Análisis y Gestión de Riesgo en Proyectos Software

Un nuevo modelo integrando la metodología SEI y Magerit2

Caballero S. D., Kuna H.D.

Facultad de Ciencias Exactas Químicas y Naturales / Universidad Nacional de Misiones

{sergiodcaballero@gmail.com, hdkuna@gmail.com}

Resumen

Hablar de riesgos es hablar de futuro, de probabilidades, de incertidumbre, de avances o retrocesos.

Toda actividad implica un riesgo, y aunque algunos ubican la etimología en la palabra en *risco*, esto no implica de por sí una valoración negativa, todo cambio implica peligros, pero el peor peligro es la inmovilidad.

Un Riesgo es la probabilidad que ocurra una perdida. Los riesgos técnicos del software son la medida de la probabilidad y severidad de que se produzcan efectos adversos en el desarrollo, adquisición, mantenimiento etc. de sistema.

Todas las áreas en el desarrollo de sistemas son fuentes potenciales de riesgos de software.

Debido a la importancia de estos, en los proyectos software, se realizará una investigación de distintas metodologías para detectar, analizar, eliminar o minimizar los posibles riesgos a los cuales se somete un proyecto software de pequeña a mediana envergadura durante su ciclo de vida (Planificación, análisis, desarrollo, implementación y mantenimiento) y los riesgos generales a los que se somete el TI[1] de estas organizaciones. Basados en metodologías de análisis y gestión de riesgos estándares de la TI se busca lograr un método ágil, flexible, rápido y sencillo de utilizar por organización que no cuentan con los medios para poder afrontar los altos costos de los estudios de análisis y gestión de riesgos realizados por consultoras privadas o por soporte informático especializado. Y como resultado de la investigación se generará un software prototipo basado en las mejores técnicas de las metodologías investigadas.

Palabras clave: Análisis y Gestión de Riesgos, Auditoría, Ingeniería del Software

Contexto

Trabajo de Investigación para la generación de la Tesis de Maestría en Tecnologías de la Información UNNE-UNAM.

Introducción

El objetivo de esta investigación es generar un método de análisis y gestión de riesgos adaptando los requerimientos y necesidades informáticas y tecnológicas de las organizaciones pyme, se busca crear un método simple, ágil y de económica implementación, utilizando como base de estudio dos de las metodologías más importantes de análisis y gestión de riesgos en TI[1], utilizando la metodología SEI[2] CRM[3] y adaptando técnicas y elementos de la metodología Magerit V3; para facilitar y automatizar la alta carga de trabajo, gestión, control y mantenimiento de proyectos basados en el método creado, en el marco de estas investigación se realizará una herramienta software. El método y la herramienta servirán para analizar y gestionar los posibles riesgos que pueden

[1] Tecnología de la informatica

[2] Software Engineering Institute - Carnegie Mellon University

[3] Continuous Risk Management

tener los activos; generar un procedimiento de seguimiento de los planes de acción de los riesgos gestionados, comunicar y registrar los incidentes ocurridos para evaluar posteriormente el nivel de los ajustes a realizar en el AGR[4], esto ayudará a eliminar o minimizar los incidentes ocurridos, además, resguardar los activos de las organizaciones para que estos no corran riesgos desconocidos o que su impacto sea mínimo y controlado.

Líneas de investigación y desarrollo

El uso de la TI ha crecido considerablemente en los últimos años y las organizaciones cada vez dependen más de ella para garantizar el éxito en el entorno de negocios actual; la habilidad que tenga la organización para implantar las tecnologías modernas que soporten de manera eficiente y controlada a los procesos de negocio críticos, tiene un gran impacto en su grado de competitividad[2].

Los planes estratégicos de negocio actualmente incluyen iniciativas que involucran la optimización de los recursos informáticos para asegurar la consecución de los objetivos de la organización; como consecuencia de lo anterior, los altos ejecutivos están cada vez más alertas sobre la forma en que la tecnología soporta al negocio y dependen cada día más en los Directores de Tecnología de Información para optimizar la organización. [3]

Este incremento ha añadido complejidad a las arquitecturas tecnológicas y a los procesos para su implantación y administración; por consiguiente, se presentan nuevos riesgos que deben ser mitigados de forma efectiva y eficiente para mantener el cumplimiento de los objetivos de control. Dichos riesgos se encuentran en su mayoría inmersos en los cada vez más complejos sistemas de cómputos, recursos humanos en la etapa de su desarrollo, implementación y mantenimiento, y de TI en general.

