Propuesta de guía de implementación de mejores prácticas en gestión de riesgos de tecnologías de información en universidades privadas

PROYECTO DE GRADO

Andrés Mauricio Posada Brícoli
Sergio Gómez Collazos

Asesor
Hernando Peña Villamil
Magíster en Teleinformática
Certificado PMP, ITIL, COBIT, ISO27001
Consultor de Gobierno de IT

FACULTAD DE INGENIERÍA
DEPARTAMENTO ACADÉMICO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES
MAESTRÍA EN GESTIÓN INFORMÁTICA Y TELECOMUNICACIONES
SANTIAGO DE CALI
2012

Propuesta de guía de implementación de mejores prácticas en gestión de riesgos de tecnologías de información en universidades privadas

Andrés Mauricio Posada Brícoli
Sergio Gómez Collazos

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

Asesor
Hernando Peña Villamil
Magíster en Teleinformática
Certificado PMP, ITIL, COBIT, ISO27001
Consultor de Gobierno de IT

FACULTAD DE INGENIERÍA
DEPARTAMENTO ACADÉMICO DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES
MAESTRÍA EN GESTIÓN INFORMÁTICA Y TELECOMUNICACIONES
SANTIAGO DE CALI
2012

Nota de aceptación

_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Santiago de Cali, Noviembre 12 de 2012

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

pág.

LISTA DE ANEXOS

pág.

RESUMEN

Las tecnologías de información o T.I. están cumpliendo un rol cada vez más importante en las organizaciones alrededor del mundo: la digitalización y automatización de sistemas críticos para la organización es un fenómeno que ha venido creciendo exponencialmente en los últimos años, lo cual ha hecho que las mismas sean cada vez más eficientes y productivas. Sin embargo, no hay tecnologías perfectas: todas presentan vulnerabilidades, errores o deficiencias, además que su administración es cada vez más compleja; por tanto, su implementación conlleva un gran riesgo. Esto es conocido como riesgo de T.I., y el no gestionarlo puede generar altos costos para la organización.

Teniendo en cuenta lo anterior, el entorno educativo no es la excepción. Los departamentos de TI de las instituciones privadas de educación superior en Cali tienen inconvenientes en su operación diaria; esto se debe a diversos factores, entre los cuales se encuentra una gestión inadecuada de riesgos de TI. El problema a tratar es que, a pesar que existen diversos conjuntos de marcos de referencia y metodologías para trabajar en la gestión de riesgos de TI, no existe una guía de implementación ajustada a las necesidades del sector. El objetivo es generar una propuesta de guía de implementación de mejores prácticas en gestión de riesgos de tecnologías de información en entidades privadas de educación superior.

Tras una búsqueda en fuentes confiables referente a marcos de trabajo, normas y guías metodológicas para la implementación de procesos de gestión de riesgos de TI en universidades privadas, no se encontró algún resultado significativo aplicado al sector que detalle la manera cómo éstas instituciones estén trabajando actualmente el tema. Por esta razón, el motivo de este trabajo es desarrollar una guía metodológica que proponga un proceso de gestión de riesgos de T.I. que permita la fácil implementación del mismo en las instituciones del sector, enmarcado en unas mejores prácticas.

1. INTRODUCCIÓN

1.1 CONTEXTO DEL TRABAJO

Es innegable la gran influencia que han tenido las tecnologías de información (TI) en las organizaciones. En la actualidad se evidencia que los rubros de inversión de TI se han incrementado, con el propósito de digitalizar y automatizar sistemas financieros y contables, aplicaciones de planificación de recursos empresariales (ERP, según sus siglas en inglés), sistemas de gestión humana y muchos otros elementos del negocio. Pocas firmas están en la capacidad de ignorar estos avances tecnológicos, debido a que esto conlleva perder ventajas competitivas frente a empresas rivales.
Debido a estos avances, la sociedad cada vez es más dependiente de las TI, las cuales se han convertido en el centro de las actividades de las organizaciones. Con el objetivo de mejorar su eficiencia y productividad, las empresas están entregando a TI cada vez una porción más grande de las responsabilidades críticas para el negocio. Sin embargo, no hay tecnologías perfectas: todas, en mayor o menor medida, presentan vulnerabilidades, errores o deficiencias, sin contar la gran complejidad que requiere administrarlas. Por tanto, su implementación en las empresas comprende un gran riesgo, pues los procesos de negocio están dependiendo cada vez más de ellas para operar. Lo anterior genera lo conocido como riesgo de TI; se hace necesario gestionar estos riesgos, pues el no hacerlo puede generar altos costos para la organización.[1]

De acuerdo a *Risk IT* (uno de los marcos de trabajo relacionados con el tema)[2], "el riesgo de TI se define como un riesgo del negocio; específicamente, es el riesgo de negocio asociado al uso, propiedad, operación, involucramiento, influencia y adopción de las TI en una empresa. Comprende eventos y condiciones relacionados con TI que puede afectar potencialmente al negocio. Puede tener una magnitud y frecuencia incierta y crea retos en el establecimiento de metas y objetivos estratégicos."

¿El manejo de riesgos de TI es relevante para las empresas? Claro que sí. De acuerdo a un estudio realizado por la Economist Intelligence Unit de The Economist[3], "el riesgo de TI es una de las amenazas más importantes para las operaciones comerciales de empresas de carácter global: un 48% de gerentes

[1] GÓMEZ, Ricardo; PÉREZ, Diego Hernán; DONOSO, Yesid; et. al. Metodología y gobierno de la gestión de riesgos de tecnologías de la información. En: Revista de Ingeniería. No. 31 (Ene.-Jun. 2010). Bogotá: Universidad de los Andes, 2010. 148 p. Semestral. ISSN 0121-4993. pp. 109-118.
[2] ISACA. The Risk IT Framework. 2009. Rolling Meadows, Illinois, Estados Unidos de América: ISACA, 2009. p. 7. ISBN 978-1-60420-111-6.
[3] THE ECONOMIST. Digital risk: The challenge for the CRO. s.l.: The Economist, 2005. p. 4

senior afirma que los riesgos de TI representan una amenaza alta o muy alta para sus negocios. Las TI son suficientemente importantes en más de un tercio de las firmas, por tanto requieren una supervisión mucho más cercana por parte de los presidentes ejecutivos (*CEO*, según sus siglas en inglés).” Esta preocupación frente a los diversos tipos de riesgo y en particular al riesgo de TI, se puede observar en la figura 1 que se ilustra a continuación.

Figura 1. Riesgos que representan amenazas para la operación de las organizaciones. (Traducido al español) Fuente: The Economist[4]

Como se puede observar en la imagen, el estudio realizado muestra que el riesgo de TI ocupa el segundo puesto entre los que más se percibe una amenaza alta o muy alta para las operaciones de los negocios.

Al igual que en otros sectores de la economía, en las universidades se perciben varias dificultades y falencias en el área de tecnología relacionados con los riesgos de tecnología: incumplimientos en los tiempos de entrega de los proyectos por no considerar riesgos que generan retrasos y reprocesos; la falta de alineación entre la identificación de riesgos de TI y los del negocio; la falta de un liderazgo en los temas de riesgos de TI y la incapacidad de no ver más allá de los riesgos inherentes a la operación diaria del área de TI, entre otros. Estos temas son de gran interés para las universidades y motivó a la búsqueda de un proceso que estuviese ajustado a las necesidades del sector y que permitiese responder rápida y eficientemente a los problemas de la operación que están asociados con los riesgos de TI.
Al buscar soluciones para este problema en las bases de datos académicas acreditadas en Colombia, se concluyó que no existen estudios de implementación de riesgos de TI en las universidades de la región.

[4] Ibid., p. 4

Teniendo en cuenta lo anterior, el trabajo a desarrollar se enfocará en las entidades educativas privadas de la región. El sector educativo y sus áreas de TI poseen ciertos elementos que lo caracterizan:

- Por ley, son instituciones sin ánimo de lucro, por tanto su objetivo principal no es generar utilidades.
- La infraestructura tecnológica de los planteles no tiene la criticidad de estar en línea venticuatro horas al día y siete días a la semana, como en entornos del sector industrial.
- Los servicios ofrecidos por el área de TI usualmente están enfocados hacia la comunidad académica (profesores y estudiantes).
- Apoyan muchos de sus procesos académico-administrativos vitales en los servicios ofrecidos por el área de TI.
- Tiene un período específico cada semestre en el que se ejecuta un proceso crítico: matrícula académica y financiera. Otros procesos críticos en otro tipo de organizaciones (cierres, por ejemplo) no tienen la relevancia en este sector.
- Manejan un volumen de información inferior en comparación a otro tipo de organizaciones.

El sector es interesante ya que la educación y las TICs son áreas estratégicas del plan de competitividad de país. En específico, el gobierno reconoce la relevancia de las TIC y considera importante que en el sector educativo se refuerce este componente: "El Gobierno nacional consolidará a las TIC como plataforma tecnológica para mejorar la cobertura, la calidad y la pertinencia de los procesos educativos, fortalecer la fuerza laboral en el uso de las TIC y promover la generación y uso de contenidos educativos"[5]. Además, como lineamientos del Ministerio de Educación, en el apartado de "Cinco acciones que están transformando la educación en Colombia" aparece como cuarto elemento "Una educación que incorpora mejores prácticas de gestión en todos los niveles del sistema, con herramientas adecuadas e innovadoras, capaz de responder a las expectativas del país"[6]. Con esta investigación se apoyarán estas iniciativas del gobierno, haciendo que las TIC en las entidades de educación superior sean más eficientes y efectivas; permitiendo de esta manera nuevos y mejores servicios para la comunidad universitaria y el público en general.

1.2 PLANTEAMIENTO DEL PROBLEMA

Hoy en día, los departamentos de TI de las universidades privadas en Cali tienen inconvenientes en su operación diaria, debido en parte a una gestión inadecuada de riesgos de TI. El problema a tratar es que, a pesar que existen diversos

[5] COLOMBIA, DEPARTAMENTO NACIONAL DE PLANEACIÓN. III. Crecimiento sostenible y competitividad [En línea]. <http://www.dnp.gov.co/LinkClick.aspx?fileticket=6yjofaugVUQ%3D&tabid=1238> [citado en 1 de abril de 2012]

[6] COLOMBIA. MINISTERIO DE EDUCACIÓN. Cinco acciones que están transformando la educación en Colombia. [En línea]. <http://www.mineducacion.gov.co/1621/propertyvalue-40524.html> [citado en 1 de abril de 2012]

conjuntos de marcos de referencia para trabajar en la gestión de riesgos de TI, no existe un modelo de implementación ajustado a las necesidades del sector.

1.3 OBJETIVOS

1.3.1 Objetivo General

Generar una propuesta de guía de implementación de mejores prácticas en gestión de riesgos de tecnologías de información en universidades privadas.

1.3.2 Objetivos Específicos:

- Realizar el levantamiento y síntesis de la información sobre manejo de riesgos de TI en las universidades privadas, aplicando una encuesta a partir del estudio de los marcos de referencia.

- Comparar los marcos de referencia de gestión de riesgos de tecnología más importantes y generar un listado de las características más importantes.

- Generar la propuesta de guía de implementación de mejores prácticas en gestión de riesgos de TI, definiendo los pasos y las herramientas adecuadas a las necesidades y particularidades de las universidades privadas.

- Validar a través de una mesa de expertos la pertinencia de la guía de implementación.

1.4 RESUMEN DEL MODELO PROPUESTO

En este proyecto se propuso una guía de implementación de gestión de riesgos de T.I., basada en un marco común de mejores prácticas ofrecidas por los marcos de trabajo y normas de referencia de mayor uso a nivel mundial y nacional, adaptado al ámbito universitario.

Para la guía se desarrollaron seis procesos, los cuales se componen a su vez de actividades y tareas. La relación entre los mismos se ilustra de manera global en la figura 2.

A continuación se hace un breve recuento de cada uno de los procesos y sus componentes principales.

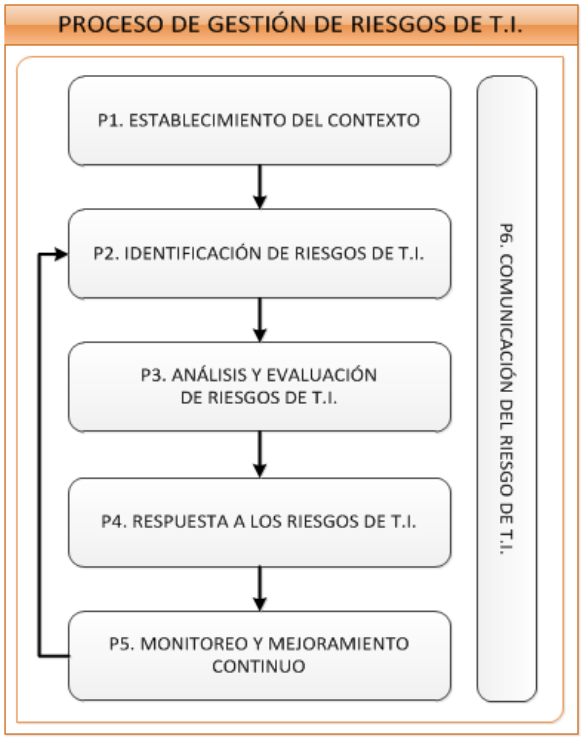

Figura 2. Procesos de gestión de riesgos de T.I. propuesta
Fuente: Propia

- **Proceso P1: Establecimiento del contexto**

En este proceso se busca contextualizar la institución dentro de lo que será el proceso de gestión de riesgos de tecnología que se implementará en la institución. El director del área de T.I. deberá de manera concisa definir el alcance, los objetivos y beneficios que la gestión de riesgos de tecnología traerá a la institución, enmarcado en los objetivos estratégicos de la misma. Posteriormente, deberá presentar la propuesta de implementación de la gestión de riesgos de T.I. al comité directivo de la institución, con el objetivo de socializarlo y obtener su aprobación.

Después de contar con el apoyo de la gerencia, se debe definir el usuario líder del proceso y crear el grupo que trabajará durante todo el proceso de implementación. Finalmente, se define el conjunto de servicios de T.I. de la organización y los criterios con los que se clasificarán los riesgos de T.I., los cuales deberán ser puestos a consideración del comité directivo para su revisión y aprobación.

Este proceso se compone de las actividades y tareas descritas a continuación.

Actividad A1.1: Iniciar el proceso.	Esta actividad pretende establecer los objetivos, el alcance y la justificación del proceso de gestión de riesgos de T.I. Esta actividad contiene la siguiente tarea: *Tarea T1.1.1*: Establecer el alcance, los objetivos y la justificación del proceso de gestión de riesgos de T.I.
Actividad A1.2: Obtener aprobación y compromiso por parte del comité directivo.	Esta actividad busca obtener la aprobación de la implementación del proceso de gestión de riesgos de T.I. por parte del comité directivo, como también su apoyo y compromiso hacia el mismo. Esta actividad contiene la siguiente tarea: *Tarea T1.2.1*: Obtener aprobación y compromiso por parte del comité directivo
Actividad A1.3: Socializar y definir interesados del proceso.	Esta actividad busca socializar a la comunidad universitaria los beneficios esperados que se derivarán de la implementación de una gestión de riesgos de T.I., para lograr de esta manera un entendimiento básico del esfuerzo a emprender y un apoyo de la gente en caso que se requiera su colaboración a lo largo de la ejecución del proceso. De igual manera, en esta actividad se debe definir un usuario líder del proceso. Se propone la conformación de un grupo de trabajo (denominado GARTI), el cual será el responsable del buen funcionamiento del proceso de gestión de riesgos de T.I. Esta actividad contiene las siguientes tareas: *Tarea T1.3.1*: Socializar a la comunidad el proceso *Tarea T1.3.2*: Definir líder del proceso *Tarea T1.3.3*: Definir el grupo de trabajo de gestión de riesgos de T.I. – GARTI
Actividad A1.4: Definir los criterios de análisis de riesgos de T.I.	Esta actividad tiene como fin definir los criterios con los cuales serán listados y evaluados los riesgos de T.I. Estos criterios serán usados para determinar la prioridad de los riesgos y la manera de tratarlos. Esta actividad contiene las siguientes tareas: *Tarea T1.4.1:* Definir listado de servicios de T.I. *Tarea T1.4.2.* Definir criterios de probabilidad de ocurrencia del riesgo *Tarea T1.4.3.* Definir criterios de impacto del riesgo *Tarea T1.4.4.* Definir criterios para responder al riesgo de T.I. *Tarea T1.4.5.* Priorizar servicios de T.I. y aprobar criterios de probabilidad e impacto

Tabla 1. Actividades y tareas del proceso P1.
Fuente: Propia

- **Proceso P2: Identificación de riesgos de T.I.**

Este proceso tiene como objetivo identificar aquellos riesgos relacionados con T.I. que, al afectar los servicios prestados por T.I., puedan degradar o retardar la consecución de los objetivos de la organización.
Este proceso se compone de la siguiente actividad y tarea:

Actividad A2.1: Definir el conjunto de riesgos de T.I.	En esta actividad se define el conjunto de eventos relacionados con T.I. que podrán afectar el cumplimiento de los objetivos de la Universidad. Esta actividad contiene la siguiente tarea: *Tarea T2.1.1*: Definir conjunto de riesgos de T.I. a trabajar

Tabla 2. Actividades y tareas del proceso P2.
Fuente: Propia

- **Proceso P3: Análisis y evaluación de Riesgos de T.I.**

Este proceso busca identificar y evaluar los controles existentes frente a los riesgos identificados en el proceso anterior. De igual manera, determinar el impacto y la probabilidad de los riesgos, derivando de estos valores su prioridad.

Este proceso se compone de las siguientes actividades y tareas:

Actividad A3.1: Analizar y evaluar los riesgos de T.I.	En esta actividad se busca realizar la priorización de los riesgos hallados en el proceso anterior, de acuerdo a la probabilidad e impacto del mismo basándose en los criterios definidos en el proceso de establecimiento del contexto. De igual manera, se realiza revisión de controles ya aplicados para los riesgos de T.I. a evaluar, lo que permite verificar la efectividad de los mismos y priorizar aquellos que no tienen controles o los que no tienen controles efectivos. Esta actividad contiene la siguiente tarea: *Tarea T3.1.1:* Evaluación de los riesgos de T.I. *Tarea T3.1.2:* Listado y evaluación de controles existentes para los riesgos de T.I *Tarea T3.1.3:* Priorización de riesgos de T.I.

Tabla 3. Actividades y tareas del proceso P3.
Fuente: Propia

- **Proceso P4: Respuesta a los riesgos de T.I.**

Este proceso busca tomar decisiones sobre el grado y la naturaleza de los tratamientos requeridos y sus prioridades como también desarrollar e implementar planes de respuesta eficaces en términos de costos, con el objetivo de reducir las pérdidas potenciales y/o incrementar los beneficios.

Este proceso se compone de las siguientes actividades y tareas:

Actividad A4.1: Definir los planes de respuesta a los riesgos de T.I.	En esta actividad se escoge el responsable de la ejecución de las *acciones* definidas y la respuesta o respuestas que se deben ejecutar para tratar el riesgo de T.I. Esta actividad contiene las siguientes tareas: *Tarea T4.1.1:* Asignar responsables de los planes de respuesta de los riesgos *Tarea T4.1.2:* Diseñar los posibles planes de respuesta a los riesgos de T.I. *Tarea T4.1.3.* Escoger y priorizar los planes de respuesta *Tarea T4.1.4.* Planear los planes de respuesta a los riesgos de T.I.
Actividad A4.2: Ejecutar los planes de respuesta a los riesgos de T.I.	Cada plan que fue planeado y aprobado en la tarea previa inicia su ejecución. Esta actividad contiene la siguiente tarea: *Tarea T4.2.1:* Ejecutar los planes de respuesta a los riesgos

Actividad A4.3: Monitorear la ejecución del proceso.	Esta actividad busca monitorear la eficacia de la ejecución de las actividades planeadas para dar tratamiento a los riesgos de T.I. identificados. Esta actividad contiene la siguiente tarea: *Tarea T4.3.1:* Revisión periódica del avance de la ejecución de los planes de respuesta a los riesgos

Tabla 4. Actividades y tareas del proceso P4.
Fuente: Propia

- **Proceso P5: Monitoreo y mejoramiento continuo**

Este proceso busca evaluar la eficacia del proceso de gestión de riesgo de T.I., con miras a que cumpla con los objetivos establecidos y se adapte de acuerdo a los cambios del entorno. El objetivo es aplicar una mejora continua sobre el proceso, teniendo en cuenta las lecciones aprendidas con cada iteración del mismo en la institución y las propuestas de cambio que surjan dentro del grupo.

Este proceso se compone de la siguiente actividad y tareas:

***Actividad A5.1: Mejorar continuamente el proceso*.**	Esta actividad busca que, con cada iteración del proceso de gestión de riesgos de T.I. establecido, queden documentadas las lecciones aprendidas a lo largo del mismo. De igual manera se recogen las propuestas de cambio al proceso, se evalúan y se llega a un consenso para realizar las modificaciones pertinentes. Esta actividad contiene las siguientes tareas: *Tarea T5.1.1:* Consolidación de lecciones aprendidas del proceso *Tarea T5.1.2:* Evaluación de modificaciones al proceso

Tabla 5. Actividades y tareas del proceso P5.
Fuente: Propia

- **Proceso P6. Comunicación del riesgo de T.I.**

El proceso de comunicación del riesgo de T.I. propuesto por esta metodología es un proceso transversal a todos los procesos de la misma. Tiene como objetivo mantener una comunicación adecuada y efectiva entre los interesados del proceso de gestión de riesgos de T.I., y así poder cumplir con las actividades propuestas en la metodología. Este componente está inmerso a lo largo de los otros procesos de la guía propuesta de gestión de riesgos de T.I.

Un punto importante de este proceso es concienciar a la gerencia que la gestión de los riesgos de T.I. es un proceso importante de la organización y no debe ser considerado como un esfuerzo menor y aislado del área de tecnología, sino un componente estratégico que permitirá apoyar la consecución de los objetivos de la institución.

Este proceso se compone de las siguientes actividades y tareas:

Actividad A6.1: Promover una comunicación efectiva del proceso de gestión de riesgos de T.I.	La idea de esta actividad es manejar comunicaciones efectivas en las actividades del proceso de gestión de riesgos. Para esto se han definido un conjunto de tareas de comunicación a lo largo de los procesos (que están representadas en las tareas T6.1.1 y T6.1.2) y una tarea de generación de un informe gerencial, que establezca el estado actual del proceso para mantener informado al comité directivo de la institución. Esta actividad contiene las siguientes tareas: *Tarea T6.1.1:* Comunicaciones del proceso con la gerencia *Tarea T6.1.2:* Comunicaciones del proceso con la comunidad universitaria *Tarea T6.1.3:* Informar a la gerencia del estado del proceso de gestión de riesgos de T.I.

Tabla 6. Actividades y tareas del proceso P6.
Fuente: Propia

- **Herramientas**

Con base en la guía anterior, se definió un conjunto de plantillas para cada una de las etapas definidas en el proceso.

- *GRTI-00: Listado de servicios de T.I.* Tiene como propósito definir un listado de los servicios de T.I estableciendo para cada uno de estos su responsable asociado, así como la criticidad y prioridad de acuerdo a los objetivos de la universidad.
- *GRTI-01: Universo de riesgos de T.I.* En esta plantilla se identifican y categorizan los posibles riesgos asociados a los servicios de T.I., como también su priorización inicial de acuerdo a la prioridad del servicio asociado.
- *GRTI-02: Análisis de riesgos de T.I.* Para cada riesgo del conjunto de riesgos, se procede a diligenciar sus causas, consecuencias, probabilidad de ocurrencia e impacto. Con esta información se obtiene una evaluación inicial, la cual en conjunto con la efectividad de los controles existentes para el riesgo y los criterios de probabilidad e impacto finales, permite obtener una evaluación y priorización final del riesgo.
- *GRTI-03: Respuesta a los riesgos de T.I.* En esta plantilla se documenta, para los riesgos resultantes del proceso de análisis, cuales son las opciones de manejo definidas para dar tratamiento al riesgo, así como el responsable de la ejecución de dichas acciones. Después se define la prioridad de dichas acciones, dependiendo de la factibilidad y viabilidad de las mismas, y se asigna una fecha programada de ejecución.
- *GRTI-04: Seguimiento al plan.* En esta plantilla se documenta el seguimiento a la ejecución de las acciones planteadas para dar tratamiento a los riesgos. También se recopilan las lecciones aprendidas sobre la ejecución de las acciones de tratamiento.
- *GRTI-05: Mejoramiento continuo.* En esta plantilla se documentan las lecciones aprendidas sobre los procesos, actividades y tareas del proceso de gestión de riesgos implementado en la institución, así como los cambios propuestos al mismo con sus justificaciones respectivas.

