RISK IT COMO COMPLEMENTO A LA GESTIÓN DE RIESGOS EN COMPAÑÍAS DE LA INDUSTRIA DE SOFTWARE

JOHN JAIRO MONTENEGRO HOYOS
MARIELA CECILIA RIVERA RESTREPO

FACULTAD DE INGENIERÍA
DEPARTAMENTO ACADÉMICO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES
MAESTRÍA EN GESTIÓN DE INFORMÁTICA Y TELECOMUNICACIONES
SANTIAGO DE CALI
2011

RISK IT COMO COMPLEMENTO A LA GESTIÓN DE RIESGOS EN COMPAÑÍAS DE LA INDUSTRIA DE SOFTWARE

JOHN JAIRO MONTENEGRO HOYOS
MARIELA CECILIA RIVERA RESTREPO

Trabajo de Grado para optar al título de Magister en Gestión de Informática y Telecomunicaciones con énfasis en Gerencia de Tecnologías de Información y Telecomunicaciones

Director
Msc. LILIANA GÓMEZ

FACULTAD DE INGENIERÍA
DEPARTAMENTO ACADÉMICO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES
MAESTRÍA EN GESTIÓN DE INFORMÁTICA Y TELECOMUNICACIONES
SANTIAGO DE CALI
2011

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Santiago de Cali, 11 de Diciembre de 2011

A Dios por darnos la vida, por brindarnos la oportunidad de seguir cosechando logros y por iluminarnos el camino cuando más lo necesitamos.

John Jairo: Dedico este trabajo a mi madre por ser mi guía constante, por su lucha incansable para darme ejemplo, amor y valores durante toda mi vida, siendo mi soporte para no desfallecer ante las adversidades. A mi padre por su apoyo incondicional y ofrecerme todo lo que estuviera a su alcance para darme la oportunidad de llegar hasta aquí.

Mariela: Dedico este trabajo a mis padres, a mis hermanas y a mi futuro esposo, pues sin esperar nada a cambio, me acompañan día a día con amor, fortaleza y alegría en mi camino a ser una mejor persona y una mejor profesional. Este es un paso más y cuento con la fortuna de compartirlo con estas personas tan maravillosas en mi vida.

AGRADECIMIENTOS

Mariela: Agradezco a mis padres, a mis hermanas y a mi futuro esposo, por su apoyo y compañía en los retos que afronto en todos los ámbitos, siempre ahí, a mi lado. También a todas las personas que han creído en mí y me han brindado su apoyo

John Jairo: Agradezco a mis padres por su esfuerzo y dedicación para darme siempre lo mejor, a mis hermanos por su apoyo incondicional y a todas las personas que me brindaron su apoyo y confianza para culminar con éxito esta etapa de mi vida.

Agradecemos a Liliana Gómez por ayudarnos a encontrar el camino hacia nuestros objetivos y por asesorarnos oportunamente.

A nuestros compañeros del grupo de estudio TIMO, por su amistad sincera y por las experiencias compartidas en el transcurso de la carrera.

CONTENIDO

pág.

LISTA DE CUADROS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

RESUMEN

Los modelos de mejora como el CMMI* que se usan de referente para la definición y mejora de los procesos de desarrollo/mantenimiento de software, aportan el QUÉ, es decir, el alcance de las prácticas, sin embargo no aportan herramientas útiles y tangibles que permitan a las empresas traducir estas recomendaciones en actividades específicas para decidir CÓMO llevar a cabo esos procesos.

Como propuesta para cubrir esta brecha, ISACA** en diciembre del 2009, propone un nuevo marco de referencia denominado RISK IT. Este marco de referencia brinda una guía para realizar la gestión de riesgos ampliando la visión de este proceso a un contexto más extenso basándose en el valor y en los beneficios que la organización obtiene a través de las iniciativas de TI.

En este documento se propone RISK IT como complemento a la gestión de riesgos establecida por el área de procesos RSKM del modelo CMMI, brindando a las empresas un conjunto de actividades resultantes de la alineación de las mejores prácticas de ambos frentes, permitiendo así llevar las practicas de RSKM a actividades específicas establecidas por RISKT IT.

Adicionalmente, se propone una definición de roles por actividad que, partiendo de la alineación realizada, permite determinar los participantes y responsables de cada una de las actividades del proceso de gestión de riesgos, logrando así que la organización asigné los recursos adecuados para reforzar aspectos puntuales del proceso.

---

* Capability Maturity Model Integration.

** ISACA Information Systems Audit & Control Association. Asociación de miembros profesionales, independientes y sin ánimo de lucro comprometidos con la elaboración, adopción y uso del conocimiento y las prácticas mundialmente aceptadas para los sistemas de información.

1. INTRODUCCIÓN

1.1 CONTEXTO DE TRABAJO

La industria del software se ha visto en la necesidad de adoptar diversos modelos y/o estándares de referencia que orienten a las empresas en la definición de procesos para fortalecer capacidades, desarrollar madurez y garantizar resultados de mejor calidad, generando incluso reconocimiento a nivel global en un mercado que se hace cada vez más competitivo y exigente.

Como lo muestra el Cuadro 1, uno de los modelos de madurez que han adoptado las empresas a nivel mundial es el modelo CMMI, al cual la industria del software en Colombia también se ha unido de manera creciente como estrategia en búsqueda de posicionamiento, como medio para obtener competitividad y como mecanismo para aumentar la eficiencia en la productividad de las empresas y disminución en los riesgos de TI.

(Ver Cuadro 1, página siguiente).

Cuadro 1**.** Empresas valoradas CMMI y niveles de madurez reportados al Software Engineering Institute por país.

Country	Number of Appraisals	Maturity Level 1 Reported	Maturity Level 2 Reported	Maturity Level 3 Reported	Maturity Level 4 Reported	Maturity Level 5 Reported	Country	Number of Appraisals	Maturity Level 1 Reported	Maturity Level 2 Reported	Maturity Level 3 Reported	Maturity Level 4 Reported	Maturity Level 5 Reported
Argentina	92		56	26	2	4	Macedonia	10 or fewer					
Australia	39	1	10	7	2	4	Malaysia	81		23	52		6
Austria	10 or fewer						Mauritius	10 or fewer					
Bahrain	10 or fewer						Mexico	115		50	50	4	9
Bangladesh	10 or fewer						Morocco	10 or fewer					
Belarus	10 or fewer						Nepal	10 or fewer					
Belgium	10 or fewer						Netherlands	15		5	7		1
Brazil	181	1	95	68	1	13	New Zealand	10 or fewer					
Brunei Darussalam	10 or fewer						Norway	10 or fewer					
Bulgaria	10 or fewer						Pakistan	31	1	23	4		2
Canada	65	1	17	27	5	4	Panama	10 or fewer					
Chile	45		27	15		2	Paraguay	10 or fewer					
China	1729	1	147	1436	56	64	Peru	16		7	8		
Colombia	51		20	16	4	4	Philippines	29		3	13	1	10
Costa Rica	10 or fewer						Poland	10 or fewer					
Czech Republic	10 or fewer						Portugal	16		6	8		1
Denmark	10 or fewer						Qatar	10 or fewer					
Dominican Republic	10 or fewer						Romania	10 or fewer					
Egypt	57	1	27	21	2	3	Russia	12			3	3	5
Finland	10 or fewer						Saudi Arabia	10 or fewer					
France	194	4	113	61	1	3	Singapore	24		5	13	1	4
Germany	89	9	40	20	1	1	Slovakia	10 or fewer					
Greece	10 or fewer						South Africa	10 or fewer					
Guatemala	10 or fewer						Spain	220	1	130	68	3	7
Hong Kong	21		4	11		6	Sri Lanka	15		2	13		
Hungary	10 or fewer						Sweden	10 or fewer					
India	630		20	352	26	215	Switzerland	12		8	2		
Indonesia	10 or fewer						Taiwan	157	1	83	64	4	2
Ireland	11		2	4			Thailand	44		15	26		2
Israel	23		3	12		4	Tunisia	10 or fewer					
Italy	51		22	25			Turkey	23			20		3
Japan	346	21	92	158	17	18	Ukraine	10 or fewer					
Korea, Republic Of	200	1	65	91	20	11	United Arab Emirates	10 or fewer					
Latvia	10 or fewer						United Kingdom	125	3	55	38	1	4
Lebanon	10 or fewer						United States	1871	30	668	759	23	159
Lithuania	10 or fewer						Uruguay	10 or fewer					
Luxembourg	10 or fewer						Viet Nam	20			15	2	3

Fuente: Carnegie Mellon University, Software Engineering Institute CMMI For Development SCAMPI[SM] Class A Appraisal Results 2011 [Diapositivas]. U.S. CMMI Appraisal Program. Marzo 2011. 30 Diapositivas.

Sin embargo, lo modelos de madurez como el CMMI, aun cuando presenta un conjunto de buena prácticas, se queda corto al momento de definir el CÓMO para que las empresas establezcan la manera de hacer gestión de cada uno de los procesos. Para afrontar esta carencia, alrededor de los modelos se han creado diversos marcos de referencia y estándares que buscan proveer un conjunto de prácticas para guiar a las empresas en la implementación de los QUÉ indicados por los modelos de madurez, en el caso particular de Gestión de riesgos, tenemos por ejemplo RISK IT de ISACA[*], Risk Management Framework del SEI[**], COSO[***]. ERM – Integrated Framewok, ISO20000:2005, ISO/FDIS3100:2009, PMBOK[****].

En el contexto de este trabajo, se realizará un enfoque a las empresas de software en Colombia que han implementado el modelo CMMI de manera escalonada a partir del nivel 3, que es el nivel en el cual se implementa el área de procesos para gestión de riesgos RSKM. Para complementar esta área de procesos, se empleará el marco de referencia RISK IT con el fin de generar una guía de mejores prácticas que permita a estas empresas implementar o reforzar el proceso de gestión de riesgos.

1.2 PLANTEAMIENTO DEL PROBLEMA

Los modelos de mejora como el CMMI que se usan de referente para la definición y mejora de los procesos de desarrollo/mantenimiento de software, aportan el QUÉ, es decir, el alcance de las prácticas propuestas, sin embargo no aportan herramientas útiles y tangibles que permitan a las empresas traducir estas

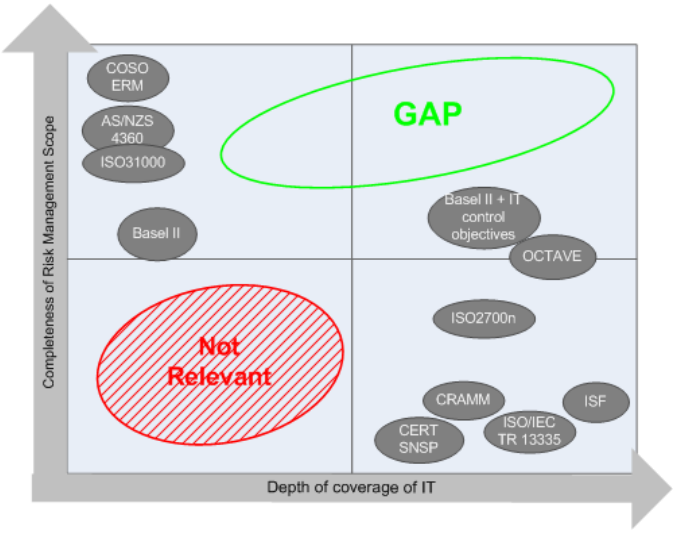
[*] ISACA Information Systems Audit & Control Association. Asociación de miembros profesionales, independientes y sin ánimo de lucro comprometidos con la elaboración, adopción y uso del conocimiento y las prácticas mundialmente aceptadas para los sistemas de información.
[**] Software Engineering Institute.
[***] Committee of Sponsoring Organizations of the Treadway Commission.
[****] Project Management Body of Knowledge.

recomendaciones en actividades específicas para decidir CÓMO llevar a cabo esos procesos.

Para las empresas desarrolladoras de software que emplean CMMI y han incluido en el alcance de mejora los procesos de Gestión de Proyectos, específicamente el relacionado con Gestión de riesgos, han encontrado que el área de proceso RSKM (Risk Management) ciertamente les aporta una orientación importante pero como ya se decía, el modelo demanda interpretación para llegar a la implementación de estas prácticas, puesto que no describe actividades específicas para saber cómo hacerlo.

Para cubrir esta necesidad, se han presentado varios marcos de referencia para gestión de riesgos, que buscan ofrecer un conjunto de prácticas avaladas por la industria, con el objetivo que las empresas aterricen u optimicen su proceso de gestión de riesgos, sin embargo, los marcos de referencia comúnmente empleados son genéricos, dejando una brecha en el cubrimiento del proceso tal como lo ilustra la figura 1.

Figura 1**.** RISK IT Framework for Management of IT Related Business Risks



Fuente: The RISK IT Framework. ISACA.

Como propuesta para cubrir esta brecha, ISACA, en diciembre del 2009, propone un nuevo marco de referencia denominado RISK IT. Este marco de referencia brinda una guía para realizar la gestión de riesgos ampliando la visión de este proceso a un contexto más extenso, donde se considera que los riesgos de la tecnología no están solamente ligados a la parte técnica sino también a otro riesgos de negocio tales como riesgos de mercado, riesgo operacionales y riesgos en la toma de decisiones.

Adicionalmente, RISK IT es un marco de referencia para gestión de riesgos basado en el valor y en los beneficios que la organización obtiene a través de las iniciativas de TI y se centra principalmente en la consecución de los objetivos de la organización al igual que lo hace COBIT* y Val IT**. No obstante, mientras que COBIT está enfocado a la gestión de procesos a través del monitoreo y control y Val IT se enfoca en la consecución de valor para la organización a través de la gestión del portafolio de iniciativas de TI, RISK IT se concentra en la gestión de los riesgos que causan la no obtención de ese valor y sus beneficios, así como del riesgo de no aprovechar las iniciativas y ventajas de TI.

Esta última definición separa a RISK IT de los demás modelos de gestión de riesgos, pues mientras los otros modelos se centran solo en mitigar los riesgos, RISK IT contempla la posibilidad de tomar riesgos que pueden traer beneficios a la organización, teniendo en cuenta que haya un adecuado balance entre el Riesgo y el Valor, para tomar ventaja de TI.

* COBIT Control Objectives for Information and related Technology. Conjunto de mejores prácticas para el manejo de información creado por ISACA y el ITGI en 1992.

** Val IT es un conjunto de documentos que proveen un marco de trabajo para el gobierno de las inversiones en TI, creado por el Instituto de Gobierno de las TI (ITGI, por sus siglas en inglés).

Por consiguiente, lo que se propone es utilizar RISK IT como complemento a la gestión de riesgos establecida por el área de procesos RSKM del modelo CMMI, brindando a las empresas un conjunto de prácticas que les permita fortalecer el proceso de gestión de riesgos mediante el cubrimiento de las brechas que pueden quedar en el proceso, pues CMMI define el QUÉ sin proveer una guía tangible de la aplicación del modelo. De este modo, las organizaciones contarán con una serie de prácticas y documentos de apoyo que les permita aplicar paso a paso las actividades del marco de referencia RISK IT, con lo cual la organización podrá cumplir no solo con los objetivos operativos, sino con los objetivos de negocio de la organización.

Actualmente son pocas las herramientas existentes que permiten a las empresas llevar las recomendaciones dadas por marcos de referencia como CMMI a la práctica. Después de realizar búsquedas de trabajos orientados a ofrecer una herramienta o guía de CÓMO realizar lo establecido por los marcos de referencia de calidad y gestión de riesgos, se identificó un estudio realizado por estudiantes de Maestría de la Universidad de los Andes[1]. Este estudio plantea una guía de buenas prácticas en gestión de riesgos de TI para el sector bancario, basada en la circular 052 de la Superintendencia Financiera de Colombia que define los requerimientos mínimos para garantizar la seguridad y la calidad en el manejo de la información y en los marcos de referencia para gestión de riesgos BS 31100, Marco 4A y RISK IT, generando así una guía para realizar el proceso de gestión de riesgos dando cumplimiento a la circular.

A la fecha de entrega de este documento no se han encontrado estudios que permitan la complementación de RSKM de CMMI-DEV basándose en RISK IT, por

[1] FIGUEROA, Luis C.; HERRERA, Andrea y GIRALDO, Olga L. Guía de buenas prácticas en gestión de riesgo de TI en el sector bancario colombiano [en línea]. Colombia: Universidad de los Andes, 2010 [consultado 16 de julio de 2011]. Disponible en Internet: http://biblioteca.uniandes.edu.co/Tesis_22010_segundo_semestre/347.pdf.

lo tanto es significativo el aporte que puede brindar a las empresas el contar con un mecanismo que les facilite y/o refuerce la implementación de esta área de proceso aprovechando las ventajas del marco de referencia RISK IT.

1.3 OBJETIVO GENERAL

Generar un conjunto de recomendaciones para gestionar los riesgos de TI en empresas ya valoradas con el modelo CMMI®-Dev1.2(+) en el nivel 3 o superior con implantación del área de procesos RSKM empleando el marco de referencia para gestión de riesgos RISK IT de ISACA.

1.4 OBJETIVOS ESPECÍFICOS

- Identificar las necesidades y/o dificultades comunes que enfrentan las empresas de desarrollo de software con nivel de madurez CMMI-Dev1.2(+) a nivel 3 o superior al momento de gestionar los riesgos de TI en su organización.

- Documentar un conjunto de actividades para gestionar los riesgos de TI, este conjunto de actividades permitirán dar cumplimiento a las metas y prácticas recomendadas por el área de proceso RSKM y a su vez se complementarán con las actividades propuestas por el marco de referencia RISK IT de ISACA.

- Verificar la claridad, validez y pertinencia de las recomendaciones planteadas para reforzar el proceso de gestión de riesgos. Con los resultados de esta valoración se realizarán las correcciones o adaptaciones a las recomendaciones establecidas.

1.5 RESUMEN DE ESTRATEGIA PROPUESTA

La estrategia propuesta para este trabajo es emplear el marco de referencia para gestión de riesgos RISK IT como complemento a la gestión de riesgos realizada en empresas valoradas CMMI nivel 3 o superior.

Para realizarlo, se toma como punto de partida el área de procesos RSKM del modelo CMMI así como también las prácticas genéricas de dicho modelo definidas para el nivel de madurez 3, a partir de este punto, se determina el cubrimiento de RISK IT que posee una empresa que ha realizado las practicas sugeridas por CMMI y a partir de esta alineación de los modelos y el resultado de una encuesta de valoración del proceso de gestión de riesgos en las empresas objetivo, se recomiendan una serie de actividades para gestionar riesgos de TI.