Podemos decir que Gestión de Riesgos es una metodología en la cual se utiliza procesos, métodos y herramientas para gestionar los riesgos encontrados en un proyecto software; posee también métodos específicos para identificar riesgos importantes y estrategias para gestionarlos. Además provee de un entorno disciplinado para la toma de decisiones de una manera proactiva basándose constantemente en identificar que puede salir mal; “la Gestión de Riesgos es importante debido a que ayuda a evitar desastres, re-trabajo y sobre-trabajo, pero aún mas importante, porque estimula la generación de situaciones del tipo ganar-ganar”[4].

Las tareas del análisis y gestión de riesgos no son un fin en si mismas, si no que se adaptan en la actividad continua de gestión de la seguridad. El análisis de riesgos permite determinar como es, cuanto vale y cómo de protegidos se encuentran los activos. [5]

Una de la metodología elegida para el desarrollo de la gestión de Riesgos es la propuesta por el SEI 5 la cual cuenta con los siguientes etapas [6]:

- Inventario de activos
- Propósitos y Objetivos del análisis de riesgos
- Equipo de Trabajo
- Taxonomía de Riesgos
- Estimación de la probabilidad
- Estimación del impacto

[4] Análisis y Gestión de Riesgos

[5] Software Engineering Institute

- Exposición al riesgo
- Gestión de los Riesgos
  - Plan de Acción
  - Plan de Contingencia

Etapas del Modelo de Gestión de Riesgos SEI– CRM [7]

1º Identificación: Permite anticipar los riesgos antes de que estos ocurran y se transformen en problemas serios afectando adversamente el desarrollo del proyecto. Cabe destacar, que la identificación de riesgos (al igual que cada una de las etapas del modelo) convendría sea realizado de manera disciplinada y consistente, estimulando a los miembros del equipo de proyecto a formular sus inquietudes y facilitando el análisis posterior.

2º Análisis: Pretende transformar una serie de datos que han sido obtenidos en la etapa de identificación, en información que permita llevar adelante una toma de decisiones enfocada en los riesgos más importantes para el proyecto. "El análisis de riesgos es un proceso sistemático de estimación de la probabilidad de ocurrencia y la magnitud de la pérdida o impacto de cada uno de los riesgos identificados mediante el cual se logra reducir la incertidumbre de la medida y del resultado del acontecimiento asociado a un riesgo." [8]

3º Planificación: Convierte a la información relacionada a cada riesgo, en medidas y acciones efectivas en un tiempo inmediato y futuro. Esta fase incluye el proceso de acciones para cada uno de los riesgos en particular, como así también, otorgar un rango de prioridad a las acciones y a la implementación de un procedimiento de administración integral de riesgos.

4º Seguimiento: Radica en monitorear continuamente el estado de los riesgos y las acciones que fueron adoptadas, con el objetivo de evitar o reducir las pérdidas. Realizar un seguimiento de los riesgos, conlleva inevitablemente a tener que tomar una serie de medidas vinculadas con la gestión, haciendo posible a los referentes de la administración del proyecto realizar una permanente y precisa revisión de los planes.

5º Control: Proporciona la factibilidad de corregir las desviaciones que puedan causarse a los planes de gestión efectuados.

La comunicación y documentación del proceso son significativas en el modelo, ya que la carencia de garantías en ellas imposibilita la aplicación de cualquier estrategia de administración. La comunicación está y se hace notoria en el modelo en distintos niveles: el primero de ellos, establece la comunicación que corresponde cumplir entre cada uno de las fases del proceso, un segundo nivel esta determinado por la comunicación dentro del equipo de proyecto y el tercer nivel por la que surge entre el proyecto y los diferentes participantes del mismo[9].

La otra metodología elegida para el trabajo es la metodología MAGERIT V3 [10][11]

La metodología Magerit (Metodología de Análisis y gestión de riesgos de los sistemas de información), es una metodología propuesta por el Ministerio de administraciones Públicas del Gobierno Español para los organismos públicos de este país, realizado por el Ministerio de Administraciones públicas, Centro Criptográfico Nacional y la Universidad Politécnica de Madrid y liberado para su ser utilizado en cualquier ámbito.

Se podría definir a los objetivos principales de Magerit V3 como:

- Concientizar a los responsables de sistemas de información (dueños del proceso) de la existencia de riesgos y procesos, y la necesidad de detenerlos a tiempo.

- Ofrecer un método sistemático para analizar tales riesgos.
- Ayudar a descubrir y planificar, las medidas eficaces para conservar los riesgos bajo control.
- Apoyar la preparación de la Organización en procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.
- Fundamentar sólidamente los argumentos que defenderán la toma de decisiones por parte de los directivos de la organización..

Esta metodología en su versión 3 se compone de tres partes, que se describen a continuación

El Método: Es el documento que describe los pasos y tareas básicas a realizar en un proyecto de análisis y gestión de riesgos, proporciona una serie de aspectos prácticos y además describe la metodología desde un punto de vista de tres ángulos.

