INVESTIGACIÓN

MODELO DE GESTIÓN DE RIESGOS EN PROYECTOS. APROXIMACIÓN CONCEPTUAL PARA PROYECTOS DE TI

MODEL OF RISK MANAGEMENT IN PROJECTS CONCEPTUAL APPROACH FOR IT PROJECTS

MSc.Torcoroma Velásquez Pérez[a], MSc. Hugo F. Castro Silva[b], MSc(c). Yesica M. Pérez[c]

[a,c] Universidad Francisco de Paula Santander Ocaña, Grupo de investigación GITYD. Via Acolsure, Sede el Algodonal, Ocaña, Colombia, tvelasquezp@ufpso.edu.co
[b] Universidad Pedagógica y Tecnológica de Colombia, Facultad de Ingenierías, Ingeniería Industrial. Avenida Central del Norte 39-115, Tunja, Boyacá, Colombia.
hugo.castro@uptc.edu.co

Fecha de recepción: 11-10-2015 **Fecha de aprobación:** 30-11-2015

Resumen: Esta investigación describe el diseño de un Modelo de Gestión de Riesgos de Proyectos de TI, se presenta la propuesta para ser contemplada en la planeación estratégica como alternativa para su implementación. El modelo surge del diagnóstico que presentan en la gestión de Riesgos de Proyectos de TI como necesidad para mejorar la calidad y seguridad de la información, garantizando así su disponibilidad, integridad y confidencialidad. Su desarrollo se basa en el ciclo PHVA (Planeación, Hacer, Verificar y Actuar) o Círculo de Deming, el triángulo organizacional (Estratégico, Táctico y Operativo), fundamentado en las buenas prácticas de Gobernabilidad de TI y seguridad de la Información contempladas en COBIT 4.1, PMBOK, NTC/ISO 27001, NTC/ISO 27002, NTC/ISO 27005, NTC/ISO 31000 y NTC 5254. Se pretende promover el uso de las buenas prácticas como gobernabilidad de TI para lograr un alineamiento estratégico.

Palabras clave: Gestión de Riesgos, Proyectos de TI, Gobernabilidad de TI.

Abstract: This research shows the design of a model Risk Management IT Projects, the proposal to be referred to in the strategic planning as an alternative for implementation is presented. The model arises from the diagnosis presented in Project Risk Management IT as a need to improve the quality and information security, ensuring their availability, integrity and confidentiality. Its development is based on the PDCA cycle (Plan, Do, Check and Act) or Circle of Deming, organizational triangle (strategic, tactical and operational), based on the best practices of IT governance and information security referred to in COBIT 4.1, PMBOK, NTC / ISO 27001, NTC / ISO 27002, NTC / ISO 27005, NTC / NTC ISO 31000 and 5254. It aims to promote the use of best practices and IT governance to achieve strategic alignment.

Keywords: Risk Management, IT Projects, IT Governance.

2. INTRODUCCIÓN

La propuesta de modelo de Gestión de Riesgo para Proyectos de TI presentada nace en la especialización de Auditoria de Sistemas, como una primera propuesta de gestión de riesgos, (Acosta et al., 2013) con los ajustes correspondientes para proyectos de TI; este busca contribuir con la línea de investigación de Gobernabilidad de TI del grupo de investigación de Tecnología y Desarrollo en Ingeniería – GITYD. Se propone este modelo de gestión de riesgo debido a que la información siempre está expuesta a amenazas y delitos informáticos lo que pone en riesgo su integridad, disponibilidad y confidencialidad, de ahí, que la estabilidad operacional, economía y buena imagen de la organización esté en riesgo; por tal motivo, se debe proteger con el fin garantizar la seguridad y calidad de la misma.