La definición de estas actividades propuestas, permitirá a las empresas dar cumplimiento a las prácticas recomendadas por el área de proceso RSKM y reforzar el proceso con las actividades adicionales propuestas por RISK IT, cuyo fuerte principal es la aplicación de Gobierno de TI.

A continuación en la figura 2 (ver página siguiente), se observa la alineación del área de proceso RSKM con RISK IT como punto de partida en el proceso, esta alineación se complementa con las brechas identificadas en el proceso de gestión de riesgos en las empresas con RSKM, dando como resultado un conjunto de actividades recomendadas para gestionar riesgos de TI.

Figura 2. Proceso de Generación de Actividades Recomendadas para Gestión de Riesgos

1.6 RESUMEN DE RESULTADOS OBTENIDOS

Una vez realizada la encuesta de valoración de gestión de riesgos en las empresas certificadas CMMI nivel 3 o superior, se evidenció que a pesar que el modelo CMMI genera un gran aporte a la gestión de riesgos, también tiene puntos importantes a complementar en diversos aspectos tales como la definición de modelos y planeación de identificación de riesgos, el apetito al riesgo, la generación de reportes para identificar oportunidades en el entorno y la comunicación con las personas interesadas.

Tomando como punto de partida estos aspectos se realizó un análisis detallado tanto de las metas específicas, como de las metas genéricas del modelo CMMI para identificar el cubrimiento de sus prácticas sobre los procesos y actividades propuestos por el marco de referencia RISK IT, así como de los roles involucrados en cada una de las actividades recomendadas por el marco de referencia.

Una vez generada la propuesta, fue presentada a las personas con conocimiento en el tema y que han estado directamente involucrados en los procesos de implementación del área de proceso RSKM, para conseguir su opinión frente a la

utilidad de la propuesta, logrando obtener alto grado de aceptación de lo planteado en ella.

1.7 ORGANIZACIÓN DEL DOCUMENTO

A continuación se detalla el contenido de cada uno de los capítulos del presente documento.

En el primer capítulo del documento se encuentra la introducción al documento. Aquí se muestra de manera general el estado del arte del proceso de gestión de riesgos en la industria del software, su importancia y la problemática a abordar con este proyecto.

El segundo capítulo se encuentra el marco teórico. Este capítulo inicia con la descripción del proceso de gestión de riesgos y su relevancia en la industria del software y continúa con la descripción del modelo de madurez CMMI y el marco de referencia RISK IT que serán los componentes con base en los cuales se apoyará la estrategia.

En el tercer capítulo se encuentra la estrategia propuesta. En este capítulo se detalla la forma en la cual abordaremos la problemática planteada referente al proceso de gestión de riesgos de TI basada en el marco teórico presentando.

Finalmente, en el cuarto capítulo, se encuentran los resultados obtenidos. Aquí se presenta la información obtenida al momento de presentar y validar la propuesta planteada a una muestra de las empresas objetivo de estudio obteniendo su retroalimentación acerca del aporte que genera el planteamiento en su proceso de gestión de riesgos.

2. MARCO TEÓRICO

De acuerdo al *Chaos Report*[*] liberado en el año 2009 por el Standish Group[**], se tienen las siguientes cifras con respecto a los proyectos de TI:

- 32% de los proyectos de TI son exitosos, es decir, son entregados en el plazo estipulado, dentro del presupuesto y con las características funcionales requeridas.

- 44% de los proyectos fueron finalizados con tiempos mayores a los establecidos, mayores presupuestos y/o sin las características funcionales requeridas.

- 24% de los proyectos no fueron exitosos, pues fueron cancelados antes de su finalización o fueron liberados pero nunca usados.

Estas cifras muestran que los proyectos de desarrollo de software y en general la industria de software, es un negocio de alto riesgo y de ahí la importancia de definir y realizar un proceso adecuado para gestión de los mismos.

A partir del análisis de las compañías que terminaron con éxito sus proyectos y expertos en el área de riesgos presentado en el 2009 en la Conferencia Internacional sobre la Gestión de la Información e Ingeniería[2], se ha identificado una lista de los 10 riesgos principales a los que se ven enfrentados los proyectos:

- Carencia de personal

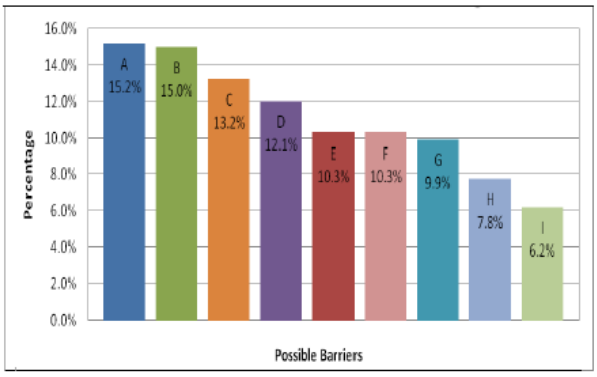
[*] Reporte creado por el Standish Group que lleva el registro de las tasas de fracaso de los proyectos a través de una amplia gama de empresas e industrias.
** El Standish Group es una compañía localizada en West Yarmouth, Massachusetts, dedicada a la investigación y consultoría de tecnologías de información.
2 ZARDARI, Shehnila. Software Risk Management. IEEE.

- Presupuesto y programación poco realista
- Desarrollo incorrecto de propiedades y funcionalidades
- Desarrollo incorrecto de la interfaz de usuario
- Invertir esfuerzo más allá del valor agregado que aporta
- Cambio continuo de los requerimientos
- Déficit en componentes externos
- Déficit en desarrollos externos
- Déficit en desempeño en tiempo real
- Forzar las capacidades de la informática

Para hacer gestión a los riesgos existen varios enfoques, uno de ellos es el conocido como "gestión proactiva del riesgo"[3], que se centra en evaluar la probabilidad de ocurrencia del riesgo, los disparadores de los eventos de riesgo, los eventos de riesgo, la probabilidad de impacto y el impacto de los disparadores de riesgos antes de que el riesgo suceda; justamente a éste enfoque responden las prácticas enmarcadas en la PA RSKM-Gestión de riesgos del modelo CMMI-Dev1.2, sin embargo, estudios como el realizado en Irlanda del Norte[4] sobre la precepción acerca del proceso de gestión de riesgos, demuestran que al momento de realizar este proceso se presentan barreras e inconvenientes como las que se muestran en la figura 3 (ver página siguiente), que dificultan el máximo aprovechamiento de éstas prácticas.

[3] Ibíd.,
[4] Edzreena Edza Odzaly, Des Greer, Paul Sage. Software Risk Management Barriers: an Empirical Study. IEEE.

Figura 3**.** Barreras percibidas en la gestión de riesgos



	Possible Barriers	%
A	Visible (and tangible) development costs get more attention than intangibles like loss of net profit / downstream liability.	15.2%
B	There are no resources available.	15.0%
C	Mitigation actions may require organizational or process changes.	13.2%
D	Risk management seems difficult or there are too many risks to handle.	12.1%
E	Value of risk management not easily proved.	10.3%
F	Project teams (and managers) see reward for problem-solving, not prevention.	10.3%
G	Overconfidence (e.g. risks implicitly handled)	9.9%
H	Discussing risks goes against cultural norms (e.g viewed as negative thinking)	7.8%
I	Fatalism (e.g., software is always late)	6.2%

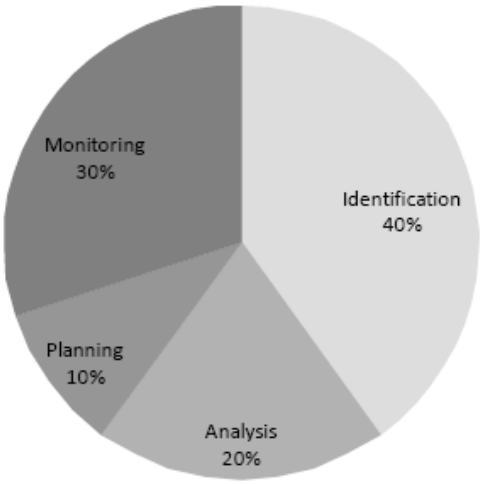
Fuente: Edzreena Edza Odzaly, Des Greer, Paul Sage. Software Risk Management Barriers: an Empirical Study. IEEE.

El estudio mencionado[5], seleccionó un conjunto inicial de 89 compañías de desarrollo se software del cual se excluyeron las empresas con menos de 10 empleados evitando así compañías que fueran inmaduras y por implicación, menos probable que se hubieran establecido plenamente los procesos de software, con esta clasificación solo respondieron 18 empresas.

De la población final, 12 compañías reportaron tener un proceso definido de gestión de riesgos, estas compañías fueron entrevistadas y se recopilaron las percepciones acerca de los procesos para gestión de riesgos llevados a cabo, entre otros, determinó que el esfuerzo invertido que perciben las compañías en cada una de las fases del proceso de gestión de riesgos se distribuye como muestra la figura 4 (ver página siguiente), donde se aprecia que el mayor esfuerzo invertido corresponde a las fases de identificación del riesgo con 40% y monitoreo con 30%.

[5] Edzreena Edza Odzaly, Des Greer, Paul Sage. Software Risk Management Barriers: an Empirical Study. IEEE.

Figura 4**.** Esfuerzos por actividades de gestión de riesgos



Fuente: Edzreena Edza Odzaly, Des Greer, Paul Sage. Software Risk Management Barriers: an Empirical Study. IEEE.

Antes de iniciar a revisar las diferentes estrategias que han adoptado las empresas para afrontar la problemática referente al proceso de gestión de riesgos, es importante realizar una revisión del proceso de gestión de riesgos de TI, con los diferentes conceptos de riesgo manejados por la industria, para posteriormente pasar a describir el proceso de gestión de riesgos de CMMI con su área de proceso RSKM y RISK IT que serán los marcos de referencia seleccionados en nuestra propuesta enfocados a gestionar los riesgos de TI.

2.1 RIESGOS DE TI

Para guardar coherencia entre los diferentes conceptos relacionados con la gestión de riesgos de TI, las siguientes definiciones se basan en el artículo "Different Techniques For Risk Management In Software Engineering: A Review" [6] publicado por Carleton University.

6 MISRA, Subhas C.; KUMAR, Vinod y KUMAR, Uma. DIFFERENT TECHNIQUES FOR RISK MANAGEMENT IN SOFTWARE ENGINEERING: A REVIEW. Disponible en internet: http://attila.acadiau.ca/library/ASAC/v27/content/authors/m/misra,%20subhas/DIFFERENT%20TECHNIQUES.pdf

El diccionario define “Riesgo” como “La probabilidad de pérdidas o perjuicios”7. Este término tiene su origen etimológico en el latín “Resceare”, que traduce “Reducir”. Desde ese entonces ha evolucionado como la palabra francesa “risqué” y la italiana “risco”. Este término es usado universalmente bajo diferentes contextos; por ejemplo, es usado en el sector financiero para establecer la posibilidad de incurrir en pérdidas financieras, en el campo médico para establecer la posibilidad de pérdida fisiológica de la vida.

En el mundo del “software”, los riesgos son un tópico de gran importancia que a menudo hacen referencia a las fuentes de peligro para el desarrollo de software, compra o adquisición y mantenimiento. Una de las consideraciones más importantes que agobia a los investigadores de gestión de riesgos es su propia definición. En otras palabras, antes de proponer un marco de referencia para la gestión de riesgos se necesita especificar/cuantificar las “dimensiones” de los riesgos. Esto se debe a la complejidad de acordar una única definición de Riesgo. Existes diversas definiciones formales de Riesgo disponibles en la literatura, algunas de las cuales presentamos a continuación.

“Un posible evento a futuro que, si se presenta, llevará a un resultado indeseable” (Leishman and VanBuren, 2003).

“El Riesgo es una combinación de eventos anormales o fallas, y las consecuencias de estos en un operador del sistema, usuarios o ambientes. Un Riesgo puede catalogarse desde catastrófico (pérdida total del sistema, pedida de la vida o incapacidad permanente) hasta despreciable (sin impacto al sistema)” (Glutch, 1994).

---

[7] Diccionario Merriam-Webster.

“Los Riesgos incurren en la posibilidad de pérdida, la pérdida en si o cualquier característica, objeto o acción que esté asociada con esta posibilidad” (Kontio, 2001).

2.1.1 ¿Qué es la gestión de riesgos? La gestión de riesgos simplemente es una manera de administrar los riesgos. En otras palabras, es lo concerniente a todas las actividades que son realizadas para reducir la incertidumbre asociada a ciertas tareas o eventos. En el contexto de proyectos, la gestión de riesgos reduce el impacto de eventos indeseables sobre un proyecto. La gestión de riesgos en cualquier proyecto requiere que se cumplan actividades de toma de decisiones.

2.1.1.1 Origen de la gestión de riesgos. La gestión de riesgos tiene sus raíces en la teoría de la probabilidad y la toma de decisiones bajo incertidumbre. Tres de las más reconocidas teorías en estas áreas – Teoría de la utilidad esperada (Bernoulli 1954; Hogarth 1987), Teoría de la racionalidad limitada (Simon, 1979), y la teoría de la perspectiva (Kahneman and Tversky, 1973; Kaheman et al., 1982) – fueron de gran influencia. Estas teorías pueden ser consideradas como disciplinas por sí mismas, por lo que, para contextualizar nuestra discusión en la gestión de riesgos, a continuación mencionamos brevemente lo que cada uno de estas teorías propone.

En resumen, la teoría de la utilidad esperada discute como las personas toman decisiones desde diferentes puntos de vista, basados en la utilidad esperada.

La teoría de la racionalidad limitada determina que los eventos de la vida real, los resultados y sus probabilidades asociadas son comprendidos muy limitadamente por las personas al momento de tomar las decisiones que maximizarán su utilidad esperada, por lo cual, las personas tienden a definir objetivos de aspiraciones en

la vida eliminando alternativas de las diferentes opciones que tienen. Esta teoría es útil al momento de modelar comportamientos de proyectos de administración del personal encargado de la gestión de riesgos.

La teoría de la perspectiva, que tiene sus orígenes en la Psicología, ayuda a modelar el como la percepción de los hombres influye en la toma de decisiones sobre sus opciones disponibles. Esto, por lo tanto, ayuda a la compresión y estimación de pérdida de utilidades de las diferentes alternativas mientras se analizan los riesgos en la gestión de riesgos.

2.1.1.2 Propósito de la gestión de riesgos en la ingeniería de software. La gestión de riesgos en proyectos de software tiene múltiples usos. Ayuda a evitar la falla de los proyectos debido a diferentes factores tales como la no terminación de los proyectos dentro del cronograma establecido, restricciones de presupuestos y el no cumplimiento de la especificación del cliente.

La gestión de riesgos analiza los proyectos desde diferentes perspectivas para asegurar que las amenazas a los proyectos sean identificadas, revisadas y se definan las debidas estrategias para controlar y mitigar los riesgos.

Las estrategias de mitigación no siempre implica la eliminación de tareas que presenten factores de riesgo. Muchas tareas son implementadas en la industria de software aun sabiendo que su ejecución presenta un alto margen de riesgos. Las tareas de alto riesgo son a veces importantes para proveer a las industrias una ventaja sobre sus competidores.

El principal propósito de la gestión de riesgos es conocer todos los posibles riesgos de un proyecto, evaluar su severidad y consecuencias, y entonces poder determinar los pasos a seguir dependiendo de la naturaleza de los riesgos. La

idea principal es poder minimizar cualquier problema imprevisto que surja durante la ejecución del proyecto a través de la planeación de eventualidades. Una correcta planeación conduce a minimizar las incertidumbres, las cuales pueden llevar a una terminación “turbulenta” o a la cancelación de los proyectos.

La gestión de riesgos en la ingeniería de software presenta un acercamiento preventivo en pro de la terminación de los proyectos en un tiempo y dinero estipulado; de hecho, los proyectos basados en la gestión de riegos tienen la habilidad de reducir costos del proyecto, tiempos de terminación y el incremento en la calidad en los proyectos entregados. Sin estos factores, los proyectos tendrían grandes riesgos en los ingresos, confiabilidad del cliente o en el peor escenario una completa bancarrota de las compañías participantes del proyecto.

2.1.2 Gestión de riesgos en la ingeniería de software. La gestión de riesgos en software ha existido por muchas décadas. Sin embargo, como hemos mencionado anteriormente, solamente en esta última década ha adquirido una gran importancia en la comunidad de software.

Los proyectos de desarrollo de software en los inicios del último siglo aplicaban la gestión de riesgo utilizando diferentes enfoques ad-hoc, sin implementar metodologías sistemáticas. Sin embargo, con el incremento en la complejidad del desarrollo de software, las industrias han determinado la importancia en la gestión de riesgos, porque contribuye en la reducción de incertidumbres involucradas en el desarrollo de software y en la reducción de posibles fallas en el proyecto.

Antes de aplicar cualquier proceso de gestión de riesgos, el equipo de trabajo debe tener claro las siguientes dimensiones de riesgos en sus proyectos:

- La naturaleza de la incertidumbre involucrada y la probabilidad que el riesgo ocurra.
- La pérdida incurrida por la presencia del riesgo. Las pérdidas en proyectos de software pueden tomar muchas formas incluyendo pérdida de ingresos, penetración en el mercado y pérdida de la confianza del cliente.
- La gravedad de las pérdidas.
- La duración de los riesgos[8].

2.1.3 Modelos populares de gestión de riegos. Varios enfoques de software de gestión de riesgos se han propuesto en el pasado, de los cuales la mayoría evalúan los riesgos en todas las fases del desarrollo de software integrando prácticas de la gestión de riesgos con el proceso de desarrollo de software. Como resultado de estos acercamientos, el modelo de gestión de riesgos se ha encaminado hacia un proceso disciplinado. Estos acercamientos son:

- Modelo de gestión de riesgo de Boehm (Win - Win) (Boehm 1988; Boehm and Ross 1989; Boehm and Bose 1994; Boehm et al 1998).
- Software de modelo de gestión de riesgos de SEI (DRE Version 2.0) (Williams et al 1999).
- Modelo de gestión de riesgos de Hall (P I) (Hall 1998).
- Modelo de gestión de riesgos de Karolak (Just-In-Time Software) (Karolak 1998).
- Metodología RiskIt de Kontio (Kontio 1997; Kontio 2001).

[8] Smith and Pichler, 2005.

