en conjunto con la alta dirección del país, ha trazado políticas y estrategias para lograr incorporar de forma ambiciosa las Tecnologías de la Informática y las Comunicaciones (TIC) en la salud cubana, todo esto persiguiendo un único objetivo, la búsqueda de nuevas formas que brinden una atención con mejor calidad al pueblo, incrementando la eficiencia y calidad en los servicios. El proceso de informatización es dirigido por el MINSAP y el Ministerio de la Informática y las Comunicaciones (MIC), jugando un papel fundamental la empresa Softel.

Entre los objetivos del MIC se encuentra la producción de soluciones informáticas para lograr la informatización de la sociedad, garantizando la invulnerabilidad y la independencia tecnológica. Softel es una empresa del MIC a la cual le ha correspondido el cumplimiento de dicho objetivo en el campo de la salud, para lo cual se ha propuesto, entre otros, implementar un sistema de excelencia para el desarrollo y mantenimiento de productos de software especializados de salud (Softel, 2009), a partir de las prioridades establecidas por el MINSAP. Para el logro de este objetivo tiene, en su estructura, a la Dirección de Desarrollo de Software, siendo la Factoría de Software uno de los Grupos de Trabajo diseñados para ello (Softel, 2009).

Softel, además, trabaja en la elaboración del Expediente de Perfeccionamiento Empresarial y en la implantación, cada vez más profunda, de la Resolución 297/03 del Ministerio de Finanzas y Precios (MFP). Como parte de este proceso, trabaja en la definición y perfeccionamiento de los procedimientos de trabajo y procesos de cada una de sus Direcciones y aspira a la Certificación ISO 9000 de sus áreas. Además de ello, ha estudiado el modelo de calidad CMMI, como un patrón, ya que el mismo constituye un marco de referencia de la capacidad de las organizaciones de desarrollo de software en el desempeño de sus diferentes procesos, proporcionando una base para la evaluación de la madurez de las mismas y una guía para implementar una estrategia para su mejora continua.

Softel, con el objetivo de hacer eficiente y mejorar la calidad de sus productos y la prestación de servicios realizó, en el año 2008, un diagnóstico a diferentes procesos y áreas de la empresa. Ello incluyó la Factoría de Software. Como resultado, se obtuvo el mapa de algunos de los

principales procesos de las áreas de la empresa, se realizó la descripción y la determinación de algunos de los problemas que afectan dichos procesos y las áreas donde los mismos intervienen (Martínez C.D, 2008). Los mismos se han tomado como base para lograr la mejora de algunos procesos y sobre ellos se han basado algunas de las Tesis de Maestría presentadas por Especialistas de la empresa en el año 2009. Es importante destacar que algunos de los problemas identificados en este estudio todavía se mantienen debido a la carencia de un proceso de gestión de riesgos. Otros han sido resueltos parcial o totalmente por acciones concretas que se han venido realizando pero sin un proceso formal y ordenado de gestión de riesgos.

En el curso escolar 2006-2007, se realizaron en la Universidad de las Ciencias Informáticas (UCI) cinco Trabajos de Diploma relacionados con el tema de la gestión de riesgos. Dos de ellos contaron con tutores de Softel, debido a la importancia que la empresa está dando a este proceso. En particular, el trabajo de Figueredo define la propuesta de la metodología PMI (*Project Management Institute*) para el desarrollo del proceso de gestión de riesgos para el proyecto Atención Primaria de Salud (APS) (Figueredo, 2007). También se realizaron otras tesis donde fueron entrevistados especialistas de la empresa debido a la experiencia acumulada en la gestión y desarrollo de proyectos de software. Zulueta, en su Tesis de Maestría, hace una valoración acerca de los cinco Trabajos de Diploma mencionados. Plantea que aunque se han dado algunos pasos en el estudio y aplicación de la gestión de riesgos al calor del desarrollo de los Trabajos de Diplomas mencionados, en las entrevistas y encuestas realizadas durante la investigación a los involucrados con Proyectos de Software (gestores, ingenieros de software, clientes, estudiantes, profesores), se reconoce la carencia de conocimientos sobre los marcos para la gestión de riesgos y por tanto de su aplicación. De cierta forma, se conocen informalmente los riesgos que podrían afectar el trabajo, pero estos no son registrados y mucho menos se procede a su análisis o gestión. No obstante, debe reconocerse que la asignación de los temas de riesgos para los trabajos de diploma ha constituido un factor impulsor de los estudios y aplicación de la gestión de riesgos en la Universidad de las Ciencias Informáticas (UCI) (Zulueta, 2007a).

Del Castillo (2009) y Bernaza (2009), ambas de Softel, en sus Tesis de Maestría incluyen la gestión de riesgos de dos proyectos que constituyen soluciones informáticas destinadas a la informatización de los Bancos de Sangre y Policlínicos del país. Las mismas dan la medida de la toma de conciencia que va teniendo este tema en los proyectos que se llevan a cabo en la empresa (Bernaza, 2009; del Castillo, 2009). Además, tres de las cinco Tesis de Maestría de

Softel del 2009, siguieron las prácticas de PMBoK (*Project Management Body of Knowledge*). Del Castillo (2009) siguió las buenas prácticas de PMBoK para los procesos de Gestión de la Integración enmarcados dentro de cada uno de los Grupos de Procesos de la Dirección de Proyectos y de las Fases del Ciclo de Vida propuesto para el mismo (Concepción, Elaboración, Ejecución, y Cierre), lo cual permitió definir la Solución propuesta a partir de los resultados obtenidos del diagnóstico de la situación actual de los Bancos de Sangre para la evaluación de las necesidades del proyecto e implantar la misma (del Castillo, 2009). Bernaza (2009), para el proceso de Gestión de la Integración de la Solución Informática para los Policlínicos, que es un área de conocimiento de PMBoK para la dirección del proyecto, adaptó la implementación de sus siete procesos, enmarcados dentro de cada una de las fases del ciclo de vida de ese proyecto, lográndose su culminación exitosa (Bernaza, 2009). Cabrera (2009) decidió utilizar la propuesta del PMI con la Guía del PMBoK como un modelo formal, consistente y ajustable, que da la posibilidad de trabajar con equipos grandes y geográficamente dispersos, que requieren de una comunicación formal; características propias del proyecto de investigación, profundizando en la Gestión de la Integración del Proyecto, para cumplir los objetivos y lograr proyectos disciplinados y exitosos (Cabrera, 2009).

Cué (2009) en su Tesis de Maestría realiza una investigación sobre el proceso de mejora, llegándose a definir un modelo para organizar la mejora continua en la empresa, en el cual se integran estándares y normas internacionales de la familia ISO y el modelo CMMI, así como los métodos IDEAL y Seis Sigma. En la plantilla propuesta para el Plan de Mejora se incluyen los Riesgos del proyecto con el objetivo de identificar los riesgos que pudieran impedir la ejecución del proyecto de mejora, establecer cómo mitigarlos o un plan de contingencia (Cué, 2009). Esto resalta la importancia de tener definido en la empresa un proceso de gestión de riesgos que se adecue a las características propias de la empresa y que puede seguir su evolución aplicando este modelo de mejora propuesto.

A pesar de que la empresa Softel ha comenzado a dar pasos en la mejora de la gestión de los riesgos este tema no se ha colocado conscientemente como parte de la gestión de los proyectos de desarrollo de software, aunque de forma empírica se han mitigado y hasta eliminado muchos de ellos. Una de las causas fundamentales es la falta de preparación de los especialistas en este tema, que no es muy difícil de lograr desde el punto de vista teórico, pero su desconocimiento hace que no se manifieste conscientemente en la práctica. La falta de definición de un proceso de gestión de riesgos en la empresa o la aplicación de alguno existente ha impedido que se hayan realizado las actividades de identificación, análisis,

planificación de respuestas y seguimiento y control de los riesgos a los proyectos. A lo sumo se han identificado algunos riesgos que han sido resueltos, mitigados o que se mantienen iguales o peores por la falta de planes que contribuyan a su control.

Actualmente Softel, en su Factoría de Software, cuenta con un numeroso grupo de productos que se encuentran en fase de mantenimiento. Una parte de ellos son sistemas heredados, los cuales llevan años funcionando establemente en hospitales, bancos de sangre y policlínicos cubanos con un negocio sólido, ya que durante el tiempo que llevan en explotación han seguido evolucionando a partir de la interacción directa y permanente con los clientes. La otra parte fueron desarrollados utilizando arquitectura SOA (arquitectura orientada a servicios) y basados en componentes, usando software libre. Tienen algunos años desde el inicio de su desarrollo y el equipo de proyecto original ya no existe. También las herramientas de desarrollo (libres) empleadas en aquel momento han seguido evolucionando, sin garantizar la compatibilidad total con sus versiones anteriores. Además, de los productos que se encuentran en fase de mantenimiento, existe un gran número de productos que se encuentran en fase de desarrollo; algunos en su primera versión y otros como nueva versión de los sistemas heredados. En su mayoría, son para arquitectura SOA (orientados a servicios) y basados en componentes, lo cual introduce complejidades importantes a estos nuevos desarrollos. Se emplean, además, herramientas inteligentes para la generación de código como GeneXus y Java como lenguaje de programación para complementar estos desarrollos, además de otros que se encuentran libres en el mercado. Se utilizan también herramientas de software libre para la generación de reportes y sincronización de aplicaciones, entre otras.

Para el desarrollo y mantenimiento de los productos de software y lograr el cumplimiento de las prioridades establecidas por el MINSAP, Softel necesita gestionar adecuadamente sus proyectos con la seriedad y constancia requeridas. Esto incluye la gestión de los equipos de proyecto que intervienen, del cronograma de tareas del proyecto, de la tecnología que se emplea para el desarrollo y mantenimiento de las aplicaciones, del entorno de desarrollo que garantiza el ambiente de integración y despliegue y del dominio del negocio a informatizar, entre otros. En la Factoría de Software, todavía la gestión de proyectos no se realiza con el rigor necesario, debido a que sus equipos de proyecto han sido recientemente reestructurados con personal muy bien preparado técnicamente, pero con poca experiencia profesional, en sistemas integrados, empleo de arquitectura SOA, conocimiento de GeneXus y en el negocio que se está informatizando. Aunque se han ido mejorando los resultados que se esperan, los Jefes de Proyecto tienen que invertir mucho tiempo en el análisis y diseño de sistemas, en la integración

y pruebas de las aplicaciones y en la formación de los nuevos integrantes. Ello tiene un alto impacto en el incumplimiento de los cronogramas de trabajo. También hay falta de datos históricos, por la poca trazabilidad de las tareas y documentación que se registra, que permita la adopción de métricas necesarias para planificarlas. Además, como los equipos de proyecto están en proceso de consolidación, la productividad todavía no se encuentra en los niveles deseados, aunque se ha elevado en el transcurso del tiempo.

Aunque la Factoría de Software se encuentra en un proceso de maduración y consolidación en ascenso permanente, existen características y necesidades propias que hacen que la empresa necesite definir e implantar un grupo de procesos y herramientas que contribuyan al cumplimiento de su misión. Entre los procesos a definir, la gestión de riesgos, puede contribuir al fortalecimiento de la gestión de proyectos y, como consecuencia, al cumplimiento de los objetivos que se han ido trazando para cada uno de ellos.

Por todo lo anterior, se define el siguiente **problema**: El proceso que se realiza actualmente en Softel para la gestión de los riesgos en los proyectos de software que se ejecutan no se corresponde con las necesidades reales de la empresa.

Con vistas a la solución del problema planteado, se define el proceso de gestión de proyectos como el **objeto de estudio** de la investigación.

El **objetivo** de esta investigación es definir un proceso para la gestión de los riesgos en los proyectos de software que se ejecutan que se corresponda con las necesidades reales de Softel, siendo el **campo de acción** la gestión de riesgos en los proyectos de Softel.

La **hipótesis** de la investigación es: si se evalúan las condiciones actuales de la gestión de riesgos en los proyectos que se ejecutan en Softel se podrá definir un proceso para su gestión que se corresponda con las necesidades reales de la empresa.

Para lograr el objetivo y contrastar la hipótesis se propusieron los siguientes **Objetivos Específicos**:

1. Elaborar el marco teórico de la investigación.
2. Diagnosticar el estado actual de la gestión de riesgos en los proyectos de desarrollo de software de Softel.
3. Definir el proceso de gestión de riesgos para los proyectos de desarrollo de software de Softel.

4. Evaluar el proceso definido de gestión de riesgos para los proyectos de desarrollo de software de Softel utilizando criterios de expertos.

Con el resultado alcanzado la empresa contará con un proceso que podrá ser aplicado a los proyectos de software que desarrolla para mejorar la gestión de riesgos, lo cual traerá como consecuencia que sean desarrollados proyectos encaminados a resolver las problemáticas concretas del cliente en la situación actual de Cuba, contribuyendo a una mejor informatización del sector de la salud. En el futuro, con la aplicación y mejora continua de este proceso se acumularán experiencias que permitirán seguir mejorando el mismo y contribuirán a mejorar este proceso también en otras empresas e instituciones que desarrollan software, trayendo beneficios a otros sectores, además de la salud.

Estructura y contenido de la tesis.

En el *Capítulo I: Fundamentos teóricos de la gestión de riesgos*, se establece el fundamento teórico de la investigación a partir de hacer un análisis crítico de la bibliografía existente, lo que permite sustentar teóricamente la investigación.

En el *Capítulo II: Diagnóstico del estado actual*, se exponen los métodos científicos utilizados en la investigación. Se realiza el diagnóstico del estado actual de la gestión de riesgos en entidades cubanas, fundamentalmente en Softel y de la gestión de riesgos en los proyectos de desarrollo de software de la empresa. Se hace un análisis de los resultados obtenidos en cada caso, empleando la Taxonomía Ajustada (Maniasi, 2005) para agrupar los riesgos en categorías y conocer cuáles son los que más inciden, y se demuestra que no existe un proceso formal ni se realiza adecuadamente la gestión de riesgos en los proyectos de desarrollo de software de la empresa.

En el *Capítulo III: Definición del Proceso para la gestión de riesgos y evaluación del proceso propuesto*, se define el proceso para la Gestión de Riesgos de los proyectos de desarrollo de software de Softel, para lo cual se determina los elementos tomados de los marcos de gestión de riesgos analizados en el Capítulo I. Además, se exponen las actividades de preparación realizadas en la empresa para elevar la cultura sobre riesgos y su gestión y preparar a la organización en el proceso definido. Se realiza la evaluación teórica del mismo utilizando criterios de expertos con el objetivo de determinar si el proceso garantiza una adecuada gestión de los proyectos de software de Softel, entre otras contribuciones. Al final del capítulo se resumen algunos resultados que se han obtenido en los proyectos de la Factoría de Software de Softel.

Capítulo I. Fundamentos teóricos de la gestión de riesgos.

Introducción.

En este capítulo se establece el fundamento teórico de la investigación a partir de hacer un análisis crítico de la bibliografía existente, lo que permite sustentar teóricamente la investigación. Se formalizan los conceptos de riesgo y su gestión ofrecidos por varios autores, se narran algunos de sus antecedentes, se analizan los riesgos en el contexto empresarial y la importancia de gestionar los mismos. Se evalúan, además, diferentes marcos para la gestión de riesgos, así como herramientas, técnicas, experiencias alcanzadas y estudios sobre la gestión de riesgos en Cuba.

1.1 Riesgo.

Robert Charette (1989) expone la siguiente definición de riesgo: “En primer lugar, el riesgo concierne a lo que ocurra en el futuro. El hoy y el ayer no nos conciernen realmente, porque ahora ya estamos recogiendo los frutos de lo que sembramos en el pasado. La cuestión es si podemos, entonces, modificando nuestras acciones en este momento, crear una oportunidad para una situación diferente y más esperanzadora de nuestro mañana. Esto significa, en segundo lugar, que el riesgo implica un cambio, que puede venir dado por cambio de opiniones, acciones o lugares. En tercer lugar, el riesgo implica una elección, y la falta de certeza de que la elección sea correcta. Así, paradójicamente, el riesgo como la muerte o los impuestos, es una de las pocas cosas inevitables de la vida” (Charette, 1989).

El SEI (*Software Engineering Institute*) expresa la definición de riesgo como la posibilidad de sufrir una pérdida, como una medida de la posibilidad de que una amenaza conlleve a una pérdida con un impacto asociado (Audrey, 2009).

MSF (*Microsoft Solution Frameworks*) plantea que suele ser común el confundir preocupaciones, riesgos y problemas: una preocupación es cualquier situación sobre la cual existen dudas al respecto en algún determinado contexto y que, por lo tanto, será evaluada como un posible riesgo, un problema es un riesgo que, efectivamente, se ha producido (Figura 1.1) (Microsoft, 2002).



Figura 1.1. Preocupaciones, Riesgos y Problemas.

Según Rosenberg (1999), un riesgo se describe mediante una expresión en lenguaje natural que expresa la relación entre una situación real de proyecto y otra situación no realizada. La primera parte de la definición se denomina condición y representa una situación existente en el proyecto que el equipo prevé que puede resultar en una pérdida o en una reducción de beneficios; mientras que la segunda parte de la declaración se denomina consecuencia y describe la situación no deseable para el proyecto que puede derivarse de la ocurrencia de la condición. Las dos oraciones deben unirse a través de algún indicador de relación que de idea de incertidumbre y que, a su vez, implique una relación de tipo causal, tales como “por lo tanto” o “como consecuencia” (Figura 1.2) (Rosenberg, 1999).

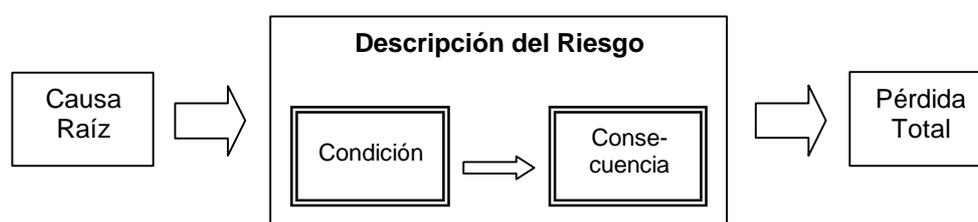


Figura 1.2. Descripción de Riesgos.

Una frase para describir un riesgo debe ser lo suficientemente completa y directa como para posibilitar el análisis de su causa raíz, discutir su impacto y desarrollar un conjunto de respuestas o acciones para prevenirlo o reducir sus consecuencias. En las frases empleadas se debe evitar el uso de abreviaciones o acrónimos que resulten difíciles de comprender y las generalizaciones y detalles irrelevantes. En algunos casos, puede ser útil agregar información de contexto a un riesgo para facilitar su entendimiento a personas que puedan no conocer todos los detalles del proyecto (ya sea en la actualidad como en el futuro) (Rosenberg, 1999).

1.2 Gestión de Riesgos.

Un efectivo proceso de gestión de riesgos es un importante componente en todo proyecto de desarrollo de software exitoso. La gestión de riesgos permite definir en forma estructurada, operacional y organizacional, una serie de actividades para gestionar los riesgos de los proyectos a lo largo de todas las fases de su ciclo de vida de desarrollo de software. Esto se traduce en la creación de planes tendientes a impedir que los riesgos se transformen en problemas o a minimizar su probabilidad de ocurrencia o impacto (Maniasi, 2005).

Para MSF (*Microsoft Solution Frameworks*), la gestión de riesgos es el proceso para identificar, analizar y dirigir los riesgos del proyecto proactivamente. El objetivo de la gestión de riesgos es maximizar los impactos positivos (oportunidades) mientras se minimizan los impactos negativos

(pérdidas) asociados con los riesgos del proyecto. Microsoft expone los principios básicos sobre los cuales se debería basar un proceso de gestión de riesgos, incluyendo la necesidad de potenciar la comunicación, aprender de todas las experiencias, ser proactivos y valorar continuamente los riesgos, entre otros (Microsoft, 2002).

Aún cuando la gestión de riesgos es fundamental para proyectos de cualquier tipo, para los proyectos de desarrollo de software, la gestión de riesgos constituye una actividad fundamental debido a que dichos emprendimientos se ven caracterizados por aspectos particulares que incrementan la presión sobre el proyecto a medida que dificultan la toma de decisiones, entre ellos: constantes presiones internas y externas; cambios normativos y evolución de las técnicas que pueden derivar en una alteración de los planes y de las estrategias; continuos y comunes cambios en los requerimientos de los usuarios; nuevas herramientas y tecnologías existentes en el mercado; periódicas amenazas de seguridad; variabilidad de los equipos de proyecto (Maniasi, 2005).

El SEI define la gestión de riesgos como el proceso formal en el que los factores de riesgos son sistemáticamente identificados, evaluados y mitigados; se inicia en la primera etapa de un proyecto de software (durante la exploración de conceptos) y se desarrolla a lo largo de todo su ciclo de vida (hasta la aceptación del producto del proyecto) (Higuera, 1996).

Rosenberg plantea que la gestión de riesgos es importante debido a que ayuda a evitar desastres, re-trabajo y sobre-trabajo, pero aún más importante, porque estimula la generación de situaciones del tipo ganar-ganar. Una correcta gestión de riesgos posibilita el aprovechamiento óptimo de recursos, el aumento de ganancias y la disminución de pérdidas. La ausencia de una apropiada gestión de riesgos conlleva a la imposibilidad de lograr el control efectivo de un proyecto, afectando su adecuada gestión. Por ello, la gestión de riesgos debe ser enfatizada y considerada como una actividad clave en todo tipo de proyectos y, particularmente, en proyectos de desarrollo de software (Rosenberg, 1999).

La Dirección Nacional de Aduanas de Chile, de forma muy similar a otras organizaciones e instituciones, ha definido su proceso de gestión de riesgos como el proceso de toma de decisiones en un ambiente de incertidumbre sobre un acción que va a suceder y sobre las consecuencias que existirán si esta acción ocurre (Dirección Nacional de Aduanas, 2007).

La Gestión de Riesgos es la práctica compuesta de procesos, métodos y herramientas que posibilita la gestión de los riesgos en un proyecto y que provee de un entorno disciplinado para

la toma de decisiones preactiva en base a determinar constantemente qué puede ir mal, identificar los riesgos más importantes en los cuales enfocarse e implementar estrategias para gestionarlos; se inicia en la primera etapa de un proyecto y se desarrolla a lo largo de su ciclo de vida. La Identificación de Riesgos en proyectos de software consiste en la determinación de elementos de riesgos potenciales mediante la utilización de algún método consistente y estructurado (Maniasi, 2005).

La Gestión de Riesgos en base a Taxonomías implica el utilizar una estructura agrupadora de los mismos de acuerdo a sus diferentes clases como una lista de consulta durante la actividad de Identificación de los Riesgos (Maniasi, 2005).

1.3 Estrategias de riesgo reactivas y proactivas.

Según Pressman (2005), en el mejor de los casos, la estrategia reactiva supervisa el proyecto en previsión de posibles riesgos. Los recursos se ponen aparte, en caso de que pudieran convertirse en problemas reales. Lo más frecuente es que el equipo de software no haga nada respecto a los riesgos hasta que algo va mal. Después el equipo vuela para corregir el problema rápidamente. Este es el método denominado a menudo "de bomberos". Cuando falla, "la gestión de crisis" entra en acción y el proyecto se encuentra en peligro real. Es por ello que una estrategia considerablemente más inteligente para el control del riesgo es ser proactivo. Empieza mucho antes de que comiencen los trabajos técnicos. Se identifican los riesgos potenciales, se valoran su probabilidad e impacto y se establece una prioridad según su importancia. Después el equipo de software establece un plan para controlar el riesgo. El primer objetivo es evitar el riesgo, poco común es que se pueden evitar todos los riesgos. El equipo trabaja para desarrollar un plan de contingencia que le permita responder de una manera eficaz y controlada (Pressman, 2005; Universidad de Murcia, 2006).

1.4 Algunos antecedentes sobre los riesgos del software y su gestión.

Boehm (1991) plantea que como en muchos campos en sus etapas tempranas, el campo del software ha tenido su porción de desastres en proyectos. La frecuencia de los desastres del software es una preocupación seria: un estudio de seiscientas empresas indicó que 35% de ellas tenían, al menos, un proyecto de software clandestino. Muchos de los desastres de los proyectos de software después de muertos, han indicado que sus problemas se habrían evitado o reducido fuertemente, si hubiese existido una temprana preocupación explícita relacionada con la identificación y solución de sus elementos de alto riesgo. Frecuentemente, estos proyectos fueron barridos a lo largo de la marea de entusiasmo optimista durante sus fases

tempranas por omitir problemas de alto riesgo que demostraron ser después su fracaso (Boehm, 1991).

Un modelo que surgió muy fuertemente fue que los gestores de proyecto exitosos eran buenos gestores de riesgo. Aunque generalmente no se usaron los términos de “identificación de riesgo”, “evaluación de riesgo”, “plan para gestionar el riesgo” o “monitoreo del riesgo”, se utilizó un concepto general de exposición al riesgo (pérdida potencial por la probabilidad de pérdida) para guiar sus prioridades y acciones. Esto provocó que los proyectos tendieran a evitar trampas y produjeran buenos productos (Boehm, 1991).

En la tesis desarrollada por *Matsuo* (1999), sobre la evaluación de riesgos en el desarrollo de software incremental, plantea que con el crecimiento de la tecnología en proporciones exponenciales y la explosión de aplicaciones de software con funcionalidades complejas, el proceso de desarrollo de software se ha vuelto sumamente complicado y difícil de manejar. En 1994, un estudio de más de ochocientos treinta proyectos comerciales de software intensivo encontró la mayor cantidad de proyectos por encima del presupuesto, detrás de la planificación, o que tenían pocas características o funciones que las originalmente especificadas. En 1995, por encima de un cuarto de trillón dólares fue gastado en más de ciento sesenta y cinco mil proyectos de software a lo largo de los Estados Unidos. Un cuarto de ese dinero fue gastado en los desbordamientos del costo y otro tercio en proyectos cancelados. Estos resultados se pueden haber atribuido a la falta de gestión de riesgos. No obstante, la aplicación de la gestión de riesgos a los proyectos de desarrollo de software no actúa como una “bala plateada”, sino que ayuda a resolver y mitigar muchos problemas que los gestores de proyecto encuentran. Existen directivas que muestran el énfasis en la gestión de riesgos. Por ejemplo, el estándar EIA/IEEE en su sección 5.19.1 define: “El desarrollador debe ejecutar la gestión de riesgos a través de todo el proceso de desarrollo. Los desarrolladores deberán identificar, analizar y priorizar las áreas del proyecto de desarrollo de software en las cuales existen riesgos potenciales (riesgos técnicos, costos o calendario); desarrollando las estrategias para gestionar dichos riesgos, recopilándolos en el plan de desarrollo e implementando las estrategias de acuerdo al plan” (Matsuo, 1999).

Esteves (2005) refiere que aunque los diversos enfoques de gestión del riesgo aparecieron hace más de una década, sigue siendo evidente la poca utilización de sus técnicas en los proyectos de desarrollo de software actuales. La investigación en la gestión de riesgos en el ámbito del software procura formalizar conocimiento orientado a minimizar o evitar riesgos en

proyectos de desarrollo de software, mediante la generación de principios y buenas prácticas de aplicación realista. Hasta el momento se han propuesto y utilizado diferentes enfoques de gestión del riesgo desde que *Boehm* (1991) atrajo a la comunidad de ingeniería del software hacia la gestión del riesgo. Sin embargo, es evidente que pocas organizaciones utilizan todavía de una forma explícita y sistemática métodos específicos para gestionar los riesgos en sus proyectos de software. Así, por ejemplo, *KLCI* (2001) realizó y publicó un estudio con doscientas sesenta y ocho organizaciones de todo el mundo y el resultado fue que: el 3% no utilizaba ningún marco de gestión del riesgo, el 18% utilizaba algún marco caótico para identificar sus riesgos, el 37% de los participantes habían utilizado algún marco informal, el 28% utilizaban procedimientos repetitivos y sólo un 14% utilizaba un enfoque formal para identificar riesgos. Según este estudio, las razones más comunes para utilizar un marco informal son: falta de procedimientos, necesidades del proyecto no adecuadas, organización inmadura y compromiso del equipo. Según *Hoffman* (1998), aunque algunas organizaciones usen procesos formales de gestión del riesgo para otras partes de su negocio, demuestran una gestión de riesgos pobre en el ámbito general de los sistemas de información. *Kontio y Basili* (1997) creen que hay tres razones principales para la baja tasa de divulgación de tecnologías de gestión del riesgo: falta de conocimiento sobre posibles métodos y herramientas, limitaciones prácticas y teóricas de los marcos de gestión de riesgos que entorpecen la facilidad de uso de estos métodos, y tercero, todavía hay pocos informes con evaluaciones sistemáticas o científicas que proporcionen *feedback* empírico sobre su viabilidad y beneficios (*Esteves*, 2005).

El riesgo en un proyecto de desarrollo de software incluye componentes técnicos y de conocimiento del riesgo. Diferentes estudios han mostrado que la mayoría de los proyectos fallan sobre todo en gestión, no tecnológicamente. Además, son los temas de naturaleza organizacional los factores de riesgos del proyecto más dominantes a la vez que son los que se tratan satisfactoriamente en menos de la tercera parte de los proyectos de desarrollo. *Schmidt, Lyytinen y Keil* (2001) han observado que jefes de proyecto exitosos puntúan bajo aquellos factores sobre los que no tienen control o influencia como: conflictos entre departamentos, usuarios, cambio del propietario o responsable ejecutivo del proyecto, volatilidad del personal, número de unidades de la organización implicadas y proyectos que involucran a múltiples proveedores. Otro aspecto que influye es la falta de reconocimiento sobre la importancia de los aspectos organizacionales que existe en gran parte de la comunidad profesional y académica vinculada a las tecnologías de la información y la comunicación (*Esteves*, 2005).

Fairley (2006) plantea que algunos proyectos de software fallan en la entrega de sistemas aceptables dentro del horario y presupuesto y que muchos de estos fracasos se podrían haber evitado si el equipo de proyecto hubiese evaluado y mitigado debidamente los factores de riesgo, aún cuando la gestión de riesgos es raramente aplicada como una actividad explícita de gestión de proyectos (*Fairley*, 2006).

