Universidad de las Ciencias Informáticas

Título: Proceso de Gestión de Riesgos para el Desarrollo de Aplicaciones Informáticas en la UCI

Tesis en opción al título de
Máster en Calidad de Software

Autora:
Ing. Dariena Ramirez Luján

Tutoras:
MSc. Yeleny Zulueta Véliz
MSc. Yadira Ruiz Constanten

Consultora:
Dra. Natalia Martínez Sánchez

La Habana, Noviembre de 2012

Declaración Jurada de Autoría

Declaro que soy la única autora del presente trabajo. Autorizo al Centro Nacional de Calidad de Software (Calisoft) y la Universidad de las Ciencias Informáticas (UCI) a hacer uso del mismo en su beneficio.

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

_____
Ing. Dariena Ramirez Luján
Autora

_____ _____
MSc. Yeleny Zulueta Véliz MSc. Yadira Ruiz Constanten
Tutora Tutora

Dedicatoria

A mi madre por ser mi luz.

Agradecimientos

A mi madre por la fe y el apoyo.

A mi familia por creer en mí.

A mi hermanita del alma, Kari, por las risas, las lágrimas y los consejos.

A mis amigos por escuchar siempre.

A mis tutoras por el apoyo, los consejos y la atención.

A todos los que imprimieron su esfuerzo incondicional en este trabajo.

A la UCI por la oportunidad.

Resumen en Español

Incluirse en el poderoso mercado internacional del software requiere de un alto nivel de capacidad por parte de la Industria Cubana del Software (ICSW). La capacidad de los procesos de la organización permite mejorar la eficiencia y la eficacia a través de múltiples disciplinas de procesos en una organización, además de ofrecer ventajas competitivas para obtener negocios importantes. El Modelo de Capacidad y Madurez Integrado (CMMI), de gran prestigio internacional, evalúa la capacidad de los procesos de la organización otorgando niveles de madurez/capacidad.

La Universidad de las Ciencias Informáticas (UCI), centro de avanzada en el desarrollo de software cubano alcanzó el nivel 2 de CMMI, por lo que muchos de sus procesos presentan un nivel de madurez que permite la obtención de resultados favorables a partir de procesos eficientes. Sin embargo la gestión de riesgos (GR) como proceso se evalúa en el nivel 3 de acuerdo con la representación escalonada de CMMI, por lo cual se observan deficiencias a tratar en cuanto a la capacidad del mismo aunque existen acercamientos a una GR adecuada de acuerdo con lo indicado en otras áreas de proceso evaluadas en el nivel de madurez 2.

La investigación incluye un Proceso de GR para el Desarrollo de Aplicaciones Informáticas, con productos de trabajo, técnicas e indicadores. Además se propone el uso de una herramienta inteligente que utilice la experiencia de la organización para identificar riesgos y estrategias de mitigación. Se utiliza para validar la implantación del proceso en algunos proyectos el Método Estándar de Evaluación CMMI para mejora de procesos (SCAMPI).

La investigación permitió concluir que la aplicación del Proceso de GR para el Desarrollo de Aplicaciones Informáticas definido apoya a la organización con resultados que permiten tomar decisiones acertadas relacionadas con la GR y mejorar el propio proceso de GR, constituyendo un paso de avance significativo para elevar el nivel de capacidad de la GR en la UCI al nivel 5 de CMMI.

Palabras clave: CMMI, gestión de riesgos, inteligencia artificial, procesos, riesgo.

Abstract

To include itself in a powerful international market such as software, the Cuban Software Industry requires a high level of competence. International assessments and certifications have the benefit of bestowing competitive advantages on those organizations that undertake them. The capability of the organization processes improves efficiency and efficacy through multiple process disciplines. The Capability and Maturity Model Integrated (CMMI) is internationally well regarded and evaluates the capacity of the organization processes, granting levels of maturity.

The University of Informatics Sciences (UCI), a cutting edge center of software development in Cuba, has reached level 2 of CMMI. This means that many of its processes present a level of maturity that allows obtaining favorable results through efficient processes. However, Risk Management (GR) as a process is evaluated in CMMI level 3, and it thus shows deficiencies to address regarding its capacity. There are approaches to a proper GR following the indications of other process areas already evaluated in level 2, though.

This research includes a Risk Management Process for Software Development, with artifacts, techniques and indicators. Also, an intelligent tool that uses the experience of the organization to identify risks and mitigation strategies is proposed. The Standard CMMI Assessment Method for Process Improvement (SCAMPI) method is used to validate the implementation of the process in selected projects.

This research concluded that the application of this Risk Management Process for Software Development supports the organization with results that allow the taking of decisions regarding Risk Management and the improvement of the process itself. These results constitute a significant step forward to raise the capacity level of Risk Management in the UCI to CMMI level 5.

Keywords: artificial intelligence, CMMI, process, risk, risk management.

Índice de Contenidos

Índice de Tablas

Índice de Gráficos

Índice de Ilustraciones

Introducción

De acuerdo con el Informe *"Global 100 Software Leaders, Key Players & Market trends"* (Líderes mundiales, principales actores y tendencias del mercado del software) emitido por el consorcio internacional PwC en 2011, la industria del software actualmente es un mercado de $250B que impulsa muchas de las innovaciones tecnológicas y sociales y contribuye a la productividad y el crecimiento general de la economía debido a los altos niveles de competitividad y la innovación que aporta a otras industrias, así como el papel que juega en cambiar la forma de hacer negocios en otros sectores (PwC, 2011). El también conocido *Global 100* presenta como países líderes en la exportación de software a China, Estados Unidos y la India, dada su posición por el porciento de ingresos en concepto de software de empresas punteras como Microsoft (77%), IBM (21%) y Oracle (83%).

En los resultados publicados por el Software Engineering Institute (SEI) acerca de la evaluación en cuanto a los niveles de madurez y capacidad de los procesos de las empresas a través del Modelo de Capacidad y Madurez Integrado (CMMI), los países mencionados además son líderes en cuanto a la cantidad de evaluaciones alcanzadas: China 1048, Estado Unidos 680 y la India 294 (SEI, 2012).

Estos informes demuestran que la obtención de una certificación o evaluación de prestigio internacional aporta beneficios considerables a la organización, que puede presumir de la capacidad de la misma para desarrollar software de calidad, imprimiendo ventajas competitivas frente a otras organizaciones al obtener proyectos complejos que ofrecen ganancias significativas. La utilización de CMMI favorece a las organizaciones porque: (SEI, 2012)

- *Proporciona una guía para mejorar la eficiencia y la eficacia a través de múltiples disciplinas de procesos en una organización.*
- *Proporciona una visión común e integrada de mejora.*
- *Mejora el rendimiento que significa menores costos, mejora de la entrega a tiempo, mejora de la productividad, mejora la calidad y la satisfacción del cliente.*

La Industria Cubana de Software (ICSW) ha ido ganando terreno en la exportación de software según las cifras aportadas en 2011 por la Oficina Nacional

de Estadísticas e Información (ONEI), mostrando un incremento en los últimos años con un total de ingresos por concepto de exportación de software en 2008 de 1,465.4 CUC, en 2009 de 1,376.4 CUC y en 2010 de 2,935.7 CUC (ONEI, 2011). Sin embargo estos logros aún no son significativos para insertarse en el mercado internacional de software. *La exportación de la capacidad cubana para la realización de proyectos informáticos obliga a sus organizaciones a ser competitivas en un mundo globalizado y regido por indicadores que han marcado y definido empresas e instituciones con un posicionamiento en el mercado de la producción de software* (Tardío, et al., 2011).

Dentro de los pasos importantes que debe seguir la ICSW para posicionarse en el mercado internacional está alcanzar una madurez en los procesos de las organizaciones que permita una evaluación satisfactoria por un estándar internacional. Uno de los principales obstáculos que enfrenta la ICSW en este aspecto es el elevado costo de las certificaciones y evaluaciones. La Organización Internacional de Estándares (ISO, por sus siglas en inglés) establece costos de implementación y costos de auditoría y certificación determinados por el tamaño de la empresa, el sistema de calidad utilizado, el tiempo que pueden dedicar los especialistas de la organización para ofrecer al proyecto de certificación y si existe la necesidad de utilizar un asesor, sumado a los precios de la documentación y herramientas a usar (ISO, 2012). CMMI evalúa los procesos de los proyectos variando sus precios al incluir los costos del evaluador habilitado por el SEI que en el caso cubano sería extranjero adicionando gastos de viático, costos del equipo de evaluación que puede ser propio y de la consultora, costos externos resultado del contrato de una entidad consultora y los costos de los cursos oficiales que deben recibir las personas del equipo de evaluación (SEI, 2011). Especialistas de la Dirección de Calidad de Software (Calisoft) plantean que al cumplirse tres años luego que la institución es evaluada, dado el carácter de mejora continua de CMMI, debe decidirse si se mantiene el nivel alcanzado que incluye costos de mantenimiento o si se aspira a elevar la evaluación a otro nivel, caso en el cual se realizaría una nueva negociación.

Cuba es un país tercermundista, enfrascado en un proceso de mejora de la economía que había sufrido un deterioro importante durante los últimos años. Alcanzar una excelencia en la ICSW en cuanto a la capacidad de los procesos de las organizaciones, debe ser un proyecto interno del país que permita adquirir los beneficios de una evaluación o certificación internacional utilizando las habilidades

de los especialistas cubanos sin incurrir en costos elevados que el país no puede sufragar. Aun así la Universidad de las Ciencias Informáticas (UCI), entidad vanguardia en el desarrollo de software cubano, alcanzó el nivel 2 de CMMI en 3 de sus centros de investigación y desarrollo, y las prácticas aplicadas y evaluadas para los mismos se generalizaron el resto de los centros. Los procesos evaluados fueron:

- Administración de requisitos - REQM
- Planeación de proyecto - PP
- Monitoreo y control de proyecto - PMC
- Gestión de acuerdos con proveedores - SAM
- Medición y análisis - MA
- Aseguramiento de la calidad de proceso y de producto - PPQA
- Gestión de configuración - CM

Para gestionar un proyecto de software con éxito, debe comprenderse qué puede ir mal y cómo hacerlo bien (Pressman, 2010), pues durante cualquier etapa de su desarrollo, factores como el entorno tecnológico, los recursos necesarios, las herramientas utilizadas, los requerimientos del cliente y la estabilidad del personal, pueden modificarse sustancialmente y, por tanto, pueden darse consecuencias no previstas inicialmente que alteren su buen término. Estos eventos que pueden ocurrir o no, ocasionando cambios en los objetivos de un proyecto, son los riesgos.

Cuando se considera el riesgo en el contexto de la gestión de proyectos de software, a pesar de que se han producido amplios debates sobre la definición adecuada (Boehm, et al., 1997; Charette, 1989; Higuera, et al., 1996; Jacobson, et al., 2000; Mochal, 2002; del Toro, et al., 2005; Cancelado, 2006; Bannerman, 2008; Power, 2008), hay acuerdo común en que este implica dos dimensiones:

- Incertidumbre: El acontecimiento que caracteriza al riesgo puede, o no, ocurrir.
- Efecto en los objetivos: Si el riesgo se convierte en una realidad, esto tendrá consecuencias para el proyecto.

La dirección del Gobierno, conjuntamente con otros órganos y organismos del Estado, ha desarrollado un constante y sostenido esfuerzo por consolidar el control interno en las diferentes entidades. Esta voluntad se ha visto reforzada por la promulgación de la Resolución No. 297-2003 del Ministerio de Finanzas y Precio de

Cuba (MFP, 2003), la cual declara la Evaluación de Riesgos como uno de los componentes del control interno pues debido a que las condiciones económicas, industriales, normativas y operacionales se modifican de forma continua, se hacen necesarios mecanismos para identificar y minimizar los riesgos específicos asociados con el cambio, por lo que cada vez es mayor la necesidad de evaluar los riesgos previo al establecimiento de objetivos en cada nivel de la organización (del Toro, et al., 2005).

En 2011, dada la necesidad de continuar perfeccionando el control interno la Contralora General de la República emitió la Resolución No. 60/11, que deroga la Resolución No. 297-2003 y es una nueva norma atemperada a las disposiciones que regulan esta actividad y a los requerimientos del desarrollo económico-administrativo del país (CGR, 2011). La Resolución o Ley 60 define:

> *Control Interno como el proceso integrado a las operaciones con un enfoque de mejoramiento continuo,(…); se implementa mediante un sistema integrado de normas y procedimientos, que contribuyen a prever y limitar los riesgos internos y externos, proporciona una seguridad razonable al logro de los objetivos institucionales (…).*

El Componente Gestión y Prevención de Riesgos desarrollado en la Sección Segunda de la Ley 60 establece las bases para la identificación y análisis de los riesgos que enfrentan los órganos, organismos, organizaciones y demás entidades para alcanzar sus objetivos (CGR, 2011). En el Artículo 11 b) se enfatiza:

> *Toda entidad debe disponer de procedimientos capaces de captar e informar oportunamente los cambios registrados o inminentes en su ambiente interno y externo, que puedan conspirar contra la posibilidad de alcanzar sus objetivos en las condiciones deseadas.*

Existe una variedad significativa de modelos entorno a la GR que permitirían trabajar en función de las metas enunciadas anteriormente. De ellos, los de uso más extendido y tomados como base en otras modificaciones son:

- La visión holística del SEI que incluye el Paradigma de Gestión de Riesgos (SEI, 1992), taxonomías para la identificación de riesgos (SEI, 2007; SEI, 2010), una estructura para describir los riesgos de desarrollo de software (SEI, 1994), un método para la evaluación de riesgos de software (SEI,

1999; SEI, 2012), la definición de una guía para la Gestión de Riesgos Continua (SEI, 1996), entre otras aproximaciones.

- La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, MAGERIT (MAP, 2012).
- Los procesos de GR descritos en la Guía de los Fundamentos de la Dirección de Proyectos (PMI, 2008) del Instituto de Gestión de Proyectos.
- Estándares de la Organización Internacional de Estandarización. (ISO/IEC, 2004)
- El área de proceso de GR definida en el Modelo de Capacidad y Madurez Integrado desarrollado por el SEI. (SEI, 2010)

A partir de un análisis de estos y otros modelos, pudieron identificarse algunos de los retos que enfrenta la GR (Kontio, 2002; Zulueta, 2008; Zulueta, 2009):

- Utilización inadecuada de las técnicas para la identificación y análisis de riesgos.
- Las actividades relacionadas con los riesgos, definidas en las metodologías de desarrollo de software no garantizan su correcta gestión, por tanto se hace más difícil integrar ambos procesos, así como las responsabilidades de los roles que intervienen en ellos.
- Deficiencias en el seguimiento y control de los riesgos lo que provoca que no se puedan ilustrar completamente los resultados de la implementación de la GR y los planes de mitigación y/o contingencia.
- La conceptualización de nuevas soluciones en el campo de la GR no ha estado aparejada a la automatización de herramientas de apoyo a los procesos, con facilidades de configuración y uso.

La revisión de los resultados de entrevistas a líderes de proyectos de software de la UCI arrojó, que se realiza la GR de acuerdo con actividades de planificación de la GR en el plan de desarrollo de software, identificación y priorización de los riesgos siguiendo un análisis cualitativo usando la técnica Matriz de probabilidad / impacto. Además se realiza la planificación de estrategias de mitigación y contingencia, así como un análisis de las desviaciones que provocarían los riesgos en el cronograma general del proyecto definiendo acciones correctivas. Estas actividades cumplen con lo establecido en el Área de Proceso (PA) Planeación de Proyecto (PP), en la Práctica Específica (SP) 2.2 Identificar los riesgos del proyecto

y el PA Monitoreo y Control del Proyecto (PMC), que se enfoca en la monitorización de los riesgos del proyecto (SP 1.3).

Al realizar las actividades de GR establecidas en las PA PP y PMC en la UCI se cumple con el nivel 2 de CMMI alcanzado por la universidad, sin embargo los líderes plantean que el análisis se ejecuta solo en su expresión cualitativa, se determinan solo los riesgos que pueden convertirse en amenazas perdiendo las oportunidades que ofrecen los riesgos positivos. Además, el seguimiento y control de los mismos se ejecuta sin aplicar ninguna técnica formal que apoye la actividad y se utilizan insuficientes indicadores para obtener la información de mejora necesaria. Algunos de los eventos que se han manifestado producto de la ausencia de estas actividades en la GR desarrollada actualmente son decisiones erradas ante estimaciones irreales, enfrentamiento a muchos imprevistos, un control interno inadecuado y la pérdida de oportunidades importantes que propiciarían mejoras a la organización en materia de negocios.

En el artículo *Primeras ideas de un Modelo cubano de referencia para el desarrollo de aplicaciones informáticas* se exponen ideas con respecto a la creación en el país de un Modelo Cubano de Desarrollo de Aplicaciones Informáticas (MCDAI), tomando como debilidad que el país no cuenta con un marco nacional de *referencia que identifique las particularidades del sistema organizacional cubano y se alinee con los reconocidos modelos internacionales para la producción de software* (Tardío, et al., 2011). El modelo debe apegarse a las directrices establecidas en la Guía de los Fundamentos para la Dirección de Proyectos. (PMBOK, por sus siglas en inglés) y basarse en normas y estándares internacionales, fundamentalmente en CMMI para lograr que las organizaciones mejoren sus procesos teniendo en cuenta esta importante referencia de evaluación.

Al tomar en consideración las tendencias actuales en la GR, el encargo social de la ICSW y las potencialidades y recursos con que cuenta, y valorar la voluntad del país en cuanto al control interno, el MCDAI y la necesidad de una correcta evaluación de los riesgos en la UCI, se evidencia una contradicción entre estos elementos que no son satisfechas por los modelos que hoy existen; lo cual sugiere el siguiente **problema de investigación**: *¿Cómo contribuir a la toma de decisiones relacionadas con la GR en el desarrollo de aplicaciones informáticas en la UCI?*

Con vista a la solución del problema planteado, la investigación se enfoca en el **Objeto de estudio**: los procesos de GR para el desarrollo de aplicaciones informáticas.

Para solucionar el problema planteado, se concibe como **Objetivo General**, *diseñar e implantar un proceso de GR para el desarrollo de aplicaciones informáticas en la UCI que permita obtener resultados que apoyen la toma de decisiones relacionadas con la GR.* Se precisa la mejora de la capacidad del proceso de GR para el desarrollo de aplicaciones informáticas en la UCI, como **Campo de acción**.

Objetivos específicos:

1. Evaluar el estado actual de los modelos, metodologías, métodos, procedimientos, herramientas y técnicas, utilizados para la GR sobre la base de las exigencias cubanas.
2. Definir el proceso de GR para el desarrollo de aplicaciones informáticas.
3. Proponer una herramienta inteligente que permita identificar y definir la mitigación de los riesgos identificados para un proyecto de software.
4. Validar los resultados a través de la implantación del proceso de GR en proyectos informáticos de los centros de desarrollo de la Facultad 2 y la evaluación de esta actividad utilizando el método SCAMPI.

El desarrollo de la investigación estará guiado por la **Hipótesis**: *el diseño y la implantación de un proceso de GR para el desarrollo de aplicaciones informáticas en la UCI, permitirá obtener resultados que apoyen la toma de decisiones relacionadas con la GR y la mejora de la capacidad del proceso de GR.*

Se definen las siguientes **tareas de investigación** para apoyar el cumplimiento de los objetivos específicos:

1. Realizar un estudio del estado del arte de la GR teniendo en cuenta marcos de referencia internacional y nacional.
2. Obtener información de GR contextualizada en la UCI entrevistando a protagonistas del desarrollo de aplicaciones informáticas en la universidad.
3. Analizar técnicas de inteligencia artificial para utilizar la experiencia en función del proceso de GR.
4. Definir las actividades que conformen el proceso de GR para el desarrollo de aplicaciones informáticas.

5. Determinar los productos de trabajo resultantes de la realización del proceso de GR para el desarrollo de aplicaciones informáticas.
6. Determinar técnicas que apoyan la ejecución del proceso de GR para el desarrollo de aplicaciones informáticas.
7. Elaborar los indicadores que permitan obtener resultados medibles de la ejecución del proceso de GR para el desarrollo de aplicaciones informáticas.
8. Proponer el uso de una herramienta inteligente que permita utilizar la experiencia de la organización en la identificación y mitigación de riesgos.
9. Analizar el Método Estándar de Evaluación CMMI para mejora de procesos (SCAMPI, por sus siglas en inglés) con el fin de diagnosticar la capacidad del proceso de GR en algunos proyectos.
10. Aplicar SCAMPI a modo de diagnóstico para determinar el estado del proceso de GR en algunos proyectos de la Facultad 2.
11. Implantar como experimento el proceso de GR para el desarrollo de aplicaciones informáticas definido en algunos proyectos de la Facultad 2.
12. Aplicar SCAMPI luego de experimentar la implantación del proceso de GR para el desarrollo de aplicaciones informáticas en algunos proyectos de la Facultad 2 y determinar el nivel de capacidad que se alcanza.

Para el desarrollo de esta investigación se propone seguir una Estrategia Explicativa pues los conocimientos precedentes acerca del problema han sido suficientes para plantear una hipótesis explicativa y la representación del problema es clara en lo referente a la caracterización del fenómeno en sus aspectos externos. Esta estrategia podrá llevarse a cabo con la ayuda de métodos científicos:

Métodos teóricos:

- Análisis Histórico-Lógico: para profundizar en los antecedentes y las tendencias actuales en la GR.
- Analítico-Sintético: para el estudio y el establecimiento del estado del arte de la GR.
- Modelación: para la conceptualización del proceso de GR.

Métodos empíricos:

- Entrevista: para recopilar información de tendencias, comportamientos o estadística en la investigación, en el estudio del objeto y el campo de acción de la investigación.

- Observación: para la recopilación de la información in situ de las características y comportamientos de las unidades de estudio. Se utilizará en este caso una observación participativa.
- Experimento: como vía de constatación preliminar de la efectividad del proceso.

Métodos matemáticos:

- Estadística Descriptiva: para determinar los valores promedio o más frecuentes obtenidos por la aplicación de los métodos empíricos utilizados.
- Análisis Porcentual: para determinar los valores porcentuales significativos en los métodos empíricos utilizados.

Vale señalar, el uso de la triangulación teórica, como procedimiento que permitirá relacionar los resultados de los diferentes métodos y enfoques, así como examinar el desarrollo de la GR desde múltiples perspectivas teóricas, con el fin de tener una comprensión más profunda, contextualizada y holística del fenómeno.

La **significación práctica** de la investigación es la siguiente:

La definición y fundamentación de un proceso de GR para el desarrollo de aplicaciones informáticas, con nuevas actividades, técnicas, roles definidos y productos de trabajo de salida cuyos resultados apoyen la toma de decisiones relacionadas con la GR y la mejora del proceso de GR. La aplicación de este proceso apoyada en un sistema inteligente, elevará la capacidad del proceso de GR en la organización, preparándola para una futura evaluación.

Para facilitar su comprensión, el documento está estructurado en tres capítulos:

En el **Capítulo I**. Fundamentos teóricos de la Gestión de Riesgos, se establecen los supuestos teóricos sobre los que se basa esta investigación y se formalizan conceptos relacionados con la GR. Se analizan algunos estudios sobre procesos para la GR y se define la posición de la autora al respecto. Además se ofrecen datos sobre análisis recientes de la importancia del tema y se plantean valoraciones sobre su trascendencia y perspectivas futuras. Se presentan elementos de Inteligencia Artificial, los Sistemas Basados en el Conocimiento y el Razonamiento basado en casos utilizados en la herramienta inteligente.

En el **Capítulo II**. Proceso de Gestión de Riesgos para el Desarrollo de Aplicaciones Informáticas, se realiza una conceptualización de la GR en la UCI y se presentan las descripciones gráfica y textual del proceso. Se describe cada producto de trabajo resultado de la ejecución de las actividades, así como las técnicas e indicadores a utilizar y la herramienta propuesta.

En el **Capítulo III**. Análisis de los Resultados, se presenta la correspondencia de la propuesta con modelos internacionales y la Resolución No. 60/11, de obligado cumplimiento en las empresas cubanas. Se aplica un diagnóstico utilizando SCAMPI para determinar el estado de la GR antes y después de implantar el proceso de GR propuesto de forma que pueda comprobarse el cumplimiento de los objetivos de la investigación y la contrastación de la hipótesis propuesta.

Capítulo 1. Fundamentos Teóricos de la Gestión de Riesgos

Introducción

En este capítulo se establecen los supuestos teóricos que sustentan esta investigación. Se esclarece el lugar que ocupa la GR como parte de la Gestión de Proyectos. Se describen elementos fundamentales sobre los riesgos en el contexto del desarrollo de aplicaciones informáticas; se analizan algunos estudios sobre modelos para la GR y se define la posición de la autora al respecto. Por último se ofrecen datos sobre análisis recientes de la importancia del tema y se plantean valoraciones sobre su trascendencia y perspectivas futuras.

Riesgos de Software

Un proyecto es definido por el Project Management Institute (PMI, 2008) como el esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único. Sobre esta base, la dirección de proyectos implica por lo general identificar requisitos, abordar las diversas necesidades, inquietudes y expectativas de los interesados según se planifica y efectúa el proyecto, equilibrar las restricciones contrapuestas del proyecto que se relacionan, entre otros aspectos, con:

- el alcance
- la calidad
- el cronograma
- el presupuesto
- los recursos
- el riesgo

Los riesgos de software son eventos no previstos que de concretarse se transformarían en un problema para la organización, por lo que los riesgos no son un problema, un problema es un riesgo hecho realidad.

Robert Charette (Charette 1989) presenta la siguiente definición de riesgo:

> En primer lugar, el riesgo afecta a los futuros acontecimientos (…) La pregunta es, podemos por tanto, cambiando nuestras acciones actuales, crear una oportunidad para una situación diferente y, con suerte, mejor para nosotros en el futuro. Esto significa, en segundo lugar, que el riesgo implica cambio, que puede venir dado por cambios de opinión, de acciones, de

lugares... En tercer lugar, el riesgo implica elección y la incertidumbre que entraña la elección. Por tanto, el riesgo, como la muerte, es una de las pocas cosas inevitables de la vida.

Según el SEI (SEI, 2012), para que un riesgo sea entendible debe ser expresado claramente y su declaración, debe incluir:

- Una descripción de las condiciones actuales que pueden conducir a la pérdida.
- Una descripción de la pérdida.

A continuación se presentan otras definiciones:

- El riesgo es la posibilidad de sufrir una pérdida (SEI, 2012).
- Una medida de la exposición a la que está sujeta un sistema o sistema potencial (CRAMM, 2003).
- Un evento o una condición que, si ocurre, tiene un efecto positivo o negativo sobre los objetivos de un proyecto (PMI, 2008).
- La posibilidad de que una amenaza dada impacte las vulnerabilidades de un activo o grupo de activos y cause así, daños a la organización (ISO/IEC, 2004).
- Posibilidad de que se produzca un impacto determinado en un activo, en un dominio o en toda la Organización (MAP, 2012).

El riesgo siempre implica dos dimensiones:

- Incertidumbre: El acontecimiento que caracteriza al riesgo puede, o no, ocurrir.
- Efecto en los objetivos: Si el riesgo se convierte en una realidad, esto tendrá consecuencias para el proyecto.

Los términos **probabilidad** e **impacto** son los de uso frecuente para describir estas dos dimensiones, refiriéndose la probabilidad a la posibilidad con que un evento o condición puede ocurrir (incertidumbre), y el impacto, al alcance de lo que sucedería si el riesgo se materializa (efecto en los objetivos). Cuando se evalúa el significado de un riesgo en particular, es necesario considerar ambas dimensiones.

La oportunidad en la definición del riesgo

En cuanto al efecto en los objetivos, como puede apreciarse en las definiciones, algunos autores solo consideran las consecuencias negativas en estos, mientras

que otros, reflexionan sobre los beneficios que también puede entrañar un riesgo para el proyecto.

En los 80 Barry Boehm y Bob Charette, sintetizaron algunas aproximaciones para gestionar los riesgos de proyectos de software individuales (Boehm, et al., 1997; Charette, 1989). En los 90, las prácticas de GR llegaron a la industria fundamentalmente gracias a los enfoques del SEI y a partir de ahí grandes mejoras tuvieron lugar (SEI, 1997). Luego, pocas ideas se introdujeron, los eventos del SEI dejaron de realizarse, se publicaba menos en el tema y las compañías estaban menos interesadas en estas prácticas (Kontio, 2002).

Según Jirki Kontio (Kontio, 2002) una de las causas de este fenómeno residió en que el **.com** impulsó una percepción falsa de éxito**.** La industria del dot-com creció con dramática velocidad en los finales del pasado *milenio con un gran impacto en la bolsa de valores. En este crecimiento, las compañías no estaban preocupadas por los riesgos sino que solo buscaban las oportunidades. Los inversionistas estaban igualmente desinteresados en ideas conservadoras de inversión (donde los riesgos son menores) e incentivaron inversiones en proyectos riesgosos. Este fenómeno creó una atmósfera contra las sólidas prácticas de GR. Hubo poca motivación hacia las investigaciones y la aplicación de los resultados en el área.*

Este hecho precisamente provocó un giro en la propia definición de riesgo. Inicialmente los autores solo tenían en cuenta los impactos negativos de un riesgo en los objetivos del proyecto a pesar de que ya en los años 90 se advertía que el riesgo en sí no es malo y que deben balancearse sus posibles consecuencias negativas contra los beneficios potenciales de la oportunidad asociada. No fue hasta los inicios del milenio, que comenzaron a tenerse en cuenta en definiciones formales, las oportunidades y beneficios que también puede entrañar un riesgo para el proyecto (Kahkonen, 2001; Mochal, 2002; Cancelado, 2006; DACS, 2012; PMI, 2008; Bannerman, 2008; Hall, 2011), lo que suele llamarse riesgo positivo.

La definición de “riesgo positivo” se refiere a las oportunidades que puede aprovechar el proyecto si las respuestas a los riesgos son traducidas en acciones precisas iniciadas en el momento exacto. Kahkonen identifica algunas fuentes de estas oportunidades (Kahkonen, 2001):

- Del negocio: desarrollo del producto, atención del cliente durante el ciclo de vida del proyecto y atención enfocada a las actividades de alto margen de beneficios.
- Operacionales: valor agregado, “hacer lo que es importante”, minimizar el retrabajo.
- Sistémicas: proporcionan ahorros a largo plazo como resultado de la mejora de la seguridad y la protección.

En las definiciones analizadas (Alberts, 2006; Pressman, 2010), los riesgos son analizados teniendo en cuenta la dimensión del producto, de los procesos y del proyecto; no obstante, se minimiza la relación de los riesgos con las personas, que integran los proyectos, definen los procesos y desarrollan las aplicaciones informáticas. Esta observación determinar que esta investigación defienda el riesgo como *la medida de la probabilidad y la pérdida de un acontecimiento que puede impactar el proyecto, proceso o producto de software y/o a las personas que lo desarrollan* (Zulueta, 2008)**.**

Clasificación de los Riesgos

Cuando se analizan los riesgos es importante cuantificar el nivel de incertidumbre y el grado de pérdidas asociados con cada riesgo. Este trabajo se facilita al considerar diferentes categorías de riesgos. A continuación se presenta en la Tabla 1, un resumen de la clasificación de los riesgos relacionados con proyectos de software.