Estos acercamientos son resumidos a continuación. Una comparación horizontal sobre estos acercamientos podría no ser justa, a pesar que cada uno de ellos referencia la gestión de riesgos, se desarrollaron bajo diferentes circunstancias por lo que sus enfoques difieren. Por ejemplo, el modelo de gestión de Hall fue desarrollado desde un punto de vista de modelamiento de la gestión de riesgos. Por otra parte, El modelo Win-Win de Boehm se desarrolló principalmente como un nuevo modelo de proceso de desarrollo de software (Desarrollo en espiral) con un acercamiento basado en riesgos. Más adelante se presenta un resumen más detallado sobre estos acercamientos.

- **Contribuciones fundamentales de Boehm***:* Boehm propuso un modelo de desarrollo de software basado en los riesgos. El fuerte de este modelo, referenciado como el modelo original de espiral (Boehm 1988), elimina los riesgos desde las primeras etapas del desarrollo de software en lugar de encontrar barreras al proyecto en las etapas finales.

Boehm extendió su modelo original de espiral usando la teoría W (Win-Win) (Boehm and Ross, 1988; Boehm and Bose, 1994), cuyo final era cumplir el alcance de los objetivos y las preocupaciones de los interesados. El modelo Win-Win también soporta la identificación de riesgos, resolución y el continuo monitoreo de estos. Aunque la estrategia abordada por el modelo Win-Win puede no ser siempre implementada en la práctica es una importante contribución al momento de involucrar los interesados en el proceso de gestión de riesgos.

Boehm (1991) también propuso un Framework para la gestión de riesgos, el cual ayuda a identificar las principales fuentes de riesgos, analizarlas y

resolverlas. Este Framework para la gestión de riesgos se puede integrar al modelo original de espiral o al modelo Win-Win.

- **Acercamiento a la gestión de riegos en software de SEI***:* El SEI proveyó un Framework compuesto en los siguientes tres grupos de prácticas: Evaluación del riesgo de software, gestión de riesgos continua y un equipo de gestión de riesgos.

La evaluación de riesgos de software se ocupa de las estrategias de identificación, análisis, comunicación y mitigación en la gestión de riesgos. Este acercamiento depende, entre otras cosas, de la taxonomía de los riesgos, la que consiste en estructuras usadas para la organización de la información de los riesgos. La taxonomía provee un instrumento (Cuestionarios) que permite identificar las diferentes clases de riesgos.

La taxonomía completa de riesgos se puede encontrar en (Higuera and Haimes, 1996) y se omite a partir de este momento. La taxonomía clasifica los riesgos en categorías tales como riesgos de requerimiento, riesgos de diseño, riesgos de implementación y pruebas, riesgos de contrato, riesgos de recursos entre otros.

La gestión de riesgo continua aborda un acercamiento basado en principios para proveer proceso, métodos y herramientas para la continua gestión de riesgos durante todas las fases del ciclo de vida del software.

El equipo de gestión de riesgos, por otra parte, es también una práctica basada en principios, pero se enfoca en el desarrollo de metodologías, procesos y herramientas para mejorar las relaciones entre el proveedor y el cliente. Estos tres grupos de prácticas son colaborativas. Por ejemplo,

tomando el acercamiento de un equipo orientado a la gestión de riesgos ayuda continuamente a la administración de los riesgos.

- **Acercamiento de Hall:** Hall (1998) realizó un acercamiento a la gestión de riesgos identificando 4 factores que tenían el potencial de alterar los resultados en un proyecto. Estos factores son la gente, los procesos, la infraestructura y la implementación.

El factor Personas se ocupa de los aspectos del recurso humano para la gestión de riesgos. Esto es muy importante porque el éxito de cualquier actividad de gestión de riesgos depende de la comunicación efectiva de los inconvenientes que surjan durante estas actividades.

El factor Proceso define que procesos deben implementarse para la minimización de la incertidumbre involucrada en el proyecto.

El factor Infraestructura a define los requerimientos, recursos y resultados requeridos para ejecutar actividades de gestión de riesgos en las organizaciones.

El factor Implementación se ocupa de la implementación de actividades de gestión de riesgos tales como establecer la iniciativa de gestión de riesgos, ejecución del plan, personalización de los procesos estándares para cumplir los requerimientos del proyecto, evaluación y control de riesgos.

- **Acercamiento de Karolak:** Karolak (1998) llevó un acercamiento Just-In-Time para la gestión de riesgos en la ingeniería de software. Este acercamiento trata de minimizar la cantidad de riesgos involucrados, mientras se optimizan las estrategias de contingencia sobre situaciones

problemáticas. Toma un acercamiento inducido al riesgo y aboga por el principio de la gestión de riesgos durante las primeras fases del ciclo de vida de desarrollo de software para reducir el costo y tiempo del proyecto y mejora las expectativas del cliente.

En su acercamiento, primero identifica un set de categorías de alto nivel. Luego asocia estas categorías a factores de riesgo, métricas y preguntas para ser respondidas por los involucrados en el proyecto. Estas preguntas son usadas con listas de chequeo para identificar las diferentes clases de riesgos.

- **Acercamiento RiskIt de Kontio**: Kontio (2001) propuso la metodología RiskIt, la cual provee un muy completo Framework conceptual para la gestión de riesgos haciendo uso de un objetivo. Intenta gestionar los riesgos determinando las intenciones de los involucrados en el proceso de gestión de riesgos. La implementación de esta metodología ayuda a los gerentes de proyecto con una diseminación precisa acerca de la información del proyecto, oportunidad y riesgos de los distintos involucrados, por lo que permite tomar decisiones críticas para el cumplimiento del proyecto.

RiskIt también ayuda a gestionar los proyectos de una manera sistemática, iniciando con la identificación y análisis de los riesgos hasta su monitoreo y control. El principal objetivo de RISK IT es el diseño de un grafo de análisis, para analizar los riesgos, factores, eventos de riesgo, resultados, acciones correctivas, efecto y pérdidas que puedan suceder debido a los eventos de riesgo.

Con este acercamiento también se propone el uso de conceptos de La Experience Factory de Victor Basilis (Basili, 1993). El Framework de

mejoramiento de procesos de gestión (PMI) requiere una comprensión del repositorio de experiencias. Sin entrar en detalle del repositorio de experiencias, mencionamos que la idea esencial del marco de referencia PMI de riesgos de TI de Kontio es utilizar la experiencia y la información de anteriores proyectos de desarrollo para gestionar los riesgos en el proyecto actual.

- **Avances recientes.** Después de discutir la importancia de los modelos de gestión de riesgos de software analizamos más adelante 5 recientes contribuciones al área. Estos proponen principalmente el análisis de metodologías de riesgos y no un completo Framework de gestión de riesgos, lo contrario a lo establecido hasta este punto.

- **Acercamiento de Foo y Murugananthan***:* Foo y Murugananthan (2000) propusieron un acercamiento basado en cuestionarios para el análisis de riesgos y así proveer su evaluación cuantitativa. Este acercamiento puede ser utilizado para cuantificar los elementos de riesgo y usarlos para estimar el valor normalizado de riesgo sobre todos los proyectos.

Su modelo, denominado Modelo evaluativo de riesgos de software (SRAM), está basado en el uso de factores situacionales para predecir los riesgos del proyecto. En otras palabras, la evaluación de los riesgos en este modelo depende de la naturaleza del proyecto y las situaciones que enfrenta.

Este modelo se basa en cuestionarios y análisis de riesgos para brindar sus evaluaciones cuantitativas. En su modelo, consideran nueve elementos de criticidad: Complejidad del software, equipo de trabajo, confiabilidad objetivo, requerimientos del producto, metodologías de estimación, metodologías de monitoreo, proceso de desarrollo, usabilidad y herramientas. Por lo cual,

ellos encasillan una lista de preguntas para el asesor de riesgos, brindando tres opciones para cada uno de los elementos críticos de riesgos descritos anteriormente. Las respuestas del asesor son evaluadas y ordenadas de acuerdo a los niveles incrementales de riesgo.

- **Acercamiento de Deursen and Kuiper***:* Deursen and Kuiper (2003) propusieron una nueva metodología de evaluación de riesgos identificando los diferentes factores primarios y secundarios en un proyecto. Los factores primarios se obtienen entrevistando a los diferentes involucrados, revisando documentos de contratos, planes de proyectos, especificaciones de requerimiento y documentos de diseño. Finalmente, los factores primarios y secundarios se analizan en conjunto, se comparan y se observa si los riesgos percibidos desde ambos ángulos son consistentes entre sí.

Esta metodología de evaluaciones de riesgo es diferente a la tradicional gestión de riesgos de productos y procesos. Su ventaja radica en combinar las ventajas de las dos gestiones de riesgos mencionadas para evitar los riesgos de puntos de vista conflictivos entre las partes involucradas.

- **Acercamiento de Roy***:* Roy (2004) desarrolló el Framework de gestión ProRisk, extendiendo el estándar AS/NZS 4350. Este categoriza las actividades de gestión de riesgo en dominio del negocio y ámbito operativo. Realiza diferentes actividades tales como identificación de los involucrados, identificación de factores de riesgo, construcción de un modelo libre de riesgos, calibrando este modelo, estimando las probabilidades de eventos de riesgo, evaluación de combinaciones de riesgo, desarrollo de planes de acción y monitoreo de procesos.

El Framework ProRisk identifica 2 puntos focales importantes en los proyectos de administración de riesgos:

- **Dominio del negocio***:* Se concentra en la perspectiva del dominio de la organización y el proyecto. Identifica los parámetros del negocio en el ambiente donde se aplicará el proyecto.

- **Ámbito operativo***:* Se concentra en el modelado formal de diferentes aspectos de la gestión de riesgos del proyecto. Actividades típicas que constituyen el ámbito operativo son la medición de riesgos, realización de evaluaciones de riesgo, identificación y propuesta de planes de acción para mitigar riesgos, implementación y continua administración de estos.

- **Acercamiento de Tiwana and Keil***:* Recientemente, Tiwana and Keil (2004) desarrollaron una herramienta muy útil para el desarrollo de evaluación de riesgo (Metodología) para que los gerentes de proyectos pudieran evaluar de manera inmediata algunos de los riesgos más importantes de los proyectos y sus efectos.

Esta herramienta y sus cuestionarios fueron el resultado de la recolección de información de gestión de riesgos de alrededor de 60 compañías. El más grande logro de esta herramienta es que puede ayudar, de manera muy rápida, evaluar riesgos importantes al proyecto, en lugar de desplegar una metodología de gestión de riesgos de alto consumo de presupuesto y tiempo.

- **Acercamiento et al de Misra:** Misra et al. (2005) también propuso un acercamiento para la gestión de riesgos en la ingeniería de software. Este acercamiento podría ser usado por gerentes de proyectos para modelar y

controlar los riesgos en proyectos de software. No existen acercamientos similares en modelado de riesgos de proyectos de software.

Este acercamiento es relativamente nuevo en el área de gestión de riesgos de software. El acercamiento es útil para gerentes de proyecto que desean realizar análisis de fines y medios, descubriendo así el origen estructural de los riesgos en un proyecto, y cómo las causas de estos riesgos se pueden controlar desde las primeras etapas de los proyectos.

Aunque se han realizado intentos por modelar la gestión de riesgos en sistemas de información empresariales usando técnicas de modelado convencionales, como diagramas de flujo y UML, los anteriores trabajos han analizado y modelado lo mismo solo referenciando el “Qué” es un proceso. Sin embargo no hacen referencia al “Por qué” el procesos es de la manera que es.

El acercamiento propuesto referencia la limitación de modelos de gestión de riesgo de software existentes explorando las dependencias estratégicas entre los actores del proyecto, analizando las motivaciones, intenciones y racionalidades detrás de las entidades y actividades en los proyectos.

El concepto de dependencias estratégicas entre actores de un proyecto es nuevo. Una buena revisión del concepto se puede hallar en Chung et al. (2000). Este acercamiento está restringido a proveer una metodología que se pueda usar en el ciclo de vida de los modelos de gestión de riesgos para analizar y descubrir la estructura origen de los riesgos y controlar estos en las fases iníciales de los proyectos.

- **Otros trabajos relacionados.** Los acercamientos descritos anteriormente no ayudan a predecir la confiabilidad de los productos finales. Otra clase de investigadores realizaron estudios sobre la gestión de riesgos desde el punto de vista de la calidad final del producto. Realizaron un acercamiento probabilístico para evaluar los riesgos de software midiendo la confiabilidad de los productos.

  Específicamente, no resuelven los problemas de gestión de riesgos en fallas a proyectos debido a la inhabilidad de finalizar dentro del presupuesto y cronograma establecidos. Por lo que, como mencionamos antes, en este artículo omitimos intencionalmente la discusión sobre estos acercamientos y limitamos el alcance a la discusión de proyectos y metodologías de gestión de riesgos. Sin embargo, por el bienestar de la completitud, mencionamos algunos excelentes trabajos sobre gestión de riesgo de productos (específicamente confiabilidad de software) que pueden ser encontrados en Karunanithi and Whitley (1992), Lanning (1995), Lyu (1995), y Musa (1998).

2.2 MARCO DE REFERENCIA RISK IT

Origen: ISACA es un líder mundialmente reconocido como proveedor de conocimiento, certificaciones, apoyo y educación en seguridad y aseguramiento de sistemas de información, gobierno empresarial, administración de TI, al igual que riesgos y cumplimiento relacionados con TI.

ISACA desarrolla estándares internacionales de auditoría y control de sistemas de información que ayuda a los profesionales y líderes empresariales de TI a cumplir con sus responsabilidades de administración y gestión, particularmente en las áreas de aseguramiento, seguridad, riesgo y control, con el objetivo de agregar valor al negocio.

Una de las publicaciones más reconocidas de ISACA, enmarcada en los principios de Gobierno de TI, es el marco de referencia para gestión de riesgos “The RISK IT Framework”, el cual ha sido diseñado y creado principalmente como un recurso educativo para los oficiales de información (CIOs), la alta dirección y administración de TI.

El marco de RISK IT se basa en los principios de gestión de los riesgos organizacionales (ERM), las normas y marcos como COSO ERM 2 y AS/NZS 43603 (que pronto serán complementados o sustituidos por la norma ISO 31000), y provee información acerca de cómo aplicar estos principios a las TI. RISK IT aplica los conceptos generalmente aceptados de los principales estándares y marcos, así como los principales conceptos de la gestión de otros riesgos de TI, relacionados con las normas.

Definición: RISK IT es un marco de referencia para gestión de riesgos basado en el valor y beneficios que la organización obtiene a través de las iniciativas de TI. Se centra principalmente en la consecución de los objetivos de la organización y en la gestión de los riesgos que causan la no obtención de valor y sus beneficios, de igual manera analiza el riesgo de no aprovechar las iniciativas y ventajas de TI.

Esta última definición separa a RISK IT de los demás modelos de gestión de riesgos. Mientras los otros modelos se centran en eliminar los riesgos, RISK IT contempla la posibilidad de tomar riesgos que pueden traer beneficios a la organización, teniendo en cuenta que haya un adecuado balance entre el Riesgo y el Valor para tomar ventaja de TI.

Alcance: Teniendo en cuenta que el Gobierno de TI se define como la estructura de relaciones y procesos para dirigir y controlar la empresa hacia el logro de sus objetivos, por medio de agregar valor, al tiempo que se obtiene un balance entre el riesgo y el retorno sobre las TI y sus procesos; RISK IT brinda a las

organizaciones una propuesta para identificar, gobernar y administrar los riesgos relacionados con TI, alineándolos con los objetivos del negocio. Es un marco basado en un conjunto de principios, guías, procesos de negocio y directrices de gestión el cual permite aterrizar los procesos de la empresa en prácticas para la gestión de riesgos.

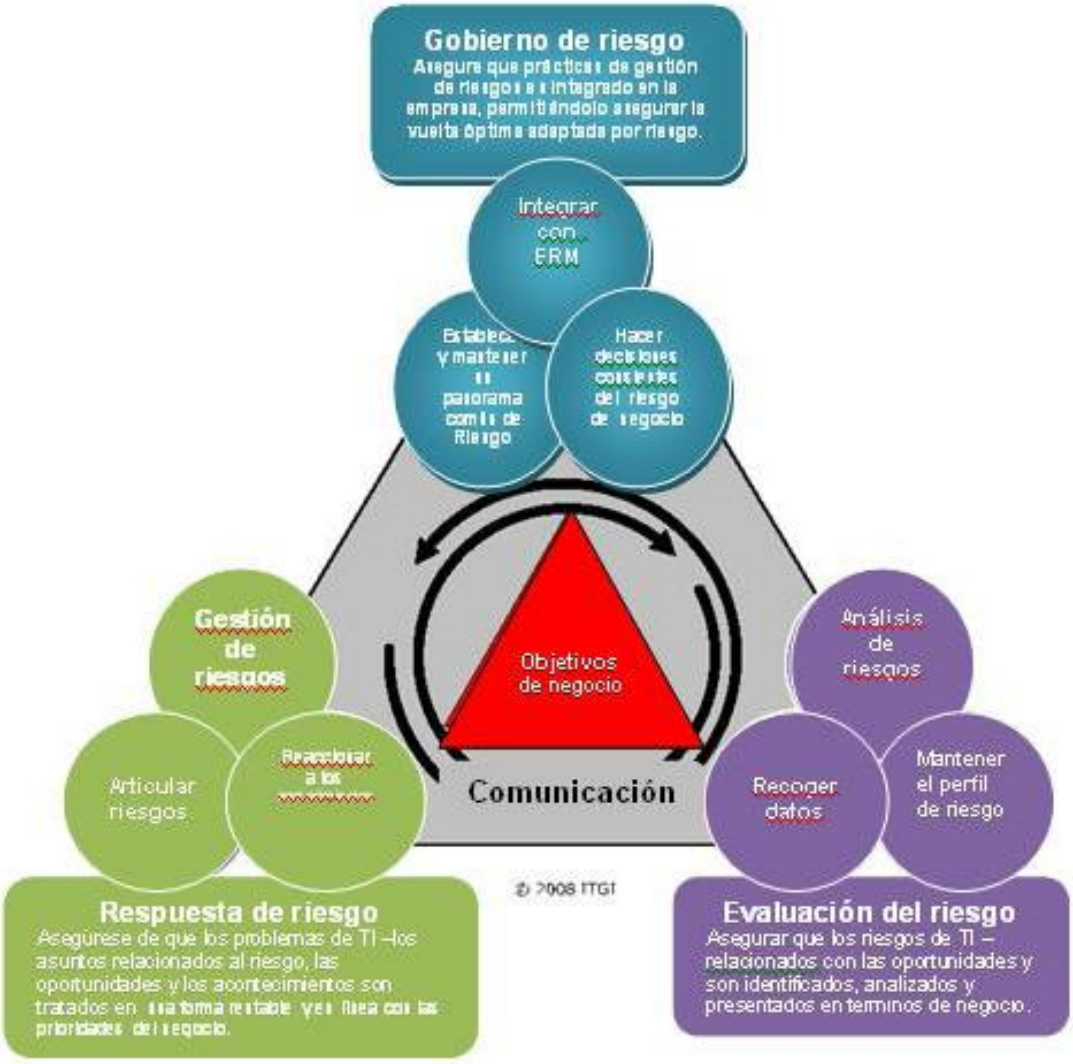
RISK IT cuenta con unos principios que le permiten tener un control adecuado de los riesgos a lo largo de los modelos organizacionales dentro de los cuales encontramos:

- Debe siempre estar conectado con los objetivos de la organización.
- Permitir la alineación de riesgos relacionados con la gestión de TI con los riesgos de toda la organización.
- Tener presente el balance de costos y beneficios en la gestión de riesgos.
- Promover una comunicación abierta y justa de los riesgos de TI.
- Establecer el tono correcto desde la alta dirección mientras se define y refuerza la responsabilidad del personal para operar en niveles de tolerancia aceptables y bien definidos.
- Entender que se trata de un proceso continuo y forma parte de las actividades diarias.