Según *Boehm* (1991), los diez factores de riesgo que más se presentan en los proyectos de software son: insuficiencias del personal; presupuestos y planificaciones poco realistas; desarrollo de funciones y propiedades erróneas; desarrollo de una mala interfaz de usuario, incorporación de funciones o características innecesarias; cambios continuos en los requerimientos; insuficiencias en los componentes suministrados externamente; insuficiencias en las tareas ejecutadas externamente; insuficiencias en la ejecución en tiempo real y tensionadas las capacidades de la ciencia de la computación (*Boehm*, 1991).

Según *Barki* (1993), los factores de riesgo que intervienen en la evaluación de riesgos en proyectos de desarrollo de software son: Tecnológico, Tamaño de la aplicación, Falta de experiencia, Complejidad de la aplicación y Ambiente organizacional (*Zulueta*, 2007a).

Matos (2009) en una entrevista realizada en abril del 2009 al gurú del software *Capers Jones*, plantea que las cuatro razones principales por la que fracasan los proyectos son: las estimaciones tempranas son inexactas y rechazadas por los clientes; el control de calidad no es muy bueno; el control de cambio no es muy bueno; el rastreo del progreso es sumamente malo. Además plantea que el control de la calidad es la clave del éxito en los proyectos de software. Ante la pregunta, ¿Considera que los mismos problemas que generan fracasos están mejorando o empeorando?, respondió: “Hasta la recesión del 2008, los proyectos que usaron *Agile*, TSP, RUP o habían encabezado el nivel 3 en CMM fueron hechos bastante bien. Ahora que la recesión es mundial y el crecimiento desacelerado, habrá tantos fracasos de negocios y despidos que el futuro ya no es previsible. Lo que me preocupa es que las empresas y los proyectos intentarán y escatimarán en el control de calidad, y naturalmente esta acción incrementará la probabilidad de fracasos” (*Matos*, 2009).

1.5 Los riesgos en el contexto empresarial.

La gestión de riesgos empresariales está siendo reconocida por el mundo como una actividad útil necesaria e independiente sobre la base de que posee una técnica propicia de aplicación, rápidamente identificable con los procesos que tienen que ver con la identificación, reducción y transferencia de riesgos (*Iglesias*, 2006).

La gestión de riesgos es parte fundamental de la estrategia y del proceso de toma de decisiones en la empresa y, por tanto, ha de contribuir a la creación de valor en todos los niveles, siendo imprescindible que la alta dirección lidere el proceso (González-Cueto, 2002).

Cuando hablamos de riesgos nos referimos también al contexto empresarial donde muchos de ellos se desarrollan, mantienen y soportan. Los riesgos a los cuales están expuestas las empresas son muchos y los mismos deben imperiosamente ponerse bajo control. El constante avance que en los diversos países hace la burocracia estatal y para-estatal sobre los entes privados, ha llevado a éstos a la búsqueda de herramientas o instrumentos que permitan suprimir y/o disminuir significativamente los riesgos a los cuales se encuentran expuestos. Una empresa está expuesta a errores internos de buena fe y a acciones que, de manera accidental o no, exponen a la misma a pérdidas y hasta ponen en riesgo su continuidad (Lefcovich, 2003).

Muy pocas empresas tienen políticas, planes y metodologías sistemáticamente conformadas para evitar los riesgos. Generalmente accionan por experiencia, intuición o planifican de manera parcializada. Actualmente ninguna empresa sería, que aspire o no a la excelencia, puede continuar operando de tal forma. Una de las gravísimas falencias de las auditorías externas está justamente en no controlar y evaluar apropiadamente los controles internos en su totalidad, como así tampoco evaluar desde un punto de vista sistémico a las empresas auditadas. Se propone como herramienta de control, para las auditorías internas y externas, la Matriz de Control Interno. La misma es una forma de pensar, de planificar, de delegar, de adoptar decisiones y resolver problemas, y de ver la organización en su totalidad (Lefcovich, 2003).

La *Treadway Commission's Committee of Sponsoring Organizations (COSO)*, emitió en el 2004 una plataforma integrada para la Gestión de Riesgos Empresariales (*ERM*) después de completar un proyecto de desarrollo que duró tres años, para satisfacer sus necesidades de control interno y moverse hacia un proceso más abarcador de gestión de riesgos (Protiviti, 2007). La plataforma integrada suministra ocho componentes para ser utilizadas cuando se está evaluando la Gestión de Riesgos Empresariales: ambiente interno; definición de objetivos; identificación de eventos; evaluación del riesgo; respuesta al riesgo; actividades de control; información y comunicación; monitoreo (COSO, 2004).

En Cuba, el Ministerio de Finanzas y Precios, puso en vigor la Resolución No. 297 del 2003 que comprende la definición de Control Interno, el contenido de los componentes y las normas para su implementación y evaluación. Posee 5 componentes que son: Ambiente de Control, Evaluación de Riesgos, Actividades de Control, Información y Comunicación y Supervisión y

Monitoreo (del Toro Ríos, 2005). El componente “Evaluación de riesgos” aporta mucho a las organizaciones, ya que las mismas, cualquiera sea su tamaño, se enfrentan a diversos riesgos de origen externos e internos que deben ser evaluados. La evaluación de los riesgos consiste en la identificación y el análisis de los riesgos relevantes para lograr los objetivos, y sirve de base para determinar cómo han de ser gestionados los riesgos. Debido a que las condiciones económicas, industriales, legislativas y operativas continuarán cambiando continuamente, es necesario disponer de mecanismos para identificar y afrontar los riesgos asociados con el cambio. La evaluación del riesgo debe ser un proceso continuo, una actividad básica de la organización, como la evaluación continua de la utilización de los sistemas de información o la mejora continua de los procesos.

Los procesos de evaluación del riesgo deben estar orientados al futuro, permitiendo a la dirección anticipar los nuevos riesgos y adoptar las medidas oportunas para minimizar y/o eliminar el impacto de los mismos en el logro de los resultados esperados. La evaluación del riesgo tiene un carácter preventivo y se debe convertir en parte natural del proceso de planificación de la empresa (Solórzano, 2006).

La resolución 297/03 del MFP no ofrece una metodología o procedimientos para que todas las entidades puedan gestionar efectivamente los riesgos a que están expuestas. En octubre de 2009, la Contraloría General de la República de Cuba publicó una Guía de Autocontrol destinada a las empresas, donde define un grupo de preguntas para que las mismas puedan evaluar el estado actual de su control interno. Se incluyen las preguntas relacionadas con el componente Evaluación de Riesgos (Contraloría General de la República de Cuba, 2009).

Quincosa (2007) plantea que una gestión de riesgos eficiente se traduce en efectos económicos incalculables para cualquier organización, constituyendo una herramienta imprescindible para la toma de decisiones. La gestión de riesgos ha pasado a ocupar un importante papel en la empresa moderna, contribuyendo cada vez más al cumplimiento de los objetivos y metas previstas en la organización hasta el punto que no se concibe una organización que pretenda avanzar con pasos firmes hacia el éxito sin contar con la actividad de gestionar los riesgos bien organizada. Propone una metodología para la gestión de riesgos empresariales, resumida en once operaciones fundamentales a realizar, la cual integra de una manera armónica los requisitos comprendidos en la Resolución 297/03 del Ministerio de Finanzas y Precios, los requisitos de la gestión de la calidad y la secuencia lógica para la aplicación de los sistemas de análisis de peligros y puntos críticos de control (APPCC), estos adaptados a las expectativas

que demandan los sistemas de control interno. La misma puede ser empleada como una herramienta para gestionar riesgos al nivel de toda la organización (Quincosa, 2006).

1.6 Necesidad de gestionar los riesgos.

La necesidad de gestionar los riesgos se incrementa con la complejidad del sistema: cuando se incrementan los riesgos técnicos y no técnicos (costo y planificación). Existe una necesidad creciente de métodos más sistemáticos y herramientas para complementar el conocimiento individual, el juicio y la experiencia. Muchos gerentes creen que están gestionando el riesgo en sus dimensiones multifacéticas, cuando en realidad están gestionando meramente el costo y la planificación con casos aislados de riesgos técnicos. El Programa de Riesgos del SEI proporciona un proceso estructurado, soportado por métodos y herramientas, para identificar, analizar y mitigar las incertidumbres encontradas. Muchos de los problemas más serios encontrados en la adquisición del sistema son el resultado de riesgos que han permanecido sin ser reconocidos y/o ignorados hasta que han provocado consecuencias serias. Este enfoque en la gestión de riesgo es importante porque estructuró técnicas, que pueden ser efectivas en la identificación del riesgo, procedimientos y técnicas que existen para la mitigación de riesgo (Higuera, 1996).

La experiencia ha mostrado que sólo unos pocos programas están gestionando el riesgo de una manera sistemática, y que el acercamiento de los programas a gestionar el riesgo tiende a ser *ad hoc*, indocumentado e incompleto. Los equipos del SEI también han encontrado que el riesgo del software está entre el menos medido o gestionado en un sistema (Higuera, 1996).

Según *Walsh*, a pesar del progreso significativo que han tenido las metodologías de desarrollo de software, continúan existiendo fallos en los proyectos de software. El trabajo realizado hasta el momento en la gestión de riesgos ha encontrado varios factores de riesgo y ha desarrollado métodos para evitar aquellos que causan fallos en los proyectos de software. Sin embargo, el desarrollo de software sigue siendo una tarea arriesgada donde deben tomarse decisiones sin poseer la información completa (Walsh, 2002).

Christopher Alberts y *Audrey Dorofee* del SEI, en el año 2006, definen algunos elementos que impactan en el análisis de riesgo para organizaciones de alto desempeño. Primeramente describen los cambios que han ocurrido en el ambiente operacional: del control de los procesos de gestión centralizados al control de los procesos de gestión distribuidos; de tecnologías aisladas y dedicadas a tecnologías conectadas en redes e interoperables; de la empresa permanente, definida por una estructura organizacional a empresas virtuales, definidas por una

misión; de un equipo y una misión a muchos equipos y una misión; de una vista compartimentada de los riesgos (por ejemplo, proyecto, seguridad) a una vista integrada de los riesgos. Debido a ello se hacen necesarias técnicas de riesgo más avanzadas. El ambiente operacional es más complejo (por ejemplo, los procesos distribuidos), apareciendo nuevos tipos de riesgo: riesgos heredados, nuevas fuentes de riesgo, riesgos de efectos combinados, riesgos de consecuencias en cascada, riesgos de amenazas emergentes (Alberts, 2006).

Las empresas se enfrentan con situaciones o sucesos que constituyen oportunidades para obtener beneficios o amenazas para sus éxitos. La gestión eficaz permite aprovechar las oportunidades y evitar las amenazas (O. N. Normalización, Cuba, 2008).

El desafío actual de la economía global, las oportunidades de negocio y los riesgos están en constante cambio. Existe la necesidad de identificar, evaluar y monitorear las oportunidades de negocio y los riesgos de la organización. Por lo tanto, es importante para una organización conocer cómo seguir pasos prácticos para integrar las oportunidades y los riesgos cuando se administran los negocios, así como qué hacer para gestionar los riesgos (Protiviti, 2007).

La adquisición, desarrollo y despliegue de los programas continúan sufriendo costos elevados, retrasos en las planificaciones y pobre ejecución técnica. Generalmente, esto es el resultado de un tratamiento inapropiado de la incertidumbre en la adquisición y desarrollo de sistemas de software intensivos y dependientes complejos. A la adquisición y las comunidades de desarrollo les falta una manera sistemática de identificar, comunicar, y resolver la incertidumbre técnica. A menudo la atención está en los síntomas de sobrepaso del costo y retrasos en la planificación en lugar de la raíz de las causas de la adquisición y desarrollo del producto. Todas las áreas en el desarrollo de los sistemas son fuentes potenciales de riesgos del software debido a que involucra tecnología, hardware, software, personas, costo y planificación (Higuera, 1996).

1.7 Marcos para la gestión de riesgos.

1.7.1 Generaciones.

Marcelo, en su estudio exploratorio sobre los métodos de gestión de proyectos de alto riesgo, muestra una clasificación de la gestión de riesgos para exponer mejor las características y evolución de cada una. Dichas generaciones son las siguientes (Marcelo, 2003):

G1. **Casuística:** Identificación de riesgos en los sistemas de los setenta y la previa en los negocios, todas basadas en cuestionarios.

- G2. **Taxonómica:** Análisis de riesgo en los proyectos. Traduce a ese sector el análisis de riesgos en los sistemas, desarrollado en los 80 junto a intentos poco articulados de análisis de riesgo en los negocios. Ejemplos: McFarlan, Boehm, PMI, SEI, Hall, SPR, SERIM.
- G3. **Causal o Emergente:** Es la primera que puede calificarse como gestión de riesgos en proyectos, aprovecha los métodos de gestión de riesgos usados en los sistemas. Referida en particular a proyectos informáticos. Nace de forma simultánea en Europa y en EE.UU., partiendo de la preocupación por proyectos de tanto riesgo como la adquisición o el desarrollo de software. Su enfoque, más completo y sistemático que el de la G2, ha seguido básicamente en Europa dos líneas paralelas, una financiada por la Comisión Europea (RiskMan, DriveSPI, RiskDriver) que parece haberse estancado; y otra impulsada por la propia Comisión para la Gestión de sus Compras (Eurométodo, ISPL (*Information Services Procurement Library*)), en cuyos desarrollos los autores han participado de forma continuada. Pone un énfasis particular en la evaluación de los modelos de riesgos y en la estimación de los recursos. Estos métodos de la G3, nacidos a mediados de los años noventa y actualmente aún en plena discusión, se apoyan en modelos sistémicos, relacionales (redes de causas-efectos) y proactivos en el aseguramiento de los proyectos (es decir, con resultados más predecibles). Tienden a superar así los modelos G1 de la primera generación, limitados a modelos casuísticos (listas de incidencias y de las medidas para contrarrestarlas); y los G2 de la segunda, meramente reactivos, con unas relaciones de causa-efecto basadas sólo en una confianza que parte de experiencias poco validadas.

1.7.2 McFarlan.

Puede considerarse como adelanto muy simplificado de la generación G3. Tras considerar las 5 consecuencias clásicas del riesgo (fracaso en beneficios, coste, plazo del proyecto; rendimiento; compatibilidad con otros sistemas), se centra en 3 factores de riesgo que afectan a su implantación (tras usar los medios adecuados), ordenados por su influencia (Marcelo, 2001, , 2003):

- ? Inexperiencia en la tecnología como factor subjetivo interno del equipo de realización
- ? Intransferencia del proyecto desde el usuario-cliente como factor subjetivo externo al equipo
- ? Envergadura del proyecto como factor objetivo.

McFarlan no se asume porque no define explícitamente un proceso para gestionar riesgos.

1.7.3 Boehm.

Según *Boehm*, la gestión de riesgos involucra dos pasos primarios, cada uno de los cuales tiene tres pasos subsiguientes. Ellos son (Boehm, 1991):

1. **Evaluación de riesgos:** Incluye:
 - a. **Identificación de los riesgos.** Produce las listas de elementos de riesgo del proyecto.
 - b. **Análisis de riesgos.** Evalúa la probabilidad de ocurrencia y la magnitud del impacto para cada elemento de riesgo identificado.
 - c. **Priorización de los riesgos.** Produce una lista ordenada de los elementos de riesgo identificados y analizados.
2. **Control del riesgo:** Involucra:
 - a. **Plan de gestión del riesgo.** Ayuda en la preparación para dirigir cada elemento de riesgo (por ejemplo, la vía para obtener información, anular el riesgo, transferir el riesgo o reducir el riesgo), incluyendo la coordinación de los planes de los elementos de riesgo individuales entre sí y con el plan del proyecto global.
 - b. **Resolución de riesgos.** Los elementos de riesgo son eliminados o, de lo contrario, resueltos (por ejemplo, la anulación de un riesgo a través de la relajación de requisitos).
 - c. **Monitoreo del riesgo.** Seguimiento del progreso del proyecto hacia la solución de sus elementos de riesgo y tomando acciones correctivas donde sea apropiado.

No se asume a Boehm por no incluir la Comunicación como parte del proceso, ni los riesgos empresariales, ni definir explícitamente una plantilla para la planificación y registro de riesgos.

1.7.4 Gestión de riesgos de proyectos de PMI.

La metodología de gestión de proyectos de PMI, el *Project Management Body of Knowledge* (PMBok), es la suma del conocimiento dentro de la profesión de dirección del proyecto. El cuerpo del conocimiento se apoya en los practicantes y académicos que lo aplican y le aportan. Incluye prácticas tradicionales demostradas que son ampliamente aplicadas, así como prácticas innovadoras que están surgiendo, incluyendo las publicadas y el material inédito. Como resultado, el PMBoK está evolucionando constantemente. Incluye los procesos relacionados a la Planificación de la gestión de riesgos, Identificación de Riesgos, Análisis cualitativo de riesgos, Análisis cuantitativo de riesgos, Planificación de respuestas a los riesgos y Seguimiento y control de los riesgos. Los objetivos de la Gestión de Riesgos del Proyecto son incrementar la probabilidad y el impacto de los eventos positivos y disminuir la probabilidad y el impacto de los eventos adversos al proyecto (PMI, 2004).

La metodología propuesta por PMI a través del PMBoK no se ajusta completamente a las necesidades de Softel, ya que no incluye la Comunicación como parte del proceso, ni aporta las plantillas para el plan de gestión de riesgos ni el registro de riesgos.

1.7.5 Programa de gestión de riesgos del SEI.

En su esfuerzo por responder a los problemas que presenta la gestión de riesgos, el objetivo del Programa de Riesgo del SEI es mejorar el proceso para la adquisición y desarrollo de sistemas de software intensivos. Para ello ha desarrollado una metodología para la Gestión de los Riesgos del Software (*Software Risk Management – SRM*) dirigida al ciclo de vida completo del software: adquisición, desarrollo y mantenimiento. Está soportado por tres grupos de prácticas: Evaluación del Riesgo del Software (SRE), Gestión Continua del Riesgo (CRM) y la Gestión del Equipo de Riesgo (TRM). Los mismos están soportados en tres estructuras básicas o construcciones que son: Paradigma para la Gestión de Riesgos, Taxonomía del Riesgo y Clínica del Riesgo.

El Paradigma para la Gestión de Riesgos está compuesto por las actividades: Identificación, Análisis, Planificación, Seguimiento, Control y Comunicación (Figura 1.3).

La Taxonomía de riesgos del SEI provee un marco para organizar los datos y la información. Se utiliza con el objetivo de identificar los riesgos. El modelo SW-CMM proporciona, a las organizaciones de software, una guía de cómo ganar control de sus procesos para desarrollar y mantener el software y cómo evolucionar hacia una cultura de excelencia en la ingeniería de software. El modelo SA-CMM está basado en los principios del SW-CMM. Describe cinco niveles de madurez para la adquisición de software organizacional (Higuera, 1996).

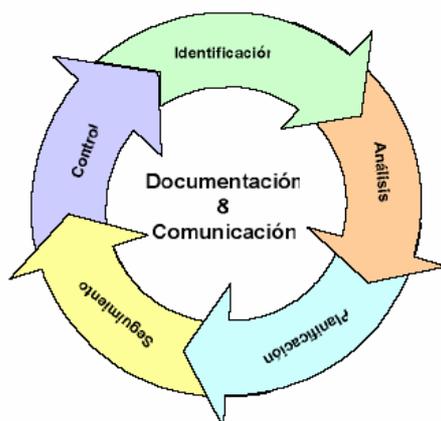


Figura 1.3. Paradigma para la Gestión de Riesgos.

El SEI no se asume como proceso para Softel porque no propone explícitamente un proceso

para planificar la gestión de riesgos. Su taxonomía responde fundamentalmente a riesgos típicos que existen en organizaciones grandes, generalmente militares, con proyectos de desarrollo de software también grandes y no incluye los factores organizacionales de riesgo.

1.7.6 Modelo de Hall.

Define dos actividades principales: la evaluación y el control del riesgo. La gestión de riesgos genera estrategias para decidir qué hacer en cada momento y está basada en nueve teorías (Marcelo, 2001, , 2003):

- ? Razona sobre la vulnerabilidad -probabilidad de riesgo- usando las Teorías de probabilidad, de incertidumbre y la de portfolio.
- ? Razona sobre el impacto -consecuencia del riesgo-, usando las Teorías de la utilidad, de juegos, del caos y/o la creatividad.
- ? Combina vulnerabilidad e impacto en el tiempo, usando la Teoría de la decisión y el Teorema de Bayes para elecciones dinámicas.

El modelo 6-D, de las 6 disciplinas PPMDD (Planear, Producir, Medir, Mejorar, Diseñar, Descubrir) soporta la mejora continua del proceso SEI o modelo de madurez de procesos en el desarrollo de software CMM (*Capability Maturity Model*) (Marcelo, 2001, , 2003):

- ? Diseñar. Transformar ideas en objetivos, creando y difundiendo la visión organizacional (CMM nivel 1).
- ? Planear. Confrontar los recursos disponibles y los requerimientos derivados de los objetivos del proyecto (CMM nivel 2).
- ? Producir. Implementar el plan para lograr el producto (CMM nivel 3).
- ? Medir. Comparar los resultados esperados y los realiza (CMM nivel 4).
- ? Mejorar. Aprender de experiencias como cambiar el plan (CMM nivel 5).
- ? Descubrir. Concienciar sobre el futuro, razona sobre posibilidades con resultados inciertos buenos (oportunidades) o malos (riesgos).

Este modelo amplía el concepto del riesgo en sentido revolucionario de oportunidad (consecuencias positivas) y soporta la mejora continua (modelo basado en la conciencia del pasado) y la reingeniería (modelo basado en la conciencia de futuro) (Marcelo, 2003).

No se asume el modelo de Hall porque no se definen explícitamente los procesos asociados a la planificación de la gestión de riesgos y a la comunicación.

1.7.7 Modelo SERIM de Karolak (IEEE).

Karolak aporta una visión integral del riesgo en la gestión empresarial y en el desarrollo tecnológico de los proyectos. Su manual SERIM de Gestión del Riesgo en Ingeniería de Software distingue los riesgos en el negocio (coste, plazo) y la tecnología, pero los vincula más a ésta, al estudiarlos en las seis Etapas del ciclo clásico de desarrollo (pre-requisitos, requisitos, diseño, codificación, pruebas, implantación/entrega/mantenimiento), con cuatro Etapas progresivas (Identificar, Estimar, Planear, Reducir los Riesgos) y dos Etapas realimentadoras del modelo (Informar, Predecir los riesgos) (Marcelo, 2003).

No se asume el modelo SERIM porque no se definen explícitamente la comunicación.

1.7.8 Modelo de Barki.

El Modelo 'integrativo' de 'contingencia' de Barki toma como hipótesis la influencia de dos variables: Nivel de Exposición al riesgo del proyecto y Perfil de la Gestión de su riesgo (cómo se maneja) en el Rendimiento del proyecto. El modelo emplea, como variable de intermediación, la adecuación de la Gestión respecto a la Exposición. Barki resume como hipótesis central que "el Rendimiento del proyecto será tanto mayor cuanto mejor se acople el Perfil de Gestión del Riesgo al nivel de su Exposición". Además la gestión de un proyecto de alto riesgo requiere: mucha integración interna y altos niveles de planificación formal (con alta capacidad de proceso de información) si se busca el cumplimiento de presupuesto; y/o mucha integración externa (participación del usuario), si se busca la calidad del producto (Marcelo, 2003).

No se asume el modelo de Barki porque no se definen explícitamente los procesos asociados a la gestión de riesgos. El mismo depende de la adecuación de la gestión respecto a la exposición, para lo cual se necesitan altos niveles de planificación formal, no existentes actualmente en Softel.

1.7.9 Pressman.

Pressman (2005) define un proceso para gestionar los riesgos de un proyecto de software que incluye la identificación (evaluación global del riesgo, componentes y controladores del riesgo); la proyección o estimación del riesgo (tabla de riesgo, evaluación del impacto del riesgo, evaluación del riesgo); el refinamiento del riesgo y la reducción, supervisión y gestión del riesgo (evitar, supervisar y gestionar el riesgo, además de los planes de contingencia). Se refiere al método de la Lista de comprobación de los elementos de riesgo para identificar riesgos. Expone algunas preguntas que se pueden hacer para saber qué tan grave puede ser el riesgo y poder

realizar la evaluación global de riesgos del proyecto, así como el formato y contenido de la tabla que se puede emplear para ello (Pressman, 2005).

Para la estimación del riesgo, se puede emplear la Tabla de riesgos, en la cual se listan y categorizan todos los riesgos, se determina su probabilidad de aparición e impacto. Los riesgos de alta probabilidad y alto impacto pasan a lo alto de la tabla. Para poder priorizar los riesgos de primer orden, se debe estudiar la tabla ya ordenada, dibujando una línea de corte, de forma horizontal desde un punto en la tabla. Esto implicará que sólo a los riesgos que queden por encima de esta línea de corte, se les prestará atención en adelante y se les definirá el Plan de reducción, supervisión y gestión del riesgo (Pressman, 2005).

No se asume Pressman como proceso, pues el mismo no profundiza en todas las actividades asociados a la gestión de riesgos y no incluye la planificación de la gestión de riesgos ni la comunicación.

1.7.10 IEEE Computer Society.

La IEEE *Computer Society* (*Computer Society of the Institute of Electrical and Electronics Engineers*) y otras organizaciones están conduciendo una cantidad de proyectos que dependen de la evolución de la Guía SWEBOK (*SoftWare Engineering Body Of Knowledge*). La Guía 2004 es la edición actual de una guía que continuará evolucionando para encontrar las necesidades de la comunidad de ingeniería de software. Establece por primera vez una línea base para el cuerpo de conocimientos en el campo de la ingeniería de software. Posee 10 Áreas de Conocimiento (KAs). Como un tópico del Plan de Proyecto de Software se encuentra la Administración de Riesgos. Incluye la identificación y análisis de riesgo y la evaluación de riesgos críticos, la mitigación de riesgo y los planes de contingencia. Durante la actividad "Proceso de Monitoreo", el perfil de riesgos del proyecto es vuelto a visitar y es evaluada la adherencia para los requisitos de calidad. La exposición e influencia del riesgo son recalculados y se vuelven a ejecutar los árboles de decisión y las simulaciones de acuerdo a los nuevos datos. Durante la actividad "Proceso de Control", se realizan los cambios al proyecto de acuerdo a los resultados obtenidos durante el Proceso de Monitoreo. Por lo tanto, es aquí donde el impacto y los riesgos asociados son modelados y administrados. Pueden incorporarse nuevas contingencias y hasta decidir que se debe abandonar el proyecto (IEEE, 2004).

No se asume la Guía SWEBOK de la IEEE ya que no incluye la planificación de la gestión de riesgos ni la comunicación. Además no incluye plantillas para el registro de riesgos ni es rico en herramientas y técnicas para el proceso.

1.7.11 Richard Fairley (IEEE).

Fairley define un proceso de siete pasos para la gestión de riesgos: identificar los factores de riesgo, evaluar las probabilidades del riesgo y sus efectos en el proyecto, desarrollar estrategias para mitigar los riesgos identificados, monitorear los factores de riesgo, invocar el plan de contingencia cuando el indicador del riesgo cruza el umbral predeterminado, gestionar la crisis y recuperarse de la crisis. Está basado en varios años de trabajo con numerosas organizaciones para identificar y superar los factores de riesgo en proyectos de software donde, al interactuar con sus clientes, han utilizado variedad de técnicas de gestión de riesgos dentro del proyecto: modelar costos basado en regresiones, teoría de la decisión, tablas de riesgo y modelos de proceso en espiral (Fairley, 2006).

No se asume el proceso propuesto por Fairley, ya que no incluye la planificación de la gestión de riesgos ni la comunicación.

1.7.12 Microsoft Solutions Frameworks (MSF).

La Gestión de Riesgos es una disciplina central de *Microsoft Solutions Framework* (MSF). Reconoce que los cambios y la incertidumbre resultante son aspectos heredados del ciclo de vida de las tecnologías de la información. MSF define un Proceso de Gestión de Riesgos para la gestión continua de los riesgos. Está compuesto de 6 pasos: identificación, análisis y priorización, planificación (formular estrategias, planes y acciones y actualizar el plan del proyecto), seguimiento, control y aprendizaje (formaliza las lecciones aprendidas y artefactos del proyecto pertinentes y herramientas y captura el conocimiento de forma tal que pueda ser reutilizado dentro del equipo y por la empresa) (Microsoft, 2002).

No se asume MSF por no contemplar explícitamente la comunicación como un proceso. No obstante, incluye el aprendizaje para comunicar las lecciones aprendidas sobre los riesgos del proyecto y tener una retroalimentación a nivel empresarial sobre los recursos destinados a la gestión de riesgos para mantener una base de conocimiento de riesgos a nivel organizacional. No incluye plantillas para la planificación ni el registro de riesgos.

1.7.13 MAGERIT.

MAGERIT (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas), desarrollada por el Ministerio de Administraciones Públicas de España, es una metodología enfocada a la seguridad del sistema en el desarrollo del mismo. Permite un seguimiento exhaustivo de la seguridad del sistema ajustándose a criterios como los de ITSEC o Criterios Comunes de Evaluación de la Seguridad de los Productos y Sistemas de

Información, que permitan la posterior homologación y certificación del sistema de información desde el punto de vista de la seguridad. Consta de tres fases, que incluyen actividades y tareas (ADMINISTRACIONES PÚBLICAS, 2006):

1. **Planificación del Proyecto de Riesgos:** estimaciones iniciales de los riesgos que pueden afectar al sistema de información así como del tiempo y los recursos que su tratamiento conllevará. El objetivo principal de este proceso es establecer el marco general de referencia para todo el proyecto.
2. **Análisis de Riesgos:** se estima el impacto que tendrán los riesgos en la organización.
3. **Gestión de riesgos:** Se procesan los impactos y riesgos identificados en el proceso anterior, bien asumiéndolos, bien afrontándolos. Para afrontar los riesgos que se consideren inaceptables se llevará a cabo un plan de seguridad que corrija la situación actual.

No se asume MAGERIT ya que el mismo está encaminado a garantizar la seguridad del sistema en su desarrollo y no incluye la comunicación como un proceso.