Tabla 1. Clasificación de los Riesgos de Software.

Criterio	Clasificación	Descripción
Nivel de conocimiento (Pressman, 2010)	Conocidos	Basta con una cuidadosa evaluación del plan del proyecto para que sean descubiertos.
	Predecibles	Se extrapolan de la experiencia en proyectos anteriores.
	Impredecibles	Pueden ocurrir, pero son extremadamente difíciles de identificar por adelantado.
Nivel de afectación (Pressman, 2010)	Genéricos	Amenaza potencial para todos los proyectos de software.
	Específicos	Relacionados con la tecnología, el personal y el entorno específico del proyecto en cuestión.
Según el área que	Del proyecto	Amenazan los recursos o al

amenazan **(Fuente, 2006)**		plan del proyecto en general.
	Técnicos	Amenazan la calidad y/o el desempeño del software en desarrollo.
	Del negocio	Amenazan la viabilidad del software a construir y a la organización que desarrolla el software.
Según su naturaleza (Alberts, 2006)	Especulativos	Dinámicos: que tienen asociadas tanto pérdidas como ganancias.
	Puros	Estáticos: Tienen asociadas solo pérdidas potenciales[1].

Gestión de Riesgos en el contexto del desarrollo de aplicaciones informáticas

Diferentes definiciones de la GR, pueden ayudar a tomar partido por una posición u otra, a continuación se citan algunas:

- *La identificación, análisis y mitigación de riesgos en sistemas de información, a un nivel acorde al valor de los activos protegidos* (CIAO, 2000).
- *La Gestión del Riesgo es una técnica que maneja los recursos empleables en el proyecto para limitar la diferencia entre su Estado Final Deseado (EFD) y su Estado Final Conseguido (EFC). Si la diferencia supera un límite establecido, se materializa un riesgo de incumplimiento del objetivo. Para asegurar la pertinencia del resultado suelen requerirse decisiones de realización de nuevas acciones que permitan reducir esa diferencia. Si el EFC está muy alejado del EFD, el proyecto incumplirá el objetivo; hasta su misma consecución puede resultar imposible* (Marcelo, 2003).
- *Enfoque sistemático para reducir la probabilidad de riesgos y/o limitar los daños causados por el riesgo mediante el uso de contramedidas adecuadas o acciones preventivas* (MAP, 2012).
- *Selección e implantación de las medidas o 'salvaguardas' de seguridad adecuadas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados y así reducir al mínimo su potencialidad o sus*

[1] Podrán tener asociadas solo pérdidas o ganancias según la posición que se tome frente al *Riesgo* en cuanto al efecto en los objetivos. Autores como Cancelado así lo refieren. (Cancelado, 2006)

posibles perjuicios. La GR se basa en los resultados obtenidos en el análisis de los riesgos (MAP, 2012).

- *El proceso formal en el que los factores de riesgos son sistemáticamente identificados, evaluados y mitigados* (SEI, 2012).

Sobre la utilización del término *Gestión de Riesgos*, cabe señalar que existen posiciones que separan las actividades de análisis de las de gestión y también se utilizan los términos *tratamiento* y *administración* de riesgos. En esta investigación GR se refiere a los procesos que *se encargan tanto de planificar, identificar y analizar, como de responder al riesgo y seguir y controlar las actividades planificadas al respecto* (PMI, 2008).

La investigación en la GR en el ámbito del software procura formalizar conocimiento orientado a minimizar y/o evitar los riesgos, mediante la generación de principios y buenas prácticas de aplicación realista (Roppponen, 2000). Hasta el momento se han propuesto y utilizado diferentes perspectivas de GR desde que Boehm (Boehm, 1988) atrajo a la comunidad de Ingeniería del Software hacia esta rama. Sin embargo, es evidente que pocas organizaciones utilizan todavía de una forma explícita y sistemática métodos específicos para gestionar los riesgos en sus proyectos software (Kontio, et al., 1997; Kulik, 2001; Estéves J., 2005; Gómez , et al., 2010; Harvard_Business_Review, 2011).

Kontio y Basili (Kontio, et al., 1997) enumeran tres razones principales para la baja tasa de divulgación de tecnologías de GR: falta de conocimiento sobre posibles métodos y herramientas, limitaciones prácticas y teóricas de los marcos de GR que entorpecen la facilidad de uso de estos métodos, y tercero, todavía hay pocos informes con evaluaciones sistemáticas o científicas que proporcionen feedback empírico sobre su viabilidad y beneficios.

El riesgo en un proyecto de desarrollo de software incluye componentes técnicos y de conocimiento del riesgo (Jiang, 2001). Diferentes estudios han mostrado que la mayoría de los proyectos fallan sobre todo en gestión, no tecnológicamente (Peng, et al., 2009; Song, et al., 2009; Pritchard, 2010). Además, son los temas de naturaleza organizacional los factores de riesgos del proyecto más dominantes a la vez que son los que se tratan satisfactoriamente en menos de la tercera parte de los proyectos de desarrollo (Doherty N., 2001). Schmidt (Schmidt, 2001) plantea que los jefes de proyecto exitosos puntúan bajo aquellos factores sobre los que no tienen control o influencia como: conflictos entre departamentos usuarios, cambio del propietario o responsable ejecutivo del proyecto, volatilidad del personal, número de unidades de la organización

implicadas y proyectos que involucran a múltiples proveedores. Otro elemento que influye en estos temas es la falta de reconocimiento sobre la importancia de los aspectos organizacionales que existe en gran parte de la comunidad profesional y académica vinculada a las tecnologías de la información y la comunicación, como muestran Doherty y King (Doherty N., 2001).

El reporte publicado en el Harvard Business Review Analitic Services titulado Risk Management in a Time of Global Uncertainty (La gestión de riesgos en tiempos de Incertidumbre Global), durante el año 2011, aportó consideraciones relevantes acerca de la situación actual de 13 grandes compañías entrevistando a 1419 directivos relacionados o no con el proceso de GR (Harvard_Business_Review, 2011).

Entre los datos analizados se determinó el impacto de la administración en la creación de una cultura de GR (Gráfico 1) donde los resultados de la encuesta indicaron que el nivel 7 en una escala del 1 al 10 fue el de mayor incidencia, lo cual demuestra que se trabaja en función de crear la cultura de GR pero los esfuerzos aún no son suficientes.

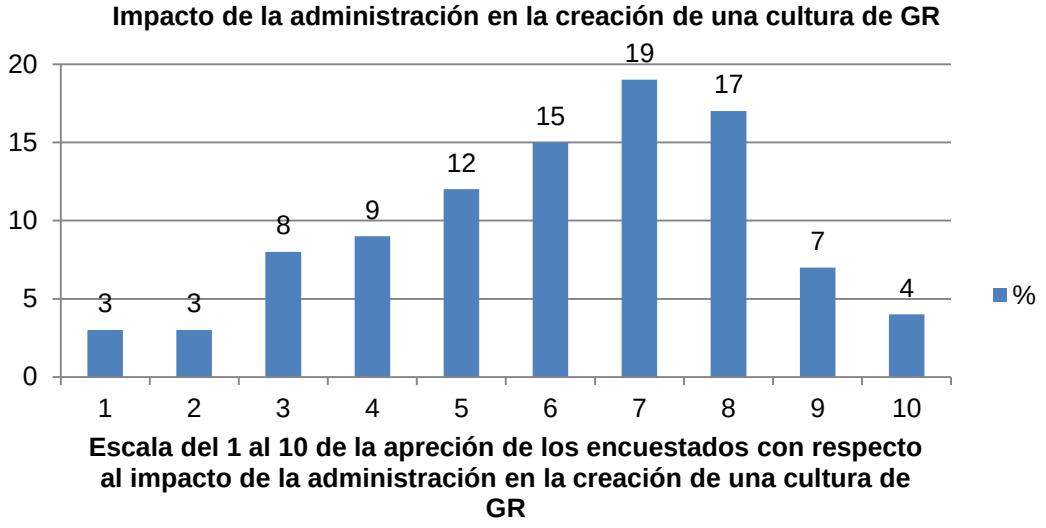


Gráfico 1. Impacto de la administración en la creación de una cultura de GR (Harvard_Business_Review, 2011).

Según la revisión existe una brecha con respecto a lo que realizan las compañías en la GR y lo que consideran importante que debe hacerse en este proceso. El Gráfico 2 indica que en todos los casos el porciento de las acciones implementadas no es suficiente para cubrir los objetivos de GR que las empresas consideran importantes.

Gráfico 2. Actividades de GR: Aplicación vs. Importancia (Harvard_Business_Review, 2011).

La revisión indica que durante los últimos tres años se han realizado avances en el proceso de GR en las compañías, entre las que destacan revisar y si es necesario reestructurar las cadenas de responsabilidad y reportes relacionadas con los riesgos y profundizar y extender los enlaces entre la GR y la estrategia general de la organización. En el Gráfico 3 se expone el porciento de mejoras apreciado en los años de 2009 a 2011.

Gráfico 3. Mejoras en el Proceso de GR (2009 - 2011) (Harvard_Business_Review, 2011).

Enfoques para la GR

Modelo de Boehm

La propuesta de Boehm (Boehm, 1988; Boehm, 1991; Boehm, et al., 1997; Boehm, et al., 1998; Boehm, et al., 2010) aunque se basa en una lista limitada de

riesgos y técnicas de GR, constituye el pilar de los modelos que siguen la secuencia tradicional de identificación-análisis-respuesta a los riesgos. Según este autor, la GR pasa por dos fases fundamentales: Valoración del riesgo y Control del riesgo.

Boehm incluye en su estudio una lista de diez riesgos (*Top 10 Software RiskÍtems*) muy generales y que pueden estar presentes en cualquier proyecto. Además plantea una serie de técnicas que pueden ser aplicadas para combatir cada uno de los riesgos (Anexo 1), los cuales son muy comunes y no se puede considerar precisamente una revelación en la actualidad. Incluso algún autor, como Sommerville (Sommerville, 2007), los encuentra *un poco arbitrarios*.

Marco del SEI para la GR

El SEI expone tres dimensiones que representan la visión holística de GR de software: la dimensión temporal, la dimensión humana y la dimensión metodológica (Higuera, et al., 1996).

1. La dimensión temporal, se descompone en la visión Macro, que representa la perspectiva global del ciclo de vida de adquisición y la visión Micro, que representa la vista del gerente del proyecto.
2. La dimensión humana se refiere a la dimensión intelectual de adquisición del software, la dimensión más crítica, pues el desarrollo del software es actividad intelectual. Esta dimensión aborda el aspecto individual, del equipo, la gestión y los involucrados (incluyendo los usuarios y los clientes).
3. La dimensión metodológica está dirigida a la adquisición y desarrollo de software para el cumplimiento de estas metas, el marco metodológico se articula en dos grandes bloques: el Modelo de Madurez de Adquisición de Capacidad (SA-CMM) y el Modelo de Capacidad de Madurez del Software (SW-CMM); que su vez se basan en tres grupos de prácticas o metodologías apoyadas en estructuras básicas.

Prácticas:

- Evaluación de Riesgos de Software (SRE)
- Gestión Continua de Riesgos (CRM)
- Gestión de Riesgos del Equipo (TRM)
- Métrica de Riesgo

Estructuras Básicas:

- Paradigma de GR

- Taxonomía de Riesgo
- Clínica de Riesgos

El Paradigma de GR, no es por sí solo una metodología, pero se discute bajo un marco metodológico. En la Ilustración 1 se muestran las principales actividades como un círculo para representar que es este un proceso continuo con centro en la comunicación, que se convierte en el canal de información y a menudo es por esta razón el obstáculo mayor en la GR.

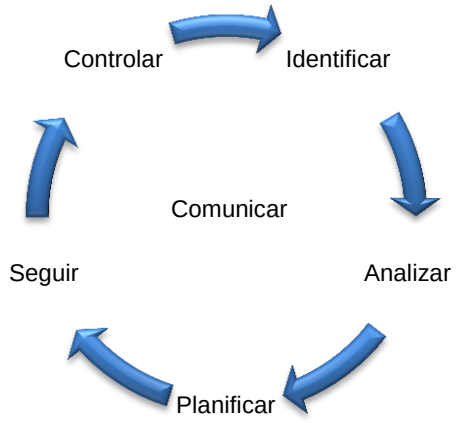


Ilustración 1. Actividades en el Paradigma SEI de GR.

El Marco SEI puede parecer complejo, sin embargo su visión completa, su dimensión humana y la importancia de la comunicación en su Paradigma, son aspectos que lo hacen valioso para la GR.

Procesos de Gestión de Riesgos en la Guía de los Fundamentos para la Dirección de Proyectos[2]

La metodología de gestión de proyectos del PMI ha sido frecuentemente aplicada a la industria. Es una de las más completas en cuanto a las funciones básicas que cubre y que deben llevarse a cabo para una gestión efectiva de los riesgos “antes de que estos lleguen a ser amenazas para el éxito”. La Ilustración 2 provee una vista general de los procesos principales (PMI, 2008).

[2] Project Management Body of Knowledge (PMBoK)

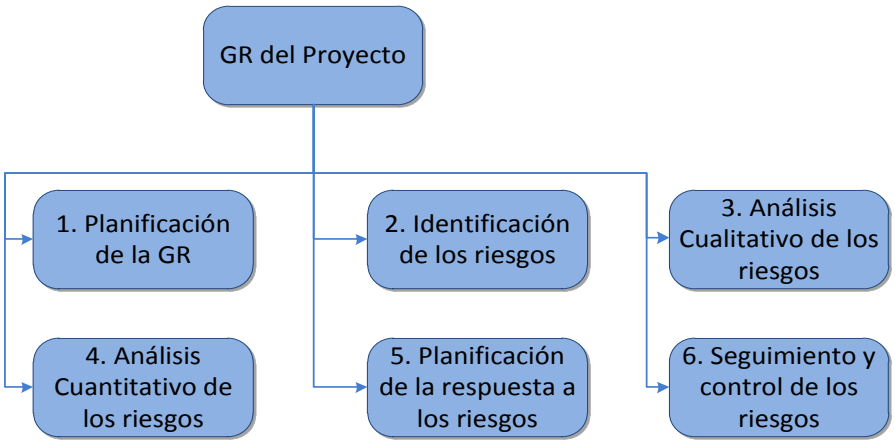


Ilustración 2. Procesos para la GR según PMI.

Estos procesos interactúan entre ellos y con otros procesos en otras áreas de conocimiento también. Cada proceso puede involucrar el esfuerzo de uno o más individuos o grupos de individuos basado en las necesidades del proyecto y cada proceso ocurre generalmente al menos una vez en cada fase del proyecto. A continuación se explican brevemente y en el Anexo 2 se ilustran los datos de entrada, herramientas y técnicas y resultados de estos procesos.

Planificación de la GR: Donde se definen y planifican las actividades del proyecto.

Identificación del riesgo: Consiste en determinar qué riesgos tienen probabilidad de afectar el proyecto y documentar las características de cada uno, esto no es un evento que ocurra una sola vez; este deberá ser ejecutado regularmente sobre la duración del proyecto y deberá atender tanto los riesgos internos como externos.

Análisis Cualitativo del riesgo: Se centra en la priorización de los riesgos de forma subjetiva estimando y combinando su probabilidad de ocurrencia e impacto.

Análisis Cuantitativo: Se centra en la cuantificación y priorización de los riesgos de forma objetiva. Se pueden resaltar sus principales funciones: determinar la probabilidad de realizar un objetivo específico del proyecto y cuantificar el riesgo del proyecto y determinar el tamaño de costo.

Planificación de las Respuestas al riesgo: Es el proceso que permite desarrollar opciones y determinar acciones para reducir las amenazas de los objetivos del proyecto. Incluye la identificación y la asignación de individuos para tomar la responsabilidad de cada respuesta de cada riesgo.

Seguimiento y control del riesgo: Debe determinarse si las respuestas planificadas han sido ejecutadas como fue previsto, si han sido eficaces o si han provocado nuevas respuestas. Además debe determinarse si los supuestos del proyecto continúan siendo válidos, verificar si la exposición al riesgo ha cambiado y además analizar si se siguen las políticas y procedimientos adecuados.

MAGERIT

MAGERIT es una metodología española de carácter público, creada con los siguientes objetivos (MAP, 2012):

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

En la Ilustración 3 se muestra el modelo de proceso en MAGERIT.

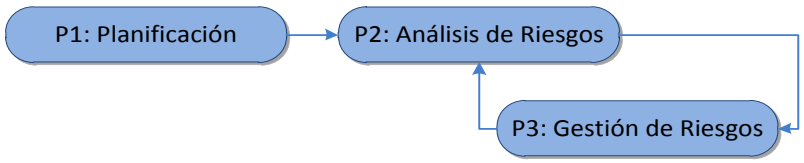


Ilustración 3. Modelo de procesos en MAGERIT.

Proceso P1 Planificación: Se establecen las consideraciones necesarias para arrancar el proyecto de *Análisis y Gestión de Riesgos*; se investiga la oportunidad de realizarlo; se definen los objetivos que ha de cumplir y el dominio (ámbito) que abarcará; se planifican los medios materiales y humanos para su realización; se procede al lanzamiento del proyecto.

Proceso P2 Análisis de riesgos: Se identifican los activos[3] a tratar, las relaciones entre ellos y la valoración que merecen; se identifican las amenazas significativas sobre aquellos activos y se valoran en términos de frecuencia de ocurrencia y degradación que causan sobre el valor del activo afectado; se identifican las salvaguardas[4] existentes y se valora la eficacia de su

[3] Recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección (MAP, 2012).

[4] Procedimiento o mecanismo tecnológico que reduce el riesgo (MAP, 2012).

implantación; se estima el impacto y el riesgo al que están expuestos los activos del sistema; se interpreta el significado del impacto y el riesgo.

Proceso P3 GR: Se elige una estrategia para mitigar impacto y riesgo; se determinan las salvaguardas oportunas para el objetivo anterior; se determina la calidad necesaria para dichas salvaguardas: se diseña un plan de seguridad (plan de acción o plan director) para llevar el impacto y el riesgo a niveles aceptables; se lleva a cabo el plan de seguridad.

Estos tres procesos no son necesariamente secuenciales. El proceso P1 es claramente el iniciador del proyecto. El proceso P2 funciona como soporte del proceso P3 en el sentido de que la GR (P3) es una tarea continua soportada por las técnicas de análisis (P2). La GR supone siempre la alteración del conjunto de salvaguardas, bien porque aparecen nuevas salvaguardas, bien porque se reemplazan unas por otras, bien porque se mejoran las existentes. La GR puede suponer la alteración del conjunto de activos, porque aparecen nuevos activos (elementos de salvaguarda que pasan a formar parte del sistema) o porque se eliminan activos del sistema. En definitiva, a lo largo del proceso P3 se recurrirá a tareas del proceso P2.

Gestión de Riesgos en las normas de la ISO

ISO/IEC 16085: 2006 Ingeniería de Software y Sistemas- Procesos del Ciclo de Vida- Gestión de Riesgos.

Este estándar define un proceso continuo de GR durante la adquisición, provisión, desarrollo, operaciones y mantenimiento de un sistema o software.

El propósito de este estándar es ofrecer a los proveedores o contratistas, adquiridores, desarrolladores y gerentes, una serie sencilla de requerimientos apropiados y procesos para la gestión de una gran variedad de riesgos. No detalla las técnicas a utilizar, pero se enfoca en la definición de un proceso en el que puedan ser usadas varias técnicas. Además propone tres artefactos fundamentales: el Plan de Gestión de Riesgos, Solicitud de acción sobre los riesgos y el Plan de Tratamiento de riesgos.

ISO/IEC 27005:2008 Tecnologías de la Información - Técnicas de Seguridad - Gestión de riesgos[5].

[5] Information technology, Security techniques, Information security risk management.

Aunque como indica su nombre, este estándar está enfocado a los sistemas de seguridad de la información, propone la implementación de este sobre la base de la GR. Contiene procesos, actividades y tareas para aplicar durante la adquisición de un sistema que contiene software, un producto software puro o un servicio software y durante el suministro, desarrollo, operación y mantenimiento de productos software. Los procesos que se emplean son: los principales, los de apoyo y los organizativos del ciclo de vida.

Dentro de los procesos organizativos del ciclo de vida se incluye la GR que tiene en este caso el propósito de identificar, analizar, tratar y monitorear los riesgos continuamente (Walz, 2010). Para su exitosa implementación se deben realizar las siguientes actividades:

1. Determinar el alcance de la GR a ser ejecutado.
2. Definir e implementar estrategias apropiadas para la GR.
3. Identificar los riesgos en la planificación de proyectos.
4. Analizar los riesgos en términos de probabilidad y consecuencias y determinar la prioridad en el tratamiento de estos riesgos.
5. Definir, aplicar y evaluar las mediciones de riesgos para determinar los daños, el estado del riesgo y el progreso de las actividades de tratamiento.
6. Seguir el tratamiento apropiado para corregir o evitar el impacto del riesgo basados en su prioridad, probabilidad y consecuencia u otros principios de riesgo definidos.

Este estándar puede ser utilizado para gestionar los riesgos de nivel organizacional o del proyecto, en cualquier dominio o etapa del ciclo de vida, para apoyar las perspectivas o ideas de los gerentes, participantes y otros involucrados.

ISO 31000:2009 Gestión de Riesgos- Principios y directrices.

Esta guía no fue concebida para certificación pero proporciona directrices para supervisar de forma proactiva, identificar, analizar y abordar los riesgos en toda la organización, y para ayudar a garantizar iniciativas de gestión de riesgos estructuradas, transparentes y dinámicas para el cambio.

Al mismo tiempo la ISO lanzó la **Guía 73:2009 Gestión de Riesgos- Vocabulario**, que promueve un enfoque coherente y entendimiento común acerca de la descripción de las actividades y el uso de la terminología de la GR (Purdy, 2010).

Los documentos serán de utilidad para:

- Los responsables de la aplicación de la GR dentro de sus organizaciones.
- Aquellas personas que necesitan para garantizar que una organización gestione los riesgos.
- Aquellos que necesitan para evaluar las prácticas de GR en una organización.
- Los desarrolladores de los estándares, guías de procedimientos y códigos de prácticas relativos a la GR.

Área de Proceso Gestión de Riesgos en el Modelo Integrado de Madurez y Capacidad

El Modelo Integrado de Madurez y Capacidad (CMMI) consiste en las mejores prácticas que tratan las actividades de desarrollo y de mantenimiento que cubren el ciclo de vida del producto, desde la concepción a la entrega y el mantenimiento de mejora de los procesos para el desarrollo de productos y de servicios. CMMI contempla 5 niveles de madurez y 6 de capacidad de acuerdo con la representación escalonada o continua de las organizaciones.

La representación continua permite a una organización seleccionar un Área de Proceso (PA, por sus siglas en inglés) (o un grupo de PAs) y mejorar los procesos relacionados con ésta. Esta representación utiliza unos niveles de capacidad para caracterizar la mejora concerniente a un PA individual. La representación por etapas utiliza conjuntos predefinidos de PAs para definir un camino de mejora para una organización. Este camino de mejora se caracteriza por diversos niveles de madurez. Cada nivel de madurez proporciona un conjunto de PAs que caracterizan diferentes comportamientos organizativos (SEI, 2010).

En el PA Planeación de Proyectos se plantea que el plan debe incluir la identificación y análisis de los posibles riesgos que pueda tener el proyecto; pero la GR, como PA (RSKM, por su acrónimo de acuerdo con CMMI), es contemplada en el nivel 3 de madurez y en la categoría Gestión de Proyecto. El propósito de la GR 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”.

El PA RSKM de CMMI es un proceso continuo que debe considerar fuentes tanto internas como externas para riesgos de coste, de calendario y de rendimiento, así como de otros tipos; y 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.

Para llevar a cabo una exitosa GR, CMMI plantea las siguientes metas y prácticas específicas.

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.

Las PAs de Gestión de Proyectos definidas en CMMI se integran de manera tal que existe una relación cercana entre las prácticas llevadas a cabo en un PA con respecto a otra. En el caso de RSKM se relaciona con el PA Planeación de Proyecto (PP) en las prácticas relacionadas con la identificación de riesgos y la planificación de las partes relevantes. Monitoreo y Control de Proyecto (PMC) y RSKM aúnan sus esfuerzos en la monitorización de los riesgos y el PA Análisis de decisiones y resolución (DAR) ofrece a RSKM la posibilidad de evaluar alternativas para la selección y la mitigación de los riesgos identificados. A continuación se muestra en la Ilustración 4 la relación que existe de RSKM con las PAs mencionadas.

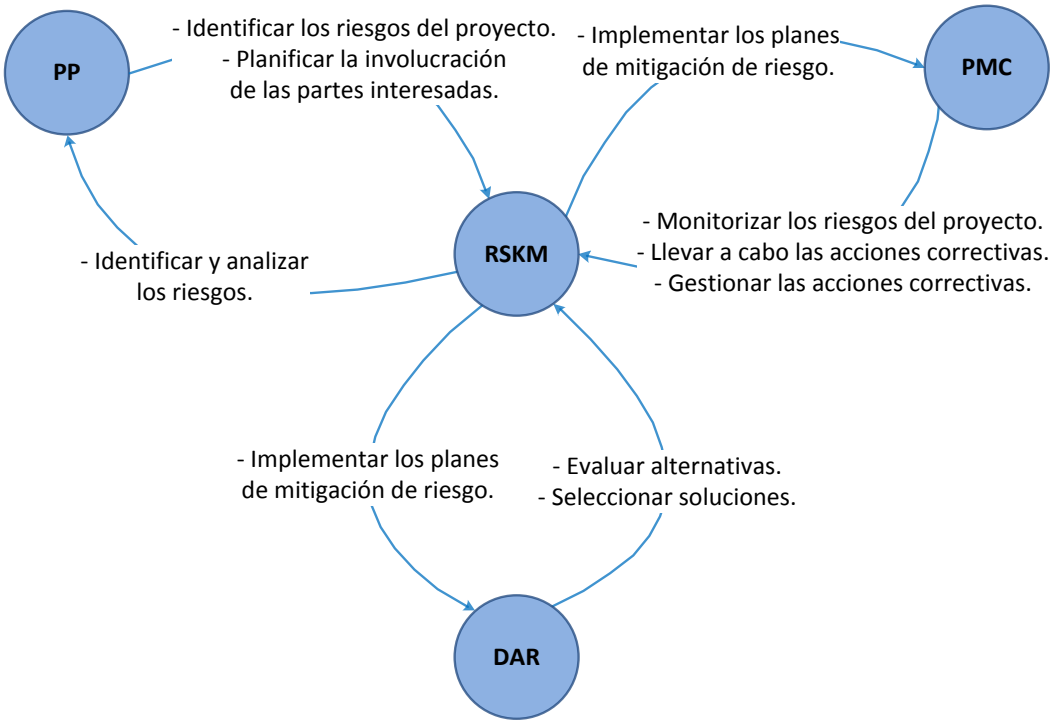


Ilustración 4. Relación de RSKM con otras PA.

Tratamiento de riesgos en el Proceso Unificado de Desarrollo de Software

El Proceso Unificado de Desarrollo de Software[6] (RUP) es una metodología guiada por casos de uso, centrada en la arquitectura, iterativa e incremental. RUP plantea que el primer paso hacia la división del proceso de desarrollo de software, consiste en separar las partes en cuatro fases atendiendo al momento en que se realizan: inicio, elaboración, construcción y transición. Cada una de las fases se divide una o más iteraciones.

En una iteración, deben entenderse las secuencias de actividades diferentes y buscarse el equilibrio entre ellas. Algunas secuencias de actividades han sido identificadas y descritas en los flujos de trabajo fundamentales de RUP. Hay otras secuencias que Jacobson, Booch y Rumbaugh (Jacobson, et al., 2000), reconocen no haber identificado formalmente, pero que perfectamente podrían ser tratadas de la misma forma que los flujos de trabajo, entre ellas, la *administración de riesgos*.

RUP propone crear una lista de riesgo en la fase de inicio. Al principio esto puede ser difícil por la falta de información pero conforme se va realizando el

[6] Rational Unified Process

trabajo inicial se va apreciando cuáles serán los riesgos críticos, aquellos que han de ser mitigados para poder ofrecer una planificación y un coste y para determinar un objetivo de calidad. Para facilitar la administración de la lista de riesgos, se plantea seguir el siguiente esquema:

- **Descripción**: Comienza con una breve descripción y se van añadiendo detalles conforme se va aprendiendo.
- **Prioridad**: Se le asigna una prioridad al riesgo: crítico, significativo o rutinario
- **Impacto**: Qué partes del proyecto o del sistema se verán afectados por el riesgo.
- **Monitor**: Quién es responsable del seguimiento de un riesgo persistente.
- **Responsabilidad**: Qué individuo o unidad de la organización es responsable de eliminar el riesgo.
- **Contingencia**: Lo que ha de hacerse en caso de que el riesgo se materialice.

Los autores de la metodología refieren como una mala experiencia, el no tener una planificación de riesgos. Cuando no existe un esfuerzo consciente para actuar pronto sobre los riesgos, estos se manifiestan usualmente al final de la planificación, mientras se realizan las pruebas de integración y de sistema. Resolver a esa altura cualquier problema serio, que puede requerir amplias modificaciones del sistema, puede retrasar la entrega.

Al explicar los pasos a seguir en cada fase del proyecto, en RUP se perciben las siguientes actividades relacionadas con los riesgos:

1. **Inicio**: identificar los riesgos críticos, es decir, los que afectan la capacidad de construir el sistema y determinar si puede encontrarse una forma de mitigarlos, quizás en una etapa posterior. En esta fase se consideran solo los riesgos que afectan la viabilidad del sistema. Los no críticos son colocados en la lista de riesgos.
2. **Elaboración**: identificar los riesgos significativos, los que podrían perturbar los planes, costes y planificaciones de fases posteriores y los reduce a actividades que pueden ser medidas y presupuestadas.
3. **Construcción**: materializar la monitorización de los riesgos críticos y significativos arrastrados desde las dos primeras fases y su mitigación.
4. **Transición**: no se definen tareas relacionadas con los riesgos.

Como puede analizarse en los elementos anteriormente descritos, si bien se define la identificación de los riesgos, las demás etapas que garantizan su gestión, no son suficientemente explicadas en RUP y no se exponen procedimientos a seguir para cumplir con las incompletas actividades propuestas. El formato para el registro de riesgos es ambiguo en cuanto a que *se van añadiendo detalles conforme se va aprendiendo*, no se describen cuáles son los detalles, ni qué debe aprenderse. Por otra parte, el análisis del riesgo no va más allá de la referencia al impacto solo como las *partes del proyecto o del sistema se verán afectados,* sin especificar la forma o al menos la profundidad del daño.

NIST 800-30 Guía para Gestión de Riesgos para Sistemas de Información y Tecnología

El Departamento de Comercio, la Administración de Tecnología y el Instituto Nacional de Estándares y Tecnología[7] de los Estados Unidos, publicaron en julio de 2002 una **Guía de Gestión de Riesgos para Sistemas de Información y Tecnología** (Stoneburner, et al., 2002) en la que se afirma que una efectiva gestión de riesgos debe estar totalmente integrada en el Ciclo de Vida del desarrollo del sistema (de tecnología) y se especifican las características de esta integración a través de la Tabla 2 que resume las fases del ciclo y sus características y el soporte que estas necesitan desde las actividades de GR. En algunos casos, un sistema TI puede ocupar varias de estas fases simultáneamente, pero la metodología de GR es la misma a pesar de la fase en la cual se analizan los riesgos: la gestión de riesgos es un proceso iterativo que puede ser realizado durante cada fase del ciclo de vida.