Estructura: RISK IT se encuentra dividido en tres grandes dominios que incluyen: Gobierno de Riesgos, Evaluación de Riesgos y Respuesta al Riesgo, cada uno con tres procesos, los cuales le permiten a este marco de referencia ser una excelente herramienta para ofrecer y mantener valor en las empresas.

Como se ilustra en la figura 5 (ver página siguiente), los procesos que constituyen el marco de referencia se encuentran distribuidos de la siguiente manera:

Figura 5**.** Marco de Referencia RISK IT.



Fuente: The RISK IT Framework. ISACA.

- **Gobierno de riesgos (GR)**

✓ RG1 Establecer y mantener una vista de riesgo común.

✓ RG2 Integrar con ERM.

✓ RG3 Tomar decisiones conscientes de los riesgos del negocio.

- **Evaluación de riesgos (RE)**

✓ RE1 Recopilar los datos.
✓ RE2 Analizar los riesgos.
✓ RE3 Mantener perfil de riesgo.

- **Respuesta de riesgos (RR)**

✓ RR1 Articular los Riesgo
✓ RR2 Manejar riesgos
✓ RR3 Reaccionar a acontecimientos

Cada uno de estos procesos es clave en la consecución de los objetivos de TI y de la empresa en general y como todo proceso presenta una serie de actividades que deben ser realizados por diversos roles de la empresa, con el objetivo de conseguir que los riesgos sean gestionados.

A continuación se presentan las actividades que componen cada proceso y que se presentan como referencia por parte del RISK IT para logar implementar cada proceso de gestión de riesgos en la empresa.

RG1 Establecer y mantener una vista de riesgo común.

- RG1.1 Realizar una evaluación de riesgos de TI en toda la empresa
- RG1.2 Proponer los umbrales de tolerancia de riesgo de TI
- RG1.3 Aprobar la tolerancia al riesgo.
- RG1.4. Alinear la política de riesgos de TI.
- RG1.5 Promover la cultura consiente de los riesgos de TI.
- RG1.6 Promover una comunicación efectiva de los riesgos de TI

RG2 Integrar con ERM.

- RG2.1 Establecer la rendición de cuentas de la gestión de los riesgos de TI en toda la empresa.
- RG2.2 Coordinar la estrategia de riesgos de TI y la estrategia de riesgo empresarial.
- RG2.3 Adaptar las prácticas de riesgos de TI a las prácticas de riesgo de la empresa.
- RG2.4 Proporcionar recursos adecuados para la gestión de riesgos.
- RG2.5 Garantizar el aseguramiento independiente sobre la gestión de riesgos.

RG3 Tomar decisiones conscientes de los riesgos del negocio.

- RG3.1 Obtener ganancia de la gestión de compra para el enfoque de análisis de riesgos.
- RG3.2 Aprobar los resultados del análisis de riesgo.
- RG3.3 Incorporar la consideración de los riesgos de TI en la toma de decisiones estratégicas de negocio.
- RG3.4 Aceptar el riesgo de TI.
- RG3.5 Priorizar actividades de respuesta a los riesgos de TI

RE1 Recopilar datos.

- RE1.1 Establecer y mantener un modelo para la recolección de datos.
- RE1.2 Recopilar datos sobre el entorno externo.
- RE1.3 Recopilar datos sobre eventos de riesgo.
- RE1.4 Identificar factores de riesgo.

RE2 Analizar los riesgos.

- RE2.1 Definir Alcance del Análisis de Riesgos.
- RE2.2 Estimar los riesgos de TI.
- RE2.3 Identificar las opciones de respuesta de riesgo.
- RE2.4 Realizar una revisión de pares de los resultados de análisis de riesgos de TI.

RE3 Mantener el perfil de riesgo.

- RE3.1. Mapear los recursos de TI para procesos de negocio.
- RE3.2 Determinar la criticidad de negocio de los recursos de TI.
- RE3.3 Entender las capacidades de TI
- RE3.4 Actualizar los componentes de los escenario de riesgos de TI.
- RE3.5 Mantener el registro de los riesgos de TI y el mapa de riesgos de TI.
- RE3.6 Diseñar y comunicar los indicadores de riesgo de TI.

RR1 Articular riesgos.

- RR1.1 Informar los resultados de análisis de riesgos de TI.
- RR1.2 Reportar las actividades de gestión de riesgos de TI y el estado de cumplimiento.
- RR1.3 Interpretar los resultados de la evaluación independiente de TI.
- RR1.4 Identificar las oportunidades relacionadas con TI.

RR2 Manejar los riesgos

- RR2.1 Controles del inventario.

- RR2.2 Supervisar la alineación operacional de los umbrales de tolerancia al riesgo.
- RR2.3Responder a la exposición al riesgo descubierto y la oportunidad.
- RR2.4 Implementar los controles.
- RR2.5 Informar el progreso del plan de acción de riesgos de TI.

RR3 Reaccionar a acontecimientos

- RR3.1 Mantener los planes de respuesta a incidentes.
- RR3.2 Supervisión de riesgos de TI
- RR3.3 Iniciar planes de respuesta a incidentes
- RR3.4 Comunicar las lecciones aprendidas de eventos de riesgo.

Es importante tener en cuenta que estas actividades se proponen exclusivamente como referencia y no son una norma, por lo tanto se deben adaptar a las prácticas y el contexto de la organización que desee guiarse a través de ellas.

Beneficios: dentro de los beneficios, el marco de RISK IT aborda muchas cuestiones a las cuales las organizaciones se enfrentan hoy en día. Es notable su necesidad de:

- Una visión precisa del presente y del futuro próximo sobre los riesgos relacionados con TI en toda la organización y el éxito con el que la organización se ocupa de dichos riesgos.

- Orientación de principio a fin sobre la forma de gestionar los riesgos relacionados con TI, más allá de medidas puramente técnicas de control y de seguridad.

- Comprensión de cómo capitalizar una inversión realizada en un sistema de control interno de TI ya existente para gestionar los riesgos relacionados con TI.

- En cuanto a la evaluación y gestión de los riesgos de TI, la integración con el riesgo global y el cumplimiento de las estructuras dentro de la organización.

- Un marco/lengua común para ayudar a gestionar la relación entre los ejecutivos encargados de adoptar decisiones (o junta de los altos directivos), el director de información (CIO) y la organización de gestión del riesgo, o entre los auditores y la dirección.

- Promoción de la responsabilidad del riesgo y su aceptación en toda la organización.

- Un perfil de riesgo completo para entender mejor el riesgo y aprovechar mejor los recursos de la organización.

Para realizar la gestión de riesgos encontramos en la industria múltiples estándares y marcos de referencia que establecen un conjunto de buenas prácticas, sin embargo encontramos que RISK IT posee ciertas características que le dan ventaja frente a otros marcos de referencia de Gestión de Riesgos. A continuación, en el Cuadro 2 (ver página siguiente), se muestra un cuadro comparativo entre los marcos y estándares para gestión de riesgos comúnmente usados en la industria[9]:

[9] Edzreena Edza Odzaly, Des Greer, Paul Sage. Óp.,cit.

Cuadro 2**.** Comparativo de marcos de referencia y estándares para gestión de riesgos

Principle/Feature	Risk IT		COSO ERM–Integrated Framework, 2004	ISO/FDIS 31000:2009	AS/NZS 4360:2004	ARMS, 2002		ISO 20000: 2005, Parts 1 and 2	PMBOK	ISO/IEC 27005:2008 ISO/IEC 27001:2005 ISO/IEC 27002:2005
Risk IT Principles										
Always connect to business objectives										
Align the management of IT-related business risk with overall ERM										
Balance the costs and benefits of managing risk										
Promote fair and open communication of IT risk										
Establish the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels										
Are a continuous process and part of daily activity										
Additional Features										
Availability (to the general public)										
Comprehensive view on IT (related) risk										
Dedicated focus on risk management practices for specific IT areas (project management, service management, security, etc.)										
Provide a detailed process model with management guidelines and maturity models										
Legend: Blue—Principle/feature is fully covered. Gray—Principle/feature is partially covered. White—Principle/feature is not covered.										

Fuente: The RISK IT Framework. ISACA.

2.3 MODELO DE MADUREZ CMMI

Origen: las dimensiones críticas de una empresa son: la gente, los procedimientos y métodos, y las herramientas y equipo. Los procesos son los encargados de unir tales dimensiones con el propósito de alcanzar los objetivos del negocio. El enfoque en los procesos ayuda a construir una plataforma de mejora continua, ya que se está de acuerdo en que la gente y la tecnología cambian y son sólo los procesos los que transcienden en el tiempo, adaptándose a nuevas personas y tecnologías.

El Software Engineering Institute (SEI) de la Carnegie Mellon University de los Estados Unidos, creador del modelo CMMI y de la mayoría de sus predecesores, ha elaborado sus modelos bajo la premisa que la calidad de un producto o servicio está altamente influenciada por la calidad de los procesos que los producen y los mantienen[10]. Es por ello que la mejora continua de los procesos debiese ir paulatinamente incrementando el nivel de capacidad y madurez de una organización.

Los procesos en conjunto transitan desde procesos no definidos, es decir, procesos cuya organización cuenta con poca capacidad y con inmadurez para realizarlos, a procesos disciplinados cuya organización cuenta con la capacidad y madurez suficiente para desarrollarlos con calidad probada. Luego una organización es capaz de definir su calidad total por medio del nivel de madurez de capacidades en que se encuentre de acuerdo a sus procesos.

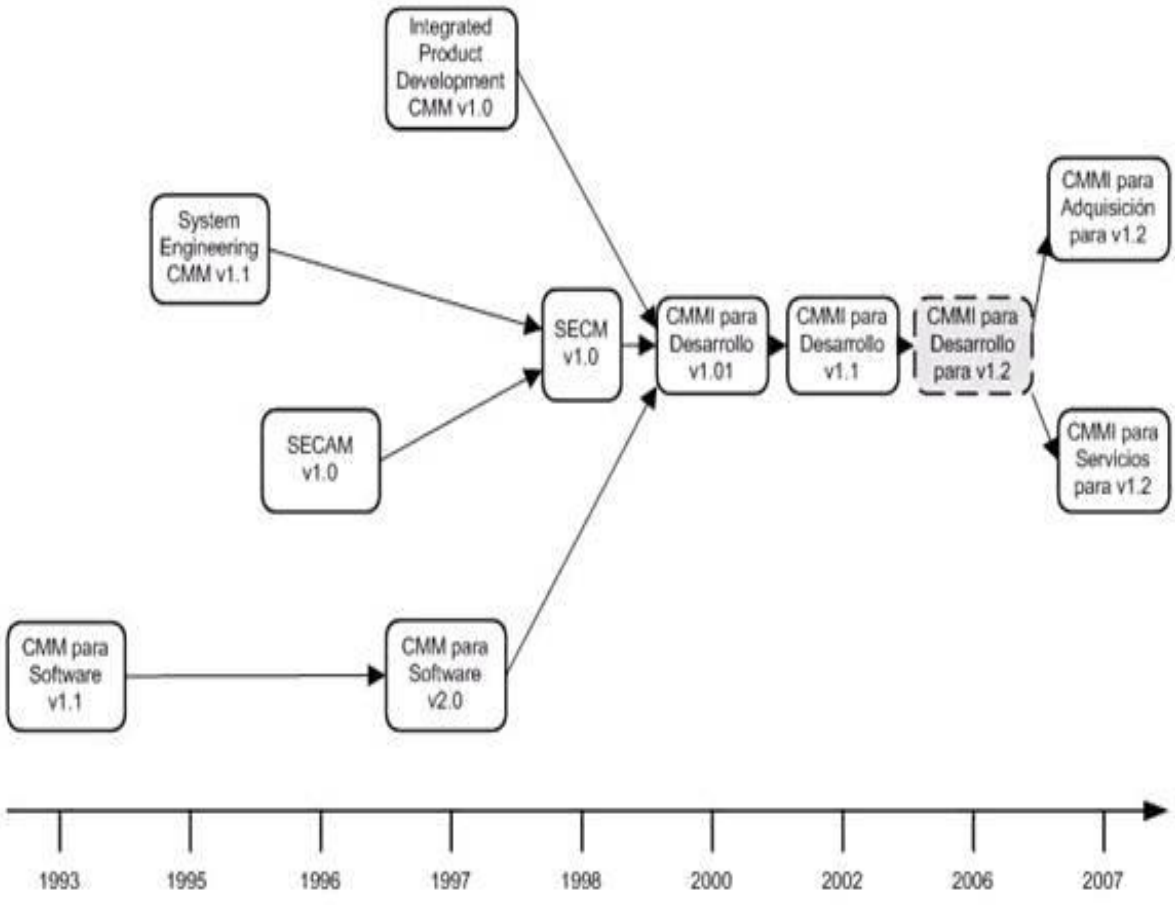
Modelos Previos: uno de los propósitos de CMMI fue unir en forma coherente varios modelos que eran utilizados en conjunto dentro de una organización y que

[10] CHRISSIS, Mary Beth; KONRAD, Mike y SHRUM, Sandy. "CMMI® for Development, v1.2", 2006.

generaban repetición de contenido provocando que el proceso de mejora llevado a cabo en la organización fuera más difícil y costoso.

Estos modelos integrados por CMMI, que serán descritos a continuación y que se ilustran en la Figura 6, eran modelos enfocados en el desarrollo de sistemas software (SW-CMM), en la ingeniería de sistemas (SECM) y en el desarrollo de productos integrados (IPD-CMM).

Figura 6**.** Modelos Previos a CMMI



Fuente: Capability Maturity Model Integration (CMMI). Software Engineering Institute.

CMMI Versión 1.2

Capability Maturity Model® Integration (CMMI) es un modelo de aseguramiento de la calidad que busca la mejora continua de las organizaciones mediante el análisis y re-diseño de los procesos que subyacen en la organización.

Fue creado por el SEI (Software Engineering Institute) de la Universidad de Carnegie-Mellon y patrocinado por el Ministerio de Defensa de los Estados Unidos. Con el propósito de lograr la mejora de los procesos, CMMI provee:

- Una forma de integrar los elementos funcionales de una organización[11].

- Un conjunto de mejores prácticas basadas en casos de éxito probado de organizaciones experimentadas en la mejora de procesos.

- Ayuda para identificar objetivos y prioridades para mejorar los procesos de la organización[12], dependiendo de las fortalezas y debilidades de la organización que son obtenidas mediante un método de evaluación.

- Un apoyo para que las empresas complejas en actividades productivas puedan coordinar sus actividades en la mejora de los procesos.

- Un punto de referencia para evaluar los procesos actuales de la organización[13].

CMMI v1.2 corresponde a la tercera versión entregable del modelo CMMI, posterior a las versiones 1.02 (primera versión año 2000) y 1.1 (año 2002). Las

[11] Software Engineering Institute, Carnegie Mellon University: What is CMMI?, [en línea]. Estados Unidos: SEI, septiembre 2007 [consultado Julio de 2011]. Disponible en Internet: http://www.sei.cmu.edu/cmmi/general/index.html.
[12] Ibíd., Disponible en Internet: http://www.sei.cmu.edu/cmmi/general/index.html.
[13] Ibíd., Disponible en Internet: http://www.sei.cmu.edu/cmmi/general/index.html.

versiones previas sirvieron como retroalimentación para que los propios usuarios, evaluadores y evaluados hicieran acotaciones sobre posibles mejoras, las cuales fueron estudiadas, refinadas y algunas incluidas en la versión 1.2. CMMI v1.2 para desarrollo, que corresponde a una de tres constelaciones de prácticas, es una guía que ayuda a manejar, medir y monitorear procesos[14] utilizados en el desarrollo de productos y servicios de una organización, y contiene prácticas ligadas a la administración de proyectos, administración de procesos, ingeniería y soporte.

Las otras dos constelaciones son CMMI para Adquisición que provee una guía para liderar la adquisición informada y decisiva[15], y CMMI para Servicios que proporciona una guía para la entrega de servicios a clientes internos y externos de la organización[16]. Ambas constelaciones se encuentran aún en desarrollo.

Junto con CMMI se desarrolló y publicó el método de evaluación "Assessment Requirements for CMMI (ARC)"[17] en el año 2000, el cual define los requerimientos considerados esenciales para realizar una evaluación de CMMI en una organización y "Standard CMMI Appraisal Method for Process Improvement", (SCAMPI)[18], manual seguido por los evaluadores para medir el nivel de madurez de una organización. Estos dos documentos también se han actualizado como consecuencia de la retroalimentación de la comunidad involucrada en CMMI,

[14] Software Engineering Institute, University Carnegie-Mellon: "Capability Maturity Model® Integration (CMMI), Version 1.2 Overview" [en línea]. Estados Unidos: SEI, 2007 [consultado Julio de 2011]. Disponible en Internet: http://www.sei.cmu.edu/cmmi/adoption/pdf/cmmi-overview07.pdf.
[15] Disponible en Internet: http://www.sei.cmu.edu/cmmi/adoption/pdf/cmmi-overview07.pdf.
[16] Disponible en Internet: http://www.sei.cmu.edu/cmmi/adoption/pdf/cmmi-overview07.pdf.
[17] Software Engineering Institute, Carnegie Mellon University: "ARC, V1.0 Assessment Requirements for CMMI Version 1.0" [en línea]. Estados Unidos: SEI, 2000 [consultado Julio de 2011]. Disponible en Internet: http://www.sei.cmu.edu/pub/documents/00.reports/pdf/00tr011.pdf.
[18] Software Engineering Institute, Carnegie Mellon University: "Standard CMMI Appraisal Method for Process Improvement (SCAMPI) Version 1.1: Method Definition Document" [en línea]. Estados Unidos: SEI, 2001 [consultado Julio de 2011]. Disponible en Internet: http://www.sei.cmu.edu/pub/documents/01.reports/pdf/01hb001.pdf.

generando la última versión 1.2 de SCAMPI[19] y ARC[20] ambas publicadas el año 2006.