1.5 RESUMEN DE RESULTADOS OBTENIDOS

La guía propuesta de implementación de buenas prácticas de gestión de riesgos de T.I. se expuso a juicio de expertos con el objetivo de validar el proceso de gestión de riesgos de T.I propuesto. Para esto, se definió un perfil de evaluadores el cual permitió identificar y enviar vía correo electrónico la participación en la validación a seis personas que cumplían con el perfil.

Se obtuvieron por parte de dicha evaluación algunas observaciones de mejora sobre algunas tareas de los subprocesos, las cuales fueron tenidas en cuenta y se aplicaron sobre los mismos.

Finalmente, se puede concluir que como resultado de la validación, el proceso es relevante, coherente y claro; tanto a nivel general como a nivel de los subprocesos de establecimiento de contexto, identificación de riesgos, análisis de riesgos, evaluación de riesgos, tratamiento del riesgo, monitoreo y revisión, así como comunicación y consulta.

1.6 ORGANIZACIÓN DEL DOCUMENTO

Este documento se compone de seis capítulos. El primer capítulo muestra la introducción, en donde se plantea el contexto de trabajo, el planteamiento del problema, los objetivos generales y específicos, se resume el modelo propuesto y los resultados obtenidos. El segundo capítulo contiene la información referente al marco teórico, donde se hace un resumen y un comparativo de los documentos técnicos en los cuales se basa esta propuesta de guía, además de los resultados de la encuesta del estado del arte aplicada a las universidades. El tercer capítulo contiene el desarrollo de la guía propuesta de implementación de mejores prácticas en gestión de riesgos de T.I. en universidades privadas. Posteriormente se encuentra el capítulo cuarto donde se describe la validación de la propuesta usando el juicio de expertos, dando paso al capítulo quinto donde se ilustran los resultados del juicio de expertos. Finalmente se encuentra el capítulo seis, donde se encuentran las conclusiones y el trabajo futuro.

2. MARCO TEÓRICO

Las organizaciones se están volviendo cada vez más dependientes de las TI, las cuales se han convertido en el centro de las actividades de las organizaciones. Con el objetivo de mejorar su eficiencia y productividad, las empresas están entregando a TI cada vez una porción más grande de las responsabilidades críticas para el negocio, sistematizando cada vez más sus procesos internos.
Como lo comentan Fernández y Llorens en su trabajo "Gobierno de las TI para universidades"[7], "las organizaciones deben gestionar el riesgo que en un momento dado pueda afectar e impactar negativamente en sus actividades y procesos, lo cual pondría en peligro la consecución de sus objetivos. En el ámbito de las TI, es necesario analizar cómo preservar el valor del negocio a través de la seguridad que les proporcione las TI para proteger sus activos, conservar la continuidad de los servicios y recuperarlos después de un desastre. Pero al diseñar sus estrategias futuras también deben evaluar los nuevos riesgos que aparecen a partir de la incorporación de las TI en los procedimientos y estrategias de la organización."
Teniendo en cuenta la importancia que posee el tema de gestión de riesgos, se han elaborado diversos marcos de trabajo y metodologías que pretenden atacar este problema. Para la elaboración de la guía de implementación propuesta, se tomó como base y referencia tres normas técnicas (ISO 27000, ISO 31000 y NTC 5254), dos marcos de trabajo (Risk IT de ISACA y el Risk Management Framework de EDUCAUSE) y una metodología (MAGERIT). A continuación se encuentra la información general de cada una de estas referencias.

2.1 BASES DEL PROYECTO

2.1.1 Familia de estándares ISO 27000

La Organización Internacional para la Estandarización (ISO por sus siglas en inglés)[8] "es el desarrollador más grande del mundo de estándares internacionales voluntarios. Estos estándares ofrecen el estado del arte de las especificaciones para productos, servicios y buenas prácticas, ayudando a hacer la industria más eficiente y efectiva. Desarrollados a través de un consenso global, los estándares ayudan a eliminar barreras para el intercambio internacional."
De este organismo se estudiaron dos estándares que conforman la familia ISO 27000: ISO 27001:2005 e ISO 27005:2008.

[7] FERNANDEZ MARTÍNEZ, Antonio y LLORENS LARGO, Faraón. Gobierno de TI para universidades. Madrid, España: Conferencia de Rectores de las Universidades (CRUE), s.f. p. 58.
[8] INTERNATIONAL ORGANIZATION FOR STANDARIZATION. About ISO – ISO [En línea]. <http://www.iso.org/iso/home/about.htm> [Citado en 4 de noviembre de 2012].

El estándar **ISO 27001:2005** es una norma que proporciona un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). Al adoptar la aproximación de procesos de este estándar (que comprende la aplicación de un sistema de procesos dentro de la organización, junto con la identificación e interacción de los procesos y su respectiva gestión) motiva a los usuarios a enfatizar la importancia de:

- Entender los requisitos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información;
- Implementar y operar controles para manejar los riesgos de la seguridad de la información;
- Monitorear y revisar el desempeño y la efectividad del SGSI; y
- Mejorar continuamente basándose en una medición objetiva.[9]

Este estándar adopta el modelo PHVA (planear-hacer-verificar-actuar), el cual es usado para estructurar todos los procesos del SGSI. En la figura 3 se ilustra cómo un SGSI toma como información base los requisitos de seguridad de información y las expectativas de las partes interesadas y, a través de las acciones y procesos necesarios, producen resultados de seguridad de información que cumplen estos requisitos y expectativas. De igual manera, la figura 3 ilustra los vínculos entre los procesos que componen este estándar.

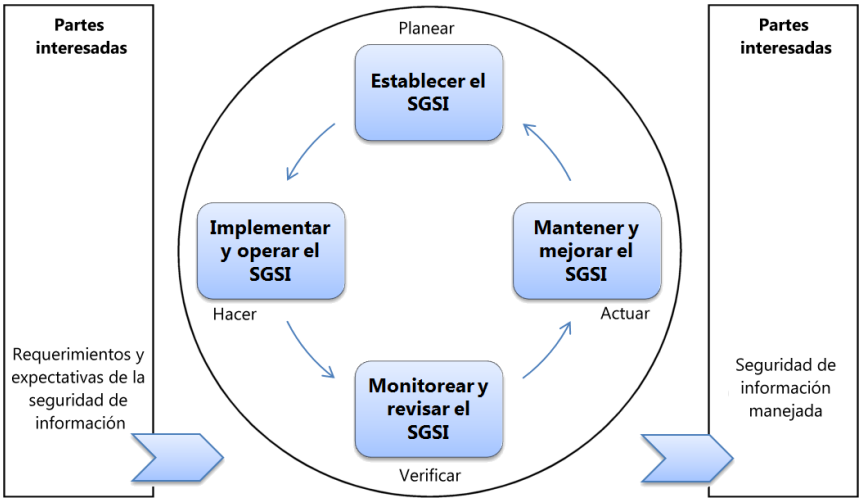

Figura 3. Modelo PHVA aplicado a los procesos del SGSI
(Adaptado al español) Fuente: ISO[10]

[9] INTERNATIONAL ORGANIZATION FOR STANDARIZATION. Information technology – Security techniques – Information security management systems – Requirements. Suiza: ISO, 2009. p. v. (ISO 27001:2005)
[10] Ibid., p. vi

A grandes rasgos se describe la relación entre el modelo PHVA y los procesos del SGSI en la tabla 7 que se encuentra a continuación.

Planear (Establecer el SGSI)	Establecer las políticas, los objetivos, los procesos y procedimientos del SGSI relevantes a la administración de los riesgos y el mejoramiento de la seguridad de la información, para entregar resultados de acuerdo a las políticas y objetivos generales de la organización.
Hacer (Implementar y operar el SGSI)	Implementar y operar las políticas, controles, procesos y procedimientos del SGSI.
Verificar (Monitorear y revisar el SGSI)	Evaluar y, donde aplique, medir el desempeño de los procesos de acuerdo a las políticas, objetivos y experiencia práctica del SGSI, y reportar los resultados a la administración para su evaluación.
Actuar (Mantener y mejorar el SGSI)	Tomar acciones correctivas y preventivas, basadas en los resultados de las auditorías del SGSI, revisiones de la gerencia u otra información relevante, para alcanzar un mejoramiento continuo del SGSI.

Tabla 7. Relación entre el modelo PHVA y los procesos del SGSI (Traducido al español). Fuente: ISO[11]

Un SGSI debe ser definido en términos de las características del negocio, su ubicación, activos y tecnología. Debe incluir un marco de trabajo que establezca los objetivos, una dirección común y unos principios para actuar con respecto a la seguridad de la información. De igual manera, debe tomar en cuenta requisitos legales y del negocio, debe cumplir con un contexto del riesgo estratégico de la organización y recibir la aprobación de la administración.

En su contenido, el SGSI debe contar con una propuesta para la evaluación del riesgo y una propuesta de administración del riesgo, que permita identificar los riesgos, analizarlos y evaluarlos, además de identificar y evaluar las posibles opciones para el tratamiento de los mismos.

El estándar **ISO 27005:2008** contiene la descripción de los procesos y actividades de la administración de riesgos de seguridad informática. Este estándar apoya los conceptos especificados en los estándares ISO/IEC 27001 e ISO/IEC 27002 y está diseñado para apoyar la implementación satisfactoria de esquemas de seguridad de la información en el enfoque de la administración de riesgos.

El estándar se basa en el principio que para identificar las necesidades de la organización con respecto a los requisitos de seguridad de la información de un sistema de administración de la seguridad de la información es necesario un enfoque sistemático para la gestión de riesgos de seguridad de la información

[11] Ibid., p. vi

(SGSI por sus siglas en ingles). Este enfoque debe ser adecuado para el entorno de la organización, y en particular, debe estar alineado con la gestión global de los riesgos empresariales. Los esfuerzos de seguridad deben abordar los riesgos de una manera eficaz y oportuna, donde y cuando se necesitan.

Según el estándar, la gestión de riesgos de seguridad de la información debe contribuir con los siguientes factores dentro de la organización:

- Los riesgos se identifican
- Los riesgos se evalúan en términos de sus consecuencias para la empresa y la probabilidad de su ocurrencia
- La probabilidad y las consecuencias de estos riesgos se comunica y entiende
- Se establece el orden de prioridad para el tratamiento del riesgo
- Prioridad de las acciones para reducir la ocurrencia de los riesgos
- Las partes interesadas están involucradas en tomas de decisiones de gestión de riesgos y se mantienen informados del estado de la gestión de riesgos
- Eficacia del seguimiento de los tratamientos de riesgos
- Los riesgos y el proceso de gestión de riesgos se monitorea y es revisado regularmente
- Se captura información para mejorar el enfoque de la gestión de riesgos
- Se forma a los administradores y el personal sobre los riesgos y las medidas adoptadas para mitigarlos

El estándar aclara que el proceso de gestión de riesgos de seguridad de la información puede aplicarse a una organización como un todo, una parte discreta de la misma (p. ej. Un departamento, una locación física, un servicio), cualquier sistema de información, aspectos de control existentes o planeados (p. ej. Planeación de la continuidad del negocio).

El estándar propone un proceso de gestión de riesgos de seguridad de la información, el cual es ilustrado en la figura 4 que se encuentra en la página siguiente.

Como se puede observar en la figura 4, el proceso de gestión de riesgos propone un establecimiento del contexto de los riesgos, luego una valoración de riesgos, luego un tratamiento de riesgos, luego una etapa de monitoreo y revisión la cual al igual que la etapa de comunicación y consulta son transversales a las demás fases.[12]

[12] INTERNATIONAL ORGANIZATION FOR STANDARIZATION. Information technology – Security techniques – Information security risk management ISO/IEC 27005. Suiza: ISO, 2008. p. 3. (ISO 27005:2008)

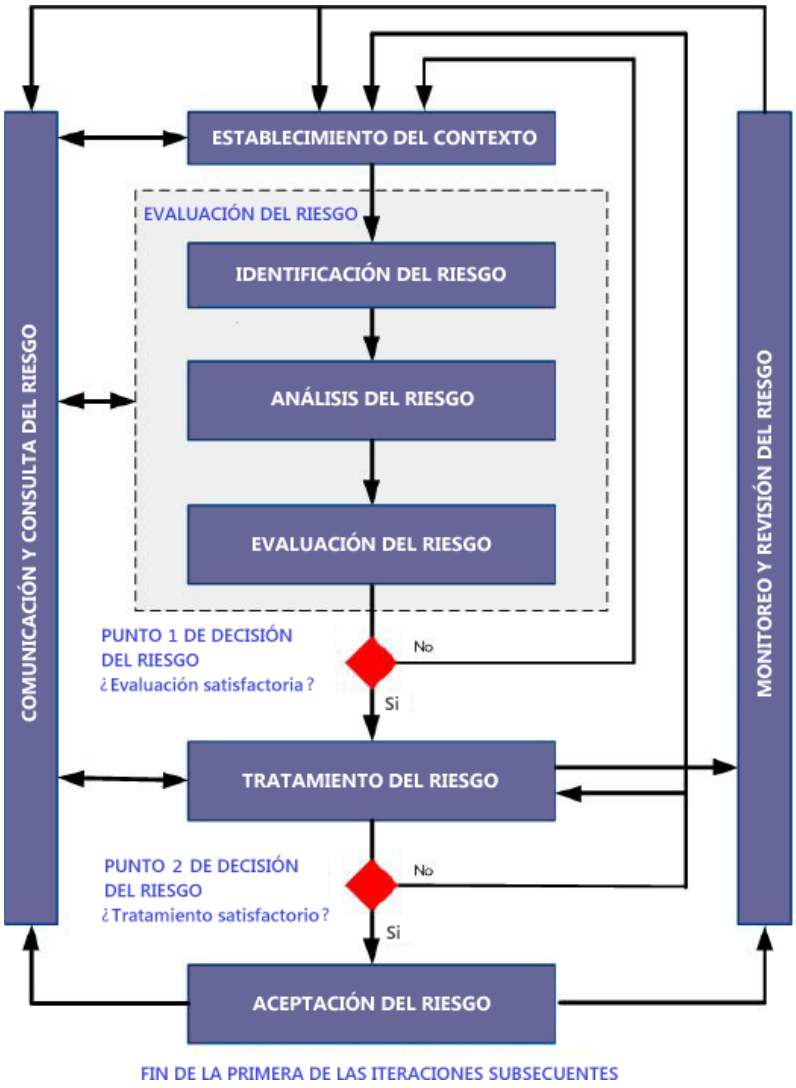

Figura 4. Proceso de gestión de riesgos de ISO 27005
(Traducido al español). Fuente: ISO[13]

A continuación se detalla a grandes rasgos los procesos propuestos por el estándar para la gestión de riesgos de seguridad de la información.

- *Establecimiento del contexto*

Este proceso tiene como finalidad apoyar a la organización en la definición del alcance y los limites de la gestión de riesgos de seguridad de la información.

El proceso se detalla a nivel macro a continuación.

[13] Ibid., p. 8

Entradas: Toda la información de la organización relevante al proceso de establecimiento del contexto de la gestión de riesgos.

Acciones: El contexto externo e interno para la gestión de riesgos de seguridad de información debe ser establecido, el cual consiste en fijar los criterios básicos necesarios para la gestión de riesgos de seguridad de información, definiendo el alcance y los límites, y el establecimiento de una organización apropiada para utilizar la gestión de riesgos de seguridad de la información

Salidas: La especificación de los criterios básicos, el alcance, los límites y la organización para el proceso de gestión de riesgos de seguridad de la información.

- *Evaluación de riesgos*

Un riesgo es una combinación de las consecuencias que podrían derivarse de la ocurrencia de un evento no deseado y la probabilidad de la ocurrencia del evento. La evaluación del riesgo cuantifica o describe cualitativamente el riesgo y permite a los administradores priorizar los riesgos en función de su gravedad percibida u otros criterios establecidos.
El proceso se detalla a nivel macro a continuación.

Entradas: Los criterios básicos, el alcance, los límites y la organización para el proceso de gestión de riesgos de seguridad de la información establecidos.

Acciones: Los riesgos deben ser identificados, cuantificados o descritos cualitativamente, y priorizados acorde a los criterios de evaluación del riesgo y objetivos relevantes para la organización.

Salidas: Una lista de los riesgos evaluados y priorizados de acuerdo a los criterios de evaluación de riesgos.

El estándar divide este proceso en las siguientes actividades:
- Identificación del riesgo
- Análisis del riesgo
- Evaluación del riesgo

- *Tratamiento del riesgo*

Este proceso busca dar tratamiento a todos los riesgos resultantes de la evaluación de riesgos, mediante cuatro opciones definidas por el estándar: modificación del riesgo, retención del riesgo, evitar el riesgo y compartir el riesgo.
El proceso se detalla a nivel macro a continuación.

Entradas: Una lista de los riesgos priorizados de acuerdo a los criterios de evaluación de riesgos en relación con los escenarios de incidentes que conducen a dichos riesgos.

Acciones: Se deben establecer controles para reducir, retener, evitar, o compartir el riesgo, así como un plan de tratamiento para los mismos.

Salidas: Plan de tratamiento de riesgos y los riesgos residuales sometidos a la decisión de aceptación de los directivos de la organización.

- *Aceptación del riesgo*

Este proceso revisa los planes de tratamiento de los riesgos y los riesgos residuales resultantes de aplicar los controles, definiendo y documentando niveles de aceptación para los riesgos que no cumplan con los criterios de aceptación de riesgos ya establecidos por la organización.
El proceso se detalla a nivel macro a continuación.

Entradas: Evaluación de planes de tratamiento de riesgos y riesgos residuales sujetas a la decisión de aceptación por parte de los administradores de la organización.

Acciones: La decisión de aceptar los riesgos y las responsabilidades de la decisión se efectúan y se guardan en registros documentando las mismas (esto acorde a ISO/IEC 27001:2005 párrafo 4.2.1 h)

Salidas: Una lista de riesgos aceptados con sus justificaciones para aquellos que no cumplen los criterios de aceptación de riesgos de la organización.

- *Comunicación y consulta*

La comunicación de riesgos es una actividad que busca lograr un acuerdo sobre la forma de gestionar los riesgos mediante el intercambio y/o compartimiento de información acerca de los riesgos entre los responsables de decisión y otras partes interesadas. La información incluye, pero no está limitada a la existencia, naturaleza, forma, probabilidad, gravedad, tratamiento, y la aceptación de los riesgos. El proceso busca lograr también una comunicación eficaz entre las partes interesadas, ya que esto puede tener un impacto significativo en las decisiones que se deben tomar. La comunicación se asegurará de que los responsables de la aplicación de la gestión de riesgos, así como otros interesados entiendan la base sobre la cual se toman las decisiones y por qué determinadas acciones son obligatorias. La comunicación es bidireccional.
El proceso se detalla a nivel macro a continuación.

Entradas: Toda la información obtenida de las actividades de gestión de riesgos.

Acciones: La información relacionada con riesgos debe ser intercambiada y/o compartida entre las personas que toman decisiones relacionadas con el proceso y otros interesados.

Salidas: Generar un entendimiento continuo del proceso de gestión de riesgos de seguridad de la información y sus resultados.

- *Monitoreo y revisión*

La organización debe asegurarse de que la gestión de riesgos de seguridad de la información y sus actividades conexas sigue siendo apropiada en las circunstancias actuales. Todas las mejoras acordadas o las acciones necesarias para mejorar la conformidad del proceso se deben notificar a los gerentes apropiados para tener la seguridad de que ningún elemento de riesgo o riesgo se pasen por alto o subestimen y que las acciones necesarias se toman, así como se tomen decisiones para proporcionar una comprensión realista del riesgo y la capacidad de respuesta.
El proceso se detalla a nivel macro a continuación.
Entradas: Toda la información obtenida de las actividades de gestión de riesgos.

Acciones: Los riesgos y sus factores (p. ej. Evaluación de valor, impactos, amenazas, vulnerabilidades, probabilidad de ocurrencia) deben ser monitoreados y revisados para identificar cualquier cambio en el contexto de la organización en una etapa temprana, para mantener una visión general y completa de los riesgos.

Salidas: Alineación continua de la gestión de los riesgos con los objetivos de negocio de la organización, así como con los criterios de aceptación de riesgos.

2.1.2 Estándar ISO 31000

El estándar **ISO 31000:2009**[14] establece un conjunto de principios que deben ser satisfechos para hacer una efectiva gestión de los riesgos. Este estándar internacional recomienda que las organizaciones desarrollen, implementen y mejoren continuamente un marco de trabajo, que tenga como propósito integrar el proceso de la gestión de riesgos en el gobierno, la estrategia, la planeación, la administración, los procesos de reporte, las políticas, los valores y la cultura general de la organización.

El enfoque genérico descrito en este estándar internacional provee los principios y guías para administrar cualquier tipo de riesgo de una manera sistemática, transparente, creíble y en cualquier ámbito y contexto. Una gestión de riesgos,

[14] INTERNATIONAL ORGANIZATION FOR STANDARIZATION. Risk management — Principles and guidelines. ISO 31000:2009. Suiza: ISO, 2009. pp 8-20. (ISO 31000:2009)

cuando se implementa y mantiene de acuerdo a este estándar, permite, entre otros:

- Mejorar la probabilidad de alcanzar los objetivos.
- Estar informado de la necesidad de identificar y tratar los riesgos a lo largo de la organización
- Mejorar la identificación de oportunidades y amenazas
- Asignar y usar de manera efectiva los recursos para el tratamiento de los riesgos
- Minimizar pérdidas.

Las relaciones entre los principios para gestionar los riesgos, el marco en el que ocurre y el proceso de gestión de riesgos descrito en el estándar ISO 31000 se encuentra en la figura 5:

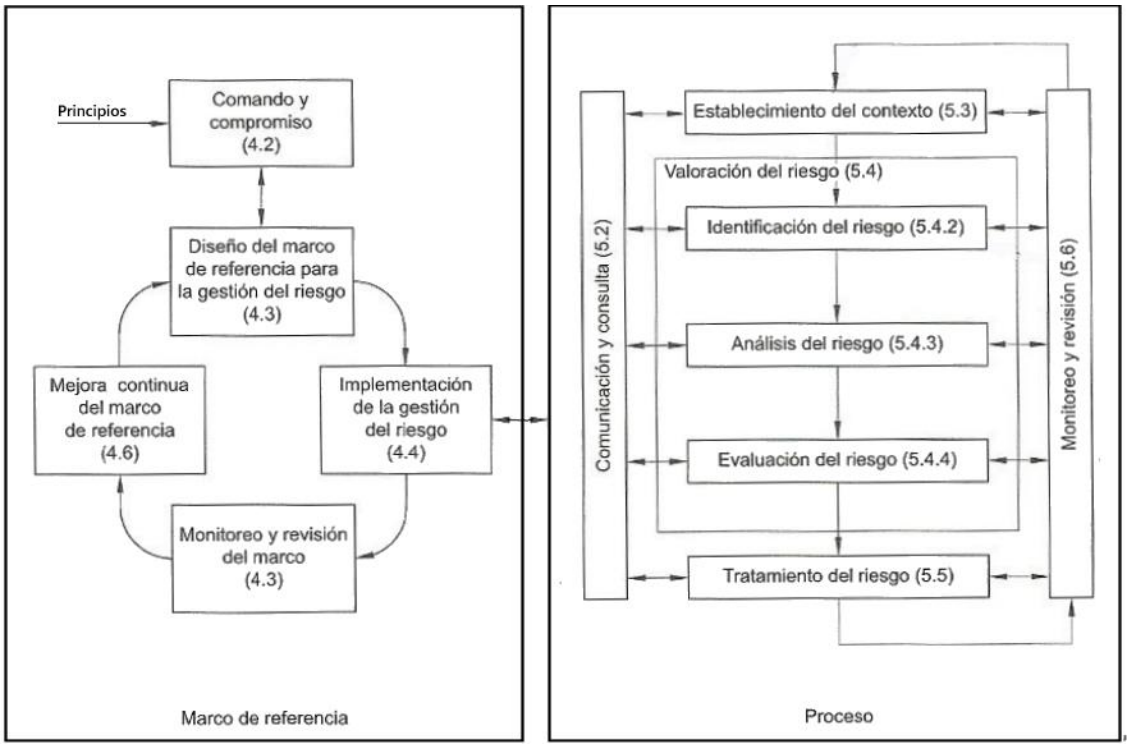

Figura 5. Relaciones entre principios, marco de referencia y procesos de gestión de riesgos de ISO 31000
(Modificada y traducida al español). Fuente: ISO[15]

Una breve descripción de cada uno de los pasos ilustrados en la figura 5 se muestra a continuación.

[15] Ibid., p.vii

- *Comando y compromiso*

La introducción de la gestión del riesgo y el aseguramiento de su eficacia continua, requiere de un compromiso fuerte y sostenido por parte de la dirección de la organización, así como de planificación estratégica y rigurosa para lograr el compromiso a todo nivel. Entre otras, la dirección debería definir y aprobar la política para la gestión del riesgo, garantizar que la cultura organizacional y la política para la gestión del riesgo estén alineadas, alinear los objetivos de la gestión del riesgo con los de la organización, garantizar la asignación de recursos para la gestión del riesgo, comunicar los beneficios de la gestión del riesgo a todas las partes involucradas y garantizar que el marco permanezca adecuado en el tiempo.