1.7.14 Dirección Nacional de Aduanas de Chile.

La Dirección Nacional de Aduanas de Chile ha definido su proceso de gestión de riesgos, que incluye las siguientes etapas: establecimiento del contexto, identificación de los riesgos, análisis de riesgos, evaluación y priorización de los riesgos, tratamiento de los riesgos y monitoreo y revisión. A continuación se destacan características y/o métodos que se pueden aplicar en algunas etapas (Dirección Nacional de Aduanas, 2007):

- ? Definición del Contexto: Identificar la contribución que hará a la organización en el logro de sus objetivos, valores, políticas y estrategias, cuando tome decisiones acerca de los riesgos.
- ? Identificación de Riesgos. Identificar los riesgos. Se pueden utilizar los métodos: diagramas de flujo; técnicas de análisis de sistemas; discusiones de grupo o entrevistas; experiencia personal del funcionario; inspecciones físicas y auditorías anteriores; tormenta de ideas; encuestas y cuestionarios; técnica Delphi; estudio de la experiencia extranjera o nacional; juicios, consensos especulativos, conjeturas, intuiciones.
- ? Análisis de riesgos. Analizar la posibilidad y consecuencias de cada factor de riesgo para establecer el nivel de riesgos. Las categorías de métodos utilizados para determinar el nivel de riesgo son: Cualitativos, Semi-cuantitativos y Cuantitativos. El enfoque que se utiliza con mayor frecuencia tiende a ser cualitativo: el juicio y la intuición para tomar sus decisiones. El nivel de riesgo puede ser calculado utilizando el método cuantitativo cuando la probabilidad de ocurrencia y las consecuencias puedan ser cuantificadas (Tabla 1.1).

Tabla 1.1. Métodos Cuantitativos y Cualitativos.

Métodos Cuantitativos	Métodos Cualitativos
1. El análisis de probabilidad.	1. Tormenta de ideas.
2. El análisis de consecuencias.	2. Cuestionario y entrevistas estructuradas.
3. La modelación o simulación computacional.	3. La evaluación que utiliza grupos multidisciplinares.
4. El análisis estadístico / numérico.	4. El juicio de especialistas y expertos, como la técnica Delphi.
5. La investigación de mercado.	
6. Análisis de redes.	
7. Análisis de costo del ciclo de vida.	
8. Árboles de decisión.	
9. Los árboles de falta y los análisis de árbol de eventos.	
10. Diagramas de influencia.	

- ? Evaluación y priorización de riesgos. Se clasifican los riesgos más importantes para identificar las prioridades de gestión.
- ? Tratamiento de riesgos. Pauta general: los riesgos de bajo nivel pueden ser aceptados y puede no ser necesaria una acción adicional; los niveles de riesgo significativos o más importantes deben ser tratados; los niveles altos de riesgo requieren de una cuidadosa gestión y de la preparación de un plan formal para gestionar los riesgos. Las opciones para el tratamiento de los riesgos son: evitarlo, reducir el nivel de riesgo, transferirlo o aceptarlo.
- ? Monitoreo y revisión. Es necesario monitorear: los riesgos, la efectividad del plan, las estrategias y el sistema de gestión establecido para controlar la implementación de los tratamientos de riesgo.

No se asume el proceso de la Dirección Nacional de Aduanas de Chile porque no incluye la comunicación como parte del proceso. Además, la información que suministra acerca de fuentes de riesgo, áreas de impacto, así como la necesaria para identificar riesgos es relativa a la aduana. No ofrece plantillas para la definición del contexto (planificación de la gestión de riesgos) ni el registro de riesgos.

1.7.15 Modelo Gestión Riesgos en Proyectos de Desarrollo de Software (MoGeRi).

Zulueta (2007) en su Tesis de Maestría, a partir del estudio profundo del tema de gestión de riesgos en el mundo, en Cuba y, particularmente en la UCI, propone el modelo MoGeRi para la gestión de riesgos en los proyectos de desarrollo de software, que consta de seis procesos: Planificación de la gestión de riesgos; Identificación de los riesgos; Análisis de los riesgos;

Planificación de las respuestas; Seguimiento y control y Comunicación de la información sobre los riesgos. Propone un marco para la gestión de riesgos tomando elementos del SEI y de PMI, por su reconocimiento, integralidad, actualidad y aplicación internacional y teniendo en cuenta las características propias de la UCI. Para cada proceso definido se describen sus actividades y tareas (Zulueta, 2007a, , 2007b).

No se asume MoGeRi porque este proceso fue concebido teniendo en cuenta las características propias de la UCI y no incluye una plantilla para el Plan de Gestión de Riesgos.

1.7.16 La Evaluación de Riesgos del Sistema de Control Interno.

El segundo componente del Sistema de Control Interno es la Evaluación de Riesgos. Sus Normas son las siguientes (del Toro Ríos, 2005):

1. Identificación del Riesgo. Determinar la exposición de una empresa o negocio a un riesgo o pérdida. Se realiza un análisis, caracterización de los riesgos y establecimiento de las relaciones entre el riesgo y/o las causas que los originan.
2. Estimación del riesgo: Cuantificar las exposiciones al riesgo, basada en su impacto financiero en la entidad y expresada en términos monetarios. Permite priorizar los riesgos. Se determina el impacto y probabilidad de ocurrencia.
3. Determinación de los objetivos de control: Diseñar los objetivos de control para minimizar los riesgos identificados como relevantes y determinar qué técnica(s) de control se utilizarán para implementarlo.
4. Detección del cambio: Disponer de procedimientos capaces de captar e informar oportunamente los cambios registrados o inminentes en el ambiente interno y externo, que puedan conspirar el alcance de sus objetivos.

A pesar de que Softel es una empresa y tiene que tener implementados todos los componentes de la resolución 297/03 del MFP, la Evaluación de Riesgos que propone no es suficiente para los proyectos de desarrollo de software de la empresa, pues no fue concebido para estos fines. No incluye taxonomías de riesgos adecuadas, no es rico en herramientas y técnicas que se pueden aplicar a los proyectos, no es exhaustivo en la caracterización de los riesgos, no ofrece plantillas para el registro de riesgos ni para la planificación de dicha actividad. Por todo lo anterior no se puede emplear para los proyectos de desarrollo de software.

1.7.17 Modelos de Calidad.

1.7.17.1 CMMI.

CMMI se ha convertido en el nuevo estándar a nivel mundial para la medición de la calidad de los procesos de desarrollo de software, presenta como una de sus PA (Áreas de Proceso) fundamentales, de Nivel 3, la Gestión de Riesgos, que es un proceso continuo, de mirar hacia delante que constituye una parte importante de la gestión; debe dirigirse a problemas que pudieran poner en peligro el logro de objetivos críticos; es aplicado para anticiparse eficazmente y mitigar los riesgos que pueden tener un impacto crítico en el proyecto (Maniasi, 2005).

El Área de procesos de Gestión de Riesgos de CMMI describe prácticas específicas para sistemáticamente planear, anticipar y mitigar los riesgos para minimizar de forma proactiva su impacto en el proyecto. Aunque el énfasis primario del Área de Procesos de Gestión de Riesgos es en el proyecto, los conceptos pueden ser aplicados para gestionar los riesgos organizacionales (CMMI Product Team, 2006).

Entre sus fortalezas se destacan (de la Villa, 2004):

- ? Inclusión de las prácticas de institucionalización, que permiten asegurar que los procesos asociados con cada área de proceso serán efectivos, repetibles y duraderos.
- ? Guía paso a paso para la mejora, a través de niveles de madurez y capacidad (frente a ISO).
- ? Transición del 'aprendizaje individual' al 'aprendizaje de la organización' por mejora continua, lecciones aprendidas y uso de bibliotecas y bases de datos de proyectos mejorados.

Algunas de sus debilidades son:

- ? El CMMI puede llegar a ser excesivamente detallado para algunas organizaciones.
- ? Puede ser considerado prescriptivo.
- ? Requiere mayor inversión para ser completamente implementado.
- ? Puede ser difícil de entender.

1.7.17.2 ISO/IEC 12207.

La Norma ISO/IEC 12207 se publicó el primero de agosto de 1995 y es la primera Norma Internacional en proporcionar un conjunto detallado de procesos, actividades y tareas del ciclo de vida para el software (O. N. d. Normalización, 2007). La ISO/IEC 12207: 2008 establece una plataforma común para los procesos del ciclo de vida del software, con terminología bien definida, que puede ser referenciada por la industria del software. Proporciona los procesos, actividades y tareas de apoyo necesarias, y los procesos, actividades y tareas organizacionales

para la gestión y mejora de los procesos. Dentro de la Sección 6.3 Procesos del Proyecto, define el Proceso de Gestión de Riesgos (sección 6.3.4) que incluye las actividades: planificación de la gestión de riesgo, gestión del perfil de riesgo, análisis de riesgo, tratamiento del riesgo, monitoreo del riesgo y evaluación del proceso de gestión de riesgo. Para cada actividad define las tareas que se ejecutan (Mutafelija, 2009).

1.7.17.3 Norma cubana NC-ISO/IEC Guía 51: 1999.

Es una adopción idéntica por el método de traducción de la ISO/IEC Guía 51:1999, del mismo nombre, segunda edición. Pone a disposición de los elaboradores de las normas las directivas para la inclusión de los aspectos de seguridad. Adopta un enfoque basado en la reducción del riesgo y se dirige al uso de los productos, procesos o servicios.

La seguridad es alcanzada por la reducción del riesgo hasta un nivel tolerable, empleando el siguiente procedimiento: identificar los posibles grupos de usuarios del producto, proceso o servicio; identificar el uso previsto y estimar el mal uso que razonablemente pueda esperarse del producto, proceso o servicio; identificar cada peligro (incluyendo cualquier situación peligrosa y evento peligroso) que surja en todas las etapas y condiciones para el uso del producto, proceso o servicio, incluyendo la instalación, mantenimiento, reparación y destrucción/eliminación; estimar y evaluar el riesgo, para cada grupo de usuario/grupo de contacto proveniente del peligro(s) identificado; juzgar si el riesgo es tolerable, (ej. por la comparación con similares productos, procesos o servicios); si el riesgo no es tolerable, reducir el riesgo hasta convertirlo en tolerable (O. N. Normalización, Cuba, 2000).

1.7.17.4 Norma cubana NC-ISO/IEC Guía 73: 2008.

Es una adopción idéntica por el método de traducción de la Guía Internacional ISO/IEC Guía 73:2002 *Risk management. Vocabulary. Guidelines for use in standards*. La gestión del riesgo forma parte de los procesos de gestión de las organizaciones. Cada vez con más frecuencia, las organizaciones utilizan procesos de gestión del riesgo con objeto de optimizar la gestión de sus oportunidades potenciales. Esto difiere del proceso de gestión del riesgo explicado en la NC-ISO/IEC Guía 51, donde el riesgo se considera únicamente como generador de consecuencias negativas. Sin embargo, esta Guía se ocupa de ambas situaciones. Define la Gestión del Riesgo como el conjunto de actividades coordinadas para dirigir y controlar una organización, con respecto al riesgo. Sus actividades son (O. N. Normalización, Cuba, 2008):

1. **Apreciación del Riesgo:** Formado por el análisis del riesgo y la evaluación del riesgo:

- 1.1. **Análisis del Riesgo:** Utilización sistemática de información para identificar los orígenes y para estimar el riesgo.
 - 1.1.1. **Identificación del origen:** Encontrar, listar y caracterizar los riesgos.
 - 1.1.2. **Estimación del riesgo:** Asignar valores a la probabilidad y consecuencias del riesgo.
- 1.2. **Evaluación del riesgo:** Comparación del riesgo estimado con respecto a los criterios de riesgo dados, para determinar la importancia del riesgo.
2. **Tratamiento del Riesgo:** Selección e implantación de medidas para modificar el riesgo.
 - 2.1. **Evitación del riesgo:** Decisión para no estar implicado en una situación de riesgo, o la acción para retirarse de ella. Se puede basar en los resultados de la evaluación del riesgo.
 - 2.2. **Optimización del riesgo:** Minimizar las consecuencias negativas y maximizar las positivas y sus respectivas probabilidades.
 - 2.3. **Traspaso del riesgo:** Repartición con otra parte de la carga de las pérdidas o del beneficio de las ganancias de un riesgo. Se puede realizar mediante seguros u otros acuerdos contractuales y puede generar nuevos riesgos o modificar el existente.
 - 2.4. **Retención del riesgo:** Aceptación de la carga de las pérdidas o del beneficio de las ganancias debidas a un riesgo particular. Incluye la aceptación de los riesgos que no hayan sido identificados.
3. **Aceptación del Riesgo:** Decisión de aceptar un riesgo.
4. **Comunicación del Riesgo:** Intercambio o reparto de información relativa al riesgo entre el decidor y otras partes partícipes en la empresa. La información puede estar relacionada con la existencia, la naturaleza, la forma, la probabilidad, la severidad, la aceptabilidad, el tratamiento u otros aspectos del riesgo.

1.8 Algunas herramientas y técnicas.

1.8.1 Para la identificación de riesgos.

Existen varios métodos y herramientas para la identificación de riesgos. La decisión respecto a qué método utilizar se basa en las características particulares del equipo de proyecto. Entre las técnicas más popularmente aceptadas se encuentran: tormenta de ideas, encuestas, entrevistas, grupos de trabajo, conocimiento por experiencia o documentado, taxonomías de riesgos, plantillas de ingeniería y de camino crítico, entre otras (Maniasi, 2005).

Maniasi, en su Tesis de Maestría, propone la construcción de una herramienta, llamada "Asistente" para la identificación de riesgos. La Tabla 1.2 resume las características principales de las herramientas de software que fueron estudiadas por él (Maniasi, 2005).

Tabla 1.2. Herramientas para la identificación de riesgos.

Producto	Proveedor	Descripción	Plataforma
Active Risk Manager (ARM)	Strategic Thought	Herramienta integrada de Administración de Riesgos que brinda una solución para la Identificación de Riesgos mediante la utilización de la información contenida en la WBS de proyecto.	Web Based
Technical Risk Identification and Mitigation System (TRIMS)	Best Manufacturing Practices	Herramienta integrada de Administración de Riesgos que emplea ingeniería de conocimientos y que se enfocada en la identificación y medición de riesgos técnicos de proyectos.	Win32
RiskTrak	Risk Services & Technology	Herramienta integrada de Administración de Riesgos que brinda una solución para la Identificación de Riesgos mediante el empleo de base de datos.	Win32
WelcomRisk	Welcom	Herramienta integrada de Administración de Riesgos que brinda una solución para la Identificación Sistemática de Riesgos mediante la utilización de bibliotecas configurables de categorías de riesgos.	Win32

La Tabla 1.3 permite realizar una comparación entre las principales características de las herramientas analizadas en la Tabla 1.2 y la herramienta “Asistente” propuesta por Maniasi. En su análisis plantea que no existen herramientas que brinden un soporte adecuado y estandarizado a los administradores de proyectos específicamente durante la fase de identificación de riesgos en organizaciones que comienzan con la implementación formal de las tareas de gestión de riesgos; las herramientas existentes o bien se enfocan solo en una categoría de riesgos [TRIMS, 2004], o bien están orientadas a compañías que poseen una amplia base de datos organizacional que les permite generar información de categorías propias de riesgos [RiskTrak, 2004; WelcomRisk, 2004], o bien emplean un mecanismo que no se orienta al uso de taxonomías [Active Risk Manager, 2004] (Maniasi, 2005).

Tabla 1.3. Comparación de Herramientas de soporte de Identificación de Riesgos.

	ARM	TRIMS	RiskTrak	WelcomRisk	Asistente
Taxonomías estándar	No	Sí	No	No	Sí
Riesgos de todo tipo	Sí	No	Sí	Sí	Sí
Multiplataforma	Sí	No	No	No	Sí
Portable a varios idiomas	No	No	No	No	Sí

Modelo completo	Sí	Sí	Sí	Sí	No
Interfaz gráfica	Sí	Sí	Sí	Sí	Sí
Reportes	Sí	Sí	Sí	Sí	Sí

El objetivo de la herramienta “Asistente” es brindar la posibilidad de efectuar tareas de Identificación de Riesgos en base a taxonomías estándar en organizaciones de software de cualquier tipo. Para ello se consideraron una serie de taxonomías estándar de la industria ([Marvin J. Carr et al., 1993], [Caper Jones, 1994], [TeraQuest, 1998], [Microsoft, 2002] y [TBS, 2002]) y luego de varias sesiones de tipo *Wideband Delphi* entre expertos del dominio, se generó una Taxonomía de Riesgos Ajustada que contiene un compendio de la información y categorías propuestas por diferentes autores y entidades; criterios de aplicabilidad; relaciones causales y probabilidades de ocurrencia en base a tipos de proyectos que han sido determinados y validados en base a la experiencia y conocimiento. La Taxonomía de Riesgos Ajustada contempla 114 Factores de riesgo (Maniasi, 2005).

1.8.2 Para el control de las organizaciones: Matriz de Control Interno.

La alta Gerencia puede verificar por medio de la Matriz de Control Interno que se esté dando cumplimiento a todos los controles, quiénes están a cargo de dichas verificaciones, cuándo fue la última vez que realizaron los controles para cada punto y con qué frecuencia. En función de la importancia relativa de los distintos puntos y de sus problemas se le dará la prioridad de control y corrección. La matriz contempla el 100% de los factores de riesgo siendo de tal forma un vehículo formidable para evitar o corregir defectos que perjudiquen patrimonial y económicamente a la entidad. Una rápida visión de dicha matriz, por parte de los Directivos le permiten saber las áreas que comprometen a la empresa, y proceder a analizar las causas o motivos, para luego aplicar las correspondientes medidas de ajuste (Lefcovich, 2003).

1.9 Experiencia de la Universitat Politècnica de Catalunya (UPC). Proyecto PRISMA.

En el 2001 la UPC decidió unificar la gestión de los estudios de toda la universidad en un único sistema, surgiendo así el proyecto PRISMA (Esteves, 2005). Una de las primeras fases estuvo orientada a la selección de un método para gestionar los riesgos, para lo cual trabajaron en la identificación, evaluación y selección de los diferentes métodos existentes para organizar la implementación de las funciones básicas que deben llevarse a cabo para una gestión efectiva de los riesgos “antes de que estos lleguen a ser amenazas para el éxito”. La Tabla 1.4 muestra los métodos que fueron evaluados, ampliamente conocidos y fácilmente accesibles por sus nombres o por las organizaciones que los avalan: Euromethod, Safe, SEI-CRM, RiskIt y los métodos para la gestión de riesgos del IEEE y del PMI (Esteves, 2005).

Tabla 1.4. Lista de los métodos de gestión del riesgo evaluados en el proyecto PRISMA.

	Euromethod	Safe	SEI	IEEE	Riskit	PMI
Plan de Gestión						X
Identificación	X	X	X	X	X	X
Estimación	X		X	X	X	X
Evaluación	X	X	X	X	X	X
Planificación	X	X	X	X	X	X
Tratamiento	X	X	X	X	X	X
Seguimiento y control	X	X	X	X	X	X
Comunicación			X			

El proyecto PRISMA adoptó el método SEI-CRM, extendiéndolo con la fase de definición del plan de gestión del riesgo del modelo del PMI y adicionando a la taxonomía del SEI otra categoría de factores de riesgo, los factores organizacionales de riesgo, importados y adaptados de los factores organizacionales y estratégicos identificados por Esteves y Pastor para la implementación de sistemas integrados ERP (*Enterprise Resource Planning*). El proceso implementado consta de las fases: Identificación de Riesgos y Proceso continuado de gestión del riesgo (análisis, planificación, seguimiento, control y comunicación) (Esteves, 2005).

1.10 Estudios sobre la gestión de riesgos en Cuba.

En Cuba, como parte del Sistema de Control Interno, muchas entidades han comenzado a identificar y evaluar sus riesgos, lo cual no significa que en todos los casos se haga una correcta gestión de los mismos. Bolaños hace un análisis de la evaluación de riesgos como parte del Sistema de Control Interno en las universidades cubanas. Reconoce que existen en la actividad universitaria muchas fuentes de riesgos (internas y externas) que se desglosan, lo cual puede contribuir a crear una lista de chequeo y realizar la evaluación a la medida de cada entidad, con la estrategia y seguimiento de acuerdo a sus características (Bolaños, 2008).

Zulueta (2007) plantea que los resultados de las encuestas y entrevistas realizadas demostraron la inexistencia de una cultura general sobre la gestión de riesgos en proyectos de desarrollo de software. Se identificaron problemas merecedores de una profunda investigación en el dominio de RUP y su uso y adaptabilidad al entorno UCI. A pesar de la carencia de conocimientos sobre los marcos de gestión de riesgos, se reconoció unánimemente la importancia de sus prácticas para el cumplimiento de los objetivos del proyecto y la necesidad de guiar las acciones hacia la creación e implantación de un modelo de gestión de riesgos, MoGeRi, en el desarrollo de software en la UCI (Zulueta, 2007a). Zulueta (2009) publicó un nuevo estudio que propone un conjunto de principios que deben ser considerados para lograr dimensionar la gestión de riesgos en el plano pedagógico: educación temprana en la gestión de

riesgos; integración interdisciplinaria; fusión Gestión de riesgos-desarrollo de software. Para ello en la UCI se concibió un curso de gestión de riesgos como parte del segundo perfil Calidad de Software que ha sido recibido por estudiantes de los grupos de calidad de las 10 facultades. En el caso de postgrado, se imparte el Curso de Gestión de Riesgos en Proyectos Informáticos a los profesores universitarios (Zulueta, 2009).

El modelo MoGeRi comenzó su implantación en el año 2006 en seis proyectos, lo cual permitió identificar sus bondades, debilidades y las acciones necesarias para generalizarlo en el proceso productivo UCI. De manera general los proyectos incluidos en el estudio presentaron problemas en la planificación y gestión, lo cual implicó que el proceso de planificación de la gestión de riesgos no se realizara con la madurez requerida. En todos los casos, los equipos de gestión de riesgos presentaron cuestionarios ajustados a los proyectos, a partir de la taxonomía del SEI fundamentalmente, para facilitar la identificación de los riesgos, lográndose muy buena comunicación con el equipo. A pesar de las limitaciones que existieron en la aplicación de MoGeRi, la exposición al riesgo se redujo en más de un 50% en todos los proyectos. Los principales riesgos identificados fueron: insuficiente implicación de los usuarios; estimaciones de productividad y calidad que no tienen en cuenta los datos históricos; cambios significativos en la estructura organizacional del proyecto; las políticas y estándares no se encuentran definidos o no son seguidos; inestabilidad en los requerimientos; las características del producto dificultan la realización de pruebas; programa de formación inadecuado (Zulueta, 2009).

Conclusiones parciales.

1. Después del análisis de la bibliografía sobre riesgos y su gestión se pudo concluir que ninguno de los procesos o marcos de gestión de riesgos estudiados se ajusta a las necesidades de Softel. Es por ello que no se puede emplear directamente ninguno de los estudiados.
2. Para la definición del Proceso de Gestión de Riesgos para los proyectos de desarrollo de software de Softel, se decidió hacer una adecuación del Área de Conocimiento “Gestión de los Riesgos del Proyecto” de la metodología de gestión de proyectos del PMI, el PMBoK.

Capítulo II. Diagnóstico del estado actual.

Introducción.

En este capítulo se exponen los métodos científicos utilizados en la investigación. Se realiza el diagnóstico del estado actual de la gestión de riesgos en entidades cubanas, fundamentalmente en Softel y de la gestión de riesgos en los proyectos de desarrollo de software de la empresa. Se hace un análisis de los resultados obtenidos en cada caso, empleando la Taxonomía Ajustada (Maniasi, 2005) para agrupar los riesgos en categorías y conocer cuáles son los que más inciden. Se demuestra que no existe un proceso formal ni se realiza adecuadamente la gestión de riesgos en los proyectos de desarrollo de software de la empresa.

2.1 Métodos Científicos de Investigación.

Para el diseño de la investigación se utilizó como referencia el libro “El paradigma cuantitativo de la investigación científica” (Hernández L.R.A., 2002).

La **Estrategia de la investigación** utilizada fue Descriptiva.

Los **Métodos teóricos** utilizados para este estudio fueron (Hernández L.R.A., 2002):

- ? Histórico: Para realizar el estudio del estado del arte, al analizar la trayectoria completa de la gestión de riesgos, su condicionamiento a los diferentes períodos de la historia, las etapas principales de su desenvolvimiento y las conexiones históricas fundamentales, permitiendo la extracción de los elementos más importantes que se relacionan con el proceso de gestión de riesgos.
- ? Lógico: Para constatar teóricamente cómo ha evolucionado el fenómeno de la gestión de riesgos permitiendo determinar cambios en su funcionamiento y aportes relevantes, entre otras características que puedan servirle a la investigación.
 - o Hipotético – Deductivo: A partir del estado actual de la gestión de riesgos en los proyectos de desarrollo de software de la empresa y la obtención del estado del arte de este tema, se podrán prever, como resultado de esta investigación, la definición de este proceso para dichos proyectos.
 - o Sistémico: No se puede ver la gestión de riesgos como un proceso aislado, sino como parte del proceso de desarrollo de software y en interacción directa con todos los procesos de la organización en la cual se desarrolla y hacia quién va dirigido el producto que se desea obtener.

- Dialéctico: A través del conocimiento de las relaciones contradictorias esenciales que caracteriza el comportamiento del proceso de gestión de riesgos podremos resolver el problema que dio inicio a la investigación.

Como **Método Empírico General** se utilizó la Observación para observar el conocimiento y estado de la gestión de riesgos en entidades cubanas que pudieran aportar elementos relevantes a la investigación y para observar el desarrollo de los proyectos de software de Softel y comprender, desde afuera, algunas de las causas que pueden estar atentando contra el buen desenvolvimiento de los proyectos. Los **Métodos Empíricos Particulares** que se utilizaron fueron la encuesta y la entrevista. La encuesta se empleó como medio de medir el estado actual de la gestión de riesgos y el nivel de conocimiento sobre el tema en entidades cubanas que desarrollan software, incluyendo Softel. Además, se aplicaron entrevistas apreciativas a Jefes de Grupo, Jefes de Proyecto y Analistas, Programadores y Diseñador Gráfico, pertenecientes a la Factoría de Software de Desarrollo de Software, para recolectar información más detallada sobre el proceso de gestión de riesgos, que puedan aportar a la investigación, así como identificar los riesgos que están afectando a los proyectos de la Factoría de Software y sus causas, y recoger propuestas concretas de acciones para mitigarlos. La aplicación de las encuestas y realización de las entrevistas contribuyeron a determinar los problemas y elaborar el diagnóstico del proceso de gestión de riesgos de los proyectos de desarrollo de software de la empresa y aportaron elementos para el desarrollo del proceso de gestión de riesgos que se obtuvo como resultado de la investigación.

Como **tratamiento estadístico** se utilizó el cálculo porcentual para determinar los por cientos de los indicadores medidos en las entrevistas y encuestas.

Método para evaluar el proceso definido.

Para realizar la evaluación del proceso definido como resultado de la investigación se empleó el método de evaluación de proyectos. Según Urda (1998) existen tres tipos de métodos generales para evaluar proyectos: los métodos cuantitativos basados fundamentalmente en criterios económicos, los métodos multicriterios basados en los aspectos cualitativos evaluados por expertos y la revisión por pares que se basa en que el juicio del mérito lo dan expertos que trabajan la temática mediante consenso. El procedimiento que se utilizó en esta investigación es el método multicriterio. A partir de criterios de expertos se verificó la consistencia en el trabajo, para lo que se utilizó el coeficiente de concordancia de Kendall (W) y el estadígrafo Chi cuadrado (χ^2) (Hernández, 2009). Al ocurrir observaciones ligadas, a cada una de ellas se le

asignó el promedio de los rangos que se le habría asignado si no hubieran ocurrido ligas. El efecto de los rangos ligados es introducir una corrección que incrementa ligeramente el valor de W sobre el obtenido sin corrección, si la proporción de ligas es grande, quedando el coeficiente de concordancia de Kendall de la siguiente manera (Siegel, 1974):

$$W = \frac{S}{\frac{k^2(N^3 - N)}{12} - T}, \text{ donde:}$$

• k = Número de Expertos

• N = Cantidad de criterios

• $T = \frac{\sum t^3 - \sum t}{12}$ = factor de corrección, donde:

- t = número de observaciones en un grupo ligado por un rango dado.
- S indica sumar todos los grupos de ligas dentro de cualquiera de las ordenaciones k .

Para muestras grandes, cuando $N > 7$, la expresión $\chi^2 = k(N-1)W$ está aproximadamente distribuida como chi cuadrado con $gl = N - 1$. Para que exista concordancia en el trabajo de los expertos debe cumplirse que $\chi^2_{real} > \chi^2_{tabla}$ (Siegel, 1974), en cuyo caso, el peso relativo de cada criterio se determina promediando lo que cada Experto le asigna a cada criterio entre 100. Conociendo el peso relativo de cada criterio y la calificación cuantitativa dada por los Expertos a cada criterio en una escala de 1 a 5 (Malo, Cuestionable, Aceptable, Bueno, Excelente) se determina de manera muy rápida un índice de aceptación (IA) del proceso propuesto utilizando la fórmula siguiente (Hernández, 2009):

$$IA = p * c / 5 \text{ donde:}$$

• p : peso relativo de cada criterio

• c : criterio promedio concedido por los Expertos

Si:

• $IA > 0,7$: Alta probabilidad de éxito

• $0,7 > IA > 0,5$: Probabilidad media de éxito

- ? $0,5 > IA > 0,3$: Probabilidad de éxito baja
- ? $0,3 > IA$: Fracaso seguro

2.2 Estado actual de la gestión de riesgos en entidades cubanas.

Para el análisis del estado actual de la gestión de riesgos se realizó un estudio que incluyó a Directivos vinculados a la gestión de proyectos de las 6 entidades del Ministerio de Informática y Comunicaciones (MIC) de Ciudad de la Habana, que producen software. A continuación se describen los resultados del mismo.

2.2.1 Encuestas.

La Población estudiada fueron los Directivos vinculados a la gestión de proyectos de las 6 entidades del Ministerio de Informática y Comunicaciones (MIC) de Ciudad de la Habana, que producen software, con el objetivo de obtener elementos que puedan enriquecer la propuesta del proceso de gestión de riesgos que se propone definir. Se tomó como muestra el 100% de la población y como unidad de estudio los Directivos vinculados a la gestión de proyectos.