Tabla 2. Integración de las actividades GR en el ciclo de desarrollo.

Fase	Soporte de las actividades de Gestión de Riesgos
Inicio	La identificación es utilizada para apoyar el desarrollo de los requisitos del sistema, incluyendo los de seguridad.
Desarrollo o Adquisición	Los riesgos identificados durante esta fase pueden ser usados para apoyar análisis de seguridad que pueden guiar la arquitectura y el diseño y causar daños durante el desarrollo del sistema.
Implementación	El proceso de GR apoya la evaluación de la implementación del sistema contra los requisitos.
Operación o Mantenimiento	Las actividades de GR son realizadas para una reautorización o reacreditación periódica, o cuando son desarrollados grandes cambios

[7] National Institute of Standards and Technology (NIST)

	en el ambiente de producción operacional del sistema IT. (Ej. nuevas interfaces)
Cierre	Las actividades de GR son realizadas para componentes del sistema que entrarán en cierre o serán reemplazados, para asegurar que el hardware y el software son adecuadamente manipulados y que la migración del sistema es conducida de manera segura y sistemática.

Enfoques para la Gestión de Riesgos en Cuba

Resolución No. 60/11

En Gaceta Oficial No. 013 Extraordinaria del 3 de marzo de 2011, la Contraloría General de la República de Cuba publicó la Resolución No. 60/11 que aconseja dejar sin efectos legales las resoluciones No. 297, de 23 de septiembre de 2003, dictada por la Ministra de Finanzas y Precios y No. 13, de 18 de enero de 2006, dictada por la Ministra de Auditoría y Control. Estas derogaciones se realizan por la *necesidad de continuar perfeccionando el control interno, al emitir una nueva norma atemperada a las disposiciones que regulan esta actividad y a los requerimientos del desarrollo económico-administrativo del país* (CGR, 2011).

Esta resolución es de obligatorio cumplimiento por todas las entidades del país para la elaboración del sistema de control interno de cada organización. Sus componentes son: Ambiente de Control, Gestión y Prevención de Riesgos, Actividades de Control, Información y Comunicación y Supervisión y Monitoreo, y se encuentran estructurados en normas. En el caso específico del componente Gestión y Prevención de Riesgos la Resolución 60/11 establece la creación en cada institución del Plan de Prevención de Riesgos y el seguimiento de las normas:

- Identificación de riesgos y detección del cambio
- Determinación de los objetivos de control
- Prevención de riesgos

Aunque la Resolución presenta un componente específico de GR, todas las demás normas organizadas por componentes contribuyen al establecimiento de bases relacionadas con la preparación de la organización para enfrentar situaciones desconocidas de forma exitosa.

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

Resultado de una investigación para obtener el título de Máster en Ciencias, (Zulueta, 2007) se definió un modelo basado en el análisis de los puntos en común de varias metodologías y estándares reconocidos a nivel internacional. Se creó MoGeRi adaptándolo a las características de la Universidad de las Ciencias Informáticas (UCI). Evidencia de ello han sido las varias aplicaciones de este modelo en proyectos de desarrollo de la UCI con resultados satisfactorios (González, 2008; Gutiérrez, 2008; Palarea, 2008; Escobar, 2009; Reyes, 2009; Álvarez, 2011).

Las actividades de MoGeRi se organizan en seis procesos que permiten la identificación de los riesgos, su análisis y la planificación de respuestas a los mismos, así como su seguimiento y control. Estas actividades se muestran en la Ilustración 5.

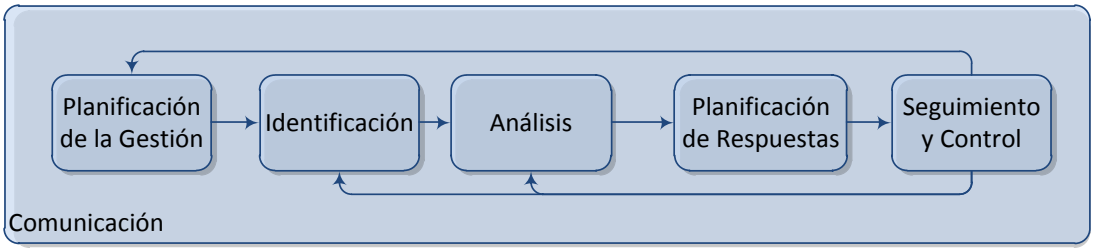


Ilustración 5. Procesos definidos en MoGeRi[8]

Su correcto uso beneficia a los proyectos de desarrollo de Software (Zulueta, 2007):

- Recoge las prácticas adecuadas según el entorno donde debe aplicarse, no es una réplica descontextualizada de otros marcos de GR analizados.
- Fomenta la comunicación del equipo de proyecto, dentro de este y de este con su entorno.
- Promueve la reutilización y registro de datos, no solo de los riesgos sino de la información histórica del proyecto.
- Se inserta, apoya y complementa la planificación, seguimiento y control, y de forma general, la Gestión de Proyectos.
- Apoya la gestión de los recursos en el proyecto, pues el impacto de los riesgos afectan directamente los recursos.

[8] Elaborado a partir de (Zulueta, 2007)

- Los procesos, actividades y tareas propuestos, son aplicables en cualquier fase del proyecto, lo que facilita su implantación en todo proyecto donde sea oportuna la GR.
- Recoge las actividades propuestas por estándares de calidad internacionales.
- Los resultados de los instrumentos aplicados ayudaron a identificar otros problemas de investigación.
- Los expertos concuerdan en su efectividad, tanto en la concepción teórica como en los resultados que se obtendrán con su aplicación.

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

Definido en 2010 en la tesis para optar por el título de Máster en Ciencias (Valladares, 2010) el Proceso de Gestión de riesgos para proyectos de desarrollo de software de Softel está completamente contextualizado en el marco de desarrollo de software en esa entidad a partir del estudio de sus características.

El proceso definido fue evaluado por método de expertos luego de ser aplicado en Softel, demostrando su utilidad práctica para continuar su implantación y ser generalizado a otros proyectos con un gran impacto en la mejora de la gestión de los proyectos de la organización siempre que cumplan las características de este tipo de organización de desarrollo de software (Valladares, 2010).

Modelo de un Sistema de Razonamiento Basado en Casos para el Análisis en la Gestión de Riesgos

Propone un modelo para el análisis en la GR que incluye mecanismos para la acumulación de experiencia utilizando la técnica de Razonamiento Basado en Casos (RBC). Este modelo es resultado de una tesis para optar por el título de Máster en Ciencias aplicable a proyectos de producción de software que deseen implementar una GR periódica con el objetivo de realizar un análisis de los riesgos ya identificados previamente, para determinar los riesgos más similares y con ello sus respuestas o planes de mitigación, que permitirá disminuir las amenazas y aumentar las oportunidades (Rivera, 2010).

Perspectivas y retos de la Gestión de Riesgos

El análisis de la bibliografía permitió constatar que para resolver la problemática actual en el desarrollo de aplicaciones informáticas no es necesario determinar cuál enfoque de GR es el mejor, sino cuál es el adecuado de acuerdo con las características únicas de los proyectos y su entorno de trabajo. Muchos de los marcos de GR analizados requieren del proyecto una sólida cultura de gestión (SEI y PMI) o demanda una profunda capacitación del personal en cuanto a las técnicas a aplicar (MAGERIT).

Sin embargo, los diferentes enfoques de GR estudiados ofrecen fortalezas útiles para la conformación de una propuesta idónea que elimine las debilidades identificadas en estos marcos de GR, en busca de un proceso capaz, que permita su mejora continua teniendo en cuenta las particularidades del proyecto. El estudio de varios enfoques de GR, algunos de ellos descritos anteriormente, demuestra que la GR enfrenta retos que pueden resumirse de la siguiente forma:

1. Mito del análisis cuantitativo: Establecer el análisis cuantitativo como una etapa que profundiza los resultados del análisis cualitativo con las mismas actividades, técnicas y herramientas, enfocando las diferencias solo en que el primero se basa en cuantificaciones y el segundo en estimaciones, es lo planteado en muchos modelos. En varios casos no se realiza un análisis cuantitativo por falta de conocimiento o se ejecuta de manera incorrecta, olvidando la definición de objetivos cuantificables de acuerdo con las características del proyecto.
2. Insuficiente integración de la GR en el desarrollo de software: Una práctica común en el desarrollo de aplicaciones informáticas es la realización de un análisis inicial de riesgos y no un análisis frecuente integrado a las actividades cotidianas de gestión de proyecto. Las actividades de GR, sus roles y responsabilidades se perciben como un contenido adicional de trabajo y no como un elemento importante de retroalimentación útil para la toma de decisiones de gestión del proyecto.
3. Débil seguimiento y control: Las actividades que presentan mayores deficiencias son la ejecución de los planes de mitigación y contingencia y el seguimiento y control de los riesgos. No usar suficientes indicadores que permitan retroalimentar y mejorar el proceso de GR implica que en el proyecto no se obtengan resultados que permitan tomar decisiones acertadas relacionadas con la GR. Las mediciones generalmente están

orientadas a caracterizar y evaluar el impacto y probabilidad de ocurrencia de los riesgos, y en consecuencia la exposición al riesgo.

4. Deficiente automatización: La automatización de todo o parte de los procesos de GR conceptualizados ha quedado rezagada. Se idean nuevas propuestas de GR para los proyectos pero no se ofrecen facilidades que permitan manejar la información resultado de las actividades de GR, la utilización del conocimiento histórico en la GR del proyecto y la interpretación de los indicadores.

Herramientas de Gestión de Riesgos

Las herramientas software de GR disponibles en el mercado siguen determinadas metodologías (Mathkour, et al., 2008). Se enfocan sólo en una categoría de riesgos (TRIMS – Sistema de Mitigación e Identificación de Riesgos Técnicos / Technical Risk Identification and Mitigation System), o están orientadas a compañías maduras que poseen una amplia base de datos organizacional que les permite generar información de categorías propias de riesgos (Risk Trak y Welcome Risk), o bien emplean un mecanismo que no se orienta al uso de clasificaciones de riesgos (ARM – Active Risk Manager).

Se destaca, la herramienta Chinchón–Análisis del riesgo, desarrollada en Java, libre, basada en el modelo MAGERIT, pero sólo se enfoca en la fase de análisis cuantitativo del riesgo. La Tabla 3 describe algunas herramientas para la GR a través de sus elementos más representativos.

Tabla 3. Herramientas para la Gestión de Riesgos.

Producto	Proveedor	Descripción
Active Risk Manager (ARM) (Active Risk, 2012)	Strategic Thought	Herramienta integrada de GR que brinda una solución para la identificación de riesgos mediante la utilización de la información contenida en el WBS de proyecto.
Technical Risk Identification and Mitigation System (TRIMS) **(ACC, 2009)**	Best Manufacturing Practices	Herramienta integrada de GR que emplea ingeniería de conocimientos y que se enfoca en la identificación y medición de riesgos técnicos de proyectos.
RiskTrak	Risk Services &Technology	Herramienta integrada de

(RTI, 2010)		GR que brinda una solución para la identificación de riesgos mediante el empleo de bases de datos.
WelcomRisk **(ACC, 2005)**	Welcom	Herramienta integrada de GR que brinda una solución para la identificación sistemática de riesgos mediante la utilización de bibliotecas configurables de categorías de riesgos.
Chinchón – Análisis del riesgo (Argemí, 2002)	Free	Herramienta para analizar cuantitativamente el riesgo de un sistema de información. La herramienta sigue el modelo MAGERIT V1.0.
Pilar (Huerta, 2012)	Free	PILAR 5.2.3 es una aplicación implementada en java basada en MAGERIT V2.0. La herramienta permite la realización de análisis de riesgos bajo un enfoque tanto cualitativo como cuantitativo y la realización de análisis de impacto en el ámbito de la continuidad de negocio.

En la actualidad, las herramientas existentes no sólo se basan en la madurez de las empresas o de sus bases de datos organizacionales, sino que también incluyen patrones de reconocimiento de comportamientos o experiencias anteriores, es decir herramientas que aprovechando las novedosas técnicas de inteligencia artificial, facilitan o ayudan a dar solución a la problemática de la GR.

Antecedentes y situación actual de las herramientas Inteligentes para la gestión de riesgos

Si bien las ideas fundamentales de la Inteligencia Artificial (IA), se remontan a la lógica y algoritmos de los griegos, y a las matemáticas de los árabes, varios siglos antes de Cristo, el concepto de obtener razonamiento artificial aparece en el siglo XIV. A finales del siglo XIX se obtienen lógicas formales suficientemente poderosas y a mediados del siglo XX, se obtienen máquinas capaces de hacer uso de tales lógicas y algoritmos de solución. Esta ciencia surge en una reunión realizada en el Dartmouth College (Hanover, EEUU) en 1956 (Aguirre, 2010).

A pesar de que la mayoría de los intentos para definir términos complejos y a la vez ampliamente usados suelen ser inútiles, es positivo al menos esbozar los límites aproximados, en los que enmarcar el concepto de IA. Esta ciencia estudia cómo lograr que las máquinas realicen tareas que, por el momento son realizadas mejor por los humanos.

Algunas de las técnicas difundidas de la IA son las redes neuronales, algoritmos genéticos, colonias de hormigas, razonamiento basado en reglas y razonamiento basado en casos. Las redes neuronales se enfocan en problemas donde las entradas presentan ruido o están incompletas, como el Análisis y Procesado de señales, Reconocimiento de Imágenes o Robótica (Basogain, 2008; Lundström, et al., 2008; Anthony, et al., 2009). La aplicación más común de los algoritmos genéticos ha sido la solución de problemas de optimización, en donde han mostrado ser muy eficientes y confiables (Gonçalves, et al., 2008; Altiparmak, et al., 2009). Las colonias de hormigas son algoritmos multiagentes diseñados para trabajar en un ambiente con obstáculos y encontrar una solución cercana a la óptima, analizan distribuciones matemáticas, problemas de distribución geográfica y caminos más cortos (Pachón, 2009; Dorigo, et al., 2010). El razonamiento basado en reglas resuelve un problema real de un tamaño lo suficientemente grande como para poder evaluar la validez de las heurísticas obtenidas a partir de un experto humano e implementadas como reglas de un sistema experto, y al mismo tiempo lo suficientemente pequeño como para que el tiempo de cálculo sea mínimo (Gong, et al., 2011). El razonamiento basado en casos es un método con un alto grado de conocimiento y que reconoce experiencias pasadas, además mejora los métodos existentes para solucionar problemas (Cunningham, 2009). La técnica adecuada para utilizar la experiencia existente en la universidad en cuanto a la GR es utilizar el razonamiento basado en casos, teniendo en cuenta la gran cantidad de proyectos con características diversas que no pueden ser restringidos a un conjunto pequeño de reglas pero que constituyen al mismo tiempo un caudal considerable de conocimiento acumulado.

Existen diferentes herramientas que permiten, con el uso de técnicas de IA, la GR. En estos sistemas, o los riesgos que gestionan son ajenos a los del ciclo de vida del software o se centran en etapas específicas del análisis de los riesgos. Por otra parte constituyen ejemplos de sistemas o herramientas que tratan riesgos de diferentes tipos, según las características para las cuales se concibieron.

Sistema Inteligente de Administración de Riesgo SIAR®

El SIAR® es una solución automatizada para las aduanas que utiliza modelos econométricos que identifican los criterios relacionados con la evaluación del riesgo en el ámbito de las transacciones comerciales (COTECNA, 2011). Desarrollado por Cotecna, con sede en Suiza, aplica una serie de criterios de manera sistemática para determinar el nivel de riesgo de cada transacción y asigna los niveles de intervención de las aduanas según el nivel de riesgo determinado y los recursos disponibles. El SIAR® es un sistema innovador que ayuda a las administraciones aduaneras ya que ofrece las siguientes ventajas:

- Un enfoque automatizado: Se evalúan los envíos y se designan niveles de riesgo de manera automática como parte del proceso de trabajo habitual dentro del SIAR® sin necesidad de intervención manual.
- Un enfoque centralizado: Se asignan niveles específicos y apropiados de intervención a cada envío basándose en el riesgo; de esta manera se obtiene un uso de los recursos más eficaz y efectivo.
- Un enfoque dinámico: El SIAR® tiene en cuenta los resultados de las intervenciones (incluyendo el aforo físico, el examen y/o el escaneado) para actualizar continuamente su base de datos; esto permite al sistema responder de manera adecuada frente a los cambios de patrones por incumplimiento.

Sistema Inteligente de Gestión de Vulnerabilidades Informáticas (SIGVI) - (Ecuador 2008-2009)

Este proyecto tiene como finalidad el propiciar la construcción de la aplicación computacional SIGVI, un software desarrollado dentro del compromiso institucional de la Fundación Universitaria Iberoamericana (FUNIBER) con el software libre. SIGVI facilita la gestión de alertas por vulnerabilidades para que las organizaciones actúen con tiempo suficiente para poder corregir las vulnerabilidades antes de que el riesgo potencial de su ocurrencia se convierta en una amenaza real o en un desastre (FUNIBER, 2012).

SIGVI resulta útil a diversas organizaciones que deben superar una serie de vulnerabilidades y que no cuentan con un mecanismo certero, seguro, confiable y constante de recepción, procesamiento, discernimiento y ejecución de las alertas que se reciben. Con SIGVI una organización puede procesar las alertas con eficiencia y eficacia y rápidamente plantear, generar y ejecutar una solución o una

actuación que evite la vulnerabilidad probable. SIGVI se alimenta de un base de datos que permite, por un lado, contar con un gran recurso de información de diversos sistemas de alertas aglutinando a otros sistemas de alertas y, por otro lado, el mecanismo automatizado de gestión de vulnerabilidades y el propio sistema de análisis y búsqueda de información en la base de datos propia y en bases de datos externas transfiriendo la experiencia y el know-how que se va acumulando en el propio sistema.

Herramientas inteligentes en Cuba

En Cuba, las principales manifestaciones de esta ciencia, se centran fundamentalmente en el campo de la medicina, se han experimentado avances en este sentido a través de historias clínicas electrónicas con insospechadas posibilidades en el futuro, sistemas para tratamientos estadísticos como el APUS que es capaz de ofrecer información gerencial para la toma de decisiones, agentes inteligentes para el diagnóstico de trastornos ginecológicos (Expósito, et al., 2008). Además, Cuba cuenta con un Centro de Cibernética Aplicada a la Medicina (CECAM), que concentra esfuerzos en disímiles direcciones de las aplicaciones e investigaciones médicas y con intereses marcados en el campo del intelecto artificial.

Sistemas Basados en el Conocimiento. Razonamiento Basado en Casos (RBC)

Los sistemas expertos o basados en el conocimiento (SBC), típicos del campo de la IA, son programas para computadoras que simulan las cadenas de razonamiento que realiza un experto para resolver un problema de su dominio (Li, et al., 2008; Chang, et al., 2008). Para conseguirlo, se dota al sistema de un conjunto de principios o reglas que infieren nuevas evidencias a partir de la información previamente conocida.

A los SBC lo caracterizan más rasgos que simplemente el hecho de duplicar el conocimiento y la experticia de un humano para un dominio específico. Los SRBC se sustentan en tres principios básicos (Cortez, et al., 2010):

- Solución de problemas superpuestos: se aplica en casos que utiliza casos resueltos menores.
- Principio de optimalidad de Bellman: memoriza la mejor solución, luego de un proceso de selección.

- Memorización: memoriza las soluciones obtenidas en la librería de casos para uso posterior.

El Razonamiento Basado en Casos (RBC) representa un método para resolver problemas no estructurados, en el cual el razonamiento se realiza a partir de una memoria asociativa que usa un algoritmo para determinar una medida de semejanza entre dos objetos. Debe destacarse que es una técnica, en la cual la memoria se sitúa como fundamento de la IA, concretamente de los SBC.

Arquitectura de los sistemas basados en casos

Un sistema basado en casos tiene dos componentes principales: una base de casos y un resolvedor de problemas (Sentí, 2010). La base de casos contiene las descripciones de los problemas resueltos previamente. Cada caso puede describir un episodio particular o una generalización de un conjunto de episodios relacionados. En el estilo de solución de problemas se recupera un caso semejante al nuevo y la solución del problema recuperado se propone como solución potencial del nuevo problema. Esto se deriva de un proceso de adaptación en el cual se adecua la vieja solución a la nueva situación. La arquitectura de los Sistemas Basados en Casos se muestra en la Ilustración 6.

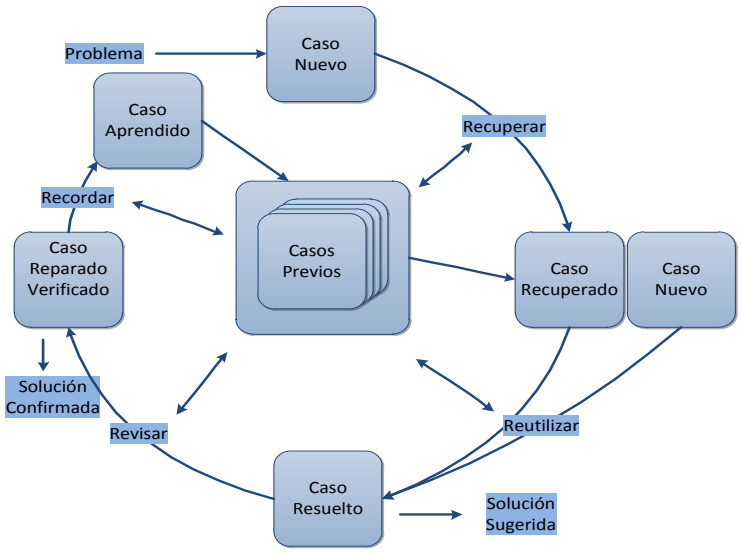


Ilustración 6. Ciclo de Razonamiento Basado en Casos. (Sentí, 2010)

Herramientas que utilizan Sistemas Basados en Casos

Un ejemplo relevante en Cuba, es el Sistema Inteligente de Selección de Información (SISI), elaborado en el Centro de Cibernética Aplicada a la Medicina

(CECAM), que implementa el razonamiento basado en casos orientado a tareas de diagnóstico médico. Este sistema o herramienta recoge elementos actualizados que son capaces de simular en una mayor escala el proceso de enseñanza y aprendizaje en un entorno Web donde se integran la programación para el cliente (Javascript) y para el servidor (PHP); bases de datos en MYSQL e información sobre todo lo relacionado con sistemas tutoriales inteligentes, inteligencia artificial distribuida y multimedia.

Conclusiones Parciales

Se evaluó el estado de los marcos fundamentales para la GR sobre la base de las exigencias cubanas, concluyendo que los mismos no se ajustan a las necesidades que enfrenta hoy la GR en la UCI aunque presentan fortalezas relevantes que se pueden utilizar en la conceptualización de un nuevo enfoque idóneo para esta entidad. Se evaluó la aplicación de técnicas de IA en la resolución de problemas relacionados con la GR resaltando el uso de la experiencia en la identificación y mitigación de los riesgos.

El estudio de los fundamentos teóricos de GR y las oportunidades existentes en las técnicas de IA apoyaron la decisión de diseñar un proceso de GR que permita con su implantación apoyar la toma de decisiones relacionadas con la GR y elevar el nivel de capacidad del proceso de GR, utilizando la experiencia de la organización en la identificación y mitigación de los riesgos.

Capítulo 2. Proceso de Gestión de Riesgos para el Desarrollo de Aplicaciones informáticas

Introducción

En este capítulo se describe el Proceso de GR para el Desarrollo de Aplicaciones Informáticas, detallando cada una de sus actividades. Contiene las responsabilidades de cada rol que interviene en el proceso y los productos de trabajo que resultan como salida de las actividades. Se incluye una propuesta de técnicas para la realización del proceso, así como una herramienta inteligente para la identificación y mitigación de los riesgos.

Análisis de la Gestión de Riesgos en la UCI

El año 2007 marcó el inicio de las investigaciones relacionadas con la GR en la UCI. Se estudiaron los problemas principales que enfrentaba la GR y se implementaron soluciones que respondían a muchos de ellos. Una de las soluciones fue la creación de MoGeRi *(Ver epígrafe Modelo de Gestión de Riesgos en Proyectos de Desarrollo de Software (MoGeRi)),* que indicó cómo realizar una correcta GR en proyectos de desarrollo de Software. Este modelo fue aplicado en varios proyectos proporcionando experiencias para mejorar el mismo y los productos de salida de los procesos que define, sin embargo no es una práctica generalizada en la universidad. A continuación (Gráfico 4) se presentan las escalas de los problemas mayormente analizados de la GR en la UCI, durante los últimos 5 años.

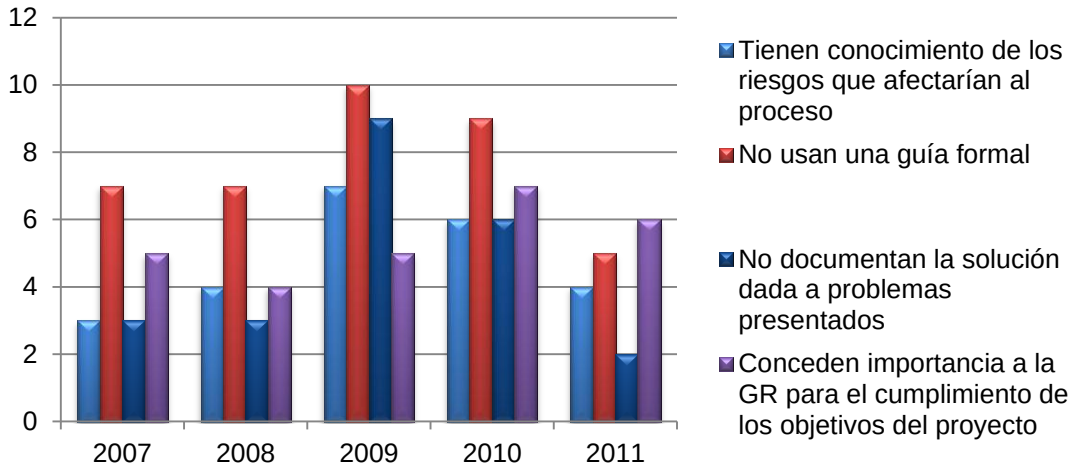


Gráfico 4. Principales problemas identificados en las investigaciones de GR en la UCI. [9]

[9] Elaborado a partir de la información obtenida en http://biblioteca.uci.cu/.

La UCI establece un Expediente de Proyecto que contiene la información de los mismos de acuerdo con plantillas establecidas. La reciente evaluación de algunos centros de desarrollo de la universidad en el nivel 2 de CMMI ha estimulado que se actualice el expediente de acuerdo con lo planteado en las PAs de este nivel. Cumpliendo lo normado en las áreas PP y PMC se creó la Plantilla Planes y Registro de Monitoreo que permite realizar la identificación de los riesgos. Se realiza además un análisis cualitativo basado en la Matriz de probabilidad/impacto y se establecen estrategias de mitigación y contingencia, así como un plan de seguimiento.

Como resultado de entrevistas realizadas a líderes de proyecto de 10 de los centros de desarrollo de la UCI, se arribó a la conclusión de que el mayor reto que presenta hoy la GR es lograr que se realicen en cada uno de los proyectos las actividades comprendidas para planificar la GR, identificar, evaluar, determinar respuestas y monitorear los riesgos en todas las etapas del proyecto, dado que una práctica común es realizar un análisis inicial y no un análisis frecuente de cada amenaza u oportunidad identificada. Estas últimas quedan desatendidas durante la GR dado que las plantillas definidas y establecidas en la universidad solo indican el análisis cualitativo, utilizando de la técnica Matriz de probabilidad/impacto lo referente a las combinaciones de probabilidad e impacto para priorizar los riesgos negativos, no los positivos. Tampoco se evidencia un análisis cuantitativo que ofrezca resultados fiables para la toma decisiones ante determinados eventos y la mejora del proceso de GR. La Plantilla Planes y Registro de Monitoreo se ajusta al nivel 2 de CMMI mas se omiten elementos claves del PA Administración de Riesgos (RISKM) desarrollada en el nivel 3 y que influyen en la mejora del proceso de GR:

SG 1 Preparar la gestión de riesgos.

SP 1.1 Determinar las fuentes y las categorías de los riesgos.

SP 1.3 Establecer una estrategia de gestión de riesgos.

SG 2 Identificar y analizar los riesgos.

SP 2.2 Evaluar, categorizar y priorizar los riesgos.

Proceso de Gestión de Riesgos para el Desarrollo de Aplicaciones Informáticas

Descripción gráfica del Proceso de Gestión de Riesgos para el Desarrollo de Aplicaciones Informáticas

El Proceso de GR para el Desarrollo de Aplicaciones Informáticas contiene elementos positivos de los modelos más populares, especialmente MoGeRi, uno de los más aplicados en la UCI. Persigue el objetivo de ser sencillo, fácil de aplicar y que utilice como entradas o salidas la documentación necesaria.

Si se aplica el Proceso de GR para el Desarrollo de Aplicaciones Informáticas definido y en la organización están completamente implementadas todas las demás PAs necesarias para alcanzar el nivel 3 de madurez de CMMI se puede aspirar a una evaluación satisfactoria de este nivel en una representación escalonada. En caso que se siga una representación continua de CMMI el Proceso de GR para el Desarrollo de Aplicaciones Informáticas definido permite alcanzar el nivel 5 de capacidad en el PA RSKM.

Ilustración 7. Proceso de Gestión de Riesgos.

El Proceso de GR para el Desarrollo de Aplicaciones Informáticas se presenta a través de una descripción gráfica (Ilustración 7 y 8) que abarca todas sus actividades y las entradas y salidas de cada una de ellas especificando el rol responsable de ejecutar la acción. Además contiene las guías de apoyo o métodos que pueden ayudar al equipo en el desarrollo de las actividades propuestas. Se incluyen los criterios de entrada al proceso: información general del proyecto y el ambiente; y de salida luego de la ejecución de todas las actividades: registro de riesgos con la estrategia de mitigación y contingencia y un conjunto de elementos relevantes para la toma de decisiones.