- *Diseño del marco de referencia para la gestión del riesgo*

Antes de empezar el diseño y la implementación del marco de referencia para la gestión del riesgo, es importante evaluar y entender el contexto tanto externo como interno de la organización, dado que éste puede tener influencia significativa en el diseño del marco. Este proceso se compone de siete actividades: entender a la organización y su contexto; establecer la política para la gestión del riesgo; rendición de cuentas; integración en los procesos de la organización; consecución de recursos; establecer mecanismos para la comunicación interna y la presentación de informes y establecer mecanismos para la comunicación externa y la presentación de informes.

- *Implementación de la gestión del riesgo*

Este proceso involucra dos actividades macro: implementar el marco de referencia para la gestión del riesgo y la implementación del proceso para la gestión del riesgo.

- *Monitoreo y revisión del marco*

Con el fin de garantizar que la gestión del riesgo es eficaz y continúa sustentando el desempeño de la organización, la organización debe medir el desempeño de la gestión del riesgo frente a los indicadores, medir periódicamente el progreso frente al plan, revisar periódicamente si el marco de referencia sigue siendo adecuados según el contexto de la organización, presentar informes sobre el riesgo y revisar la eficacia del marco definido.

- *Mejora continua del marco de referencia*

Con base en los resultados del monitoreo y las revisiones, se deberían tomar decisiones sobre la forma en que se podrían mejorar el marco de referencia, la

política y el plan para la gestión del riesgo. Estas decisiones deberían originar mejores en la gestión del riesgo de la organización y en su cultura.

- *Comunicación y consulta*

La comunicación y la consulta con las partes involucradas externas o internas deberían tener lugar durante todas las etapas del proceso para la gestión del riesgo. Por lo tanto, se deberían desarrollar tempranamente estos planes de comunicación y consulta. Éstos deben tratar aspectos relacionados con el propio riesgo, sus causas y consecuencias (si son conocidas) y las medidas que se tomarán para hacerlo. Este proceso debería facilitar los intercambios de información veraz, pertinente, precisa y fácil de entender, teniendo en cuneta los aspectos de la integridad personal y confidencial.

- *Establecimiento del contexto*

Al establecer el contexto, la organización articula sus objetivos, define los parámetros externos e internos que se van a considerar al gestionar el riesgo y establece el alcance y los criterios del riesgo para el resto del proceso. En esta etapa se retoma la información obtenida en el proceso del diseño del marco de referencia descrito previamente y se detallan los parámetros en más detalle.

- *Identificación del riesgo*

El objeto de esta fase es generar una lista exhaustiva de riesgos con base en aquellos eventos que podrían crear, aumentar, prevenir, degradar, acelerar o retrasar el logro de los objetivos. Esta identificación exhaustiva es crítica, dado que un riesgo que no se identifique en esta fase no será incluido en el análisis posterior.

- *Análisis del riesgo*

El análisis del riesgo implica el desarrollo y la comprensión del riesgo. Este análisis brinda una entrada para la evaluación del riesgo y para las decisiones, sobre si es necesario o no tratar los riesgos y sobre las estrategias y métodos más adecuados par su tratamiento. De igual manera, también brinda una entrada para la toma de decisiones, en la cual se deben hacer elecciones y las opciones implican diversos tipos y niveles de riesgo.

- *Evaluación del riesgo*

El propósito de la evaluación del riesgo es facilitar la toma de decisiones basada en los resultados del análisis anterior, sobre cuáles riesgos necesitan tratamiento y la prioridad para la implementación del mismo.

- *Tratamiento del riesgo*

Este proceso involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales opciones. Una vez implementado, el tratamiento suministra o modifica controles para el riesgo.

- *Monitoreo y revisión*

La organización debe asegurarse de que la gestión de riesgos y sus actividades conexas sigue siendo apropiada en las circunstancias actuales. Debe ser una parte planeada del proceso de gestión de riesgos e involucra un monitoreo o chequeo regular. Puede ser periódico o cuando sea necesario. Los resultados del monitoreo y revisión deben ser almacenados y reportados externa e internamente como sea apropiado; de igual manera, deberían ser usados como entradas para la revisión del marco de trabajo de gestión de riesgos.

2.1.3 Norma NTC 5254

La norma técnica **NTC 5254** fue desarrollada por el ICONTEC y es una adopción de la norma AS/NZ 4360:2004. Esta norma es la vigente en territorio colombiano.
NTC 5254 provee una guía genérica para el establecimiento e implementación el proceso de administración de riesgos, involucrando el establecimiento del contexto y la identificación, análisis, evaluación, tratamiento, comunicación y el monitoreo en curso de los riesgos.[16]

Esta norma tiene como objeto proporcionar una guía para que cualquier empresa que se base en ella para realizar la gestión de riesgo logre:

- Una base más rigurosa y confiable para la toma de decisiones y la planificación.
- Mejor identificación de las oportunidades y las amenazas.
- Ganar valor a partir de la incertidumbre y la variabilidad.
- Una gestión proactiva y no reactiva.
- Asignación y uso más eficiente de los recursos.
- Mejorar la gestión de incidentes y la reducción en las pérdidas y el costo del riesgo, incluyendo primas de seguros comerciales.
- Mejorar la confianza de las partes involucradas.
- Mejorar la conformidad con la legislación pertinente.
- Mejor dirección corporativa.[17]

Los principales elementos del proceso de gestión del riesgo se ilustran a continuación en la figura 6 que se encuentra a continuación.

[16] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Norma Técnica Colombiana NTC 5254. Gestión del Riesgo. Bogotá, Colombia: ICONTEC, 2006. p.1
[17] Ibid., p. 1-2

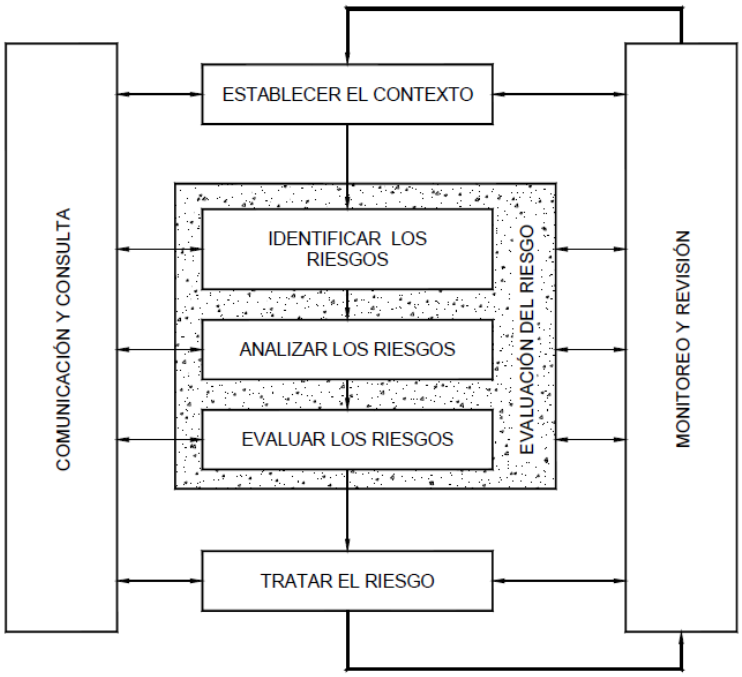

Figura 6. Proceso de gestión del riesgo NTC 5254 – Visión general
Fuente: ICONTEC[18]

Como se ve en la figura 6, el proceso general de gestión de riesgo está compuesto por siete elementos principales, los cuales serán descritos a continuación:

- *Comunicación y consulta*: En esta etapa (que está presente a lo largo de todo el proceso) se comunica y consulta con las partes involucradas, internas y externas, según sea adecuado.
- *Establecimiento del contexto*: En esta etapa se establece el contexto interno y externo de la gestión de riesgo en el cual tendrá lugar el resto del proceso. En este punto se tiene en cuenta el contexto interno y externo, el contexto de la gestión del riesgo, los criterios de desarrollo y la definición de la estructura del proceso.
- *Identificación de los riesgos*: En esta etapa se identifica dónde, cuándo, por qué y cómo podrían los eventos prevenir, degradar, retardar o potenciar el logro de los objetivos.
- *Análisis de los riesgos*: En esta etapa se identifica y evalúa los controles existentes. Se determinan las consecuencias y la posibilidad, las cuales conforman el nivel del riesgo.
- *Evaluación de los riesgos*: En esta etapa se comparan los niveles estimados de riesgo frente a los criterios pre-establecidos y se considera el equilibrio entre beneficios potenciales y resultados adversos. Esto permite tomar decisiones

[18] Ibid., p. 7

sobre el grado y la naturaleza de los tratamientos requeridos y sobre las prioridades.

- *Tratamiento de los riesgos*: En esta etapa se desarrollan e implementan estrategias específicas eficaces en términos de costos y planes de acción para incrementar los beneficios potenciales y reducir las pérdidas potenciales.
- *Monitoreo y revisión*: En esta etapa (que está presente a lo largo de todo el proceso) se realiza el monitoreo de la eficacia de todas las etapas del proceso de gestión del riesgo, lo cual es importante para la mejora continua del mismo. De igual manera, se monitorean los riesgos y la eficacia de las medidas de tratamiento para asegurar que las circunstancias cambiantes no alteran las prioridades de los mismos.

2.1.4 Risk IT

El marco de trabajo de **Risk IT** (elaborado por ISACA, organización mundialmente reconocida por sus aportes en seguridad y aseguramiento de sistemas de información, gobierno empresarial y administración de TI) explica el riesgo de TI, permite a la empresa tomar decisiones apropiadas teniendo en mente el riesgo y permite a los usuarios integrar la administración de TI en la administración general de riesgos de la empresa (ERM por sus siglas en inglés), tomando decisiones bien informadas sobre la medida, el apetito y la tolerancia al riesgo de la empresa y entendiendo cómo responder al riesgo. Con Risk IT, los ejecutivos *senior* podrán tener un claro entendimiento de la función y el riesgo de TI, teniendo un marco de referencia para priorizarlo y administrarlo.

Risk IT, como marco de trabajo, está basado en un conjunto de principios que tienen como propósito facilitar la administración efectiva de riesgos de TI. Éstos por lo general están basados en principios reconocidos de ERM que han sido aplicados al dominio de TI. El modelo de procesos de Risk IT está diseñado y estructurado para permitir a las empresas aplicar los principios en la práctica y comparar sus resultados.[19]

Como marco de trabajo, Risk IT se ha desarrollado como un modelo completo que agrupa un número de actividades claves en procesos, los cuales a su vez se agrupan en tres grandes dominios: Gobierno de Riesgos (RG – Risk Governance), Evaluación de Riesgos (RE – Risk Evaluation) y Respuesta a los Riesgos (RR – Risk Response). [20] Cada uno de estos dominios están divididos en tres procesos, entre los cuales se establece un flujo de información. En la figura 7 se puede ver una visión general de lo que es el modelo de procesos de Risk IT descrito previamente.

[19] ISACA. The Risk IT Framework. Rolling Meadows, Estados Unidos de América: ISACA, 2009. p. 13.
[20] Ibid., p. 15.

Cada uno los dominios antes descritos tienen asociados un modelo de madurez, el cual está basado en el conjunto de actividades clave que apoyan la consecución de los objetivos por cada dominio.

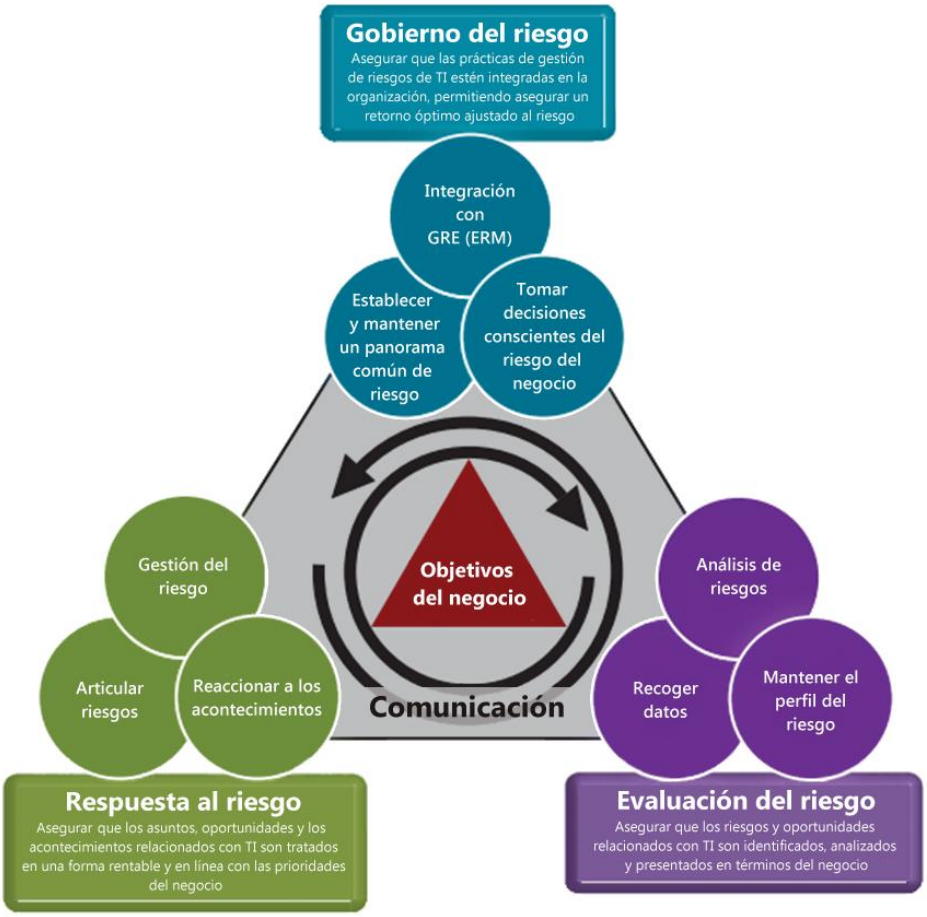

Figura 7. Vista general del marco de trabajo de Risk IT
(Traducido al español) Fuente: The Risk IT Framework [21]

A continuación se realizará una breve descripción de cada uno de los dominios ilustrados en la figura 7.

- *Gobierno del riesgo (Risk Governance - RG)*

El objetivo del dominio consiste en asegurar que las prácticas de gestión de riesgos de TI estén integradas en la organización, permitiendo asegurar una óptima rentabilidad ajustada al riesgo. Este dominio tiene una métrica asociada, consistente en el grado en que el uso estratégico de las TIC en el apalancamiento de recursos de la empresa reduzca el riesgo global de la misma.

[21] Ibid., p. 15.

Este dominio está compuesto de tres grandes procesos, a saber:

- [RG1] Establecer y mantener un panorama común de riesgo: Este proceso tiene como finalidad asegurar que las actividades de gestión de riesgos se alinean con la capacidad objetiva y la percepción subjetiva de la gerencia de la empresa para tolerar pérdidas relacionadas con TI.
- [RG2] Integración con una gestión de riesgos empresarial (ERM por sus siglas en inglés): Este proceso tiene como finalidad integrar la estrategia y operación de riesgos TI con las decisiones estratégicas de riesgo del negocio que se hayan hecho a nivel institucional.
- [RG3] Tomar decisiones conscientes del riesgo del negocio: Este proceso tiene como objetivo asegurar que las decisiones de la empresa consideren el rango completo de oportunidades y consecuencias de la dependencia en TI para alcanzar el éxito.

Cada uno de estos procesos cuenta con un conjunto de actividades claves que permiten alcanzar los objetivos definidos.

- *Evaluación de riesgos (Risk Evaluation - RE)*

Este dominio tiene como objetivo asegurar que los riesgos y oportunidades relacionados con TI sean identificados, analizados y presentados en términos del negocio. Cuenta con una métrica, la cual consiste en el impacto del negocio acumulado de incidentes y eventos relacionados con TI no identificados por los procesos de evaluación de riesgos.

Este dominio está compuesto de tres grandes procesos, a saber:

- [RE1] Recolección de datos: Este proceso tiene como objetivo identificar información relevante para permitir una identificación, análisis y reporte de riesgos relacionados con TI.
- [RE2] Análisis del riesgo: Este proceso tiene como finalidad desarrollar información útil para soportar decisiones relacionadas con riesgos, que tengan en cuenta la relevancia en el negocio de los factores asociados al riesgo.
- [RE3] Mantenimiento de un perfil de riesgos: Este proceso tiene como objetivo mantener un inventario actualizado y completo de los atributos y riesgos conocidos y de los recursos, capacidades y controles de TI, entendiéndolos en el contexto de productos, servicios y procesos del negocio.

Cada uno de estos procesos cuenta con un conjunto de actividades claves que permiten alcanzar los objetivos definidos.

- *Respuesta a riesgos (Risk Response – RR)*

Este dominio tiene como objetivo asegurar que los problemas, las oportunidades y los eventos relacionados con riesgos de TI son tratados en una forma rentable y en línea con las prioridades del negocio. Este dominio tiene una métrica asociada,

consistente en el impacto acumulado en el negocio derivado de los incidentes y eventos de TI previstos por los procesos de evaluación de riesgo, pero que aún no han sido objetos de medidas de mitigación.

Este dominio está compuesto de tres grandes procesos, a saber:

- [RR1] Articular riesgos: Este proceso tiene como objetivo asegurar que la información sobre el verdadero estado de la exposición y las oportunidades relacionadas con TI, se dispongan de manera oportuna y a las personas adecuadas para dar respuestas apropiadas.
- [RR2] Este proceso tiene como finalidad garantizar que las medidas para ajustar las oportunidades estratégicas y reducción de riesgos a un nivel aceptable, son gestionadas como un portafolio.
- [RR3] Este proceso tiene como objetivo asegurar que las medidas para aprovechar oportunidades inmediatas o limitar la magnitud de pérdidas de eventos relacionados con TI sean activadas de manera oportuna y sean efectivas.

Cada uno de estos procesos cuenta con un conjunto de actividades claves que permiten alcanzar los objetivos definidos.

2.1.5 EDUCAUSE risk assessment/management framework

De acuerdo a su página Web[22], EDUCAUSE es "una asociación sin ánimo de lucro, cuya misión es avanzar la educación superior a través del uso de las tecnologías de información. EDUCAUSE ayuda a aquellos que lideran, administran y usan TI para formar decisiones estratégicas a todo nivel. La membresía está abierta a instituciones de educación superior, corporaciones que sirven el mercado de tecnologías de información de educación superior y otras asociaciones y organizaciones relacionadas. Los programas y recursos de EDUCAUSE incluyen actividades de desarrollo profesional; publicaciones impresas y electrónicas (incluyendo libros) y EDUCAUSE Review, su revista líder; apoyo jurídico; iniciativas de enseñanza y aprendizaje; datos, investigaciones y análisis; comunidades de interés especial; premios y servicios de información en línea. EDUCAUSE tiene oficinas en Louisville, Colorado y Washington, D.C."
Uno de los documentos que se encuentra en el sitio web de EDUCAUSE es el correspondiente al "*EDUCAUSE/Internet2 Higher Education Information Security Council risk assessment / management framework*"[23]. Su propósito consiste en establecer una guía de alto nivel para proveer unos procesos de evaluación y administración de riesgos cibernéticos para instituciones de educación superior. La

[22] EDUCAUSE. Artículo de contenido "About EDUCAUSE" [En línea]. <http://www.educause.edu/about> [citado en 4 de noviembre de 2012]
[23] EDUCAUSE. Risk Management Framework [En línea]. <https://wiki.internet2.edu/confluence/display/itsg2/Risk+Management+Framework> [Citado en 5 de noviembre de 2012]

idea es proveer un proceso modelo que puede ser adaptado según se necesite, de acuerdo a las características de tamaño, modelo de fundación o cultura.

Como una introducción al marco, se comienza definiendo dos términos esenciales para el desarrollo del mismo:

- "Administración del riesgo", el cual consiste en el proceso de identificación de los riesgos y la implementación de los planes para manejarlos. Los riesgos se definen de acuerdo a la amenaza asociada al riesgo, la probabilidad que ésta se materialice y el impacto que puede causar en los activos valiosos de la institución.
- "Evaluación del riesgo" es la parte del proceso de gestión de riesgos en ejecución que asigna prioridades relativas para los planes de mitigación e implementación.

La visión general del marco propuesto por EDUCAUSE se ilustra en la figura 8:

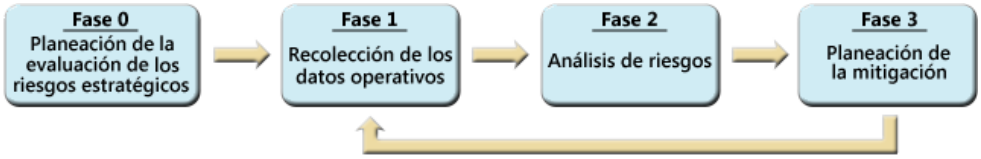

Figura 8. Visión general del marco de trabajo EDUCAUSE
(Traducido al español). Fuente: EDUCAUSE[24]

En la figura 8 se ilustra que el marco se encuentra dividido en cuatro fases, las cuales se describen a continuación.

- *Fase 0: Planeación de la evaluación de los riesgos estratégicos*

En esta fase se establece la estrategia de evaluación de los riesgos. Aquí se determinará los criterios que serán usados para evaluar la importancia estratégica de los activos (actividad también conocida como "clasificación de activos"), las amenazas y las vulnerabilidades. Esta fase usualmente sólo se ejecuta una vez, pero es posible que en algún momento de la ejecución del proceso de riesgos se requiera añadir o descubrir criterios adicionales que deben ser incorporados al mismo, para lo cual deben ser ejecutadas nuevamente las actividades que se requieran.
En esta fase se ejecutan cuatro procesos, a saber: establecer criterios que serán usados para clasificar y priorizar los activos de datos; aplicar los criterios de clasificación para priorizar los activos de datos y demás recursos de TI relacionados; identificar amenazas, vulnerabilidades y controles que serán evaluados; y establecer criterios que serán usados para evaluar las amenazas, vulnerabilidades y controles.

[24] Ibid.

- *Fase 1: Recolección de los datos operativos*

En esta fase se identifican y priorizan los activos críticos de la institución. SE identifican las amenazas y vulnerabilidades clave que pueden comprometer la confidencialidad, integridad y disponibilidad de estos activos. De igual manera, se identifica toda la protección implantada para proteger estos activos y qué vulnerabilidades y amenazas impactan.
En esta fase se ejecutan cuatro procesos: “Obtención de la perspectiva estratégica – administración *senior”* (donde se obtiene de la gerencia su visión estratégica y sus necesidades, además de obtener la aprobación del proyecto); “obtención de la perspectiva operativa: infraestructura – equipo de trabajo técnico” (donde se obtiene del personal técnico sus opiniones sobre las vulnerabilidades, amenazas y controles existentes); “obtención de la perspectiva operativa: aplicaciones y equipo de trabajo en general” (donde se obtiene del personal operativo sus opiniones sobre las vulnerabilidades, amenazas y controles existentes); y finalmente “obtención de la perspectiva técnica – análisis técnico” (donde se analizan los componentes técnicos asociados con los activos identificados en la fase 0, se escogen las herramientas para evaluar los componentes técnicos y finalmente aplicar las herramientas en los componentes técnicos para obtener unos resultados).

- *Fase 2: Análisis de riesgos*

En esta fase, se crean perfiles de riesgo para las amenazas que tendrán más probabilidad de causar un mayor impacto en las vulnerabilidades de los activos. Esta información puede ser usada para priorizar la asignación de recursos de manera efectiva en costos; asegurando así una mitigación apropiada de los riesgos más importantes y balanceando usabilidad con seguridad.

En esta fase se ejecutan dos procesos: “revisión de documentación e información técnica” (políticas, reportes, análisis técnicos, rastreos, etc.) y “consolidación y priorización de perspectivas” (basándose en la información de la fase 1 y en el proceso anterior, se generan los perfiles para los riesgos más significativos).

- *Fase 3: Planeación de la mitigación*

En esta fase se documenta la estrategia de protección para la mitigación del riesgo. Usando los perfiles realizados en la fase 2, se determinan qué riesgos serán manejados en la estrategia final de mitigación. De igual manera, se evalúa la efectividad del proceso de evaluación de riesgos y se inicia la planeación de la siguiente evaluación, considerando las lecciones aprendidas en el proceso actual.
Esta fase consta de tres procesos: “acuerdo en una estrategia para mitigar los riesgos”, “documentar e implementar el plan de mitigación” y “evaluar el progreso de la mitigación y planear la siguiente evaluación”.

2.1.6 MAGERIT

La metodología MAGERIT (Metodología de análisis y gestión de riesgos de T.I) fue desarrollada por el consejo superior de administración electrónica, y publicada por el ministerio de administraciones publicas de España. Es una metodología pública y de amplio uso en el ámbito español y de uso obligatorio para las entidades publicas de dicho país.