Se encuentran diferentes tipos de proyectos (Estay & Blasco, 1998) como industriales, de investigación, técnicos, informáticos o proyectos de Tecnología de Información (TI) entre otros; esta diversidad ha llevado a que algunos investigadores sugieran la existencia de una Teoría de Proyectos, donde se conjugue el aspecto práctico y de acción de la experiencia. El termino proyecto, según el Diccionario de la Real Academia Española, se define como "Planta y disposición que se forma para un tratado, o para la ejecución de una cosa de importancia, anotando y extendiendo todas las circunstancias principales que deben concurrir para su logro." (RAE, 1992), según el Diccionari de la Llengua Catalana del Intitut d'Estudis Catalans, es "Allò que hom pensa portar a acompliment; pla propossat per a realitzar-ho; estudi detallat d'una cosa realitzar." (IEC, 1995), para el Diccionario Oxford, es "Make plans for" (Hornby, 1974).

Se pueden ver los proyectos como consecución de objetivos "Un proyecto es una secuencia única de actividades complejas e interconectadas que tienen un objetivo o propósito que debe ser alcanzado en un plazo establecido, dentro de un presupuesto y de acuerdo con unas especificaciones" (Ribera, 2000). "A temporary endeavor undertaken to create a unique product or service" (PMI, 1996). "Assemblage of resources to solve a one-of-a-kind problem" (Jurison, 1999). Las diferencias conceptuales o epistemológicas sobre lo que es un proyecto han llevado a hablar de una Teoría de Proyectos, así, Gómez-Senent et. al (1996) han planteado que el conocimiento sobre proyectos se puede organizar en tres niveles, los cuales son de menor a mayor abstracción, y de mayor a menor volumen de aportaciones conceptuales.

En todo proyecto y en especial en los proyectos de TI, la seguridad de la información (NTC ISO/IEC 27001, 2006) es un elemento fundamental para el logro de los objetivos propuestos. La gestión de riesgo de TI tiene relación directa con el concepto de Sistemas de Gestión de la Seguridad de la Información (SGSI), esto involucra el estudio de la familia de normas ISO 27000. El modelo de gestión es un esquema o marco de referencia para la administración de una entidad, los cuales pueden ser aplicados tanto en las empresas privadas como públicas o en proyectos particulares.

La información es fundamental como estrategia para el crecimiento sostenido y sustentable. Por tanto, es importante

gestionar estratégicamente el desarrollo de capacidades tecnológicas (Carroz, 2005), a partir de la detección e implementación de actividades relacionadas; entre otras, la negociación, adquisición, asimilación y adaptación de tecnología. Logrando conceptualizar el crecimiento sostenido y sustentable, en aquellos procesos mediante el cual se diseñe políticas de orden económico, social, fiscal, comercial, energético, agrícola e industrial que conduzcan a un desarrollo sostenido en lo económico, social y ecológico.

La Seguridad de la Información (NTC ISO/IEC 27002, 2007) consiste en la preservación de la confidencialidad, la integridad y la disponibilidad de la información. Cuando se habla de seguridad de la información en los proyectos se piensa irremediablemente en la manera de identificar y combatir los riesgos a la que se somete permanentemente. Riesgo es la probabilidad de que una amenaza cause un impacto, siendo la Amenaza la causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización; estas amenazas pueden impactar cualquier activo. Se considera Activo a cualquier cosa que representa o que tiene un valor para la organización, los cuales pueden presentar vulnerabilidades que permiten ser aprovechadas por las amenazas para ser impactados. La Vulnerabilidad hace referencia a la debilidad de un activo o grupo de activos que pueden ser aprovechadas por una o varias amenazas.

3. METODOLOGÍA

Teniendo en cuenta todos los principios descritos anteriormente se plantea la Gestión del Riesgo de Proyectos de Tecnologías de la Información (TI) como parte del desarrollo del proyecto para cumplir con el objetivo propuesto del diseño de un Modelo de Gestión un esquema o marco de referencia para la administración de proyectos. Para el modelo planteado, se hace necesario realizar un Análisis, Evaluación, Valoración y Tratamiento del riesgo; de esta manera, en el proyecto cuando se habla de un Control se hace referencia a los medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal. Cabe aclarar, que aplicar un control no es sinónimo de eliminación total del riesgo, esto conlleva contemplar el concepto de Riesgo Residual el cual describe el nivel restante de riesgo después del tratamiento del riesgo (NTC ISO 31000, 2011). La investigación se enmarca dentro de un enfoque descriptivo.