Proceso de Gestión de Riesgos para el Desarrollo de Aplicaciones Informáticas				
Criterios de Entrada	Características del negocio, del proyecto y del entorno del mismo.			
Criterios de Salida	Registro de Riesgos priorizados, planes de mitigación y contingencia y elementos para la toma de decisiones.			
Roles	Entrada	Técnicas	Actividades	Salida
			Inicio	
- Equipo de Proyecto	- Documentación histórica del proyecto - Plan de Proyecto (PP) - Informe preliminar	- Entrevistas - Reuniones - Análisis costo-beneficio	1. Determinación del alcance y la factibilidad de la GR en el proyecto.	- Objetivos de la GR - Restricciones generales - Dominio de la GR - Responsables de unidades del dominio - Gestor y equipo de GR - Comité de Seguimiento y Control - Informe de estudio de factibilidad de la GR - Informe de aprobación de la GR
- Gestor de Riesgos - Equipo de GR - Responsables de unidades del dominio - Comité de Seguimiento y Control	- Objetivos de la GR - Restricciones generales - Dominio de la GR en el proyecto	- Reuniones - Estructura de desglose del riesgo	2. Planificación de la GR.	- Plan de GR (PGR) - Recursos necesarios - Cronograma de GR en el proyecto - Responsabilidades de los participantes - Descripción de hitos - Fuentes y categorías de riesgos
- Equipo de GR - Gestor de Riesgos	- Objetivos de la GR - Restricciones generales - Dominio de la GR en el proyecto - Información histórica	- SIMR - Identificación de riesgos basada en rasgos - Diagrama causa-efecto - Método Delphi	3. Identificación de riesgos.	- PGR - Registro de riesgos
- Gestor de Riesgos	- Registro de riesgos	- Matriz de probabilidad/impacto - Método Delphi - Análisis mediante árbol de decisiones	[NO] 4. Análisis cualitativo y cuantitativo de los riesgos.	- PGR - Riesgos priorizados según su probabilidad de ocurrencia e impacto
- Equipo de GR	- Riesgos priorizados según su probabilidad de ocurrencia e impacto - PP - PGR	- SIMR - Externalización de la Situación - Clasificación de la causa raíz - Tormenta de ideas	5. Valoración y planificación de la estrategia para enfrentar el riesgo.	- PGR - Plan de mitigación - Planes de contingencia
- Equipo de GR - Comité de Seguimiento y Control	- PGR	- Reevaluación de los riesgos - Reuniones sobre el Estado de la Situación	6. Seguimiento y control de los riesgos.	- Informe sobre aplicación de indicadores - Elementos para la toma de decisiones - Lecciones aprendidas
			7. ¿Es el fin del Proyecto?	
			[SI] Fin	

Ilustración 8. Descripción Gráfica del Proceso de Gestión de Riesgos.

Descripción del Proceso de Gestión de Riesgos para el Desarrollo de Aplicaciones Informáticas

La descripción del proceso de GR en la Tabla 4 permite detallar cada una de las actividades propuestas, particularizando en las sub-actividades que deben ejecutarse para alcanzar las salidas propuestas.

Tabla 4. Descripción del Proceso de Gestión de Riesgos.

Proceso de Gestión de Riesgos para el Desarrollo de Aplicaciones Informáticas		
Criterios de Entrada	**Características del negocio, del proyecto y del entorno del mismo.**	
Criterios de Salida	**Registro de riesgos priorizados, planes de mitigación y contingencia y elementos para la toma de decisiones.**	
N.	**Descripción**	**Salida**
1.	**Determinación del alcance y la factibilidad de la GR en el proyecto** 1.1 El equipo de proyecto debe determinar los objetivos de la GR en el proyecto y las restricciones generales que se imponen. 1.2 El equipo de proyecto define el dominio e identifica el entorno y las relaciones dominio-entorno, así como los límites del alcance de la GR. 1.3 El Gestor de Riesgos y el Equipo de GR estiman los costos y determinan el volumen de recursos necesarios para la ejecución de la GR: humanos, temporales y financieros. Luego emiten una decisión a partir de la factibilidad determinada, si es pertinente o no, proceder con la realización de la GR o si es necesario modificar parámetros analizados. 1.4 Los resultados de la ejecución de la actividad deben ser comunicados al proyecto, de manera tal que exista un conocimiento generalizado del estado de las actividades. Además debe generarse documentación que incluye las experiencias personales y datos que puedan servir para análisis posteriores.	- Objetivos de la GR - Restricciones generales - Dominio de la GR - Responsables de unidades del dominio - Gestor y equipo de GR - Comité de seguimiento de GR - Informe de estudio de factibilidad de la GR - Informe de aprobación de la GR
2.	**Planificación de la GR** 2.1 En la planificación de la GR participan el Gestor de Riesgos, el Equipo de GR, los responsables de las unidades de dominio y el Comité de Seguimiento y	- Plan de GR (PGR) - Recursos necesarios - Cronograma de GR en el proyecto - Descripción de hitos

Control. Los mismos se encargan de plantear y programar las actividades de la GR. 2.2 La planificación debe incluir la determinación y asignación de los recursos necesarios (humanos, de organización, técnicos, etc.) para la realización de la GR. 2.3 El equipo debe definir las funciones y responsabilidades de los participantes, elaborar el calendario concreto de realización de las distintas etapas, actividades y tareas de GR en el proyecto y verificar la disponibilidad de los medios materiales necesarios. 2.4 Deben determinarse las fuentes y las categorías de los riesgos del proyecto. 2.5 Los resultados de la ejecución de la actividad deben ser comunicados al proyecto, de manera tal que exista un conocimiento generalizado del estado de las actividades. Además debe generarse documentación que incluye las experiencias personales y datos que puedan servir para análisis posteriores.	- Responsabilidades de los participantes - Fuentes y categorías de riesgo
3. Identificación de riesgos 3.1 El equipo de proyecto debe apoyar la actividad de identificación de los riesgos desde la visión particular de cada integrante de acuerdo con la unidad de dominio a la que pertenecen. 3.2 La caracterización de los riesgos se debe realizar para cada uno de los riesgos definidos, buscando el mayor detalle en la identificación para lograr un mejor análisis del riesgo. 3.3 SIMR (*ver epígrafe Sistema Inteligente de Mitigación de Riesgos*) ofrece un listado de posibles riesgos que pueden afectar al proyecto, estos deben filtrarse para verificar que los riesgos identificados estén acordes con los elementos particulares del proyecto. 3.4 Los resultados de la ejecución de la actividad deben ser comunicados al proyecto, de manera tal que exista un conocimiento generalizado del	- Registro de riesgos

	estado de las actividades. Además debe generarse documentación que incluye las experiencias personales y datos que puedan servir para análisis posteriores.	
4.	**Análisis cualitativo y/o cuantitativo de los riesgos** 4.1 El gestor de riesgos apoyado por el equipo de gestión de riesgos se encarga de estimar la probabilidad de ocurrencia y el impacto del riesgo. 4.2 La criticidad del riesgo, dada por la multiplicación de la probabilidad por el impacto, constituye el elemento esencial para priorizar el riesgo tomando como base la caracterización del análisis cualitativo. 4.3 La realización de un análisis cuantitativo se enfoca en cuantificar la probabilidad de ocurrencia y el impacto del riesgo basándose en el costo como elemento crítico de afectación. 4.4 De acuerdo con el resultado que aporta el análisis cuantitativo se analiza nuevamente la prioridad del riesgo. 4.5 Se verifica la exactitud de los datos, estimaciones y cálculos realizados y la exactitud de los atributos de probabilidad e impacto estimados o calculados, para asegurar la precisión del análisis. 4.6 Los resultados de la ejecución de la actividad deben ser comunicados al proyecto, de manera tal que exista un conocimiento generalizado del estado de las actividades. Además debe generarse documentación que incluye las experiencias personales y datos que puedan servir para análisis posteriores.	- Riesgos priorizados según su probabilidad de ocurrencia e impacto
5.	**Valoración y planificación de la estrategia para enfrentar el riesgo** 5.1 El equipo debe identificar las estrategias viables frente al riesgo y seleccionar una de ellas para determinar de acuerdo con el resultado del análisis cómo se enfrentará a una amenaza u oportunidad ofrecida por el riesgo. 5.2 Las respuestas o acciones concretas a ejecutar de	- Plan de mitigación - Planes de contingencia

acuerdo con la estrategia seleccionada deben contribuir al cumplimiento de la misma. 5.3 El Gestor de Riesgos debe ajustar el uso de los recursos y el cronograma para que las respuestas sean llevadas a cabo satisfactoriamente. Esta acción debe realizarse a partir de una valoración de la factibilidad de ejecutar determinadas acciones, pues estas tendrán efecto en la línea base del proyecto. 5.4 SIMR (*ver epígrafe Sistema Inteligente de Mitigación de Riesgos*) ofrece un listado de posibles riesgos con su correspondiente estrategia de mitigación, las cuales deben filtrarse para verificar que en realidad se adecúen a los elementos particulares del proyecto. 5.5 Los resultados de la ejecución de la actividad deben ser comunicados al proyecto, de manera tal que exista un conocimiento generalizado del estado de las actividades. Además debe generarse documentación que incluye las experiencias personales y datos que puedan servir para análisis posteriores.	
6. Seguimiento y control de los riesgos 6.1 El Comité de Seguimiento y Control debe manejar indicadores para valorar la calidad del proceso de GR, buscando mantener o mejorar la eficacia del mismo. 6.2 Cada riesgo identificado y analizado debe monitorearse de acuerdo con las respuestas ejecutadas, actualizando el estado del mismo en un periodo definido por el Gestor de Riesgos. 6.3 Se debe realizar un control de las actividades y la ejecución de las respuestas verificando que los hitos de GR se hayan cumplido exitosamente. 6.4 Teniendo en cuenta los objetivos de GR definidos, los indicadores analizados y los controles realizados se deben tomar decisiones sobre la GR. Podrán mantenerse las pautas anteriores si la gestión ha sido eficaz, pueden necesitarse más	- Informe sobre análisis de indicadores - Elementos para toma de decisiones - Lecciones aprendidas

	elementos para su mejor análisis, o bien redefinirse en caso de no obtenerse los resultados esperados.	
	6.5 Cuando en el proyecto se decida registrar los productos de trabajo en la base de conocimientos, entonces debe preparase un Informe de preparación de la GR, con los elementos esenciales de los productos Objetivos de la GR, Restricciones generales, Dominio de la GR, Informe de estudio de factibilidad de la GR e Informe de aprobación de la GR.	
	6.6 Los resultados de la ejecución de la actividad deben ser comunicados al proyecto, de manera tal que exista un conocimiento generalizado del estado de las actividades. Además debe generarse documentación que incluye las experiencias personales y datos que puedan servir para análisis posteriores.	
7.	7.1 Si es el fin del proyecto ir a Fin. 7.2 Si no es el fin del proyecto ir a la actividad 2.	

Roles del proceso y sus responsabilidades

Cada rol implicado en el Proceso GR para el Desarrollo de Aplicaciones Informáticas presenta un conjunto de responsabilidades (Tabla 5) que lo comprometen con el buen funcionamiento del proceso propuesto. Es por ello relevante que las responsabilidades estén debidamente definidas y distribuidas y que cada rol conozca y esté apto para el cumplimiento de las mismas.

Tabla 5. Responsabilidades de cada Rol definido.

Rol	Responsabilidades
Gestor de Riesgos	- Dirige y monitoriza el Proceso de GR para el Desarrollo de Aplicaciones Informáticas. - Realiza el PGR teniendo en cuenta los recursos necesarios, el cronograma de actividades y los hitos correspondientes. - Define las responsabilidades de los involucrados. - Define herramientas y técnicas a aplicar en el Proceso de GR para el Desarrollo de Aplicaciones Informáticas. - Identifica, evalúa, categoriza y prioriza los riesgos. - Realiza un análisis cualitativo y cuantitativo de los riesgos.

	- Controla la probabilidad de ocurrencia de los riesgos. - Dirige la ejecución de los planes de mitigación y contingencia. - Participa activamente en la elaboración de la estrategia para enfrentar el riesgo. - Propicia marcos de intercambio de experiencias y la correspondiente documentación de las mismas. - Toma decisiones acertadas con el fin de realizar una correcta GR, mejorar continuamente el proceso de GR y corregir las causas de los problemas detectados.
Responsables de unidades de dominio	- Participa en la realización del PGR. - Identifica, evalúa, categoriza y prioriza los riesgos. - Participa en la elaboración de la estrategia para enfrentar el riesgo.
Comité de Seguimiento y Control	- Participa en la realización del PGR. - Verifica el cumplimiento de las actividades e hitos planificados. - Emplea indicadores de valoración de la calidad del proceso. - Identifica elementos resultantes del proceso que influyan en la toma de decisiones para la mejora del proceso de GR. - Controla la probabilidad de ocurrencia de los riesgos. - Monitoriza la ejecución de los planes de mitigación y contingencia.
Equipo de GR	- Participa en la elaboración de la estrategia para enfrentar el riesgo. - Realiza las actividades de la GR. - Documenta las experiencias adquiridas durante la GR.
Equipo del Proyecto	- Participa en las reuniones relaciones con la planificación y determinación del alcance y la factibilidad de la GR aportando elementos de relevancia para la toma de decisiones relacionadas con el proceso de GR. - Participa en los marcos de intercambio de experiencias relacionadas con la GR en el proyecto.

Productos de trabajo

Las salidas de cada actividad del proceso constituyen productos de trabajo, que son el resultado de la aplicación de las técnicas y herramientas seleccionadas para llevar a cabo la acción correspondiente. Estos productos de trabajo a su vez pueden ser utilizados como entrada en otras actividades.

- ***Objetivos de la GR:*** *Los objetivos de la Gestión de los Riesgos del Proyecto son aumentar la probabilidad y el impacto de los eventos positivos, y disminuir la probabilidad y el impacto de los eventos adversos para el proyecto* (PMI, 2008). La organización debe

proponerse objetivos realistas y medibles que le permitan manejar las amenazas de forma proactiva en función de obtener beneficios para la organización.

- ***Restricciones generales:*** la definición de las restricciones de la organización para con la GR responde a las características de la misma y puede estar influenciada por situaciones externas o internas. Zulueta en la definición de MoGeRi (Zulueta, 2008) propone grupos de restricciones que facilitan la identificación de las mismas: Anexo 7.
    - Restricciones políticas o gerenciales
    - Restricciones estratégicas
    - Restricciones geográficas
    - Restricciones temporales
    - Restricciones estructurales
    - Restricciones funcionales
    - Restricciones legales
    - Restricciones metodológicas
    - Restricciones culturales
    - Restricciones presupuestarias
- ***Dominio de la GR:*** definido como *unidades en las que se centra la GR* (Zulueta, 2008) debe ser determinado por la organización para abarcar las áreas claves de acuerdo con los Objetivos y Restricciones de GR definidas.
- ***Roles y responsabilidades de la GR:*** este producto de trabajo puede ser la actualización del documento de roles y responsabilidades de la organización. Debe detallarse qué responsabilidades son asignadas a cada rol en dependencia de la experiencia y las habilidades de los miembros del equipo.
- ***Informe de estudio de factibilidad de la GR:*** contiene un estudio económico financiero basado en la aplicación del método análisis coste-beneficio para definir si es factible o no realizar la GR.
- ***Informe de aprobación de la GR:*** el proceso de GR debe estar aprobado por la dirección de la organización, que provee recursos humanos y materiales para la ejecución de la GR. Este informe resume el compromiso de la dirección con la realización de las actividades de GR.

- ***Plan de GR (PGR):*** documento de relevancia en la GR, contiene los elementos necesarios que permiten a la organización ejecutar de forma correcta el proceso. Es elaborado por el Gestor de Riesgos con la colaboración del Equipo de Proyecto y principalmente de los responsables de cada unidad de dominio de la GR definido previamente. Sobre estos últimos recae la responsabilidad de registrar los riesgos de la organización por cada unidad de dominio, así como las estrategias de mitigación y contingencia. El Expediente de Proyecto v3.3 utilizado en la UCI que cumple con el nivel 2 de CMMI, otorgado recientemente, contiene en la sección Gestión de Proyecto la Plantilla de Planes y Registro de Monitoreo. La misma trata varios de los resultados de las actividades de GR, pero enfocado en el registro de los riesgos y la priorización de los mismos basado en su criticidad (impacto*probabilidad). Según CMMI *la estrategia de gestión de riesgos se documenta a menudo en un plan de gestión de riesgos de la organización o de un proyecto* (SEI, 2010) y la misma debe contener el alcance del esfuerzo de la gestión de riesgos, los métodos y las herramientas que se usarán para la identificación de riesgos, su análisis, mitigación, monitorización y comunicación, técnicas de mitigación de riesgos que serán usadas e intervalos de tiempo para la monitorización o revisión del riesgo. Se considera necesario la utilización de un producto de trabajo, el PGR, que abarque los elementos contenidos en la Plantilla de Planes y Registro de Monitoreo relacionados con los riesgos y los elementos propuestos por CMMI que no están contenidos en dicho documento:
    - Productos incluidos en la Plantilla de Planes y Registro de Monitoreo
        - Registro de riesgos
        - Riesgos priorizados según su probabilidad de ocurrencia e impacto
        - Plan de Mitigación
        - Planes de Contingencia
    - Productos necesarios en el PGR
        - Herramientas y técnicas a aplicar
        - Recursos necesarios

        - Cronograma de GR en el proyecto, deben determinarse las actividades de GR e incluirse en el cronograma general del proyecto
        - Descripción de hitos
        - Fuentes de riesgos
        - Categorías de riesgos
        - Políticas de la GR
- ***Informe sobre análisis de indicadores:*** contiene las medidas colectadas y el procesamiento de las mismas resultando indicadores que permiten medir el proceso y constituyen elementos para la toma de decisiones. Es relevante que se grafiquen los resultados aportando mayor visibilidad a los mismos.
- ***Lecciones aprendidas:*** Observaciones que resulten interesantes para su reutilización y aplicación en problemas similares. No se define un contenido específico para que exista la libertad de escribir sin ataduras todas las experiencias que se consideren necesarias.

Productos de trabajo a incorporar en la Base de Conocimientos

Los productos de trabajo a incorporar en la Base de Conocimientos de la organización deben contener información relevante y útil para posteriores análisis de enfrentamiento a situaciones similares. Además debe consultarse, actualizarse y ampliarse durante el ciclo de vida del proyecto, pues constituye una herramienta de trabajo que viabiliza el proceso de GR.

- ***Informe de preparación de la GR:*** documento que abarque la esencia de la información ofrecida en los análisis para obtener:
    - Objetivos de la GR
    - Restricciones generales
    - Dominio de la GR
    - Informe de estudio de factibilidad de la GR
    - Informe de aprobación de la GR
- ***Plan de GR (PGR):*** documento central de la GR donde se detallan, los resultados de las actividades de planificación, el registro de riesgos priorizados de acuerdo con los análisis cualitativo y/o cuantitativo, ejecutados con las técnicas y herramientas seleccionadas. Presenta las estrategias a seguir para enfrentar cada riesgo de acuerdo con actividades de mitigación y contingencia. Su aporte a la base de

conocimientos es relevante pues toda la información que incluye puede utilizarse en la solución y definición de propuestas que resuelvan problemas posteriores. Además constituye un documento de obligada consulta y actualización durante el ciclo de vida del proyecto.

- ***Informe sobre análisis de indicadores:*** debe contener los elementos para la toma de decisiones y va a aportar a la base de conocimientos cifras importantes para la obtención de estadísticas de la organización.
- ***Lecciones aprendidas:*** las experiencias adquiridas durante el proceso de GR son de relevancia para la gestión del conocimiento de la organización de manera tal que existan referencias cercanas para enfrentar problemas similares.

Técnicas que apoyan la ejecución del Proceso de GR para el Desarrollo de Aplicaciones Informáticas

Las técnicas aplicadas en los procesos facilitan la obtención de resultados y el análisis de los mismos. Pueden aplicarse varias técnicas en la búsqueda de alternativas de presentación y observación de los resultados.

A continuación se detallan técnicas concebidas en el marco de esta investigación y que apoyan las actividades de identificación de riesgos y valoración y planificación de la estrategia para enfrentar el riesgo.

1. ***Identificación de riesgos basado en rasgos:*** la técnica parte de la utilización de un sistema basado en casos (*Ver epígrafe Sistema Inteligente de Mitigación de Riesgos*), que arroja a partir de rasgos predefinidos un conjunto de riesgos de la base de casos que tengan un porciento de semejanza elevado. Utilizando este conjunto de riesgos se realiza un análisis, cuyo objetivo es identificar qué rasgos están relacionados con cada uno de los riesgos identificados. Una vez encontrada la relación entre los riesgos y los rasgos se determinan aquellos riesgos que no se relacionan con los rasgos del proyecto, estos son identificados por el sistema basado en casos dada su naturaleza de funcionamiento que utiliza porcientos de semejanzas que nunca son exactos. Esta técnica se usa como un refinamiento humano de los resultados preliminares obtenidos por el sistema de IA.
2. ***Externalización de la situación:*** análogo a la actividad de algunas empresas actuales que envían sus problemas o situaciones a una comunidad de usuarios con el objetivo de que estos identifiquen, exploten y

mitiguen los riesgos que puedan encontrarse en los productos que están siendo expuestos. Los riesgos identificados se someten a un proceso de reformulación de manera que los datos particulares expuestos que relacionan al riesgo con el proyecto sean eliminados de la forma del riesgo que se va a exponer a la comunidad. El resultado de este proceso es una formulación de riesgos más abstracta que permite a personal no autorizado o no familiarizado con el proyecto resolver los problemas que este presenta. La comunidad puede estar motivada económicamente, intelectualmente o políticamente y sus participantes pueden estar organizados por una compañía intermedia o por el mismo proyecto. La técnica se aplica para problemas de una complejidad especial determinada por el proyecto o cuando el personal de la organización no está preparada para enfrentarlo.

3. ***Clasificación de la causa raíz:*** utiliza el análisis de la causa raíz para obtener la causa de un riesgo determinado, una vez obtenida la misma se clasifica en ocasional, recurrente o perenne. Esta clasificación influye en la acción con la cual se va a responder el riesgo. Las acciones que se van a elegir teniendo en cuenta esta clasificación pueden o no estar entre las acciones sugeridas por el sistema basado en casos dado que el mismo no realiza dicho análisis humano.
   - Ocasional: indica que la causa es puramente coyuntural y no se prevé que se repita en el futuro. Estas causas normalmente son el resultado de la acción de factores fuera del control de la organización, aleatorios o imprevisibles.
   - Recurrente: consecuencia de problemas crónicos de la organización o factores establecidos en el contexto en el cual la organización opera, sea este contexto de cualquier naturaleza. Se prevé que estas causas ocurran periódicamente.
   - Perenne: derivada de la naturaleza misma de la actividad de la organización o del personal que en ella opera. Los riesgos que estas provocan son muy difíciles de resolver y probablemente resistan cualquier acción que se realice para mitigarlos. En estos casos los riesgos deben ser seguidos y su impacto minimizado.

Se plantea el uso de técnicas propuestas en otros enfoques de GR y que por su versatilidad pueden ser utilizadas para apoyar las actividades del Proceso de GR para el Desarrollo de Aplicaciones Informáticas.

1. ***Tormenta de ideas:*** técnica ideada en 1938 por Alex Faickney Osborn, definida por el Webster´s International Dictionary (Merrian-Webster, 2012) como *la práctica de una técnica de conferencia en la que un grupo de personas busca la solución a un problema específico, juntando todas las ideas aportadas en forma espontánea por sus integrantes*. Su regla fundamental es la prohibición de toda crítica a los planteamientos logrando una desinhibición que estimula el proceso creativo de los panelistas.
2. ***Entrevistas:*** método de investigación empírica que constituye una de las principales vías de recopilación de información. La experiencia de los entrevistados puede fortalecer los resultados en la identificación y caracterización de los riesgos.
3. ***Método Delphi:*** técnica creada por la Corporación RAND, que realiza pronósticos basados en la consulta de expertos. Sus características fundamentales son el anonimato, la iteración y realimentación controlada y la respuesta del grupo en forma estadística (Jeste, et al., 2010).
4. ***Diagrama causa efecto, Fishbone o Ishikawa:*** creado por Kaoru Ishikawa, responde a "Diagrama Espina de Pescado" o "Diagrama Fishbone" dada su forma similar a la cabeza de un pescado y sus espinas principales. Se basa en la identificación de las causas de los problemas, por lo cual puede ser perfectamente utilizado como complemento al uso de la técnica Clasificación de la causa raíz.
5. ***Estructura de Desglose del Riesgo (RBS)***: La caracterización de los riesgos puede realizarse a partir de esta técnica (PMI, 2008) estableciendo categorías de riesgo durante la planificación de la GR. Aunque varios autores (SEI, 2007; PMI, 2008; SEI, 2010) han definido categorías de riesgos a partir de sus fuentes más comunes es importante que la organización defina sus categorías de riesgos estableciendo niveles y personalizando las causas que pueden provocarlos. Anexo 5.
6. ***Matriz de probabilidad/impacto:*** especifica combinaciones de probabilidad e impacto que llevan a la calificación de los riesgos como *de prioridad baja, moderada o alta* (PMI, 2008). Es responsabilidad de la organización definir en qué escala se encuentra la combinación de probabilidad e impacto. Comúnmente se han definido colores (rojo, verde y amarillo) para asociar las prioridades y facilitar el análisis cualitativo de la amenaza o la oportunidad. Anexo 6.
7. ***Análisis mediante árbol de decisiones:*** se estructura usando un diagrama de árbol de decisiones que describe una situación que se está

considerando, y las implicaciones de cada una de las opciones disponibles y los posibles escenarios (PMI, 2008). Está conformado por puntos de decisión, alternativas, puntos de azar, estados de la naturaleza con sus probabilidades y resultados.

8. ***Análisis costo–beneficio:*** brinda los argumentos necesarios para definir si el proyecto puede tener un resultado favorable de forma tal que la empresa o entidad que lo ejecute pueda obtener el resultado que espera atendiendo al alcance, tiempo y costes del proyecto (Rodríguez, 2006). El objetivo de la técnica consiste en comparar los beneficios de un proyecto con los costos necesarios para llevarlo a la práctica.
9. ***Reevaluación de los Riesgos:*** Las reevaluaciones de los riesgos del proyecto deben ser programadas con regularidad. La cantidad y el nivel de detalle de las repeticiones que corresponda hacer dependerán de cómo avance el proyecto en relación con sus objetivos (PMI, 2008).
10. ***Reuniones sobre el Estado de la Situación:*** La GR del proyecto puede ser un punto del orden del día en las reuniones periódicas sobre el estado de la situación. Las discusiones frecuentes sobre los riesgos hacen que sea más fácil hablar de los riesgos, en particular de las amenazas, y que se haga con mayor exactitud (PMI, 2008).

Indicadores

Las razones para realizar mediciones del proceso y del producto, se enfocan en caracterizar, evaluar, predecir y mejorar. (Gao, et al., 2012) Se caracteriza para obtener una línea base necesaria para futuras valoraciones. Se evalúa para determinar el estado del proceso o producto de acuerdo con lo planificado. Se realiza una predicción basada en la medición con el fin de plantearse objetivos medibles y reales de acuerdo con el costo y el cronograma. La mejora como razón de medición apunta a identificar debilidades y oportunidades que se desprenden de los resultados y así planificar los esfuerzos necesarios para la mejora.

Los indicadores son parámetros utilizados para medir el nivel de cumplimiento de una actividad o un evento. Un indicador es una medida cuantitativa que puede usarse como guía para controlar y valorar la calidad de las diferentes actividades. Es decir, la forma particular (numérica) en la que se mide o evalúa cada uno de los criterios (García, et al., 2003). El uso de indicadores en la actividad ***Seguimiento y control de los riesgos*** para medir los resultados de la GR permitirá apoyar la toma de decisiones en la organización y mejorar la capacidad del proceso de GR.

Indicador 1. Exposición al riesgo del proyecto o vulnerabilidad

- **Objetivo:** Determinar cuán vulnerable es el proyecto en el enfrentamiento a los riesgos.
- **Fórmula**

  ER = $\frac{(c_b * B + c_m * M + c_a * A)}{T}$ Donde $0 \leq ER \leq 1$

  c_b: índice de afectación de un riesgo bajo

  c_m: índice de afectación de un riesgo medio

  c_a = 1: índice de afectación de un riesgo alto

  B = $\sum_{i=1}^{b} P_i$

  M = $\sum_{i=1}^{m} P_i$

  A = $\sum_{i=1}^{a} P_i$

  T = B + M + A
- **Interpretación**

  La fórmula general está compuesta por las sumatorias de las probabilidades de ocurrencia de cada riesgo multiplicados por los índices de afectación, los cuales pueden ser seleccionados por el gestor de riesgos de acuerdo con las características del proyecto o el nivel cuantitativo de importancia de los riesgos bajos, medios o altos. Sin embargo se propone que se usen:

  c_b = 0.2, c_m = 0.3, c_a = 1

  P_i es la probabilidad de ocurrencia del riesgo. Si no se puede estimar se hace una estimación pesimista. (Pi = 1: $\forall \{ Ai; Bi; Ci \}$)

  Los índices de afectación (c) bajan si el proyecto puede enfrentar los riesgos, sube de lo contrario. Valores: 0 < c ≤ 1. c_a = 1 siempre

  - 0 < ER ≤ 0.3 completamente expuesto al riesgo
  - 0.3 < ER ≤ 0.75 medianamente expuesto al riesgo
  - 0.75 < ER ≤ 1 mínimamente expuesto al riesgo
- **Fuentes de recolección**

  Los datos necesarios pueden encontrarse en el PGR, que debe estar actualizado para que los resultados sean fiables.

Nota: Este indicador puede utilizarse para determinar además el nivel de oportunidad que puede aprovechar el proyecto, basta hacer la misma consulta en la información referente a las oportunidades identificadas.

Indicador 2. Efectividad de las respuestas ejecutadas

- **Objetivo:** Determinar si el plan de respuestas que se está utilizando es en realidad efectivo de acuerdo con los resultados de aplicación de la estrategia, enfatizando en la necesidad de mitigar riesgos críticos.
- **Fórmula**

  $ER = \left|\text{SIGNO}\left(\frac{r_c - r_{cm}}{(r_c - r_{cm}) + 1}\right) - 1\right| * \left(\frac{c_{rae}}{c_{ra}} * 100\right)$

  ER: efectividad de las respuestas

  r_c: cantidad de riesgos críticos

  r_{cm}: cantidad de riesgos críticos mitigados

  c_{rae}: cantidad de respuestas aplicadas efectivas

  c_{ra}: cantidad de respuestas
- **Interpretación**

  La función *SIGNO* se encarga de devolver 1 si el número resultado es positivo, 0 si el número resultado es 0 y -1 si el número resultado es negativo. Aplicando el módulo a la función *SIGNO* que se aplica analizando la relevancia y priorización de los riesgos críticos mitigados en cuanto a la efectividad de las respuestas, se obtiene 1 o 0. Al multiplicarlo por el porciento de respuestas aplicadas efectivas se obtendrá el porcentaje de efectividad de las respuestas aplicadas siempre y cuando los riesgos críticos hayan sido mitigados. En caso contrario la efectividad de las respuestas es nula.
  - ER = 0, la efectividad de las respuestas es nula porque no se han mitigado los riesgos críticos.
  - ER = x %, la efectividad de las respuestas está dada por el porciento resultado de la fórmula.
- **Fuentes de recolección**

  Los datos necesarios se encuentran en el PGR que debe estar actualizado para que las respuestas sean fiables.
- **Gráfico de apoyo**

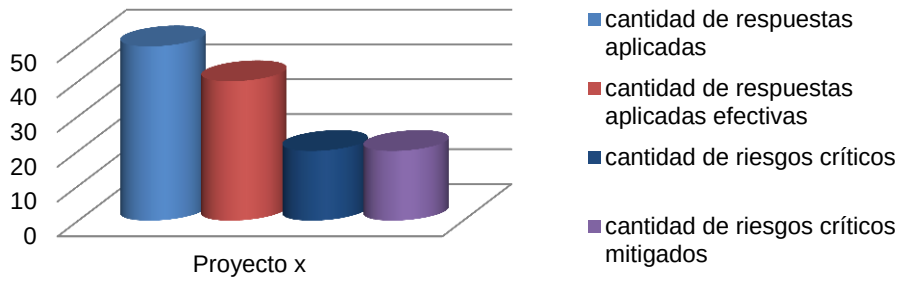


Gráfico 5. Gráfico de apoyo para el Indicador 2.