Representaciones: la representación usada en CMMI entrega una guía para efectuar las actividades de mejora de los procesos y es utilizada en el método de evaluación. Según el modelo se tienen dos formas para mejorar. Una forma es mejorar un proceso específico o un conjunto de ellos usando la Representación Continua (Continuous Representation) y la otra es la mejora de la organización completa según los procesos definidos y ocupados usando la Representación Escalonada o por Etapas (Staged Representation). En el Cuadro 3 (ver página siguiente), se muestran los niveles para estos dos tipos de representaciones.

Representación Continua: la representación continua se focaliza en la mejora de un proceso o un conjunto de ellos relacionado(s) estrechamente a un área de proceso en que una organización desea mejorar, por lo tanto una organización puede ser certificada para un área de proceso en cierto nivel de capacidad.

Existen seis niveles de capacidad por donde transitan los procesos asociados a un área de proceso y cada nivel es construido sobre el nivel anterior, es decir para que un proceso alcance un nivel de capacidad necesariamente debe haber alcanzado el nivel anterior.

[19] Software Engineering Institute, Carnegie Mellon University: "A Standard CMMI Appraisal Method for Process Improvement (SCAMPI) Version 1.2: Method Definition Document" [en línea]. Estados Unidos: SEI, 2006 [consultado Julio de 2011]. Disponible en Internet: http://www.sei.cmu.edu/pub/documents/06.reports/pdf/06hb002.pdf.

[20] Software Engineering Institute, Carnegie Mellon University: "Appraisal Requirements for CMMI, Version 1.2 (ARC, V1.2)" [en línea]. Estados Unidos: SEI, 2006 [consultado Julio de 2011]. http://www.sei.cmu.edu/pub/documents/06.reports/pdf/06tr011.pdf.

Cuadro 3**.** Niveles de Representación continua y escalonada

	Representación Continua	*Representación Escalonada*
	Nivel de Capacidad	Nivel de Madurez
Nivel 0	Incompleto	-
Nivel 1	Realizado	Inicial
Nivel 2	Manejado	Manejado
Nivel 3	Definido	Definido
Nivel 4	Manejado cuantitativamente	Manejado cuantitativamente
Nivel 5	Optimizando	Optimizando

Fuente: CHRISSIS, Mary Beth; KONRAD, Mike y SHRUM, Sandy. "CMMI® for Development, v1.2", 2006.

Los niveles de capacidad son:

- Nivel 0 - Incompleto: Un proceso es denominado "proceso incompleto" cuando una o más objetivos específicos del área de proceso no son satisfechos.

- Nivel 1 – Realizado: Un proceso es denominado "proceso realizado" cuando satisface todos los objetivos específicos del área de proceso. Soporta y permite el trabajo necesario para producir artefactos[21].

- Nivel 2 – Manejado: Un proceso es denominado como "proceso manejado" cuando tiene la infraestructura base para apoyar el proceso. El proceso es planeado y ejecutado en concordancia con la política, emplea gente calificada los cuales tienen recursos adecuados para producir salidas controladas; involucra partes interesadas; es monitoreado, controlado y revisado; y es evaluado según la descripción del proceso[22].

[21] CHRISSIS, Mary Beth; KONRAD, Mike y SHRUM, Sandy. Óp., cit.
[22] Ibíd.,

- Nivel 3 – Definido: Un proceso denominado "proceso definido" es adaptado desde el conjunto de procesos estándares de la organización de acuerdo a las guías de adaptación de la organización, y aporta artefactos, medidas, y otra información de mejora a los activos organizacionales[23].

- Nivel 4 – Manejado cuantitativamente: Un proceso denominado "proceso manejado cuantitativamente" es controlado usando técnicas estadísticas y otras técnicas cuantitativas. Objetivos cuantitativos para la calidad y realización del proceso son establecidos y usados como criterios para manejar el proceso[24].

- Nivel 5 – Optimización: Un proceso denominado "proceso optimización es mejorado basado en el entendimiento de causas comunes de variación del proceso. Un proceso en optimización se focaliza en la mejora continua del proceso realizado a través de mejoras incrementales y usando innovación tecnológica[25]. Para más información consultar[26] y [27].

Representación Escalonada: en la representación escalonada o por etapas se ofrece un método estructurado y sistemático de mejoramiento de procesos, que implica mejorar por etapas o niveles.

Al alcanzar un nivel, la organización se asegura de contar con una infraestructura robusta en términos de procesos para optar a alcanzar el nivel siguiente. Por lo tanto es una organización la que puede ser certificada bajo un nivel, en este caso llamado nivel de madurez.

---

[23] Ibíd.,
[24] Ibíd.,
[25] Ibíd.,
[26] KULPA, Margaret K. y JOHNSON, Kent A. Interpreting the CMMI: A Process Improvement Approach, 2003.
[27] CHRISSIS, Mary Beth; KONRAD, Mike y SHRUM, Sandy. Óp., cit.

Según esta representación un nivel de madurez está compuesto por áreas de proceso (ver Cuadro 4) en donde los objetivos asociados a ese nivel deben ser cumplidos para que la organización pueda certificarse en aquel nivel de madurez. Hay cinco niveles de madurez, los que son descritos a continuación:

Cuadro 4**.** Áreas de Proceso del modelo CMMI

Área de proceso	**Categoría**	**Nivel de Madurez**
Análisis y Resolución Causales (CAR)	Soporte	5
Análisis y Resolución de Decisiones (DAR)	Soporte	3
Aseguramiento de la Calidad de Procesos y Productos (PPQA)	Soporte	2
Definición de Procesos Organizacionales +IPPD(OPD +IPPD)	Gestión de procesos	3
Desarrollo de Requerimientos (RD)	Ingeniería	3
Entrenamiento Organizacional (OT)	Gestión de procesos	3
Administración Cuantitativa de Proyectos (QPM)	Gestión de proyectos	3
Administración de Acuerdos con Proveedores (SAM)	Ingeniería	2
Administración de Requerimientos (REQM)	Gestión de proyectos	3
Administración de Riesgos (RSKM)	Soporte	2
Administración de la Configuración (CM)	Gestión de proyectos	3

Cuadro 4. (Continuación)

Área de proceso	Categoría	Nivel de Madurez
Administración Integral de Proyecto + IPD (IPM+IPPD) 1	Gestión de proyectos	3
Innovación y Despliegue Organizacional (OID)	Gestión de procesos	5
Integración de Producto (PI)	Ingeniería	3
Medición y Análisis (MA)	Soporte	2
Monitoreo y Control de Proyecto (PMC)	Gestión de proyectos	2
Planificación de Proyecto (PP)	Gestión de proyectos	2
Procesos Orientados a la Organizacionales (OPF)	Gestión de procesos	3
Rendimiento de Procesos Organizacionales (OPP)	Gestión de procesos	4
Solución Técnica (TS)	Ingeniería	3
Validación (VAL)	Ingeniería	3
Verificación (VER)	Ingeniería	3

Nivel 1: Iniciado

En el nivel de madurez 1, la mayoría de los procesos son "ad-hoc" y caóticos. La organización usualmente no provee un ambiente estable para soportar los

procesos. Éxitos en estas organizaciones se debe a la competencia y esfuerzos heroicos de la gente dentro de la organización y no al uso de procesos probados.

A pesar de este caos, organizaciones pertenecientes al nivel de madurez 1 con frecuencia producen productos y servicios que funcionan; sin embargo, ellos frecuentemente exceden sus presupuestos y no cumplen sus planes. Estas organizaciones son caracterizadas por la tendencia a no cumplir sus compromisos, al abandono de procesos durante tiempos de crisis, y a la incapacidad para repetir sus éxitos[28].

El Nivel 1 está caracterizado además por la realización de trabajo redundante, por personas que no comparten sus métodos de trabajo a lo largo de la organización y cuando una persona clave en un área de negocio específica dentro de la organización se marcha, su conocimiento se va con ella y se pierde para la organización. Es claro que el Nivel 1 es uno donde ninguna organización quiere estar y donde por lo general la mayoría que no tiene sus procesos definidos se encuentra.

- **Nivel 2: Manejado**

En el nivel de madurez 2 se ordena el caos. En el nivel 2 las organizaciones se enfocan en tareas cotidianas referentes a la administración. Cada proyecto de la organización cuenta con una serie de procesos para llevarlo a cabo, los cuales son planeados y ejecutados de acuerdo con políticas establecidas; los proyectos utilizan gente capacitada quienes disponen de recursos para producir salidas controladas; se involucran a las partes interesadas; son monitoreados, controlados y revisados; y son evaluados según la descripción del proceso.

[28] Ibíd.,

La disciplina del proceso reflejada por el nivel de madurez 2 ayuda a asegurar que existen prácticas y los proyectos son realizados y manejados de acuerdo a los planes documentados. En el nivel de madurez 2 el estado de los artefactos y la entrega de los servicios siguen planes definidos.

Acuerdos son establecidos entre partes interesadas y son revisados cuando sea necesario[29]. Los artefactos y servicios son apropiadamente controlados. Estos además satisfacen sus descripciones especificadas, estándares, y procedimientos[30].

- **Nivel 3: Definido**

En el nivel de madurez 3, procesos son caracterizados y entendidos de buena forma, y son descritos en estándares, procedimientos, herramientas, y métodos. El conjunto de procesos estándares de la organización, los cuales son la base para el nivel de madurez 3, es establecido y mejorado continuamente. Estos procesos estándares son usados para establecer consistencia a través de la organización. Los proyectos establecen sus procesos adaptando el conjunto de procesos estándares de la organización de acuerdo a guías de adaptación[31].

Una diferencia importante entre el nivel 2 y 3 es el alcance de los estándares: la descripción de procesos y los procedimientos. En el nivel de madurez 2, los estándares pueden ser un poco diferentes en cada instancia específica del proceso (por ejemplo sobre un proyecto particular). En el nivel de madurez 3, los estándares, descripción de procesos y procedimientos para un proyecto, son

[29] Ibíd.,
[30] Ibíd.,
[31] Ibíd.,

adaptados desde un conjunto de procesos estándares de la organización a un particular proyecto o unidad organizacional y así son más consistentes[32].

Otra distinción crítica es que el nivel de madurez 3, los procesos son típicamente descritos más rigurosamente que en el nivel 2. Un proceso definido claramente plantea el propósito, entradas, criterios de entrada, actividades, roles, medidas, pasos de verificación, salidas y criterios de salida. En el nivel de madurez 3, procesos son manejados más proactivamente entendiendo las interrelaciones de las actividades y medidas detalladas del proceso, sus artefactos y sus servicios[33].

- **Nivel 4: Manejado cuantitativamente**

En el nivel de madurez 4, la organización y proyectos establecen objetivos cuantitativos para medir la calidad y realización de los procesos y los usa como criterios en el manejo de ellos. Los objetivos cuantitativos son definidos en base a las necesidades de clientes, usuarios finales, organización, y actores de los procesos. La calidad y realización de procesos son entendidos en términos estadísticos y son manejados durante todo el ciclo de vida del proceso[34].

Para subprocesos seleccionados, se recolectan y analizan estadísticamente medidas sobre la realización de procesos. Estas métricas son incorporadas en el repositorio de métricas de la organización para apoyar la toma de decisiones. Causas especiales de variación de procesos son identificadas y, cuando sea necesario, las fuentes de estas causas son corregidas para prevenir futuras ocurrencias.

[32] Ibíd.,

[33] Ibíd.,
[34] Ibíd.,

Una diferencia importante entre los niveles 3 y 4 es la capacidad de predicción de la realización del proceso. En el nivel de madurez 4, la realización de procesos es controlada usando técnicas estadísticas y cuantitativas, y el proceso es cuantitativamente predecible, en cambio en el nivel de madurez 3 la realización del proceso es sólo predecible cualitativamente[35].

- **Nivel 5: Optimizado**

En el nivel de madurez 5, una organización mejora continuamente sus procesos basándose en el conocimiento de las causas comunes de variación inherente en los procesos. El nivel de madurez 5 se focaliza sobre la mejora continua de los procesos a través de mejoras continuas, incrementales y tecnológicas.

Los objetivos de mejora cuantitativa de procesos para la organización son establecidos, continuamente revisados para reflejar cambios en los objetivos del negocio y usados como criterio en la mejora de procesos. Los efectos del empleo de las mejoras de procesos son medidos y evaluados contra los objetivos de mejora cuantitativa del proceso.

Una diferencia importante entre el nivel de madurez 4 y 5 es el enfoque de la variación de los procesos. En el nivel de madurez 4, la organización está orientada a encontrar causas especiales de variación y proveer una predicción estadística de los resultados. Sin embargo, los resultados pueden ser insuficientes para alcanzar los objetivos establecidos. En el nivel de madurez 5 la organización está enfocada en las causas comunes de variación de procesos y modificar los procesos afectados para mejorar la realización de ellos y alcanzar los objetivos cuantitativos de mejora de procesos[36].

[35] Ibíd.,
[36] Ibíd.,

Dado a que la organización con que se trabajará quiere certificarse en forma organizacional en Nivel de madurez 3, en adelante sólo se detallará el modelo según la Representación Escalonada.

Estructura del CMMI: Un área de proceso es un conjunto de prácticas relacionadas que cuando son implementadas colectivamente, satisfacen un conjunto objetivos considerados importantes para mejorar esa área de proceso. Las áreas de proceso del modelo son 22. En el Cuadro 4 se indica los nombres de las áreas de proceso junto con su abreviación.

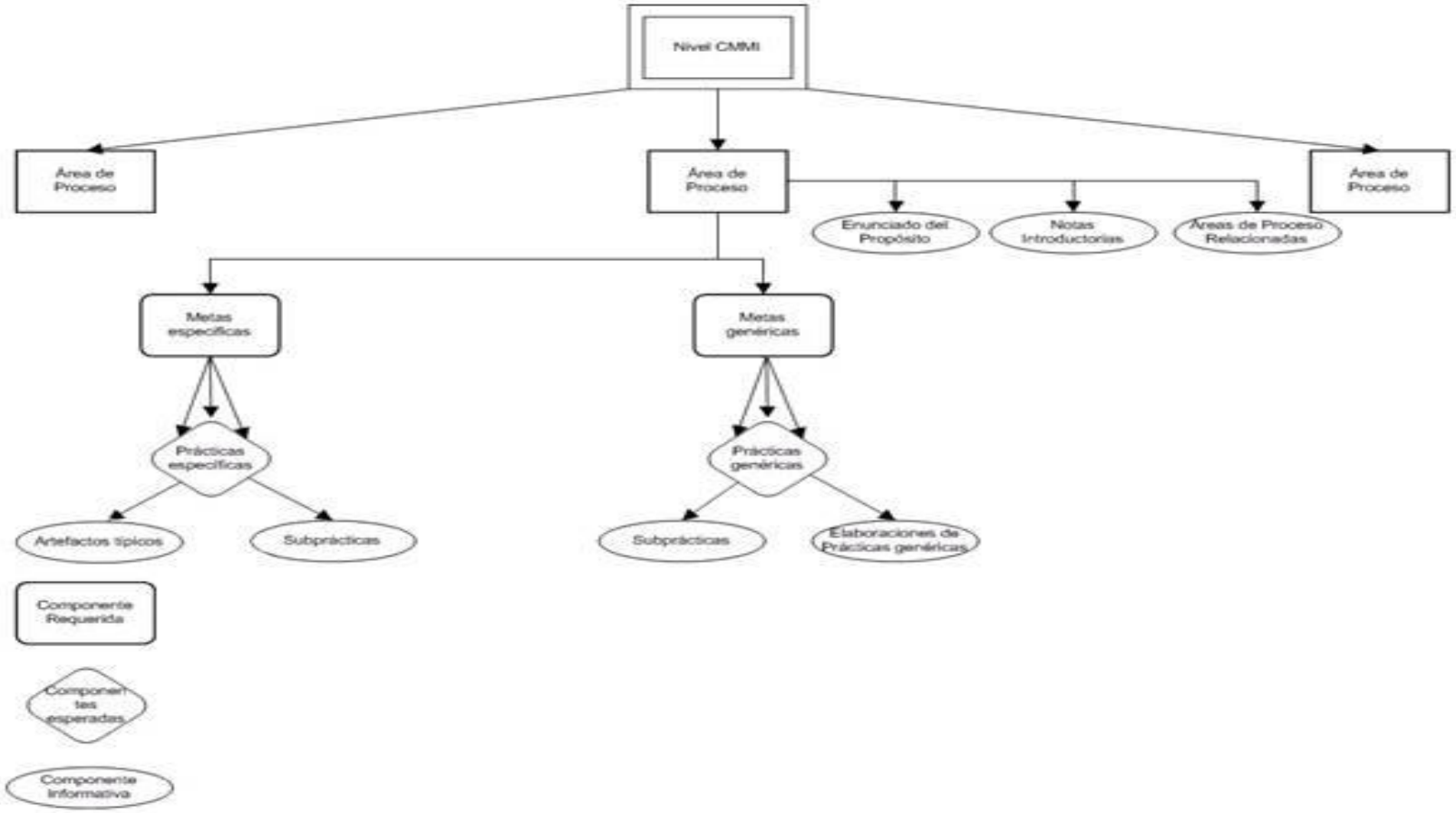
Cada una de ellas es implementada para alcanzar el nivel de madurez correspondiente y se agrupan de acuerdo a cuatro categorías: Administración de Procesos, Administración de Proyectos, Ingeniería y Soporte. Este agrupamiento es realizado para mostrar cómo se relaciona cada área de proceso dentro de una categoría. Sin embargo, áreas de procesos de distintas categorías pueden encontrarse relacionadas.

- **Componentes.** Aunque los componentes son independientes de la representación elegida, se definirán de acuerdo al esquema propuesto por la Representación Escalonada que es la requerida por ORDEN Integración.

Como se puede apreciar en la Figura 7 (ver página siguiente) un área de proceso está asociado a un nivel de madurez dentro de CMMI; tiene además un conjunto de objetivos específicos y uno o varios objetivos genéricos asociados, dependiendo del nivel de madurez al cual pertenece el área de proceso; los objetivos específicos y genéricos cuentan con un conjunto de prácticas específicas y prácticas genéricas respectivamente.