4. RESULTADOS

El proceso de gobernabilidad de una empresa (COBIT, 2003), se refiere al conjunto de responsabilidades y prácticas ejecutadas por el comité directivo de la misma, con el objetivo de proveer dirección estratégica a la compañía, asegurando que los objetivos definidos sean alcanzados, verificando que los riesgos sean administrados apropiadamente y que los recursos sean utilizados responsablemente. Inspirados en diversos elementos como: el modelo inter-empresa de Santana (Santana, 2008), los conceptos de madurez y los objetivos de control (COBIT 4.0, 2006), se diseñó un marco conceptual de Gobernabilidad de TI (Velásquez, 2010) donde se identifican los principales componentes de la organización y las

maneras en que estos componentes trabajan juntos con el fin de alcanzar los objetivos del negocio. Los componentes o niveles, comprenden procesos de modelado de negocios, arquitectura de SI/TI, Aplicativos de apoyo, y Tecnologías de Información y Comunicación.

Cumpliendo con el marco contextual, el cual aplica desde el punto de vista de Gobernabilidad de TI al área de Estrategias de TI y Arquitectura de TI, se contemplaron los resultados anteriores obtenidos en el cumplimiento de controles a nivel estratégico y de gestión de riesgo de TI, respectivamente. Como resultado del análisis se obtuvo dos estrategias principales: La definición del plan estratégico (estrategia E1) y el diseño de un modelo de gestión de riesgos de proyectos de TI (estrategia E2). De acuerdo a lo anterior, se desarrolló el plan estratégico de TI (cuyo alcance contempló las dos estrategias mencionadas), basado en las buenas prácticas de COBIT 4.1 en su objetivo de control PO1 (definir el plan estratégico de TI), PO9 (evaluar y administrar riesgos de TI), PO10 (Administración de proyectos).

Complementando este estudio se implementó la metodología PMBOK como buenas prácticas para la gestión de proyectos propuesta por PMI (Project Management Institute), para la planeación de la gestión del proyecto de diseño del modelo de gestión de riesgo de TI. Igualmente, como verificación al cumplimiento de la gestión del proyecto se realizó una auditoría basada en los requerimientos propuestos por las buenas prácticas de PMBOK identificando los riesgos y recomendaciones necesarias.

Los elementos del modelo de gestión de riesgos de proyectos de TI (Ver Figura 1) se definieron enfocadas desde tres puntos de vista estratégico, táctico y operativo. El estratégico con el componente de gobernanza en cuanto a las estrategias, metas y objetivos, políticas y procedimientos; el táctico todo lo correspondiente a gestión de riesgos y en el operativo todo lo correspondiente al cumplimiento con sus procesos, controles y actividades. Se definen los elementos del modelo de acuerdo a la normatividad y buenas prácticas mencionadas tomando el Ciclo PHVA de Deming (Planear, Hacer, Verificar, Actuar), en cada una de sus etapas.

Figura 1. Modelo de gestión de riesgos de Proyectos de TI

Se aplica la normatividad y buenas prácticas a nivel estratégico con NTC ISO/IEC 27001; en el nivel táctico NTC ISO/IEC 27002 y NTC ISO/IEC 27005 y en el nivel operativo con NTC ISO 31000 y NTC 5254, siendo COBIT y PMBOK transversal en cada elemento.

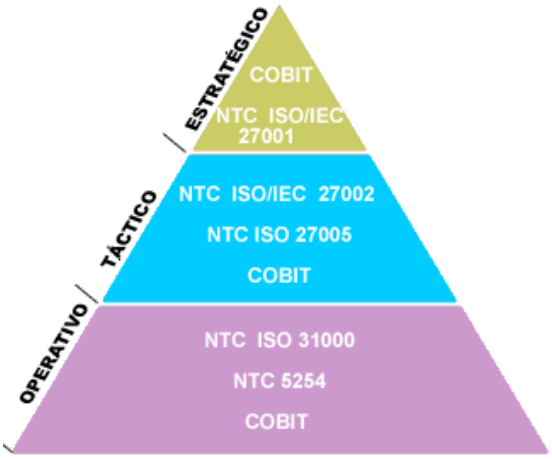

Figura 2. Normograma de Gestión de Riesgos de TI

El proceso de Gestión de Riesgos debe ser documentado en forma apropiada, esta documentación debe incluir los métodos, fuentes de datos y resultados. Se define un modelo documental (Ver Figura 3) a nivel estratégico, táctico y operativo que incluye: La definición de la política y objetivos del modelo, su definición del alcance, la descripción de los elementos, relación y referencia de documentos, la definición de los documentos y registros del Modelo.