Indicador 3. Intervalo de seguimiento y control

- **Objetivo:** Determinar si el periodo de tiempo entre un seguimiento y control de los riesgos y otro es óptimo.
- **Fórmula**

  ISC = $T_{j-1} - T_{j-1} * t$ si j > n

  ISC = T si j ≤ n

$$t = \begin{cases} c, SIGNO(r_{nm}) > 0 \\ c * SIGNO(\sum_{i=j-n}^{n} SIGNO\ (r_j - r_i)), SIGNO(r_{nm}) = 0 \end{cases}$$

  T: cantidad de días entre un seguimiento y otro (actualmente)

  j: ordinal del seguimiento actual

  n: cantidad de seguimientos utilizados para establecer la tendencia de los riesgos

  t: factor de variación de T, -1 < t <1

  r_{nm}: cantidad de riesgos no monitoreados en un periodo de seguimiento y control

  c: coeficiente de severidad de la variación de T, 0 < c <1, se propone utilizar 0.5

- **Interpretación**

  t devolverá el valor del coeficiente (c) propuesto en caso de que la cantidad de riesgos no monitoreados detectados en el último periodo de seguimiento sea mayor que 0. En caso que sea igual a 0, o sea, no ocurren riesgos no monitoreados en ese periodo, t es el resultado de la multiplicación del coeficiente por el SIGNO de la sumatoria de los SIGNOS de las diferencias entre los riesgos monitoreados en la reunión actual y cada uno de los riesgos de las n reuniones anteriores.

  ISC es igual a 7 si la cantidad de reuniones que se han realizado no son suficientes para establecer una tendencia. En caso contrario ISC es el resultado de la diferencia entre el periodo anterior y la multiplicación del periodo anterior por el coeficiente de variación t.

  Un valor negativo de t denota una tendencia a la reducción de los riesgos monitoreados con relación a los riesgos monitoreados en seguimientos anteriores. Por consiguiente ISC se modifica aumentando su valor, lo que indica que los intervalos de seguimiento se harán más largos, liberando

recursos del proyecto para otras tareas. Un valor de 1 en t indica exactamente lo contrario.

Un valor de 0 de t puede deberse a uno de los siguientes casos:

- No se ha detectado variación alguna en los riesgos monitoreados en los puntos de seguimiento (de no haber variación el intervalo de seguimiento no varía).
- Las variaciones de los puntos de seguimiento utilizados se cancelan los unos a los otros denotando una gran variabilidad de la incidencia de los riesgos en el proyecto.

- **Fuentes de recolección**

  Los datos necesarios se encuentran en el Plan de Proyecto, que debe estar actualizado para que el porcentaje de esfuerzo en la mitigación de riesgos sea fiable.

- **Gráfico de apoyo**

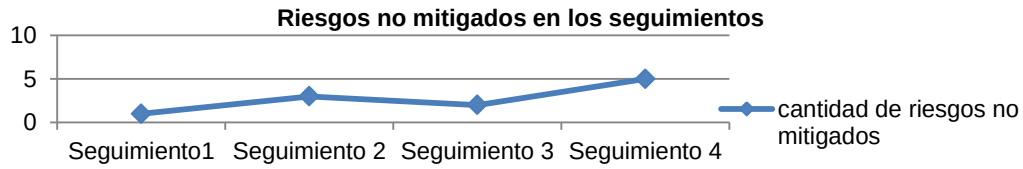


Gráfico 6. Gráfico de apoyo para el Indicador 3.

Indicador 4. Porcentaje de Esfuerzo de mitigación

- **Objetivo:** Determinar el esfuerzo que se está dedicando a la mitigación de riesgos con el fin de conocer al combinarlo con el resultado de otros indicadores si el esfuerzo realizado es el necesario.
- **Fórmula**

  EM = $\frac{EM}{EF} * 100$

  EM: esfuerzo de mitigación dado en horas/hombre

  EP: esfuerzo del proyecto dado en horas/hombre

- **Interpretación**

  El porcentaje de esfuerzo de mitigación permite conocer si el proyecto dedica un tiempo prudencial o no a la mitigación de riesgos. Este indicador debe combinarse con el resultado de otros indicadores como la efectividad de las respuestas, exposición al riesgo del proyecto o vulnerabilidad y el

intervalo de seguimiento y control para determinar si el esfuerzo dedicado con los resultados obtenidos es el óptimo.

- **Fuentes de recolección**

  Los datos necesarios se encuentran en el Plan de Proyecto, que debe estar actualizado para que el porcentaje de esfuerzo en la mitigación de riesgos sea fiable.

Indicador 5. Posibilidad de interrupción del servicio

- **Objetivo:** Determinar si existe o no la posibilidad de interrupción del servicio en casos de software de misión crítica.
- **Fórmula**

  P ∈ {0,1}

  Donde 0 es que no existe ningún riesgo identificado cuyo impacto sea suficiente para provocar una interrupción del servicio y 1 indica que existe al menos un riesgo identificado que podría provocar dicha interrupción. Los riesgos afectan este indicador sin tener en cuenta su probabilidad de ocurrencia, solo su impacto.

  $p = 1 \; \exists \, r : r \in \{riesgos \; con \; impacto > u\}$

  u: umbral de impacto de interrupción de servicio, definido por el gestor de riesgos. Se sugiere u > 0.80.

- **Interpretación**

  Indicador relevante para productos que sean de misión crítica o que entre sus requisitos no funcionales se haya especificado la disponibilidad continua del servicio. En el caso particular de la UCI sería útil para el soporte de proyectos de exportación y aplicaciones de prueba o desarrollo internas que necesitan estar corriendo todo el tiempo porque de ello dependen otras actividades con respecto al software.

  p = 0, no existe posibilidad de interrumpir el servicio

  p = 1, existe la posibilidad de interrumpir el servicio

- **Fuentes de recolección**

  Los datos necesarios se toman de los riesgos del PGR de acuerdo con su impacto y tipo.

Sistema Inteligente de Mitigación de Riesgos

Se propone el uso del Sistema Inteligente de Mitigación de Riesgos (SIMR), que se basa en la información que introduce el usuario referente a la descripción de un proyecto. Utiliza técnicas de IA, específicamente de un sistema de RBC para distinguir por rasgos la descripción dada. Luego, los compara con los almacenados en la base de casos con que cuenta y devuelve un grupo de casos semejantes. Adapta la solución y retorna una respuesta obteniéndose las posibles acciones a realizar o estrategias a tomar, permitiendo la retroalimentación y aprendizaje del sistema.

SIMR apoya las actividades **Identificación de riesgos** y **Valoración y planificación de la estrategia para enfrentar el riesgo** del Proceso de GR para el Desarrollo de Aplicaciones Informáticas al proporcionar un listado de riesgos con su correspondiente estrategia de mitigación. Estos resultados son valorados por el Equipo de GR determinando cuáles son los adecuados para el proyecto, de manera que se depura la solución brindada por SIMR y se alimenta a su vez la base de casos con una nueva experiencia. En la Ilustración 9 se presenta la interacción del Proceso de GR para el Desarrollo de Aplicaciones Informáticas con SIMR.

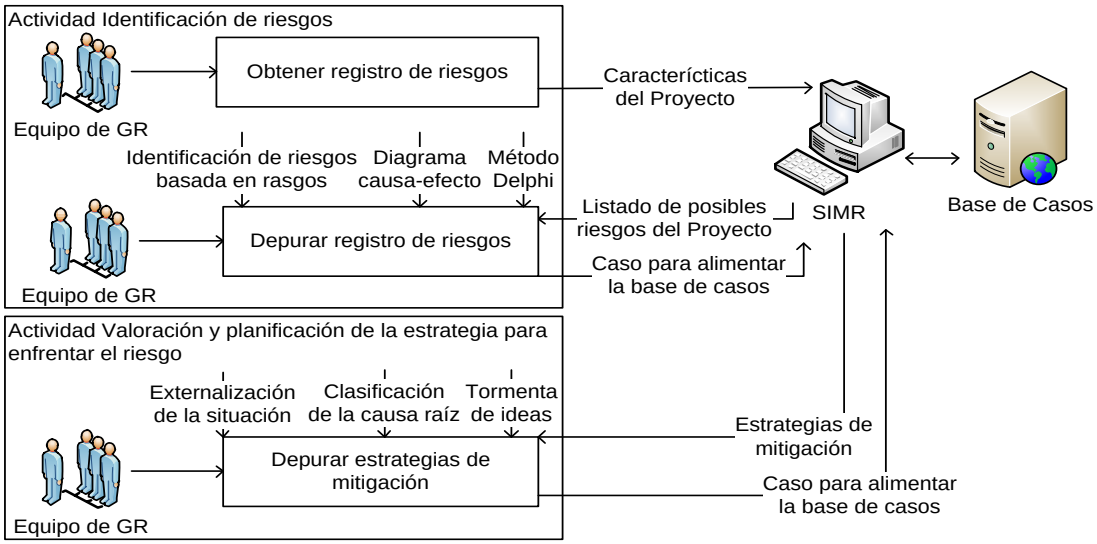


Ilustración 9. Interacción del Proceso de GR para el Desarrollo de Aplicaciones Informáticas con SIMR.

Este sistema está contextualizado en la UCI, particularmente en la Facultad 2 donde fue desarrollado, sin embargo dadas las características comunes de la mayor cantidad de proyectos de la universidad es perfectamente aplicable a la

totalidad de los mismos, o externalizarlo al país teniendo en cuenta las características avanzadas de la institución con respecto al proceso de desarrollo de software. Es perfectamente utilizable para aplicar únicamente el Proceso de GR definido y no la totalidad de procesos que incluye la Gestión de Proyectos.

SIMR es un híbrido de sistema de gestión web con técnicas de RBC. Se desarrolló sobre la plataforma java, utilizando el framework Grails[10]. Gestiona la información de los proyectos utilizándola además como rasgos a manejar en la base de casos para identificar los riesgos y las posibles estrategias de mitigación. Esta base de casos contiene como conocimiento almacenado, las características de los proyectos y los riesgos con sus clasificaciones y planes de mitigación, información que es utilizada a partir del ciclo mostrado en la Ilustración 6. El sistema presenta niveles de acceso para los roles definidos, garantizando la integridad de la información almacenada. Este mecanismo se basa en el framework de seguridad Grails Spring Security Core 1.0.1.

Base de casos definida y el proceso de identificación de riesgos

Cada pieza de experiencia almacenada constituye un conocimiento definido por el contexto de la misma. Las características que identifican al proyecto serán los rasgos predictores, a partir de los cuales se podrá identificar la ocurrencia de los riesgos y los rasgos objetivos, determinados según los posibles riesgos que pueden afectar a la organización. SIMR contiene una base de casos con 23 rasgos predictores que responden a características de los proyectos, a través de las cuales es posible predecir el advenimiento de situaciones no previstas teniendo en cuenta las experiencias acopiadas en la base de casos. Los rasgos que componen los casos almacenados en la base de casos, están formados por: el nombre, el valor y la relevancia (peso). La Tabla 6 muestra los rasgos definidos en la base de casos exponiendo también los valores de dominio y el tipo de las variables correspondientes.

Tabla 6. Conjunto de rasgos de la Base de casos, valores de dominio y tipo de variables respectivos.

Nombre del Rasgo	Valor de Dominio	Tipo
Modelo de proyecto	Muy Alta, Alta, Media, Baja, Ninguna	Ordinal
Dominio del negocio		
Experiencia en la plataforma		

[10] Marco de Trabajo (Framework) de desarrollo web. Desarrollado sobre la plataforma Java Enterprise Edition (JEE) que utiliza el lenguaje de programación Groovy.

Nivel de conocimiento del lenguaje	Mucha, Media, Baja, Ninguna	
Nivel de conocimiento de las herramientas		
Nivel de conocimiento de los desarrolladores		
Experiencia de trabajo en equipo		
Motivación		
Experiencia en el desarrollo de aplicaciones similares		
Nivel de dificultad del lenguaje		
Cohesión del equipo		
Estabilidad de los requisitos	Muy Estables, Estables, Poco estables, Inestables	
Complejidad de la aplicación	Alta, Media, Baja	
Relación con el cliente	Buena, Regular Mala	
Cronograma	Muy Variable, Variable, Poco variable	
Información que se maneja	Confidencial, Pública, Privada	Literal
Cantidad de especialistas a tiempo parcial	[1…n]	Numérico
Cantidad de especialistas a tiempo completo	[1…n]	
Cantidad de Computadoras	[1…n]	
Cantidad de funcionalidades simples	[1…n]	
Cantidad de funcionalidades medias	[1…n]	
Cantidad de funcionalidades complejas	[1…n]	

Los rasgos de la base de casos están determinados a partir de las variables ordinales, literales y numéricas. Estas variables permiten definir qué función de comparación se utilizará en cada caso. El uso de variables literales se enfoca en diferenciar la relevancia de la semejanza de cada valor de dominio según ocurra. El rasgo que se identifica de acuerdo con una variable literal es *Información que se maneja* para el cual el análisis va dirigido a que es más importante el manejo de información confidencial que pública. Se utiliza una variación de la función de comparación Manhattan ajustada para los rasgos cuyo valor es definido de acuerdo con una variable numérica. Esta función transforma el cálculo de la distancia entre dos valores en un intervalo definido o en un conjunto del cual se conozcan el mínimo y el máximo valor a un resultado que se define como semejanza. Las variables de tipo ordinal discreto, definen los rasgos que expresan cualidades que no pueden ser calculadas objetivamente, por lo cual la esencia a analizar es su orden relativo. Esta es la razón por la cual son normalizados para posteriormente ser comparados de acuerdo con la función de comparación de Manhattan (Anexo 8).

Para identificar los riesgos del proyecto se parte de la inserción de los datos del mismo, SIMR compara los datos entrados con los casos almacenados de acuerdo con las funciones de comparación presentadas para cada tipo de rasgo, que según su valor de dominio tendrá una función de semejanza, la cual compara dicho valor con su rasgo correspondiente en cada caso de la base de conocimientos. Una vez se han seleccionado las soluciones candidatas se adapta la solución de acuerdo con los pasos del RBC presentado en la Ilustración 6, para finalmente alimentar con el nuevo caso la base de conocimientos.

Conclusiones Parciales

Se contextualizó la GR en los proyectos de la UCI. Entrevistas a los líderes de dichos proyectos arrojaron como resultado que la GR realizada presentaba deficiencias de acuerdo con lo planteado en el PA RSKM. Se elaboró un Proceso de GR para el Desarrollo de Aplicaciones Informáticas que contiene una descripción gráfica y textual, compuesto por actividades, realizadas por roles con responsabilidades definidas, utilizando técnicas y productos de entrada y salida, cumpliendo con lo definido por CMMI. Se describieron técnicas e indicadores que apoyan la ejecución de las actividades del proceso de GR y la mejora continua del mismo. Se propuso el uso de una herramienta inteligente, SIMR, que permita identificar y definir la mitigación de los riesgos para un proyecto de software basado en la experiencia de la organización.

Capítulo 3. Análisis de los Resultados

Introducción

En este capítulo se realiza un análisis de compatibilidad del Proceso de GR para el Desarrollo de Aplicaciones Informáticas con modelos relevantes a nivel internacional y nacional. Se describe el Método Estándar de Evaluación CMMI para mejora de procesos (Standard CMMI Appraisal Method for Process Improvement), utilizado para realizar un diagnóstico y conocer el estado de los proyectos con respecto a la ejecución de las actividades de GR. Se incluye la caracterización de cuatro proyectos que sirven como experimento para aplicar el proceso de GR y determinar a través de una evaluación utilizando SCAMPI, si es factible generalizar su uso a la organización.

Compatibilidad con modelos de calidad

Las actividades del proceso de GR cumplen con lo establecido en las normas internacionales CMMI e ISO, relevantes dados sus roles de evaluador y certificador respectivamente. Se incluye un análisis respecto al PMBoK, guía clave para la gestión de proyectos. Además se establece una comparación con lo establecido en MoGeRi y la Resolución 60, ley vigente en Cuba y de obligatorio cumplimiento para la gestión del control interno en las organizaciones. En la Tabla 7 se evidencia la compatibilidad analizada.

Tabla 7. Compatibilidad del Proceso de Gestión de Riesgos con modelos relevantes de acuerdo con el ámbito internacional y nacional.

Actividades	CMMI	ISO 31000:2009	PMBoK	MoGeRi	Res. 60
1. Determinación del alcance y la factibilidad de la GR en el proyecto.		6.3		P1	Art 10 Art 11 b)
2. Planificación de la GR.	RSKM SP 1.1, 1.2 GP 2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 3.1		11.1	P1	Art 11

3. Identificación de riesgos.	RSKM SP 2.1	6.4.2	11.2	P2	Art 11 a)
4. Análisis cualitativo y cuantitativo de la GR.	RSKM SP 2.2	6.4.3 6.4.4	11.3, 11.4	P3	Art 11 a)
5. Valoración y planificación de la estrategia para enfrentar el riesgo.	RSKM SP 1.3	6.5.2 6.5.3	11.5	P4	Art 11 c) Art 12
6. Seguimiento y control de los riesgos.	RSKM SP 3.1, 3.2, GP 2.10, 4.1, 4.2, 5.1, 5.2	6.6 6.7	11.6	P5	Art 12

Método Estándar de Evaluación CMMI SCAMPI

SCAMPI proviene de las siglas en inglés del Método Estándar de Evaluación CMMI para mejora de procesos (Standard CMMI Appraisal Method for Process Improvement), está diseñado para ofrecer una calificación relativa al nivel de madurez/capacidad de las PAs de la organización. Es aplicable a una amplia gama de modos de uso de evaluación, incluyendo proceso internos de mejora.

Existen tres tipos de evaluaciones: SCAMPI A, SACMPI B y SCAMPI C. La primera es utilizada por los evaluadores para identificar fortalezas, debilidades y brindar una calificación de acuerdo con la madurez/capacidad de las áreas de proceso de la organización (SEI, 2006). SCAMPI B es conocida como evaluación de laboratorio y se utiliza para obtener resultados previos a una implantación del método. En el caso de SCAMPI C es útil para realizar una evaluación rápida de PAs que pudieran estar en riesgo para lo cual se utiliza una recolección básica de datos.

Aunque según las recomendaciones de SCAMPI todas las evaluaciones deben ser supervisadas por expertos para evitar malas interpretaciones, en esta investigación se realizará a modo de diagnóstico para conocer el estado de la capacidad del PA de GR de algunos proyectos de la UCI.

SCAMPI puede usarse para evaluar procesos internos de mejora, selección de proveedores y para el monitoreo de procesos. En esta investigación se usará para

evaluar procesos internos de mejora, para medir el proceso de GR a modo de diagnóstico, con el objetivo de definir una línea base de los niveles de capacidad/madurez en el proceso de GR, establecer o modificar un programa de mejora de dicho proceso y medir el progreso de la implementación de dicho programa. Según (SEI, 2006) las aplicaciones de la evaluación incluyen la medición del progreso de los procesos de mejora, conducción de auditorías de procesos, el enfoque en dominios o líneas de productos específicos, la evaluación de partes específicas de la organización y la preparación para evaluaciones dirigidas por los clientes externos. En este sentido las evaluaciones de SCAMPI complementan otras herramientas para la implementación de actividades de mejora de procesos.

Tipos de evidencia

La evidencia objetiva en la que se basa SCAMPI para evaluar se clasifica según:

- Documentos: información escrita relativa a la implementación de una o más prácticas de CMMI.
- Entrevistas: Interacción oral con aquellos que implementan o usan los procesos en la organización.

Indicadores de implementación de la práctica

La idea fundamental de los Indicadores de implementación de la práctica (PIIs) es que la aplicación de una actividad o implementación de una práctica resulta en "huellas" (evidencia que provee una base para la verificación de la actividad o practica). Son la consecuencia necesaria o incidental de la implementación de una práctica. Se dividen en categorías:

- Artefactos directos: salidas tangibles directas de la aplicación de una práctica, pueden ser los productos típicos que propone CMMI u otros definidos por la organización que demuestren la implementación de la práctica. Todas las prácticas deben tener artefactos directos como salida.
- Artefactos Indirectos: Son consecuencia de la ejecución de una práctica genérica o específica o que sustancie su implementación, pero no constituyen el propósito por el cual la práctica es realizada. Pueden ser minutas de reunión, reportes estadísticos, presentaciones o los resultados de mediciones.

- Entrevistas: sentencias orales o escritas que confirman o soportan la implementación o falta de implementación de una práctica genérica o específica. Pueden ser entrevistas, cuestionarios, presentaciones.

SACMPI propone una ***calificación por cada práctica analizada***, dada por la completitud de realización o ejecución de la misma. Siguiendo además la guía ofrecida a través de los PIIs se determina esta calificación. En la Tabla 8 se presenta la clasificación de ejecución de las prácticas.

Tabla 8. Clasificación de ejecución de las prácticas.

Calificación	Significado
CI (Completamente Implementado)	• Uno o más artefactos directos son presentados y juzgados como adecuados • Al menos un artefacto indirecto y/o una afirmación existe que confirma la implementación • No se observa ninguna debilidad
AI (Altamente Implementado)	• Uno o más artefactos directos son presentados y juzgados como adecuados • Al menos un artefacto indirecto y/o una afirmación existe que confirma la implementación • Se observan una o más debilidades
PI (Poco Implementado)	• No existen los artefactos directos o son juzgados como inadecuados • Uno o más artefactos indirectos o afirmaciones sugieren que algunos aspectos de la práctica son implementados • Se observan una o más debilidades O • Uno o más artefactos directos son presentados y juzgados como inadecuados • No existe otra evidencia (artefactos indirectos o afirmaciones) • Se observan una o más debilidades
NI (No Implementado)	• No existen los artefactos directos o son juzgados como inadecuados • No existe otra evidencia (artefactos indirectos o afirmaciones) • Se observan una o más debilidades

Para determinar cómo se aplica la práctica en la organización SCAMPI define un conjunto de ***reglas que apoyan al evaluador*** a tomar una decisión de acuerdo con lo observado en la ejecución de la evaluación. Las reglas se presentan en la Tabla 9.

Tabla 9. Reglas para componer las caracterizaciones de cada instancia.

Instancias	Salida	Observación
Todos CI	CI	Todas las instancias son caracterizadas como CI
Todos AI o CI con al menos un AI	AI	Todas las instancias son caracterizadas como AI o CI con al menos una instancia AI
Al menos un AI o CI y al menos un PI o NI	AI o PI	Al menos una instancia es caracterizada como AI o CI y al menos una instancia es caracterizada como PI o NI. El equipo debe determinar si la regla se inclina por AI o PI en dependencia de que las debilidades encontradas, en conjunto, tengan

		un significativo impacto negativo en el cumplimiento de los objetivos.
Todos PI o NI con al menos un PI	PI	Todas las instancias son caracterizadas como PI o NI con al menos un PI.
Todos NI	NI	

Planificación de la evaluación

La evaluación incluye tres fases: Planificación de la evaluación, Ejecución de la evaluación y Presentación de los resultados. Cada fase incluye procesos con actividades y un propósito definido. A continuación, en la Tabla 10, se presenta la planificación elaborada para el diagnóstico y la evaluación a aplicar en los proyectos a partir de las actividades propuestas por SCAMPI.

Tabla 10. Planificación de la evaluación SCAMPI.

Planificación de la Evaluación SCAMPI		
Fase I Planificación de la evaluación	Analizar los requisitos (objetivos, limitaciones, alcance, salidas y riesgos de la evaluación)	Entender las necesidades de negocio de la organización, establecer los objetivos, el alcance, salidas y riesgos de la evaluación.
	Desarrollar el plan de evaluación (horarios y recursos necesarios)	Documentar la planificación que incluye requisitos, acuerdos, estimaciones, riesgos y consideraciones prácticas (horarios e información contextual sobre la organización).
	Seleccionar y preparar al equipo de evaluación	Asegurarse que el equipo esté apropiadamente calificado para realizar la evaluación.
	Obtener y analizar la evidencia inicial objetiva	Obtener información que sirva de evidencia objetiva para verificar la implementación de las GG y SP.
Fase II Ejecución la evaluación	Preparar los participantes	Asegurarse de que los participantes estén informados de la evaluación, sus objetivos y propósito y estén dispuestos a participar en el proceso de evaluación.
	Examinar la evidencia objetiva	Examinar la evidencia objetiva acerca de las prácticas implementadas en la organización y describir los resultados de la evaluación.
	Documentar la evidencia objetiva	Crear registros permanentes de la información obtenida mediante la identificación y consolidación de notas, transformando los datos en registros que documentan prácticas de aplicación, así como los puntos fuertes y débiles.
	Verificar la evidencia objetiva	Verificar la aplicación de las prácticas de la organización para el proceso de GR, describiendo las lagunas en la aplicación de las prácticas del modelo.
	Validar los hallazgos preliminares	Validar los resultados preliminares, incluyendo deficiencias en la aplicación práctica con los miembros de la organización.
	Generar los resultados de la evaluación	Determinar la satisfacción de la meta basada en el grado de aplicación práctica del proceso de GR en la organización.

Fase III Presentación de los resultados	Entregar los resultados de la evaluación	Proporcionar resultados de la evaluación que se pueden utilizar para guiar las acciones futuras.
	Almacenar los activos de la evaluación.	Preservar los datos y registros importantes de la evaluación, y disponer de estos materiales sensibles de una manera apropiada.

Determinar la satisfacción de las áreas de proceso

Utilizando las definiciones de la guía de aplicación de SCAMPI se determina la satisfacción del cumplimiento de los niveles de madurez/capacidad de CMMI a partir de reglas que apoyan al equipo de evaluación para tomar la mejor decisión, basándose en el estudio de los PIIs.

- Satisfecho: las prácticas están institucionalizadas e implantadas de acuerdo con CMMI o mediante una alternativa adecuada.
- Parcialmente Satisfecho: hay inconsistencias o cobertura parcial en la implantación e institucionalización de las prácticas.
- No Satisfecho: hay debilidades significativas en la implantación e institucionalización y no existe una alternativa adecuada.
- No Aplicable: las prácticas no son aplicables en el contexto de la organización.
- No Evaluado: los hallazgos de la evaluación no cumplen los criterios de cobertura o el elemento CMMI está fuera del alcance de la evaluación.

Caracterización de la muestra de proyectos a aplicar SCAMPI B

Los resultados de las entrevistas realizadas a líderes de proyectos de 10 centros de desarrollo de la UCI, permitieron comprobar que las actividades de GR de riesgos realizadas, la forma de ejecutarlas y las deficiencias identificadas son similares. Teniendo en cuenta estos elementos y que el Proceso de GR para el Desarrollo de Aplicaciones Informáticas puede realizarse sin generar un conflicto con las actividades de gestión de proyecto y las características particulares de desarrollo de los mismos, se decidió utilizar como muestra para experimentar la aplicación del proceso a 4 proyectos de 2 de estos centros de desarrollo de la UCI, con misiones completamente diferentes. Cada proyecto a partir de sus características particulares presenta formas de hacer diferentes y riesgos que dependen de su entorno y de dichas características. Se utilizaron para la realización del diagnóstico proyectos de la Facultad 2 de los centros ISEC y TLM.

De manera general la organización de los proyectos es jerárquica, donde la autoridad principal recae en el jefe de proyecto. El mismo toma las decisiones tácticas para cumplir la estrategia dictada por las condiciones del proyecto, y es asistido en su cumplimiento por el consejo de dirección integrado por todos los roles mayores del proyecto, dígase el arquitecto, el analista, el administrador de base de datos, calidad y los jefes de equipo de programación. Esto permite que las decisiones se tomen con entrada de todos los roles y que la información fluya desde arriba a todos los niveles de la organización después de haber sido discutida en un foro común. A continuación se describen particularidades de cada proyecto diagnosticado.

Proyecto CICPC[11]

CICPC, siglas del nombre de la entidad policial científica venezolana (Cuerpo de Investigaciones Científicas, Penales y Criminalísticas) que se encarga de las investigaciones penales de Venezuela. La aplicación desarrollada por la UCI (SIIPOL, Sistema de Investigación e Información Policial) para esta entidad se encuentra en uso desde hace casi dos años y es compartida con el Cuerpo de Policía Nacional Bolivariana (CPNB) por lo cual estos dos proyectos tienen muchos puntos en común de acuerdo con el desarrollo del software aunque difieren en clientes y en la planificación de algunas actividades.

El sistema fue levantado en base a requisitos recogidos con el cliente en varias etapas. Cada una de estas levantó un conjunto de requisitos de una zona diferente del sistema, pero además este proceso sirvió como un filtro para depurar la información no considerada suficiente del levantamiento anterior. Este proceso evidencia la naturaleza iterativa de RUP, además de la depuración de la información recogida y su consiguiente re-implementación en los casos de uso (CU) y el código fuente del sistema. El mismo se desarrolló en la plataforma Java y es una aplicación Web a la medida, compatible con el navegador Mozilla Firefox versión 9.0 o superior. Utiliza como gestor de base de datos a Oracle EE 10g. Se han implementado más de 600 CU y actualmente trabajan en el proyecto cerca de 30 integrantes entre especialistas, profesores y estudiantes.

Proyecto CPNB[12]

[11] Información obtenida a partir del líder de proyecto de CICPC.
[12] Información obtenida a partir de la analista principal de CPNB.

CPNB, siglas del nombre de una de las entidades policiales venezolanas (Cuerpo de Policía Nacional Bolivariana) que presenta varios servicios a disposición de la seguridad de los ciudadanos y la prevención del delito. El sistema utilizado es una ampliación y personalización del SIIPOL, sistema desarrollado para el CICPC de Venezuela. El proyecto está conformado por 14 estudiantes y 6 profesores, que realizan el desarrollo de la aplicación en Cuba y las etapas de aceptación, piloto y despliegue en Venezuela. La definición de las funcionalidades del sistema se realizó en Venezuela teniendo en cuenta las necesidades de la organización y utilizando la metodología de desarrollo RUP. Este proceso arrojó resultados por los cuales se decidió que el CPNB utilizara el sistema desarrollado para el CICPC (SIIPOL) al cual se le realizarían determinadas personalizaciones y ampliaciones solicitadas por el cliente. El proyecto siguió las directivas en uso del CICPC acoplándose tanto las funcionalidades como el equipo de desarrollo seleccionado.

Proyecto SIGEPOL[13]

El nombre del sistema y el proyecto es Sistema de Gestión Policial (SIGEPOL), que responde a las necesidades del Viceministerio del Sistema Integrado de Policía (VISIPOL) de la República Bolivariana de Venezuela. Su propósito es apoyar los procesos de la institución para la cual fue creado. Abarca las tres direcciones generales del viceministerio, así como otras de apoyo a las actividades diarias que se realizan en la institución. El producto es una aplicación Web a la medida desarrollada en la plataforma Java, compatible con el navegador Mozilla Firefox versión 3.5.0 o superior. Se utiliza además el gestor de base de datos Oracle EE 10g release 2. Cuenta con 245 CU siguiendo la metodología de desarrollo de software RUP. El equipo de desarrollo es relativamente pequeño, incluye 9 especialistas y 7 estudiantes.