Los objetivos del proceso de análisis y gestión de riesgos propuestos en MAGERIT son[25]:

- Directos
  - Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.
  - Ofrecer un método sistemático para analizar tales riesgos.
  - Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
- Indirectos
  - Preparar a la organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

En resumen[26], MAGERIT establece que las tareas de análisis y gestión de riesgos no son un fin en sí mismas, sino que se encajan en la actividad continua de gestión de la seguridad. También establece que el análisis de riesgos permite determinar cómo es, cuánto vale y qué tan protegidos se encuentran los activos. En coordinación con los objetivos, estrategia y política de la organización, las actividades de gestión de riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que acepta la Dirección.
La implantación de los controles de seguridad requiere una organización gestionada y la participación informada de todo el personal que trabaja con el sistema de información. Es este personal el responsable de la operación diaria, de la reacción ante incidencias y de la monitorización en general del sistema para determinar si satisface con eficacia y eficiencia los objetivos propuestos.
Este esquema de trabajo debe ser repetitivo, pues los sistemas de información rara vez son inmutables; más bien se encuentran sometidos a evolución continua tanto propia (nuevos activos) como del entorno (nuevas amenazas), lo que exige una revisión periódica en la que se aprende de la experiencia y se adapta al nuevo contexto. El análisis de riesgos proporciona un modelo del sistema en términos de activos, amenazas y salvaguardas, y es la piedra angular para controlar todas las

[25] ESPAÑA, PORTAL DE ADMINISTRACIÓN ELECTRÓNICA. MAGERIT versión 2. Libro 1, p. 6 [en línea].
<http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184> [citado en 1 de abril de 2012]
[26] Ibid., p. 8

actividades con fundamento. La gestión de riesgos es la estructuración de las acciones de seguridad para satisfacer las necesidades detectadas por el análisis.
Estas actividades también son apalancadas por otros dos procesos, un proceso de concienciación y formación y un proceso de incidencias y recuperación.
El proceso de concienciación y formación busca la creación de una "cultura de seguridad" que emanado de la alta dirección, conciencie a todos los involucrados de su necesidad y pertinencia. Y el proceso de incidencias y recuperación busca que las personas involucradas deben ser conscientes de su papel y relevancia continua para prevenir problemas y reaccionar cuando se produzcan, ya que cuando se produce una incidencia, el tiempo empieza a correr en contra del sistema: su supervivencia depende de la presteza y corrección de las actividades de reporte y reacción. Cualquier error, imprecisión o ambigüedad en estos momentos críticos, se ve amplificado convirtiendo lo que podía ser un mero incidente en un desastre.

La relación entre las actividades mencionadas se puede ver en la figura 9.

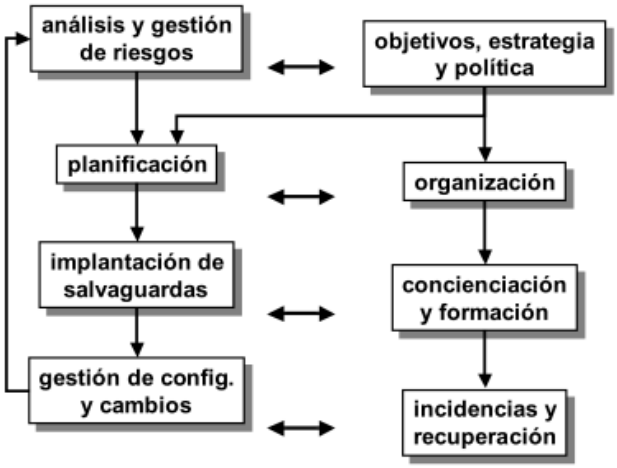

Figura 9. Tareas de análisis y gestión de riesgos propuestas por la metodología MAGERIT.
Fuente: MAGERIT[27]

La metodología se divide en tres volúmenes más una herramienta de soporte denominada PILAR II (Proceso informático-lógico para el análisis y la gestión de riesgos).
El primer volumen denominado "Volumen I – Método" es el documento principal donde se detalla el método para implementar el proceso de análisis y gestión de riesgo propuesto desde tres ángulos:

- El capítulo 2 describe los pasos para realizar un análisis del estado de riesgo y para gestionar su mitigación. Es una presentación netamente conceptual.

[27] Ibid., p. 8

- El capítulo 3 describe las tareas básicas para realizar un proyecto de análisis y gestión de riesgos, entendiendo que no basta con tener los conceptos claros, sino que es conveniente pautar roles, actividades, hitos y documentación para que la realización del proyecto de análisis y gestión de riesgos esté bajo control en todo momento.
- El capítulo 4 aplica la metodología al caso del desarrollo de sistemas de información, en el entendimiento que los proyectos de desarrollo de sistemas deben tener en cuenta los riesgos desde el primer momento, tanto los riesgos a que están expuestos, como los riesgos que las propias aplicaciones introducen en el sistema.

Como complemento, el capítulo 5 desgrana una serie de aspectos prácticos, derivados de la experiencia acumulada en el tiempo para la realización de un análisis y una gestión realmente efectivos.

El segundo volumen denominado "Volumen II – Catálogo de elementos", se busca facilitar la labor de las personas que acometen el proyecto, en el sentido de ofrecerles elementos estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis, así como homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios uniformes que permitan comparar e incluso integrar análisis realizados por diferentes equipos.

El tercer volumen "Volumen III – Guía de técnicas", se trata de una guía de consulta. Según el lector avance por las tareas del proyecto de análisis y gestión de riesgos, se le recomendará el uso de ciertas técnicas específicas, de las que esta guía busca ser una introducción, así como proporcionar referencias para que el lector profundice en las técnicas presentadas.

2.2 ESTADO DEL ARTE EN EL SECTOR

De acuerdo a la búsqueda realizada en las bases de datos académicas reconocidas, no se encontró una guía de implementación en el área de riesgos de TI para el sector de la educación superior. De hecho, no se encontró información que evidencie que las universidades privadas estén haciendo gestión de riesgos de tecnología, lo cual fue uno de los motivos para empezar este proyecto de grado.

Realizando una búsqueda más amplia a nivel nacional, se encontró en la biblioteca de la Universidad de los Andes una guía de buenas prácticas en gestión de riesgos de TI en el sector bancario colombiano[28], tesis que fue concebida con

[28] FIGUEROA MEDINA, Luis Carlos. Guía de buenas prácticas en gestión de riesgos de TI en el sector bancario colombiano. Documento de tesis en la Maestría de Ingeniería de Sistemas y Computación. Bogotá: Universidad de los Andes, 2010. p. 9.

las mismas premisas de este documento pero enfocada en el entorno financiero nacional. El objetivo de esta guía fue la construcción de un modelo que “tomó ventaja de las fortalezas de los marcos de gestión de riesgos de TI revisados y le agregó la experiencia de los bancos estudiados, lo cual ofreció a las organizaciones una guía flexible para la gestión de riesgos de TI”. El documento consta de una revisión de algunos marcos de trabajo de gestión de riesgos (BS 31100, TI4A y Risk IT), un levantamiento de información, la elaboración de la guía de gestión de riesgos para el sector bancario y finalmente una validación en algunas organizaciones. La idea de este proyecto de grado es, precisamente, lograr el mismo objetivo con las universidades; por esta razón, se considera que este documento será de gran ayuda para lograr los objetivos planteados en el trabajo.

Uno de los objetivos de este proyecto es generar el estado del arte en las universidades caleñas. Para obtener esta visión y conocer de antemano sus expectativas frente a un proceso de gestión de riesgos de T.I., se elaboró una encuesta en línea usando la tecnología de Google Docs (la cual se incluye al final del documento como el Anexo 1) y se envió por correo electrónico a los directores de T.I. de las universidades integrantes de la Asociación Red Universitaria de Alta Velocidad del Valle del Cauca (RUAV). Se aplicó un muestreo irrestricto aleatorio en el cual, de las 9 universidades que integran el grupo, se obtuvo una muestra de 3 participantes. Basándose en el análisis de las respuestas obtenidas, se obtuvo la información que se detalla a continuación.

Se consultó a los directores de T.I. sobre los riesgos relacionados con las tecnologías de información más relevantes para su organización, a lo que respondieron lo siguiente:

- Catástrofes naturales
- Fugas de información
- Ataques informáticos
- Fallas técnicas de los equipos
- Apertura de los entornos académicos y trabajo de los grupos de investigación en sus propios servidores.
- Tecnología cambiante y pocos recursos para seguir el ritmo en términos de entrenamiento para gestionar el tema de seguridad.
- Cultura organizacional, donde cada individuo no es consciente de ser parte de la cadena de aseguramiento de la información y de los procesos para reducir los riesgos tecnológicos.

Para los directores de T.I. es claro que la importancia de los riesgos está determinada por cómo atenten con la continuidad directa de la operación de la Universidad y el grado de la amenaza a los activos de información más relevantes que considere la alta dirección.

Se puede concluir de lo anterior que las universidades tienen una noción correcta de qué es un riesgo de T.I., enfocándose especialmente en aquellos relacionados con la seguridad de la información y al entorno natural. Es interesante ver que se incluye el componente de la cultura organizacional frente al riesgo, pues éste es uno de los factores que pueden incidir negativamente en una implementación de un proceso de gestión de riesgos de T.I.

Por otro lado, se preguntó qué marcos de trabajo o normas relacionadas con la gestión de riesgos de tecnologías de información conocen los directores de T.I., a lo que contestaron que conocían COBIT, PMBOK, la familia de normas ISO 27000 y Magerit. Se puede concluir que las universidades tienen conocimiento de marcos de trabajo que apoyan la gestión de riesgos de T.I. así como de gobierno de T.I.; esto es algo positivo, ya que a la hora de implementar un proceso de gestión de riesgos de T.I como el propuesto en este documento, será más fácil para el director de T.I. entender el trasfondo teórico del proceso.
Todos los directores consideraron que es necesario un proceso de gestión de riesgos de T.I. en sus organizaciones, exponiendo las siguientes razones:

- Es importante contar con un modelo que permita reducir los riesgos y sus impactos en la Universidad y asegurar la continuidad de la operación de la misma.
- Existen diversos riesgos asociados a los activos de información, los cuales podrían afectar el normal desempeño de la institución.
- Es importante porque ayuda a pasar de solo gestionar servicios a gobernarlos y esto es el punto donde el departamento de TI se lograría alinear verdaderamente con la dirección institucional, donde la toma de decisiones se realice estratégicamente.
- A partir del resultado de la matriz de riesgos avalada institucionalmente se podrían tomar con certeza las decisiones.

En este punto se puede observar las expectativas que tienen las universidades frente a un proceso de gestión de riesgos de T.I., lo cual se tuvo en cuenta en la guía de implementación propuesta más adelante. Es importante recalcar que, al preguntarles a los directores si consideraban que la implementación de un proceso de gestión de riesgos de T.I. podría mitigar los problemas con los proyectos de tecnología de las instituciones, todos respondieron afirmativamente la pregunta.

De igual manera, los directores de T.I. contestaron que sí era viable implementar un proceso de gestión de riesgos de T.I. en sus instituciones; de hecho, reconocen que este es uno de los eslabones más débiles en el proceso de gobierno de T.I. y en una de ellas ya se empezó a ejecutar una primera fase, consistente en generar conciencia y entender la importancia que tiene para la organización. Sin embargo, reconocieron que aún no se ha empezado una implementación formal de un proceso de gestión de riesgos de T.I., debido a que apenas se están considerando

temas como continuidad, procesos de recuperación de desastres, generación de cultura organizacional, entre otros temas.
La encuesta también reflejó que en caso de implementar un proceso de gestión de riesgos de T.I., todos contarían con el apoyo del comité directivo, lo cual es vital para que el proceso sea un éxito y cuente con los recursos requeridos.

Finalmente, se pudo concluir que todas las universidades participantes consideraron importantes y relevantes las siguientes premisas a la hora de implementar un proceso de gestión de riesgos de T.I.:

- El proceso de gestión de riesgos de T.I. debe estar alineado con los objetivos organizacionales.
- El proceso de gestión de riesgos de T.I. debe involucrar a toda la organización, en vez de ser sólo un esfuerzo del área de T.I.
- El proceso de gestión de riesgos de T.I. debe tener un proceso de seguimiento para evaluar la efectividad de la aplicación de los planes de acción.
- El proceso de gestión de riesgos de T.I. debe contar con un proceso de mejoramiento continuo.
- El proceso de gestión de riesgos de T.I. debe contar con un modelo de madurez para evaluar el proceso frente a las demás instituciones.
- El proceso de gestión de riesgos de T.I. debe estar integrado a otros procesos de gestión de riesgos de la organización.

2.3 COMPARATIVOS DE LOS DOCUMENTOS BASE

Para realizar una evaluación objetiva de los documentos antes mencionados, se consultó un documento que definiese los componentes esenciales de un proceso de gestión de riesgos. La organización de estándares ISO, en su Guía 51[29], define un conjunto de procesos básicos, a saber:

- Definición de uso previsto y abuso razonablemente previsible (contexto)
- Identificación de las amenazas
- Estimación del riesgo
- Evaluación del riesgo
- Reducción del riesgo

Al analizar los documentos que se describen en el punto 2.1, se observó que todos cumplían con los elementos antes mencionados; de hecho, se identificaron dos procesos adicionales (monitoreo del avance y comunicación y consulta) que fueron comunes para casi todos los documentos, como se observa en la siguiente tabla:

[29] INTERNATIONAL ORGANIZATION FOR STANDARIZATION. Safety aspects - Guidelines for their inclusion in standards. ISO/IEC Guide 51. Suiza: ISO, 1999. p. 3. (ISO/IEC Guide 51:1999)

Procesos básicos	ISO 27005	ISO 31000	NTC 5254	Risk IT	EDUCAUSE	Magerit
Definición del contexto	Si	Si	Si	Si	Si	Si
Identificación de las amenazas	Si	Si	Si	Si	Si	Si
Estimación del riesgo	Si	Si	Si	Si	Si	Si
Evaluación del riesgo	Si	Si	Si	Si	Si	Si
Reducción del riesgo	Si	Si	Si	Si	Si	Si
Monitorear el avance	Si	Si	Si	Si	Si	No
Comunicación y consulta	Si	Si	Si	Si	Si	Si

Tabla 8. Comparativo general entre documentos de gestión de riesgos de T.I.
Fuente: Propia

Teniendo en cuenta los procesos básicos, se entró en detalle para cada documento para evaluar las prácticas propuestas para cada uno, lo cual se describe en las siguientes tablas (se dividió en tres tablas para una mejor lectura).

Procesos básicos	Actividades de ISO 27005	Actividades de ISO 31000
Definición del contexto	Establecimiento del contexto	Establecimiento del contexto
Identificación de las amenazas	Identificación del riesgo	Identificación del riesgo
Estimación del riesgo	Análisis del riesgo	Análisis del riesgo
Evaluación del riesgo	Evaluación del riesgo	Evaluación del riesgo
Reducción del riesgo	Tratamiento del riesgo	Tratamiento del riesgo
Monitorear el avance	Monitoreo y revisión	Monitoreo y revisión
Comunicación y consulta	Comunicación y consulta	Comunicación y consulta

Tabla 9. Comparativo entre documentos de gestión de riesgos de T.I. (Parte 1)
Fuente: Propia

Procesos básicos	NTC 5254	EDUCAUSE Risk assessment / management framework
Definición del contexto	Literal 3.2. Establecimiento del contexto • Establecimiento del contexto externo teniendo en cuenta las partes involucradas y sus objetivos. • Establecimiento del contexto interno teniendo en cuenta las siguientes áreas clave de la organización • Establecer el contexto de la gestión de riesgo • Definir los criterios frente a los cuales se va a evaluar el riesgo. • Definir la estructura del resto del proceso.	• Fase 0 Proceso 1: Establecer criterios de evaluación de riesgo • Fase 0 Proceso 2: Aplicar los criterios de activos críticos para clasificar colecciones de datos y recursos relacionados

Identificación de las amenazas	Literal 3.3. Identificación de los riesgos • Elaboración de una lista una lista exhaustiva de las fuentes de riesgos y de los eventos que pueden tener impacto en el logro de los objetivos identificados en el contexto. • Establecer las posibles causas y escenarios para los riesgos identificados. • Definición de herramientas y técnicas	• Fase 0 Proceso 3: Identificar las amenazas, vulnerabilidades y controles que serán evaluados • Fase 1 Proceso 1: Perspectiva Estratégica - Alta Dirección • Fase 1 Proceso 2: Perspectiva Operativa: Infraestructura - Personal técnico • Fase 1 Proceso 3: Perspectiva Operativa: Aplicaciones - Personal General • Fase 1 Proceso 4: Perspectiva Técnica - Análisis Técnico
Estimación del riesgo	Literal 3.4. Análisis de riesgos • Evaluación de los controles existentes • Definir las consecuencias y posibilidades • Definir el grado del tipo de detalle del riesgo (cualitativo, semicuantativo, cuantativo) • Análisis de sensibilidad	• Fase 2 Proceso 1: Revisión de la documentación y datos técnicos • Fase 2 Proceso 2: Consolidar y priorizar perspectivas
Evaluación del riesgo	Literal 3.5. Evaluación de los riesgos	• Fase 3 Proceso 1: Ponerse de acuerdo sobre una estrategia para mitigar los riesgos
Reducción del riesgo	Literal 3.6. Tratamiento de los riesgos • Identificar las opciones para el tratamiento de los riesgos con resultados positivos • Identificar las opciones para el tratamiento de los riesgos con resultados negativos • Valorar las opciones para tratar los riesgos. • Preparación e implementación de los planes de tratamiento	• Fase 3 Proceso 1: Ponerse de acuerdo sobre una estrategia para mitigar los riesgos • Fase 3 Proceso 2: Documentar y aplicar plan de mitigación
Monitorear el avance	Literal 3.7. Monitoreo y revisión • Monitoreo y revisión de los factores de riesgos • Monitoreo, revisión y mejoramiento del manejo de riesgos	• Fase 3 Proceso 2: Documentar y aplicar plan de mitigación • Fase 3 Proceso 3: Evaluar el progreso de la mitigación y planear la siguiente evaluación

Comunicación y consulta	Literal 3.1. Comunicación y consulta La norma propone una serie de actividades para este proceso: • Desarrollar un plan de comunicación para las partes involucradas tanto internas como externas, que involucre temas relacionados con el riesgo en sí y con el proceso para gestionarlo. • Identificar y registrar las percepciones y diferentes puntos de vistas de los involucrados, ya que pueden tener un impacto significativo en el proceso de toma de decisiones involucrado. • Se debe llevar registros de la comunicación y la consulta dependiendo de la escala y sensibilidad de la actividad a ejecutar del proceso.	• Fase 1 Proceso 1: Perspectiva Estratégica - Alta Dirección • Fase 1 Proceso 2: Perspectiva Operativa: Infraestructura - Personal técnico • Fase 1 Proceso 3: Perspectiva Operativa: Aplicaciones - Personal General

Tabla 10. Comparativo entre documentos de gestión de riesgos de T.I. (Parte 2)
Fuente: Propia

Procesos básicos	MAGERIT	Risk IT
Definición del contexto	• P1.1. Se establecen las consideraciones necesarias para arrancar el proyecto AGR. • P1.2. Se investiga la oportunidad de realizarlo. • P1.3. Se definen los objetivos que ha de cumplir y el dominio (ámbito) que abarcará. • P1.4. Se planifican los medios materiales y humanos para su realización. • P1.5. Se procede al lanzamiento del proyecto.	Este proceso esta embebido en los dominios RG y RE de Risk IT: • Criterios básicos: RG2.3. Adaptar prácticas de riesgos de TI a las prácticas de riesgos del negocio. También se apoya en RG1.2 Proponer umbrales de tolerancia para los riesgos de TI, el cual describe el desarrollo de los criterios básicos para una gestión adecuada del riesgo de TI. • El alcance es cubierto por el RE2.1 Definir el alcance del análisis de riesgos de T.I. • La organización es cubierta por RG2.1 Establecer y mantener responsabilidades para la administración de riesgos de TI y por RG2.4 Proveer los recursos adecuados para la gestión de riesgos de T.I. • A través de todo el modelo de procesos de Risk IT, se definen matrices RACI las cuales son usadas para definir las buenas prácticas de asignación de roles y responsables para cada actividad.

Identificación de las amenazas	• P2.1. Se identifican los activos a tratar, las relaciones entre ellos y la valoración que merecen. • P2.2. 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.	• Este proceso es incluido en RE2.2 Estimar riesgos de TI. • La secuencia usada en ISO27005 para identificar riesgos es parcialmente alineada con el enfoque de Risk IT. La identificación de riesgos comprende los siguientes elementos en Risk IT: escenarios de riesgos y factores de riesgos
Estimación del riesgo	• P2.3. Se identifican las salvaguardas existentes y se valora la eficacia de su implantación. • P2.4. Se estima el impacto y el riesgo al que están expuestos los activos del sistema.	• RE2 - Análisis de riesgos • RE1 - Recolección de datos
Evaluación del riesgo	• P2.5. Se interpreta el significado del impacto y el riesgo.	• RE2.2 - Estimar el riesgo de T.I.
Reducción del riesgo	• P3.1. Se elige una estrategia para mitigar impacto y riesgo. • P3.2. Se determinan las salvaguardas oportunas para el objetivo anterior. • P3.3. Se determina la calidad necesaria para dichas salvaguardas. • P3.4. Se diseña un plan de seguridad (plan de acción o plan director) para llevar el impacto y el riesgo a niveles aceptables. • P3.5. Se lleva a cabo el plan de seguridad.	• El tratamiento de los riesgos se incluye en las actividades RE2.3 - Identificar opciones de respuesta a riesgos y en RR2.3 - Responder a la exposición y las oportunidades de riesgos descubiertos • La aceptación del riesgo se realiza en la actividad RG3.4 - Aceptar el riesgo de T.I.
Monitorear el avance	No aplica	• Risk IT define componentes de gestión y gobierno para el monitoreo y la revisión de los riesgos. • En la actividad RG2 - Integración con GRE (ERM) se incluye la continua alineación de las prácticas existentes de gestión de riesgos con diversos factores internos y externos. • La evaluación del ejercicio del análisis de riesgos es incluida en la actividad RE2.4 - Realizar una revisión por pares de los análisis de riesgos de T.I. • Risk IT incluye prácticas en la actividad RG2.5 para "proveer un aseguramiento independiente sobre la gestión de riesgos de T.I."

Comunicación y consulta	La metodología tiene en cuenta la comunicación y consulta de las decisiones que involucra el proceso de AGR a todos los involucrados posibles desde el nivel de gerencial hasta la operación de la organización	• El modelo de procesos de Risk IT incluye información específica a ser comunicada entre las prácticas claves. • Las actividades RG1.5. Promover una cultura orientada al riesgo de TI y RG1.6 Fomentar una comunicación efectiva del riesgo de TI se enfocan en la institucionalización de la comunicación del riesgo • Cubierto también en la actividad RE3.6. Desarrollar indicadores de riesgo de TI

Tabla 11. Comparativo entre documentos de gestión de riesgos de T.I. (Parte 3)
Fuentes: The Risk IT Practitioner Guide[30] y propia

Tomando estos comparativos como base, se generó un listado de aspectos comunes entre los documentos, los cuales se enmarcaron en las fases genéricas descritas previamente. El listado está descrito en la tabla 12.

Procesos básicos	**Aspectos Comunes**
Definición del contexto	• Se establece una visión/contexto de los riesgos de TI teniendo en cuenta las partes involucradas desde arriba hasta abajo. • Definir los criterios de evaluación de los riesgos • Se alinea el proceso con los objetivos de la empresa
Identificación de las amenazas	• Se define el universo completo de los riesgos existentes • Se establecen escenarios de riesgo • Se identifican los riesgos mas posibles • Se identifican las consecuencias
Estimación del riesgo	• Evaluación de controles existentes • Se define el método de evaluación de los riesgos • Estimación del nivel de riesgo
Evaluación del riesgo	• Se evalúa los riesgos según su impacto y probabilidad • Se interpreta el resultado y se documenta el resultado del proceso
Reducción del riesgo	• Se definen las estrategias para tratamiento de los riesgos. • Se preparan e implementan los planes de acción de riesgos
Monitorear el avance	• Se evalúa constantemente el proceso completo de la gestión de riesgos dependiendo de los cambios externos e internos relevantes para la organización • Se evalúa el cambio sobre los factores de riesgos sobre los cuales se definen los mismos.
Comunicación y consulta	• Se define un plan de comunicaciones involucrando todos los interesados del proceso de gestión de riesgos. • Se debe tener un nivel de comunicación claro y relevante a la naturaleza de los diferentes niveles jerárquicos de los interesados

Tabla 12. Aspectos comunes entre los documentos de gestión de riesgos de T.I.
Fuente: Propia

[30] ISACA. The Risk IT Practitioner Guide. Rolling Meadows, Illinois, Estados Unidos de América: ISACA, 2009. pp. 117-118. ISBN 978-1-60420-116-1.