CMMI define componentes requeridos, esperados e informativos. Los Componentes informativos sólo son una ayuda propuesta por el modelo para entender de mejor manera los componentes requeridos y esperados.

Figura 7**.** Componentes del CMMI – Representación Escalonada.



Fuente: Capability Maturity Model Integration (CMMI). Software Engineering Institute.

Componentes Requeridos: son los componentes que obligatoriamente deben ser satisfechos y visiblemente implementados para poder cumplir con un área de proceso. Un componente requerido es usado en las evaluaciones para ayudar a determinar si un área de proceso es satisfecho[37]. Existen dos componentes requeridos:

- Objetivo Específico (SG): es un enunciado que describe la única característica que deber estar presente para satisfacer el área de proceso a la cual pertenece[38]. Las SG son parte de un área de proceso.

- Objetivo Genérico (GG): es un enunciado que describe una característica que debe ser satisfechas por un conjunto de áreas de proceso según sea el caso. Las GG tienen el objetivo de institucionalizar los procesos que implementan un área de proceso y son comunes a un conjunto de áreas de proceso[39].

Componentes esperados: son los componentes que pueden ser utilizados para alcanzar un componente requerido, es decir se podrían implementar estos componentes o modificaciones válidas de ellos con el objetivo de alcanzar los objetivos genéricos o específicos. Los componentes esperados pueden ser utilizados como guías de mejora y de evaluación de procesos[40]. Existen dos tipos de componentes esperados:

- Prácticas Específicas (SP): Una práctica específica es un enunciado que describe una actividad que es importante o esperada para alcanzar un objetivo específico de cierta área de proceso[41].

---

[37] Ibíd.,
[38] Ibíd.,
[39] Ibíd.,
[40] Ibíd.,
[41] Ibíd.,

- Prácticas Genéricas (GP): Una práctica genérica es un enunciado que describe una actividad que es importante o esperada para alcanzar un objetivo genérico[42].

Descripción de las Áreas de Proceso: a continuación se hará una breve descripción de cada área de proceso nombrada en el Cuadro 4 (página 56). Explícitamente se nombra a productos pero también se puede aplicar las mismas definiciones a servicios.

- Análisis y Resolución Causales (CAR): identifica la causa de defectos u otros problemas. Luego de ellos toma acciones correctivas para prevenir la ocurrencia de tales defectos o problemas en el futuro.

- Análisis y Resolución de Decisiones (DAR): proporciona un proceso estructurado de toma de decisiones que asegura que las alternativas se comparan con criterios establecidos y objetivos para así tomar la mejor decisión posible.

- Aseguramiento de Calidad de Procesos y Productos (PPQA): proporciona un conjunto de prácticas con el objetivo de evaluar productos, servicios, procesos y sus artefactos relacionados.

- Definición de Procesos Organizacionales (OPD): establece y mantiene un conjunto de estándares tanto en procesos organizacionales como en ambientes de trabajo.

- Desarrollo de Requerimientos (RD): recopila las necesidades del cliente para convertirlas en requerimientos del producto esperado.

[42] Ibíd.,

- Entrenamiento Organizacional (OT): permite a la gente de la organización obtener habilidades y conocimientos necesarios para que el trabajo realizado por ellos sea efectivo y eficiente.

- Administración Cuantitativa de Proyectos (QPM): maneja métricas cuantitativas de los procesos con el objetivo de alcanzar los objetivos de calidad establecidos. Además mediante el análisis de estos datos permite identificar oportunidades de mejora para los procesos.

- Administración de Acuerdos con Proveedores (SAM): gestiona la adquisición de productos de proveedores con los cuales exista un acuerdo formal[43].

- Administración de Requerimientos (REQM): gestiona los requerimientos del producto durante todo el ciclo de vida de él, identificando inconsistencias con los artefactos y planes de proyecto.

- Administración de Riesgos (RSKM): identifica riesgos del proyecto para evaluarlos, priorizarlos y gestionarlos para prevenir su futura ocurrencia.

- Administración de la Configuración (CM): establece y mantiene la integridad y consistencia de los artefactos[44].

- Administración Integral de Proyecto (IPM): adapta el conjunto de procesos estándares de la organización a procesos llevados a cabo para un proyecto en particular. Además maneja a las partes interesadas involucradas en el proyecto.

---

[43] RIGONI, Cecilia: "CMMI®: Mejora del proceso en Fábricas de Software" [en línea]. España: MITYC, 2006 [consultado julio de 2011]. Disponible en Internet: http://www.mityc.es/NR/rdonlyres/A570B90C-B41A-46E2-BD39-4A31D18BB7FD/0/s01CeciliaRigoni.pdf.

[44] Ibíd., Disponible en Internet: http://www.mityc.es/NR/rdonlyres/A570B90C-B41A-46E2-BD39-4A31D18BB7FD/0/s01CeciliaRigoni.pdf.

- Innovación y Despliegue Organizacional (OID): selecciona y despliega mejoras incrementales e innovadoras que mejoran en forma medida los procesos de la organización y tecnologías, para alcanzar los objetivos de calidad organizacional y de realización de procesos derivados de los objetivos de negocio de la organización[45].

- Integración de Producto (PI): ensambla las componentes del producto para producir un producto más complejo manteniendo el cumplimiento de los requerimientos establecidos.

- Medición y Análisis (MA): establece métricas con el objetivo de entregar resultados objetivos que sirvan como base para tomar decisiones informadas y correctivas.

- Monitoreo y Control de proyecto (PMC): analiza el proyecto con el objetivo de establecer un control y evaluación según los planes establecidos, tomando acciones correctivas cuando es necesario.

- Planificación de Proyecto (PP): desarrolla y mantiene planes del proyecto, compromisos adquiridos por parte de los participantes del proyecto y gestiona las partes interesadas del proyecto.

- Procesos Orientados a la Organización (OPF): ayuda a mantener un entendimiento de los procesos por parte de los miembros de la organización. También ayuda a identificar posibles mejoras de los procesos, que son evaluadas y eventualmente implementadas.

[45] CHRISSIS, Mary Beth; KONRAD, Mike y SHRUM, Sandy. Óp., cit.

- Rendimiento de Procesos Organizacionales (OPP): deriva objetivos cuantitativos de calidad y ejecución de los procesos desde el conjunto de objetivos de negocio de la organización[46].

- Solución Técnica (TS): diseña, desarrollo e implementa soluciones para los requerimientos del producto establecido.

- Validación (VAL): Demuestra que el producto, componentes del producto y artefactos corresponden a lo esperado para su uso.

- Verificación (VER): demuestra que el producto, componentes del producto y artefactos cumplen con los requerimientos establecidos.

Área de Procesos RSKM

Propósito: el propósito de la Gestión de riesgos (RSKM) es identificar los problemas potenciales antes de que ocurran para que las actividades de tratamiento de riesgos puedan planificarse e invocarse según sea necesario a lo largo de la vida del producto o del proyecto para mitigar los impactos adversos para alcanzar los objetivos[47].

Notas introductorias: la gestión de riesgos es un proceso continuo, orientado a evaluar el futuro, y una parte importante de la gestión. La gestión de riesgos debería tratar los aspectos que podrían poner en peligro el logro de los objetivos críticos. Una aproximación de gestión de riesgos continua se aplica para anticipar y mitigar eficazmente los riesgos que puedan tener un impacto crítico sobre el proyecto.

[46] RIGONI, Cecilia. Óp., cit. Disponible en Internet: http://www.mityc.es/NR/rdonlyres/A570B90C-B41A-46E2-BD39-4A31D18BB7FD/0/s01CeciliaRigoni.pdf.
[47] CHRISSIS, Mary Beth; KONRAD, Mike y SHRUM, Sandy. Óp., cit.

La gestión de riesgos eficaz incluye la identificación temprana y agresiva de cada riesgo a través de la colaboración y la involucración de las partes interesadas relevantes, tal y como se describió en el plan para la involucración de las partes interesadas que se trata en el área de proceso de Planificación de proyecto. Es necesario un fuerte liderazgo entre las partes interesadas relevantes para establecer un entorno para la libre y abierta divulgación y discusión de los riesgos.

La gestión de riesgos debe considerar fuentes tanto internas como externas para riesgos de coste, de calendario y de rendimiento, así como de otros tipos. La detección temprana y agresiva del riesgo es importante porque normalmente es más fácil, menos costoso y menos perjudicial hacer los cambios y corregir los esfuerzos de trabajo durante las fases más tempranas del proyecto, en lugar de en fases posteriores.

La gestión de riesgos puede dividirse en tres partes: definir una estrategia de gestión de riesgos, identificar y analizar los riesgos, y manejar los riesgos identificados, incluyendo la implementación de los planes de mitigación de riesgo, cuando sea necesario.

Las organizaciones pueden inicialmente enfocarse simplemente en la identificación del riesgo para tomar conciencia del mismo, y reaccionar ante la materialización de estos riesgos a medida que ocurren.

El área de proceso de Gestión de riesgos describe una evolución de estas prácticas específicas para planificar, prevenir y mitigar los riesgos sistemáticamente a fin de minimizar proactivamente su impacto sobre el proyecto. Aunque el énfasis principal del área de proceso de Gestión de riesgos se realiza

sobre el proyecto, los conceptos también pueden aplicarse para gestionar los riesgos de la organización[48].

Resumen de Metas y prácticas específicas

Las siguientes son las metas y prácticas específicas que componen el área de proceso RSKM:

SG 1 Preparar la gestión de riesgos.

- SP 1.1 Determinar las fuentes y las categorías de los riesgos.
- SP 1.2 Definir los parámetros de los riesgos.
- SP 1.3 Establecer una estrategia de gestión de riesgos.

SG 2 Identificar y analizar los riesgos.

- SP 2.1 Identificar riesgos.
- SP 2.2 Evaluar, categorizar y priorizar los riesgos.

SG 3 Mitigar los riesgos.

- SP 3.1 Desarrollar los planes de mitigación de riesgo.
- SP 3.2 Implementar los planes de mitigación de riesgo.

[48] Ibíd.,

3. ESTRATEGIA PROPUESTA

Las empresas que emplean el modelo de mejora CMMI como referente para la definición y mejora de los procesos de desarrollo y mantenimiento de software carecen de lineamientos y herramientas tangibles que les permitan llevar las recomendaciones del modelo de madurez a actividades específicas de los procesos.

Para hacer frente a esta problemática la industria provee una serie de estándares y marcos de referencia con el fin de proveer un conjunto de mejores prácticas que permitan a las organizaciones, traducir las recomendaciones en procesos y procedimientos.

Una de los procesos de la industria que se ve afectado por esta problemática es el proceso de gestión de riesgos. En este ámbito particular, la industria ha desarrollado estándares y marcos de referencia especializados en este proceso con el objetivo de generar un conjunto de actividades para cubrir los diversos procesos necesarios en la gestión de riesgos.

La estrategia propuesta para este trabajo es emplear el marco de referencia para gestión de riesgos RISK IT como complemento a la gestión de riesgos realizada en las empresas objetivo, dando cumplimiento a los lineamientos definidos por el área de procesos RSKM del marco de referencia CMMI y reforzando el proceso mediante la aplicación de actividades propuestas en RISK IT.

3.1 ENCUESTA VALORACIÓN PROCESO DE GESTIÓN DE RIESGOS

Adicional a evidenciar que el proceso de gestión de riesgos a nivel general en la industria del software presenta barreras al momento de realizar su implementación, es importante determinar cuáles son los principales aspectos por reforzar en las empresas con valoración CMMI nivel 3. Esto debido a que las empresas que ya han implementado RSKM poseen un proceso de gestión de riesgos basado en recomendaciones dadas por el SEI y esto garantiza que se han cubierto aspectos básicos del proceso y se han superado barreras iniciales.

Para determinar el estado actual del proceso de gestión de riegos en las empresas valoradas nivel 3 o superior de CMMI con implementación escalonada, se aplicó una encuesta (ver Anexo A) a empresas del sector valoradas en el nivel objetivo (ver Anexo B).

La encuesta se encuentra orientada a determinar cuáles son los aspectos más relevantes del proceso de gestión de riesgos que poseen mayores oportunidades de mejora y reforzamiento a partir del planteamiento de la gestión de riesgos propuesta por ISACA en RISK IT.

Se busca identificar el estado de la gestión de riesgos en sus principales procesos como son la identificación, la evaluación y la respuesta al riesgo, para lo cual se generaron 16 preguntas puntuales que permiten establecer la frecuencia con la que se realizan ciertas actividades relacionadas con la gestión de riesgos.

Para determinar el nivel de frecuencia con que se realizan las actividades se estableció una escala de 5 niveles los cuales se listan en el cuadro 5.

Cuadro 5**.** Niveles de Frecuencia con los que se ejecutan actividades de gestión de riesgos.

Ítem	Nivel	Valor
1	Nunca	1
2	Rara vez	2
3	A veces	3
4	Frecuentemente	4
5	Siempre	5

Las preguntas realizadas están agrupadas en 6 categorías que son listadas en el Cuadro 6 (ver página siguiente), las cuales representan aspectos generales, fundamentales en la Gestión de riegos.

Cuadro 6**.** Categorías de preguntas para determinar el estado general de la gestión de riesgos.

Ítem	Categoría	Contexto
1	Modelos y planes definidos	Modelos y planes de Identificación y respuesta al riesgo
2	Comunicación	Comunicación de la información relacionada con la Gestión de riesgos a las personas interesadas.
3	Apetito del Riesgo	Umbrales de exposición al riesgo e identificaciones de nuevas oportunidades, incluyendo riesgos positivos.
4	Reportes	Informes de gestión y análisis de riesgos.
5	Seguimiento y Control	Análisis de desempeño y supervisión de los controles.
6	Responsabilidad	Roles y responsabilidades de las personas interesadas.

Una vez aplicada la encuesta de valoración se detectó que en la mayoría de empresas, las actividades relacionadas con la gestión de riesgos que presentan más baja frecuencia de realización, son la que corresponden a las preguntas de las categorías de Modelos y planes definidos, y Apetito al riesgo.

A partir de lo anterior puede interpretarse que las empresas a pesar que han establecido el modelo CMMI con su área de proceso RSKM para dar cumplimiento a las exigencias de valoración, no cuentan con modelos claros de identificación de riesgos, ni buscan incrementar constantemente el apetito al riesgo, enfocando esfuerzos solamente a mitigar los riesgos ya identificados por incidentes pasados o en el proceso inicial de implantación del modelo.

Se sabe que los modelos de identificación son parte fundamental de la gestión de riesgos debido a que permiten recolectar información que es relevante para la empresa, la cual muchas veces deja de ser importante a causa de la evolución natural de las organizaciones, así mismo se debería tener en cuenta información relacionada con la industria, lo cual permite realizar un mejoramiento continuo de del proceso, de sus fuentes riesgo y de sus planes de acción.

Es aquí donde modelos como CMMI se quedan cortos al no tener recomendaciones detalladas acerca de estos aspectos tan importantes y simplemente se limitan a exigirlo en los procesos de valoración, independientemente del mecanismo o completitud de los mismos.

Por otro lado se ve que las empresas tradicionales no han establecido o formalizado procesos para incrementar el apetito al riesgo, el cual cada vez toma más auge en la gestión de riesgos debido a que permite ampliar los umbrales de exposición al riesgo, lo cual trae como consecuencia la identificación de nuevas y

mejores oportunidades relacionadas con el entorno que permiten mejorar el crecimiento y el retorno de valor hacia la empresa.

Así mismo se observa que algunas empresas siguen manejando el concepto de riesgo como algo negativo, por lo cual no evalúan o analizan los riesgos positivos que pueden haber en el entorno y que traen consigo beneficios a la empresa, al controlarlos e identificarlos de manera adecuada.

Se observa que los resultados de la encuesta de gestión de riesgos permitió identificar claramente que existen oportunidades de mejora en estos aspectos, algo que el marco de referencia RISK IT tiene inmerso en las diferentes actividades que recomienda, así como en sus principios y fundamentos de gestión de riesgos que rigen dichas actividades, alineándolas siempre con los objetivos de la empresa, para obtener el mayor retorno de valor posible.

3.2 ALINEACIÓN DE RSKM CON RISK IT

Inicialmente, es importante determinar qué nivel de cubrimiento tienen las empresas valoradas nivel 3 o superior de CMMI con implementación escalonada con respecto al marco de referencia RISK IT. A nivel general, esta alineación permite tener visión general del camino ya recorrido en el proceso de gestión de riesgos establecido por RISK IT a partir de la implementación de RSKM.

Para las empresas que ya han implementado RSKM tener esta visión unificada de los modelos permite dos objetivos. El primero radica en el aprovechamiento de los procesos ya desarrollados para gestión de riesgos en la organización, pues al implementar RSKM las empresas ya han ganado experiencia en el camino recorrido y ésta debe ser reconocida y conservada. El segundo reside en la

identificación de los componentes puntuales en los cuales debe ser reforzado o complementado el proceso de gestión de riesgos desde la perspectiva de RISK IT.

Para realizar la alineación de los modelos inicialmente se debe revisar la estructura de cada uno y determinar el nivel a trabajar en cada modelo para realizar el análisis de cubrimiento de RSKM con respecto a RISK IT.

Por un lado, el modelo CMMI propone un conjunto de prácticas específicas y genéricas para cada una de las metas que componen las áreas de proceso. Este conjunto de prácticas, son una guía para la implementación de procesos orientados a satisfacer las características requeridas por las metas específicas y generales de cada área de proceso.

Por su lado, RISK IT, se compone de un conjunto de Dominios de Proceso que se subdivide en procesos que se componen de actividades. Estas actividades establecen una guía para realizar los procesos establecidos por RISK IT para llevar a cabo la gestión de riesgos.

Debido a que los niveles superiores de los modelos (metas y dominios de proceso) resultan muy generales, se hace necesario llevar el análisis a niveles inferiores de la estructura de cada uno con el fin de verificar aspectos puntuales. Cabe anotar que ambos modelos proponen una serie de recomendaciones pero ninguno obliga a realizar de manera detallada las prácticas o actividades pues estas solo establecen una guía.

A pesar de lo anterior, se analiza el modelo de CMMI a nivel de prácticas y el marco de referencia RISK IT a nivel de actividades pues este nivel de detalle nos permite aterrizar ambos modelos a aspectos puntuales permitiendo así realizar la

verificación de cubrimiento del modelo RISK IT a partir de las prácticas establecidas por RSKM de CMMI de una manera estructurada.