El Catalogo de Elementos: Es un manual que específica claramente los elementos utilizados por la metodología, define y clasifica cada uno de estos, incorporando ejemplos sencillos y aclaratorios con respecto a:

- Tipos de activos
- Dimensiones de valoración.
- Criterios de valoración.
- Amenazas típicas sobre los sistemas de información
- Salvaguardas a considerar para proteger sistemas de información.

Guía de Técnicas: Describe las técnicas utilizadas en la guía metodológica. Técnicas específicas para el análisis de riesgos, análisis mediante tablas, análisis algorítmico, árboles de ataque, técnicas generales, análisis coste-beneficio, diagramas de flujo de datos, diagramas de procesos, técnicas gráficas, planificación de proyectos, sesiones de trabajo (entrevistas, reuniones y presentaciones) y valoración Delphi6.
Tomado las 9 etapas de la metodología SEI basados en la taxonomía a contrario con los XXX etapas que utiliza Magerit V3. Y utilizando las características de Magerit V3 como ser:

- Tipos de activos
- Dimensiones de valoración de los activos
- Criterios de valoración de los activos
- Amenazas típicas sobre los sistemas de información
- Salvaguardas a considerar para proteger sistemas de información

Se crea el nuevo método el cual está conformado por las fortalezas de estas dos metodologías de AGR, la simpleza del SEI y el catálogo del MageritV3, acompañando a este nuevo método con una herramienta software para la gestión del mismo.

Resultados obtenidos/Esperados

El resultado de este proyecto es generar un método para el análisis y gestión de riesgos en el TI y una herramienta software para la gestión del mismo, integrando las mejoras prácticas de la metodología provista por el SEI análisis y gestión de riesgos basados en taxonomías y MAGERIT V3. La misma será orientada a las pequeñas y medianas organizaciones, la cuales poseen un presupuesto acotado para la inversión en la AGR. Por lo cual además del método se generará una aplicación software para asistir a la organización en la gestión de los riesgos en el ciclo de vida del proyecto software. Y se tomará como caso de estudio de la aplicación del método al SMAUNaM[7].

[6] Delphi Wideband el método de la valoración es una técnica consenso-basada de la valoración para estimar esfuerzo.
[7] Servicio Médico Asistencial de la Universidad Nacional de Misiones

Formación de recursos humanos

Tesis de Maestría en Técnología de la Información UNNE – UNaM.

Trabajo de Investigación "Análisis de Riesgo en Proyectos Software adaptados a la realidad tecnológica y Socio económica de la Pcia. de Misiones " – Secretaría de Investigación y Post Grado – FCEQyN

Referencias

[1] L. Jaunarena and C. Belletti, "Uso de métricas para la gestión de riesgos," 2002.

[2] Q. Gerard and M. O. Cinneide, "Experiences with Software Product Line Development in Risk Management Software."

[3] H. D. Kuna, S. Caballero, S. E. Jaroszczuk, and M. J. Miranda, "Plan de riesgos para la implementación, desarrollo y mantenimiento de componentes de web 2.0 en bibliotecas, caso de estudio en una biblioteca especializada," 2008.

[4] R. Bertone, P. Thomas, D. Taquias, and S. Pardo, "Herramienta para la Gestión de Riesgos en Proyectos de Software."

[5] H. Thimm, "A continuous risk estimation approach for corporate environmental compliance management," in *2015 IEEE 15th International Conference on Environment and Electrical Engineering (EEEIC)*, 2015, pp. 83–88.

[6] J. Hill and D. Victor, "The Product Engineering Class in the Software Safety Risk Taxonomy for Building Safety-Critical Systems," in *19th Australian Conference on Software Engineering (aswec 2008)*, 2008, pp. 617–626.

[7] R. P. Higuera and Y. Y. Haimes, "Software Risk Management," 1996.

[8] S. D. Maniasi, "Identificación de Riesgos de Proyectos de Software en Base a Taxonomías," Instituto Tecnológico de Buenos Aires, 2005.

[9] J. Esteves, J. Pastor, N. Rodriguez, and R. Roy, "Implementing and improving the SEI Risk Management method in a university software project," *IEEE Lat. Am. Trans.*, vol. 3, no. 1, pp. 90–97, Mar. 2005.

[10] Secretaría General de Administración Digital, "PAe - MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información." [Online]. Available: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Wq0hoLOvG01. [Accessed: 17-Mar-2018].

[11] D. Gaïti, C. IFIP World Computer Congress (19th : 2006 : Santiago, E. Tovar Caro, and V. Vega Zepeda, *Network control and engineering for QoS, security and mobility, V : IFIP 19th World Computer Congress, TC-6, 5th IFIP International Conference on Network Control and Engineering for QoS, Security and Mobility, August 20-25, 2006, Santiago, Chile*. Springer, 2006.