Para seleccionar la muestra se aplicó la técnica de muestreo no probabilística e intencional. Se consideró una muestra de 21 individuos donde quedaron representados Directivos vinculados a la gestión de proyectos (Director/Subdirector, Jefe de Grupo, Jefe Proyecto y Analista). En la Figura 2.1 aparece la composición de la muestra seleccionada.

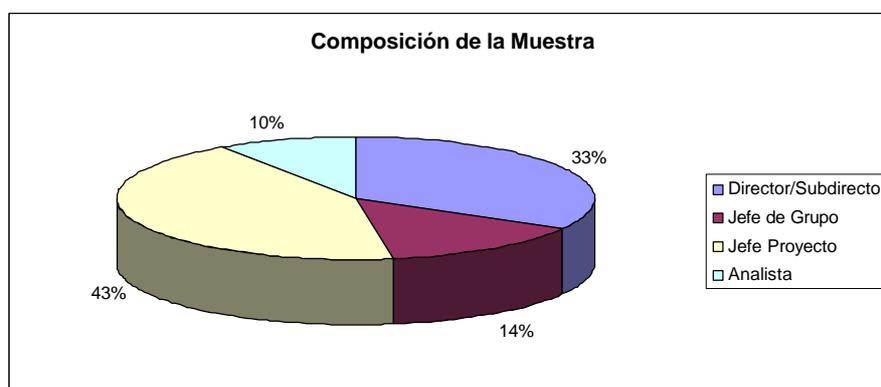


Figura 2.1. Composición cuantitativa de la muestra.

Para elaborar la encuesta se siguió un procedimiento que incluyó la identificación de las variables a evaluar, se operacionalizaron las variables para encontrar los indicadores para evaluarla, se elaboró la encuesta y se realizó un pilotaje para verificar si la misma había sido entendida correctamente. Se incluyeron preguntas cerradas, abiertas, semicerradas, directas, de contenido y de filtro. Finalmente se definió y aplicó el cuestionario que se muestra en el

Anexo 1. Los objetivos que se persiguieron fue conocer:

1. si el encuestado conoce algún marco o proceso para la gestión de riesgos,
2. si se aplica o no algún marco o proceso para la gestión de riesgos en la organización del encuestado y cuál es en el caso de aplicarse y no ser propio de la organización,
3. si se aplica o no algún marco o proceso para la gestión de riesgos en el proyecto del encuestado y cuál es en el caso de aplicarse y no ser propio del proyecto,
4. la frecuencia (Nunca, Algunas veces, Casi siempre, Siempre, No sé) con la que se han realizado en el proyecto algunas de las actividades típicas asociadas a la gestión de riesgos: identificación de riesgos, evaluación de los riesgos, aplicación de planes de mitigación y/o contingencia a los riesgos identificados, monitoreo de los riesgos del proyecto,
5. los principales riesgos que han sido identificados y/o impactado en el proyecto,
6. lo que ha hecho el encuestado en su proyecto, independientemente de utilizar o no un marco formal para la gestión de riesgos, que haya contribuido a evitar impactos negativos.

Los resultados de la encuesta se muestran en la tabla 2.1.

Tabla 2.1. Resultados de las Encuestas.

Id.	Aspecto de la Encuesta	Respuesta			
1	¿Conoce algún marco o proceso para la gestión de riesgos?	52%	Sí	Se mencionaron 16 procesos de gestión de riesgos o que contienen algún aspecto de la gestión de riesgos. Hubo personas que mencionaron más de uno.	
	¿Cuáles?	25%	Resolución 297/03		
		13%	Mapa de riesgos		
		13%	RUP		
6%	PMBok, CMMI, MoGeRi, Pressman, Boehm, McFarlan y el SEI.				
2	¿Se aplica en su organización algún marco o proceso para la gestión de riesgos?	57%	No / No Sé		
		43%	Sí		
			33%	Propio	
			67%	Conocido	83%

					17%	PMBok		
3	¿Se aplica en su proyecto algún proceso para la gestión de riesgos?	52%	No					
		48%	Sí					
			70%	Propio				
			30%	Conocido	67%	Resolución 297/03		
33%	RUP							
4	¿Se han identificado los riesgos en su proyecto?	66.7%	Algunas veces					
		14.3%	Nunca					
		9.5%	Siempre					
		9.5%	Casi Siempre					
5	¿Se han evaluado los riesgos en su proyecto?	57.1%	Algunas veces					
		19.0%	Nunca					
		14.3%	Casi Siempre					
		9.5%	Siempre					
6	¿Se han aplicado planes de mitigación y/o contingencia a los riesgos identificados en su proyecto?	42.9%	Nunca					
		33.3%	Algunas veces					
		9.5%	Siempre					
		9.5%	Casi Siempre					
		4.8%	No Sé					
7	¿Se han monitoreado los riesgos en su proyecto?	42.9%	Nunca					
		38.1%	Algunas veces					
		9.5%	Casi Siempre					
		4.8%	Siempre					
		4.8%	No Sé					

De forma general, se pudo apreciar el poco conocimiento y utilización de la gestión de riesgos tanto a nivel organizacional como en los proyectos de desarrollo de software. También se obtuvo como resultado una lista de 30 riesgos y 37 acciones de mitigación que han impactado en los proyectos en los que participan los encuestados. Para su mejor análisis, estos riesgos fueron agrupados empleando la Taxonomía de Riesgos Ajustada (Maniasi, 2005). Los resultados se muestran en la Figura 2.2.

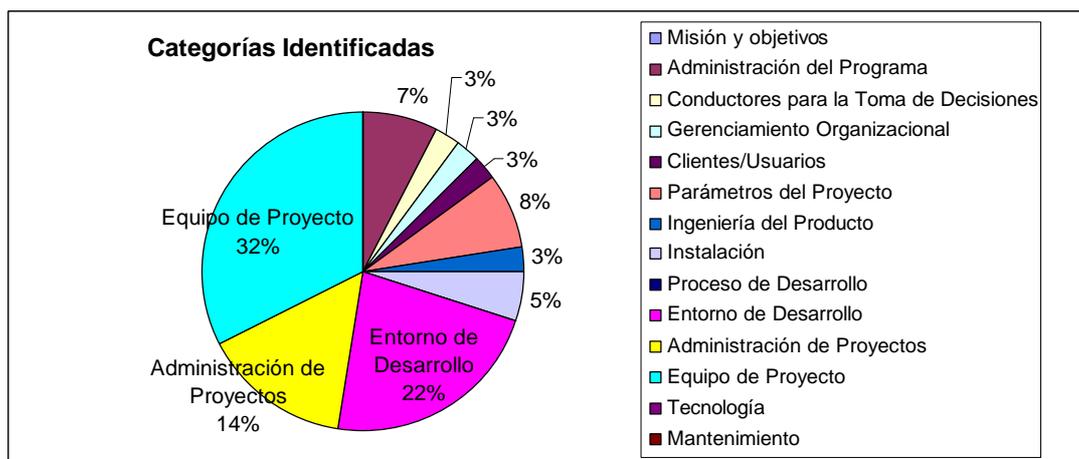


Figura 2.2. Categorías de Riesgo identificadas en las Encuestas.

En la tabla 2.2 se exponen los principales factores de riesgos asociados a las categorías que tuvieron un mayor por ciento de incidencia en las encuestas realizadas.

Tabla 2.2. Principales factores de riesgo que impactaron.

Categoría de Riesgo	Factores de Riesgo que más impactaron
Equipo de Proyecto	Entrenamiento del equipo
	Espíritu y actitud del equipo
	Experiencia con el hardware y software
	Disponibilidad de los miembros del equipo
Entorno de Desarrollo	Recuperación de desastres
	Plataforma de hardware
Administración de Proyectos	Enfoque de administración de proyectos

Conclusiones sobre las Encuestas:

? Sólo el 52% de la muestra conoce algún marco o proceso para la gestión de riesgos y afirman que el más conocido es la Resolución 297/03 del Ministerio de Finanzas Precios (25%). El mismo no ha sido diseñado expresamente para los proyectos de desarrollo de software, aunque se puede emplear como referencia. En segundo lugar se mencionan el Mapa de Riesgos (13%) y RUP (13%). Con menor incidencia, 6%, se mencionan PMBoK, CMMI, MoGeRi, Pressman, Boehm, McFarlan y el SEI, quienes en su mayoría son los que realmente han sido diseñados para proyectos de software.

- ? El 57% de los encuestados afirma que en su organización no se aplica o no sabe si se aplica algún marco o proceso para la gestión de riesgos. En este caso se menciona con mayor peso nuevamente la Resolución 297/03 del Ministerio de Finanzas Precios (83%) y, además, PMBoK (17%).
- ? El 52% de los encuestados afirma que no se aplica en su proyecto ningún marco o proceso para la gestión de riesgos. El 48% restante, indicó que el mayor por ciento es propio del proyecto y no uno ya conocido. En este caso se menciona con mayor peso nuevamente la Resolución 297/03 del Ministerio de Finanzas Precios (67%) y, además, RUP (33%).
- ? Las actividades más significativas asociadas a la gestión de riesgos: identificación, evaluación, planes de mitigación y contingencia y monitoreo de los riesgos no se realizan de forma periódica, a lo sumo algunas veces o nunca.
- ? Las principales categorías de riesgo identificadas en las entrevistas fueron: Equipo de proyecto (32%), Entorno de desarrollo (22%) y Administración de proyectos (14%).

2.3 Estado actual de la gestión de riesgos en los proyectos de desarrollo de software de Softel.

Softel representó el 51% de la muestra seleccionada para las Encuestas, por lo que los resultados anteriores son el reflejo también de la empresa en el tema de la gestión de riesgos. Al extraer de la encuesta aplicada, los datos procedentes de Softel, se obtuvieron los resultados que se muestran en la tabla 2.3.

Tabla 2.3. Resultados de las Encuestas en Softel.

Id.	Aspecto de la Encuesta	Respuesta				
1	¿Conoce algún marco o proceso para la gestión de riesgos?	55%	Sí	Se mencionaron 4 procesos de gestión de riesgos o que contienen algún aspecto de la gestión de riesgos.		
	¿Cuáles?	43%	Resolución 297/03			
		29%	RUP			
		14%	PMBoK y Pressman			
2	¿Se aplica en su organización algún marco o proceso para la gestión de riesgos?	64%	No / No Sé			
		36%	Sí			
			67%	Conocido	75%	Resolución 297/03
					25%	PMBoK
3	¿Se aplica en su proyecto	55%	No			

	algún proceso para la gestión de riesgos?	45%	Sí			
			40%	Propio		
			60%	Conocido	67%	Resolución 297/03
					33%	RUP
4	¿Se han identificado los riesgos en su proyecto?	81.8%	Algunas veces			
		18.2%	Nunca			
		0%	Siempre			
		0%	Casi Siempre			
5	¿Se han evaluado los riesgos en su proyecto?	63.6%	Algunas veces			
		27.3%	Nunca			
		9.1%	Casi Siempre			
		0%	Siempre			
6	¿Se han aplicado planes de mitigación y/o contingencia a los riesgos identificados en su proyecto?	54.5%	Nunca			
		45.5%	Algunas veces			
		0%	Siempre			
		0%	Casi Siempre			
		0%	No Sé			
7	¿Se han monitoreado los riesgos en su proyecto?	54.5%	Nunca			
		45.5%	Algunas veces			
		0%	Casi Siempre			
		0%	Siempre			
		0%	No Sé			

Conclusiones sobre las Encuestas en Softel:

- ? Sólo el 55% de la muestra conoce algún marco o proceso para la gestión de riesgos y afirman que el más conocido es la Resolución 297/03 del Ministerio de Finanzas Precios (43%). En segundo lugar se menciona RUP (29%). Con menor incidencia, 14%, se mencionan PMBoK y Pressman, quienes realmente han sido diseñados para proyectos.
- ? El 64% de los encuestados afirma que en su organización no se aplica o no sabe si se aplica algún marco o proceso para la gestión de riesgos. En este caso se menciona con mayor peso nuevamente la Resolución 297/03 del Ministerio de Finanzas Precios (75%) y, además, PMBoK (25%).
- ? El 55% de los encuestados afirma que no se aplica en su proyecto ningún marco o proceso para la gestión de riesgos. El 45% restante, indicó que el mayor por ciento es uno ya

conocido. En este caso se menciona con mayor peso nuevamente la Resolución 297/03 del Ministerio de Finanzas Precios (67%) y, además, RUP (33%).

- ? Las actividades más significativas asociadas a la gestión de riesgos: identificación, evaluación, planes de mitigación y contingencia y monitoreo de los riesgos no se realizan de forma periódica, a lo sumo algunas veces o nunca.

El estudio se profundizó con la inclusión de entrevistas apreciativas.

2.3.1 Caracterización de la Factoría de Software de Softel.

Recursos Humanos.

- ? Jefe del Grupo: Dirige a la Factoría de Software.
- ? Jefes de Proyecto y Analistas. Los Jefes de Proyecto en casi todos los casos se comportan, además, como Analistas de sistemas, integradores, etc. lo cual elimina tiempo que se debe dedicar a la gestión de los proyectos.
- ? Programadores. Compuesto por algunos técnicos medios con menor preparación para enfrentar la complejidad técnica de las aplicaciones que se desarrollan. El resto es de nivel superior, pero en su mayoría recién graduados o con pocos años de experiencia y llevan menos de un año en la empresa, lo cual ha requerido de esfuerzos en su preparación.
- ? Diseñador gráfico. Responsable del diseño gráfico de las aplicaciones que se desarrollan. Lleva poco tiempo en la empresa.

Caracterización de las aplicaciones.

1. **Mantenimiento de aplicaciones.** Existe un gran número de aplicaciones que se encuentran en fase de mantenimiento: Sistemas heredados y otros desarrollados para arquitectura SOA (orientada a servicios) y basados en componentes, usando software libre.
2. **Nuevos desarrollos.** Emplean, fundamentalmente, arquitectura SOA y GeneXus.

Principales complejidades que enfrenta el desarrollo y mantenimiento de las aplicaciones.

- ? Arquitectura SOA (orientada a servicios) y basada en componentes. Los nuevos desarrollos están basados en esta arquitectura; son aplicaciones grandes y con muchos componentes. No existe mucha experiencia en Cuba en el desarrollo de aplicaciones sobre esta arquitectura y la complejidad de aplicaciones como las que enfrentamos.
- ? Herramientas inteligentes para la generación de código. Se emplea GeneXus como herramienta inteligente para el desarrollo de las aplicaciones, por las ventajas que tiene en la generación de código para varias plataformas, entre otras. Aunque soporta la arquitectura

SOA, no fue diseñada expresamente para este tipo de desarrollo, lo cual lo hace en ocasiones complejo y que no se puedan utilizar a fondo sus potencialidades.

- ? Java como lenguaje para el desarrollo de funcionalidades. Java es el lenguaje que se emplea para combinar con GeneXus y lograr efectos y funcionalidades, fundamentalmente para la Web.
- ? Tecnologías de uso común por muchas aplicaciones para la generación de reportes, sincronización de aplicaciones, etc. La búsqueda, prueba y configuración de herramientas libres con estas posibilidades han sido necesarias para elevar la productividad y dejar establecidas las tecnologías de uso común en la Factoría.
- ? El ambiente de integración y despliegue debe ser estable y organizado, debido a que se desarrollan muchos componentes que deben ser integrados y probados para su liberación.
- ? Se debe lograr una replicación, lo más real posible, del entorno de despliegue en el cliente para lograr que las pruebas que se realizan sean lo más reales posibles, evitando así que surjan problemas una vez liberado el producto de la Factoría.
- ? Muchas aplicaciones y negocios diversos. Los productos que se desarrollan abarcan soluciones para instituciones hospitalarias, bancos de sangre, policlínicos y clínicas de diagnóstico.
- ? El MINSAP como cliente no tiene experiencia en la informatización, lo cual hace que el proceso de levantamiento de requisitos, sobre todo cuando se trata de negocios nuevos en los que la empresa no tiene experiencia, no esté completo o esté poco detallado, dejando espacio a interpretaciones erróneas de lo que el cliente deseaba tener. A veces un mismo requisito escrito es interpretado de forma diferente por varias personas.
- ? Sistemas altamente integrados. El funcionamiento de muchos componentes dependen de otros, lo cual trae aparejado que cambios en uno pueden impactar en otros, que hay componentes que tienen que ser simulados, que debe mantenerse actualizada la matriz de impacto para saber si un cambio en un componente puede impactar en otro.
- ? Adiestramiento del personal en todas las tecnologías que se emplean: Arquitectura SOA, GeneXus, Java, herramientas de software libre asumidas en la empresa para la generación de reportes, sincronización de aplicaciones, etc., conocimiento del negocio de salud y de la dependencia entre sus diversos componentes.
- ? Introducción de un proceso de desarrollo para GeneXus.

2.3.2 Entrevistas.

La Población estudiada fueron los integrantes de la Factoría de Software perteneciente a la Dirección de Desarrollo de Software de Softel, tomando como Unidad de Estudio los integrantes de la Factoría de Software y como Muestra el 70% de la población.

Para seleccionar la muestra se aplicó la técnica de muestreo no probabilística e intencional, tratando de lograr representatividad de los proyectos de desarrollo de software que se realizan en la Factoría de Software. La muestra seleccionada representó el 90% de los proyectos que se realizan en la Factoría. Los proyectos con mayor número de integrantes son “Galen Clínicas” y “Mantenimiento del RIS”. La Figura 2.3 presenta la incidencia de dichos proyectos en la muestra seleccionada. Además, se buscó representatividad de diferentes roles dentro de la Factoría de Software, para obtener mayor riqueza en el estudio y lograr una caracterización lo más completa posible de esta población.

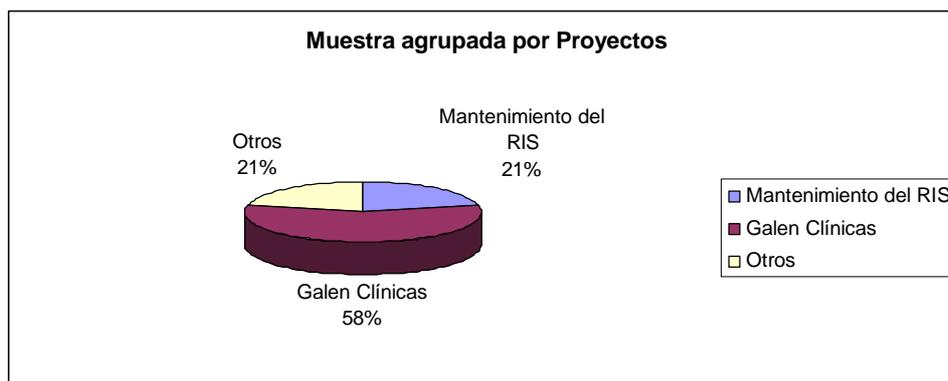


Figura 2.3. Composición de la muestra agrupada por Proyectos.

En la Figura 2.4 aparece una comparación de la población y la muestra seleccionada agrupada por roles. Se incluyó el Jefe del Grupo de la Factoría de Software, su Diseñador Gráfico, el 83% de sus Jefes de Proyecto y Analistas y el 58% de sus Programadores.

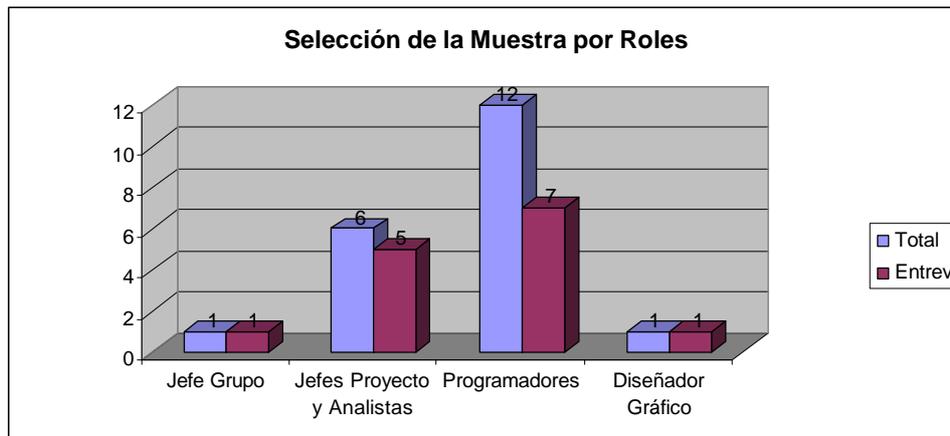


Figura 2.4. Comparación de la muestra con la población agrupada por Roles.

En la Figura 2.5 aparece la composición cuantitativa de la muestra seleccionada teniendo en cuenta lo explicado anteriormente. Como se puede apreciar, los Programadores y Jefes de Proyecto y Analistas tienen un peso importante en la muestra seleccionada, debido a que son los roles que están más presentes en este Grupo de trabajo.

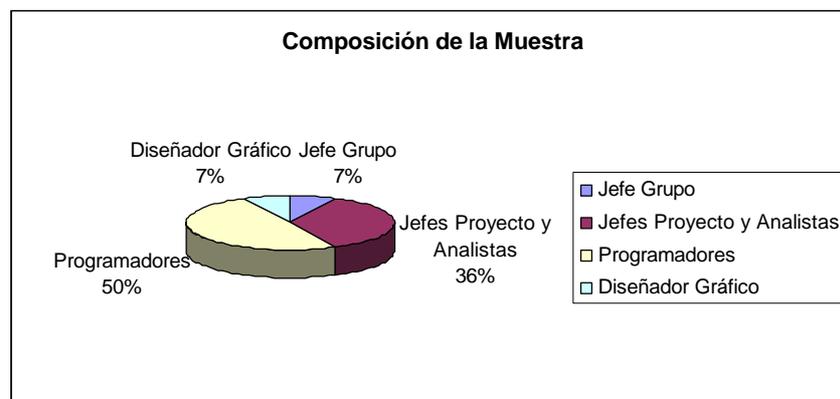


Figura 2.5. Composición Cuantitativa de la muestra.

Para elaborar la Entrevista Apreciativa se consultó la enciclopedia de preguntas positivas y se siguió el procedimiento descrito para hacer este tipo de entrevistas (Whitney, 2002, , 2005). El procedimiento a seguir en este caso indica que una guía de entrevista completa contiene seis partes:

1. Texto introductorio. Prepara el terreno para la entrevista. Incluye información sobre qué estamos haciendo y por qué; importancia de la entrevista apreciativa; la necesidad de compartir historias, detalle y nombres para que otros puedan aprender de las mejores prácticas; cómo se utilizarán las historias y la información.

2. Preguntas de preparación del terreno. Obtienen información del entrevistado.
3. Preguntas tópicas. Preguntas de profundidad acerca de los tópicos afirmativos elegidos. En nuestro caso se elaboraron preguntas concretas sobre los riesgos y su gestión.
4. Preguntas conclusivas. Cierran la entrevista.
5. Hojas de sumario. Para recoger datos de la entrevista.
6. Hojas de acción rápida. Recogen ítems de acción inmediata.

Los componentes claves de una buena entrevista apreciativa se detallan en el Anexo 2. En el Anexo 3 se muestra la entrevista elaborada. El objetivo principal fue identificar los principales riesgos que están presentes en los proyectos de desarrollo de software de Softel, así como las acciones de mitigación que se proponen emplear en cada caso. Debido al poco conocimiento o total desconocimiento por parte de los entrevistados, del concepto de riesgo y su gestión, se incluyeron dichas definiciones en el texto introductorio y fueron explicados durante el desarrollo de la entrevista de acuerdo con las necesidades del entrevistado, para lograr su mejor comprensión.

Los principales resultados fueron los siguientes:

- ? Se identificaron 49 riesgos, con su causa y planes de mitigación.
- ? En las Hojas de acción rápida fue anotado uno de los riesgos identificados para proceder rápidamente a su solución.
- ? Se categorizaron y subcategorizaron los riesgos identificados aplicando la Taxonomía de Riesgos Ajusta de Maniasi (Maniasi, 2005), para ayudar a su análisis. Los riesgos obtenidos, agrupados por categorías, se muestran en la Figura 2.6.

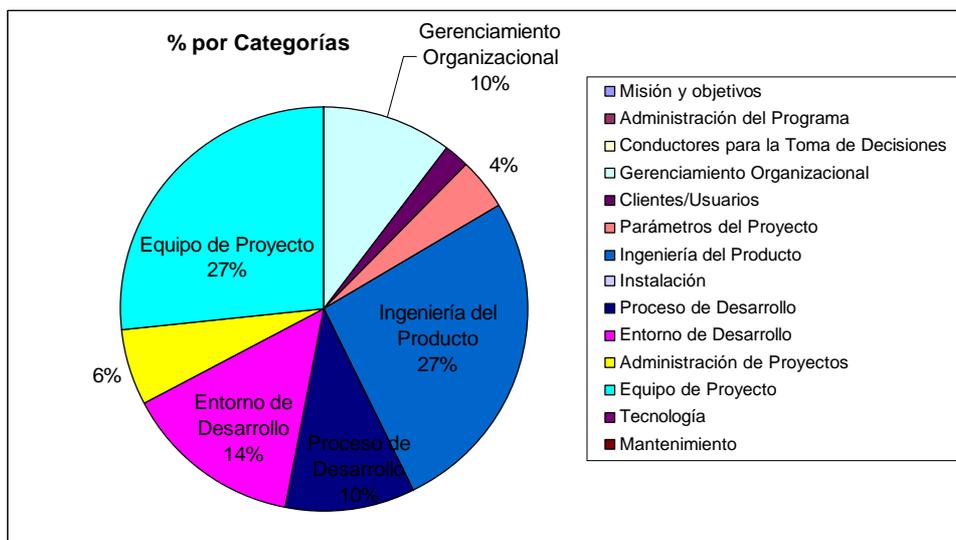


Figura 2.6. Categorías de Riesgo identificadas en las Entrevistas.

En la tabla 2.4 se exponen los principales factores de riesgos asociados a las categorías que tuvieron un mayor por ciento de incidencia en las entrevistas realizadas: Equipo de Proyecto, Ingeniería del Producto, Entorno de Desarrollo, Proceso de Desarrollo y Gerenciamiento Organizacional.

Tabla 2.4. Principales factores de riesgo que impactaron.

Categoría de Riesgo	Factores de Riesgo que más impactaron
Equipo de Proyecto	Combinación de habilidades del equipo
	Experiencia con el dominio de la aplicación
	Entrenamiento del equipo
	Comunicación interna del equipo
Ingeniería del Producto	Requerimientos - Completitud
	Requerimientos - Validez
Entorno de Desarrollo	Disponibilidad de herramientas
	Adecuación del entorno de desarrollo
	Usabilidad
Proceso de Desarrollo	El proceso de desarrollo se adecua al proyecto

Gerenciamiento Organizacional	Soporte de la gerencia
-------------------------------	------------------------

Para precisar aún más el estudio anterior, los riesgos identificados se agruparon también por proyectos de la Factoría de Software. Debido a que los más grandes son “Galen Clínicas” y “Mantenimiento RIS”, se incluyeron estos grupos y el resto de los riesgos fueron agrupados bajo la denominación “Otros”. La Figura 2.7 muestra el por ciento de incidencia de los riesgos identificados en las entrevistas, agrupados por proyectos.

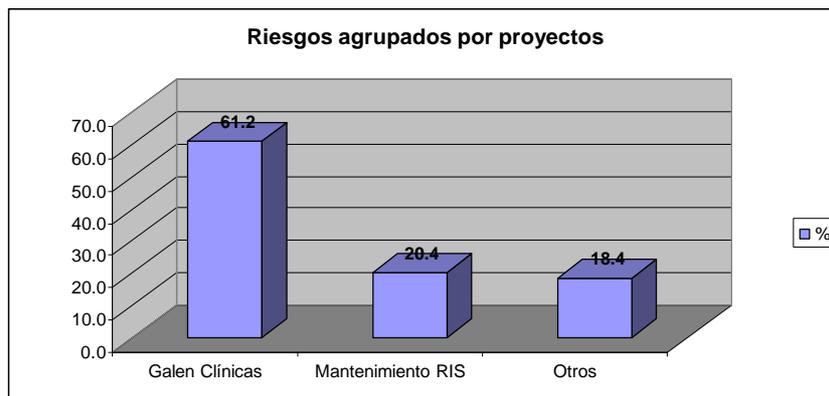


Figura 2.7. Riesgos agrupados por Proyectos.

Las Figura 2.8 muestra las categorías de riesgo identificadas en las entrevistas, pero agrupadas para el proyecto “Galen Clínicas”.

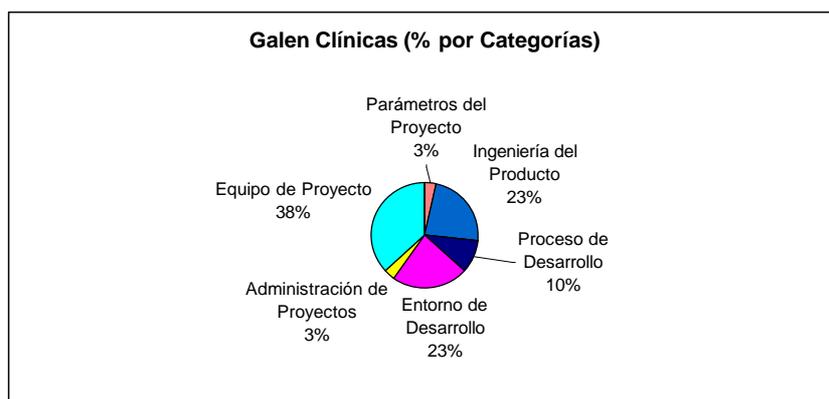


Figura 2.8. Categorías de Riesgo de “Galen Clínicas”.

Las Figura 2.9 muestra las categorías de riesgo identificadas en las entrevistas, pero agrupadas para el proyecto “Mantenimiento RIS”.

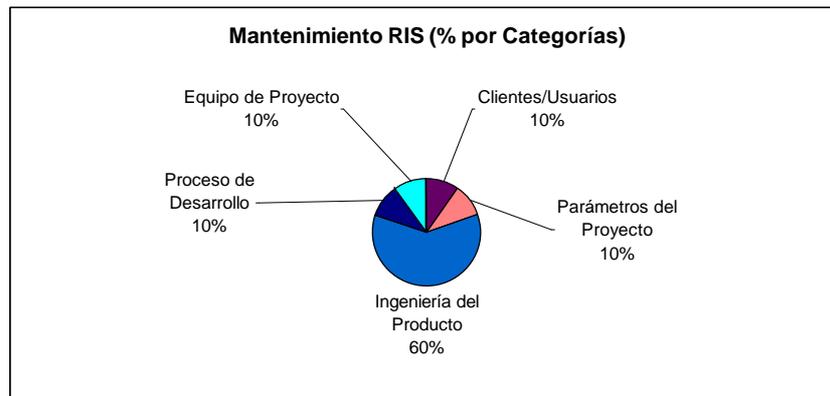


Figura 2.9. Categorías de Riesgo de “Mantenimiento RIS”.