Proyecto AuditBD[14]

El proyecto Herramienta de Auditorías a Bases de Datos y Sistemas Operativos (AuditBD) tiene como cliente a la Empresa de Telecomunicaciones de Cuba S.A (ETECSA) a partir de una necesidad surgida al aplicar de manera engorrosa las auditorías a las Sistemas Gestores de Bases de Datos. El proyecto tiene como objetivo proveer un sistema que permita realizar auditorías a los diversos gestores que presenta la red de telecomunicaciones de Cuba y que además permita evaluar

[13] Información obtenida a través del líder del proyecto SIGEPOL.
[14] Información obtenida a través del líder del proyecto AuditBD.

los resultados obtenidos. El sistema es Desktop y está actualmente está en desarrollo, utilizando Java como lenguaje de desarrollo, Spring Source como marco de trabajo y Postgres 9.1 como gestor de base de datos. El proyecto cuenta con 35 CU siguiendo la metodología RUP. El equipo de trabajo está compuesto por 6 especialistas y 11 estudiantes.

Resultados del Diagnóstico SCAMPI B

Se aplicó SCAMPI a 4 proyectos de la Facultad 2, antes caracterizados, siguiendo lo definido en su guía y bajo la planificación mostrada en el epígrafe Método Estándar de Evaluación CMMI SCAMPI. La documentación de gestión de los proyectos antes mencionados fue analizada y se entrevistaron a sus líderes de proyecto y analistas. Según los resultados del diagnóstico realizado utilizando SCAMPI, se determinó que el PA se encuentra No Satisfecha, hay debilidades significativas en la implantación e institucionalización y no existe una alternativa adecuada.

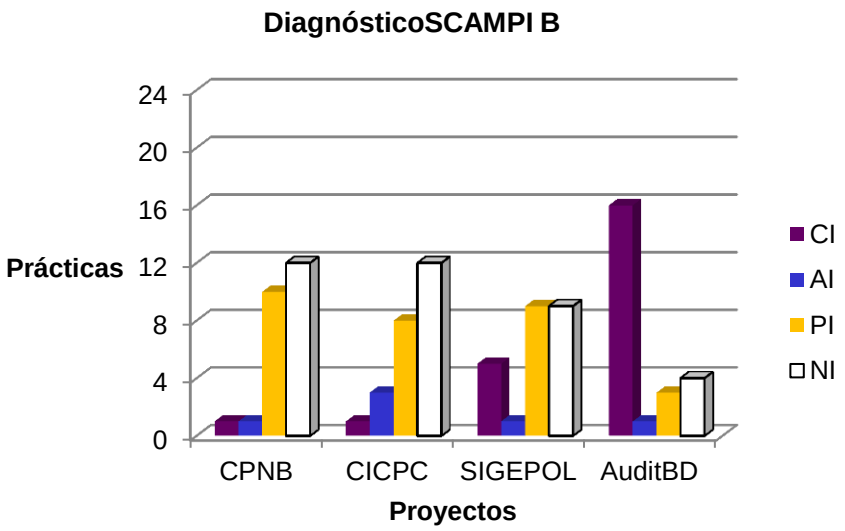


Gráfico 7. Resultados del diagnóstico SCAMPI a proyectos de la Facultad 2.

El diagnóstico con SCAMPI arrojó un conjunto de debilidades y fortalezas comunes o no en los proyectos analizados. Las debilidades encontradas determinan las acciones a realizar para elevar el nivel de capacidad del proceso de GR. Conocer qué práctica no se realiza o se realiza parcialmente indica en qué hay que trabajar. La documentación escasa o poco fundamentada es la principal debilidad de los proyectos diagnosticados junto con el no establecimiento del proceso de GR. Las actividades que se realizan responden a las prácticas dictadas

por otras PAs de CMMI como PP y PMC. En la Tabla 11 se presentan las debilidades identificadas.

Tabla 11. Debilidades encontradas durante el diagnóstico SCAMPI B.

No.	Debilidad
1.	Se identifican las fuentes de los riesgos, generalmente de forma empírica, y basado en experiencias anteriores. Se establece una pobre categorización de los riesgos.
2.	Se define la probabilidad de ocurrencia y niveles de gravedad pero los umbrales para cada categoría son ambiguos.
3.	Se sigue una estrategia empírica para mitigar los riesgos que se identifican.
4.	Se realiza la identificación de los riesgos, pero se documenta solo parte de la actividad y los resultados.
5.	Se realiza la evaluación, categorización y priorización de los riesgos, pero su documentación es poco fundamentada.
6.	Se establecen estrategias de mitigación por cada riesgo pero no existen límites de aceptación de riesgos, todos los que se identifican son inaceptables. No se analiza la relación costo-beneficio de la mitigación de cada riesgo.
7.	Se realizan reuniones de seguimiento y monitoreo pero la documentación existente no es específica.
8.	No se realizan todas las prácticas específicas del PA RSKM de CMMI.
9.	No se establece política organizacional para la GR.
10.	Se proporcionan los recursos pero no existe documentación al respecto.
11.	Se asignan las responsabilidades relacionadas con la GR, pero la documentación es en forma de tickets automatizados.
12.	No se capacita al personal para enfrentar la GR.
13.	Solo se involucran agentes relevantes en dependencia del riesgo identificado.
14.	No se analiza la adherencia de la GR con el proceso realizado.
15.	Se analiza el estado de los riesgos con la alta dirección como parte de las reuniones de estado, pero no existe documentación específica para el proceso de GR.
16.	No está establecido el proceso de GR.
17.	No se obtienen resultados de mediciones e información de mejora.
18.	No se establecen los objetivos cuantitativos para el proceso.
19.	No se estabiliza el rendimiento del proceso.
20.	No se asegura la mejora continua del proceso.
21.	No se analizan las causas raíz de los problemas.

Las fortalezas identificadas deben utilizarse en función de minimizar y solventar completamente las debilidades del proceso de GR seguido en los proyectos. El

personal dispuesto a mejorar y seguir pautas organizativas que beneficien a la organización, contar con una cantera importante de profesionales y estudiantes para conformar y perfeccionar el trabajo en los proyectos informáticos y la práctica generalizada en la universidad de mantener un estricto control sobre los elementos de configuración, son fortalezas dignas resaltar y explotar en la organización. Las fortalezas identificadas se presentan en la Tabla 12.

Tabla 12. Fortalezas encontradas durante el diagnóstico SCAMPI B.

No.	Fortaleza
1	Personal dispuesto a mejorar y seguir pautas organizativas que beneficien a la organización.
2	Cantera importante de profesionales y estudiantes para conformar y perfeccionar el trabajo en los proyectos informáticos.
3	Vinculación docencia – producción de estudiantes, profesores y especialistas que permite perfeccionar el proceso de desarrollo de software desde las aulas.
4	Realización de las actividades de identificación, evaluación, categorización y priorización de los riesgos así como el seguimiento y control de los mismos.
5	Conocimiento de las actividades de GR generales que deben aplicarse en el proyecto.
6	Directivos de los proyectos comprometidos con la mejora del proceso de GR.
7	Oportunidades de superación profesional a partir del propio desarrollo de software.
8	Posibilidad de desarrollar software para un cliente real que reconoce y participa en el proceso.
9	Contar con productos desarrollados y desplegados, actualmente en uso.
10	Obtener resultados aún con debilidades en los procesos de GR.
11	Existe un proyecto que presenta una avanzada con respecto a los demás en cuanto al cumplimiento de las prácticas de CMMI que puede aportar su experiencia al resto de la organización.

Los pasos a seguir para superar las debilidades incluyen la implantación de un proceso de GR adecuado que cumpla con las prácticas de CMMI y otros marcos internacionales, teniendo en cuenta las normas de control interno del país y otros modelos de GR desarrollados previamente y que están acorde a las características del desarrollo de software en la UCI principalmente, pero que pueden ser aplicados al resto de las organizaciones similares en el país.

Resultados de la implantación del Proceso de GR para el Desarrollo de Aplicaciones Informáticas

El Proceso de GR para el Desarrollo de Aplicaciones Informáticas se realiza en ciclos durante todo el proceso de desarrollo de software hasta su fin. La aplicación

del mismo se llevó a cabo en los proyectos realizando un ciclo completo del proceso de GR. Se utilizó además la herramienta SIMR para utilizar la experiencia de expertos y de la organización en la identificación y mitigación de los riesgos. Se utilizaron técnicas que apoyaron el proceso de análisis de los riesgos y refinaron tanto los riesgos identificados por la herramienta como las estrategias de mitigación. Se utilizó una guía que contiene la definición del proceso de GR y los elementos a incluir en los productos de trabajo, así como la descripción de cada actividad del proceso, los roles definidos y sus responsabilidades, las posibles técnicas a utilizar y los indicadores que pueden medirse para obtener elementos que sirvan para la toma de decisiones y la mejora del proceso de GR.

Resultados de la implantación del Proceso de GR para el Desarrollo de Aplicaciones Informáticas en los Proyectos CICPC y CPNB

Los Proyectos CICPC y CPNB mantienen una misma línea de desarrollo a partir del momento en el que se decide que las necesidades de ambos clientes convergen en un producto previamente desarrollado para el CICPC. Surgen entonces riesgos de integración de ambos equipos de desarrollo y las funcionalidades particulares referentes a la misión del CPNB. Es por ello que se identificaron riesgos de integración que fueron mitigados y cerrados previos al uso del Proceso de GR para el Desarrollo de Aplicaciones Informáticas. Los resultados obtenidos a partir de los indicadores varían mínimamente dada las funcionalidades implementadas para cada proyecto.

Indicadores CPNB

Tabla 13. Indicador 1. Exposición al riesgo del proyecto o vulnerabilidad

ER	Medianamente expuesto al riesgo	
Id	**Descripción**	**Valor**
ER	Exposición al riesgo del proyecto o vulnerabilidad	0.62
T	Sumatoria de las sumatorias de las probabilidades por cada tipo de riesgo	7.3
$\mathbf{c_b}$	Índice de afectación de un riesgo bajo	0.2
$\mathbf{c_m}$	Índice de afectación de un riesgo medio	0.3
$\mathbf{c_a}$	c_a = 1: índice de afectación de un riesgo alto	1
B	Sumatoria Probabilidad de Ocurrencia Riesgos Bajos	1
M	Sumatoria Probabilidad de Ocurrencia Riesgos Medios	2.8
A	Sumatoria Probabilidad de Ocurrencia Riesgos Altos	3.5

Tabla 14. Indicador 2. Índice de Oportunidad del proyecto

IOP	Existen Oportunidades que deben aprovecharse	
Id	**Descripción**	**Valor**
IOP	Índice de Oportunidad del proyecto	0.87
T	Sumatoria de las sumatorias de las probabilidades por cada tipo de riesgo	3.1
$\mathbf{c_b}$	Índice de afectación de un riesgo positivo bajo	0.2
$\mathbf{c_m}$	Índice de afectación de un riesgo positivo medio	0.3
$\mathbf{c_a}$	c_a = 1: índice de afectación de un riesgo positivo alto	1

B	Sumatoria Probabilidad de Ocurrencia Riesgos Positivos Bajos	0.5
M	Sumatoria Probabilidad de Ocurrencia Riesgos Positivos Medios	0
A	Sumatoria Probabilidad de Ocurrencia Riesgos Positivos Altos	2.6

Tabla 15. Indicador 3. Efectividad de las respuestas ejecutadas

ERE (%)	71.43	
Id	**Descripción**	**Valor**
ERE	Porciento de efectividad de las respuestas ejecutadas	71.43
r_c	Cantidad de riesgos críticos	5
r_{cm}	Cantidad de riesgos críticos mitigados	5
c_{ra}	Cantidad de respuestas	14
c_{rae}	Cantidad de respuestas aplicadas efectivas	10

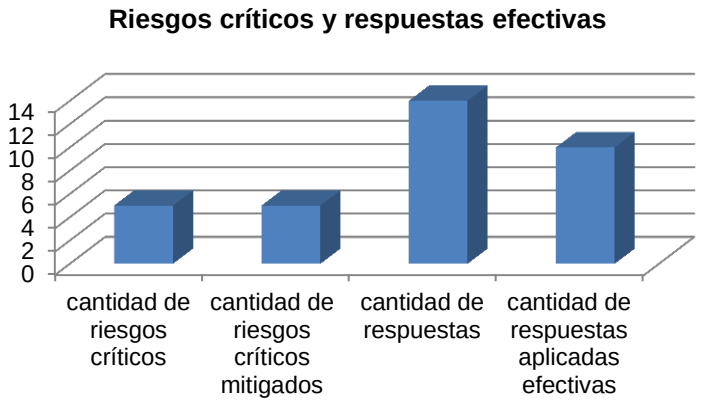


Gráfico 8. Representación de los riesgos críticos y las respuestas efectivas aplicadas.

Tabla 16. Indicador 4. Intervalo de seguimiento y control

ISC	Debe disminuir el intervalo de tiempo entre un seguimiento y otro	
Id	**Descripción**	**Valor**
ISC	Intervalo de seguimiento y control	2
T	Cantidad de días entre un seguimiento y otro (actualmente)	7
j	Ordinal del seguimiento actual	5
n	Cantidad de seguimientos utilizados para establecer la tendencia de los riesgos	4
t	Factor de variación de T, -1 < t <1	0
r_{nm}	Cantidad de riesgos no monitoreados entre en el último periodo de seguimiento	0
c	Coeficiente de severidad de la variación de T, 0 < c <1, se propone utilizar 0.5	0.5

Tabla 17. Cantidad de reuniones de seguimiento y control analizados para determinar la varianza.

	Seguimiento	Cantidad de riesgos
Actual	3	20
	2	25
	1	28

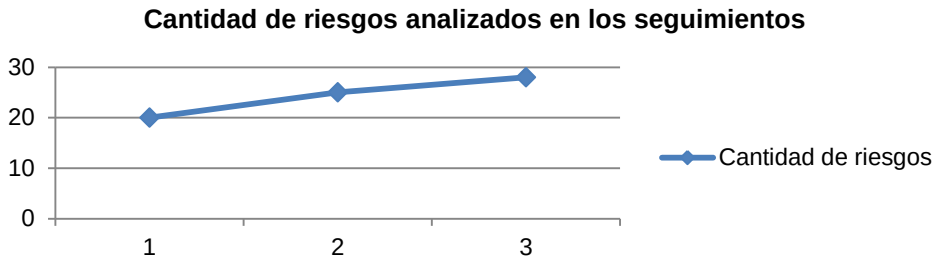


Gráfico 9. Cantidad de riesgos analizados en las reuniones de seguimiento y control que determinan la varianza.

Tabla 18. Indicador 5. Porcentaje de Esfuerzo de mitigación

PEM (%)	5.00	
Id	**Descripción**	**Valor**
PEM	Porcentaje de Esfuerzo de mitigación	5.00
EM	Esfuerzo de mitigación dado en horas/hombre	782.33
EF	Esfuerzo del proyecto dado en horas/hombre	15643.4

Tabla 19. Indicador 6. Posibilidad de interrupción del servicio

p	No existe posibilidad de interrumpir el servicio	
Id	**Descripción**	**Valor**
p	Posibilidad de interrupción del servicio	0
u	Umbral de impacto de interrupción de servicio, definido por el gestor de riesgos. Se sugiere u > 0,8.	0,8
r	Riesgos con impacto superior a 0,8.	0

Indicadores CICPC

Tabla 20. Indicador 1. Exposición al riesgo del proyecto o vulnerabilidad

ER	Medianamente expuesto al riesgo	
Id	**Descripción**	**Valor**
ER	Exposición al riesgo del proyecto o vulnerabilidad	0.50
T	Sumatoria de las sumatorias de las probabilidades por cada tipo de riesgo	6.2
c_b	Índice de afectación de un riesgo bajo	0.2
c_m	Índice de afectación de un riesgo medio	0.3
c_a	c_a = 1: índice de afectación de un riesgo alto	1
B	Sumatoria Probabilidad de Ocurrencia Riesgos Bajos	1
M	Sumatoria Probabilidad de Ocurrencia Riesgos Medios	3.3
A	Sumatoria Probabilidad de Ocurrencia Riesgos Altos	1.9

Tabla 21. Indicador 2. Índice de Oportunidad del proyecto

IOP	Existen Oportunidades que deben aprovecharse	
Id	**Descripción**	**Valor**
IOP	Índice de Oportunidad del proyecto	0.84
T	Sumatoria de las sumatorias de las probabilidades por cada tipo de riesgo	7
c_b	Índice de afectación de un riesgo positivo bajo	0.2
c_m	Índice de afectación de un riesgo positivo medio	0.3
c_a	c_a = 1: índice de afectación de un riesgo positivo alto	1
B	Sumatoria Probabilidad de Ocurrencia Riesgos Positivos Bajos	0.5
M	Sumatoria Probabilidad de Ocurrencia Riesgos Positivos Medios	1
A	Sumatoria Probabilidad de Ocurrencia Riesgos Positivos Altos	5.5

Tabla 22. Indicador 3. Efectividad de las respuestas ejecutadas

ERE (%)	71.43	
Id	**Descripción**	**Valor**
ERE	Porciento de efectividad de las respuestas ejecutadas	71.43
r_c	Cantidad de riesgos críticos	3
r_{cm}	Cantidad de riesgos críticos mitigados	3
c_{ra}	Cantidad de respuestas	14
c_{rae}	Cantidad de respuestas aplicadas efectivas	10

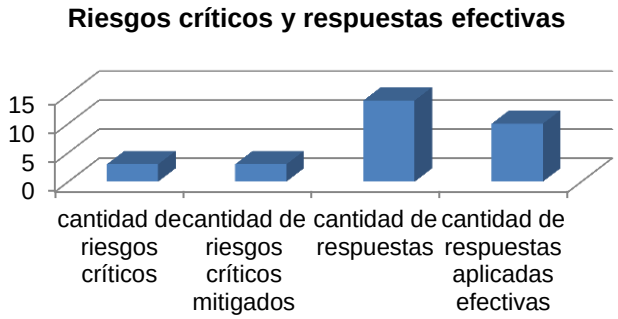


Gráfico 10. Representación de los riesgos críticos y las respuestas efectivas aplicadas.

Tabla 23. Indicador 4. Intervalo de seguimiento y control

ISC	Debe disminuir el intervalo de tiempo entre un seguimiento y otro	
Id	**Descripción**	**Valor**
ISC	Intervalo de seguimiento y control	8
T	Cantidad de días entre un seguimiento y otro (actualmente)	7
j	Ordinal del seguimiento actual	5
n	Cantidad de seguimientos utilizados para establecer la tendencia de los riesgos	4
t	Factor de variación de T, -1 < t <1	-2
r_{nm}	Cantidad de riesgos no monitoreados entre en el último periodo de seguimiento	0
c	Coeficiente de severidad de la variación de T, 0 < c <1, se propone utilizar 0.5	0.5

Tabla 24. Cantidad de reuniones de seguimiento y control analizados para determinar la varianza.

	Seguimiento	Cantidad de riesgos
	1	22
	2	25
	3	26
	4	30
Actual	5	33

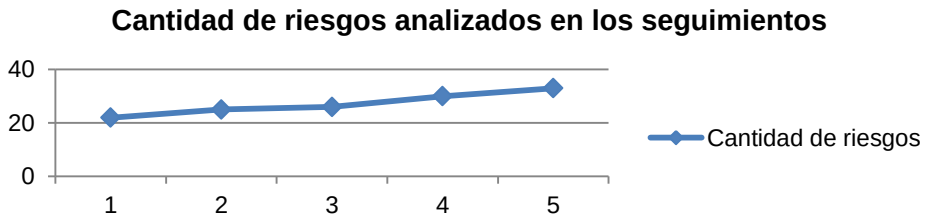


Gráfico 11. Cantidad de riesgos analizados en las reuniones de seguimiento y control que determinan la varianza.

Tabla 25. Indicador 5. Porcentaje de Esfuerzo de mitigación

PEM (%)	10.06	
Id	**Descripción**	**Valor**
PEM	Porcentaje de Esfuerzo de mitigación	10.06
EM	Esfuerzo de mitigación dado en horas/hombre	16,347
EF	Esfuerzo del proyecto dado en horas/hombre	162473.08

Tabla 26. Indicador 6. Posibilidad de interrupción del servicio

p	No existe posibilidad de interrumpir el servicio	
Id	**Descripción**	**Valor**
p	Posibilidad de interrupción del servicio	0
u	Umbral de impacto de interrupción de servicio, definido por el gestor de riesgos. Se sugiere u > 0,8.	0,8
r	Riesgos con impacto superior a 0,8.	0

Lecciones aprendidas en la implantación del Proceso de GR para el Desarrollo de Aplicaciones Informáticas en los proyectos CICPC y CPNB

- La incidencia de las acciones del proceso permite refinar las actividades del mismo y sus indicadores.
- La integración entre 2 sistemas representa una oportunidad de negocio para las 2 instituciones.
- La definición de las unidades de dominio, responde a una agrupación de actividades, condiciones de personal, situación geográfica y no solamente a la disciplina principal que las determina.
- El conocimiento del proceso de GR de los integrantes del proyecto aumenta la efectividad de las respuestas de mitigación o contingencia.
- Las responsabilidades de los roles de GR deben asignarse a una persona que no tenga otras tareas dentro del proyecto.
- Las reuniones de seguimiento y control con la participación de todos los roles fundamentales del proyecto aportando ideas con respecto a la mitigación de riesgos y la identificación de otros nuevos, enriquece el proceso de GR.
- Las reuniones de control diarias del proyecto son una fuente importante para identificar los riesgos y acciones de mitigación que puede provocar las interacciones del personal del proyecto entre sí mismos y con el cliente.

Resultados de la implantación del Proceso de GR para el Desarrollo de Aplicaciones Informáticas en el Proyecto SIGEPOL

El proyecto SIGEPOL aplicó un ciclo del Proceso de GR para el Desarrollo de Aplicaciones Informáticas y utilizó riesgos identificados previos a la

institucionalización del proceso en el proyecto para gestionarlos con la nueva estrategia propuesta.

Indicadores

Tabla 27. Indicador 1. Exposición al riesgo del proyecto o vulnerabilidad

ER	Medianamente expuesto al riesgo	
Id	**Descripción**	**Valor**
ER	Exposición al riesgo del proyecto o vulnerabilidad	0.45
T	Sumatoria de las sumatorias de las probabilidades por cada tipo de riesgo	5.7
c_b	Índice de afectación de un riesgo bajo	0.2
c_m	Índice de afectación de un riesgo medio	0.3
c_a	c_a = 1: índice de afectación de un riesgo alto	1
B	Sumatoria Probabilidad de Ocurrencia Riesgos Bajos	1
M	Sumatoria Probabilidad de Ocurrencia Riesgos Medios	3.3
A	Sumatoria Probabilidad de Ocurrencia Riesgos Altos	1.4

Tabla 28. Indicador 2. Índice de Oportunidad del proyecto

IOP	Existen Oportunidades que deben aprovecharse	
Id	**Descripción**	**Valor**
IOP	Índice de Oportunidad del proyecto	0.77
T	Sumatoria de las sumatorias de las probabilidades por cada tipo de riesgo	2.6
c_b	Índice de afectación de un riesgo positivo bajo	0.2
c_m	Índice de afectación de un riesgo positivo medio	0.3
c_a	c_a = 1: índice de afectación de un riesgo positivo alto	1
B	Sumatoria Probabilidad de Ocurrencia Riesgos Positivos Bajos	0.5
M	Sumatoria Probabilidad de Ocurrencia Riesgos Positivos Medios	0.3
A	Sumatoria Probabilidad de Ocurrencia Riesgos Positivos Altos	1.8

Tabla 29. Indicador 3. Efectividad de las respuestas ejecutadas

ERE (%)	69.23	
Id	**Descripción**	**Valor**
ERE	Porciento de efectividad de las respuestas ejecutadas	69.23
r_c	Cantidad de riesgos críticos	2
r_{cm}	Cantidad de riesgos críticos mitigados	1
c_{ra}	Cantidad de respuestas	13
c_{rae}	Cantidad de respuestas aplicadas efectivas	9

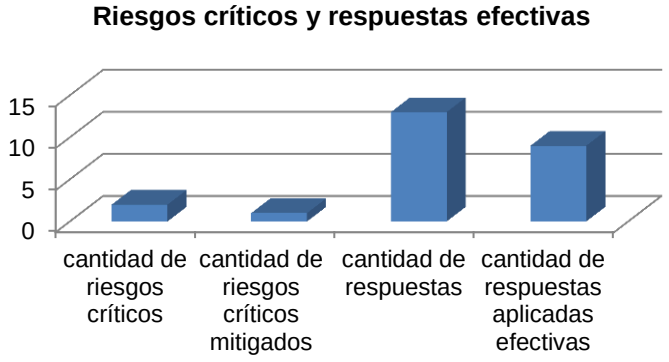


Gráfico 12. Representación de los riesgos críticos y las respuestas efectivas aplicadas.

Tabla 30. Indicador 4. Intervalo de seguimiento y control

ISC	Puede aumentar el intervalo de tiempo entre un seguimiento y otro y liberar recursos	
Id	**Descripción**	**Valor**
ISC	Intervalo de seguimiento y control	-4
T	Cantidad de días entre un seguimiento y otro (actualmente)	7
j	Ordinal del seguimiento actual	5
n	Cantidad de seguimientos utilizados para establecer la tendencia de los riesgos	4
t	Factor de variación de T, -1 < t <1	2
r_{nm}	Cantidad de riesgos no monitoreados entre en el último periodo de seguimiento	0
c	Coeficiente de severidad de la variación de T, 0 < c <1, se propone utilizar 0.5	0.5

Tabla 31. Cantidad de reuniones de seguimiento y control analizados para determinar la varianza

	Seguimiento	Cantidad de riesgos
	1	31
	2	24
Actual	3	20

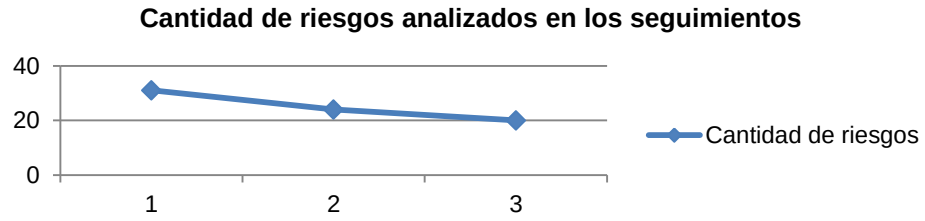


Gráfico 13. Cantidad de riesgos analizados en las reuniones de seguimiento y control que determinan la varianza.

Tabla 32. Indicador 5. Porcentaje de Esfuerzo de mitigación

PEM (%)	33.33	
Id	**Descripción**	**Valor**
PEM	Porcentaje de Esfuerzo de mitigación	33.33
EM	Esfuerzo de mitigación dado en horas/hombre	19232.89
EF	Esfuerzo del proyecto dado en horas/hombre	57698.68

Tabla 33. Indicador 6. Posibilidad de interrupción del servicio

p	No existe posibilidad de interrumpir el servicio	
Id	**Descripción**	**Valor**
p	Posibilidad de interrupción del servicio	0
u	Umbral de impacto de interrupción de servicio, definido por el gestor de riesgos. Se sugiere u > 0,8.	0,8
r	Riesgos con impacto superior a 0,8.	0

Lecciones aprendidas en la implantación del Proceso de GR para el Desarrollo de Aplicaciones Informáticas en el Proyecto SIGEPOL

- El proceso permite hacer un seguimiento de los riesgos en función del impacto que tiene en el proyecto.

- Deja constancia de la respuesta al riesgo con el objetivo de mitigarlo, lo que permite definir una estrategia para riesgos parecidos o con impacto similar en una fase futura del proyecto, por ejemplo en una nueva versión o actualización del mismo.
- Garantiza que la estimación del impacto del riesgo no sea de forma empírica como se realizaba antes.
- Con los indicadores propuestos se realizan análisis de GR que tributan a una gestión de proyecto más eficiente.
- La efectividad de las respuestas ejecutadas puede elevarse teniendo en cuenta el esfuerzo que se está dedicando a la mitigación para lo cual se debe realizar un análisis y determinar qué puede estar afectando este indicador para solucionar el problema.

Resultados de la implantación del Proceso de GR para el Desarrollo de Aplicaciones Informáticas en el Proyecto AuditBD

El proyecto AuditBD utiliza la Plantilla Planes y Registro de Monitoreo y aplicó un ciclo del proceso de GR utilizando riesgos identificados previos a la implantación del proceso en el proyecto para gestionarlos con la nueva estrategia propuesta.

Indicadores

Tabla 34. Indicador 1. Exposición al riesgo del proyecto o vulnerabilidad

ER	Completamente expuesto al riesgo	
Id	**Descripción**	**Valor**
ER	Exposición al riesgo del proyecto o vulnerabilidad	1,00
T	Sumatoria de las sumatorias de las probabilidades por cada tipo de riesgo	11,4
c_b	Índice de afectación de un riesgo bajo	0,2
c_m	Índice de afectación de un riesgo medio	0,3
c_a	c_a = 1: índice de afectación de un riesgo alto	1
B	Sumatoria Probabilidad de Ocurrencia Riesgos Bajos	0
M	Sumatoria Probabilidad de Ocurrencia Riesgos Medios	0
A	Sumatoria Probabilidad de Ocurrencia Riesgos Altos	11,4

Tabla 35. Indicador 2. Índice de Oportunidad del proyecto

IOP	No tiene Oportunidades identificadas	
Id	**Descripción**	**Valor**
IOP	Índice de Oportunidad del proyecto	0,0
T	Sumatoria de las sumatorias de las probabilidades por cada tipo de riesgo	0
c_b	Índice de afectación de un riesgo positivo bajo	0,2
c_m	Índice de afectación de un riesgo positivo medio	0,3
c_a	c_a = 1: índice de afectación de un riesgo positivo alto	1
B	Sumatoria Probabilidad de Ocurrencia Riesgos Positivos Bajos	0
M	Sumatoria Probabilidad de Ocurrencia Riesgos Positivos Medios	0
A	Sumatoria Probabilidad de Ocurrencia Riesgos Positivos Altos	0

Tabla 36. Indicador 3. Efectividad de las respuestas ejecutadas

ERE (%)	71,43	
Id	**Descripción**	**Valor**
ERE	Porciento de efectividad de las respuestas ejecutadas	71,43
r_c	Cantidad de riesgos críticos	14
r_{cm}	Cantidad de riesgos críticos mitigados	7
c_{ra}	Cantidad de respuestas	7
c_{rae}	Cantidad de respuestas aplicadas efectivas	5

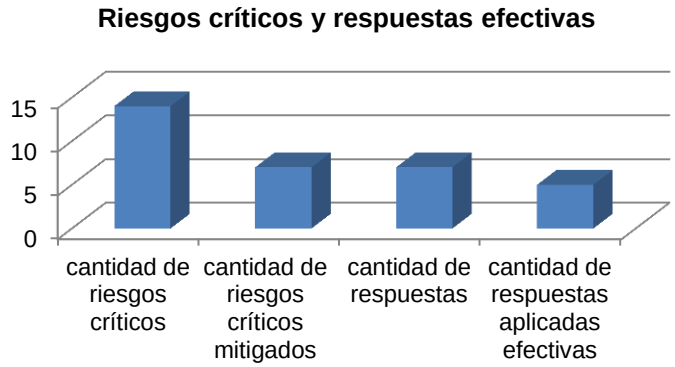


Gráfico 14. Representación de los riesgos críticos y las respuestas efectivas aplicadas.