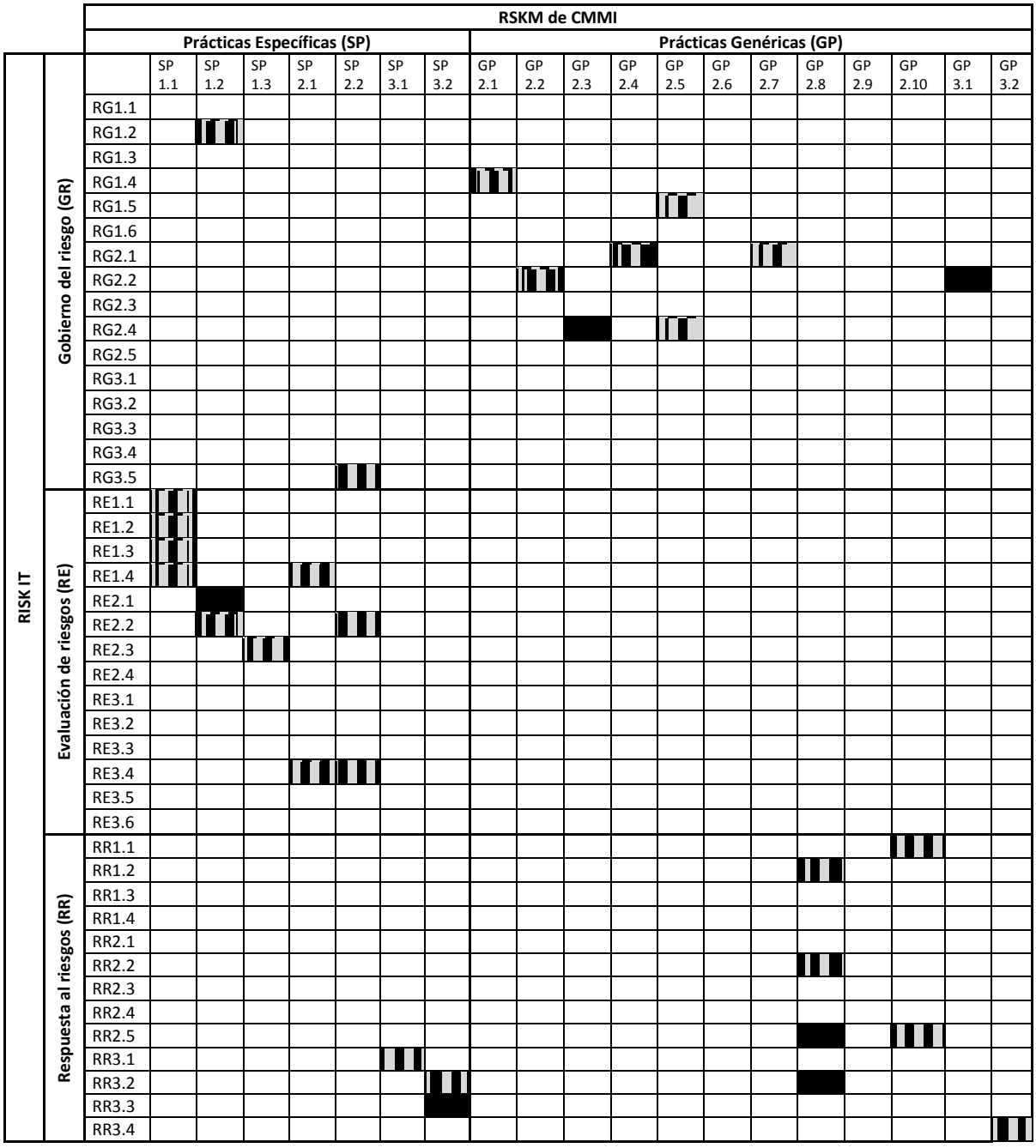
A continuación en el cuadro 7 (ver página 78), se observa un panorama general del nivel de cubrimiento para las actividades de RISK IT contribuido por cada una de las prácticas generales y específicas establecidas por el área de proceso RSKM. El nivel de cubrimiento se determina en una escala de 3 valores:

- Sin cubrimiento. Al realizar la práctica establecida por RSKM no se realiza la actividad indicada por RISK IT.
- Cubrimiento Parcial. Al realizar la práctica establecida por RSKM se realiza parcialmente la actividad indicada por RISK IT.

- Cubrimiento Total. Al realizar la práctica establecida por RSKM se realiza totalmente la actividad indicada por RISK IT.

(Ver Cuadro 7, página siguiente),

Cuadro 7**.** Cubrimiento de RISK IT a partir de las prácticas generales y específicas de RSKM



	Sin cubrimiento
	Cubrimiento parcial
	Cubrimiento total

A continuación en el Cuadro 8, se detallan las prácticas específicas de RSKM, para cada una de ellas el cubrimiento realizado de las actividades de RISK IT y el criterio empleado para indicar si el cubrimiento se realiza de manera total, parcial o no hay cubrimiento.

Cuadro8**.** Cubrimiento de RISK IT a partir de las prácticas específicas de RSKM

Practica específica	Nivel de Cubrimiento	Criterios del Cubrimiento
SP 1.1 Determinar las fuentes y las categorías de los riesgos.	Parcialmente RE1.1 Parcialmente RE1.2 Parcialmente RE1.3 Parcialmente RE1.4	RE1.1. RSKM no define un modelo para recolección de datos. Adicionalmente RISK IT establece incentivos para generación de cultura de riesgo. RE1.2. RSKM no contempla como fuentes externas información de la industria. RE1.3. Se cubre bajo la premisa que RSKM analiza información histórica de los proyectos en lo referente a riesgos. RSKM no recopila fuentes de habilitación de valor. RE1.4. RSKM no recoge información acerca de las condiciones existentes en el momento en que se presentó el evento de riesgo.
SP 1.2 Definir los parámetros de los riesgos.	Parcialmente RG1.2 Completamente RE2.1 Parcialmente RE2.2	RG1.2 RSKM no define los umbrales por el impacto particular a cada línea de negocio. No define los umbrales a partir de la relación beneficio/valor. RE2.1. RSKM define en esta práctica el alcance que se va a dar al proceso de gestión de riesgos RE2.2. RSKM define el impacto negativo (perdida) de los riesgos pero no tiene en cuenta el impacto positivo (ganancia) asociado a un riesgo.
SP 1.3 Establecer una estrategia de gestión de riesgos.	Parcialmente RE2.3	RE2.3. RSKM solo contempla la mitigación como estrategia de respuesta al riego mientras que RISK IT propone la selección de una de las respuestas al riesgo Mitigar, Aceptar, Transferir o Evitar.
SP 2.1 Identificar riesgos.	Parcialmente RE1.4 Parcialmente RE3.4	RE1.4 RSKM establece el contexto bajo el cual se presenta el riesgo. La recolección de datos es cubierta por la práctica específica 1.1 RE3.4 RSKM no establece enlaces entre los tipos de riesgos y las categorías de riesgos.

Cuadro 8. (Continuación)

Practica específica	Nivel de Cubrimiento	Criterios del Cubrimiento
SP 2.2 Evaluar, categorizar y priorizar los riesgos.	Parcialmente RE2.2 Parcialmente RE3.4 Parcialmente RG3.5	RE2.2. RSKM no establece controles operativos RE3.4 No caracteriza por sector de negocio y áreas funcionales. RG3.5. Se realiza priorización de riesgos, pero RISK IT lo hace a través de la cartera de actividades de respuesta al riesgo (revisión de costo/beneficio)
SP 3.1 Desarrollar los planes de mitigación de riesgo.	Parcialmente RR3.1	RR3.1. No tiene en cuenta en la elaboración del plan el impacto a nivel organizacional. En RSKM siempre se mitiga (Plan de mitigación o contingencia), en RISK IT es posible que la organización permanezca expuesta a un riesgo durante un determinado periodo de tiempo.
SP 3.2 Implementar los planes de mitigación de riesgo.	Parcialmente RR3.2 Completamente RR3.3	RR3.2. RSKM no establece comunicar los impactos comerciales a los tomadores de decisiones RR3.3 Se determinan los planes de acción para tratar los riesgos.

A continuación en el Cuadro 9, se detallan las prácticas genéricas de RSKM, para cada una de ellas el cubrimiento realizado de las actividades de RISK IT y el criterio empleado para indicar si el cubrimiento se realiza de manera total, parcial o no hay cubrimiento.

Cuadro 9**.** Cubrimiento de RISK IT a partir de las prácticas genéricas de RSKM.

Práctica Genérica	Nivel de Cubrimiento	Criterios del Cubrimiento
GP 2.1 establecer una política de la organización	Parcialmente RG1.4	RG1.4. Se realiza la definición de la política de gestión de riesgos pero RSKM no define apetito por el riesgo ni tolerancia

Cuadro 9. (Continuación)

Práctica Genérica	Nivel de Cubrimiento	Criterios del Cubrimiento
GP 2.2 planificar el proceso	Parcialmente RG2.2	RG2.2 RSKM no coordina la estrategia de gestión de riesgos con la estrategia de riesgo empresarial
GP 2.3 proporcionar recursos	Completamente RG2.4	RG2.4 Se identifican los recursos necesarios para la gestión de riesgos.
GP 2.4 asignar responsabilidad	Parcialmente RG2.1	RG2.1 RSKM no establece medición de desempeño ni procesos de presentación de informes.
GP 2.5 formar a las personas	Parcialmente RG1.5 Parcialmente RG2.4	RG 1.5 RSKM no fomenta la cultura del riesgo, ni genera escenarios para promover actividades no especificadas en las políticas de gestión de riesgo. RG2.4 RSKM en esta práctica hace referencia a la selección y formación de personas para el proceso de gestión de riesgos mientras que RISK IT habla de todos los recursos para el proceso.
GP 2.6 gestionar configuraciones		No hay actividades en RISK IT para el cubrimiento de esta práctica.
GP 2.7 identificar e involucrar a las partes interesadas relevantes	Parcialmente RG2.1	RG2.1 RSKM no establece medición de desempeño ni procesos de presentación de informes.
GP 2.8 monitorizar y controlar el proceso	Parcialmente RR1.2 Parcialmente RR2.2 Completamente RR2.5 Completamente RR3.2	RR1.2 En RSKM no hacen énfasis en los principios de pertinencia, eficiencia, puntualidad y precisión, para asegurar q la información sea estratégica y que no se pierda tiempo en análisis poco relevantes. RR2.2 En RSKM no se establece que se deba configurar donde enviar las notificaciones para que los implicados puedan responder oportunamente. RR2.5 Revisa los planes de acción y son de conocimiento directo de la gerencia. RR3.2 Se mide lo realizado con lo planeado a fin de identificar desviaciones y ser revisado con los tomadores de decisiones.

Cuadro 9. (Continuación)

Práctica Genérica	Nivel de Cubrimiento	Criterios del Cubrimiento
GP 2.9 evaluar objetivamente la adherencia		No hay actividades en RISK IT para el cubrimiento de esta práctica.
GP 2.10 revisar el estado con el nivel directivo	Parcialmente RR1.1 Completamente RR2.5	RR1.1 RSKM solo se concentra en mitigar los riesgos negativos y no revisa los impactos positivos ni las oportunidades para la empresa, que de ellos derivan. RR2.5 Revisa los planes de acción y son de conocimiento directo de la gerencia.
GP 3.1 establecer un proceso definido	Completamente RG2.2	RR.2.2 Permiten adaptar el proceso de gestión de riesgo a la organización, teniendo en cuenta la consecución de los objetivos empresariales.
GP 3.2 recoger información de mejora	Parcialmente RR3.4	RR3.4 RSKM no hace énfasis en el análisis de las causas de los acontecimientos adversos y pérdidas.

3.3 ACTIVIDADES POR ROL Y DOMINIO DE PROCESO PARA GESTIÓN DE RIESGOS

Al determinar el cubrimiento de RSKM sobre RISK IT es posible definir un panorama general de la empresa con respecto a los procesos recomendados por RISK IT. Esto permite a la organización determinar frentes puntuales del proceso que deben ser reforzados o complementados pues un aspecto importante a considerar, es el trabajo ya realizado por la empresa en este proceso y entrar a apoyar puntos clave en los cuales la organización determine trabajar.

Cabe anotar, que tener esta integración de los modelos, establece un cruce entre las mejores prácticas establecidas por el modelo CMMI en su área de proceso RSKM y el marco de referencia RISK IT pues ambas son un compendio de las mejores prácticas generadas por dos instituciones reconocidas en la industria como los son el SEI e ISACA respectivamente.

Adicional a la segmentación de dominios de proceso que hace RISK IT y desde la cual podemos determinar aspectos puntuales a reforzar con base en la alineación con RSKM, también se propone una estructura de roles para cada una de estas actividades. Esto facilita a la organización la definición de recursos y responsabilidades al momento de implementar cualquier acción encaminada a cubrir nuevas áreas del proceso o reforzar áreas ya existentes pues el modelo de madurez CMMI recomienda que se deba hacer para gestionar los riesgos pero no indica quien en la organización debe ser el responsable de ejecutar las actividades.

Roles y responsabilidades: con el fin de generar esta guía de roles y responsabilidades RISK IT propone una estructura de roles y responsabilidades por actividad denominada matriz RACI. Esta matriz indica los roles para cada actividad clave definidos como un grupo de apoyo a las prácticas de gestión de la

tabla de riesgos de TI. Los RACI se definen (por sus siglas en ingles) de la siguiente manera:

Responsable (R)-Los que deben garantizar las actividades se completan con éxito. Accountable (A)-Los que poseen los recursos necesarios y tienen la autoridad para aprobar la ejecución y / o aceptar el resultado de una actividad.

Consulted (C)-Los que se solicitan opiniones sobre una actividad (comunicación bidireccional).

Informed (I)-Los que se mantenga al día sobre el progreso de una actividad (de un modo de comunicación)

A continuación en el Cuadro 10 (ver página siguiente), se presenta la matriz RACI para los dominios de proceso del marco de referencia RISK IT, con el cubrimiento realizado por las prácticas de RSKM.

Cuadro 10**.** Cubrimiento de RISK IT a partir de las prácticas generales y específicas de RSKM

				Cobertura RSKM	Consejo	(CEO) Director Ejecutivo	(CRO) Jefe Oficial de Riesgo	(CIO) Jefe Oficial de Información	(CFO) Jefe Oficial de Financiero	Comité de Riesgos	Gestión empresarial	Propietario de procesos de negocio	Funciones de control de riesgos.	(RH) Recursos Humanos	Cumplimiento y Auditoría
RISK IT	Gobierno del riesgos (GR)	RG1 Establecer y mantener una vista de riesgo común.	**RG1.1**		I	A	R	R	C	I	R	C	R	C	C
			RG1.2	**SP 1.2**	I	I	C	R	C	I	A	C	C		C
			RG1.3		A	C	C	C	C	R	C	C	C	C	C
			RG1.4	**GP 2.1**	C	A	R	R	R	C	R	R	R	R	C
			RG1.5	**GP 2.5**	A	R	R	R	R	R	R	R	R	R	R
			RG1.6		R	R	R	R	R	R	A	R	R	R	R
		RG2 Integrar con ERM.	**RG2.1**	**GP 2.4 GP2.7**	A	R	R	R	R	I	I	I	C	C	C
			RG2.2	**GP 2.2 GP2.10**	A	R	C	R	C	C	R	C	C	C	I
			RG2.3				C	A / R	C	I	C	C	R	C	C
			RG2.4	**GP2.3 GP2.5**	A	R	C	R		I	C	R	C	C	
			RG2.5		A/ R	C	C	C	C	C	C	C	C	C	C
		RG3 Tomar decisiones conscientes de los riesgos del negocio.	**RG3.1**			C	A / R	R	C	C	C	C	R	C	C
			RG3.2			I	R	C	C	A	I	R	I	I	I
			RG3.3		I	C	C	A / R	C	C	C	C	R	C	I
			RG3.4		I	I	C	R	C	R	A	R	C		I
			RG3.5	**SP2.2**		I	A	R	I	C	C	R	R		I
	Evaluación de riesgos(RE)	RE1 Recoger datos.	**RE1.1**	**SP1.1**	I	I	A / R	C	C	C	C	C	C		C
			RE1.2	**SP1.1**		I	A / R	C	I	I	C	I	I	I	C
			RE1.3	**SP1.1**		I	A	R	C	I		C	C		I
			RE1.4	**SP1.1 SP2.1**			A	R	I	I	C	C	R	C	C

Cuadro 10. (Continuación).

RISK IT	Evaluación de riesgos(RE)	RE2 Analizar los riesgos.	**RE2.1**	**SP1.2**		I	R	C	I	C	A	R	C		C
			RE2.2	**SP1.2 SP2.2**		I	R	C	C	I	A/ R	R	R		C
			RE2.3	**SP1.3**				C	C	R	A	R	R		I
			RE2.4				A / R				I		I		
		RE3 mantener perfil de riesgo.	**RE3.1**				I	R			C	A / R	C		I
			RE3.2			C		R		C	A/ R	R			I
			RE3.3				C	A				C	C		I
			RE3.4	**SP2.1 SP2.2**			C	R	I	C	C	A	R		C
			RE3.5			I	A	R	I	I	I	R / C	C		I
			RE3.6				A	C			C	C	R	C	C
	Respuesta de riesgos (RR)	RR1 riesgo articulado	**RR1.1**	**GP2.10**		I	R	C	C	C	A	R	R	C	I
			RR1.2	**GP2.8**	I	I	C	R	I	A	I	I	I	I	C
			RR1.3		I	I	A / R	R	I	I	I		C	I	C
			RR1.4			I	I	R	I	I	A	R	R	I	I
		RR2 Manejar riesgos	**RR2.1**		I	A / R	C	I	I	C	C	R	C		
			RR2.2	**GP2.8**	C	C	I	A	R	R	C				
			RR2.3		I	A	C	R	C	I	R	C	C	C	
			RR2.4		I	A	C	R	C	I	R	C	C	C	I
			RR2.5	**GP2.8 GP2.10**	I	I	I	R	I	I	I	A	R	I	I
		RR3 Reaccionar a acontecimientos	**RR3.1**	**SP3.1**	I	I	I	R	C	I	I	A	R	C	I
			RR3.2	**SP3.2 GP2.8**			C	I	I	I	I	A	R	C	R
			RR3.3	**SP3.2**	I	I	I	I	I	I	R	A	R	C	I
			RR3.4	**GP3.2**	I	I	A / R	R	C	I	C	C	R	C	I

	Totalmente Cubierto
	Parcialmente Cubierto
	Sin Cubrimiento

R	Responsable
A	Accountable
C	Consulted
I	Informed

Una empresa valorada CMMI nivel 3 o superior puede usar esta propuesta como apoyo al proceso de gestión de riesgos pues en esta encuentra un mapa del proceso de gestión alineado con actividades puntuales a realizar en cada una de las practicas especificadas por RSKM. Para hacerlo, la empresa debe identificar cuáles son los aspectos de su proceso de gestión que requieren reforzamiento a ampliación, una vez identificados estos aspectos y traducidos en prácticas de RSKM o procesos de RISK IT (en caso de una ampliación) es posible determinar las actividades a realizar de RISK IT que permitirán lograr el objetivo.