Las Figura 2.10 muestra las categorías de riesgo identificadas en las entrevistas, pero agrupadas para el resto de los proyectos bajo la denominación “Otros”.

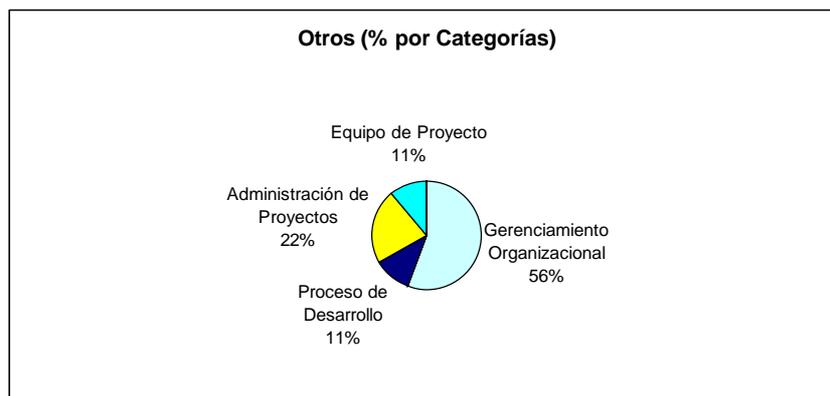


Figura 2.10. Categorías de Riesgo de “Otros”.

Conclusiones sobre las Entrevistas:

- ? Los riesgos identificados pueden servir de base para la identificación de riesgos en cada uno de los proyectos.
- ? Los planes de mitigación propuestos pueden servir de base para la planificación de las respuestas a los riesgos de cada uno de los proyectos.
- ? Existen varios riesgos de causa común que abarcan más de un proyecto en la Factoría, que pueden ser mitigados y hasta eliminados atacando la causa común.
- ? Se recuperaron experiencias importantes que contribuyeron a obtener un conjunto de valores que están presentes en el colectivo y un resumen de buenas prácticas que contribuyeron a obtener éxitos y/o experiencias importantes en las historias narradas, por lo

que son oportunidades que se pueden aprovechar en función de mejorar los resultados que se desean.

- ? Hay valores compartidos muy importantes en los miembros de la Factoría, lo cual indica que hay condiciones propicias para lograr la mejora y que se pueden producir cambios de forma rápida.
- ? Los miembros de la Factoría están identificados con su proyecto y con la empresa, se sienten parte.
- ? Los miembros de un mismo equipo logran una coincidencia importante en los riesgos que identifican. Sin embargo, la percepción de Analistas y Programadores tiene matices diferentes que permitieron obtener la información de manera más precisa y profunda.
- ? Las principales categorías de riesgo identificadas en las entrevistas fueron: Equipo de proyecto (27%), Ingeniería del Producto (27%) y Entorno de Desarrollo (14%). Le siguen el Proceso de Desarrollo (10%) y el Gerenciamiento Organizacional (10%).
- ? La mayor cantidad de riesgos identificados proceden del proyecto “Galen Clínicas”, con un 61.2% de incidencia.
- ? Las principales categorías de riesgo identificadas en las entrevistas para el proyecto “Galen Clínicas” fueron: Equipo de proyecto (38%), Ingeniería del Producto (23%), Entorno de Desarrollo (23%) y Proceso de Desarrollo (10%).
- ? La principal categoría de riesgo identificada en las entrevistas para el proyecto “Mantenimiento RIS” fue Ingeniería del Producto (60%). Le siguen con igual incidencia del 10%: Equipo de proyecto, Proceso de Desarrollo, Clientes/Usuarios y Parámetros del Proyecto.
- ? Las principales categorías de riesgo identificadas en las entrevistas para el resto de los proyectos, bajo la denominación “Otros” fue Gerenciamiento Organizacional (56%), Administración de Proyectos (22%). Le siguen con igual incidencia del 11%: Equipo de proyecto y Proceso de Desarrollo.

Conclusiones parciales.

1. Con el resultado de las encuestas y entrevistas se pudo demostrar que no existe un proceso formal ni se realiza adecuadamente la gestión de riesgos en los proyectos de desarrollo de software de la empresa, lo cual afecta la gestión de los proyectos de software. Las actividades de identificación, evaluación, planificación de respuestas a los riesgos y monitoreo y control de los mismos se realizan algunas veces o nunca.

2. Las Entrevistas Apreciativas permitieron rescatar historias de experiencias vividas por los miembros de la Factoría de Software, así como muchos de los valores presentes en este equipo. Se apreció motivación, compromiso y espíritu y confianza en la mejora. Se obtuvieron buenas prácticas que pueden ser aplicadas en los proyectos para mejorar la gestión de riesgos. Todo ello contribuyó a preparar las condiciones para la implantación del proceso definido en la Factoría de Software.

Capítulo III. Definición del Proceso para la gestión de riesgos y evaluación del proceso.***Introducción.***

En este capítulo se define el proceso para la Gestión de Riesgos de los proyectos de desarrollo de software de Softel, para lo cual se determina los elementos tomados de los marcos de gestión de riesgos analizados en el Capítulo I. Además, se exponen las actividades de preparación realizadas en la empresa, las cuales no se circunscribieron solamente a la Factoría de Software, para elevar la cultura sobre riesgos y su gestión y preparar a la organización en el proceso definido como resultado del Capítulo II. Se realiza la evaluación teórica del mismo empleando el método de expertos con el objetivo de determinar si el proceso garantiza una adecuada gestión de los proyectos de software de Softel, entre otras contribuciones. Al final del capítulo se resumen algunos resultados que se han obtenido en los proyectos de la Factoría de Software de Softel.

3.1 Proceso de gestión de riesgos para los proyectos de desarrollo de software de Softel.***3.1.1. Elementos tenidos en cuenta para la obtención del proceso.***

Como se indicó en el Capítulo I, para la propuesta del Proceso de Gestión de Riesgos para los proyectos de desarrollo de software de Softel, se decidió hacer una adecuación del Área de Conocimiento de Gestión de los Riesgos del Proyecto de la metodología PMBoK. Se asumen los siguientes conceptos de riesgo y gestión de riesgo:

Riesgo: Es la probabilidad de incurrir en una pérdida o sufrir un impacto negativo. Es sólo una posibilidad, no la certeza de una pérdida ni un resultado por debajo de lo esperado. También es la probabilidad de aprovechar una oportunidad y obtener un impacto positivo.

Gestión de Riesgos: Incluye los procesos relacionados a la planificación de la gestión de riesgos, identificación, análisis, respuestas y seguimiento y control en un proyecto. Los objetivos son incrementar la probabilidad y el impacto de los eventos positivos y disminuir la probabilidad y el impacto de los eventos adversos al proyecto.

Para la propuesta de Proceso de Gestión de Riesgos se asumen los procesos de PMBoK (PMI, 2004): Planificación de la Gestión de Riesgos, Identificación de Riesgos, Planificación de la Respuesta a los Riesgos y Seguimiento y Control de los Riesgos. Se incorpora el proceso Análisis Cualitativo de Riesgos de PMBoK como Análisis de Riesgos. Debido al poco grado de madurez de la gestión de riesgos en la empresa, al desconocimiento y poca experiencia del

proceso y de las herramientas y técnicas que se pueden emplear, sobre todo en el Análisis Cuantitativo de Riesgos y a la no existencia de datos históricos que puedan utilizarse para realizar dicha cuantificación, se decidió tomar solamente el Análisis Cualitativo de los riesgos de PMBoK, con el cual se logrará un impacto significativo con relación al nivel de madurez actual. En la medida en que se continúe aplicando el proceso que se propone y que se vaya ganando en experiencia, madurez e información histórica, se podrán incorporar gradualmente los elementos cuantitativos del análisis de riesgos propuestos por PMBoK.

A continuación se describen los elementos incorporados a los procesos asumidos de PMBoK para la definición de cada actividad del Proceso de Gestión de Riesgos que se propone como resultado de la investigación:

1. Planificación de la Gestión de Riesgos.

- ? **Salida: Plan de Gestión de Riesgos (DG-32.01):** PMBoK no propone una plantilla para la formalización de este documento que se obtiene como salida de este proceso. Entonces, a partir de lo descrito por PMBoK se incluye, en el proceso propuesto, una plantilla para la formalización del Plan de Gestión de Riesgos (DG-32.01), la cual se muestra en el Anexo 4. La misma facilita la obtención rápida del documento y proporciona una guía al autor con texto preelaborado. Incluye la Metodología a seguir; al menos los Roles y Responsabilidades que deben existir en el proyecto; una propuesta de periodicidad de realización del proceso de gestión de riesgos con facilidades para ajustarlo; la Estructura de Desglose de Riesgo (EDR) propuesta por PMBoK e incorpora también la Taxonomía Ajustada de Riesgos propuesta por Maniasi (Maniasi, 2005) para los proyectos de desarrollo de software (con fichero Excel adjunto que incluye la taxonomía con sus 114 factores de riesgo agrupados por categorías y subcategorías); las definiciones de probabilidad e impacto que se proponen para los proyectos, las cuales fueron enriquecidas al combinar lo planteado por PMBoK con lo propuesto por Pérez Villaseñor (Pérez, 2007), donde plantea que se deben evitar las escalas de 3 valores (Bajo, Medio, Alto) por la tendencia de seleccionar el valor medio, lo cual complica la discriminación de los riesgos; la matriz de probabilidad e impacto con su interpretación de magnitud e importancia y la acción de respuesta que corresponde en cada caso; el formato a seguir para el Registro de Riesgos y cómo se documentarán los resultados; así como la descripción de cómo se realizará el seguimiento al proceso.
- ? **Salida: Publicar el Plan de gestión de riesgos.** No aparece explícitamente como una salida del proceso, por lo que se incluye explícitamente como una salida del proceso

definido, para indicar que el Plan de Gestión de Riesgos (DG-32.01) obtenido debe ser publicado en la carpeta creada para tal efecto, con vistas a que el mismo pueda ser conocido por otros proyectos y por la empresa y, a su vez, servir como ejemplo o plantilla.

2. Identificación de los Riesgos.

- ? **Técnicas de Recopilación de Información.** Se incluye la Entrevista Apreciativa (Whitney, 2002) presentada como una modalidad de Entrevista que no busca sólo los datos, sino también las experiencias y relaciones. La misma fue aplicada como técnica en la investigación con resultados muy positivos. Se adiciona también la Técnica de Grupo Nominal, propuesta por Pérez Villaseñor (Pérez, 2007), la cual puede ser fácil de aplicar en los proyectos de la empresa. Se enriquece la Técnica de Tormenta de Ideas con algunos elementos extraídos de Maniasi (Maniasi, 2005).
 - ? **Salida: Registro de Riesgos (DG-32.02):** PMBoK no propone una plantilla para la formalización de este documento que se obtiene como salida de este proceso ni es muy rico en detallar la información exacta que se debe registrar. Entonces, a partir de lo descrito por PMBoK se incluye una plantilla para la formalización del Registro de Riesgos (DG-32.02), la cual se muestra en el Anexo 5. La misma facilita la obtención más cómoda del documento y proporciona una guía al autor con texto preelaborado. Incluye todos los aspectos que se van enriqueciendo durante el proceso y en cada actividad se especifica lo que se incorpora y/o actualiza. Además, para obtener la plantilla Registro de Riesgos, se tomaron algunos elementos de la plantilla Lista de Riesgos establecida en la Dirección de Desarrollo, de formatos que se han establecido como resultado del componente de Evaluación de Riesgos de la resolución 297/03 del MFP, de algunos elementos aportados por Pérez Villaseñor (Pérez, 2007) relacionados con la información del riesgo y se enriqueció con algunos aportes resultantes de la experiencia de la investigadora en la definición y puesta en marcha de algunos procedimientos de la empresa.
 - ? **Salida: Publicar el Registro de riesgos.** No aparece explícitamente como una salida del proceso de PMBoK, por lo que se incluye explícitamente como una salida del proceso propuesto, para indicar que el Registro de Riesgos (DG-32.02) obtenido debe ser publicado en la carpeta creada para tal efecto, con vistas a que el mismo pueda ser conocido por otros proyectos y por la empresa y, a su vez, servir como ejemplo o plantilla.
- ## 3. Análisis de Riesgos.
- Se define a partir del proceso Análisis Cualitativo de Riesgos de PMBoK.

- ? **Herramienta: Evaluación de Probabilidad e Impacto de los Riesgos.** Se enriquece con dos métodos: Método Promedio y Método de Expertos, aportados por Pérez Villaseñor (Pérez, 2007).
- ? **Herramienta: Matriz de Probabilidad e Impacto.** Se complementa con el método aportado por Pérez Villaseñor (Pérez, 2007).
- ? **Salida: Registro de Riesgos (DG-32.02):** Al igual que en los anteriores, se actualiza esta plantilla de acuerdo a lo que señala PMBoK como resultado de esta actividad, pero PMBoK no define exactamente la información que se registra en cada salida. Por ello fue necesario diseñar cada una de ellas (tablas con columnas específicas) y se incluyó la actualización de la caracterización de los riesgos de acuerdo a los nuevos elementos que se aportan en esta etapa (Anexo 5).
- ? **Salida: Publicar el Registro de riesgos.** No aparece explícitamente como una salida del proceso de PMBoK, por lo que se incluye explícitamente como una salida del proceso propuesto, para indicar que el Plan de Gestión de Riesgos (DG-32.01) obtenido debe ser publicado en la carpeta creada para tal efecto, con vistas a que el mismo pueda ser conocido por otros proyectos y por la empresa y, a su vez, servir como ejemplo o plantilla.

4. Planificación de Respuestas a los Riesgos.

- ? **Salida: Registro de Riesgos (DG-32.02):** Al igual que en los anteriores, se actualiza esta plantilla de acuerdo a lo que señala PMBoK como resultado de esta actividad, pero PMBoK no define exactamente la información que se registra en cada salida. Por ello fue necesario diseñar cada una de ellas (tablas con columnas específicas) y se incluyó la actualización de la caracterización de los riesgos de acuerdo a los nuevos elementos que se aportan en esta etapa (Anexo 5).
- ? **Salida: Publicar el Registro de riesgos.** No aparece explícitamente como una salida del proceso de PMBoK, por lo que se incluye explícitamente como una salida del proceso propuesto, para indicar que el Plan de Gestión de Riesgos (DG-32.01) obtenido debe ser publicado en la carpeta creada para tal efecto, con vistas a que el mismo pueda ser conocido por otros proyectos y por la empresa y, a su vez, servir como ejemplo o plantilla.

5. Seguimiento y Control de los Riesgos.

- ? **Entradas:** No se incluyen los Informes de Rendimiento de PMBoK, ya que la Entrada Información sobre el Rendimiento del Trabajo contiene información suficiente para esta actividad.

-
- ? **Herramientas y Técnicas:** No se incluyen las siguientes herramientas y técnicas de PMBoK: Análisis de Variación y de Tendencias, Medición del Rendimiento Técnico y Análisis de Reserva debido a que el nivel de madurez de la gestión de los proyectos de la empresa no tiene en cuenta estos aspectos.
 - ? **Salida: Registro de Riesgos (DG-32.02):** Al igual que en los anteriores, se actualiza esta plantilla de acuerdo a lo que señala PMBoK como resultado de esta actividad que, en este caso, incluye mucha información resultante que puede ser de gran utilidad para proyectos futuros (Anexo 5).
 - ? **Salida:** No se incluyen las siguientes salidas de PMBoK por estar muy atadas a otras áreas de conocimiento de PMBoK que no están contenidas en el alcance del proceso definido: Acciones correctivas recomendadas y Acciones Preventivas Recomendadas.
 - ? **Salida: Publicar los Activos de los Procesos de la Organización actualizados.** No aparece explícitamente como una salida del proceso de PMBoK, por lo que se incluye explícitamente como una salida del proceso propuesto, para publicar todos los Activos de los Procesos de la Organización que fueron actualizados en esta actividad, incluyendo el Registro de Riesgos (DG-32.02), con vistas a que puedan ser conocidos por otros proyectos y por la empresa y, a su vez, servir como ejemplos o plantillas.

6. Comunicación.

- ? No aparece explícitamente definido en PMBoK, aunque existen elementos de la comunicación que están implícitos en la definición de los diferentes pasos del proceso y en la inclusión de participantes de otros proyectos, áreas de la empresa o de fuera de ésta.
- ? Se tomaron elementos del Programa de gestión de riesgos del SEI (Higuera, 1996) para describir el alcance de esta actividad. Se incluyeron acciones y buenas prácticas extraídas del SEI, de *Microsoft Solution Frameworks (MSF)* (Microsoft, 2002) y de *Boehm* (Boehm, 1991). Este último con la publicación de los diez elementos de riesgo más frecuentes.

El proceso de gestión de riesgos definido, se puede enmarcar en la Generación Taxonómica (G2) pero con un enfoque más proactivo y menos reactivo, pues existe experiencia en la empresa en el desarrollo de los tipos de proyectos que enfrenta y los mismos no son considerados de alto riesgo, por lo que se pueden obtener resultados más predecibles. Debido a que todavía hay inmadurez en la gestión de los proyectos de desarrollo de software de Softel

no podemos enmarcarlo en la Generación Causal (G3), donde se aspira a la gestión del proyecto por sus riesgos.

Con la implantación del proceso y la madurez que vaya alcanzando el mismo, se podrá elevar la gestión de riesgos en los proyectos e incluir el Análisis Cuantitativo de Riesgos de PMBoK.

3.1.2. Proceso de Gestión de Riesgos.

La Figura 3.1 muestra el proceso de gestión de riesgos definido para los proyectos de desarrollo de software de Softel (Valladares, 2010c).

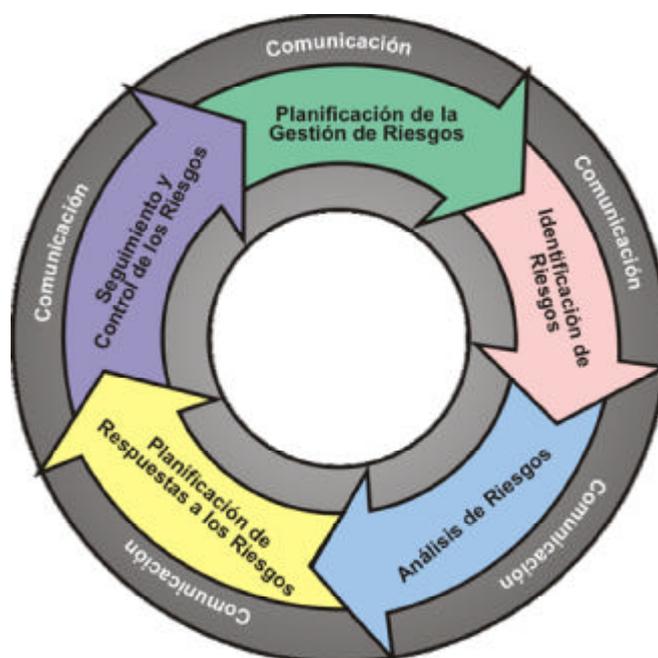


Figura 3.1. Proceso de Gestión de Riesgos.

Para su definición, se siguió la plantilla definida en Softel para estos fines (Martínez, 2007).

Proceso: Gestión de Riesgos para los proyectos de Softel
Objetivos: <ul style="list-style-type: none"> ? Gestionar los riesgos de forma continua y proactiva, desde el inicio del proyecto y durante todo su ciclo de vida. ? Aumentar la probabilidad y el impacto de los eventos positivos, y disminuir la probabilidad y el impacto de los eventos adversos para el proyecto.
Responsable: Gestor de Riesgos

Ejecutor (es): Gestor de Riesgos, Jefe de Proyecto, Equipo de Gestión de Riesgos (si se define), miembros del equipo de proyecto, interesados en el proyecto seleccionados, miembros de la organización con la responsabilidad de gestionar la planificación y ejecución de riesgos, otras personas según sea necesario.

Descripción del proceso.

El proceso de Gestión de los Riesgos del Proyecto está compuesto por un conjunto de actividades que interactúan entre sí y también con el resto de los procesos que intervienen en el desarrollo de los proyectos. Cada actividad puede implicar el esfuerzo de una o más personas o grupos de personas, dependiendo de las necesidades del proyecto. Cada actividad tiene lugar por lo menos una vez en cada proyecto y se realiza en una o más fases del proyecto, si el proyecto se encuentra dividido en fases. Las actividades son:

1. **Planificación de la Gestión de Riesgos:** decidir cómo enfocar, planificar y ejecutar las actividades de gestión de riesgos para un proyecto.
2. **Identificación de Riesgos:** determinar qué riesgos pueden afectar al proyecto y documentar sus características.
3. **Análisis de Riesgos:** priorizar los riesgos para realizar otros análisis o acciones posteriores, evaluando y combinando su probabilidad de ocurrencia y su impacto.
4. **Planificación de la Respuesta a los Riesgos:** desarrollar opciones y acciones para mejorar las oportunidades y reducir las amenazas a los objetivos del proyecto.
5. **Seguimiento y Control de los Riesgos:** realizar el seguimiento de los riesgos identificados, supervisar los riesgos residuales, identificar nuevos riesgos, ejecutar planes de respuesta a los riesgos y evaluar su efectividad a lo largo del ciclo de vida del proyecto.
6. **Comunicación:** Se encuentra presente durante todo el Proceso de Gestión de Riesgos. Sin una comunicación eficaz, la gestión de riesgos no puede ser viable.

Resumen de las actividades necesarias para el proceso Gestión de Riesgos para los proyectos de Softel.

Actividad: Planificación de la Gestión de Riesgos.

Propósito:

Decidir cómo enfocar, planificar y ejecutar las actividades de gestión de riesgos para un proyecto. Debe completarse en las fases tempranas de la planificación del proyecto, dado que

es crucial para realizar con éxito las demás actividades asociadas a la gestión de riesgos.

Tareas:

1. Recopilar las fuentes de información, útiles y necesarias, para la Planificación de la gestión de riesgos del proyecto, es decir, las entradas a esta actividad.
2. Organizar y realizar las reuniones de análisis y planificación para obtener el Plan de Gestión de riesgos del proyecto (DG-32.01) (Anexo 4) como resultado de:
 - a. Definir los métodos, las herramientas y las fuentes de información que pueden utilizarse para realizar la gestión de riesgos en el proyecto.
 - b. Definir el líder, el apoyo y los miembros del equipo de gestión de riesgos para cada tipo de actividad del Plan de Gestión de Riesgos, asigna personas a estos roles y explica sus responsabilidades.
 - c. Identificar las necesidades de capacitación de los miembros del proyecto para llevar a cabo la gestión de los riesgos. Incluye el conocimiento que debe tener cada cual sobre el proceso de acuerdo a su rol y la capacitación sobre las herramientas y técnicas que se emplearán durante el proceso.
 - d. Definir cuándo y con qué frecuencia se realizará el proceso de gestión de riesgos durante el ciclo de vida del proyecto, y establecer las actividades de gestión de riesgos que se incluirán en el cronograma del proyecto.
 - e. Determinar el método a seguir para la identificación sistemática de riesgos y las Categorías de riesgo del proyecto: Taxonomías, Estructuras de Desglose de Riesgos u otras.
 - f. Definir los niveles de probabilidad de ocurrencia e impacto sobre los objetivos del proyecto.
 - g. Determinar el método a seguir para priorizar los riesgos según sus implicaciones para lograr los objetivos del proyecto.
 - h. Describir el formato de informe a utilizar para registrar los riesgos, así como cualquier otro que se considere necesario.
 - i. Definir cómo se documentarán, analizarán y comunicarán los resultados de las actividades de gestión de riesgos.
 - j. Documentar cómo se llevará a cabo el seguimiento: cómo todas las facetas de las actividades de riesgo serán registradas para beneficio del proyecto actual, para futuras necesidades y para las lecciones aprendidas; si serán auditadas las actividades de gestión de riesgos y cómo se realizará dicha auditoría.

3. Publicar el Plan de Gestión de Riesgos (DG-32.01) obtenido.
Entradas: <ol style="list-style-type: none"> 1. Factores ambientales de la organización. 2. Activos de los procesos de la organización. 3. Enunciado del alcance del proyecto. 4. Plan de gestión del proyecto.
Herramientas y Técnicas: <ol style="list-style-type: none"> 1. Reuniones y análisis de planificación.
Salidas: <ol style="list-style-type: none"> 1. Plan de gestión de riesgos (DG-32.01). 2. Publicar el Plan de Gestión de riesgos (DG-32.01).
Responsable: Gestor de Riesgos
Participantes: Gestor de Riesgos del proyecto, Jefe del proyecto, miembros del equipo del proyecto, interesados en el proyecto que sean seleccionados, miembros de la organización con la responsabilidad de gestionar la planificación y ejecución de riesgos, otras personas según sea necesario.

Actividad: Identificación de Riesgos.
Propósito: Determinar qué riesgos pueden afectar al proyecto y documentar sus características.
Tareas: <ol style="list-style-type: none"> 1. Recopilar las fuentes de información, útiles y necesarias, para la identificación de los riesgos del proyecto, es decir, las entradas a esta actividad. 2. Aplicar las herramientas y técnicas planificadas en el Plan de Gestión de Riesgos (DG-32.01) para identificar los riesgos del proyecto. 3. Inicializar o actualizar en el Registro de Riesgos (DG-32.02) la siguiente información (Anexo 5): <ol style="list-style-type: none"> a. Lista de riesgos identificados. Utilizar la tabla “Lista de prioridades o clasificaciones relativas de los riesgos del proyecto” aunque todavía los riesgos no se ordenen por

prioridades.

- b. Caracterización de los riesgos: Identificador del riesgo, Nombre del riesgo, Descripción del riesgo, Categoría del riesgo, Fecha de detección, Causa y efecto, Fechas en que puede afectar, Indicadores y disparadores y lista de posibles respuestas, que pueden ser útiles como entradas a la actividad Planificación de Respuestas a los riesgos.

4. Actualizar las categorías de riesgo si fuese necesario.
5. Publicar el Registro de Riesgos (DG-32.02) como resultado de esta actividad.

Entradas:

1. Factores ambientales de la organización.
2. Activos de los procesos de la organización.
3. Enunciado del alcance del proyecto.
4. Plan de gestión del proyecto.
5. Plan de gestión de riesgos (DG-32.01).

Herramientas y Técnicas:

1. Revisiones de documentación.
2. Técnicas de recopilación de información (Tormenta de ideas, Entrevistas, Técnica Delphi (Astigarraga, 2008), Análisis DAFO, etc.).
3. Análisis de lista de chequeo
4. Análisis de asunciones
5. Técnicas de diagramación

Salidas:

1. Registro de riesgos (DG-32.02).
2. Publicar el Registro de riesgos (DG-32.02).

Responsable: Gestor de Riesgos

Participantes:

Gestor de Riesgos del proyecto, Jefe del proyecto, miembros del equipo del proyecto, equipo de gestión de riesgos (si se asigna uno), expertos en la materia ajenos al equipo del proyecto, clientes, usuarios finales, otros Jefes de proyectos, interesados y expertos en gestión de riesgos.

El éxito depende de la participación conjunta para la generación de ideas en base a la

combinación de experiencias y opiniones.

Actividad: Análisis de Riesgos.

Propósito:

Priorizar los riesgos para realizar otros análisis o acciones posteriores, evaluando y combinando su probabilidad de ocurrencia y su impacto.

Tareas:

1. Recopilar las fuentes de información, útiles y necesarias, para el análisis de los riesgos del proyecto, es decir, las entradas a esta actividad.
2. Evaluar la probabilidad de ocurrencia e impacto asociado de cada riesgo del proyecto, de acuerdo a los valores definidos en el Plan de gestión de riesgos (DG-32.01).
3. Aplicar el método definido en el Plan de gestión de riesgos (DG-32.01) para priorizar los riesgos según sus implicaciones para lograr los objetivos del proyecto.
4. Determinar los riesgos que irán a la lista de supervisión de riesgos de baja prioridad.
5. Actualizar en el Registro de Riesgos (DG-32.02) la siguiente información (Anexo 5):
 - a. Lista de prioridades o clasificaciones relativas de los riesgos del proyecto. Resultado de la tarea 3.
 - b. Lista de Riesgos agrupados por categorías. Igual al listado anterior, pero ordenados por Categoría de riesgo.
 - c. Lista de riesgos que requieren respuesta a corto plazo. Se indica en la columna ¿Respuesta a corto plazo? de la tabla “Lista de riesgos agrupados por categorías”.
 - d. Lista de riesgos que requieren análisis y respuesta adicionales. Se indica en la columna ¿Análisis y respuesta adicionales? de la tabla “Lista de riesgos agrupados por categorías”.
 - e. Caracterización de los riesgos. Actualizar y completar Magnitud del Riesgo, Probabilidad de ocurrencia e Impacto.
 - f. Lista de supervisión de riesgos de baja prioridad.
6. Publicar el Registro de Riesgos (DG-32.02) actualizado como resultado de esta actividad.