3. PROPUESTA DE GUÍA DE IMPLEMENTACIÓN

En este trabajo se propone una guía de implementación de gestión de riesgos de T.I. básica, la cual cumple con los procesos genéricos de gestión de riesgos definidos en la guía 51 de ISO[31] y se apoya en los aspectos comunes encontrados al realizar el comparativo de todos los documentos del marco teórico presentados en la tabla 12 del capítulo anterior.

Esta guía de implementación está construida usando un modelo por procesos, lo cual facilita su implementación en los procesos institucionales de las universidades y va en línea con los esfuerzos realizados por las mismas para las acreditaciones institucionales. De esta manera, se desarrollaron seis procesos cuya relación se ilustra de manera global en la figura 10.

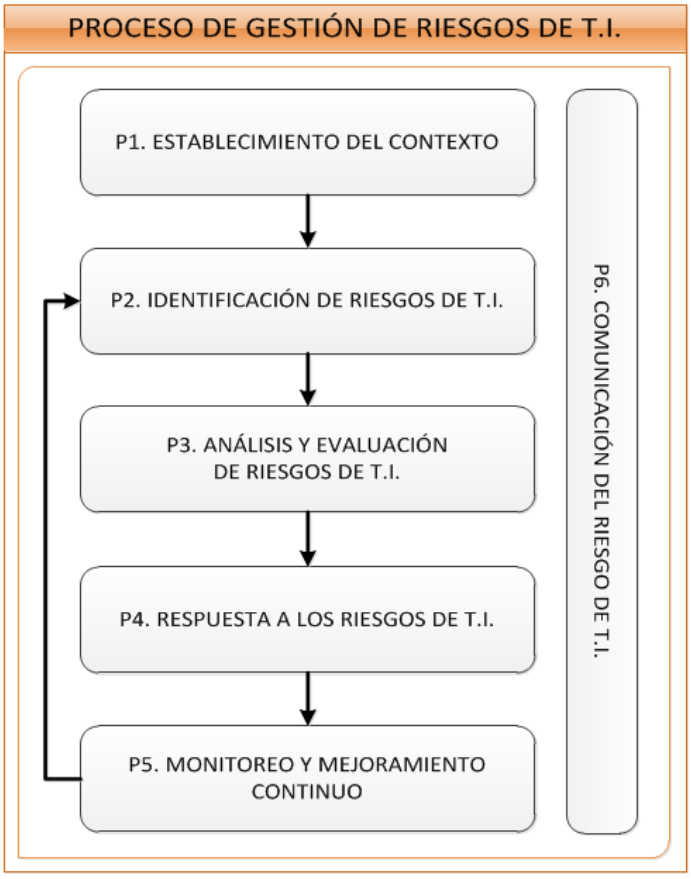

Figura 10. Procesos de gestión de riesgos propuesta
Fuente: Propia

[31] INTERNATIONAL ORGANIZATION FOR STANDARIZATION. Safety aspects - Guidelines for their inclusion in standards. ISO/IEC Guide 51. Suiza: ISO, 1999. p. 3. (ISO/IEC Guide 51:1999)

La guía de implementación inicia su ciclo de vida con una iteración inicial en la cual se ejecutará todo el proceso en orden desde el establecimiento del contexto (P1). En futuras iteraciones, el proceso P1 no requiere ser ejecutado de nuevo, a menos que se manifiesten cambios relevantes en la institución que requieran modificar los objetivos y/o el alcance del proceso de gestión de riesgos propuesto. Al incorporar en el proceso las fases de "monitoreo del avance" y "comunicación y consulta", se adoptan buenas prácticas que permiten el mejoramiento continuo del proceso, con miras a lograr una futura madurez del mismo que permita incorporar buenas prácticas de procesos de gestión de riesgos más maduros como Risk IT ó ISO 31000.

A continuación se detallarán los procesos de la guía de implementación.

3.1 PROCESO P1: ESTABLECIMIENTO DEL CONTEXTO

En las figuras 11 y 12 se ilustra de manera general los componentes del proceso, incluyendo actividades, tareas, involucrados, entradas, salidas y herramientas.

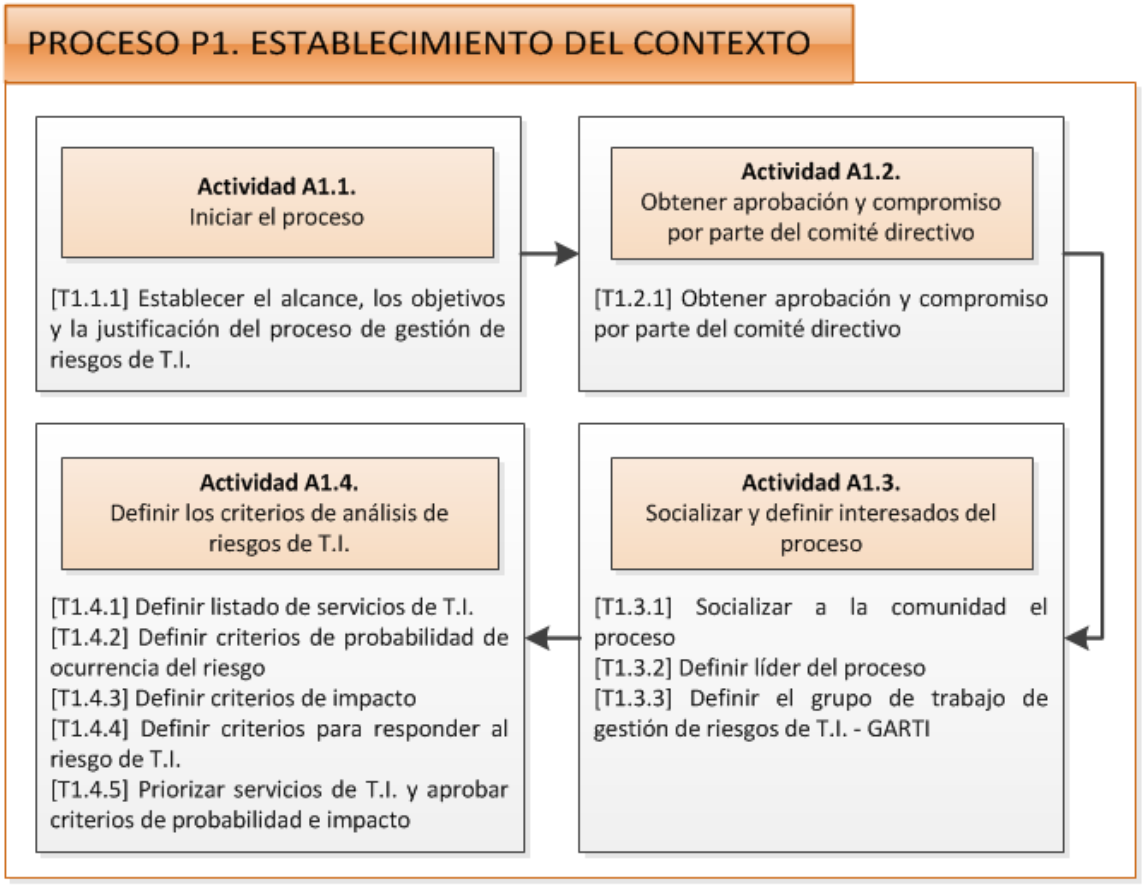

Figura 11. Componentes del proceso P1: Establecimiento del contexto
Fuente: Propia

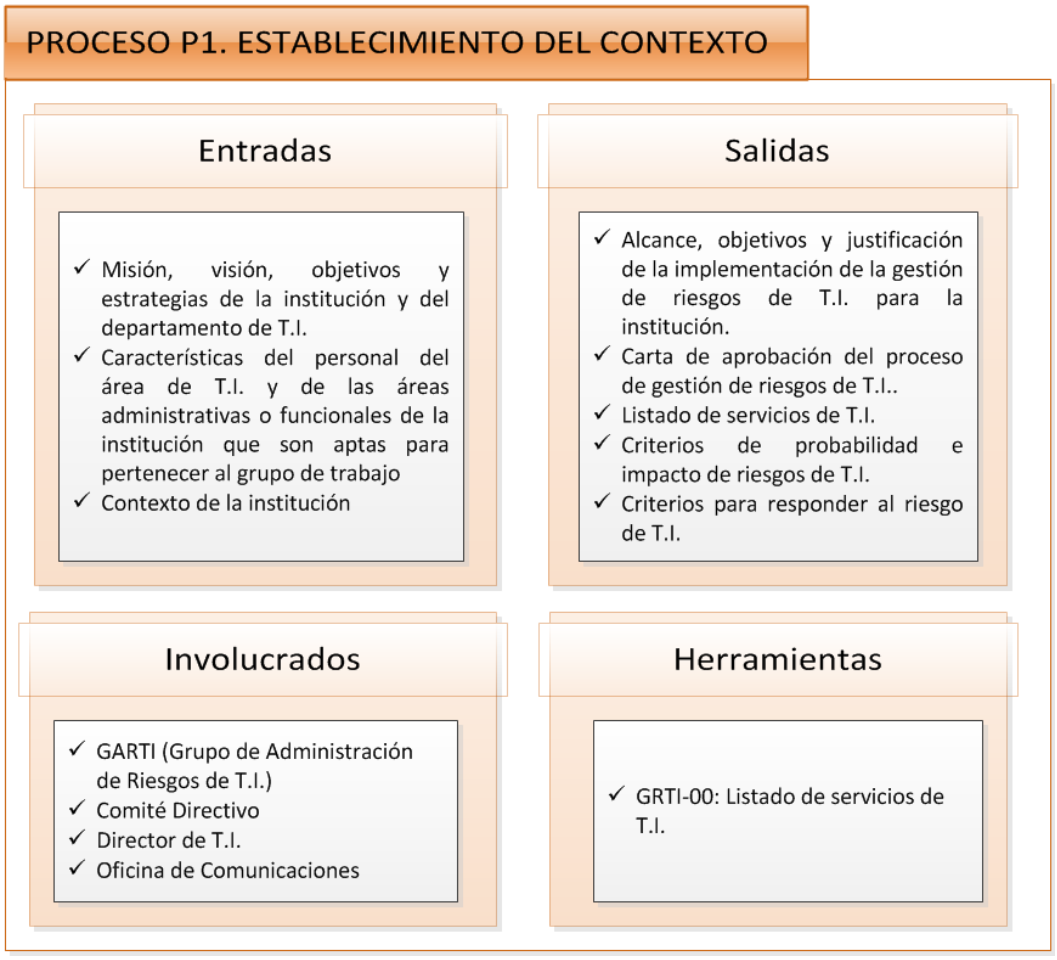

Figura 12. Componentes del proceso P1: Establecimiento del contexto (Continuación)
Fuente: Propia

El proceso P1 busca contextualizar la institución dentro de lo que será el proceso de gestión de riesgos de tecnología que se implementará en la institución. Para ello, el director del área de T.I. deberá de manera concisa definir el alcance, los objetivos y beneficios que la gestión de riesgos de tecnología traerá a la institución, enmarcado en los objetivos estratégicos de la misma. Después de definir estos aspectos, deberá presentar la propuesta de implementación de la gestión de riesgos de T.I. al comité directivo de la institución, con el objetivo de socializar y obtener su aprobación.

Después de contar con el apoyo de la gerencia, se debe definir el usuario líder del proceso y crear el grupo que trabajará durante todo el proceso de implementación. Finalmente, se define el conjunto de servicios de T.I. de la organización (que servirán como insumo para generar el listado de riesgos de T.I. en el próximo proceso) y los criterios con los que se clasificarán los riesgos de T.I. Éstos últimos dos elementos deberán ser puestos a consideración del comité directivo para su revisión y aprobación.

Este proceso se compone de las siguientes actividades y tareas:

3.1.1 Actividad A1.1: Iniciar el proceso

Esta actividad pretende establecer los objetivos, el alcance y la justificación del proceso de gestión de riesgos de T.I., insumos para la presentación de la propuesta de implementación que se realiza en la siguiente actividad.

Para cumplir los objetivos de la actividad se cuenta con la siguiente tarea:

Tarea	T1.1.1: Establecer el alcance, los objetivos y la justificación del proceso de gestión de riesgos de T.I.
Objetivos	Definir el alcance, los objetivos y la justificación de la gestión de riesgos de T.I. de la Institución
Entradas	Misión, visión, objetivos y estrategias de la institución y del departamento de T.I.
Salidas	Alcance, objetivos y justificación de la implementación de la gestión de riesgos de T.I. para la institución.
Involucrados	Director de T.I.

Tabla 13. Descripción de la tarea T1.1.1.
Fuente: Propia

El director de T.I., usando el contexto dado por la misión, visión, objetivos y estrategias tanto de la institución como del departamento de T.I., debe definir el alcance, los objetivos y la justificación de la implementación de la gestión de riesgos de T.I en la institución.

3.1.2 Actividad A1.2: Obtener aprobación y compromiso por parte del comité directivo

Esta actividad busca obtener la aprobación de la implementación del proceso de gestión de riesgos de T.I. por parte del comité directivo, como también su apoyo y compromiso hacia el mismo. Dado que eventualmente se requerirán recursos para afrontar los riesgos, es importante cumplir esta actividad para que la gerencia, con el compromiso adquirido al inicio del proceso, lo respalde y apruebe el presupuesto que se requiera.

Para cumplir los objetivos de la actividad se cuenta con la siguiente tarea:

Tarea	T1.2.1: Obtener aprobación y compromiso por parte del comité

	directivo
Objetivos	Obtener la aprobación y compromiso del proceso de gestión de riesgos de T.I. por parte del comité directivo.
Entradas	Alcance, objetivos y justificación de la implementación del proceso de gestión de riesgos de T.I.
Salidas	Carta de aprobación del proceso de gestión de riesgos de T.I. Acta de la reunión
Involucrados	Director de T.I., Comité Directivo

Tabla 14. Descripción de la tarea T1.2.1.
Fuente: Propia

El director del área de T.I., teniendo ya claros los objetivos, el alcance y la justificación de la implementación de la gestión de riesgos de T.I en la institución, debe exponer a un nivel gerencial el proceso de gestión de riesgos de T.I. al comité directivo de la institución, haciendo énfasis en los objetivos, alcance y beneficios esperados que se obtendrán a partir de la implementación del proceso.

Finalmente, después de la revisión y acatando las observaciones dadas por el comité directivo respecto al proceso, se firma en conjunto una carta de aprobación y compromiso del proceso de gestión de riesgos de T.I.

3.1.3 Actividad A1.3: Socializar y definir interesados del proceso

Esta actividad busca socializar a la comunidad universitaria los beneficios esperados que se derivarán de la implementación de una gestión de riesgos de T.I., para lograr de esta manera un entendimiento básico del esfuerzo a emprender y un apoyo de la gente en caso que se requiera su colaboración a lo largo de la ejecución del proceso.

De igual manera, en esta actividad se debe definir un usuario líder del proceso. Se propone la conformación de un grupo de trabajo, el cual será el responsable del buen funcionamiento del proceso de gestión de riesgos de T.I.

Para cumplir los objetivos de la actividad se cuenta con las siguientes tareas:

Tarea	T1.3.1: Socializar a la comunidad el proceso
Objetivos	Comunicar a la comunidad universitaria la implementación del proceso de gestión de riesgos de T.I., haciendo énfasis en sus beneficios esperados
Entradas	Alcance, objetivos y justificación de la implementación de la gestión de riesgos de T.I. para la institución.
Salidas	Comunidad universitaria con el conocimiento básico del proceso y sus beneficios esperados
Involucrados	Director de T.I., oficina de comunicaciones, comunidad universitaria

Tabla 15. Descripción de la tarea T1.3.1.
Fuente: Propia

Esta tarea consiste en comunicar a la comunidad universitaria la implementación del proceso de gestión de riesgos de T.I., para que haya un entendimiento básico del proceso y poder contar con el apoyo de la gente en caso que se requiera su colaboración a lo largo de la ejecución del proceso.
Se recomienda que la estrategia de comunicación sea coordinada con el apoyo de la oficina de comunicaciones de la institución, con el objetivo de tener más impacto y llegar de manera más efectiva a la comunidad universitaria.

Tarea	T1.3.2: Definir líder del proceso de gestión de riesgos de T.I.
Objetivos	Definir la persona responsable del proceso
Entradas	Posibles candidatos al rol
Salidas	Líder del proceso definido
Involucrados	Director de T.I.

Tabla 16. Descripción de la tarea T1.3.2.
Fuente: Propia

El director del área de T.I. debe definir una persona que será el usuario líder del proceso. Ésta persona será el responsable de la gestión de los documentos que soportan el proceso, será la única persona autorizada para hacer cambios en el mismo y tendrá la responsabilidad de asegurar su efectividad. Finalmente, será el punto de contacto para cualquier información relativa al proceso y será el responsable de elaborar los informes gerenciales[32].

[32] WIKIPEDIA. Artículo “Business process improvement”, sección “Process Owner” [en línea] <http://en.wikipedia.org/wiki/Business_process_improvement> [citado en 30 de octubre de 2012]

Tarea	T1.3.3: Definir el grupo de trabajo de gestión de riesgos de T.I. - GARTI
Objetivos	Conformar un grupo que esté al frente de la ejecución y mejoramiento continuo del proceso de gestión de riesgos de T.I.
Entradas	Características del personal del área de T.I. y de las áreas administrativas o funcionales de la institución que son aptas para pertenecer al grupo de trabajo
Salidas	Definición del grupo de administración de riesgos de T.I., GARTI.
Involucrados	Director de T.I.

Tabla 17. Descripción de la tarea T1.3.3.
Fuente: Propia

El director del área de T.I. y el líder del proceso deben definir qué personas son piezas claves que contribuyan a la ejecución del proceso de gestión de riesgos de T.I. Para esto, se debe tener en cuenta el nivel de conocimiento, experiencia y empoderamiento necesario para poder ser responsable de un plan de respuesta a un riesgo de T.I. En el proceso, este grupo de personas será denominado el grupo de administración de riesgos de T.I., GARTI.

En este grupo se coordinarán todas las actividades relacionadas con la gestión de riesgos y serán los responsables de llevar a cabo las acciones que deriven de la ejecución del proceso, además de garantizar su efectividad.

Se recomienda que el grupo GARTI sea interdisciplinario y esté conformado por el director del área de T.I., el líder del proceso de gestión de riesgos de T.I. y al menos un representante de las siguientes oficinas de la institución:

- Oficina de infraestructura de T.I.
- Oficina de soporte o mesa de ayuda
- Oficina de desarrollo de aplicaciones (si aplica)
- Oficina de planta física o servicios generales
- Departamento académico de TIC's o decanatura de ingeniería (si aplica)

3.1.4 Actividad A1.4: Definir los criterios de análisis de riesgos de T.I.

Esta actividad tiene como fin definir los criterios con los cuales serán listados y evaluados los riesgos de T.I. Estos criterios serán usados para determinar la prioridad de los riesgos y la manera de tratarlos.

Para cumplir los objetivos de la actividad se cuenta con las siguientes tareas:

Tarea	T1.4.1: Definir listado de servicios de T.I.
Objetivos	Definir un listado de los servicios de T.I. de la institución.
Entradas	Conocimiento de los servicios ofrecidos por el área de T.I.
Salidas	Listado de servicios de T.I. definido [Plantilla GRTI-00]
Involucrados	Director de T.I., grupo GARTI

Tabla 18. Descripción de la tarea T1.4.1.
Fuente: Propia

El director de T.I., en compañía con el grupo GARTI, elaborará un listado de todos los servicios que presta el área de T.I. sobre los cuales se apoya la operación de la institución. De acuerdo a ITIL[33], "un servicio de T.I. se compone de una combinación de personas, procesos y tecnología, basado en el uso de las T.I. y soportando uno o más procesos de negocio de la institución.".
Estos servicios están apoyados en los recursos que ofrece a institución. Usando la definición de CobiT[34], los recursos de TI pueden clasificarse en cuatro categorías:

- Las aplicaciones, incluyendo tanto sistemas de usuario automatizados como procedimientos manuales que procesan información.
- La información, que son los datos en todas sus formas, procesados y generados por los sistemas de información, en cualquier forma en que sean utilizados por el negocio
- La infraestructura, que es la tecnología y las instalaciones (hardware, sistemas operativos, sistemas de administración de base de datos, redes, multimedia, etc., así como el sitio donde se encuentran y el ambiente que los soporta) que permiten el procesamiento de las aplicaciones.
- Las personas, que son el personal requerido para planear, organizar, adquirir, implementar, entregar, soportar, monitorear y evaluar los sistemas y los servicios de información. Estas pueden ser internas, por tercerización o contratadas, de acuerdo a como se requieran.

Como apoyo a esta tarea se propone el uso de la plantilla [GRTI-00 - Listado de servicios de T.I.], en la cual se ofrece un listado de servicios genéricos en los que cada institución puede basarse para agregar o eliminar registros si es necesario.

[33] ITIL® Glossary v01, 1 May 2006: Acronyms. [en línea]. <http://www.itil-officialsite.com/nmsruntime/saveasdialog.aspx?lID=925&sID> p. 56. [citado en 14 de diciembre de 2012]
[34] ISACA. CobiT®. Versión 4.1. Rolling Meadows, Illinois, Estados Unidos de América: ISACA, 2007. p. 12. ISBN 1-933284-72-2.

Tarea	T1.4.2. Definir criterios de probabilidad de ocurrencia del riesgo
Objetivos	Definir un esquema cualitativo y cuantitativo que permita analizar la probabilidad de ocurrencia de un riesgo de T.I. en la institución
Entradas	Contexto de la institución
Salidas	Criterios de probabilidad de riesgos de T.I.
Involucrados	Director de T.I., Grupo GARTI

Tabla 19. Descripción de la tarea T1.4.2.
Fuente: Propia

El director de T.I., en compañía con el grupo GARTI, se encargará de definir un esquema cualitativo y/o cuantitativo que les permita determinar la probabilidad de ocurrencia de los riesgos a analizar, de acuerdo al contexto de la institución.

Esta guía propone el siguiente esquema cualitativo y cuantitativo para definir la probabilidad de los riesgos a analizar por el proceso de gestión de riesgos de T.I., basado en el documento "Managing IT Risk University-Wide" de Ian Waters[35], la cual puede ser ajustada al contexto de la institución.

- *(1)-Bajo*: El riesgo puede ocurrir con una frecuencia de seis meses o más, dadas las condiciones normales de operación de la institución.

- *(2)-Medio*: El riesgo puede ocurrir con una frecuencia de tres a seis meses, dadas las condiciones normales de operación de la institución.

- *(3)-Alto*: El riesgo puede ocurrir con una frecuencia de uno a tres meses, dadas las condiciones normales de operación de la institución.

- *(4)-Muy alto*: El riesgo puede ocurrir con una frecuencia de un mes o menos, dadas las condiciones normales de operación de la institución.

Estos criterios de probabilidad definidos serán usados como herramienta de análisis en el proceso de análisis de riesgos de T.I. e irán de la mano con la plantilla propuesta para dicho proceso [GRTI-02 - Análisis de riesgos de T.I.]

[35] WATERS, Ian. Managing IT Risk University-Wide [documento electrónico] <http://www.caudit.edu.au/educauseaustralasia07/authors_papers/Waters-212.pdf> p. 3. [citado en 30 de octubre de 2012]

Tarea	T1.4.3. Definir criterios de impacto del riesgo
Objetivos	Definir un esquema cualitativo y cuantitativo que permita analizar el impacto dada la ocurrencia de un riesgo de T.I. en la institución
Entradas	Contexto de la institución
Salidas	Criterios de impacto de riesgos de T.I.
Involucrados	Director de T.I., Grupo GARTI

Tabla 20. Descripción de la tarea T1.4.3.
Fuente: Propia

El director de T.I., en compañía con el grupo GARTI, se encargará de elaborar un esquema cualitativo y/o cuantitativo que les permita medir el impacto que pueda tener el riesgo de T.I. en la continuidad de los servicios de la institución, de acuerdo al contexto de la institución.

Como ejemplo la metodología propone el siguiente esquema cualitativo y cuantitativo para definir el impacto de los riesgos a analizar por el proceso de gestión de riesgos de T.I., basado de igual manera en el documento "Managing IT Risk University-Wide" de Ian Waters[36]:

- *(1)-Bajo*: Podrá tener un efecto menor sobre el servicio, pero no requerirá de una inversión extra para reparar o reconfigurar el sistema.

- *(2)-Medio*: Podrá existir un daño tangible, aunque no muy grande y tal vez sea perceptible sólo por unas pocas personas. Puede requerir una pequeña cantidad de recursos para solucionar el problema.

- *(3)-Alto*: Puede causar una caída prolongada de los sistemas y/o pérdida de clientes o confianza en el negocio. Gran cantidad de información o servicios de la institución pueden quedar comprometidos. Puede requerir gran cantidad de recursos para solucionar el problema.