Figura 3. Modelo documental

Para el modelo se utiliza nomenclatura (Ver Tabla 1) Dentro de los formatos, procedimientos y registros contemplados para el modelo de gestión de riesgos de TI[1].

Tabla 1. Nomenclatura modelo documental

PGR	Política de Gestión de Riesgo de TI
PE	Plan Estratégico de TI
PMC	Plan de mejora continua
PGRTI	Proceso de Gestión de Riesgos de TI
PA	Plan de Auditoría
PCC	Plan de Comunicación y consulta

5. CONCLUSIONES

Dentro de la línea de investigación Gobernabilidad de TI, la cual busca el alineamiento de la tecnología de información con la misión, visión y objetivos del negocio o direccionamiento estratégico, se definen áreas de aplicación para la especialización como Arquitectura o Estrategias de TI. El proyecto contribuye con una Arquitectura, la cual cumple con los controles a nivel estratégico y de gestión de riesgo de TI, respectivamente. Resultado del análisis se presenta como estrategia el diseño de un modelo de gestión de riesgos de proyectos de TI.

El modelo diseñado genera una directriz para la gestión de riesgo de los proyectos de TI desarrollados en la Universidad Francisco de Paula Santander Ocaña, tanto a nivel

1 Procedimiento de Valoración y Evaluación de Riesgos de TI **PVER**, Plan de tratamiento de riesgo de TI **PTR**, Procedimiento de reporte de riesgo de TI **PRR**, Procedimiento de Gestión de riesgos de TI **PRC**, Formato de reporte de Riesgos de TI **FRR**, Base de datos **BD**, la Matriz de riesgos, el Inventario de Activos **INVA** y el Inventario de Amenazas **INAM**.

interno como para aquellos que se plantean hacia la comunidad; esto contribuye con una adecuada Gestión de proyectos.

Para el desarrollo del proyecto se incorporaron estándares, modelos o buenas prácticas, estableciendo como directrices el marco conceptual de Gobernabilidad de TI, la Gestión de Proyectos de TI, Objetivos de Control de TI y Sistemas de gestión de la seguridad de la información. Esto permite el cumplimiento de objetivos de control que repercuten en unos niveles de madurez más avanzados.

Se integran como elementos del modelo de gestión de riesgos de proyectos de TI enfoques desde el punto de vista estratégico, táctico y operativo, en conjunto a la aplicación del ciclo PHVA (Planear, Hacer, Verificar, Actuar), en cada una de sus etapas, aplicando la normatividad y buenas prácticas de seguridad de la información contempladas en la NTC ISO/IEC 27001, NTC ISO/IEC 27002, NTC ISO/IEC 27005, NTC ISO 31000, NTC 5254, COBIT y PMBOK.

Este proyecto contribuye con los lineamientos descritos en el proyecto "Establecimiento de criterios de gobernabilidad de TI", desarrollados por el Grupo de Investigación de Tecnología y Desarrollo en Ingeniería (GITYD). Aplicando este modelo propuesto en los diferentes tipos de empresas, donde se implemente el marco conceptual de gobernabilidad de TI como lineamiento para avanzar en los niveles de madurez.

6. RECOMENDACIONES

El paso siguiente es la validación del modelo planteado, para lo cual se propone la incorporación del mismo en los trabajos desarrollados de laboratorio de auditoría dentro de la especialización; aplicándolo tanto en Gestión de proyectos como en Auditoria al desarrollo de proyectos de Ingeniería. Se puede ir validando el modelo teniendo en cuenta los diferentes sectores de empresa que se manejan en la línea de investigación el sector bancario, educativo, penitenciario y salud, lo que permitirá ir refinando el modelo y establecer si es adaptable a cualquier sector.