Entradas:

1. Activos de los procesos de la organización.
2. Enunciado del alcance del proyecto.

<ol style="list-style-type: none"> 3. Plan de gestión de riesgos (DG-32.01). 4. Registro de Riesgos (DG-32.02).
<p>Herramientas y Técnicas:</p> <ol style="list-style-type: none"> 1. Evaluación de probabilidad e impacto de los riesgos. 2. Matriz de probabilidad e impacto. 3. Evaluación de la calidad de los datos sobre riesgos. 4. Categorización de los riesgos. 5. Evaluación de la urgencia del riesgo.
<p>Salidas:</p> <ol style="list-style-type: none"> 1. Registro de riesgos (DG-32.02) actualizado. 2. Publicar el Registro de riesgos (DG-32.02) actualizado.
<p>Responsable: Gestor de Riesgos</p>
<p>Participantes:</p> <p>Gestor de Riesgos del proyecto, Jefe del proyecto, miembros del equipo del proyecto, equipo de gestión de riesgos (si se asigna uno), expertos o familiarizados con las categorías de riesgo a evaluar, expertos ajenos al proyecto.</p>

<p>Actividad: Planificación de la Respuesta a los Riesgos.</p>
<p>Propósito:</p> <p>Desarrollar opciones y acciones para mejorar las oportunidades y reducir las amenazas a los objetivos del proyecto.</p>
<p>Tareas:</p> <ol style="list-style-type: none"> 1. Acordar la estrategia de respuesta para los riesgos identificados en el Registro de Riesgos (DG-32.02) (Anexo 5) de acuerdo a lo especificado en el Plan de gestión de riesgos (DG-32.01), priorizando los riesgos de mayor exposición. También se pueden agrupar los riesgos por su causa y seleccionar las causas que generen el mayor número de riesgos. Las estrategias de respuesta pueden ser: <ol style="list-style-type: none"> a. Riesgos negativos o amenazas: Evitar, Transferir, Mitigar, Aceptar b. Riesgos positivos u oportunidades: Explotar, Compartir, Mejorar, Aceptar 2. Definir las acciones concretar para cumplir con la estrategia de respuesta acordada. En el caso de los riesgos negativos o amenazas, obtener el plan de Mitigación y el de

Contingencia, si procede.

3. Asignar propietarios a los riesgos y definir sus responsabilidades.
4. Actualizar la lista de supervisión de riesgos de baja prioridad con los riesgos residuales que se espera que queden después de haber implementado las respuestas planificadas, así como los que han sido deliberadamente aceptados y los riesgos secundarios que surgen como resultado directo de la implementación de una respuesta a los riesgos.
5. Realizar los acuerdos contractuales como acuerdos por seguros, servicios y otros temas, según corresponda, para especificar la responsabilidad de cada parte en cuanto a los riesgos específicos, en caso de que ocurran.
6. Actualizar en el Registro de Riesgos (DG-32.02) la siguiente información resultante de haber ejecutado las tareas de esta actividad (Anexo 5):
 - a. Lista de prioridades o clasificaciones relativas de los riesgos del proyecto. Resultado de la actividad “Evaluación de Riesgos”.
 - b. Lista de Riesgos agrupados por categorías. Resultado de la actividad “Evaluación de Riesgos”.
 - c. Caracterización de los riesgos. Actualizar y completar Propietario del riesgo y responsabilidades, Estrategia de respuesta acordada, Indicadores y Disparadores y acciones específicas para implementar la estrategia de respuesta elegida.
 - d. Plan de acción para implementar las estrategias de respuesta: Acciones propuestas, Responsable, Ejecutantes y Fecha de cumplimiento.
 - e. Lista de supervisión de riesgos de baja prioridad. Riesgos residuales (después de implementar respuestas planificadas, deliberadamente aceptados) y secundarios.
7. Actualizar el Plan de gestión del proyecto con las tareas identificadas en el “Plan de acción para implementar las estrategias de respuesta”, del Registro de Riesgos (DG-32.02).
8. Publicar el Registro de Riesgos (DG-32.02) actualizado como resultado de esta actividad.

Entradas:

1. Plan de gestión de riesgos (DG-32.01).
2. Registro de Riesgos (DG-32.02).

Herramientas y Técnicas:

1. Estrategias para riesgos negativos o amenazas.
2. Estrategias para riesgos positivos u oportunidades.

3. Estrategia común ante amenazas y oportunidades.
4. Estrategia de respuesta para contingencias.

Salidas:

1. Registro de riesgos (DG-32.02) actualizado.
2. Plan de gestión del proyecto (actualizado).
3. Acuerdos contractuales relacionados con el riesgo.
4. Publicar el Registro de riesgos (DG-32.02) actualizado.

Responsable: Gestor de Riesgos

Participantes:

Gestor de Riesgos del proyecto, Jefe del proyecto, miembros del equipo del proyecto, equipo de gestión de riesgos (si se asigna uno), expertos ajenos al proyecto.

Se emplean los Roles y Responsabilidades definidos en el Plan de Gestión de Riesgos del Proyecto (DG-32.01) para asignar responsables a los riesgos.

Actividad: Seguimiento y Control de los Riesgos.**Propósito:**

Realizar el seguimiento a los riesgos identificados, identificar, analizar y planificar nuevos riesgos, supervisar los riesgos residuales, ejecutar planes de respuesta a los riesgos y evaluar su efectividad a lo largo del ciclo de vida del proyecto.

Tareas:

1. Ejecutar las tareas de reevaluación de los riesgos previstas en el Plan de Gestión de Riesgos (DG-32.01) para identificar nuevos riesgos y reevaluar los riesgos del proyecto.
2. Ejecutar las auditorías a los riesgos para examinar y documentar la efectividad de las respuestas a los riesgos para tratar los riesgos identificados y sus causas, así como la efectividad del proceso de gestión de riesgos.
3. Efectuar las reuniones sobre el estado de situación de los riesgos del proyecto. La información sobre el rendimiento del trabajo proporciona el avance del cronograma; productos entregables que han sido completados y aquellos que no han sido completados; actividades del cronograma que se han iniciado y aquellas que se han finalizado; alcance del cumplimiento de los estándares de calidad; costes autorizados e incurridos; estimaciones hasta la conclusión de las actividades del cronograma que se

han iniciado; porcentaje físicamente completado de las actividades del cronograma en desarrollo; lecciones aprendidas documentadas registradas en la base de conocimientos de lecciones aprendidas; detalle de la utilización de recursos. Puede implicar elegir estrategias alternativas, ejecutar un plan para contingencias, adoptar acciones correctivas y modificar el plan de gestión del proyecto.

4. Informar periódicamente al Gestor de Riesgos o al Jefe del proyecto, por parte del propietario de los riesgos, acerca de la efectividad del plan, de cualquier efecto no anticipado y cualquier corrección sobre la marcha que sea necesaria para gestionar el riesgo correctamente.
5. Preparar los cambios solicitados como consecuencia de la implementación de planes para contingencias o soluciones alternativas para actualizar el plan de gestión del proyecto.
6. Actualizar en el Registro de Riesgos (DG-32.02) la siguiente información (Anexo 5):
 - a. Resultados de las reevaluaciones, auditorías y revisiones periódicas de los riesgos. Pueden incluir actualizaciones de la probabilidad, impacto, prioridad, planes de respuesta, propiedad y otros elementos del Registro de Riesgos (DG-32.02). Los resultados también pueden incluir cerrar los riesgos que ya no sean aplicables.
 - b. Los resultados reales de los riesgos del proyecto, y de las respuestas a los riesgos que pueden ayudar a los Gestores de Riesgo y Jefes de proyecto en la planificación de riesgos para toda la organización, así como en proyectos futuros. Pasa a ser parte de los documentos de cierre del proyecto.
7. Actualizar los Activos de los Procesos de la Organización para proyectos futuros. Incluye:
 - a. Plantillas: Plan de Gestión de Riesgos (DG-32.01) y Registro de Riesgos (DG-32.02)
 - b. Plan de Gestión de Riesgos (DG-32.01) actualizado: Matriz de probabilidad e impacto, método para identificar y categorizar los riesgos estructuras de desglose de riesgos, etc.
 - c. Registro de Riesgos (DG-32.02) actualizado: resultados de las reevaluaciones, auditorías y revisiones periódicas, así como los resultados reales de los riesgos del proyecto, y de las respuestas a los riesgos.
 - d. Documentación ampliada sobre los riesgos del proyecto y la estructura o taxonomía empleada en el proyecto.
 - e. Lecciones aprendidas para actualizar la base de datos de lecciones aprendidas.
 - f. Datos sobre los costes reales y las duraciones de las actividades del proyecto para actualizar las bases de datos de la organización.

8. Publicar los Activos de los Procesos de la Organización que incluyen el Registro de Riesgos (DG-32.02) actualizado como resultado de esta actividad.

Entradas:

1. Plan de gestión de riesgos (DG-32.01).
2. Registro de Riesgos (DG-32.02).
3. Información sobre el rendimiento del trabajo.

Herramientas y Técnicas:

1. Reevaluación de los riesgos.
2. Auditorías de los riesgos.
3. Reuniones sobre el estado de la situación.

Salidas:

1. Registro de riesgos (DG-32.02) actualizado.
2. Cambios solicitados.
3. Activos de los procesos de la organización (actualizados)
4. Plan de gestión del proyecto (actualizado).
5. Publicar los Activos de los Procesos de la Organización actualizados.

Responsable: Gestor de Riesgos

Participantes:

Gestor de Riesgos del proyecto, Jefe del proyecto, miembros del equipo del proyecto, propietarios de los riesgos, equipo de gestión de riesgos (si se asigna uno), expertos ajenos al proyecto.

Actividad: Comunicación.**Propósito:**

Lograr, durante todo el Proceso de Gestión de Riesgos, la comunicación entre los diferentes pasos del proceso, la interna del equipo de proyecto y la que surge entre el proyecto y los diferentes participantes del mismo, incluyendo la comunicación hacia y entre los niveles apropiados de la organización.

Tareas:

1. Definir el canal de comunicación. La organización debe disponer una carpeta en la Intranet de la empresa para publicar la información relacionada a los Activos de los

Procesos de la Organización que sirven como entrada y/o salida a diferentes actividades del Proceso de Gestión de Riesgos y contribuyan a la realización de proyectos futuros.

2. Potenciar la comunicación. Los riesgos deben discutirse de forma abierta, tanto dentro como fuera del equipo de proyecto. Todos los integrantes del equipo deben participar, en mayor o menor medida, de las diferentes tareas relacionadas con la gestión de riesgos. Los miembros de un equipo no deben tener reservas de ningún tipo en comunicar sus opiniones con libertad para, de esta forma, evaluar con mayor precisión el estado del proyecto y tomar decisiones consensuadas.
3. Aprender de todas las experiencias. El conocimiento obtenido en un proyecto puede reducir la incertidumbre de la toma de decisiones en otros proyectos cuando la información es poco fiable. El análisis directo de los resultados de proyectos anteriores fomenta el aprendizaje dentro del equipo mediante el intercambio de opiniones entre sus miembros.
4. Mantener publicada la lista de los diez elementos de riesgo más frecuentes. Puede ser publicada semanalmente, mensualmente o en la revisión de los hitos del proyecto, seguidos apropiadamente con la reevaluación de los elementos de riesgo o acciones correctivas.
5. Identificar, capturar y comunicar la información pertinente desde fuentes internas y externas, de arriba hacia abajo, de abajo hacia arriba y a través de toda la organización.
6. Mantener actualizada la Base de Datos de Riesgos de Proyecto separada con la lista de los riesgos y la información relacionada con su estado actual e historia reciente.
7. Acrecentar la información contenida en una Base de Datos de Riesgos Organizacional a partir de la información contenida en la Base de Datos de Riesgos de Proyecto.

Entradas:

1. Información que se desea comunicar: Activos de los Procesos de la Organización actualizados, Plan de gestión de riesgos (DG-32.01), Registro de Riesgos (DG-32.02), etc.
2. Especificación de los canales de comunicación a utilizar.

Herramientas y Técnicas:

1. Carpetas compartidas en la Intranet de la empresa.
2. Correo Electrónico.
3. Base de datos organizacionales y de proyecto con lecciones aprendidas.
4. Reuniones de chequeo.

<p>5. Consejillos, Despachos y Consejos de Producción.</p> <p>6. Comités Técnicos, Talleres, Cursos, Seminarios.</p> <p>7. Publicaciones.</p> <p>8. Información digital o impresa.</p>
<p>Salidas:</p> <p>1. Información comunicada a través de los canales de comunicación especificados.</p>
<p>Responsable: Gestor de Riesgos</p>
<p>Participantes:</p> <p>Gestor de Riesgos del proyecto, Jefe del proyecto, miembros del equipo del proyecto, equipo de gestión de riesgos (si se asigna uno), expertos ajenos al proyecto.</p>

Flujo de información del proceso.

Al Proceso Gestión de Riesgos le entra:

1. Factores ambientales de la organización.
 - ? Cultura y estructura de la organización.
 - ? Normas gubernamentales o industriales (por ejemplo, reglamentaciones de agencias reguladoras, normas de productos, estándares de calidad y normas de fabricación).
 - ? Infraestructura (por ejemplo, instalaciones existentes y equipos de capital).
 - ? Recursos humanos existentes (por ejemplo, habilidades, disciplinas y conocimientos, tales como diseño, desarrollo, legales, contrataciones y compras).
 - ? Administración de personal (por ejemplo, guías de contratación, evaluaciones del rendimiento de los empleados y registros de formación).
 - ? Condiciones del mercado.
 - ? Tolerancia al riesgo de los interesados.
 - ? Bases de datos comerciales (por ejemplo, datos de estimación de costes estandarizados, información de estudios de riesgo de la industria y bases de datos de riesgos).
 - ? Sistemas de información de la gestión de proyectos (por ejemplo, los conjuntos de herramientas automatizadas, tales como las herramientas de software para la elaboración de cronogramas, los sistemas de gestión de la configuración, los sistemas de recogida y distribución de información, o las interfaces Web con otros sistemas automatizados en línea).
2. Activos de los procesos de la organización.

-
- ? Procesos y procedimientos de la organización para realizar el trabajo.
 - ? Base de conocimiento corporativa de la organización para almacenar y recuperar información.
3. Enunciado del alcance del proyecto.
- ? Objetivos del proyecto.
 - ? Descripción del alcance del producto.
 - ? Requisitos del proyecto.
 - ? Asunciones del proyecto.
 - ? Riesgos iniciales definidos, es decir, los que son conocidos desde el inicio.
 - ? Hitos del cronograma que pueden tratarse como restricciones, a partir de fechas impuestas por el cliente o la organización.
4. Plan de gestión del proyecto.
- ? Descripción de las herramientas y técnicas para la ejecución del proyecto.
 - ? Cómo se ejecutará el trabajo para alcanzar los objetivos del proyecto.
 - ? Cómo se supervisarán y controlarán los cambios.
 - ? Cómo se realizará la gestión de la configuración.
 - ? La necesidad y las técnicas para la comunicación entre los interesados.
 - ? Cronograma del proyecto.
 - ? Recursos del proyecto.

En el Proceso Gestión de Riesgos se genera:

- ? Plan de gestión de riesgos (DG-32.01).
- ? Registro de Riesgos (DG-32.02).
- ? Acuerdos contractuales relacionados con el riesgo.
- ? Cambios solicitados.
- ? Activos de los procesos de la organización (actualizado).
- ? Plan de gestión del proyecto (actualizado).

3.2 Preparación para la introducción del proceso propuesto.

Debido al desconocimiento sobre el tema de la gestión de riesgos en la empresa fue impartida la Conferencia “Conferencia sobre Riesgos y su Gestión” con el objetivo de elevar la cultura organizacional sobre los riesgos y su gestión, ya que no es posible implementar un proceso sin el apoyo de la organización. Para ello se organizaron dos grupos integrados por Directores, Jefes de Grupo, Jefes de Proyecto y otros compañeros con diferentes roles en Softel,

incluyendo miembros de la Factoría de Software. Abarcó los temas siguientes: concepto de riesgo (positivo y negativo) y gestión de riesgos, estrategias de riesgo: reactivas y proactivas, política de riesgos a nivel organizacional, reglas básicas de gestión de riesgos según la *American Systems Corporation (ASC)*, principios básicos de la gestión de riesgos según Microsoft, principales elementos de los procesos de gestión de riesgos de PMI y el SEI, Factores de riesgo organizacionales, estratégicos y tácticos según Esteves y Pastor, factores de riesgo más frecuentes (Boehm, 1991), Lista de comprobación de riesgos (Pressman), otras técnicas para identificar riesgos y estrategias para Evitar, Transferir y Mitigar el riesgo (Valladares, 2010b). Este proceso sirvió de base para que las Direcciones y muchos Proyectos pudieran formalizar sus riesgos, al menos en una primera aproximación, incluyendo los proyectos Mantenimiento del RIS y Galen Clínica, pertenecientes a la Factoría de Software.

A continuación, fue impartido un nuevo ciclo de conferencias: “Proceso de Gestión de Riesgos” para preparar a la empresa y, fundamentalmente, a la Factoría de Software en el Proceso de Gestión de Riesgos propuesto como resultado de esta investigación. En la misma se analizó con mayor profundidad el concepto de riesgo utilizando como ejemplo la escritura de algunos de los riesgos identificados en los proyectos “Mantenimiento del RIS” y “Galen Clínicas” (Valladares, 2010a).

Las dos conferencias fueron publicadas en la Intranet de la empresa, incluyendo la grabación que se hizo de la segunda Conferencia, para que la misma sirva de material de estudio del proceso.

Fue creado a nivel organizacional el Grupo Empresarial de Gestión de Riesgos con vistas a gestionar los riesgos de la empresa. Está constituido por diez compañeros, que son los Gestores de Riesgo principales que representan a los Grupos de trabajo más representativos de la empresa. Entre ellos se encuentra el de la Factoría de Software. Este grupo contribuirá a la comunicación entre el equipo de proyecto y la organización en todos los sentidos; convocará a los expertos que sean necesarios para la identificación y evaluación de riesgos, además de otras actividades del proceso; trabajará en la mejora continua del proceso; elaborará los informes correspondientes sobre el estado de los riesgos en el grupo que representa.

3.3 Análisis de los resultados de la evaluación del proceso de gestión de riesgos definido.

Para la evaluación teórica del proceso de gestión de riesgos definido se empleó el método definido en el Capítulo II (Hernández, 2009).

Objetivo de la evaluación.

Evaluar el proceso teóricamente desde el punto de vista de su aplicación práctica en la empresa y del impacto que se obtendrá en la medida en que sea implantado y generalizado.

Selección de los Expertos.

Debido a que el proceso definido fue realizado teniendo en cuenta las características de la empresa y para resolver la problemática que dio inicio a esta investigación, todos los expertos seleccionados pertenecen a Softel, teniendo en cuenta su experiencia en la gestión de proyectos, el rol que desempeña, las vivencias que ha tenido en el proceso de gestión de riesgos, la disposición a participar en la encuesta, el espíritu colectivista y autocrítico, así como sus efectividad en la actividad profesional. Todos han alcanzando conocimientos sobre riesgos y su gestión y sobre el proceso definido, debido a las conferencias que fueron impartidas como parte de la introducción del proceso y algunos están participando directamente en su implantación.

La cantidad de expertos a participar se determinó según la propuesta de Dalkay (1969): 10 expertos para lograr un error del 10% (Fernández, 2005).

Elaboración del cuestionario.

Para la elaboración del cuestionario se prepararon los criterios a medir, se clasificaron en grupos y se asignó un peso general a cada grupo, sometiéndolos a la valoración de los expertos. Con el resultado de las opiniones se obtuvo la tabla 3.1.

Tabla 3.1. Grupos, Criterios y Pesos por grupos.

Criterios de implantación			40
G1	C1	Necesidad del empleo del proceso	
	C2	Conocimiento del proceso propuesto	
	C3	Satisfacción de las necesidades de la producción	
	C4	Garantía de principios básicos de la gestión de proyectos	

Criterios de generalización			35
G2	C5	Facilidad de comprensión	
	C6	Disponibilidad de documentación para su estudio	
	C7	Facilidad de uso	
	C8	Adaptabilidad a diferentes proyectos y áreas de la empresa	
Criterios de impacto			25
G3	C9	Contribución al cumplimiento del Componente Evaluación de Riesgos de la Resolución 297/03 del MFP	
	C10	Contribución al desarrollo de la Gestión de Proyectos	
	C11	Contribución al fortalecimiento de la Comunicación Organizacional	

Con la tabla obtenida se elaboró el cuestionario que se muestra en el Anexo 6, para la asignación de los pesos a cada uno de los criterios, y el que se presenta en el Anexo 7, para la calificación cuantitativa de cada criterio y la cualitativa final del proceso definido. En ambos casos se emplea la escala de 1 a 5 (Malo, Cuestionable, Aceptable, Bueno, Excelente).

Entrega y resultados de los cuestionarios.

Se entregó el primer cuestionario (Anexo 6) y, después de dos rondas, se obtuvo el resultado que se muestra en la tabla 3.2.

Tabla 3.2. Resultados de la asignación de pesos a los criterios.

Grupo = Peso	Criterios	Expertos										Peso Promedio
		E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	
G1 = 40	C1	12	12	9	11	10	10	11	8	11	8	10.2
	C2	9	8	8	10	9	13	11	7	9	8	9.2
	C3	9	10	12	10	11	10	11	15	12	12	11.2
	C4	10	10	11	9	10	7	7	10	8	12	9.4
G2 = 35	C5	8	8	7	9	10	10	8	7	8	7	8.2
	C6	9	8	7	9	8	10	7	10	7	8	8.3
	C7	9	9	8	9	12	10	9	8	9	9	9.2
	C8	9	10	13	8	5	5	11	10	11	11	9.3
G3 = 25	C9	10	5	8	7	5	5	5	8	8	8	6.9
	C10	8	12	10	9	12	10	10	10	10	10	10.1
	C11	7	8	7	9	8	10	10	7	7	7	8.0
Total		100										

Se verificó la consistencia en el trabajo de expertos, utilizando el coeficiente de concordancia de Kendall (W) con ligas y el estadígrafo Chi cuadrado (χ^2), siguiendo lo descrito en el Capítulo II. Para ello, a partir de la tabla anterior, se creó la tabla 3.3 de rangos de puntajes ligados.

Tabla 3.3. Rangos de puntajes ligados.

	G1				G2				G3		
	C1	C2	C3	C4	C5	C6	C7	C8	C9	C10	C11
E1	11.00	6.00	6.00	9.50	2.50	6.00	6.00	6.00	9.50	2.50	1.00
E2	10.50	3.50	8.00	8.00	3.50	3.50	6.00	8.00	1.00	10.50	3.50
E3	7.00	5.00	10.00	9.00	2.00	2.00	5.00	11.00	5.00	8.00	2.00
E4	11.00	9.50	9.50	5.50	5.50	5.50	5.50	2.00	1.00	5.50	5.50
E5	7.00	5.00	9.00	7.00	7.00	3.50	10.50	1.50	1.50	10.50	3.50
E6	7.00	11.00	7.00	3.00	7.00	7.00	7.00	1.50	1.50	7.00	7.00
E7	9.50	9.50	9.50	2.50	4.00	2.50	5.00	9.50	1.00	6.50	6.50
E8	5.00	2.00	11.00	8.50	2.00	8.50	5.00	8.50	5.00	8.50	2.00
E9	9.50	6.50	11.00	4.00	4.00	1.50	6.50	9.50	4.00	8.00	1.50
E10	4.50	4.50	10.50	10.50	1.50	4.50	7.00	9.00	4.50	8.00	1.50

A partir de la información anterior, se obtuvieron los resultados que se muestran en la tabla 3.4.

Tabla 3.4. Resultados para determinar la concordancia de los Expertos.

k	N	S	χ^2_T	W	χ^2_{real}	$\chi^2_{0.01;10}$
10	11	3851.5	97	0.3839	38.39	23.21

Como se cumple que $\chi^2_{real} > \chi^2_{0.01;10}$, esta última obtenida de la tabla de valores críticos de χ^2 (Siegel, 1974), entonces se puede concluir que existe concordancia entre los expertos en cuanto al peso asignado a los criterios, rechazándose la hipótesis de nulidad de que las k ordenaciones no están relacionadas.

Para realizar la evaluación cuantitativa y cualitativa del proceso de gestión de riesgos definido se entregó a los Expertos el segundo cuestionario (Anexo 7). La evaluación de los Expertos, así como el promedio de las mismas se muestra en la tabla 3.5.

Tabla 3.5. Evaluación Cuantitativa y Cualitativa de los Expertos.

	Criterio	E1	E2	E3	E4	E5	E6	E7	E8	E9	E10	Promedio
Evaluación Cuantitativa	C1	5	4	4	5	4	4	5	4	4	4	4
	C2	4	3	4	5	4	4	5	3	4	4	4
	C3	5	4	4	4	5	4	5	5	4	4	4
	C4	5	5	4	4	4	5	5	3	5	4	4
	C5	4	3	4	5	5	4	5	3	4	4	4
	C6	4	4	4	5	4	5	4	4	4	4	4
	C7	4	4	4	4	5	4	5	4	4	4	4
	C8	5	5	3	3	3	5	5	4	5	3	4
	C9	5	3	5	5	3	5	3	4	5	4	4
	C10	5	5	4	5	5	5	4	4	5	4	5
	C11	4	4	4	5	4	4	4	5	4	4	4
	Evaluación Cualitativa	4	5	4	5	4	4	5	4	4	4	4

A partir de las evaluaciones cuantitativas de los Expertos y el promedio de las mismas para cada criterio (Tabla 3.5), se realizó la evaluación cuantitativa del proceso. Los resultados se muestran en la tabla 3.6.

Tabla 3.6. Resultados de las evaluaciones.

Criterios	c = Calificación Cuantitativa de los Expertos					p = Peso Relativo	p * c
	1	2	3	4	5		
C1	0	0	0	1	0	0.1020	0.41
C2	0	0	0	1	0	0.0920	0.37
C3	0	0	0	1	0	0.1120	0.45
C4	0	0	0	1	0	0.0940	0.38
C5	0	0	0	1	0	0.0820	0.33
C6	0	0	0	1	0	0.0830	0.33
C7	0	0	0	1	0	0.0920	0.37
C8	0	0	0	1	0	0.0930	0.37

C9	0	0	0	1	0	0.0690	0.28
C10	0	0	0	0	1	0.1010	0.51
C11	0	0	0	1	0	0.0800	0.32
							4.10

A partir de la Tabla 3.6 se determinó el Índice de Aceptación del Proceso de Gestión de Riesgos definido en la investigación, conociendo el peso relativo de cada criterio y la calificación dada por los Expertos: $IA = p * c / 5 = 4.10 / 5 = \mathbf{0.82}$. Como $IA = 0.82 > 0.7$ la probabilidad de éxito del proceso es alta. La evaluación cualitativa realizada por los Expertos al proceso de Gestión de Riesgos (Tabla 3.5) definido en la investigación fue Bueno (Hernández, 2009).

3.4 Otros resultados alcanzados.

Antes de realizar las acciones de preparación para la introducción del proceso propuesto nunca se había llevado a cabo un proceso formal de gestión de riesgos, no existían conocimientos sobre esta actividad y no se habían identificado riesgos en los proyectos de la Factoría de Software.

Después de la Conferencia impartida “Conferencia sobre Riesgos y su Gestión” (Valladares, 2010b), empleando la plantilla Lista de Riesgos, establecida en la Dirección de Desarrollo, los proyectos “Mantenimiento del RIS” y “Galen Clínicas” obtuvieron una lista de 10 y 14 riesgos, respectivamente (González, 2010; Sandra Gutiérrez, 2010) a los cuales se les determinó probabilidad de ocurrencia, impacto, magnitud del riesgo, indicadores, estrategia para mitigarlo y planes de contingencia. En ambos proyectos solamente se realizaron las actividades de identificación, análisis y planificación de respuestas, pero no se realizaron actividades de seguimiento y control de los riesgos, debido al desconocimiento sobre el proceso completo.

En el proyecto “Mantenimiento del RIS” ya se está aplicando el proceso propuesto. Fue definido el Plan de Gestión de Riesgos (DG-32.01) (Sandra Gutiérrez, 2010a) y el Registro de Riesgos (DG-32.02) (Sandra Gutiérrez, 2010b). Se decidió aplicar la Taxonomía Ajustada de Maniasi (Maniasi, 2005). Fueron identificados, caracterizados y evaluados 73 riesgos. Al definir la probabilidad e impacto de cada uno y ubicarlos en la Matriz de probabilidad e impacto se obtuvieron los resultados que se muestran en la tabla 3.7.

Tabla 3.7. Riesgos identificados y evaluados.

Prioridad	Cantidad	Estrategia definida
Alta	18	Mitigar
Moderada	26	Aceptar
Baja	29	Documentar

Todos los riesgos identificados en las entrevistas apreciativas están contenidos en el Registro de Riesgos obtenido (Sandra Gutiérrez, 2010b). Se definieron los planes de mitigación de los 18 riesgos de prioridad alta, donde sirvieron como base los planes de mitigación obtenidos en las entrevistas apreciativas.

Toda la información generada por el proyecto se encuentra publicada para su uso y conocimiento por el resto de los proyectos de la organización que están implantando el proceso.

Conclusiones parciales.

1. Se definió el proceso para la Gestión de Riesgos para los proyectos de desarrollo de software de Softel, así como cada una de sus actividades, tomando como base los procedimientos que sustentaron la propuesta a partir del análisis realizado en el Capítulo I.
2. Se ha elevado la cultura organizacional sobre los riesgos y su gestión contribuyendo a la toma de conciencia sobre la importancia de implementar este proceso en la empresa.
3. Se preparó al personal de la empresa, fundamentalmente al de la Factoría de Software, en el proceso definido para lograr su implantación, con resultados más palpables en el proyecto "Mantenimiento del RIS".
4. A partir de la evaluación cuantitativa realizada en el trabajo con los expertos se determinó que la probabilidad de éxito del proceso es alta y en la evaluación cualitativa realizada por los expertos el proceso fue catalogado de Bueno.

Conclusiones.

1. Después de haber elaborado el marco teórico de la investigación, estudiado las tendencias actuales sobre la gestión de riesgos, así como los principales marcos o procesos de gestión de riesgos y su evolución, no se encontró ningún marco o proceso que se ajustara a las necesidades de Softel y resolviera el problema que dio inicio a la investigación.
2. El estudio y diagnóstico del estado actual de la gestión de riesgos en algunas entidades cubanas y, fundamentalmente, en los proyectos de desarrollo de software de Softel permitió demostrar la existencia del problema que dio inicio a la investigación.
3. Se definió el Proceso de Gestión de Riesgos para los proyectos de desarrollo de software de Softel, el cual está sustentado por el estudio realizado.
4. El proceso definido fue evaluado por método de expertos, demostrando su utilidad práctica para continuar su implantación y ser generalizado a otros proyectos con un gran impacto en la mejora de la gestión de los proyectos de la organización.

Recomendaciones.