- *(4)-Muy alto*: Puede causar que los sistemas queden permanentemente fuera de línea y/o deban ser remplazados por otros entornos más seguros. Puede resultar en una afectación completa de todos los servicios de la institución.

Estos criterios de impacto definidos serán usados como herramienta de análisis en el proceso de análisis de riesgos de T.I. e irán de la mano con la plantilla propuesta para dicho proceso [GRTI-02 - Análisis de riesgos de T.I.].

36 Ibid., p. 3.

Tarea	T1.4.4. Definir criterios para responder al riesgo de T.I.
Objetivos	Definir los criterios para responder a los riesgos de T.I.
Entradas	Contexto de la institución
Salidas	Criterios para responder al riesgo de T.I.
Involucrados	Director de T.I., Grupo GARTI

Tabla 21. Descripción de la tarea T1.4.4.
Fuente: Propia

En este punto, y de acuerdo con los criterios que se definieron en las dos tareas previas, se debe definir cuál será la respuesta de parte de la oficina de T.I. para responder al riesgo que se está evaluando.
Tomando como base los criterios de Risk IT[37], se definen las siguientes categorías de respuesta al riesgo de T.I.:

Aceptar Aceptación significa que no se toman medidas relativas con un riesgo de T.I particular, y la pérdida es aceptada si se produce. A diferencia de ignorar el riesgo, aceptar el riesgo supone que el riesgo es conocido; es decir, es una decisión informada y se ha aceptado por los directivos de la institución.

Transferir Transferir o compartir significa reducir la probabilidad del riesgo o su impacto mediante la transferencia o distribución de una parte del riesgo. Las técnicas más comunes es adquirir seguros o realizar tercerizaciones (*outsourcing*) para tratar el riesgo.

Mitigar La mitigación o reducción significa que están siendo tomadas medidas para detectar el riesgo, seguido por la definición de una acción y unos controles para reducir la probabilidad y/o el impacto de un riesgo de T.I.

Evitar Evitar significa no permitir la ejecución de las actividades o de las condiciones que dan lugar a riesgo de T.I. Esta categoría se aplica cuando no hay otra respuesta adecuada al riesgo debido a su costo o impacto.

Para decidir qué respuesta al riesgo se debe ejecutar, esta guía propone la siguiente evaluación, basado en el documento “Managing IT Risk University-Wide” de Ian Waters[38], la cual puede ser modificada para ajustarse al contexto de la institución. Bajo esta evaluación, la calificación del riesgo estará dada por la multiplicación entre el valor de la probabilidad con el valor del impacto:

Calificación = Probabilidad x Impacto

[37] ISACA. The Risk IT Framework. 2009. Rolling Meadows, Illinois, Estados Unidos de América: ISACA, 2009. p. 14. ISBN 978-1-60420-111-6.
[38] WATERS, Ian. Op Cit., p. 4. [citado en 30 de octubre de 2012]

Teniendo en cuenta estos valores, se define la siguiente matriz de calificación:

PROBABILIDAD \ IMPACTO	1	2	3	4
1	Bajo	Bajo	Medio	Medio
2	Bajo	Medio	Medio	Alto
3	Medio	Medio	Alto	Alto
4	Medio	Alto	Alto	Muy alto

Tabla 22. Matriz de calificación de riesgos
Fuente: Propia

Y se obtienen estas franjas de valores, las cuales podrán representar una opción de respuesta al riesgo de T.I:

Calificación / Franja	**Opciones de respuesta**	**Comentarios**
< 2: Bajo	Aceptar	Dada su bajo impacto o probabilidad puede ser más costoso ejecutar acciones que reduzcan la amenaza que el riesgo como tal, por lo que se recomienda la aceptación del mismo. Sin embargo, se debe realizar un seguimiento para evaluar si posteriormente cambian las características del riesgo y se requiera la implementación de controles.
3-6: Medio	Aceptar Mitigar	A pesar que no son riesgos críticos y no perjudican los intereses de la Universidad, se sugiere implementar acciones preventivas que reduzcan el impacto o probabilidad de la ocurrencia del riesgo.
7-12: Alto	Transferir Mitigar	La criticidad de estos riesgos es considerable y por tanto requieren un tratamiento oportuno para evitar que se materialicen y pongan en riesgo a la organización.
> 13: Muy alto	Transferir Mitigar Evitar	Debido a su alta criticidad, se deben tomar acciones correctivas inmediatas para prevenir la inminente materialización del riesgo de T.I; de lo contrario, se pueden ver perjudicados los intereses de la Universidad.

Tabla 23. Opciones de respuesta al riesgo de T.I.
Fuente: Propia

Tarea	T1.4.5. Priorizar servicios de T.I. y aprobar criterios de probabilidad e impacto
Objetivos	Obtener la aprobación de la gerencia de los criterios para calificar a los riesgos Priorizar los servicios de T.I. de acuerdo a los criterios de la gerencia
Entradas	Criterios de probabilidad e impacto de los riesgos y criterios para responder a los riesgos Listado de servicios de T.I. [GRTI-00: Listado de servicios de T.I.]
Salidas	Criterios aprobados Listado de servicios de T.I. priorizada [GRTI-00: Listado de servicios de T.I.]
Involucrados	Director de T.I., Comité directivo

Tabla 24. Descripción de la tarea T1.4.5.
Fuente: Propia

El director de T.I., después de ejecutar las tareas previas en conjunto con el grupo GARTI, debe reunirse con el comité directivo y exponer los criterios de probabilidad e impacto de los riesgos y los criterios para responder a los riesgos para obtener su aprobación.
De igual manera el comité directivo, de acuerdo a su criterio, debe realizar una priorización del listado de servicios acorde a la criticidad que representa cada uno para la institución.

3.2 PROCESO P2: IDENTIFICACIÓN DE RIESGOS DE T.I.

En la figura 13 se ilustra de manera general los componentes del proceso, incluyendo actividades, tareas, involucrados, entradas, salidas y herramientas.

Este proceso tiene como objetivo identificar aquellos riesgos relacionados con T.I. que, al afectar los servicios prestados por T.I., puedan degradar o retardar la consecución de los objetivos de la organización. Tomando como insumo el listado priorizado de servicios de T.I., el grupo de trabajo de riesgos de T.I. (GARTI), en conjunto con invitados que el grupo considere necesarios, realizan la identificación de todos los eventos que pueda afectar los servicios y por ende la operación de la institución; conformando así el conjunto de riesgos de T.I. a trabajar en la iteración del proceso de gestión de riesgos de T.I.

Este proceso se compone de las actividades y tareas que se encuentran en la siguiente página.

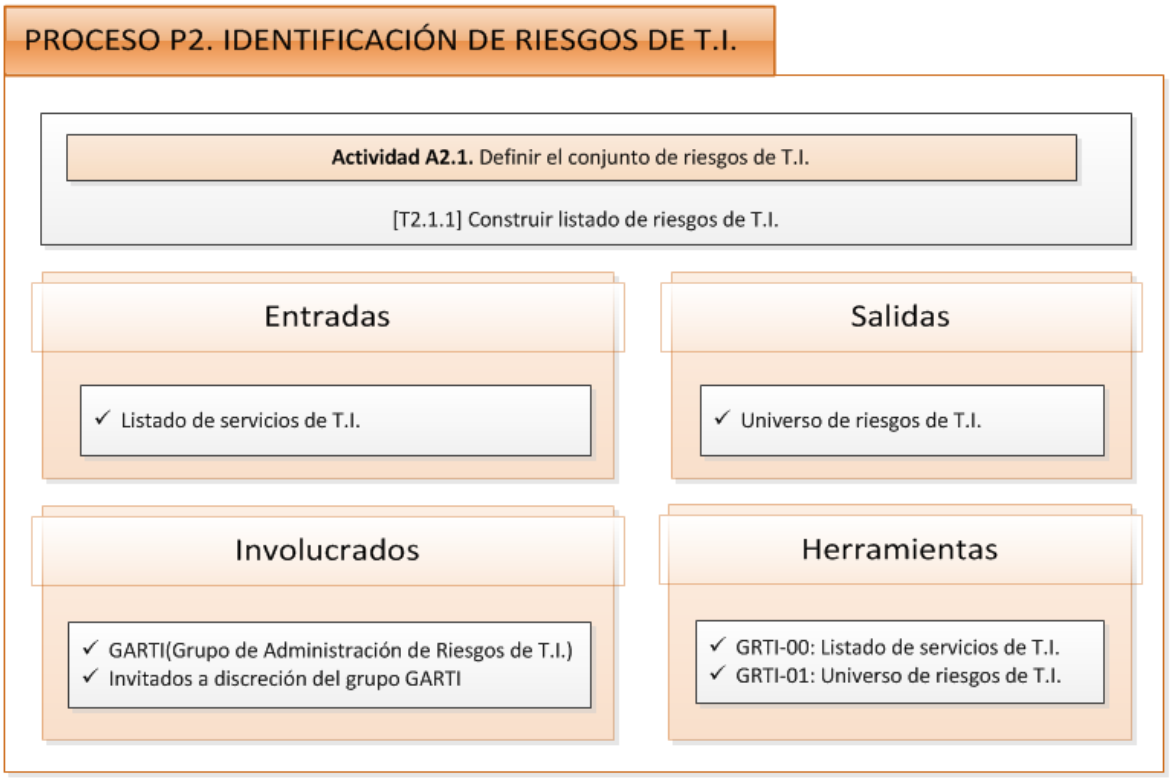

Figura 13. Componentes del proceso P2: Identificación de riesgos de T.I.
Fuente: Propia

3.2.1 Actividad A2.1: Definir el conjunto de riesgos de T.I.

En esta actividad se define el conjunto de eventos relacionados con T.I. que podrán afectar el cumplimiento de los objetivos de la Universidad.

Para cumplir los objetivos de la actividad se cuenta con la siguiente tarea:

Tarea	T2.1.1: Definir conjunto de riesgos de T.I. a trabajar
Objetivos	Definir el conjunto de eventos relacionados con T.I. que podrán afectar el cumplimiento de los objetivos de la organización.
Entradas	Listado de servicios de T.I [GRTI-00 - Listado de servicios de T.I.]
Salidas	Universo de riesgos de T.I [GRTI-01 - Universo de riesgos de T.I.]
Involucrados	Grupo GARTI, Invitados a discreción de GARTI

Tabla 25. Descripción de la tarea T2.1.1.
Fuente: Propia

En esta tarea se debe generar un listado de todos los eventos relacionados con tecnología que pueden afectar los servicios de T.I con mayor prioridad definidos por la Universidad. Para realizar este listado de riesgos, se propone que se tome como base el listado de servicios de T.I. priorizado creado previamente, concentrándose en los servicios de T.I. más críticos para la organización (se recomienda empezar por los diez primeros). En ejecuciones posteriores del proceso, se podrán analizar los siguientes servicios que no hayan sido tenidos en cuenta en las iteraciones anteriores.

Por cada servicio definido, se debe pensar qué eventos o amenazas pueden afectar el funcionamiento del mismo afectando la correcta disponibilidad de los servicios ofrecidos por la Universidad; esta información puede ser generada basada en experiencias pasadas o apoyándose en catálogos como el ofrecido por Magerit[39]. En la plantilla propuesta GRTI-01, la institución podrá diligenciar los riesgos que se consideren pertinentes. Vale aclarar que la prioridad del servicio dependerá de cada universidad que implemente el proceso.

Esta tarea debe ser llevada a cabo por el grupo GARTI. Sin embargo, dependiendo de la experticia sobre los servicios de T.I. analizados, el grupo puede invitar a participar de esta actividad a las personas que considere necesarios, con miras a cubrir todos los riesgos sobre los servicios de T.I.

Como apoyo a esta tarea se propone el uso de la plantilla [GRTI-01 - Universo de riesgos de T.I.]

3.3 PROCESO P3: ANÁLISIS Y EVALUACIÓN DE RIESGOS DE T.I.

En la figura 14 se ilustra de manera general los componentes del proceso, incluyendo actividades, tareas, involucrados, entradas, salidas y herramientas.

En este proceso se define para cada riesgo las causas y posibles consecuencias del mismo, así como se evalúa su impacto y probabilidad según los criterios establecidos en el proceso P1. Con la evaluación de los controles existentes, el impacto y probabilidad resultantes para cada riesgo, se obtiene una evaluación final de cada riesgo de T.I. Finalmente, se priorizan los riesgos de T.I., con miras a planificar las acciones para aquellos más críticos y que puedan afectar en mayor grado los objetivos institucionales.

[39] ESPAÑA, PORTAL DE ADMINISTRACIÓN ELECTRÓNICA. MAGERIT versión 2. Libro II. Catálogo de elementos. p. 27 [documento electrónico]. <http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184>. [citado en 30 de octubre de 2012]

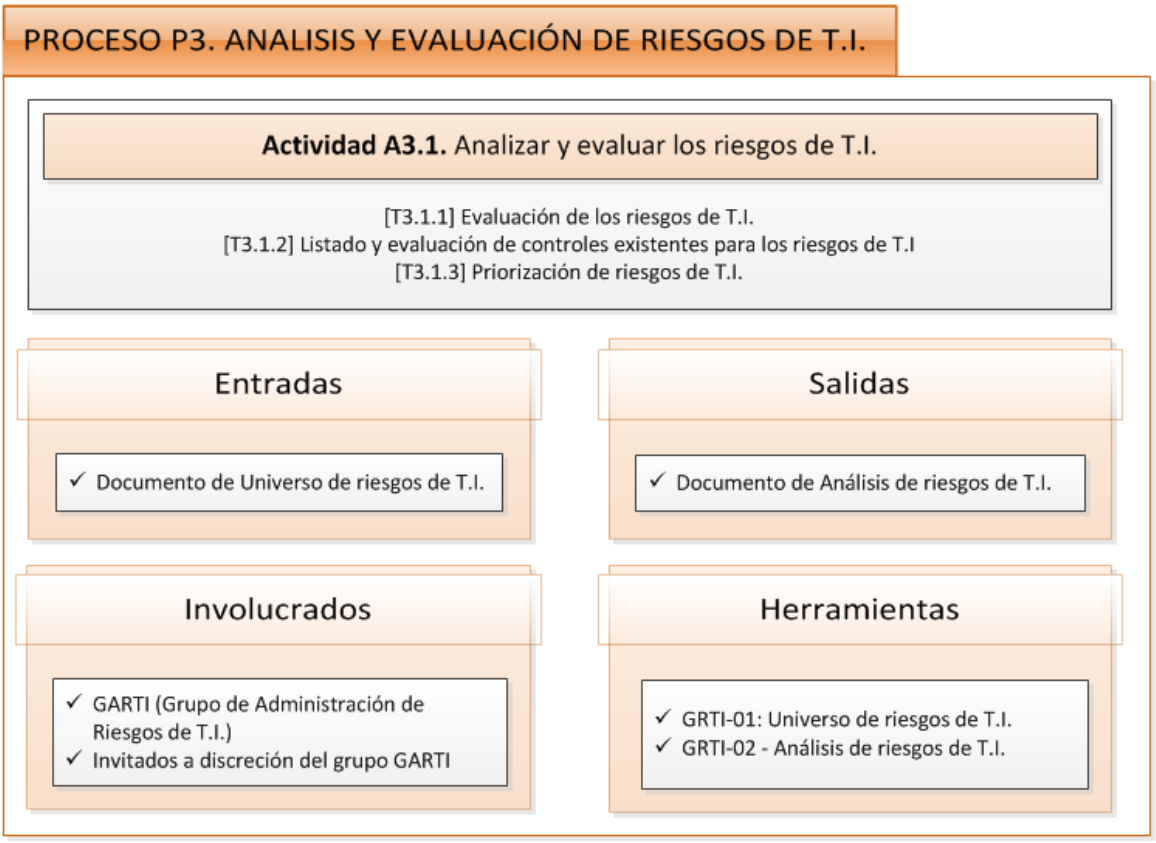

Figura 14. Componentes del proceso P3: Análisis y evaluación de riesgos de T.I.
Fuente: Propia

Este proceso se compone de la actividad y tareas descritas en la siguiente página.

3.3.1 Actividad A3.1: Analizar y evaluar los riesgos de T.I.

En esta actividad se busca realizar la priorización de los riesgos hallados en el proceso anterior, de acuerdo a la probabilidad e impacto del mismo basándose en los criterios definidos en el proceso de establecimiento del contexto. De igual manera, se realiza la revisión de controles ya aplicados para los riesgos de T.I. a evaluar, lo que permite verificar la efectividad de los mismos y priorizar aquellos que no tienen controles o los que no tienen controles efectivos.

Para cumplir los objetivos de la actividad se cuenta con las siguientes tareas:

Tarea	T3.1.1: Evaluación de los riesgos de T.I.
Objetivos	Realizar una evaluación de cada uno de los riesgos, analizando su probabilidad e impacto en la organización.
Entradas	Universo de riesgos de T.I. [GRTI-01 - Universo de riesgos de T.I.]
Salidas	Riesgos evaluados según su probabilidad e impacto, sin tener en cuenta controles establecidos [GRTI-02 - Análisis de riesgos de T.I.]
Involucrados	Grupo GARTI, Invitados a discreción de GARTI

Tabla 26. Descripción de la tarea T3.1.1.
Fuente: Propia

En esta tarea se busca evaluar cada uno de los riesgos del listado elaborado en la tarea T2.1.1 y evaluar su probabilidad y el impacto que puedan tener en la Universidad. Para empezar, para cada riesgo se deben describir las causas y posibles consecuencias del mismo en la institución, de tal manera que se tenga claro de dónde surge y qué puede afectar, para poder generar unos planes de respuesta adecuados. Posteriormente, se realizará una evaluación de cada riesgo.

La evaluación deberá hacerse en dos partes:

- En la primera parte (la que corresponde a esta tarea) se evaluará la probabilidad y el impacto que puede tener el riesgo, sin tener en cuenta los controles existentes que pudieran existir para el mismo en la institución en el momento de la evaluación.

- En la segunda parte, se listarán los controles que estén implementados para contrarrestar al riesgo y se hará una nueva evaluación del riesgo (teniendo en cuenta los controles), para determinar si las respuestas implementadas están siendo efectivas. Esta parte se describe en la tarea T.3.1.2.

Teniendo en cuenta lo anterior, en esta tarea se debe generar un valor inicial de probabilidad e impacto tomando como base las métricas establecidas en las tareas T1.4.2 y T1.4.3, sin contar con los controles establecidos para el riesgo.
Usando las métricas establecidas en la tarea T1.4.4, nos entregará una evaluación inicial del riesgo. Los encargados de llevar a cabo esta tarea son los miembros de GARTI y algún invitado de las áreas ajenas al grupo, del cual puedan requerir apoyo a la hora de analizar un riesgo de T.I. del cual no dominen su contexto.

Como apoyo a esta tarea se propone el uso de la plantilla [GRTI-02 - Análisis de riesgos de T.I.]

Tarea	T3.1.2: Listado y evaluación de controles existentes para los riesgos de T.I
Objetivos	Registrar qué controles están implementados actualmente en la organización y verificar su utilidad en el proceso.
Entradas	Riesgos evaluados según su probabilidad e impacto en la plantilla [GRTI-02 - Análisis de riesgos de T.I.]
Salidas	Riesgos evaluados según su probabilidad e impacto, teniendo en cuenta los controles aplicados en la institución [GRTI-02 - Análisis de riesgos de T.I.]
Involucrados	Grupo GARTI

Tabla 27. Descripción de la tarea T3.1.2.
Fuente: Propia

En esta tarea, el grupo GARTI complementa el análisis realizado del riesgo, listando los controles que ya han sido establecidos previamente en la institución para los riesgos de T.I. correspondientes.

Dependiendo si los controles para el riesgo son efectivos o no (es decir, si al ser aplicado disminuye la probabilidad y/o impacto iniciales), pueden modificar los valores de probabilidad o impacto iniciales (calculados en la tarea anterior). Por esto, en esta tarea se debe evaluar nuevamente y determinar el valor final de probabilidad e impacto, tomando como base las métricas establecidas en las tareas T1.4.2 y T1.4.3. Finalmente, usando las métricas establecidas en la tarea T1.4.4, nos entregará la evaluación definitiva del riesgo, lo que permitirá su priorización en la siguiente tarea.

Esta tarea nos permitirá analizar si los controles están siendo realmente efectivos, de tal manera que en el momento de generar el plan de respuesta al riesgo se tenga en cuenta esta información.

Como apoyo a esta tarea, se propone el uso de la plantilla [GRTI-02 - Análisis de riesgos de T.I.]

Tarea	T3.1.3: Priorización de riesgos de T.I.
Objetivos	Establecer una priorización de los riesgos, de tal manera que se pueda contar con un orden para elaborar los planes de respuesta a los riesgos.
Entradas	Riesgos evaluados según su probabilidad e impacto más controles aplicados históricamente en la plantilla [GRTI-02 - Análisis de riesgos de T.I.]
Salidas	Plantilla [GRTI-02 - Análisis de riesgos de T.I.] completada
Involucrados	Grupo GARTI

Tabla 28. Descripción de la tarea T3.1.3.
Fuente: Propia

En esta tarea el GARTI establece la priorización de los riesgos de T.I., basándose en la información obtenida de la probabilidad e impacto de los mismos y teniendo en cuenta los controles ya establecidos y la evaluación final de cada riesgo de T.I. Esta tarea tiene como fines enfocarse primero en los planes de respuesta para los riesgos de T.I más críticos que puedan repercutir en los objetivos institucionales.
Como apoyo a esta tarea se propone el uso de la plantilla [GRTI-02 - Análisis de riesgos de T.I.]

3.4 PROCESO P4: RESPUESTA A LOS RIESGOS DE T.I.

En las figuras 15 y 16 se ilustra de manera general los componentes del proceso, incluyendo actividades, tareas, involucrados, entradas, salidas y herramientas.

Este proceso busca tomar decisiones sobre el grado y la naturaleza de los tratamientos requeridos y sus prioridades, como también desarrollar e implementar planes de respuesta eficaces en términos de costos y con el objetivo de reducir las pérdidas potenciales y/o incrementar los beneficios. En este proceso se definen los responsables para dar tratamiento a cada uno de los riesgos resultantes del proceso anterior, para que ésta persona se encargue de elaborar un plan de acciones para dar una adecuada respuesta al riesgo. Posteriormente las posibles acciones para tratar el riesgo son aprobadas, priorizadas y planeadas por parte del encargado del grupo GARTI. Finalmente, el grupo GARTI realizará un seguimiento documentado a la ejecución de las acciones para tratar el riesgo.

Este proceso se compone de las siguientes actividades y tareas:

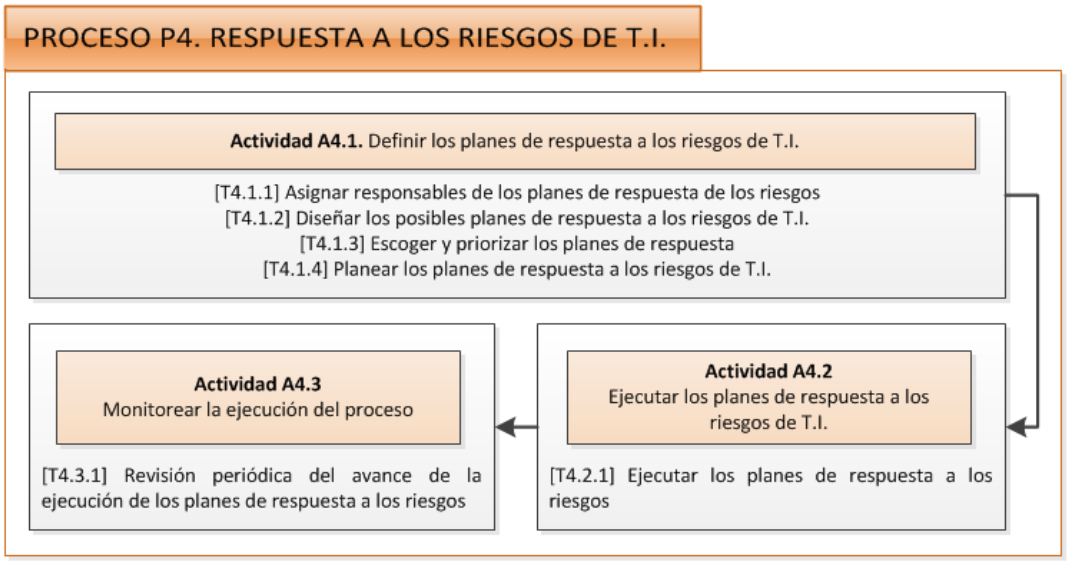

Figura 15. Componentes del proceso P4: Respuesta a los riesgos de T.I.
Fuente: Propia

Figura 16. Componentes del proceso P4: Respuesta a los riesgos de T.I. (Continuación)
Fuente: Propia

3.4.1 Actividad A4.1: Definir los planes de respuesta a los riesgos de T.I.

En esta actividad se escoge el responsable de la ejecución de las acciones definidas y la respuesta o respuestas que se deben ejecutar para tratar el riesgo de T.I.
Para cumplir los objetivos de la actividad se cuenta con las siguientes tareas:

Tarea	T4.1.1: Asignar responsables de los planes de respuesta de los riesgos
Objetivos	Asignar un responsable a cada riesgo que requiera un plan de respuesta
Entradas	Análisis de riesgos de T.I. [GRTI-02 - Análisis de riesgos de T.I.]
Salidas	Asignación de un responsable para la elaboración del plan de respuesta a cada riesgo a tratar
Involucrados	Grupo GARTI

Tabla 29. Descripción de la tarea T4.1.1.
Fuente: Propia

En esta tarea se asigna una persona responsable para cada riesgo de T.I. que requiera un plan de respuesta. La asignación, en lo posible, debe ser a la persona más idónea o que tenga más información y poder de decisión para poder dar tratamiento al riesgo de T.I. en revisión. Como candidatos a responsables de planes de respuesta para un riesgo de T.I. pueden ser tenidos en cuenta en primera instancia los miembros de GARTI; sin embargo, si dentro del grupo no hay una persona que cuente con las facultades de conocimiento o empoderamiento suficiente para poder llevar a cabo la planeación y ejecución del tratamiento del riesgo de T.I., se debe buscar el apoyo de una persona externa al grupo que pueda hacerlo. Si la persona elegida como responsable de plan de respuesta no pertenece a GARTI, se le debe explicar cuáles son sus responsabilidades con el proceso de gestión de riesgos de T.I. y se le faculta para que evalúe las posibilidades para enfrentar el riesgo de T.I.
Como apoyo a esta tarea se propone el uso de la plantilla [GRTI-03 - Respuesta a los riesgos de T.I.]