Tabla 37. Indicador 4. Intervalo de seguimiento y control

ISC	Debe disminuir el intervalo de tiempo entre un seguimiento y otro	
Id	**Descripción**	**Valor**
ISC	Intervalo de seguimiento y control	2
T	Cantidad de días entre un seguimiento y otro (actualmente)	7
j	Ordinal del seguimiento actual	5
n	Cantidad de seguimientos utilizados para establecer la tendencia de los riesgos	4
t	Factor de variación de T, -1 < t <1	0
rnm	Cantidad de riesgos no monitoreados entre en el último periodo de seguimiento	0
c	Coeficiente de severidad de la variación de T, 0 < c <1, se propone utilizar 0.5	0,5

Tabla 38. Cantidad de reuniones de seguimiento y control analizados para determinar la varianza

	Seguimiento	Cantidad de riesgos
	1	12
	2	14
Actual	3	15

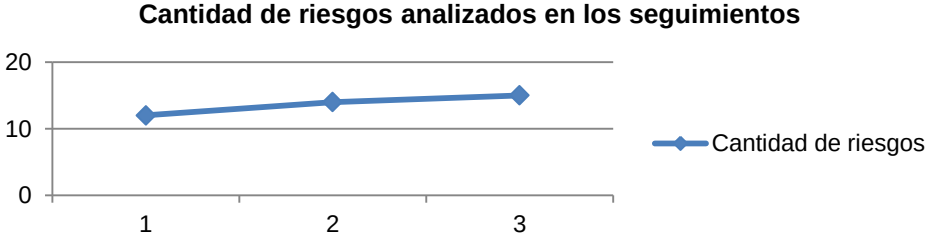


Gráfico 15. Cantidad de riesgos analizados en las reuniones de seguimiento y control que determinan la varianza.

Tabla 39. Indicador 5. Porcentaje de Esfuerzo de mitigación

PEM (%)	33,33	
Id	**Descripción**	**Valor**
PEM	Porcentaje de Esfuerzo de mitigación	33,33
EM	Esfuerzo de mitigación dado en horas/hombre	19232,89
EF	Esfuerzo del proyecto dado en horas/hombre	57698,68

Tabla 40. Indicador 6. Posibilidad de interrupción del servicio

p	No existe posibilidad de interrumpir el servicio	
Id	**Descripción**	**Valor**
p	Posibilidad de interrupción del servicio	0
u	Umbral de impacto de interrupción de servicio, definido por el gestor de riesgos. Se sugiere u > 0,8.	0,8
r	Riesgos con impacto superior a 0,8.	0

Lecciones aprendidas en la implantación del Proceso de GR para el Desarrollo de Aplicaciones Informáticas en el Proyecto AuditBD

- El uso de la técnica de Clasificación de la Causa Raíz permitió refinar las estrategias de mitigación propuestas, por lo cual se recomienda para analizar la mitigación de los riesgos por identificar.
- Durante el ciclo del proceso de GR aplicado no se identificaron oportunidades, de acuerdo con la etapa en que se encuentra el proyecto, pero el producto puede presentar oportunidades de negocio que no deben dejar de identificarse en etapas posteriores, por lo cual debe seguirse el Indicador Índice de Oportunidad del proyecto.
- Establecer como práctica en el seguimiento y control el análisis de los indicadores calculados a partir de la identificación y mitigación de riesgos realizada.
- Seguir los resultados de los indicadores Efectividad de las respuestas ejecutadas, Intervalo de seguimiento y control y Porcentaje de Esfuerzo de mitigación, porque juntos permiten determinar si se están ejecutando idóneamente las actividades de mitigación.

Evaluación a través SCAMPI B de la implantación del Proceso de GR para el Desarrollo de Aplicaciones Informáticas

La aplicación de SCAMPI B a modo de evaluación una vez se empleó un ciclo del proceso de GR propuesto, permitió comprobar que la realización de las actividades y la obtención de los productos de trabajo utilizando las técnicas indicadas, es un primer paso de avance para alcanzar un nivel de capacidad superior en el PA de RSKM. Es necesario lograr la implicación de todos los niveles directivos con el fin de institucionalizar el proceso y obtener resultados más reales y factibles que permitan la mejora continua del proceso de GR. El Gráfico 16 muestra la completitud de la implementación de las prácticas de CMMI utilizando como guía

el proceso propuesto. El mayor porciento de prácticas son implementadas en su totalidad, mientras que solo 2 se observan altamente implementadas, no existiendo ninguna poco implementada o no implementada. Según los resultados de la evaluación realizada utilizando SCAMPI, se determinó que el nivel de capacidad 5 del PA RSKM se encuentra Satisfecha, las prácticas están institucionalizadas e implantadas de acuerdo con CMMI y mediante una alternativa adecuada.

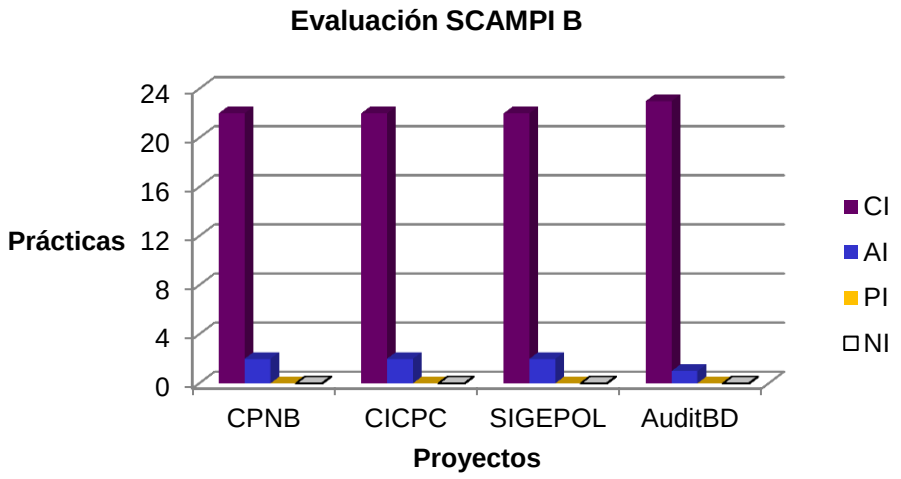


Gráfico 16. Resultados de la evaluación SCAMPI a proyectos de la Facultad 2.

A continuación se presentan en las tablas 41 - 48 los resultados de la evaluación utilizando SCAMPI en cada proyecto ilustrando la implementación de las prácticas genéricas (GG) y específicas (SP) de PA RSKM de CMMI, antes y después de aplicar el Proceso de GR para el Desarrollo de Aplicaciones Informáticas.

1. Proyecto CPNB

Antes:

Tabla 41. Diagnóstico de GR al Proyecto CPNB utilizando SCAMPI B.

AP	Metas	Prácticas									
RSKM	SG1	SP1.1	SP1.2	SP1.3							
		PI	PI	PI							
	SG2	SP2.1	SP2.2								
		PI	PI								
	SG3	SP3.1	SP3.2								
		PI	NI								
	GG1	GP1.1									
	GG2	GP2.1	GP2.2	GP2.3	GP2.4	GP2.5	GP2.6	GP2.7	GP2.8	GP2.9	GP2.10
		NI	NI	NI	PI	PI	NI	CI	PI	PI	NI
	GG 3	GP3.1	GP3.2								
		AI	NI								
	GG 4	GP4.1	GP4.2								
		AI	NI								
	GG 5	GP5.1	GP5.2								
		AI	NI								

Después:

Tabla 42. Evaluación de GR al Proyecto CPNB utilizando SCAMPI B.

AP	Metas	Prácticas									
RSKM	SG1	SP1.1	SP1.2	SP1.3							
		CI	CI	CI							
	SG2	SP2.1	SP2.2								
		CI	CI								
	SG3	SP3.1	SP3.2								
		CI	CI								
	GG1	GP1.1									
	GG2	GP2.1	GP2.2	GP2.3	GP2.4	GP2.5	GP2.6	GP2.7	GP2.8	GP2.9	GP2.10
		CI	AI	CI	CI	CI	AI	CI	CI	CI	CI
	GG 3	GP3.1	GP3.2								
		CI	CI								
	GG 4	GP4.1	GP4.2								
		CI	CI								
	GG 5	GP5.1	GP5.2								
		CI	CI								

2. Proyecto CICPC

Antes:

Tabla 43. Diagnóstico de GR al Proyecto CICPC utilizando SCAMPI B.

AP	Metas	Prácticas									
RSKM	SG1	SP1.1	SP1.2	SP1.3							
		PI	PI	PI							
	SG2	SP2.1	SP2.2								
		AI	PI								
	SG3	SP3.1	SP3.2								
		PI	NI								
	GG1	GP1.1									
	GG2	GP2.1	GP2.2	GP2.3	GP2.4	GP2.5	GP2.6	GP2.7	GP2.8	GP2.9	GP2.10
		NI	NI	NI	PI	PI	NI	CI	PI	AI	NI
	GG 3	GP3.1	GP3.2								
		AI	NI								
	GG 4	GP4.1	GP4.2								
		AI	NI								
	GG 5	GP5.1	GP5.2								
		AI	NI								

Después:

Tabla 44. Evaluación de GR al Proyecto CICPC utilizando SCAMPI B.

AP	Metas	Prácticas									
RSKM	SG1	SP1.1	SP1.2	SP1.3							
		CI	CI	CI							
	SG2	SP2.1	SP2.2								
		CI	CI								
	SG3	SP3.1	SP3.2								
		CI	CI								
	GG1	GP1.1									
	GG2	GP2.1	GP2.2	GP2.3	GP2.4	GP2.5	GP2.6	GP2.7	GP2.8	GP2.9	GP2.10
		CI	AI	CI	CI	CI	AI	CI	CI	CI	CI
	GG 3	GP3.1	GP3.2								
		CI	CI								
	GG 4	GP4.1	GP4.2								
		CI	CI								
	GG 5	GP5.1	GP5.2								
		CI	CI								

3. *Proyecto SIGEPOL*

Antes:

Tabla 45. Diagnóstico de GR al Proyecto SIGEPOL utilizando SCAMPI B.

AP	Metas	Prácticas									
RSKM	SG1	SP1.1	SP1.2	SP1.3							
		CI	PI	CI							
	SG2	SP2.1	SP2.2								
		CI	PI								
	SG3	SP3.1	SP3.2								
		AI	NI								
	GG1	GP1.1									
	GG2	GP2.1	GP2.2	GP2.3	GP2.4	GP2.5	GP2.6	GP2.7	GP2.8	GP2.9	GP2.10
		NI	CI	CI	PI	PI	PI	NI	PI	PI	PI
	GG 3	GP3.1	GP3.2								
		PI	NI								
	GG 4	GP4.1	GP4.2								
		PI	NI								
	GG 5	GP5.1	GP5.2								
		PI	NI								

Después:

Tabla 46. Evaluación de GR al Proyecto SIGEPOL utilizando SCAMPI B.

AP	Metas	Prácticas									
RSKM	SG1	SP1.1	SP1.2	SP1.3							
		CI	CI	CI							
	SG2	SP2.1	SP2.2								
		CI	CI								
	SG3	SP3.1	SP3.2								
		CI	CI								
	GG1	GP1.1									
	GG2	GP2.1	GP2.2	GP2.3	GP2.4	GP2.5	GP2.6	GP2.7	GP2.8	GP2.9	GP2.10
		CI	AI	CI	CI	CI	AI	CI	CI	CI	CI
	GG 3	GP3.1	GP3.2								
		CI	CI								
	GG 4	GP4.1	GP4.2								
		CI	CI								
	GG 5	GP5.1	GP5.2								
		CI	CI								

4. *Proyecto AuditBD*

Antes:

Tabla 47. Diagnóstico de GR al Proyecto AuditBD utilizando SCAMPI B.

AP	Metas	Prácticas									
RSKM	SG1	SP1.1	SP1.2	SP1.3							
		CI	CI	AI							
	SG2	SP2.1	SP2.2								
		CI	CI								
	SG3	SP3.1	SP3.2								
		CI	CI								
	GG1	GP1.1									
	GG2	GP2.1	GP2.2	GP2.3	GP2.4	GP2.5	GP2.6	GP2.7	GP2.8	GP2.9	GP2.10
		CI	CI	CI	CI	CI	PI	CI	CI	CI	CI
	GG 3	GP3.1	GP3.2								
		CI	PI								
	GG 4	GP4.1	GP4.2								
		CI	PI								
	GG 5	GP5.1	GP5.2								
		CI	PI								

Después:

Tabla 48. Evaluación de GR al Proyecto AuditBD utilizando SCAMPI B.

AP	Metas	Prácticas									
RSKM	SG1	SP1.1	SP1.2	SP1.3							
		CI	CI	CI							
	SG2	SP2.1	SP2.2								
		CI	CI								
	SG3	SP3.1	SP3.2								
		CI	CI								
	GG1	GP1.1									
	GG2	GP2.1	GP2.2	GP2.3	GP2.4	GP2.5	GP2.6	GP2.7	GP2.8	GP2.9	GP2.10
		CI	CI	CI	CI	CI	AI	CI	CI	CI	CI
	GG 3	GP3.1	GP3.2								
		CI	CI								
	GG 4	GP4.1	GP4.2								
		CI	CI								
	GG 5	GP5.1	GP5.2								
		CI	CI								

Observaciones de la aplicación de SCAMPI B

- Se utilizó el proceso de GR para el Desarrollo de Aplicaciones Informáticas como estrategia de GR del proyecto, que cumple con lo establecido en el área de proceso RSKM y las metas genéricas GG 1, GG 2, GG 3, GG 4 y GG 5 de obligatorio cumplimiento para el nivel de capacidad 5 de CMMI.
- Se asignaron los roles de GR y los recursos necesarios para mitigar los riesgos.
- La capacitación del personal es aún una práctica incompleta dado que los proyectos incluyeron estos conocimientos en el Plan de Capacitación pero no se evidenció la aplicación del mismo en sus actividades.
- Como salida de las actividades se obtuvieron productos de trabajo sencillos de utilizar durante todas las etapas del proyecto.
- Se utilizó una herramienta inteligente que apoya las actividades de identificación y mitigación de riesgos, teniendo en cuenta la experiencia acumulada en la organización.
- La inclusión del análisis de oportunidades a partir de la identificación de riesgos positivos incrementó las posibilidades de las organizaciones de encontrar nuevos negocios.
- Se utilizaron técnicas que apoyan las actividades del proceso relacionadas con la identificación filtrando los resultados obtenidos por la herramienta para lograr una mayor particularidad de los riesgos identificados.

- La información resultado del análisis de los indicadores permitió tomar decisiones que influyeron positivamente en la mejora del proceso de GR.

Conclusiones Parciales

Se caracterizó SCAMPI y se aplicó a modo de diagnóstico a los proyectos CICPC, CPNB, SIGEPOL y AuditBD estableciendo una base del estado de los proyectos antes de implantar el Proceso de GR para el Desarrollo de Aplicaciones Informáticas definido. Se muestran los resultados de la implantación del Proceso de GR para el Desarrollo de Aplicaciones Informáticas, obtenidos a través de indicadores y lecciones aprendidas. La evaluación realizada utilizando SCAMPI B permitió analizar cómo al ejecutar las actividades propuestas los proyectos tenían un elevado cumplimiento de las GG y SP relacionadas con el PA RSKM de CMMI. Los proyectos pudieron utilizar la información ofrecida por el propio proceso de GR para moldearlo de manera tal que el tratamiento a los riesgos fue proactivo y se tomaron decisiones acertadas.

Conclusiones

La investigación concluye que la implantación del Proceso de GR para el Desarrollo de Aplicaciones Informáticas definido constituye un paso de avance significativo para elevar el nivel de capacidad de la GR en la UCI al nivel 5 de CMMI, considerando los siguientes resultados alcanzados:

- A partir del estudio de los fundamentos teóricos de la GR se determinó que los marcos analizados no constituyen una estrategia a seguir dadas las características de la universidad.
- Se elaboró un Proceso de GR para el Desarrollo de Aplicaciones Informáticas que cumple con las GG y SP del nivel de capacidad 5 del PA RSKM de CMMI, definiendo actividades, roles, responsabilidades, productos de trabajo, indicadores y técnicas. El proceso incluye el uso de SIMR, para utilizar la experiencia de la organización en la identificación y mitigación de los riesgos.
- Se analizaron técnicas de IA vinculadas a la GR y se determinó la aplicación de los Sistemas Basados en Casos para utilizar la experiencia acumulada de la organización en la identificación y mitigación de riesgos.
- Se aplicó el Proceso de GR para el Desarrollo de Aplicaciones Informáticas propuesto obteniendo los artefactos definidos, a través del uso de técnicas, herramientas e indicadores que aportaron información relevante para la toma de decisiones relacionadas con la GR y la mejora de la capacidad del proceso de GR.
- Se utilizó SCAMPI B como método para diagnosticar y evaluar el estado de la GR en los proyectos, que permitió corroborar que luego de la implantación del Proceso de GR para el Desarrollo de Aplicaciones Informáticas en los proyectos aumentó en los mismos la implementación de las GG y SP relacionadas con el PA RSKM de CMMI.
- El diseño del Proceso de GR para el Desarrollo de Aplicaciones Informáticas y su posterior implantación en 4 proyectos de 2 centros de desarrollo de la UCI permitió comprobar que los mismos obtuvieron resultados que apoyaron la toma de decisiones relacionadas con la GR.

Recomendaciones

Se recomienda:

- Institucionalizar el Proceso de GR para el Desarrollo de Aplicaciones Informáticas definido para alcanzar el nivel de capacidad 5 en el PA RSKM de CMMI y contribuir a la mejora continua del proceso de GR.
- Integrar el Proceso de GR para el Desarrollo de Aplicaciones Informáticas en el Modelo Cubano para el Desarrollo de Aplicaciones Informáticas.
- Incluir en el Expediente de Proyecto de la UCI los artefactos y roles resultantes del Proceso de GR para el Desarrollo de Aplicaciones Informáticas.
- Recomendar la implantación del Proceso de GR para el Desarrollo de Aplicaciones Informáticas a otras empresas de desarrollo de software cubanas.

Referencias Bibliográficas

ACC. 2009. Technical Risk Identification and Mitigation System (TRIMS). *Acquisition Community Connection.* [Online] 2012. https://acc.dau.mil/CommunityBrowser.aspx?id=19151. ID: 19151.

—. 2005. WelcomRisk. *Acquisition Community Connection.* [Online] 2012. https://acc.dau.mil/CommunityBrowser.aspx?id=19170. ID: 19170.

Active Risk. 2012. Active Risk Manager (ARM): The Technology Behind Leading Edge Risk Management. *Active Risk Solutions.* [Online] 2012. http://www.activerisk.com/solutions/active-risk-manager-arm/.

Aguirre, Ana Paulina. 2010. Historia de la Inteligencia Artificial. *Ingeniería y Ciencia by Suite 101.* [Online] 2012. http://suite101.net/article/historia-de-la-inteligencia-artificial-a25035.

Alberts, Christopher J. 2006. Common Elements of Risk. Pittsburgh : Carnegie Mellon University, 2006. CMU/SEI-2006-TN-014.

Altiparmak, Fulya , et al. 2009. A steady-state genetic algorithm for multi-product supply chain network design. *Computers & Industrial Engineering.* 2009, Vol. 56, 2, pp. 521–537.

Álvarez, Eylena. 2011. Procedimiento para la Gestión de Riesgos en el Proyecto Minería. *UCI | Dirección de Información.* [Online] 2012. http://catalogoenlinea.uci.cu/cgi-bin/koha/opac-detail.pl?biblionumber=10768.

Anthony, Martin and Bartlett, Peter L. 2009. *Neural Network Learning: Theoretical Foundations.* New York : Cambridge University Press, 2009. ISBN: 978-0-521-57353-5.

Argemí, José Antonio Mañas. 2002. CHINCHON Versión 1.3. *CriptoRed.* [Online] 2012. http://www.criptored.upm.es/software/sw_m214_01.htm.

Bannerman, Paul L. 2008. Risk and risk management in software projects: A reassessment. *Journal of Systems and Software.* 2008, Vol. 8, 12, págs. 2118–2133.

Basogain, Xavier. 2008. Redes Neuronales Artificiales y sus aplicaciones. *OpenCourseWare.* [Online] 2012. http://ocw.ehu.es/ensenanzas-tecnicas/redes-neuronales-artificiales-y-sus-aplicaciones/contenidos/pdf/libro-del-curso.

Boehm, B. 1988. A Spiral Model of Software Development and Enhancement. *Computer.* s.l. : IEEE Computer Society, 1988. Vol. 21, 5, pp. 61-72. ISSN: 0018-9162.

Boehm, B. and DeMarco, T. 1997. Software Risk Management. *IEEE Software.* 1997. Vol. 14, 3, pp. 17-19. ISSN: 0740-7459.

Boehm, B. 1991. Software risk management: principles and practices. *IEEE Software.* Arlington : s.n., 1991. Vol. 8, 1, pp. 32 - 41. ISSN: 0740-7459.

Boehm, B., Jo, Ann Lane and Koolmanojwong, Supannika. 2010. *A Risk-Driven Decision Table for Software Process Selection.* California : University of Southern California, Center for Systems and Software Engineering (USC-CSSE), 2010.

Boehm, B., et al. 1998. Using the WinWin spiral model: a case study. *Computer.* Los Ángeles : s.n., 1998. Vol. 31, 7, págs. 33-44. ISSN: 0018-9162.

Cancelado, Alberto. 2006. *Sistema de administración de riesgos en tecnología informática.* s.l. : IBM Business Global Services, 2006. http://www.um.edu.ar/catedras/claroline/backends/download.php?url=L0xpYy5fUm9sYW5kb19Db25kZS8yLjBfcmllc2dvc2luZm9yLnJ0Zg%3D%3D&cidReset=true&cidReq=II020.

CGR. 2011. Resolución No. 60/11. [ed.] Contraloría General de la República. *Gaceta Oficial de la República de Cuba.* La Habana : Ministerio de Justicia, 2011. No. 013 Extraordinaria. ISSN 1682-7511.

Chang, Pei-Chann, Liu, Chen-Hao and Lai, Robert K. 2008. A fuzzy case-basedreasoning model for sales forecasting in print circuit board industries. *Expert Systems with Applications.* 2008, Vol. 34, 3, pp. 2049–2058.

Charette, Robert N. 1989. Software Engineering Risk Analysis and Management. *IEEE Software.* s.l. : McGraw-Hill, 1989. Digitalizado en 2009. ISSN: 0070106614.

CIAO. 2000. Practices for Securing Critical Information Assets. *NCJRS.* [Online] 2012. http://www.ncjrs.gov/App/publications/abstract.aspx?ID=189897.

Cortez, Augusto, Navarro, Carlos and Pariona, Jaime. 2010. Sistemas de razonamiento basado en casos aplicado a sistemas de líneas de productos software. *Revista de investigación de sistemas e informática, Facultad de Ingeniería de Sistemas e Informática (RISI), Universidad Nacional Mayor de San Marcos.* 2010, Vol. 7, 2. http://sisbib.unmsm.edu.pe/bibvirtual/publicaciones/risi/2010_n2/v7n2/a05v7n2.pdf.

COTECNA. 2011. SIAR® - Sistema Inteligente de Administración de Riesgo. *COTECNA.com.* [Online] 2012. http://www.cotecna.com/es-ES/News-and-Media/Glossary/CRMS.

CRAMM. 2003. *CCTA Risk Analysis and Management Method User Guide version 5.0.* s.l. : Siemens, 2003.

Cunningham, P. 2009. A Taxonomy of Similarity Mechanisms for Case-Based Reasoning. *Knowledge and Data Engineering, IEEE Transactions on.* 2009, Vol. 21, 11, pp. 1532-1543 .

DACS. 2012. Software Acquisition Gold Practices. Formal Risk Management. *GoldPractice.* [Online] 2012. https://goldpractice.thecsiac.com/practices/frm/.

del Toro, José Carlos, et al. 2005. Control Interno. II Programa de preparación económica para cuadros. *CSIAC.* [Online] 2005. www.sld.cu/galerias/doc/sitios/infodir/ci_mes.doc. ISBN: 959-7185-04-0.

Doherty N., K., M. 2001. An investigation of the factors affecting the successful treatment of organizational issues in systems development projects. *European Journal of Information Systems.* 2001, Vol. 10, 3, pp. 147-160(14).

Dorigo, Marco and Stützle, Thomas . 2010. Ant Colony Optimization: Overview and Recent Advances. *International Series in Operations Research & Management Science.* 2010, Vol. 146, pp. 227-263.

Escobar, Mercedes. 2009. Aplicación y Mejora del Modelo de Gestión de Riesgos MoGeRi en el proyecto productivo Sistema de Facturación y Cobro para la Empresa de Gas Manufacturado. *UCI | Dirección de Información.* [Online] 2012. http://catalogoenlinea.uci.cu/cgi-bin/koha/opac-detail.pl?biblionumber=8282. http://catalogoenlinea.uci.cu/cgi-bin/koha/opac-detail.pl?biblionumber=8282.

Estéves J., Pastor J. A. 2005. Implementación y Mejora del Método de Gestión Riesgos del SEI en un proyecto universitario de desarrollo de software. *IEEE Latin America Transactions.* 2005, Vol. 3, 1.

Expósito, María del Carmen and Ávila, Rafael. 2008. Aplicaciones de la inteligencia artificial en la Medicina: perspectivas y problemas. *IMBIOMED.* [Online] 2012. http://www.imbiomed.com.mx/1/1/articulos.php?method=showDetail&id_articulo=51320&id_seccion=2663&id_ejemplar=5205&id_revista=51. ISSN: 1561-2880.

Fuente, A. A. J. and J. M. C. Lovelle. 2006. *Proyectos informáticos.* s.l. : Servitec, 2006. p. 105. ISBN: 8468972762, 9788468972763.

FUNIBER. 2012. Sistema Inteligente de Gestión de Vulnerabilidades Informáticas (SIGVI) - (Ecuador 2008-2009). *FUNIBER.* [Online] Fundación Universitaria Iberoamericana, 2012. http://www.funiber.org/proyectos/idi/sistema-inteligente-de-gestion-de-vulnerabilidades-informaticas-sigvi-ecuador-2008-2009/.

Gao, Kehan , Khoshgoftaar, Taghi M. and Seliya, Naeem. 2012. Predicting high-risk program modules by selecting the right software measurements. *Software Quality Journal.* 2012, Vol. 20, 1, pp. 3-42.

García, Manuel, et al. 2003. *Sistema de Indicadores de Calidad I.* [ed.] UNMSM Instituto de Investigación Facultad de Ingeniería Industrial. s.l. : Industrial Data, 2003. pp. 66-73. Vol. 6.

Gómez , Ricardo , et al. 2010. Methodology and Governance of the IT Risk Management. [ed.] Facultad de Ingeniería, Universidad de los Andes Revista de Ingeniería. *Revista de Ingeniería.* 2010, 31. http://www.scielo.org.co/scielo.php?pid=S0121-49932010000100012&script=sci_arttext&tlng=en.

Gonçalves, J. F., Mendes, J.J.M. and Resende, M.G.C. 2008. A genetic algorithm for the resource constrained multi-project scheduling problem. *European Journal of Operational Research.* 2008, Vol. 189, 3, pp. 1171–1190.

Gong, Saisai and Weiyi, Ge. 2011. A Reasoning Approach to Rule Based Reasoning for Semantic Web Browsers. *Journal of Nanjing Normal University (Engineering and Technology) [J. Nanjing Norm. Univ. (Eng. Technol.)].* 2011, Vol. 11, 4, pp. 40-46.

González, Yusleimi. 2008. Gestión de Riesgos del Proyecto Sistema de Gestión Penitenciaria (SIGEP). *UCI | Dirección de Información.* [Online] 2012. http://catalogoenlinea.uci.cu/cgi-bin/koha/opac-detail.pl?biblionumber=6550.

Gutiérrez, Carlos. 2008. Gestión de los Riesgos en el Proyecto "A Jugar". *UCI | Dirección de Información.* [Online] 2012. http://catalogoenlinea.uci.cu/cgi-bin/koha/opac-detail.pl?biblionumber=6282.

Hall, David C. 2011. Making risk assessments more comparable and repeatable. *Systems Engineering.* 2011, Vol. 14, 2, págs. 173–179.

Harvard_Business_Review. 2011. Harvard Business Review Analitic Services. Risk Management in a Time of Global Uncertainty. *Zurich Insurance Group.* [Online] 2012. http://www.zurich.com/internet/main/sitecollectiondocuments/insight/risk-management-in-a-time-of-global-uncertainty.pdf.

Higuera, R. P. and Haimes, Y. Y. 1996. *Software Risk Management.* Pittsburgh : Software Engineering Institute, 1996. CMU/SEI-96-TR-012.

Huerta, Antonio. 2012. Deconstruyendo a PILAR. *Security Art Work.* [Online] 2012. http://www.securityartwork.es/2012/09/14/deconstruyendo-a-pilar/.

ISO. 2012. La certificación ISO 9001: Cuanto cuesta? *Normas9000.com.* [Online] 2012. http://www.normas9000.com/cuanto-cuesta-iso-9001.html.

ISO/IEC. 2004. *ISO/IEC 13335-1:2004. Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management.* 2004.

Jacobson, I., Booch, G. and Rumbaugh, J. 2000. *El proceso unificado de desarrollo de software.* Madrid : Pearson Educación S.A., 2000. ISBN: 80-7829-036-2.

Jeste, Dilip V. , et al. 2010. Expert Consensus on Characteristics of Wisdom: A Delphi Method Study. *The Gerontologist.* 2010, Vol. 50, 5, pp. 668-680.

Jiang, J., G. Klein, et al. 2001. *Information Systems Success as impacted by risks and development strategies.* s.l. : IEEE transactions on Engineering Management 48: 46-55., 2001. Vol. 48. ISSN: 0018-9391.

Kahkonen, K. 2001. *Integration of Risk and Opportunity Thinking in Projects.* London : Fourth European Project Management Conference, PMI Europe 2001, 2001.

Kontio, Jirky and Basili, V. R. 1997. *Empirical Evaluation of a risk management Method.* Pittsburgh : Software Engineering Institute, Proceedings of the SEI Conference on Risk Management, 1997.

Kontio, Jirky. 2002. *Risk Management: What went wrong and what is the new agenda?* [Conference Notes Helsinki: Center for Excellence Finland] Helsinki, Finlandia : Quality Connection - 7th European Conference on Software Quality, 2002.

Kulik, P. and C. Weber. 2001. *Software Risk Management Practices.* Dayton : KLCI Research Group, 2001.

Li, Hui and Sun, Jie. 2008. Ranking-order case-based reasoning for financial distress prediction. *Knowledge-Based Systems.* 2008, Vol. 21, 8, pp. 868–878.

Lundström, Jesper , et al. 2008. Pcons: A neural-network–based consensus predictor that improves fold recognition. *Protein Science.* 2008, Vol. 10, 11, pp. 2354–2362.

MAP. 2012. *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método.* Madrid : Ministerio de Hacienda y Administraciones Públicas, 2012.