1. Establecer en Softel como norma de trabajo el proceso propuesto.
2. Divulgar el proceso propuesto para su uso en otras empresas productoras de software.
3. Seguir enriqueciendo el proceso a partir de su implantación en los proyectos de la empresa y aplicando el modelo para la organización de la mejora continua en la ingeniería de software en Softel (Cué, 2009).
4. Mantener una comunicación con la UCI para seguir de cerca los resultados de la aplicación práctica del Modelo de Gestión de Riesgos MoGeRi con vistas a mejorar el proceso propuesto y viceversa.
5. Poner a disposición de otras entidades cubanas el proceso propuesto para su uso.

Referencia Bibliográfica.

- ADMINISTRACIONES PÚBLICAS, M. D. (Ed.). (2006). *MAGERIT - versión 2: Metodología de Análisis y Gestión de riesgos de los Sistemas de Información*. Madrid: MINISTERIO DE ADMINISTRACIONES PÚBLICAS.
- Alberts, C. a. D., Audrey (2006). *Advanced Risk Analysis for High-Performing Organizations* [Electronic Version]. Retrieved Septiembre/2007 from <http://www.sei.cmu.edu/risk/advancedrisk.pdf>
- Astigarraga, E. (2008, 18/1/2008). *El Método Delphi*. Retrieved 1/18/2008, 2008, from http://www.codesyntax.com/prospectiva/Metodo_delphi.pdf
- Audrey, D. (2009). *Rethinking Risk Management*. Paper presented at the NDIA Systems Engineering.
- Bernaza, I. R. E. (2009). *Solución Informática para los Policlínicos*. Unpublished Maestría, UCI, Ciudad Habana.
- Boehm, B. W. (1991). *Software risk management: principles and practices* [Electronic Version], 2007, 10. Retrieved Septiembre/2007 from http://www.inf.ed.ac.uk/teaching/courses/seoc/2006_2007/resources/PM_SRM.pdf
- Bolaños, A. R. (2008). *La evaluación de riesgos como parte del Sistema de Control Interno en las universidades cubanas*. [Electronic Version], 10. Retrieved Septiembre/2008.
- Cabrera, H. M. (2009). *Gestión de la integración del Proyecto Registro Informatizado de Salud (RIS)*. Unpublished Tesis de Maestría, UCI, Ciudad Habana.
- CMMI Product Team. (2006). *CMMI for Development, Version 1.2* (Final No. CMU/SEI-2006-TR-008). Pittsburg: Carnegie Mellon, Software Engineering Institute (SEI).
- Contraloría General de la República de Cuba. (2009). *GUÍA DE AUTOCONTROL DEL SISTEMA DE CONTROL INTERNO*. Unpublished manuscript, Ciudad Habana.
- COSO, C. o. S. O. o. t. T. C. (2004). *Enterprise Risk Management — Integrated Framework. Executive Summary*. Committee of Sponsoring Organizations of the Treadway Commission (COSO).
- Cué, D. R. L. (2009). *Modelo para la organización de la mejora continua en la ingeniería de software en Softel*. Unpublished Maestría, UCI, Ciudad Habana.
- Charette, R. (1989). *Software engineering risk analysis and management*. New York: McGraw-Hill.
- de la Villa, M. y. o. (2004). *Modelos de Evaluación y Mejora de Procesos: Análisis Comparativo*. Retrieved Enero/2008, 2008, from <http://www.sc.ehu.es/jwdocoj/remis/docs/DelaVillaadis2004.doc>

- del Castillo, M. M. R. (2009). Tesis de Maestría "Solución Informática para la Red Nacional de Bancos de Sangre".
- del Toro Ríos, J. C. y. o. (2005). Control Interno. Preparación Económica para Cuadros. Dirección Nacional de Aduanas, C. (2007). El proceso de gestión de riesgo. Retrieved 18/1/2008, 2008, from http://www.aduana.cl/prontus_aduana/site/artic/20070228/pags/20070228130834.html
- Esteves, J., Pastor Joan y otros. (2005). Implementación y Mejora del Método de Gestión de Riesgos del SEI en un proyecto universitario de desarrollo de software. *Revista IEEE América Latina*, 2007.
- Fairley, R. (2006). Risk Management for software projects - IEEE Software. Retrieved Octubre 2007, 2007, from http://www.inf.ed.ac.uk/teaching/courses/seoc/2006_2007/resources/PM_RMS.pdf
- Feiler, P. H. (1993). *Reengineering: An Engineering Problem* (No. CMU/SEI-93-SR-5). Pittsburgh, Pennsylvania 15213: SEI.
- Fernández, A. R. (2005). Los métodos de evaluación de expertos para valorar resultados de las investigaciones.
- Figueredo, C. Y. (2007). Trabajo de Diploma "Análisis y Gestión de Riesgo para el desarrollo de las aplicaciones del proyecto Atención Primaria de Salud (APS)".
- free-soft.org. (2003, 6/1/2003). Free Software (Open Source). Retrieved Junio/2010, 2010, from <http://www.free-soft.org/>
- Gonda, B. y. J., Nicolás. (2009). *GeneXus Philosophy*. Montevideo, Uruguay: Artech.
- González-Cueto, L., Dra. Aleida. (2002). La Administración del Riesgo cambiario en el contexto de la economía cubana. *Gerencia: del propósito a la acción*, Editorial Félix Varela.
- González, C. N. (2010). Lista de Riesgos - Proyecto Galen Clínicas.
- Gutiérrez, S. (2010a). DG-32.01: Plan de Gestión de Riesgos - Mantenimiento del RIS. 2010
- Gutiérrez, S. (2010b). DG-32.02: Registro de Riesgos - Mantenimiento del RIS. 2010
- Gutiérrez, S. (2010). Lista de Riesgos - Proyecto Mantenimiento del RIS. 2010
- Hernández L.R.A., C. G. S. (2002). *El paradigma cuantitativo de la investigación científica* (Vol. 1). Ciudad de la Habana: EDUNIV, Editorial Universitaria.
- Hernández, L. R. A. (2009). *Una Introducción a la Gestión de Proyectos*.
- Higuera, R. P. a. H., Yacov Y. (1996). *Software Risk Management* (Final No. CMU/SEI-96-TR-012, ESC-TR-96-012). USA: Software Engineering Institute (SEI).
- Humphrey, W. S. (1999). *Introduction to the Team Software Process*: Addison Wesley.

REFERENCIA BIBLIOGRÁFICA

- I. Jacobson, G. B., J. Rumbaugh. (2000). *El Proceso Unificado de Desarrollo de Software. La guía completa del Proceso Unificado escrita por sus creadores*. Madrid: PEARSON EDUCACIÓN S.A.
- IEEE, C. S. P. P. C. (2004). *Guide to the Software Engineering Body of Knowledge (SWEBOK)*. Los Alamitos, California. EEUU.: IEEE Computer Society.
- Iglesias, E. E. P. (2006). La administración de riesgos. Su impacto en la empresa cubana. Retrieved Octubre/2007, 2007, from <http://www.monografias.com/trabajos35/administracion-de-riesgos/administracion-de-riesgos.shtml>
- Jeannine Sivi, M. L. P., Erin Harper. (2005). *Relationships Between CMMI and Six Sigma* (No. CMU-SEI-2005-TN-005). Pittsburgh, Pennsylvania 15213: SEI, CMU.
- Lefcovich, M. L. (2003). Matriz de control interno. Retrieved Octubre/2007, 2007, from <http://www.monografias.com/trabajos14/matriz-control/matriz-control.shtml?monosearch>
- Lewis, G. A. (2008). *SMART: Analyzing the Reuse Potential of Legacy Components in a Service-Oriented Architecture Environment* (No. CMU/SEI-2008-TN-008). Pittsburgh, Pennsylvania 15213: SEI.
- Maniasi, S. D. (2005). *Identificación de riesgos de proyectos de software en base a taxonomías*. Unpublished Maestría, ITBA, Córdoba.
- Marcelo, C. J. (2001, 2001). de la Gestión de los Riesgos en los Proyectos a la Gestión de los Proyectos por sus Riesgos. Retrieved Mayo/2010, 2010
- Marcelo, C. J. (2003). ESTUDIO EXPLORATORIO SOBRE LOS MÉTODOS DE GESTIÓN DE PROYECTOS DE ALTO RIESGO.
- Martínez C.D, C. D. R. (2008, 4/4/2008). Informe final sobre el Diagnóstico realizado a los Procesos de la Empresa SOFTEL. Retrieved Diciembre/2009, 2009
- Martínez, C. D. (2007, 2007). Plantilla para la definición de los procesos de Softel. Retrieved Abril/2010, 2010
- Matos, L. E. (2009). Entrevista a Capers Jones: "El control de la calidad es la clave del éxito en los proyectos de software" [Electronic Version]. *LiderDeProyecto.com*, 3. Retrieved 23/04/2010 from http://www.liderdeproyecto.com/articulos/entrevista_a_capers_jones.html.
- Matsuo, E. K. (1999). *Risk assessment in incremental software development*. Unpublished Maestría, Naval Postgraduate School, Monterrey, California.
- McFeeley, B. (1996). *IDEALSM: A User's Guide for Software Process Improvement*. Software Engineering Institute, Carnegie Mellon University, Pittsburgh, Pennsylvania 15213.

- Microsoft, C. (2002). *MSF Risk Management Discipline v.1.1*: Microsoft.
- Mutafelija, B. S. H. (2009, 15/09/2009). ISO 12207:2008 to CMMI v1.2 Map. *SEI* Retrieved Junio/2010, 2010, from www.sei.cmu.edu/cmmi/casestudies/mappings/pdfs/upload/ISO-12207-2008-Mapping.pdf
- Normalización, O. N., Cuba. (2000). NC-ISO/IEC GUÍA 51: 2000 (pp. 16): Publicada por la ISO en 1999.
- Normalización, O. N., Cuba. (2008). NC-ISO/IEC GUÍA 73: 2008 (pp. 19): Publicada por la ISO en 2002.
- Normalización, O. N. d. (2007). Norma Cubana ISO/IEC 12207: 2007. *ISO*.
- Palacio, J. (2006). Gestión de proyectos ágil: conceptos básicos [Electronic Version]. *Navegapolis.Net*. Retrieved Junio/2010 from www.navegapolis.net/files/s/NST-003_01.pdf.
- Pérez, V. J. E. (2007). Administración de Riesgos en Pequeñas Empresas: Factor de Éxito en la Mejora de Procesos (pp. Administración de Riesgos en Pequeñas Empresas: Factor de Éxito en la Mejora de Procesos). Monterrey: ESI Center (Centro de Excelencia para la Industria del Software) - Tecnológico de Monterrey.
- PMI, P. M. I.-. (2004). *Guía de los Fundamentos de la Dirección de Proyectos (Tercera Edición) (Guía del PMBOK)*. Pennsylvania: Project Management Institute Inc. Four Campus Boulevard. Newtown Square, Pennsylvania 19073-3299 EEUU.
- Pressman, R. S. (2005). *Ingeniería del Software: Un enfoque práctico*. (Vol. 1). La Habana: Félix Varela.
- Protiviti. (2007). Guide to Enterprise Risk Management. Frequently asked questions. Retrieved Octubre/2007, 2007, from http://www.ucop.edu/riskmgt/erm/documents/protiviti_faiguide1.pdf
- Quincosa, D. Y. (2006). Metodología para Gestionar Riesgos Empresariales. Una herramienta indispensable para la empresa moderna [Electronic Version]. *monografias.com*, 30. Retrieved 28/08/2007.
- Rosenberg, L. H.-T. H.-A. G. (1999, Febrero/1999). *Continuous Risk Management at NASA*. Paper presented at the Applied Software Measurement / Software Management Conference, San José, California.
- Siegel, S. (1974). *Estadística no paramétrica aplicada a las ciencias de la conducta* (2 ed.). México: Editorial Triller.
- Softel. (2009, Diciembre/2009). Subsistema Organización General - Perfeccionamiento Empresarial. Retrieved Junio/2010, 2010

- Solórzano, P. M. P. (2006). Los cinco componentes del control interno [Electronic Version], 8. Retrieved Octubre/2007 from <http://www.monografias.com/trabajos42/componentes-control-interno/componentes-control-interno.shtml#Relacionados>.
- Uch, P. d. e. d. r. h., Administración y gerencia. (2002, 13/06/2002). ISO 9001. Retrieved 21/6/2010, 2010, from <http://www.gestiopolis.com/recursos/documentos/fulldocs/ger/iso9001uch.htm>
- Universidad de Murcia. (2006, 17/06/2006). Apuntes. Gestión de riesgos. MAGERIT. Informática Aplicada a la Gestión Pública 2005/06-5. Retrieved Enero/2008, 2008, from <http://www.um.es/docencia/barzana/IAGP/lagp05.pdf>
- Valladares, A. A. S. (2010a, Marzo/2010). *Conferencia sobre el Proceso de Gestión de Riesgos*. Paper presented at the Conferencia sobre el Proceso de Gestión de Riesgos, Softel.
- Valladares, A. A. S. (2010b, Febrero/2010). *Conferencia sobre Riesgos y su Gestión*. Paper presented at the Conferencia sobre Riesgos y su Gestión, Softel.
- Valladares, A. A. S. (2010c, Enero/2010). Proceso de Gestión de Riesgos para los Proyectos de Softel. Retrieved Enero/2010, 2010
- Walsh, K. R. (2002). The role of motivation and risk behaviour in software development success. *Information Research Vol. 7 No. 3, April(3)*, 129.
- Whitney, D. (2002). *The Power of Appreciative Inquiry. A Practical Guide to Positive Change*. San Francisco: Berrett-Koehler Publishers, Inc.
- Whitney, D. (2005). *Encyclopedia of positive questions, Volume one, Using Appreciative Inquiry to bring out the best in your organization* (Volume One ed. Vol. 1). San Francisco: Crown Custom Publishing, USA.
- Zulueta, V. Y. (2007a). *Modelo de Gestión de Riesgos en Proyectos de Desarrollo de Software*. Unpublished Maestría, Universidad de las Ciencias Informáticas (UCI), Ciudad Habana.
- Zulueta, V. Y. (2007b, 21/06/2007). Tendencias actuales de la Gestión de Riesgos. *RevistaCiencias.com*.
- Zulueta, V. Y. (2009). La gestión de riesgos en la producción de software y la formación de profesionales de la informática: experiencias de una universidad cubana. *Revista Española de Innovación, Calidad e Ingeniería de Software (REICIS)*, 5, No. 3, 18.

Glosario de Términos y Acrónimos.

Aceptar el riesgo: Reconocimiento de la existencia de un factor de riesgo junto con la decisión para aceptar las consecuencias si el problema correspondiente ocurre.

Agile: (Ágil). Tiene como objetivo dar garantías a las cuatro demandas principales de la industria en la que se ha generado: Valor, reducción del tiempo de desarrollo, agilidad y fiabilidad (Palacio, 2006).

Análisis de la causa-raíz: Es la determinación de la causa subyacente o causas de un problema potencial (factor de riesgo).

Análisis de riesgo: Proceso de examinar los factores de riesgo identificados para determinar la probabilidad de ocurrencia, las pérdidas potenciales (impacto) y las estrategias para manejar el riesgo.

Anular el riesgo: Curso de acciones para eliminar un factor de riesgo (por ejemplo, cambiando los requisitos, extendiendo la planificación o transfiriendo el factor de riesgo a otro dominio).

CMMI (*Capability Maturity Model Integrated*): Modelo integrado para la determinación de la madurez de la capacidad de un proceso de software (Jeannine Sivi, 2005).

Control Interno: Es el proceso integrado a las operaciones efectuado por la dirección y el resto del personal de una entidad para proporcionar una seguridad RAZONABLE al logro de los objetivos siguientes: confiabilidad de la información, eficiencia y eficacia de las operaciones, cumplimiento de las leyes, reglamentos y políticas establecidas y control de los recursos, de todo tipo, a disposición de la entidad (del Toro Ríos, 2005).

Exposición al riesgo: Es el producto de la probabilidad y la pérdida potencial para un factor de riesgo; usualmente expresado en unidades monetarias o utilidad (del Toro Ríos, 2005).

Factor de riesgo: Problema potencial que sería perjudicial a una actividad planeada, proyecto, o programa, caracterizado por la probabilidad de ocurrencia del problema ($0 < p < 1$) y la pérdida potencial (de vida, dinero, propiedad, reputación, y otras) si el problema ocurriera. Ambos, la probabilidad y la pérdida potencial, pueden cambiar con el tiempo (del Toro Ríos, 2005).

GeneXus: Herramienta de desarrollo de software basada en conocimiento, orientada principalmente a aplicaciones de clase empresarial para la Web y plataformas Windows. El

desarrollador especifica sus aplicaciones en alto nivel (de manera mayormente declarativa), a partir de lo cual se genera código para múltiples entornos (Gonda, 2009).

Gestión de riesgos: Incluye los procesos relacionados a la planificación de la gestión de riesgos, identificación, análisis, respuestas y monitoreo y control en un proyecto. Los objetivos son incrementar la probabilidad y el impacto de los eventos positivos y disminuir la probabilidad y el impacto de los eventos adversos al proyecto.

Gestión continua del riesgo: Es el proceso de analizar el progreso de una actividad planeada, proyecto o programa en una base periódica, continuada y manejando los factores de riesgo identificados; incluye el desarrollo de opciones y posiciones de retroceso para permitir soluciones alternativas encaminadas a reducir el impacto, si un factor de riesgo se convierte en un problema.

IDEAL: Método que implementa su modelo sobre la base del resultado del proceso de evaluación de las prácticas actuales de una organización que utilice al modelo CMMI para su mejora. Reconoce dos dimensiones o niveles para las actividades del proceso de mejora: el nivel estratégico y el nivel táctico. A su vez consta de cinco fases (McFeeley, 1996):

1. **Iniciación**: Fundamentos para iniciar un proceso de mejoras.
2. **Diagnóstico**: Determinar en donde está la organización y cuál es el estado futuro deseado.
3. **Establecimiento**: Planear, de forma específica, cómo se alcanzará el estado deseado.
4. **Actuación**: Ejecución del trabajo de acuerdo al plan establecido.
5. **L – Aprendizaje**: Formalizar toda la experiencia adquirida para institucionalizar las prácticas.

Identificación del riesgo: Un acercamiento organizado y sistemático para determinar los factores de riesgo asociado con una actividad planeada, proyecto, o programa.

IEEE: Institute of Electrical and Electronics Engineers.

Incertidumbre: Resultado de no tener conocimiento exacto o suficiente de una situación. A menudo la causa de la raíz de un factor de riesgo.

ISO: Organización Internacional para la Estandarización. Es una federación mundial de cuerpos de normas nacionales de aproximadamente 140 países. Es una organización no gubernamental

establecida en 1947. Su misión es promover el desarrollo de la estandarización y de las actividades relacionadas en el mundo, con la idea de facilitar el cambio internacional de bienes y servicios, y la cooperación que se desarrolla en las esferas de la actividad intelectual, la actividad científica, tecnológica y económica (Uch, 2002).

MIC: Ministerio de Informática y Comunicaciones, Cuba.

Mitigación del riesgo: Curso de acciones tomadas para reducir la probabilidad y/o pérdida potencial de un factor de riesgo; incluye la ejecución de planes de contingencia cuando la métrica de un riesgo cruza un umbral predeterminado (cuando un factor de riesgo se convierte en un problema).

Oficina Nacional de Normalización (NC): Es el Organismo Nacional de Normalización de la República de Cuba y representa al país ante las organizaciones internacionales y regionales de Normalización (O. N. Normalización, Cuba, 2000).

Plan de contingencia: Plan para tratar con los factores de riesgo si se convirtieran en un problema.

PMBok (Project Management Body of Knowledge): Metodología de gestión de proyectos de PMI. Es la suma de conocimiento dentro de la profesión de dirección de proyecto (PMI, 2004).

PMI (Project Management Institute): Es una organización mundialmente reconocida (PMI, 2004).

Problema: Una situación negativa a vencer. Un factor de riesgo se vuelve un problema cuando la métrica del riesgo (una medida objetiva) cruza un umbral predeterminado (el que dispara el problema).

Reducción del riesgo: Reducir la probabilidad y/o impacto potencial de un factor de riesgo. La reducción del riesgo podría involucrar la investigación, el prototipo, y otros medios de exploración.

Resolución No. 297/03: Resolución puesta en vigor en Cuba, en el año 2003, por el Ministerio de Finanzas y Precios (MFP). Comprende la definición de Control Interno, el contenido de los componentes y las normas para su implementación y evaluación (del Toro Ríos, 2005).

Riesgo: Es la probabilidad de incurrir en una pérdida o sufrir un impacto negativo. Es sólo una

posibilidad, no la certeza de una pérdida ni un resultado por debajo de lo esperado. También es la probabilidad de aprovechar una oportunidad y obtener un impacto positivo (Maniasi, 2005).

RUP: *Rational Unified Process*. Es un proceso de desarrollo de software dirigido por casos de uso, centrado en la arquitectura, iterativo e incremental (I. Jacobson, 2000).

SEI: Instituto de Ingeniería de Software de los EE.UU (*Software Engineering Institute*). Organismo financiado por el gobierno federal de los EE.UU y operado por la Universidad Carnegie Mellon de ese país. Existe para ayudar a las organizaciones a mejorar el estado de las prácticas de ingeniería, con el fin de incrementar la calidad de los sistemas que dependen del software y la ingeniería de sistemas (Maniasi, 2005).

Seis Sigma: Método estadístico para la mejora de proceso que incluye una filosofía, una medición de la ejecución, un modelo de mejora y un conjunto de herramientas, con el propósito de complementar y mejorar los procesos existentes de ingeniería, servicios y producción. Su filosofía es mejorar la satisfacción del cliente a través de la prevención y eliminación de los errores, obteniéndose como resultado un incremento ventajoso en el negocio (Jeannine Sivi, 2005).

Sistemas heredados (*Legacy Systems*): Sistemas desarrollados que han sido sometidos a la aprobación de usuarios reales con respecto a su funcionalidad conociendo sus necesidades reales. Las propiedades no funcionales como la ejecución y seguridad han sido puestas a punto. El mantenimiento correctivo ha traído como resultado un código "robusto" y una riqueza de pruebas y capacidades de validación. La historia del sistema existe en la forma de diseñadores originales, actuales y en los que han dado mantenimientos al sistema, así como los reportes de errores y registros de órdenes de cambio. En muchos casos, algunas de las causas raíz y sus implicaciones pueden entenderse por algunos expertos, pero no están documentadas y disponibles a la mayoría de ingenieros del software. La información sobre los sistemas es bastante limitada, usualmente el código de fuente y/o ejecutable, un manual de funcionamiento, y las personas que lo mantienen (Feiler, 1993).

SOA (*Services Oriented Architecture*): Arquitectura Orientada a Servicios. Es una vía para diseñar sistemas compuestos de servicios que son invocados de una manera estándar. Es un estilo de arquitectura, no una arquitectura de sistema ni un sistema completo. A un alto nivel, un sistema orientado a servicios está compuesta de Servicios (componentes reusables que representan negocio o tareas de misión), Consumidores de Servicios (clientes para la

funcionalidad suministrada por los servicios) e infraestructura SOA (infraestructura que conecta a los consumidores de servicios con los servicios) (Lewis, 2008).

Software Libre: Software distribuido en código fuente, el cual puede ser libremente modificado y redistribuido (*freely modifiable and redistributable software*). Esto no se refiere a software con costo cero (free-soft.org, 2003).

Taxonomías: Según el diccionario Webster son clasificaciones ordenadas de plantas y animales de acuerdo a sus relaciones naturales presumidas, esta definición suele ser ampliada especificando a las Taxonomías como las clasificaciones ordenadas de elementos de acuerdo a sus relaciones presumidas; así consideradas, puede emplearse a las taxonomías como herramientas de suma utilidad en diferentes ramas de la ciencia y la industria donde se pretende organizar y facilitar el acceso a un número importante de elementos que se encuentran mutuamente relacionados de alguna manera relevante (Maniasi, 2005).

TSP (Team Software Process): Provee un énfasis balanceado del proceso, el producto y el equipo de trabajo, y los capitaliza sobre la base de la experiencia industrial en la planificación y gestión de proyectos de software. Constituye una guía para planificar y gestionar equipos de proyecto (Humphrey, 1999).

Softel: Empresa de software para la Técnica Electrónica, perteneciente al Ministerio de Informática y Comunicaciones (MIC), destinada a la informatización del sector de la salud. Radica dentro de la Universidad de las Ciencias Informáticas (UCI).

Transferir el riesgo: Transferir la responsabilidad de gestionar un factor de riesgo a otra organización o entidad funcional capaz de mitigar el factor de riesgo.

UCI: Universidad de las Ciencias Informáticas, La Habana, Cuba.

Universitat Politècnica de Catalunya (UPC): Institución pública de enseñanza superior cuyos objetivos prioritarios son el estudio, la docencia, la investigación y la transferencia de tecnología de calidad. Uno de sus principales objetivos es transferir los resultados de sus investigaciones a las empresas (Esteves, 2005).

Anexos.**Anexo 1. Encuesta sobre gestión de riesgos.****Encuesta****Introducción:**

El objetivo de esta encuesta consiste en conocer si se aplica algún marco formal o informal para la gestión de riesgos en su organización y en el proyecto en el que trabaja, así como los principales riesgos que ha enfrentado y las medidas que ha aplicado.

Datos generales:

Nombre de su organización: _____ Provincia: _____
Organismo al que pertenece: _____

Tipo de Proyecto en el que participa:

- ___ Gestión empresarial (Directivo de la entidad o miembro de las áreas de gestión: Economía, Capital Humano, Administración u otro)
___ Productivo
 ___ de Desarrollo de Software
 ___ de Implementación de aplicaciones
 ___ Otro: ¿Cuál? _____

Cargo o Rol que desempeña en su organización o proyecto: _____

Desarrollo:

1. ¿Conoce algún marco o proceso para la gestión de riesgos? ¿Cuál(es)?

2. ¿Se aplica en su **organización** algún marco o proceso para la gestión de riesgos?
 - a. ___ Sí
 - b. ___ No
 - c. ___ No sé

Si la respuesta anterior es afirmativa (Sí), responda: el marco o proceso de gestión de riesgos que se aplica ¿es propio de su organización?

- a. ___ Sí
- b. ___ No ¿Cuál es? _____

3. ¿Se aplica en su **proyecto** algún proceso para la gestión de riesgos?
 - a. ___ Sí
 - b. ___ No

Si la respuesta anterior es afirmativa, responda: el proceso de gestión de riesgos que se aplica ¿es propio de su proyecto?

- a. ___ Sí
- b. ___ No ¿Cuál es? _____

4. ¿Se han identificado los riesgos en su proyecto?
 - a. ___ Nunca

- b. Algunas veces
- c. Casi siempre
- d. Siempre
- e. No sé

5. ¿Se han evaluado los riesgos en su proyecto?

- a. Nunca
- b. Algunas veces
- c. Casi siempre
- d. Siempre
- e. No sé

6. ¿Se han aplicado planes de mitigación y/o contingencia a los riesgos identificados en su proyecto?

- a. Nunca
- b. Algunas veces
- c. Casi siempre
- d. Siempre
- e. No sé

7. ¿Se han monitoreado los riesgos en su proyecto?

- a. Nunca
- b. Algunas veces
- c. Casi siempre
- d. Siempre
- e. No sé

8. ¿Cuáles han sido los principales riesgos que han sido identificados y/o han impactado en su proyecto?

9. ¿Qué ha hecho en su proyecto (independientemente de utilizar o no un proceso formal para la gestión de riesgos) que haya contribuido a evitar impactos negativos en el mismo?

Muchas gracias.

Anexo 2. Componentes claves de la Entrevista Apreciativa.

Las mejores preguntas de una entrevista apreciativa son claras, relativamente simples, con frecuencia sutiles y provocativas. Invitan a las personas a contar historias y participar en ese nivel verdaderamente humano. Los componentes claves de las Buenas Preguntas de una Entrevista Apreciativa son (Whitney, 2005):

- ? Ayudan a forjar conexiones personales entre entrevistadores/as y entrevistados/as. Tienen una cualidad conversacional para ellos, valoran lo que es y provocan la imaginación apreciativa. Transportan recuerdos positivos incondicionales.
- ? Buscan historias más que opiniones o teorías abstractas. Son introducidas por frases como “Cuéntame acerca de” y “Descríbeme.”
- ? Son personales y afectivas, casi íntimas. Tocan los corazones y almas de las personas. Le piden a las personas que describan algo con lo que se identifican fuertemente, que recuerden algo o alguien que realmente les importó.
- ? Recurren a la experiencia de vida y trabajo de las personas. Le dan a las personas la oportunidad de aprender y darle sentido a episodios y experiencias que de otra manera podrían haber escapado a su atención.
- ? Invocan un tipo de examen mental. Obligan a pensar en una serie de experiencias o imágenes poderosamente positivas y entonces a elegir la mejor de lo mejor.
- ? Son a veces ambiguas. Le dan espacio a las personas para dar vueltas, para responder de una variedad de formas.
- ? Acompañan a las personas por un viaje interior. Les piden a las personas que interpreten o deconstruyan lo que funcionó o fue significativo en las cosas que pueden haber dado por sentadas.
- ? Son inspiradoras. Delinean panoramas positivos y atractivos. Inspiran a las personas a considerar lo que es posible.
- ? Dan rienda suelta a la imaginación. Llevan a las personas lejos en el futuro y las ayudan a imaginar infinitas posibilidades positivas.
- ? Sugieren acción. Ayudan a las personas a considerar pasos próximos inmediatos que comenzarían a moverlos hacia sus sueños.
- ? Tienen un flujo emocional y lógico. En la medida que una Guía de Entrevista pasa de una pregunta a otra, las personas son inspiradas a encontrar significados más y más profundos; a volverse cada vez más animadas e inspiradas.

Anexo 3. Entrevista Apreciativa.

Guía para la entrevista

Nombre del entrevistado: _____

Institución: _____

Cargo o rol que desempeña: _____

Fecha: _____

Introducción.

Gracias por acceder a ser entrevistado. Antes de comenzar, déjame dedicar unos minutos a compartir contigo lo que estamos haciendo con esta entrevista y por qué.

Queremos definir e implementar en Softel un proceso de gestión de riesgos acorde con nuestro nivel de madurez y que pueda servir para perfeccionar nuestro trabajo y resultados. El mismo deberá seguir mejorando en la medida en que vayamos madurando este proceso en la organización. La experiencia que obtengamos pudiera contribuir al desarrollo y perfeccionamiento de la industria cubana del software, más allá de Softel.