Tarea	T4.1.2: Diseñar los posibles planes de respuesta a los riesgos de T.I.
Objetivos	Diseñar planes de respuesta que permitan tratar el riesgo de T.I. y que sean eficaces en términos económicos
Entradas	Riesgo de T.I a tratar asignado por el GARTI.
Salidas	Alternativas de planes de respuesta al riesgo de T.I
Involucrados	Responsable de plan de respuesta a riesgos de T.I.

Tabla 30. Descripción de la tarea T4.1.2.
Fuente: Propia

En esta tarea, cada responsable de plan de respuesta a riesgos de T.I. diseñará un plan de respuesta al riesgo de T.I., teniendo en cuenta todas las posibles acciones o controles de respuesta incluyendo factores tales como complejidad, costo, esfuerzo requerido, plazo de ejecución, etc.
Se recomienda que los planes de respuesta complejos se manejen como un proyecto, incluyendo análisis de viabilidad técnica, económica y de recursos necesarios para ejecutarlo.

Tarea	T4.1.3. Escoger y priorizar los planes de respuesta
Objetivos	Seleccionar los mejores planes de respuesta al riesgo de T.I
Entradas	Alternativas de planes de respuesta al riesgo de T.I
Salidas	Plan de respuesta elegidos para dar tratamiento al riesgo de T.I., ya priorizados [GRTI-03 - Respuesta a los riesgos de T.I.]
Involucrados	Grupo GARTI, Responsable de plan de respuesta a riesgos de T.I.

Tabla 31. Descripción de la tarea T4.1.3.
Fuente: Propia

En esta tarea, cada responsable expone ante el grupo GARTI las alternativas diseñadas de planes de respuesta a riesgos de T.I. El grupo, escoge en consenso los planes de respuesta que más se ajusten a la realidad y necesidades de la organización, dependiendo de su viabilidad para ser implementados en términos de tiempo y recursos necesarios para su ejecución. Finalmente, se realiza una priorización de los planes de respuesta escogidos, para definir su orden de ejecución.

La priorización de los planes de respuesta se debe basar en la siguiente información:

- Prioridad del servicio o servicios de T.I. asociados al riesgo que se maneja

- Complejidad de los procesos de aprobación requeridos para obtener los recursos necesarios.

- Disponibilidad de los recursos necesarios para su ejecución.

- Tiempo requerido para su ejecución.

Como apoyo a esta tarea se propone el uso de la plantilla [GRTI-03 - Respuesta a los riesgos de T.I.]

Tarea	T4.1.4. Planear los planes de respuesta a los riesgos de T.I.
Objetivos	Planear el inicio de los planes de respuesta a los riesgos de T.I.
Entradas	Planes de respuesta a riesgos de T.I. elegidos para ser ejecutados [GRTI-03 - Respuesta a los riesgos de T.I.]
Salidas	Cronograma de implementación para los planes de respuesta a los riesgos de T.I
Involucrados	Grupo GARTI, Responsables de los planes de respuesta a riesgos de T.I., Comité Directivo (si es necesario)

Tabla 32. Descripción de la tarea T4.1.4.
Fuente: Propia

En este paso se debe evaluar si existe la disponibilidad de los recursos necesarios para poder elaborar un cronograma de implementación del plan de respuesta. Si el plan de respuesta de un riesgo de T.I. elegido tiene implicaciones económicas que se salen del presupuesto actual, se debe decidir si el riesgo puede dar espera al presupuesto del año siguiente o, en caso contrario, exponer la situación al comité directivo para que aprueben el presupuesto necesario y dar tratamiento oportuno al riesgo de T.I en cuestión. Después de tener definido lo anterior, los responsables de planes de respuesta de riesgos de T.I. definen el cronograma de ejecución del plan de acuerdo a la disponibilidad de recursos y la urgencia del manejo del riesgo. Como apoyo a esta tarea se propone el uso de la plantilla [GRTI-03 - Respuesta a los riesgos de T.I.]

3.4.2 Actividad A4.2: Ejecutar los planes de respuesta a los riesgos de T.I.

Cada plan que fue planeado y aprobado en la tarea previa inicia su ejecución.
Esta actividad consta de la siguiente tarea:

Tarea	T4.2.1: Ejecutar los planes de respuesta a los riesgos
Objetivos	Ejecutar cada uno de los planes de respuesta a los riesgos definidos y aprobados.
Entradas	Planes de respuesta a riesgos definidos en la actividad anterior [GRTI-03 - Respuesta a los riesgos de T.I.]
Salidas	Plantilla de análisis de riesgos actualizada [GRTI-02 - Análisis de riesgos]
Involucrados	Responsable de plan de respuesta a riesgos de T.I.

Tabla 33. Descripción de la tarea T4.2.1.
Fuente: Propia

En este punto, cada plan de respuesta que fue concebido y aprobado inicia su ejecución formal. Cuando el plan de respuesta finalice, se debe realizar la respectiva actualización del documento de análisis de riesgos de T.I., teniendo en cuenta la efectividad de los controles aplicados por el plan ejecutado.
Como apoyo a esta tarea se propone el uso de las plantillas [GRTI-03 - Respuesta a los riesgos de T.I.] y [GRTI-02 - Análisis de riesgos].

3.4.3 Actividad A4.3: Monitorear la ejecución del proceso

Esta actividad busca monitorear la eficacia de la ejecución de las actividades planeadas para dar tratamiento a los riesgos de T.I. identificados.
Para cumplir los objetivos de la actividad se cuenta con la siguiente tarea:

Tarea	T4.3.1: Revisión periódica del avance de la ejecución de los planes de respuesta a los riesgos
Objetivos	Identificar posibles fallas en la ejecución de los planes de respuesta establecidos por el proceso, para tomar acciones correctivas frente al tratamiento del riesgo de T.I.
Entradas	Planes de respuesta a riesgos de T.I. [GRTI-03 - Respuesta a los riesgos de T.I.]
Salidas	Documento de seguimiento de planes de respuesta a riesgos de T.I. [GRTI-04 - Seguimiento al plan] Lecciones aprendidas
Involucrados	Grupo GARTI, Responsable de plan de respuesta a riesgos de T.I.

Tabla 34. Descripción de la tarea T4.3.1.
Fuente: Propia

En esta tarea el grupo GARTI, en conjunto con cada encargado de la ejecución de los planes de respuesta, evalúan el avance del tratamiento de los riesgos según lo planeado, identificando las posibles causas de retraso y tomando las correcciones necesarias para poder cumplir con el objetivo propuesto del plan de respuesta. Se debe también documentar las lecciones aprendidas a lo largo de la ejecución del plan de respuesta.
Como apoyo a esta tarea se propone el uso de la plantilla [GRTI-04 - Seguimiento al plan].

3.5 PROCESO P5: MONITOREO Y MEJORAMIENTO CONTINUO

En la figura 17 se ilustra de manera general los componentes del proceso, incluyendo actividades, tareas, involucrados, entradas y salidas.

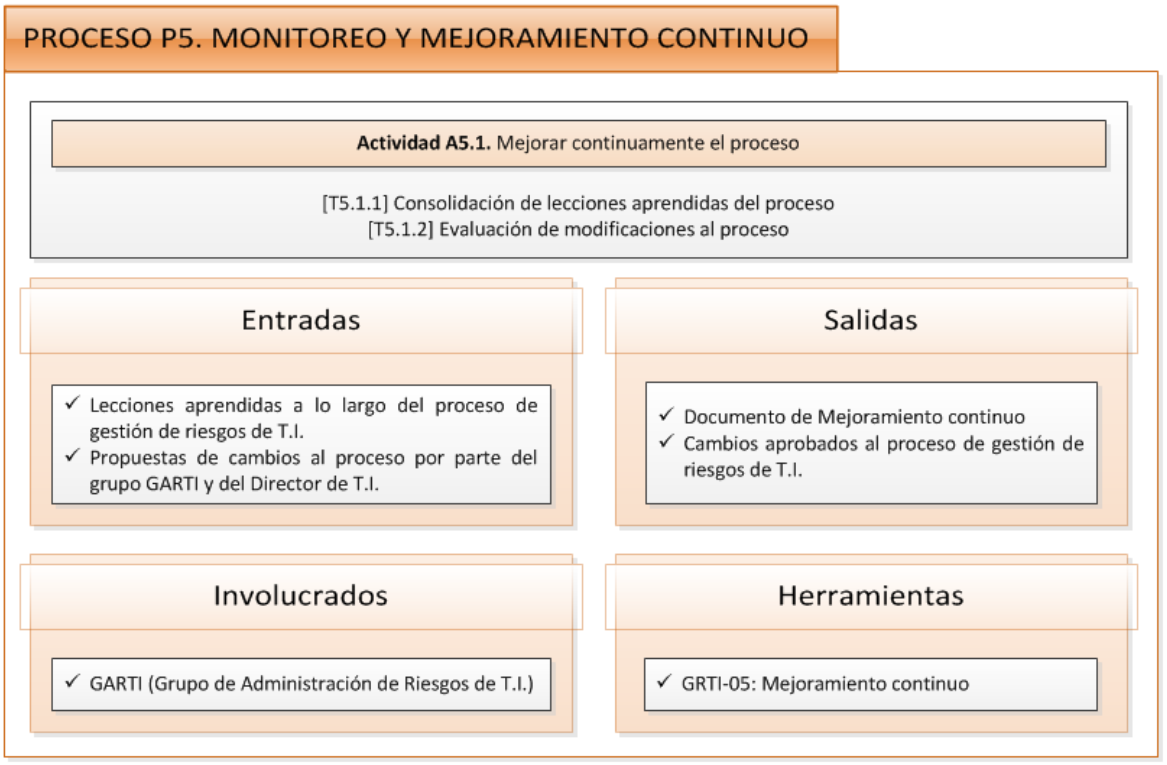

Figura 17. Componentes del proceso P5: Monitoreo y mejoramiento continuo
Fuente: Propia

Este proceso busca evaluar la eficacia del proceso de gestión de riesgo de T.I., con miras a que cumpla con los objetivos establecidos y se adapte de acuerdo a los cambios del entorno.

El objetivo es aplicar una mejora continua sobre el proceso, documentando las lecciones aprendidas con cada iteración del mismo en la institución y validando las propuestas de cambio que surjan dentro del grupo

Este proceso se compone de la siguiente actividad y tareas:

3.5.1 Actividad A5.1: Mejorar continuamente el proceso

Esta actividad busca que, con cada iteración del proceso de gestión de riesgos de T.I. establecido, queden documentadas las lecciones aprendidas a lo largo del mismo. De igual manera se recogen las propuestas de cambio al proceso, se evalúan y se llega a un consenso para realizar las modificaciones pertinentes.

Esta actividad consta de las siguientes tareas:

Tarea	T5.1.1: Consolidación de lecciones aprendidas del proceso
Objetivos	Documentar las lecciones aprendidas durante las iteraciones del proceso de gestión de riesgos de T.I.
Entradas	Lecciones aprendidas a lo largo del proceso
Salidas	Listado de lecciones aprendidas [GRTI-05: Mejoramiento continuo]
Involucrados	Grupo GARTI

Tabla 35. Descripción de la tarea T5.1.1.
Fuente: Propia

Después de cada iteración del proceso, el GARTI se reúne para recoger y analizar las lecciones aprendidas de la ejecución del mismo y se condensan en el listado de lecciones aprendidas, de tal manera que en siguientes ejecuciones se tengan en cuenta para evitar caer de nuevo en errores ya conocidos y mejorar el proceso.
De igual manera, basándose en esta información, se pueden proponer cambios que se tendrán en cuenta en la tarea siguiente.
Para esta tarea se recomienda el uso de la plantilla [GRTI-05 - Mejoramiento continuo].

Tarea	T5.1.2: Evaluación de modificaciones al proceso
Objetivos	Identificar los posibles cambios que se deben aplicar al proceso de gestión de riesgos de T.I.
Entradas	Propuestas de cambios al proceso
Salidas	Cambios al proceso [GRTI-05 - Mejoramiento continuo]
Involucrados	Grupo GARTI

Tabla 36. Descripción de la tarea T5.1.2.
Fuente: Propia

Al final de cada iteración de los procesos de gestión de riesgos de T.I., el grupo GARTI evalúa si se deben efectuar cambios sobre el proceso, sus actividades ó sus tareas, según las condiciones del entorno y las lecciones aprendidas; de esta manera, se adapta al cambio o se mejora el proceso de gestión de los riesgos de T.I. dentro de la Universidad.
Si el cambio propuesto para el proceso es significativo (es decir, modifica parámetros establecidos en el proceso de Establecimiento de contexto, tales como objetivos o los criterios de análisis), se recomienda que la siguiente iteración del proceso de gestión de riesgos debe ejecutar las tareas del proceso P1 a discreción del líder del proceso de gestión de riesgos de T.I.

Como apoyo a esta tarea se propone el uso de la plantilla [GRTI-05 - Mejoramiento continuo]

3.6 PROCESO P6. COMUNICACIÓN DEL RIESGO DE T.I.

En la figura 18 se ilustra de manera general los componentes del proceso, incluyendo actividades, tareas, involucrados, entradas y salidas.

Figura 18. Componentes del proceso P6: Comunicación del riesgo de T.I.
Fuente: Propia

El proceso de comunicación del riesgo de T.I. propuesto por esta metodología es un proceso transversal a todos los procesos de la misma. Tiene como objetivo mantener una comunicación adecuada y efectiva entre los interesados (*stakeholders*) del proceso de gestión de riesgos de T.I., y así poder cumplir con las actividades propuestas en la metodología. Este componente está inmerso a lo largo de los otros procesos de la guía propuesta de gestión de riesgos de T.I.

Un punto importante de este proceso es concienciar a la gerencia que la gestión de los riesgos de T.I. es un proceso importante de la organización y no debe ser considerado como un esfuerzo menor y aislado del área de T.I., sino un componente estratégico que permitirá apoyar la consecución de los objetivos de la institución.

Este proceso se compone de la siguiente actividad y tareas:

3.6.1 Actividad A6.1: Promover una comunicación efectiva del proceso de gestión de riesgos de T.I

La idea de esta actividad es manejar comunicaciones efectivas en las actividades del proceso de gestión de riesgos. Para esto se han definido un conjunto de tareas de comunicación a lo largo de los procesos (que están representadas en las tareas T6.1.1 y T6.1.2) y una tarea de generación de un informe gerencial, que establezca el estado actual del proceso para mantener informado al comité directivo de la institución.
Esta actividad consta de las siguientes tareas:

Tarea	T6.1.1: Comunicaciones del proceso con la gerencia
Objetivos	Involucrar y comprometer a la gerencia en el proceso de gestión de riesgos de T.I.
Entradas	Las correspondientes a las tareas T1.2.1, T1.4.5 y T4.1.4
Salidas	Las correspondientes a las tareas T1.2.1, T1.4.5 y T4.1.4
Involucrados	Director de T.I., Comité Directivo

Tabla 37. Descripción de la tarea T6.1.1.
Fuente: Propia

Ésta tarea macro tiene como objetivo principal el involucramiento de la gerencia en el proceso de gestión de riesgos de T.I. desde el principio del proceso. Dado que el proceso no es sólo responsabilidad del área de T.I., es importante contar con el apoyo de la gerencia para la toma de decisiones y la asignación de recursos correspondientes; además, al involucrar a la gerencia se hace conciencia que el proceso debe ser importante y estratégico para la institución, que permitirá apoyar la consecución de los objetivos de la misma.
Se espera que el director de T.I tenga las habilidades de negociación necesarias para obtener el patrocinio necesario del comité directivo, para poder ejecutar las acciones pertinentes ante los riesgos y la consecución de los recursos necesarios para ejecutar los planes que se definan.

Esta tarea macro está distribuida en las siguientes tareas a lo largo del proyecto:

T1.2.1. Obtener aprobación de los directivos
T1.4.5. Priorizar servicios de T.I. y aprobar criterios
T4.1.4. Planear los planes de respuesta a los riesgos

Tarea	T6.1.2: Comunicaciones del proceso con la comunidad universitaria
Objetivos	Comunicar a la comunidad universitaria la implementación del proceso de gestión de riesgos de T.I., haciendo énfasis en sus beneficios esperados
Entradas	Las correspondientes a la tarea T1.3.1
Salidas	Las correspondientes a la tarea T1.3.1
Involucrados	Director de T.I., Oficina de Comunicaciones, Comunidad universitaria

Tabla 38. Descripción de la tarea T6.1.2.
Fuente: Propia

En línea con la tarea anterior, ésta consiste en comunicar a la comunidad universitaria la implementación del proceso de gestión de riesgos de T.I., para que haya un entendimiento básico del proceso y poder generar conciencia en la gente de la importancia del proceso, en caso que se requiera su colaboración a lo largo de la ejecución del proceso. Es deseable que el director de T.I. se apoye en el área de comunicaciones de la institución para lograr este objetivo.
Esta tarea macro está representada en la tarea T1.3.1: Socializar a la comunidad el proceso, del proceso P1.

Tarea	T6.1.3: Informar a la gerencia del estado del proceso de gestión de riesgos de T.I.
Objetivos	Informar a la gerencia el estado del proceso de gestión de riesgos de T.I.
Entradas	Toda la información generada a lo largo del proceso de gestión de riesgos de T.I.
Salidas	Informe gerencial del estado del proceso de gestión de riesgos
Involucrados	Director de T.I., líder del proceso, comité directivo

Tabla 39. Descripción de la tarea T6.1.3.
Fuente: Propia

Con esta actividad se busca que el líder del proceso, con el apoyo del director de T.I., generen un informe a nivel gerencial del estado actual del proceso de gestión de riesgos de T.I. dirigido al Comité Directivo, el cual debe ser generado y presentado de manera periódica. La periodicidad de generación del informe queda a discreción del director de T.I.

De esta manera, se busca brindar el panorama general del proceso y generar conciencia de una cultura de riesgos de T.I.; haciendo énfasis en que éste es un proceso importante de la organización y no debe ser considerado como un esfuerzo menor y aislado del área de T.I., sino un componente estratégico que permite apoyar la consecución de los objetivos de la institución.

3.7 HERRAMIENTAS

Con base en la guía anterior, se ha definido una serie de plantillas para cada una de las etapas definidas en el proceso. La relación entre cada plantilla y los anexos de este documento, junto con una breve descripción del propósito de cada una de las plantillas, se encuentra en la siguiente tabla.

Plantilla	Nombre	Propósito	Anexo
GRTI-00	Listado de servicios de T.I.	La plantilla da soporte a algunas de las actividades del proceso P1–Establecimiento del contexto. Esta plantilla tiene como propósito definir un listado de los servicios de T.I, estableciendo para cada uno de ellos su responsable asociado, así como la criticidad y prioridad de acuerdo a los objetivos de la Universidad y de la percepción del comité directivo. También se recopilan las lecciones aprendidas del proceso de identificación y priorización de los servicios en este documento.	4
GRTI-01	Universo de riesgos de T.I.	La plantilla apoya las actividades del proceso P2 – Identificación de riesgos de T.I. En ésta se plasman los servicios críticos con prioridad definidos para trabajar en una iteración n, y para cada uno de estos se identifica los posibles riesgos asociados a los mismos. Una vez realizado dicho proceso, se priorizan los riesgos de acuerdo a la criticidad de los servicios que se pueden ver impactados por estos, buscando de esta manera enfocarse en dar tratamiento a los riesgos más relevantes para la organización. También se recopilan las lecciones aprendidas del proceso de identificación de riesgos en éste documento.	5
GRTI-02	Análisis de riesgos de T.I.	Ésta plantilla tiene como propósito dar soporte al proceso P3 – Análisis y evaluación de riesgos de T.I., en la cual, para cada riesgo del conjunto de riesgos a trabajar en una iteración dada, se procede a diligenciar sus causas, consecuencias, probabilidad de ocurrencia e impacto, obteniendo así una evaluación inicial. Luego, en conjunto con la efectividad de los controles existentes para el riesgo, más los criterios de probabilidad e impacto finales, se obtendrá una evaluación final del riesgo. También se recopilan las lecciones aprendidas del proceso de análisis de riesgos en éste documento.	6

GRTI-03	Respuesta a los riesgos de T.I.	Ésta plantilla tiene como propósito dar soporte al proceso P4 – Respuesta a los riesgos de T.I. En esta plantilla se documenta para aquellos riesgos resultantes del proceso de análisis cuáles son las opciones de manejo definidas para dar tratamiento al riesgo, así como el responsable de la ejecución de dichas acciones. Después, se define la prioridad de dichas acciones dependiendo de la factibilidad y viabilidad de las mismas y se asigna una fecha programada para ejecutar las acciones. También se recopilan las lecciones aprendidas del proceso de respuesta a los riesgos en éste documento.	7
GRTI-04	Seguimiento al plan	Ésta plantilla tiene como propósito dar soporte al proceso P4 – Respuesta a los riesgos de T.I. La finalidad de esta plantilla es documentar el seguimiento a la ejecución de las acciones planteadas para dar tratamiento a los riesgos. También se recopilan las lecciones aprendidas sobre la ejecución de las acciones de tratamiento a los riesgos en éste documento.	8
GRTI-05	Mejoramiento continuo	Ésta plantilla tiene como propósito dar soporte al proceso P5 – Monitoreo y mejoramiento continuo, buscando documentar las lecciones aprendidas sobre los procesos/actividades/tareas del proceso de gestión de riesgos implementado en la institución, así como los cambios aprobados ó no sobre el mismo con sus justificaciones respectivas.	9

Tabla 40. Listado de herramientas propuestas
Fuente: Propia

3.8 ROLES Y RESPONSABILIDADES

A continuación se detallan los roles involucrados en la ejecución de las tareas del proceso de gestión de riesgos de T.I.

- **Director de T.I.** Persona encargada del área de TI de la institución. Es la persona a cargo de la administración de los recursos y servicios de información de la institución que dan apoyo continuo a la operación de la Universidad.

- **Comité directivo.** Es el grupo de personas encargados de establecer los reglamentos internos, visión, misión, principios, estrategias y presupuesto para con la Universidad.

- **GARTI (Grupo de Administración de Riesgos de T.I).** Es el grupo encargado de velar por la correcta ejecución de las actividades del proceso de gestión de riesgos de T.I. así como de la mejora continua sobre el mismo a medida que se va iterando con el tiempo.

- **Líder del Proceso.** Es la persona responsable de la gestión de los documentos que soportan el proceso; será la única persona autorizada para hacer cambios en el mismo y tendrá la responsabilidad de asegurar su efectividad. Finalmente, será el punto de contacto para cualquier información relativa al proceso y será el responsable de elaborar los informes gerenciales.
- **Comunidad Universitaria**. Está integrada por estudiantes matriculados en cualquiera de las enseñanzas que se impartan en las institución, el personal investigador, el personal docente e investigador, y el de administración y servicios adscrito a la misma.

Las responsabilidades de cada uno de los roles se expresa en la siguiente matriz de asignación de responsabilidades, también conocida como matriz RACI.

Proceso/Recurso	Comité Directivo	Director de T.I.	Grupo GARTI	Líder del Proceso	Invitados por GARTI	Comunidad Universitaria
P1. Establecimiento del contexto	C	A	R	I		I
P2. Identificación de riesgos de T.I.	I	A	R	I	C*	
P3. Análisis y evaluación de riesgos de T.I.	I	A	R	I	C*	
P4. Respuesta a los riesgos de T.I.	C*	A	R	I	R*	
P5. Monitoreo y mejoramiento continuo	I	A	R	R		
P6. Comunicación del riesgo de T.I.	I	A/R	I	R		I

Tabla 41. Matriz de asignación de responsabilidades
Fuente: Propia

La descripción de las letras de la matriz anterior se detalla a continuación.