Marcelo, J., M. Rodenes, et al. 2003. *Estudio exploratorio sobre los métodos de gestión de proyectos de alto riesgo.* Valencia, España : Primer Congreso SOporte del COnocimiento con la TEcnología, SOCOTE, 2003.

Mathkour, Hassan , Assassa, Ghazy and Baihan, A. 2008. A Risk Management Tool for Extreme Programming. *IJCSNS International Journal of Computer Science and Network Security.* 2008, Vol. 8, 8.

Merrian-Webster. 2012. Merrian-Webster. *An Encyclopedia Britannica Company | Merrian-Webster.* [Online] 2012. http://www.merriam-webster.com/dictionary/brainstorming.

MFP. 2003. *Resolución No. 297-2003. Anexo 1. Definiciones del Control Interno. Contenidos de los Componentes y sus Normas.* s.l. : Ministerio de Finanzas y Precios, 2003.

Mochal, T. 2002. *Factor Positive Risk Into Project Planning.* s.l. : Tech Republic, 2002.

ONEI. 2011. Anuario estadístico de Cuba 2010. *ONEI | Oficina Nacional de Estadísticas e Información.* [Online] 2012. http://www.one.cu/aec2010/20080618index.htm.

Pachón, Álvaro. 2009. *Aplicación de la metáfora de la colonia de hormigas en la administración de direcciones en redes móviles ad hoc.* Colombia : Universidad ICESI, 2009.

Palarea, Anika. 2008. Aplicación de un modelo de Gestión de Riesgos en el Proyecto Programa Nacional de Informatización del Conocimiento Geológico. *UCI | Dirección de Información.* [Online] 2008. http://catalogoenlinea.uci.cu/cgi-bin/koha/opac-detail.pl?biblionumber=6277.

Peng, Yi, et al. 2009. Empirical Evaluation of Classifiers for Software Risk Management. *International Journal of Information Technology & Decision Making.* 2009, Vol. 8, 4.

PMI. 2008. *A guide to the Project Management Body of Knowledge. 4th Edition.* s.l. : Project Management Institute, Inc, 2008. ISBN: 978-1-933890-72-2.

Power, Michael. 2008. *Organized Uncertainty: Designing a World of Risk Management.* Oxford : Oxford University Press, 2008. ISBN: 9780199548804.

Pressman, R. S. 2010. *Ingeniería del Software. Un enfoque práctico. 7ma Edición.* s.l. : Mc Graw-Hill/Interamericana de España, S.A., 2010.

Pritchard, Carl L. 2010. *Risk Management: Concepts and Guidance 4th edition.* s.l. : ESI International ©2010, 2010. ISBN:1890367559 9781890367558.

Purdy, Grant. 2010. ISO 31000:2009—Setting a New Standard for Risk Management. *Risk Analysis.* 2010, Vol. 30, 6.

PwC. 2011. Global 100 Software Leaders, Key players & market trends. *PwC.* [Online] 2011. http://www.pwc.com/gx/en/technology/publications/global-software-100-leaders/index.jhtml.

Reyes, Yandielys. 2009. Aplicación y mejora del Modelo de Gestión de Riesgos “MoGeRi” al proyecto “Captura y Catalogación de Medias”. *UCI | Dirección de Información.* [Online] 2012. http://catalogoenlinea.uci.cu/cgi-bin/koha/opac-detail.pl?biblionumber=8288.

Rivera, Sergio. 2010. Modelo de un Sistema de Razonamiento Basado en Casos para el Análisis en la Gestión de Riesgos. *UCI | Dirección de Información.* [Online] 2012. http://catalogoenlinea.uci.cu/cgi-bin/koha/opac-detail.pl?biblionumber=11021.

Rodríguez, Gonzalo M. 2006. *La evaluación financiera y social de proyectos de inversión.* La Habana : Facultad de Economía. Universidad de La Habana , 2006. http://ccia.cujae.edu.cu/index.php/siia/siia2010/paper/view/978. ISBN: 959-16-0424-6 .

Roppponen, J. and K. Lyytinen. 2000. *Components of Software Development Risk: Hot to address Them?* s.l. : IEEE Transactions on Software Engineering 26: 98-111., 2000.

RTI. 2010. What Could One Unidentified Risk Cost ... ? TM. *RiskTrak International "Experts in Risk Management" TM.* [Online] 2012. http://risktrak.com/.

Schmidt, R., K. Lyytinen, et al. 2001. *Identifying software project risks, an international Delphi study.* s.l. : Journal of Management Information Systems 17: 5-36, 2001.

SEI. 1994. *A Construct for Describing Software Development Risks.* [Technical Report] Pittsburgh : Software Engeneering Institute | Carnegie Mellon, 1994. CMU/SEI-94-TR-14, ESC-TR-94-014..

—. 2007. A Proposed Taxonomy for Software Development Risks for High-Performance Computing (HPC) Scientific/Engineering Applications. *Software Engineering Institute | Carnegie Mellon.* [Online] 2012. http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA468594. CMU/SEI-2006-TN-039.

—. 2010. A Taxonomy of Operational Cyber Security Risks. *Software Engineering Institute | Carnegie Mellon.* [Online] 2012. http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA537111. CMU/SEI-2010-TN-028.

—. 2012. CMMI Benefits. *Software Engineering Institute | Carnegie Mellon.* [Online] Software Engineering Institute, 2012. http://www.sei.cmu.edu/cmmi/why/benefits/index.cfm.

—. 2010. CMMI for Development v1.3. *Software Engineering Institute | Carnegie Mellon.* [Online] 2012. http://www.sei.cmu.edu/reports/10tr033.pdf. CMU/SEI-2010-TR-033.

—. 2011. *CMMI Product Suite: Prices.* Pittsburgh : SEI Partner Network | Carnegie Mellon, 2011.

—. 1996. Continuous Risk Management Guidebook. *Software Engeneering Institute | Carnegie Mellon.* [Online] 2012. http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA319533.

—. 2012. Mission Risk Diagnostic (MRD) Method Description. *Software Engineering Institute | Carnegie Mellon .* [Online] 2012. http://www.sei.cmu.edu/library/abstracts/reports/12tn005.cfm. CMU/SEI-2012-TN-005.

—. 2012. Published Appraisal Results. *Software Institute Engeneering | Carnegie Mellon.* [Online] Software Institute Engeneering, 2012. https://sas.sei.cmu.edu/pars/pars.aspx.

—. 1997. *Risk Management: Implicit and Explicit.* Pittsburgh : Proceedings of the Fifth SEI Conference on Software Risk Management, 1997.

—. 1992. *Software Development Risk: Opportunity, Not Problem.* s.l. : Software Engeneering Institute | Carnegie Mellon, 1992. CMU/SEI-92-TR-30.

—. 1999. *Software Risk Evaluation (SRE) Method Description (Version 2.0).* s.l. : Software Engeneering Institute | Carnegie Mellon, 1999. CMU/SEI-99-TR-029.

—. 2006. Standard CMMI ® Appraisal Method for Process Improvement (SCAMPI SM) A, Version 1.2: Method Definition Document. *Software Engineering*

Institute | *Carnegie Mellon.* [Online] 2012. http://repository.cmu.edu/sei/661/. CMU/SEI-2006-HB-002.

Sentí, Vivian. 2010. *Conferencias Curso Gestión del Conocimiento.* UCI, La Habana : s.n., 2010.

Sommerville, I. 2007. *Software Engineering. 8va Edición.* s.l. : Pearson Education, 2007. ISBN: 7-111-19770-4.

Song, Hao, et al. 2009. Software Risks Correlation Analysis Using Meta-analysis. *Communications in Computer and Information Science.* 2009, Vol. 35, 7, pp. 559-565.

Stoneburner, G., Goguen, A. and Feringa, A. 2002. Risk Management Guide for Information Technolog y Systems. NIST SP 800-30. [Online] 2012. http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf. CODEN: NSPUE2.

Tardío, Maria Antonia, Febles, Ailyn and Perez , Deborat. 2011. *Primeras ideas de un modelo cubano de referencia para el desarrollo de aplicaciones informáticas.* [ed.] Universidad de las Ciencias Informáticas. La Habana : Ediciones Futuro, Revista Cubana de Ciencias Informáticas, 2011. ISSN: 1994-1536.

Valladares, Ana. 2010. Proceso de Gestión de riesgos para proyectos de desarrollo de software de Softel. *UCI* | *Dirección de Información.* [Online] 2012. http://catalogoenlinea.uci.cu/cgi-bin/koha/opac-detail.pl?biblionumber=9736.

Walz, John. 2010. Software And Systems EngineeringRisk Management. *Systems and Software Technology Conference, SSTC 2010.* [Online] 2012. http://sstc-online.org/2010/pdfs/JW2679.pdf..

Zulueta, Y. 2009. *La gestión de riesgos en la producción de software y la formación de profesionales de la informática: experiencias de una universidad cubana.* s.l. : Revista Española de Innovación, Calidad e Ingeniería de Software 5(3): 6-20., 2009.

—. 2007. Modelo de Gestión de Riesgos en Proyectos de Desarrollo de Software. *UCI* | *Dirección de Información.* [Online] 2012. http://catalogoenlinea.uci.cu/cgi-bin/koha/opac-detail.pl?biblionumber=5814.

—. 2008. MoGeRi: Modelo de gestión de riesgo en proyectos de desarrollo de software. *Convención Científica de Ingeniería y Arquitectura.* [Online] 2012. http://ccia.cujae.edu.cu/index.php/siia/siia2008/paper/view/1214.

—. 2008. Retos en la gestión de los riesgos en proyectos de software. *Revista Cubana de Ciencias Informáticas.* [Online] 2012. http://rcci.uci.cu/index.php/rcci/article/view/45. ISSN: 1994-1536.

Bibliografía

Boehm, B. 1988. A Spiral Model of Software Development and Enhancement. *Computer.* s.l. : IEEE Computer Society, 1988. Vol. 21, 5, pp. 61-72. ISSN: 0018-9162.

Boehm, B. and DeMarco, T. 1997. Software Risk Management. *IEEE Software.* 1997. Vol. 14, 3, pp. 17-19. ISSN: 0740-7459.

Boehm, B. 1991. Software risk management: principles and practices. *IEEE Software.* Arlington : s.n., 1991. Vol. 8, 1, pp. 32 - 41. ISSN: 0740-7459.

Boehm, B., Jo, Ann Lane and Koolmanojwong, Supannika. 2010. *A Risk-Driven Decision Table for Software Process Selection.* California : University of Southern California, Center for Systems and Software Engineering (USC-CSSE), 2010.

Boehm, B., y otros. 1998. Using the WinWin spiral model: a case study. *Computer.* Los Ángeles : s.n., 1998. Vol. 31, 7, págs. 33-44. ISSN: 0018-9162.

Chang, Pei-Chann, Liu, Chen-Hao and Lai, Robert K. 2008. A fuzzy case-basedreasoning model for sales forecasting in print circuit board industries. *Expert Systems with Applications.* 2008, Vol. 34, 3, pp. 2049–2058.

Charette, Robert N. 1989. Software Engineering Risk Analysis and Management. *IEEE Software.* s.l. : McGraw-Hill, 1989. Digitalizado en 2009. ISSN: 0070106614.

CRAMM. 2003. *CCTA Risk Analysis and Management Method User Guide version 5.0.* s.l. : Siemens, 2003.

Doherty N., K., M. 2001. An investigation of the factors affecting the successful treatment of organizational issues in systems development projects. *European Journal of Information Systems.* 2001, Vol. 10, 3, pp. 147-160(14).

Dorigo, Marco and Stützle, Thomas . 2010. Ant Colony Optimization: Overview and Recent Advances. *International Series in Operations Research & Management Science.* 2010, Vol. 146, pp. 227-263.

Fuente, A. A. J. and J. M. C. Lovelle. 2006. *Proyectos informáticos.* s.l. : Servitec, 2006. p. 105. ISBN: 8468972762, 9788468972763.

Hall, David C. 2011. Making risk assessments more comparable and repeatable. *Systems Engineering.* 2011, Vol. 14, 2, págs. 173–179.

Harvard_Business_Review. 2011. Harvard Business Review Analitic Services. Risk Management in a Time of Global Uncertainty. *Zurich Insurance Group.* [Online] 2012. http://www.zurich.com/internet/main/sitecollectiondocuments/insight/risk-management-in-a-time-of-global-uncertainty.pdf.

Higuera, R. P. and Haimes, Y. Y. 1996. *Software Risk Management.* Pittsburgh : Software Engineering Institute, 1996. CMU/SEI-96-TR-012.

ISO/IEC. 2004. *ISO/IEC 13335-1:2004. Information technology - Security techniques - Management of information and communications technology security - Part 1: Concepts and models for information and communications technology security management.* 2004.

Jacobson, I., Booch, G. and Rumbaugh, J. 2000. *El proceso unificado de desarrollo de software.* Madrid : Pearson Educación S.A., 2000. ISBN: 80-7829-036-2.

Kontio, Jirky and Basili, V. R. 1997. *Empirical Evaluation of a risk management Method.* Pittsburgh : Software Engineering Institute, Proceedings of the SEI Conference on Risk Management, 1997.

Kontio, Jirky. 2002. *Risk Management: What went wrong and what is the new agenda?* [Conference Notes Helsinki: Center for Excellence Finland] Helsinki, Finlandia : Quality Connection - 7th European Conference on Software Quality, 2002.

Kulik, P. and C. Weber. 2001. *Software Risk Management Practices.* Dayton : KLCI Research Group, 2001.

MAP. 2012. *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método.* Madrid : Ministerio de Hacienda y Administraciones Públicas, 2012.

PMI. 2008. *A guide to the Project Management Body of Knowledge. 4th Edition.* s.l. : Project Management Institute, Inc, 2008. ISBN: 978-1-933890-72-2.

Pressman, R. S. 2010. *Ingeniería del Software. Un enfoque práctico. 7ma Edición.* s.l. : Mc Graw-Hill/Interamericana de España, S.A., 2010.

PwC. 2011. Global 100 Software Leaders, Key players & market trends. *PwC.* [Online] 2011. http://www.pwc.com/gx/en/technology/publications/global-software-100-leaders/index.jhtml.

Roppponen, J. and K. Lyytinen. 2000. *Components of Software Development Risk: Hot to address Them?* s.l. : IEEE Transactions on Software Engineering 26: 98-111., 2000.

RTI. 2010. What Could One Unidentified Risk Cost ... ? TM. *RiskTrak International "Experts in Risk Management" TM.* [Online] 2012. http://risktrak.com/.

Schmidt, R., K. Lyytinen, et al. 2001. *Identifying software project risks, an international Delphi study.* s.l. : Journal of Management Information Systems 17: 5-36, 2001.

SEI. 1994. *A Construct for Describing Software Development Risks.* [Technical Report] Pittsburgh : Software Engeneering Institute | Carnegie Mellon, 1994. CMU/SEI-94-TR-14, ESC-TR-94-014..

—. 2007. A Proposed Taxonomy for Software Development Risks for High-Performance Computing (HPC) Scientific/Engineering Applications. *Software Engineering Institute | Carnegie Mellon.* [Online] 2012. http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA468594. CMU/SEI-2006-TN-039.

—. 2010. A Taxonomy of Operational Cyber Security Risks. *Software Engineering Institute | Carnegie Mellon.* [Online] 2012. http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA537111. CMU/SEI-2010-TN-028.

—. 2012. CMMI Benefits. *Software Engineering Institute | Carnegie Mellon.* [Online] Software Engineering Institute, 2012. http://www.sei.cmu.edu/cmmi/why/benefits/index.cfm.

—. 2010. CMMI for Development v1.3. *Software Engineering Institute | Carnegie Mellon.* [Online] 2012. http://www.sei.cmu.edu/reports/10tr033.pdf. CMU/SEI-2010-TR-033.

—. 1997. *Risk Management: Implicit and Explicit.* Pittsburgh : Proceedings of the Fifth SEI Conference on Software Risk Management, 1997.

—. 2006. Standard CMMI ® Appraisal Method for Process Improvement (SCAMPI SM) A, Version 1.2: Method Definition Document. *Software Engineering Institute | Carnegie Mellon.* [Online] 2012. http://repository.cmu.edu/sei/661/. CMU/SEI-2006-HB-002.

Sommerville, I. 2007. *Software Engineering. 8va Edición.* s.l. : Pearson Education, 2007. ISBN: 7-111-19770-4.

Zulueta, Y. 2009. *La gestión de riesgos en la producción de software y la formación de profesionales de la informática: experiencias de una universidad cubana.* s.l. : Revista Española de Innovación, Calidad e Ingeniería de Software 5(3): 6-20., 2009.

Anexos

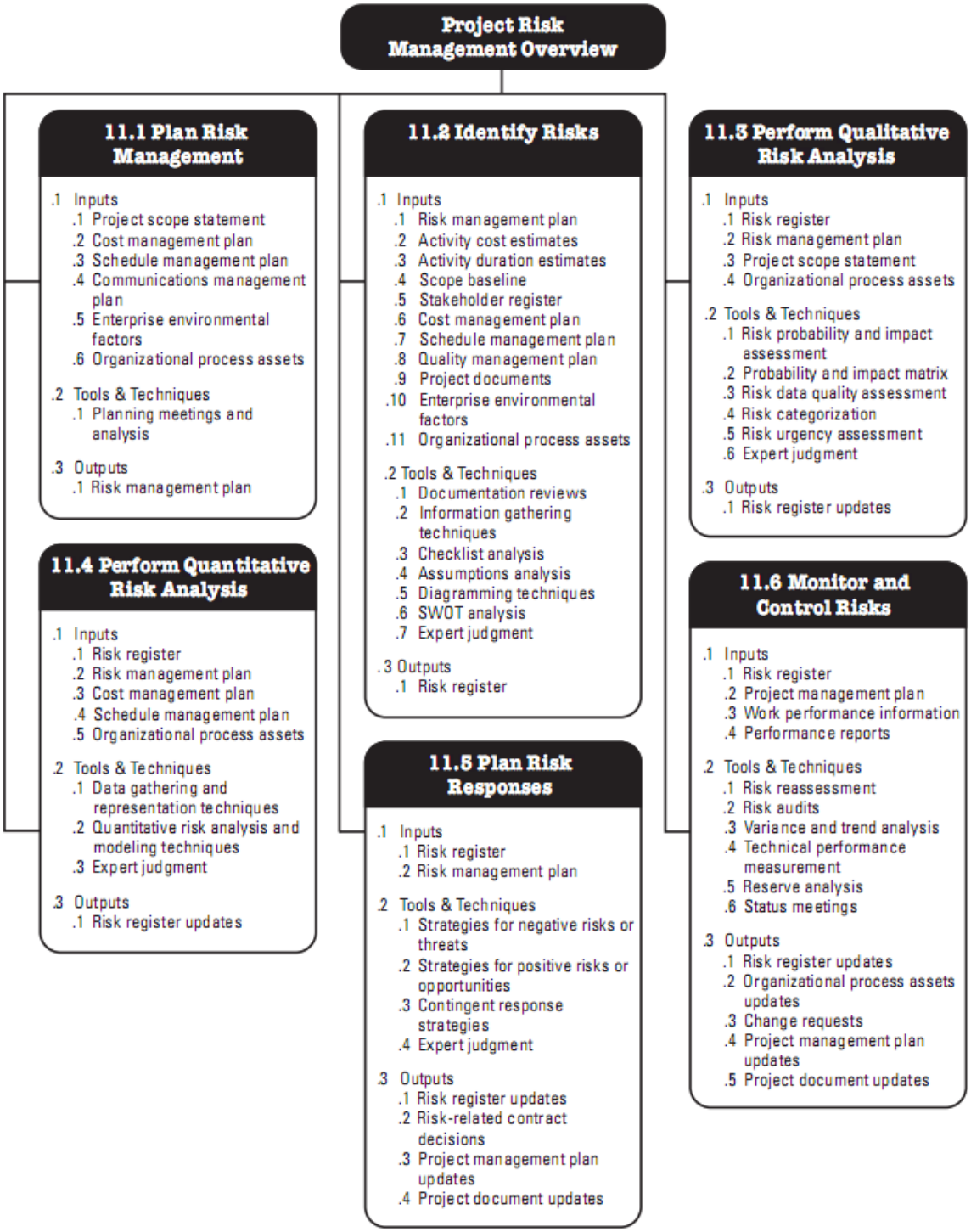
Anexo 1

Top 10 Software RiskÍtems.

Risk item	Risk management techniques
1. Personnel shortfalls	Staffing with top talent, job matching; teambuilding; morale building; cross-training; pre-scheduling key people
2. Unrealistic schedules and budgets	Detailed, multisource cost and schedule estimation; design to cost; incremental development; software reuse; requirements scrubbing
3. Developing the wrong software functions	Organization analysis; mission analysis; ops-concept formulation; user surveys; prototyping; early users' manuals
4. Developing the wrong user interface	Task analysis; prototyping; scenarios; user characterization (functionality, style, workload)
5. Gold plating	Requirements scrubbing; prototyping; cost-benefit analysis; design to cost
6. Continuing stream of requirement changes	High change threshold; information hiding; incremental development (defer changes to later increments)
7. Shortfalls in externally furnished components	Benchmarking; inspections; reference checking; compatibility analysis
8. Shortfalls in externally performed tasks	Reference checking; pre-award audits; award-fee contracts; competitive design or prototyping; teambuilding
9. Real-time performance shortfalls	Simulation; benchmarking; modeling; prototyping; instrumentation; tuning
10. Straining computer-science capabilities	Technical analysis; cost-benefit analysis; prototyping; reference checking

Anexo 2

Procesos para la GR según PMI.



Anexo 3

Entrevista realizada a líderes de proyecto de la UCI con el objetivo de analizar la situación actual de la GR en los proyectos de desarrollo de aplicaciones informáticas.

1. ¿Realizan actividades de GR? ¿Cuáles?
2. ¿Utilizan una guía formal para realizar la GR? ¿Cuál?
3. ¿Qué técnicas aplican para realizar las actividades de GR?
4. ¿Utiliza indicadores para conocer el estado de la GR y de cada riesgo? ¿Cuáles?
5. ¿Documentan los resultados de la GR? ¿En qué formato? ¿Utilizan alguna plantilla específica? Nómbrela
6. ¿Se analizan las oportunidades que proporcionan los riesgos positivos?
7. ¿Se utilizan herramientas que automaticen todo o parte del proceso de GR?
8. Mencione las dificultades que considera son resultado del proceso de GR que ejecuta en su proyecto.

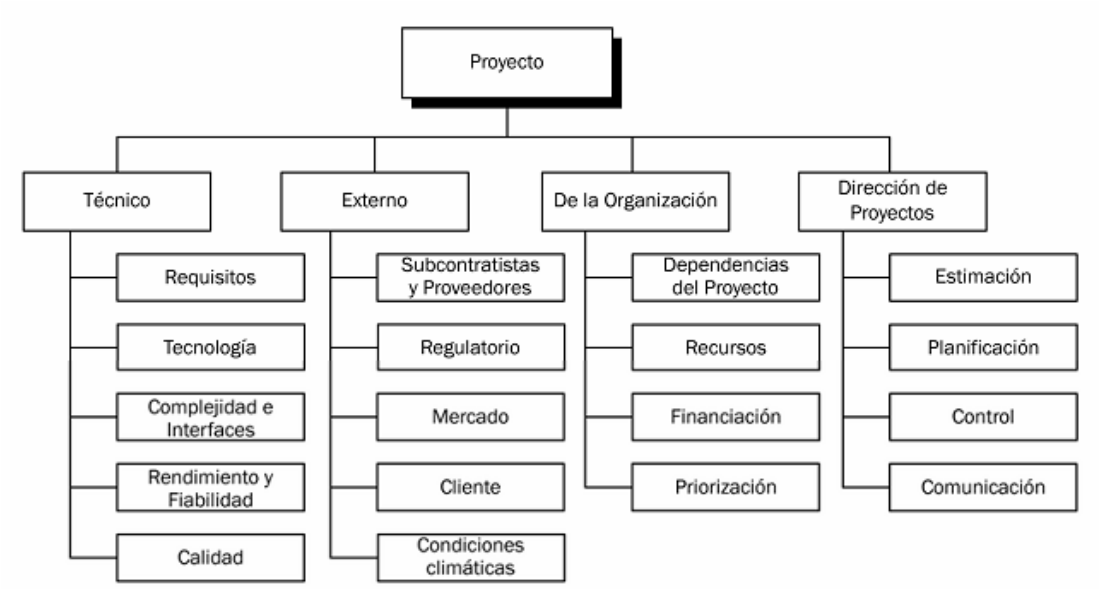
Anexo 4

Entrevista realizada a especialistas de Calisoft, con el objetivo de obtener información sobre la reciente evaluación de la UCI en el nivel 2 de CMMI.

1. Sobre la reciente evaluación de CMMI.
    a. ¿Los costos de la evaluación fueron elevados?
    b. ¿Se evaluaron todos los centros de la universidad?
    c. ¿Qué nivel se alcanzó en la evaluación?
    d. ¿Qué áreas de proceso fueron evaluadas?
    e. ¿Cómo se analizó el área de proceso RSKM durante la evaluación?
    f. ¿Qué perspectivas tiene Calisoft con respecto al área de proceso RSKM?
    g. ¿Qué perspectivas se plantea Calisoft con respecto al nivel 3 de CMMI?

Anexo 5

Estructura de Desglose del Riesgo.



Anexo 6

Matriz de Probabilidad e Impacto

Matriz de Probabilidad e Impacto

Probabilidad	Amenazas					Oportunidades				
0,90	0,05	0,09	0,18	0,36	0,72	0,72	0,36	0,18	0,09	0,05
0,70	0,04	0,07	0,14	0,28	0,56	0,56	0,28	0,14	0,07	0,04
0,50	0,03	0,05	0,10	0,20	0,40	0,40	0,20	0,10	0,05	0,03
0,30	0,02	0,03	0,06	0,12	0,24	0,24	0,12	0,06	0,03	0,02
0,10	0,01	0,01	0,02	0,04	0,08	0,08	0,04	0,02	0,01	0,01
	0,05	0,10	0,20	0,40	0,80	0,80	0,40	0,20	0,10	0,05

Impacto (escala de relación) sobre un objetivo (por ejemplo, coste, tiempo, alcance o calidad)

Cada riesgo es clasificado de acuerdo con su probabilidad de ocurrencia y el impacto sobre un objetivo en caso de que ocurra. Los umbrales de la organización para riesgos bajos, moderados o altos se muestran en la matriz y determinan si el riesgo es calificado como alto, moderado o bajo para ese objetivo.

Anexo 7

Descripción de las Restricciones de la GR (Zulueta, 2008).

1 **Restricciones políticas o gerenciales:** Típicas de organizaciones gubernamentales o fuertemente relacionadas con organismos gubernamentales, bien como proveedores o como suministradores de servicios, como es el caso de la UCI.

2 **Restricciones estratégicas:** Derivadas de los objetivos de la Organización.

3 **Restricciones geográficas:** Derivadas de la ubicación física del proyecto o de su dependencia de medios físicos de comunicaciones.

4 **Restricciones temporales:** Que toman en consideración situaciones coyunturales: conflictividad laboral, crisis internacional, cambio de la propiedad, reingeniería de procesos, etc.

5 **Restricciones estructurales:** Tomando en consideración la organización interna, por ejemplo, procedimientos de toma de decisiones, etc.

6 **Restricciones funcionales:** Que tienen en cuenta los objetivos de la institución y las empresas o entidades involucradas.

7 **Restricciones legales:** Leyes, reglamentos, regulaciones sectoriales, contratos externos e internos, etc. Restricciones relacionadas con el personal. Perfiles laborales, compromisos contractuales, compromisos sindicales, carreras profesionales, etc.

8 **Restricciones metodológicas:** Derivadas de la naturaleza de la institución o del cliente y sus hábitos o habilidades de trabajo que pueden imponer una cierta forma de hacer las cosas.

9 **Restricciones culturales:** La “cultura” o forma interna de trabajar puede ser incompatible con ciertas salvaguardas teóricamente ideales.

10 **Restricciones presupuestarias:** Limitaciones en el gasto que (aunque no se haya estimado el presupuesto de la GR) pueden o no, estar definidas.

Anexo 8

Funciones de comparación por cada tipo de variable definida en la base de casos de SIMR.

Para las **variables literales** se utiliza la siguiente función:

$$\delta_i(O_o, O_t) = \begin{cases} \omega \ X_i(O_1) = X_j(O_2) \\ \text{o e. o. c.} \end{cases} \qquad (1)$$

$X_i(O_o)$ y $X_j(O_t)$ definen los rasgos que manifiestan estas características en su comparación en los casos O_o y O_t; y $\delta(O_o, O_t)$ la semejanza entre los rasgos. El uso de ω posibilita que el resultado de la comparación manifieste valores diferentes en cada comparación eliminando la simetría en la relevancia y permitiendo dar un resultado ajustado a la solución.

Para las **variables numéricas** se utiliza una variación de la función de comparación Manhattan que transforma el cálculo de la distancia entre dos valores en un intervalo definido o en un conjunto del cual se conozcan el mínimo y el máximo valor a un resultado que se define como semejanza. La función es la siguiente:

$$\delta_i(O_o, O_t) = 1 - \left|\frac{X_i(O_o) - X_i(O_t)}{r_{máx} + r_{mín}}\right| \qquad (2)$$

$r_{mín}$ y $r_{máx}$ definen el mínimo y el máximo valor que puede alcanzar el rasgo X del caso O.

Las ***variables de tipo ordinal discreto***, son normalizadas para posteriormente ser comparados de acuerdo con la función (2). La normalización se realiza definiendo M_i como la cantidad de estados ordenados que puede tomar el rasgo i. Luego se hace corresponder a cada valor del dominio según su orden, un número entero entre 1 y M_i para finalmente aplicar la fórmula:

$$X_i = \frac{v-1}{M_i - 1} \qquad (3)$$

Donde v representa el valor del número entero asignado al rasgo.

Un ejemplo de la normalización es el rasgo Complejidad de la aplicación cuyos valores son Alta, Media y Baja. Se le hace corresponder a este dominio números enteros quedando de la siguiente forma: M_i=3; Baja=1, Media=2, Alta=3. Finalmente se aplica la función (3).

Identificación de los riesgos del proyecto: se parte de la inserción de los datos del mismo, el sistema compara los datos entrados con los casos almacenados de acuerdo con las funciones de comparación presentadas para cada tipo de rasgo, que según su valor de dominio tendrá una función de semejanza, la cual compara dicho valor con su rasgo correspondiente en cada caso de la base de conocimientos. Una vez se analiza cada rasgo predictor (columna de la Base de Casos o campo independiente), se evalúa (rasgo objetivo o fila de la Base de casos) de acuerdo con la siguiente función de evaluación:

$$\beta(O_o, O_t) = \frac{\sum_{i=1}^{n} p_i * \delta_i(O_o, O_t) * (1 - [I(Xi(O_o) - I(Xj(O_t))])}{\sum_{i=1}^{n} p_i} \qquad (4)$$

Donde n representa la cantidad de casos, p_i la relevancia de cada rasgo, $\delta(O_o, O_t)$ la semejanza entre los casos O_o y O_t y tanto $I(X_i(O_o))$ como $I(X_j(O_t))$ las incertidumbres respectivas de los rasgos comparados.