Quisiera, además, compartir dos conceptos que se aplican muchas veces, aunque en ocasiones de forma intuitiva: los conceptos de **riesgo** y **gestión de riesgos**. El **riesgo** es la exposición a una pérdida debido a que se pretende considerar no sólo la posibilidad de ocurrencia de un riesgo, sino también su impacto asociado. La **Gestión de Riesgos** es el proceso formal en el que los factores de riesgos son sistemáticamente identificados, evaluados y mitigados. Esta actividad se inicia en la primera etapa de un proyecto de software (durante la exploración de conceptos) y se desarrolla a lo largo de todo su ciclo de vida (hasta la aceptación del producto del proyecto). La Gestión de Riesgos ayuda a evitar desastres, re-trabajo y sobre-trabajo, pero aún más importante, estimula la generación de situaciones del tipo ganar-ganar.

Las preguntas que voy a hacerle se llaman preguntas apreciativas porque tratan de encontrar lo que ha funcionado o funciona – los éxitos – de manera que podamos descubrir el por qué y cómo mejorar a partir de ello. Comienzan con momentos en los que ha tenido una vivencia importante que funcionó muy bien. Este camino se diferencia del habitual de preguntar acerca de las cosas que no están funcionando bien – los problemas –. Aspiramos a la búsqueda de las principales causas de desarrollo, que minimicen entonces la ocurrencia de problemas.

Así que le agradecería la inversión de su tiempo en pensar, recordar y contar detalles de momentos, situaciones vistas, escuchadas, experimentadas o imaginadas vinculadas con riesgos y su gestión.

Preguntas.

1. Imagina una experiencia de su vida en la que previó algo que podía haber afectado su proyecto y con ello logró salvarlo de un resultado negativo o una pérdida.
 - a. Rememórela y cuénteme todo lo relacionado con ella.
 - b. ¿Qué papel desempeñó?
 - c. ¿Cómo le vieron los demás? ¿Se sumó la mayoría?

- d. ¿Cómo se sintió?
 - e. ¿Logró llevar estas experiencias a otras situaciones similares?
2. Imagine que está ahora en el mejor momento de su proyecto, que ha alcanzado el sueño que se propuso. El proyecto en el que trabajó identificó y evaluó los riesgos que podían afectar su éxito y lo hizo de manera muy efectiva. Además, logró monitorearlos sistemáticamente y los mitigó, transfiriendo a otros los que era posible evitarle al proyecto y creó planes de contingencia efectivos para recuperarse de los riesgos que fueron previstos y se produjeron. En ese sueño, dígame:
- a. ¿Cómo se sintió en el proyecto?
 - b. ¿Cómo se sintieron los demás miembros del proyecto?
 - c. ¿Desde el rol que desempeñó se sintió parte del proceso?
3. Piense ahora en lo que ha tenido que hacer para alcanzar ese sueño.
- a. ¿Cuáles son los riesgos que logró mitigar y/o enfrentar de acuerdo con las contingencias previstas?
 - b. Dígame algunas medidas para mitigar los riesgos y tareas concretas que se pueden aplicar para alcanzar el éxito.
 - c. ¿Cómo actuó en el logro de este resultado?
 - d. ¿Cuáles otras cosas cree que podría hacer en una situación similar?

Muchas gracias por su tiempo y compartir pensamientos y sentimientos conmigo.

Anexo 4. Plantilla del Plan de Gestión de Riesgos (DG-32.01).

A continuación se muestra la plantilla, casi completa, del Plan de Gestión de Riesgos (DG-32.01) propuesta como resultado del proceso de gestión de riesgos definido para Softel.

HOJA __ DE __	Plan de Gestión de Riesgos	
REVISION __	Proyecto: [Nombre del Proyecto]	
DG-32.01		

1. Objeto.

Describir cómo se estructurará y realizará la gestión de riesgos.

2. Alcance.

Describir cómo se estructurará y realizará la gestión de riesgos en el proyecto.

3. Plan de Gestión de Riesgos

3.1. Metodología.

[Definir los métodos, las herramientas y las fuentes de información que pueden utilizarse para realizar la gestión de riesgos en el proyecto.]

Proceso	Fuentes de información	Herramientas y Técnicas
Planificación de la Gestión de Riesgos	<ol style="list-style-type: none"> 4. Factores ambientales de la organización. 5. Activos de los procesos de la organización. 6. Enunciado del alcance del proyecto. 7. Plan de gestión del proyecto. 	<ol style="list-style-type: none"> 1. Reuniones y análisis de planificación.
Identificación de los Riesgos	<ol style="list-style-type: none"> 1. Factores ambientales de la organización. 2. Activos de los procesos de la organización. 3. Enunciado del alcance del proyecto. 4. Plan de gestión de riesgos. 5. Plan de gestión del proyecto. 	<ol style="list-style-type: none"> 1. Revisiones de documentación. 2. Técnicas de recopilación de información: Tormenta de Ideas, Entrevistas, Técnica Delphi, Técnica de Grupo Nominal, Identificación de la causa, Análisis DAFO 3. Análisis de lista de chequeo 4. Análisis de asunciones 5. Técnicas de diagramación: Diagramas de causa y efecto (Ishikawa o de espina de pescado), Diagramas de flujo o de sistemas, Diagramas de influencias.
Análisis de Riesgos	<ol style="list-style-type: none"> 1. Activos de los procesos de la organización. 2. Enunciado del alcance del proyecto. 3. Plan de gestión de riesgos. 4. Registro de riesgos. 	<ol style="list-style-type: none"> 1. Evaluación de probabilidad e impacto de los riesgos. 2. Matriz de probabilidad e impacto. 3. Evaluación de la calidad de los datos sobre riesgos. 4. Categorización de los riesgos. 5. Evaluación de la urgencia del riesgo.

Planificación de la Respuesta a los Riesgos	<ol style="list-style-type: none"> 1. Plan de gestión de riesgos. 2. Registro de riesgos. 	<ol style="list-style-type: none"> 1. Estrategias para riesgos negativos o amenazas. 2. Estrategias para riesgos positivos u oportunidades. 3. Estrategia común ante amenazas y oportunidades. 4. Estrategia de respuesta para contingencias. 5. Evaluación de la urgencia del riesgo.
Seguimiento y Control de Riesgos	<ol style="list-style-type: none"> 1. Plan de gestión de riesgos. 2. Registro de riesgos. 3. Solicitudes de cambio aprobadas. 4. Información sobre el rendimiento del trabajo. 	<ol style="list-style-type: none"> 1. Reevaluación de los riesgos. 2. Auditorías de los riesgos. 3. Reuniones sobre el estado de la situación.

3.2. Roles y responsabilidades.

[Definir el líder, el apoyo y los miembros del equipo de gestión de riesgos para cada tipo de actividad del plan de gestión de riesgos, asignar personas a estos roles y explicar sus responsabilidades.]

No	Rol	Responsabilidad	Miembro del equipo responsable
1	Gestor de Riesgos	Responsable por llevar a cabo el proceso de gestión de riesgos.	
2	Jefe de Proyecto	Responsable por hacer cumplir las tareas de gestión de riesgos planificadas.	

3.3. Periodicidad.

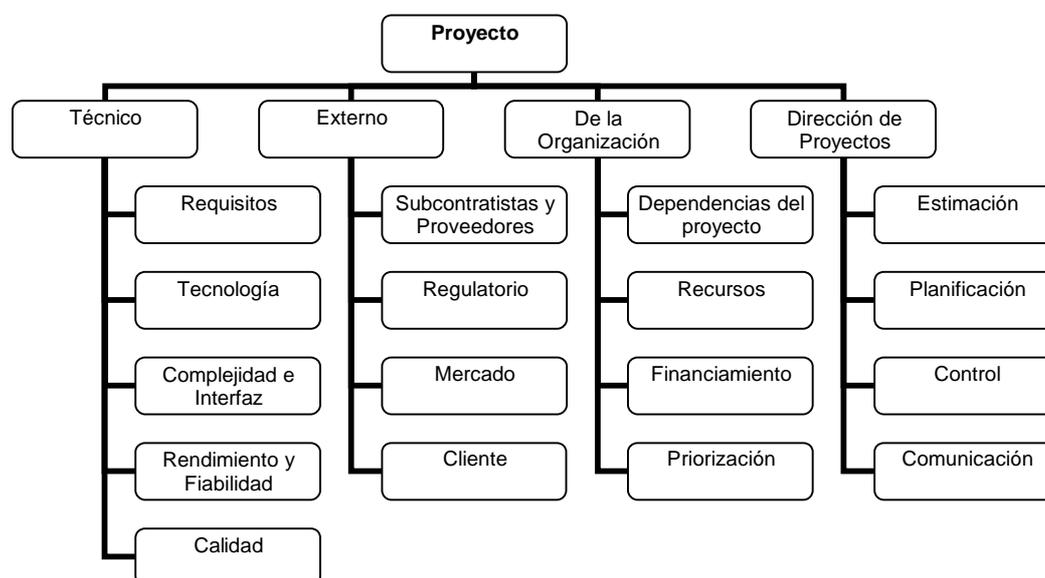
[Define cuándo y con qué frecuencia se realizará el proceso de gestión de riesgos durante el ciclo de vida del proyecto, y establece las actividades de gestión de riesgos que se incluirán en el cronograma del proyecto]

No	Actividad	Ocurrencia	Frecuencia
1	Identificación de Riesgos	Al inicio del proyecto	1 vez
		Cuando ocurren cambios que pueden impactar en los riesgos del proyecto.	Cuando ocurren cambios que impactan
2	Análisis de Riesgos	Al finalizar la identificación de riesgos.	Mensual
		Cuando hay cambios en la probabilidad o impacto de alguno de los riesgos.	Cuando ocurren cambios que impactan
		Cuando se dispara algún riesgo.	Cuando se dispara algún riesgo.
3	Planificación de la Respuesta a los Riesgos	Cuando concluye el proceso de Análisis de riesgos	Mensual
		Cuando se necesitan elaborar respuestas a corto plazo.	Cuando se necesitan elaborar respuestas a corto plazo.
		Cuando se necesitan elaborar respuestas adicionales.	Cuando se necesitan elaborar respuestas adicionales.
		Cuando se dispara algún riesgo.	Cuando se dispara algún

			<i>riesgo.</i>
4	<i>Seguimiento y Control de Riesgos</i>		

3.4. Categorías de riesgo.

[Proporciona una estructura que garantiza un proceso completo de identificación sistemática de los riesgos con un nivel de detalle uniforme, y contribuye a la efectividad y calidad de la Identificación de Riesgos. La estructura de desglose del riesgo (EDR) es uno de los métodos para proporcionar dicha estructura, pero también se puede utilizar un listado de los diversos aspectos del proyecto. Las categorías de riesgo pueden revisarse durante el proceso Identificación de Riesgos. Una buena práctica es revisar las categorías de riesgo durante el proceso Planificación de la Gestión de Riesgos antes de usarlas en el proceso Identificación de Riesgos. Es posible que sea necesario adaptar, ajustar o extender las categorías de riesgo basadas en proyectos anteriores a las nuevas situaciones, antes de que dichas categorías puedan utilizarse en el proyecto actual. Se pueden aplicar Taxonomías de Riesgos. Por ejemplo, la Taxonomía Ajustada de Maniasi.]



Se aplicará la Taxonomía Ajustada de Maniasi, la cual se aplicará en documento anexo (Fichero Excel).

No	Categoría	Subcategoría
1	<i>Misión y objetivos</i>	
2	<i>Administración del Programa</i>	
3	<i>Conductores para la Toma de Decisiones</i>	
4	<i>Gerenciamiento Organizacional</i>	
5	<i>Clientes/Usuarios</i>	
6	<i>Parámetros del Proyecto</i>	
7	<i>Ingeniería del Producto</i>	<i>Requerimientos</i>
		<i>Diseño</i>
		<i>Código y Pruebas Unitarias</i>
		<i>Integración y Pruebas</i>
		<i>Requerimientos de Calidad</i>

8	Instalación	
9	Proceso de Desarrollo	
10	Entorno de Desarrollo	
11	Administración de Proyectos	
12	Equipo de Proyecto	
13	Tecnología	
14	Mantenimiento	

3.5. Definiciones de probabilidad e impacto de los riesgos.

Probabilidad	
Valor cualitativo	Valor cuantitativo
Muy Baja	0.1
Baja	0.3
Moderada	0.5
Significativa	0.7
Alta	0.9

Impacto	
Valor cualitativo	Valor cuantitativo
Insignificante	0.1
Bajo	0.3
Tolerable	0.5
Serio	0.7
Catastrófico	0.9

[Se pueden definir condiciones para escalas de impacto de un riesgo sobre los principales objetivos del proyecto. El siguiente ejemplo muestra definiciones que se pudieran utilizar para impactos negativos. Se pueden preparar también para las oportunidades.]

3.6. Método utilizado para priorizar los riesgos.

[Los riesgos se priorizan según sus posibles implicaciones para lograr los objetivos del proyecto. El método típico para priorizar los riesgos es utilizar una tabla de búsqueda o una Matriz de Probabilidad e Impacto. La organización suele establecer las combinaciones específicas de probabilidad e impacto que llevan a que un riesgo sea calificado como de importancia o magnitud "Alta" (gris oscuro), "Moderada" (gris claro) o "Baja" (gris intermedio), con la correspondiente importancia para planificar respuestas al riesgo. Se revisan y se pueden adaptar para el proyecto específico durante el proceso Planificación de la Gestión de Riesgos]

El Método a utilizar para priorizar los riesgos del proyecto es la Matriz de probabilidad e impacto.

Riesgo (Amenaza)

Probabilidad	0.9				
	0.7				
	0.5				
	0.3				
	0.1				
	0.1	0.3	0.5	0.7	0.9
	Impacto				

Magnitud o Importancia		
Valor cualitativo	Valor Leyenda	Acción
Alta	Gris oscuro	Mitigar
Moderada	Gris claro	Aceptar
Baja	Gris intermedio	Documentar

Riesgo (Oportunidad)

Probabilidad	0.9				
	0.7				
	0.5				

Magnitud o Importancia		
Valor cualitativo	Valor Leyenda	Acción
Alta	Gris oscuro	Explotar / Compartir

0.3						<i>Moderada</i>	<i>Gris claro</i>	<i>Mejorar</i>
0.1						<i>Baja</i>	<i>Gris intermedio</i>	<i>Aceptar</i>
	0.9	0.7	0.5	0.3	0.1			

Impacto

3.7. Formatos de informe.

[Describir el contenido y el formato del registro de riesgos, así como de cualquier otro informe de riesgos que se requiera. Definir cómo se documentarán, analizarán y comunicarán los resultados de los procesos de gestión de riesgos]

- ? **Registro de Riesgos (DG-32.00):** Contiene el registro de riesgos según el formato de la plantilla DG-32.02: Registro de Riesgos.
- ? La Comunicación de los resultados de los procesos de gestión de riesgos **se realizará a través de la carpeta compartida en la Intranet de la empresa...**

3.8. Seguimiento.

[Documentar cómo serán registradas todas las facetas de las actividades de riesgo para beneficio del proyecto actual, para futuras necesidades y para las lecciones aprendidas. Documentar si serán auditados los procesos de gestión de riesgos y cómo se realizaría dicha auditoría]

Anexo 5. Plantilla del Registro de Riesgos (DG-32.02).

HOJA ___ DE ___	Registro de Riesgos	
REVISION ___	Proyecto: [Nombre del Proyecto]	
DG-32.02		

1. Objeto.

Mantener actualizado el Registro de Riesgos del proyecto a partir de la implementación del proceso DG-32.00: Proceso de Gestión de Riesgos, describiendo con exactitud los riesgos e inconvenientes que se tienen al momento de desarrollar un proyecto, con el propósito de darle seguimiento a cada uno de ellos y su posible impacto en el proyecto.

2. Alcance.

Riesgos asociados al proyecto: **[Nombre del Proyecto]**, teniendo en cuenta lo planificado en el documento DG-32.01: Plan de Gestión de Riesgos para este proyecto.

3. Definiciones, Acrónimos y Abreviaciones.

[Describir todas las definiciones, acrónimos y abreviaturas que son empleadas en el documento]

4. Referencias.

1. DG-32.00: Proceso de Gestión de Riesgos.
2. DG-32.01: Plan de Gestión de Riesgos.

[Adicionar otros documentos referenciados.

Ejemplo Documentos de casos de uso, Documento de requerimiento]

5. Lista de prioridades o clasificaciones relativas de los riesgos del proyecto.

Lista de riesgos ordenada por prioridad de acuerdo a la magnitud del riesgo, determinada a partir de la probabilidad, el impacto y su severidad. Durante el proceso de Identificación de riesgos se puede utilizar esta tabla aunque todavía no esté ordenada por prioridad:

Prioridad	Identificador del Riesgo	Nombre del Riesgo	Probabilidad	Impacto	Severidad (Probabilidad x Impacto)	Categoría

6. Lista de Riesgos agrupados por Categorías.

[Los Riesgos agrupados por categorías para descubrir las concentraciones de riesgos, puede mejorar la efectividad de las respuestas a los riesgos. Es la misma lista obtenida en el punto anterior "Lista de prioridades o clasificaciones relativas de los riesgos del proyecto" pero ordenada por categorías.]

Cate- goría	Id. del Riesgo	Nombre del Riesgo	Proba- bilidad	Impacto	Prioridad	¿Respu- est a a corto plazo?	¿Análisis y respuesta adicionales?

7. Caracterización de los Riesgos.

En el Plan de Gestión de Riesgos del proyecto (DG-32.01) se definió cómo se estructurará y realizará la gestión de riesgos en el proyecto, así como la metodología, roles y responsabilidades, periodicidad, la Estructura de Desglose del Riesgo (categorías de riesgo) a utilizar, definiciones de probabilidad e impacto y demás elementos que serán tenidos en cuenta para obtener y mantener actualizado el Registro de Riesgos del proyecto. A continuación se describen todos los riesgos del proyecto con sus características.

Riesgo 1 (Clasificación del riesgo).

Magnitud del Riesgo	<i>[Se especifica un indicador de la magnitud del Riesgo en cuanto a la gravedad de la ocurrencia del mismo. Se obtiene a partir de la evaluación de la exposición al riesgo (Exposición = Probabilidad x Impacto) empleando la Matriz de Probabilidad e Impacto. Puede ser:]</i> Alta, Moderada, Baja														
Identificador del Riesgo	<i>[Número consecutivo que se le asigna al riesgo identificado para facilitar su referencia]</i>														
Nombre del Riesgo	<i>[Nombre abreviado del riesgo]</i>														
Descripción del Riesgo	<i>[Se brinda una breve descripción del Riesgo identificado.]</i>														
Categoría del Riesgo	<i>[Los riesgos del proyecto pueden categorizarse por fuentes de riesgo (por ejemplo, usando la Estructura Desglosada de Riesgos (EDR), área del proyecto afectada u otra categoría útil para determinar las áreas del proyecto que están más expuestas a los efectos de la incertidumbre. Agrupar los riesgos por causas comunes puede contribuir a desarrollar respuestas efectivas a los riesgos)]</i>														
Fecha de detección	<i>[Fecha en que fue identificado.]</i>														
Causa y efecto del Riesgo	<i>[Descripción de la causa que lo provoca y el efecto que puede provocar su ocurrencia.]</i>														
Probabilidad de Ocurrencia	<p><i>[Se especifica una estimación de la probabilidad de ocurrencia del Riesgo, por ejemplo se puede utilizar la escala que se muestra en la tabla.</i></p> <table border="1"> <thead> <tr> <th colspan="2">Probabilidad</th> </tr> <tr> <th>Valor cualitativo</th> <th>Valor cuantitativo</th> </tr> </thead> <tbody> <tr> <td>Muy Baja</td> <td>0.1</td> </tr> <tr> <td>Baja</td> <td>0.3</td> </tr> <tr> <td>Moderada</td> <td>0.5</td> </tr> <tr> <td>Significativa</td> <td>0.7</td> </tr> <tr> <td>Alta</td> <td>0.9</td> </tr> </tbody> </table> <p><i>La escala a utilizar se debe definir en el Plan de Gestión de Riesgos del proyecto (DG-32.01).]</i></p>	Probabilidad		Valor cualitativo	Valor cuantitativo	Muy Baja	0.1	Baja	0.3	Moderada	0.5	Significativa	0.7	Alta	0.9
Probabilidad															
Valor cualitativo	Valor cuantitativo														
Muy Baja	0.1														
Baja	0.3														
Moderada	0.5														
Significativa	0.7														
Alta	0.9														
Impacto	<p><i>[Se especifica una estimación del impacto de la ocurrencia del Riesgo en el proyecto, por ejemplo utilizando la misma escala que en el punto anterior. Escoger uno de los siguientes:</i></p> <table border="1"> <thead> <tr> <th colspan="2">Impacto</th> </tr> <tr> <th>Valor cualitativo</th> <th>Valor cuantitativo</th> </tr> </thead> <tbody> <tr> <td>Insignificante</td> <td>0.1</td> </tr> <tr> <td>Bajo</td> <td>0.3</td> </tr> <tr> <td>Tolerable</td> <td>0.5</td> </tr> <tr> <td>Serio</td> <td>0.7</td> </tr> <tr> <td>Catastrófico</td> <td>0.9</td> </tr> </tbody> </table> <p><i>La escala a utilizar se debe definir en el Plan de Gestión de Riesgos del proyecto (DG-32.01).]</i></p>	Impacto		Valor cualitativo	Valor cuantitativo	Insignificante	0.1	Bajo	0.3	Tolerable	0.5	Serio	0.7	Catastrófico	0.9
Impacto															
Valor cualitativo	Valor cuantitativo														
Insignificante	0.1														
Bajo	0.3														
Tolerable	0.5														
Serio	0.7														
Catastrófico	0.9														

Fechas en que puede afectar	<i>[Se especifican las fechas en las que el riesgo pudiera afectar]</i>	
Propietario del riesgo y responsabilidades asignadas	<i>[Indicar el propietario del riesgo y las responsabilidades asignadas]</i>	
Indicadores y Disparadores	<i>[Se describe como se realizará el monitoreo y la detección de la ocurrencia o posibilidad de ocurrencia de los Riesgos identificados, incluyendo por ejemplo eventos específicos que los pudieran disparar.]</i>	
Estrategia de respuesta acordada	___ Aceptar	
	___ Negativo o Amenaza ___ Evitar ___ Transferir ___ Mitigar	___ Positivo u Oportunidades ___ Explotar ___ Compartir ___ Mejorar
Estrategia para Mitigarlo / Potenciarlo	<i>[Se describen las decisiones tomadas y las acciones previstas por el equipo para reducir la probabilidad de ocurrencia del Riesgo en el proyecto (en el caso de riesgos negativos o amenazas) o aumentar la probabilidad de ocurrencia y el impacto (en el caso de riesgos positivos u oportunidades). Se puede inicializar en la etapa de Identificación de Riesgos como posibles respuestas que pueden ser útiles como entradas al proceso Planificación de la Respuesta a los Riesgos]</i>	
Plan de Contingencia	<i>[Se describen las acciones que tomará el equipo en el caso que el Riesgo identificado se presente, como por ejemplo dar una solución alternativa, establecer reducción en la funcionalidad del Sistema, etc.]</i>	

...

Riesgo n (Clasificación del riesgo).

...

8. Plan de Acción para implementar las estrategias de respuesta.

[Reflejar las acciones que fueron determinadas para implementar la estrategia de respuesta seleccionada para cada riesgo, especificando Responsable, Ejecutantes y Fecha de cumplimiento]

Id.	Nombre del Riesgo	Medidas o acciones a tomar	Responsable	Ejecutantes	Fecha de cumplimiento

9. Lista de supervisión de riesgos de baja prioridad.

[Reflejar los riesgos que no fueron evaluados como importantes en el proceso Análisis de Riesgos para su seguimiento continuo]

Categoría	Identificador del Riesgo	Nombre del Riesgo	Probabilidad	Impacto

10. Estado actual.

Riesgo	Estado actual	Impacto
<i>[Riesgo 1</i>	<i>Nuevo</i>	<i>Alto</i>
<i>...</i>	<i>Superado</i>	<i>Alto</i>
<i>...</i>	<i>Vigente</i>	<i>Bajo</i>
<i>Riesgo n</i>	<i>Vigente</i>	<i>Bajo]</i>

[Es estado actual del riesgo puede tomar uno de los siguientes valores:]

Nombre del estado	Definición
<i>Nuevo</i>	<i>Nuevo riesgo.</i>
<i>Abierto</i>	<i>Riesgo aceptado y asignado.</i>
<i>Cancelado</i>	<i>Un riesgo que ha dejado de ser verificado por el proyecto.</i>
<i>Plan Creado</i>	<i>El plan para el riesgo ha sido creado y se encuentra pendiente de aprobación.</i>
<i>Plan Aprobado</i>	<i>El plan para el riesgo ha sido aprobado y se encuentra en condiciones de ser ejecutado.</i>
<i>Plan – Verde</i>	<i>El plan se está ejecutando según lo planificado.</i>
<i>Plan – Amarillo</i>	<i>El plan se está ejecutando con leves diferencias respecto a lo planificado.</i>
<i>Plan – Rojo</i>	<i>El plan se está ejecutando con severas diferencias respecto a lo planificado.</i>
<i>Plan completo</i>	<i>El plan se ha ejecutado por completo y se encuentra pendiente la verificación de sus resultados.</i>
<i>Completado</i>	<i>El plan ejecutado ha sido verificado y sus resultados se consideran apropiados.</i>
<i>Re-Abierto</i>	<i>El plan ejecutado ha sido verificado y sus resultados no se consideran apropiados por lo cual se solicita una nueva ejecución del ciclo de vida o proceso del riesgo.</i>
<i>Completo, luego de Re-Abierto</i>	<i>El plan ejecutado ha sido verificado y sus resultados se consideran apropiados.</i>

11. Resultados de las reevaluaciones, auditorías y revisiones periódicas de los riesgos.

[Resultados de las reevaluaciones, auditorías y revisiones periódicas de los riesgos. Estos resultados pueden incluir actualizaciones de la probabilidad, impacto, prioridad, planes de respuesta, propiedad y otros elementos del registro de riesgos. Los resultados también pueden incluir cerrar los riesgos que ya no sean aplicables]

12. Resultados reales de los riesgos del proyecto y de las respuestas a los riesgos.

[Resultados reales de los riesgos del proyecto, y de las respuestas a los riesgos que pueden ayudar a los Gestores de Riesgo y Jefes de proyecto en la planificación de riesgos para toda la organización, así como en proyectos futuros.]

Anexo 6. Cuestionario para asignación de peso a los criterios.

Cuestionario.

Introducción:

Debido a su experiencia en la gestión de proyectos, el rol que desempeña en la empresa y las vivencias que ha tenido en el proceso de gestión de riesgos, usted ha sido seleccionado como experto para la evaluación del Proceso de Gestión de Riesgos definido para los proyectos de desarrollo de software de Softel. El objetivo del cuestionario consiste en llegar a un consenso entre un grupo de integrantes de la empresa, sobre los criterios que se deben tener en cuenta para la evaluación del proceso y el peso de cada uno de los grupos de criterios para, posteriormente, realizar la evaluación. La información que suministre será manejada de forma anónima.

Desarrollo:

Usted debe asignarle el peso que considere le debe corresponder a cada criterio teniendo en cuenta que la suma de los pesos dentro de un mismo grupo no puede sobrepasar el valor del establecido para dicho grupo. Por ejemplo, el grupo G1: Criterios de implantación tiene un peso de 40 y está compuesto por 4 criterios. La suma de los pesos asignados a cada criterio debe ser exactamente igual a 40.

Los grupos definidos, sus pesos y criterios se representan en la tabla para que usted coloque el peso que considere debe tener cada uno:

Criterios de implantación			40
G1	C1	Necesidad del empleo del proceso	
	C2	Conocimiento del proceso propuesto	
	C3	Satisfacción de las necesidades de la producción	
	C4	Garantía de principios básicos de la gestión de proyectos	
Criterios de generalización			35
G2	C5	Facilidad de comprensión	
	C6	Disponibilidad de documentación para su estudio	
	C7	Facilidad de uso	
	C8	Adaptabilidad a diferentes proyectos y áreas de la empresa	
Criterios de impacto			25
G3	C9	Contribución al cumplimiento del Componente Evaluación de Riesgos de la Resolución 297/03 del MFP	
	C10	Contribución al desarrollo de la Gestión de Proyectos	
	C11	Contribución al fortalecimiento de la Comunicación Organizacional	

Muchas gracias.

Anexo 7. Cuestionario para la evaluación cuantitativa y cualitativa del proceso definido.

Cuestionario.

Introducción:

Debido a su experiencia en la gestión de proyectos, el rol que desempeña en la empresa y las vivencias que ha tenido en el proceso de gestión de riesgos, usted ha sido seleccionado como experto para la evaluación del Proceso de Gestión de Riesgos definido para los proyectos de desarrollo de software de Softel. El objetivo del cuestionario es evaluar dicho proceso por los criterios que se exponen. La información que suministre será manejada de forma anónima.

Desarrollo:

A cada criterio de la tabla le debe asignar una evaluación utilizando un rango de valores de 1 a 5 de acuerdo a la leyenda:

Valor Cuantitativo	Valor Cualitativo
1	Malo
2	Cuestionable
3	Aceptable
4	Bueno
5	Excelente

Criterios		Evaluación (1 a 5)
G1: Criterios de implantación		
C1	Necesidad del empleo del proceso	
C2	Conocimiento del proceso propuesto	
C3	Satisfacción de las necesidades de la producción	
C4	Garantía de principios básicos de la gestión de proyectos	
G2: Criterios de generalización		
C5	Facilidad de comprensión	
C6	Disponibilidad de documentación para su estudio	
C7	Facilidad de uso, disponibilidad de plantillas	
C8	Adaptabilidad a diferentes proyectos y áreas de la empresa	
G3: Criterios de impacto		
C9	Contribución al cumplimiento del Componente Evaluación de Riesgos de la Resolución 297/03 del MFP	
C10	Contribución al desarrollo de la disciplina de Gestión de Proyectos	
C11	Contribución al fortalecimiento de la Comunicación Organizacional	

Criterio sobre la evaluación final del proceso (De 1 a 5): _____

Muchas gracias.