7. BIBLIOGRAFÍA

Acosta Portillo, D., Alvarez Prada, I., Camargo Barbosa, J., & Nuñez Ascanio , K. (2013). DISEÑO DE UN MODELO DE GESTIÓN DEL RIESGO DE TECNOLOGÍAS DE INFORMACIÓN PARA LA UNIDAD DE CONTABILIDAD DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER. Ocaña: Universidad Francisco de Paula Santander Ocaña.

COBIT, GovernanceInstitute Modelo ExecutiveSummary. [Versión electrónica] Extraído el 20 de Diciembre, 2008, desde http://www.isaca.org/cobit.html, 2003

COBIT 4.0, Governance IT. [Versión electrónica] Extraído el 3 de Enero, 2009 del sitio Web del Institute, Borrad briefingon TI governance: http://www.itgi.org/Template_ITGI.cfm?Section=ITGI&Template=/Conte

ntManagement/ContentDisplay.cfm, 2006

COBIT 4.1, IT Governance. Control Objectives for Information and Related Technology. IT Governance Institute. United States of America. 2007.

Carroz D. Web . Modelo de Gestión Estratégico para el desarrollo de capacidades tecnológicas. [Versión electrónica] Extraído el 5 de diciembre, 2012 del sitio. http://www.ucla.edu.ve/dac/compendium/Revista15/DCarroz.pdf. 2005

Estay, Christian; y, Blasco, Jaume. Los Sistemas de un Proyecto. En electronic Proceedings IV International Congress of Project Engineering. Córdoba España:Universidad de Córdoba. Octubre 7-9. pp. 166-173. 1.998

Goméz-Senentt, Eliseo; Chiner, Mercedez; Capuz R., Salvador; Aragones, Pablo; y, Santamaría, José Luis. ¿Es el proyecto un Sistema? En Proceedings III International Congress of Project Engineering. Barcelona, Terrasa. Departament de Projectes de l'Enginyeria. Universitat Politécnica de Catalunya. Septiembre 12-14. pp. 131-140. 1.996.

Hornby, A. S.. Oxford Advanced Learnr's Dictionary of Curren English. Oxford University Press. 1055 pp. 1.974

IEC. Diccionari de la Llengua Catalana. Intitut d'Estudis Catalans. Enciclopèdia Catalana, S. A. i Editorial 62, S. A. Publicacions de L'Abadia de Montserrat, S. A. 1908 pp. 1.995

NTC ISO/IEC 27001. INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Tecnología de la Información. Sistema de Gestión de Seguridad de la Información (SGSI). Bogotá D.C.: ICONTEC, 2006.

NTC ISO/IEC 27002. INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Código de las Buenas Prácticas para la Gestión de la Seguridad de la Información. Bogotá D.C.: ICONTEC, 2007.

NTC ISO 31000. INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Gestión del Riesgo. Principios y Directrices. Bogotá D.C.: ICONTEC, 2011.

Jurison, Jakk.. Software project management: the manager's view. Communications of the AIS, 2(17). September. http://casi.aisnet.org. 1.999.

PMBOK. Guía de los Fundamentos para la Dirección de Proyectos. Project Management Institute. Cuarta Edición. EE.UU. 2008.

PMI.. Project Management Institute Standards committee. A guide to the Project Management Body of Knowledge. 176 pp. 1.996

RAE.. Diccionario de la Real Academia de la Lengua Española. Madrid-España. 1.992

Ribera, J. L. (2000). Project Management. MBA Course IESE, Universidad de Navarra (Spring 2000). http://web.iese.edu/ribera/. Leído el 21/6/2000.

SANTANA, M. Validating Adequacy and Suitability of Business-IT Alignment Criteria in an Inter-Enterprise Maturity Model 2008

VELASQUEZ, T. Establecimiento De Criterios De Gobernabilidad De TI En Las Empresas Colombianas. Universidad de los Andes. Mérida. Venezuela. 2010.