Adicionalmente, para el conjunto de actividades que la empresa decida implementar, se presenta la matriz RACI donde se proveen los roles recomendados para realizar la actividad y la forma en que cada uno de estos roles interactúan con el proceso y con la actividad en particular.

Aunque el alcance de la propuesta es el reforzamiento del proceso de gestión de riesgos en empresas valoradas nivel 3 de CMMI que ya cuentan con el área de proceso RSKM implementada, es posible que las organizaciones aún no valoradas o valoradas en niveles inferiores al 3 que desean implementar RSKM puedan aprovechar esta propuesta al momento de definir el proceso de gestión de riesgos. Para ello, la empresa debe identificar las actividades a realizar partiendo de las prácticas establecidas por RSKM y por medio de la matriz RACI definir los roles invlucrados en cada actividad, así este tipo de organizaciones ya cuentan con procesos y actividades definidas para gestionar sus riesgos.

Por último, es importante indicar que la propuesta es un paso inicial importante en lo referente a la traducción de las recomendaciones del QUE de CMMI en un COMO representado por las actividades propuestas por RISK IT. Sin embargo, frente a esta problemática queda aún camino por recorrer pues estas actividades propuestas deben complementarse con la recomendación de entregables,

métricas y herramientas que quien a las empresas en la definición con mayor nivel de detalle en los COMO del proceso de gestión de riesgos.

4. RESULTADOS OBTENIDOS

Después de realizar un análisis a la estrategia y metodología empleada para el levantamiento de información, el análisis de los marcos de referencia y la valoración de la propuesta, se evidenció que estos dos aspectos fueron aplicados de manera acertada, debido a que lograron generar un mecanismo que permitirá a las empresas valoradas CMMI-DEV nivel 3+ complementar la gestión de riesgos a través de un conjunto de procesos y actividades recomendadas.

Para identificar las necesidades y/o dificultades comunes que enfrentan las empresas de desarrollo de software certificadas CMMI nivel 3 o superior se utilizó como metodología para el levantamiento de información, el formato de encuesta, el cual permitió realizar un diagnóstico inicial para obtener del estado actual del proceso de gestión de riesgo en las empresas objetivo.

A través del análisis realizado a los resultados de la encuesta se detectó oportunidades de mejora en diversos aspectos, destacándose principalmente los modelos y planes de identificación de riesgos, el apetito al riesgo, la generación de reportes para identificar oportunidades en el entorno y la comunicación con las personas interesadas, en los cuales se puede trabajar ampliamente a través de la aplicación de las actividades propuestas por el modelo RISK IT, para complementar dichos aspectos.

Estos resultados permitieron evidenciar que a pesar que las empresas se encuentran certificadas CMMI nivel 3+, presentan algunos aspectos a mejorar como los descritos en el párrafo anterior, debido a la falta de prescripción del

modelo, aspectos que después de realizar el análisis al marco de referencia RISK IT, se encontró que pueden ser cubiertos y controlados de manera más detallada y precisa por este marco.

Por otro lado a través de la propuesta, se logra que una empresa que ha implementado RSKM refuerce ciertas metas específicas, guiándose a través de los procesos y actividades recomendados por el modelo RISK IT y teniendo en cuenta lo que ya ha ganado a través de la implementación del área de proceso RSKM, lo cual es descrito en el análisis de cubrimiento.

De igual manera permite a las empresas que deseen aplicar la propuesta, identificar los roles necesarios e involucrados en cada actividad recomendada por el marco de referencia RISK IT, para complementar los procesos que viene realizando a través del modelo CMMI o para implantar un nuevo proceso de los que recomienda RISK IT en sus tres dominios.

Finalmente la valoración de los expertos permitió evidenciar que la propuesta es de gran utilidad para las empresas que hoy en día basan su gestión de riesgos en RSKM, debido a que detectaron una serie de oportunidades que pueden ser aprovechadas con la implementación de los dominios de RISK IT en las empresas objetivo.

4.1 VALIDACIÓN CON EXPERTOS

Una vez generada la propuesta, fue presentada ante las personas que han estado directamente involucrados en los procesos de implementación o mantenimiento del modelo CMMI, específicamente en el área de proceso RSKM, para conseguir su opinión frente a la utilidad y facilidad de utilización de la propuesta, logrando

obtener en la totalidad de ellos un alto grado de aceptación de lo planteado en dicha propuesta.

Los resultados de dicha valoración permitieron identificar los escenarios donde la propuesta presenta gran utilidad y oportunidad de generar valor para la empresa, los cuales se presentan a continuación.

- **Reforzamiento en áreas específicas.** Una vez se ha definido que dominio de proceso o proceso en particular se requiere reforzar, a través de la propuesta se puede identificar de manera clara y sencilla las actividades que se deben realizar para complementar el proceso deseado, permitiendo así tener un mecanismo que no requiere implementar todo un marco de referencia de gestión de riesgos, sino solamente parte del mismo.

- **Cultura al riesgo.** Uno de los grandes beneficios que posee el modelo RSIK IT es que brinda la oportunidad de incentivar la cultura del riesgo a través de la implementación de los procesos de cada dominio, debido a que el modelo tiene como parte de sus principios la cultura al riesgo, la cual es pobremente inculcada y practicada en la mayoría de las empresas que gestionan sus riesgos. A través de la propuesta se puede ir incentivando la cultura al riesgo de manera implícita, al adoptar los diferentes procesos que el marco de referencia RISK IT propone.

- **Actividades Aterrizadas.** Uno de los problemas a los que se han enfrentado quienes implementan el modelo CMMI es que dice qué hacer más no lo dice cómo, por lo tanto el acercamiento que brinda la propuesta hacia marcos de referencia con actividades más específicas permite a las empresas contar con una herramienta más para definir los artefactos a utilizar en la gestión de riesgos.

- **Ampliación de Perspectiva del proceso de gestión de riesgos.** A través de la propuesta se logra llegar a actividades enfocadas a la identificación y aprovechamiento de los riesgos positivos, los cuales abren a las empresas un camino hacia la consecución de valor y oportunidades que ofrece el entorno y la industria en general, aumentando de manera controlada los umbrales de exposición al riesgo.

- **Definición de Roles.** Un proceso que requiere tiempo y esfuerzo es la identificación y definición de los roles involucrados en la gestión de riesgos, por lo tanto a través de la propuesta la empresas se pueden beneficiar al identificar claramente quienes deben ser responsables de ciertas actividades y quienes deben ser informados de los eventos que se presenten durante la gestión de riesgos.

Finalmente valorada la propuesta se presenta por parte del juicio de los expertos, como un mecanismo que puede traer grandes beneficios a las empresas que deseen utilizarla para complementar su gestión de riesgos a través del marco de referencia RISK IT.

5. CONCLUSIONES

Se evidenció que los proyectos de desarrollo de software y en general la industria de software, es de alto riesgo y de ahí la importancia de definir y realizar un proceso adecuado para gestión de los mismos.

En busca de un referente para la definición y mejora de los procesos de desarrollo/mantenimiento de software las empresas se apoyan de modelos de madurez, marcos de referencia y estándares existentes en la industria como lo es el caso de CMMI.

Sin embargo, estos modelos no aportan herramientas útiles y tangibles que permitan a las empresas traducir estas recomendaciones en actividades específicas para decidir CÓMO llevar a cabo esos procesos ni que personas en la organización podrían ser los responsables idóneos para realizarlo.

Debido a lo anterior, la industria provee marcos de referencia y estándares con el fin de suministrar herramientas que permitan aterrizar las recomendaciones para la implementación del proceso de gestión de riesgos, este es el caso de RISK IT de ISACA, Risk Management Framework del SEI, COSO ERM – Integrated Framewok, ISO20000:2005, ISO/FDIS3100:2009, PMBOK.

En este proyecto se emplea el marco de referencia RISK IT debido a que ofrece un espectro amplio en el cubrimiento del proceso de gestión de riesgos de TI. Al emplear este marco de referencia como complemento del proceso de gestión de riesgos establecido por el área RSKM de CMMI, se integran las mejores prácticas para gestión de riesgos provistas por el SEI en CMMI y por Isaca en RISK IT con el fin de reforzarlo.

Mediante la alineación inicial de los modelos, la organización puede identificar de manera clara y precisa que aspectos de RISK IT son cubiertos mediante la implementación de RSKM permitiéndole definir de manera puntual las actividades a realizar para reforzar el proceso de gestión de riesgos. Este mapa de actividades no solo le ofrece detalle de las actividades a realizar para traducir las recomendaciones sino que ofrece una definición de roles para establecer que personas en la organización son las encargadas de llevar a cabo este proceso.

Además de ofrecer un apoyo para establecer los COMO de RSKM en actividades y sus respectivos responsables, RISK IT fortalece el proceso de gestión de riesgos en los siguientes aspectos:

- Gobierno de TI. Se alinea el proceso de gestión de riesgos con la gestión de riesgos de la empresa, los objetivos de negocio y la obtención de valor de la empresa.

- Ampliación de la perspectiva del proceso de gestión de riesgos. En el enfoque de RISK IT está la identificación y el aprovechamiento de los riesgos positivos, los cuales abren a las empresas un camino hacia la consecución de valor y oportunidades que ofrece el entorno y la industria en general, aumentando de manera controlada los umbrales de exposición al riesgo.

- Generación de cultura de riesgo. Cada dominio de proceso de RISK IT promueve la comunicación e interiorización del proceso de gestión de riesgos a los miembros de la organización en todos los niveles.

Por otro lado el análisis del estado actual de la gestión de riesgos en las empresas y la validación con expertos, permitió identificar que las empresas en sus procesos formales de gestión de riesgos no contemplan la identificación de los riesgos

positivos, ni la identificación de las oportunidades existentes en el mercado, los cuales podrían traducir de manera controlada en generación de valor para sus negocios.

Por último, la propuesta generada es un aporte para el proceso de gestión de riesgos que se lleva a cabo en las empresas de desarrollo de software que han implementado el modelo CMMI incluyendo el área de proceso RSKM, no solo porque permite complementar solo determinados procesos que se quiera reforzar, sino porque brinda la posibilidad a quienes deseen implementar todas las recomendaciones del modelo RISK IT, de hacerlo de manera más rápida y eficiente debido a que no tienen necesidad de generar actividades para todos los procesos, sino simplemente para los que no están cubiertos por el modelo CMMI.

Es importante indicar que la propuesta es un paso inicial importante en lo referente a la traducción de las recomendaciones del QUE de CMMI en un COMO representado por las actividades propuestas por RISK IT. Sin embargo, frente a esta problemática queda aún camino por recorrer pues estas actividades propuestas deben complementarse con la recomendación de entregables, métricas y herramientas que quien a las empresas en la definición con mayor nivel de detalle en los COMO del proceso de gestión de riesgos.

6. TRABAJO FUTURO

Con el fin de continuar con la investigación planteada en esta propuesta se pueden considerar los siguientes puntos:

Recomendación de entregables y artefactos

Con respecto a la alineación de los marcos de referencia, es importante a futuro generar una serie de recomendaciones de los entregables a generar. Por una parte RSKM, y en general CMMI, define unos productos de trabajo y por otro lado RISK IT propone unos artefactos de salida del proceso, por ende, complementando las actividades propuestas se debe generar una recomendación de artefactos de salida para cada una de estas actividades tomando como base los dos marcos de referencia.

Paquete de Implementación

Generar un paquete de implementación de las actividades recomendadas. Esto con el fin de tener un mayor nivel de detalle de cada uno de los pasos a seguir en las actividades, así como la información de roles y entregables para cada una.

Herramienta de Gestión de Riesgos

Desarrollar una herramienta de gestión de riesgos que permita realizar el proceso de gestión de riesgos teniendo como lineamiento de proceso las actividades propuestas, permitiendo así automatizar y dar soporte a las actividades para dar cumplimiento a lo establecido por CMMI en el área de proceso RSKM y soporte a las actividades complementarias establecidas por RISK IT.

.

BIBLIOGRAFÍA

CHRISSIS, Mary Beth; KONRAD, Mike y SHRUM, Sandy. "CMMI® for Development, v1.2", 2006.

EDZREENA Edza Odzaly, Des Greer, Paul Sage. Software Risk Management Barriers: an Empirical Study. IEEE.

FIGUEROA, Luis C.; HERRERA, Andrea y GIRALDO, Olga L. Guía de buenas prácticas en gestión de riesgo de TI en el sector bancario colombiano [en línea]. Colombia: Universidad de los Andes, 2010 [consultado 16 de julio de 2011]. Disponible en Internet: http://biblioteca.uniandes.edu.co/Tesis_22010_segundo_semestre/347.pdf

KULPA, Margaret K. y JOHNSON, Kent A. Interpreting the CMMI: A Process Improvement Approach, 2003.

RIGONI, Cecilia: "CMMI®: Mejora del proceso en Fábricas de Software" [en línea]. España: MITYC, 2006 [consultado julio de 2011]. Disponible en Internet: http://www.mityc.es/NR/rdonlyres/A570B90C-B41A-46E2-BD39-4A31D18BB7FD/0/s01CeciliaRigoni.pdf.

Software Engineering Institute. Carnegie Mellon University, CMMI For Development SCAMPI^{SM} Class A Appraisal Results 2011 [Diapositivas]. U.S. CMMI Appraisal Program. Marzo 2011. 30 Diapositivas.

Software Engineering Institute, Carnegie Mellon University: "A Standard CMMI Appraisal Method for Process Improvement (SCAMPI) Version 1.2: Method Definition Document" [en línea]. Estados Unidos: SEI, 2006 [consultado Julio de 2011]. Disponible en Internet: http://www.sei.cmu.edu/pub/documents/06.reports/pdf/06hb002.pdf.

_____. Appraisal Requirements for CMMI, Version 1.2 (ARC, V1.2) [en línea]. Estados Unidos: SEI, 2006 [consultado Julio de 2011]. http://www.sei.cmu.edu/pub/documents/06.reports/pdf/06tr011.pdf.

_____. ARC, V1.0 Assessment Requirements for CMMI Version 1.0" [en línea]. Estados Unidos: SEI, 2000 [consultado Julio de 2011]. Disponible en Internet: http://www.sei.cmu.edu/pub/documents/00.reports/pdf/00tr011.pdf.

_____. Standard CMMI Appraisal Method for Process Improvement (SCAMPI) Version 1.1: Method Definition Document" [en línea]. Estados Unidos: SEI, 2001 [consultado Julio de 2011]. Disponible en Internet: http://www.sei.cmu.edu/pub/documents/01.reports/pdf/01hb001.pdf.

_____. What is CMMI?, [en línea]. Estados Unidos: SEI, septiembre 2007 [consultado Julio de 2011]. Disponible en Internet: http://www.sei.cmu.edu/cmmi/general/index.html.

_____. Capability Maturity Model® Integration (CMMI), Version 1.2 Overview [en línea]. Estados Unidos: SEI, 2007 [consultado Julio de 2011]. Disponible en Internet: http://www.sei.cmu.edu/cmmi/adoption/pdf/cmmi-overview07.pdf.

The RISK IT Practitioner Guide. ISACA.

The RISK IT Framework. ISACA.

ZARDARI, Shehnila. Software Risk Management. IEEE.

ANEXOS

Anexo A. Encuesta valoración proceso de gestión de riesgos

A continuación se encuentra la encuesta realizada a empresas de TI valoradas con nivel de madurez nivel 3 de CMMI con implantación escalonada con el fin de analizar qué actividades son realizadas para gestionar los riesgos en la organización.

Nombre de la empresa:
Nivel de madurez CMMI
Nombre del encuestado:
Cargo :

Marque con una X la respuesta más acorde a la frecuencia con la cual se realiza la actividad descrita en cada línea.

Nro.	Evaluación de Riesgos	Nunca	Rara vez	A veces	Frecuentemente	Siempre
1	Para realizar identificación de riesgos se sigue un modelo predefinido para recolectar información relevante?					
2	Se realiza identificación de los riesgos positivos?					
3	Los riesgos de TI identificados se comunican a todas las personas de la empresa, generando conciencia de los riesgos?					
4	Una vez identificados los riesgos, se determina su impacto en las demás áreas de la organización en caso de presentarse?					
5	Se tiene en cuenta la información de la industria para identificar riesgos?					
6	Se realiza identificación clara de los recursos de TI y su interrelación con los proceso de la empresa?					
7	Se tiene claramente establecida la capacidad de TI para determinar la respuesta a los diferentes eventos?					

Nro.	Evaluación de Riesgos	Nunca	Rara vez	A veces	Frecuentemente	Siempre
8	Se comunican e interiorizan los indicadores de riesgos con el fin de brindar alertas reales?					
9	Se documenta como se consideró el riesgo al momento de tomar las decisiones?					
	Respuesta a Riesgos					
10	Se elaboran informes periódicos de análisis de riesgos y son utilizados para apoyar la toma de decisiones?					
11	Dentro de los informes de análisis de riesgos se incluyen las probabilidades de pérdida o ganancia y los rangos o niveles de confianza?					
12	Se identifican oportunidades relacionadas a los riesgos a partir de la revisión de riesgos?					
13	Se identifican los procedimientos y la tecnología utilizada para supervisar el funcionamiento de los controles de riesgo?					
14	Se tienen identificados los responsables de los procesos a los cuales se va a enviar notificación cuando los controles superen los umbrales?					
15	Se evalúa el desempeño de los controles para verificar su correcto funcionamiento o para ajustarlos o incluir nuevos controles?					
16	Se comunica el plan de acción a seguir a las personas interesadas y afectadas cuando un incidente está ocurriendo?					

Anexo B. Empresas valoradas CMMI nivel 3 o superior en Colombia

Nombre de la Empresa	Nivel de Valoración
Asesoftware	3
Avansoft	3
Coomeva (Unidad de Tecnología Informática)	3
Gestiontek	3
Ilimitada	3
Red Colombia	3
Trebol Software	3
Heinsohn Software House	4
MVM Ingeniería de Software	4
Open Systems S.A.	4
Productora de Software (PSL)	5
InterGrupo	5