Rol	Descripción
[R] Responsable	Este rol realiza el trabajo y es responsable por su realización. Es quien debe ejecutar las tareas.
[A] Aprobador	Este rol se encarga de aprobar el trabajo finalizado y a partir de ese momento, se vuelve responsable por él. Es quien debe asegurar que se ejecutan las tareas
[C] Consultado	Este rol posee alguna información o capacidad necesaria para terminar el trabajo. Se le informa y se le consulta información, se utiliza una comunicación bidireccional.
[I] Informado	Este rol debe ser informado sobre el progreso y los resultados del trabajo. A diferencia del Consultado, la comunicación es unidireccional.

Tabla 42. Descripción de matriz de asignación de responsabilidades
Fuente: Propia

El asterisco indica que el involucramiento del rol es opcional.

3.9 GLOSARIO

A continuación se encuentra un glosario que puede ayudar al lector en la comprensión del documento.

Control	Medida que modifica el riesgo[40]
Evento	Ocurrencia o cambio de un conjunto particular de circunstancias[41]
Impacto	(Consecuencia) Resultado de un evento que afecta los objetivos[42]
Interesado	Persona u organización que puede afectar, ser afectado o percibirse afectado por una decisión o actividad[43]
Iteración	Método para resolver un problema mediante una serie de aproximaciones, que obtiene una solución más exacta utilizando la aproximación anterior como punto de inicio.[44]
Lección aprendida	Conocimiento obtenido del proceso de la ejecución del proyecto[45]
Probabilidad	Posibilidad que algo ocurra[46]
Recurso	Cualquier cosa que ayude a lograr los objetivos de TI. Incluye: las aplicaciones, la información, la infraestructura y las personas.[47]
Riesgo	Un evento o condición incierta que, de ocurrir, tendrá un efecto negativo o positivo en los objetivos del negocio[48]

[40] INTERNATIONAL ORGANIZATION FOR STANDARIZATION. Information technology – Security techniques – Information security risk management ISO/IEC 27005. Suiza: ISO, 2008. p. 2. (ISO 27005:2008)
[41] Ibid., p. 2.
[42] Ibid., p. 1.
[43] Ibid., p. 5.
[44] MATH DIRECTORY. Artículo “iteración” [en línea] <http://www.mathematicsdictionary.com/spanish/vmd/full/i/iteration.htm> [citado en 30 de octubre de 2012]
45 PROJECT MANAGEMENT INSTITUTE. A Guide to the Project Management Body of Knowledge (PMBOK® Guide). 4 ed. Newton Square, Pasadena, Estados Unidos de América: Project Management Institute, 2008. P.437. ISBN 978-1-933890-51-7
[46] INTERNATIONAL ORGANIZATION FOR STANDARIZATION. Op cit., p. 3.
[47] ISACA. CobiT®. Versión 4.1. Rolling Meadows, Illinois, Estados Unidos de América: ISACA, 2007. p.12. ISBN 1-933284-72-2.
[48] PROJECT MANAGEMENT INSTITUTE. Op cit., p. 446.

Riesgo de T.I.	Riesgo del negocio asociado con el uso, propiedad, operación, participación, la influencia y la adopción de las T.I. en una organización.[49]
Tecnologías de Información (T.I.)	(También conocidas como Tecnologías de Información y Comunicaciones - T.I.C.) Forma de denominar al conjunto de herramientas, habitualmente de naturaleza electrónica, utilizadas para la recolección, almacenamiento, tratamiento, difusión y transmisión de la información[50].

[49] ISACA. Op cit., p. 9.
[50] DEFINICION.ORG. Artículo “IT” [en línea] <http://www.definicion.org/it> [citado en 30 de octubre de 2012]

4. VALIDACIÓN DE LA PROPUESTA

Puesto que la propuesta de guía de implementación de mejores prácticas en gestión de riesgos de tecnologías de información fue producto de elaboración propia, debe tener un componente de validación adecuado; esto con el propósito de verificar que la guía es realmente aplicable al sector objetivo y que guarda una coherencia general en el proceso.

Debido al hecho que no se contaba con el tiempo necesario para realizar un proyecto piloto de implementación en una universidad y obtener su retroalimentación, se decidió someter la propuesta a un proceso de validación de contenido con base a un juicio de expertos.

Dado que el concepto de "experto" puede ser muy subjetivo, se definió un perfil que debía cumplir cada una de las personas para poder conformar este grupo. De esta manera, se definieron los siguientes requisitos para poder ser considerado como un experto en el área de gestión de riesgos de T.I.:

Conocimientos generales

El experto debe ser un egresado de ingeniería de sistemas o carreras afines, con conocimientos sobre uno o varios de los siguientes temas:

- Gobierno de TI
- Gestión de riesgos de TI
- Gestión de riesgos empresariales

De igual manera, es deseable que cuente con los conocimientos en uno o varios de los siguientes documentos relacionados con la gestión de riesgos de T.I.:

- PMBOK
- Risk Management SEI
- The Risk IT Framework
- Cobit
- Familia de normas ISO 27000
- Familia de normas ISO 31000
- NTC 5254
- Octave
- Magerit
- Mehari
- NIST 800-30

Experiencia:

El experto debe contar con experiencia en uno o más de los siguientes frentes:

- Experiencia en cargos relacionados con gestión de proyectos de TI
- Ser parte de un grupo de estudio de normas relacionadas con TI
- Profesor asociado o investigador de temas de TI de una asociación reconocida en el medio
- Auditor de procesos de TI

Teniendo en cuenta lo anterior, se realizó una búsqueda en Google de posibles candidatos para ser parte del juicio de expertos, como también una búsqueda entre los profesores asociados a la maestría en gestión de informática y telecomunicaciones de la Universidad Icesi. De esta manera, se obtuvieron seis perfiles que cumplían con los requisitos definidos anteriormente.
Paralelamente, se elaboró la encuesta que permitía validar la propuesta, basándose en los aspectos comunes de los documentos relacionados con la gestión de riesgos de T.I. estudiados en este proyecto, los cuales están registrados en la tabla 12 del apartado 2.3. Comparativo de los documentos base.

Posteriormente, a los expertos seleccionados se les envió un correo electrónico con instrucciones para diligenciar la encuesta que se elaboró con la herramienta Google Docs. En el anexo 2 se detalla el correo enviado a los expertos y la encuesta que se diseñó para evaluar la guía propuesta. Finalmente, los resultados de esta encuesta permitieron evaluar la guía de implementación propuesta.

5. RESULTADOS OBTENIDOS

Después de esperar respuesta por parte de los seis expertos consultados, dos personas respondieron al correo enviado, uno de manera colaborativa y el otro para notificar que no tenía disponibilidad para colaborar. De acuerdo a la respuesta del experto Andrés Ricardo Almanza, se obtuvo los siguientes resultados.

Referente a cómo el proceso de gestión de riesgos de T.I evaluado aborda el proceso de establecimiento del contexto:

- Está de acuerdo en la manera como el proceso evaluado establece una visión/contexto de los riesgos de T.I.
- Está de acuerdo con que el proceso evaluado da pautas para definir los criterios de evaluación de riesgos de T.I
- Está ligeramente de acuerdo con que el proceso de gestión de riesgos de T.I. evaluado se alinea con los objetivos de la empresa.
- Se considera en general el proceso evaluado de establecimiento del contexto como relevante, coherente y claro.

Referente a cómo el proceso de gestión de riesgos de T.I evaluado aborda el proceso de identificación de riesgos:

- Está en desacuerdo en la forma como el proceso evaluado aborda la definición del universo de los riesgos de T.I. existentes en la organización.
- Está ligeramente de acuerdo en la manera como el proceso evaluado realiza la priorización de los riesgos de T.I.
- Está ligeramente de acuerdo con la manera como el proceso evaluado identifica los riesgos de T.I. con mayor probabilidad de ocurrencia.
- Está ligeramente de acuerdo con la manera como el proceso evaluado identifica las consecuencias de los riesgos de T.I
- Se considera en el general el proceso evaluado de identificación de riesgos como relevante, coherente y claro.

Referente a como el proceso de gestión de riesgos de T.I evaluado aborda el proceso de análisis de riesgos

- Está en desacuerdo con la manera como el proceso evaluado da pautas para la evaluación de controles existentes
- Esta de acuerdo en la manera como el proceso evaluado define el método de evaluación de los riesgos de T.I.

- Está ligeramente de acuerdo en la manera como el proceso evaluado da pautas para la estimación del nivel de riesgo de los riesgos de T.I.
- Se considera en el general el proceso evaluado de análisis de riesgos como relevante, coherente y claro.

Referente a cómo el proceso de gestión de riesgos de T.I evaluado aborda el proceso de evaluación de riesgos:

- Esta de acuerdo en la manera como el proceso evaluado evalúa los riesgos de T.I. según su impacto y probabilidad.
- Está ligeramente de acuerdo en la manera como el proceso evaluado da pautas para la interpretación del resultado de la evaluación de los riesgos de T.I.
- Se considera en el general el proceso evaluado de evaluación de riesgos como relevante, coherente y claro.

Referente a cómo el proceso de gestión de riesgos de T.I evaluado aborda el proceso de tratamiento del riesgo:

- Está de acuerdo en la manera como el proceso evaluado define las estrategias para tratamiento de los riesgos de T.I.
- Está ligeramente de acuerdo en la manera como el proceso evaluado prepara e implementa los planes de acción de riesgos de T.I.
- Se considera en el general el proceso evaluado de tratamiento del riesgo como relevante, coherente y claro.

Referente a cómo el proceso de gestión de riesgos de T.I evaluado aborda el proceso de monitoreo y revisión.

- Está de acuerdo en la manera como el proceso evaluado evalúa constantemente el proceso completo de la gestión de riesgos de T.I. dependiendo de los cambios externos e internos relevantes para la organización.
- Está ligeramente de acuerdo en la manera como el proceso evaluado evalúa el cambio sobre los factores de riesgos de T.I. sobre los cuales se definen los mismos.
- Se considera en el general el proceso evaluado de monitoreo y revisión como relevante, coherente y claro.

Referente a cómo el proceso de gestión de riesgos de T.I evaluado aborda el proceso de comunicación y consulta:

- Está de acuerdo en la manera como el proceso evaluado define un plan de comunicaciones involucrando todos los interesados del proceso de gestión de riesgos de T.I.
- Está de acuerdo en la manera como el proceso evaluado define un nivel de comunicación claro y relevante a la naturaleza de los diferentes niveles jerárquicos de los interesados
- Se considera en el general el proceso evaluado de comunicación y consulta como relevante, coherente y claro.

Por último, el proceso de gestión de riesgos de T.I evaluado como un todo se considera que es relevante, coherente y claro.

Finalmente las anotaciones del juicio de experto como propuesta a mejorar el proceso evaluado fueron:

- La tabla de probabilidad por ocurrencia está mal, dado que exponen seis criterios de probabilidades en la definición y cinco en el impacto es decir de 0 a 4. Eso cambia los valores y las escalas y obviamente los rangos de aceptación de los riesgos.
- Valdría la pena que se construyeran los universos de riesgos, dado un enfoque tan específico los escenarios de riesgos son casi los mismos para todas las universidades. En ese orden la guía del apéndice de ISO 27005, sería ideal.
- Cómo se mide la efectividad de un control, basado en qué criterio, es muy importante que esto este definido de lo contrario, la subjetividad al hacer el ejercicio puede dar resultados no esperados. Así mismo que puede hacer que se definan mal las prioridades de atención de los riesgos.
- Como se calcula la probabilidad final y el impacto final, basado en que la efectividad del control, pero si eso no se cuantifica como afecta a la probabilidad e impacto inicial.
- La misma historia de la selección de los planes de mitigación de riesgos, basados en que escogen priorizar, es necesario que existan criterios más claros, dado que si lo dejan a discrecionalidad se van a enfrentar a la opinión y juicios de valor de las personas y sus intereses y eso puede desviar la atención del ejercicio.

Teniendo en cuenta estas cinco recomendaciones, se modificaron algunas tareas para acomodar el proceso de gestión de riesgos de T.I. acorde a las recomendaciones de la evaluación de juicio de expertos:

- Se modificaron las tareas de definición de criterios de probabilidad e impacto del riesgo (T1.4.2 y T1.4.3) dando como resultados cuatro niveles de probabilidad e impacto. De igual manera, se adecuó la matriz de calificación de riesgos establecida en la tarea T1.4.4 para reflejar una coherencia en criterios de aceptación de riesgos.

- Se modificaron las plantillas de identificación de servicios (GRTI-00 - Listado de servicios de T.I.) y universo de riesgos (GRTI-01 - Universo de riesgos de T.I.) con una base de información común para las universidades, apoyada en el anexo C de la norma ISO 27005 y en el libro II de Magerit.
- Se modificó la redacción de las tareas T4.1.2 y T4.1.3, dejando claro los criterios sugeridos para medir la efectividad de los controles existentes para la evaluación de riesgos.

6. CONCLUSIONES Y TRABAJO FUTURO

Como conclusiones del presente trabajo se tiene:

- Los riesgos de T.I. siempre van a existir, sean detectados o no por un proceso de gestión adecuado. Dado que no es posible eliminar los riesgos, se debe buscar la mejor manera de gestionarlos, para que haya un balance entre el costo de tratarlos y el posible impacto que puedan tener en el negocio.
- Para los directores de T.I. es claro que la importancia de los riesgos está determinada por el impacto en la continuidad de la operación de la Universidad y por la probabilidad de ocurrencia de la amenaza sobre los activos de información más relevantes que considere la alta dirección.
- Las universidades son conscientes de los riesgos de T.I., enfocándose especialmente en aquellos que afectan la seguridad de la información y el entorno natural que las rodea.
- Aunque las universidades entrevistadas no reflejaron tener implementado actualmente un proceso de gestión de riesgos de T.I, sí están interesadas en su implementación. Las mismas directivas apoyarían la implementación de un proceso de gestión de riesgos dentro de la institución, lo cual da cabida a acoger con mayor facilidad un proceso como el propuesto por este trabajo.
- Aunque los marcos de trabajo, normas y metodologías relacionadas con la gestión de riesgos de T.I. presentan una composición y contenido diferentes, giran en torno a un conjunto de buenas prácticas, las cuales fueron usadas como base para elaborar la guía de implementación.
- Todos los marcos de gestión de riesgos de T.I. hacen énfasis en la necesidad de contar con el apoyo de la gerencia desde el inicio del proceso y que se mantenga a lo largo del mismo.
- Un proceso sin una persona que lo administre, puede tener como consecuencia que el primero no sea óptimo en su ejecución, no sea consistente y, aún peor, no cumpla con su objetivo. La guía propuesta satisface esta premisa definiendo el rol de líder del proceso.
- En un proceso de gestión de riesgos de tecnología es necesario tener una visión global del negocio, lo cual requiere tener en cuenta las diversas perspectivas presentes en la institución. En la guía se sugiere la creación de GARTI, un grupo interdisciplinar de personas que contribuirán a la ejecución del proceso.
- Al realizar una comunicación efectiva entre las personas involucradas en el proceso, se logra una sensibilización que permite un entendimiento común de la importancia de la gestión de riesgos de T.I. en la institución.

6.1 TRABAJO FUTURO

Como futuros trabajos que se pueden desarrollar con base en este proyecto se tiene lo siguiente:

- Definir un modelo de madurez y unos indicadores para cada proceso de la guía, los cuales permita determinar las etapas de madurez en la implementación y facilite la comparación entre las universidades que adopten el proceso.
- Diseñar los mecanismos que permitan la alineación de un proceso de gestión de riesgos institucional con el proceso de gestión de riesgos de T.I. propuesto.
- Diseñar los mecanismos que permitan la alineación del proceso de gestión de proyectos de tecnología institucional con el proceso de gestión de riesgos de T.I. propuesto.
- Refinar el proceso de definir el conjunto de riesgos, de tal manera que se consideren también los riesgos “positivos” u oportunidades.
- Sistematizar el proceso de gestión de riesgos para las instituciones educativas, bien sea usando un software a la medida o adaptando alguno existente en el mercado, según convenga el caso.

7. BIBLIOGRAFÍA

COLOMBIA, DEPARTAMENTO NACIONAL DE PLANEACIÓN. III. Crecimiento sostenible y competitividad [En línea]. <http://www.dnp.gov.co/LinkClick.aspx?fileticket=6yjofaugVUQ%3D&tabid=1238> [citado en 1 de abril de 2012]

COLOMBIA, MINISTERIO DE EDUCACIÓN. Cinco acciones que están transformando la educación en Colombia. [En línea]. <http://www.mineducacion.gov.co/1621/propertyvalue-40524.html> [citado en 1 de abril de 2012]

DEFINICION.ORG. Artículo “IT” [en línea] <http://www.definicion.org/it> [citado en 30 de octubre de 2012]

EDUCAUSE. Artículo de contenido “About EDUCAUSE” [En línea]. <http://www.educause.edu/about> [citado en 4 de noviembre de 2012]

EDUCAUSE. Risk Management Framework [En línea]. <https://wiki.internet2.edu/confluence/display/itsg2/Risk+Management+Framework > [Citado en 5 de noviembre de 2012]

ESPAÑA, PORTAL DE ADMINISTRACIÓN ELECTRÓNICA. MAGERIT versión 2 [en línea]. <http://administracionelectronica.gob.es/?_nfpb=true&_pageLabel=PAE_PG_CTT_General&langPae=es&iniciativa=184> [citado en 1 de abril de 2012]

FERNANDEZ MARTÍNEZ, Antonio y LLORENS LARGO, Faraón. Gobierno de TI para universidades. Madrid, España: Conferencia de Rectores de las Universidades (CRUE), s.f. 215 p. ISBN: 978-84-935509-8-1.

FIGUEROA MEDINA, Luis Carlos. Guía de buenas prácticas en gestión de riesgos de TI en el sector bancario colombiano. Documento de tesis en la Maestría de Ingeniería de Sistemas y Computación. Bogotá: Universidad de los Andes, 2010. 140 p.

GÓMEZ, Ricardo; PÉREZ, Diego Hernán; DONOSO, Yesid; et. al. Metodología y gobierno de la gestión de riesgos de tecnologías de la información. En: Revista de Ingeniería. No. 31 (Ene.-Jun. 2010). Bogotá: Universidad de los Andes, 2010. 148 p. Semestral. ISSN 0121-4993.

INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. Norma Técnica Colombiana NTC 5254. Gestión del Riesgo. Bogotá, Colombia: ICONTEC, 2006. 22 p. (NTC 5254)

INTERNATIONAL ORGANIZATION FOR STANDARIZATION. About ISO – ISO [En línea]. <http://www.iso.org/iso/home/about.htm> [Citado en 4 de noviembre de 2012].

INTERNATIONAL ORGANIZATION FOR STANDARIZATION. Information technology – Security techniques – Information security management systems – Requirements. Suiza: ISO, 2009. 41 p. (ISO 27001:2005)

INTERNATIONAL ORGANIZATION FOR STANDARIZATION. Information technology – Security techniques – Information security risk management ISO/IEC 27005. Suiza: ISO, 2008. 55 p. (ISO 27005:2008)

INTERNATIONAL ORGANIZATION FOR STANDARIZATION. Risk management — Principles and guidelines. ISO 31000:2009. Suiza: ISO, 2009. 24 p. (ISO 31000:2009)

INTERNATIONAL ORGANIZATION FOR STANDARIZATION. Safety aspects - Guidelines for their inclusion in standards. ISO/IEC Guide 51. Suiza: ISO, 1999. 9 p. (ISO/IEC Guide 51:1999)

ISACA. CobiT®. Versión 4.1. Rolling Meadows, Illinois, Estados Unidos de América: ISACA, 2007. 196 p. ISBN 1-933284-72-2.

ISACA. The Risk IT Framework. Rolling Meadows, Illinois, Estados Unidos de América: ISACA, 2009. 106 p. ISBN 978-1-60420-111-6.

ISACA. The Risk IT Practitioner Guide. Rolling Meadows, Illinois, Estados Unidos de América: ISACA, 2009. 136 p. ISBN 978-1-60420-116-1.

MATH DIRECTORY. Artículo “iteración” [en línea] <http://www.mathematicsdictionary.com/spanish/vmd/full/i/iteration.htm> [citado en 30 de octubre de 2012]

PROJECT MANAGEMENT INSTITUTE. A Guide to the Project Management Body of Knowledge (PMBOK® Guide). 4 ed. Newton Square, Pasadena, Estados Unidos de América: Project Management Institute, 2008. 467 p. ISBN 978-1-933890-51-7

THE ECONOMIST. Digital risk: The challenge for the CRO. s.l.: The Economist, 2005. 23 p.

WATERS, Ian. Managing IT Risk University-Wide [documento electrónico] <http://www.caudit.edu.au/educauseaustralasia07/authors_papers/Waters-212.pdf > p. 3. [citado en 30 de octubre de 2012]

WIKIPEDIA. Artículo “Business process improvement”, sección “Process Owner” [en línea] <http://en.wikipedia.org/wiki/Business_process_improvement> [citado en 30 de octubre de 2012]

8. ANEXOS

ANEXO 1. ENCUESTA PARA OBTENER EL ESTADO DEL ARTE

En éste anexo se describe el método usado para recolectar la información que fue utilizada para levantar el estado del arte en el sector, cuyos resultados se pueden observar en el capítulo 2 de este documento. Se muestra a continuación el correo que se envió a los directores de T.I. de las universidades de la RUAV, y al finalizar del anexo se detallan las preguntas que se utilizaron dentro del cuestionario (elaborado en la herramienta de Google Docs para formularios) para el levantamiento de información en las instituciones participantes.

Correo enviado a los directores de TI para el levantamiento del estado del arte.

Apreciado director de TI, buenas tardes.

Somos Sergio Gómez y Andrés Mauricio Posada, estudiantes de la maestría de gestión de tecnologías de la información y telecomunicaciones de la Universidad Icesi.

Actualmente nos encontramos adelantando un trabajo de grado consistente en una guía de implementación de mejores prácticas de gestión de riesgos de TI en las universidades. Como parte del desarrollo del trabajo, requerimos realizar un estudio para conocer las necesidades y experiencias en torno al tema de gestión de riesgos de tecnología en el sector de la educación privada. Para esto requerimos de su valiosa ayuda, diligenciando una encuesta en línea que nos permitirá cumplir con el objetivo. La encuesta y las instrucciones podrá encontrarlas en la siguiente dirección:

(Se insertó la URL de la encuesta)

Agradecemos de antemano poder contar con su interés y participación en este proceso y ser parte de los resultados obtenidos en la investigación, los cuales compartiremos al final de la misma.

Cualquier inquietud, comentario o duda no dude en hacérnosla llegar.

Muchas gracias por su atención y colaboración,

Presentación de la encuesta

Estimado director del área de tecnología:

En la actualidad se está desarrollando un trabajo de grado de la maestría de gerencia de informática y telecomunicaciones de la Universidad Icesi, titulado "Propuesta de guía de implementación de mejores prácticas en gestión de riesgos de tecnologías de información en entidades privadas de educación superior". Esta encuesta servirá para determinar el estado del arte y las necesidades de las universidades frente a la gestión de riesgos de tecnologías de información.

La encuesta está compuesta por alrededor de 30 preguntas y responderla le tomará aproximadamente 30 minutos.

Agradecemos de antemano su participación en esta investigación. De la veracidad de sus respuestas y de su valioso aporte depende, en gran medida, el éxito de nuestra investigación.

Si tiene alguna duda o sugerencia frente al tema, no dude en contactarnos.

Cuestionario de preguntas

- ¿Cuál es el nombre de la universidad que participa en la encuesta? (Texto)
- ¿Cuál es su nombre? (Texto)
- ¿Cuáles considera Usted que son los riesgos relacionados con las tecnologías de información más relevantes para su organización? (Texto)
- ¿Conoce Usted algún marco de trabajo o norma relacionada con la gestión de riesgos de tecnologías de información? (S/N)
- ¿Qué marcos de trabajo o normas relacionadas con la gestión de riesgos de tecnologías de información conoce? (Texto)
- ¿Considera viable implementar uno de esos marcos de trabajo o normas de gestión de riesgos de tecnología en una universidad? (S/N)
- ¿Por qué considera que es o no viable la implementación de un marco de trabajo o norma de gestión de riesgos en una universidad? (Texto)
- ¿Considera necesario un proceso de gestión de riesgos de tecnologías de información en una universidad? (S/N)
- ¿Por qué considera necesario o no un proceso de gestión de riesgos de tecnologías de información en una universidad? (Texto)
- ¿Considera Usted que los problemas con los proyectos de tecnologías de información de su organización pueden ser mitigados con una adecuada gestión de riesgos de T.I.? (S/N)
- ¿Considera importante contar con el apoyo del comité directivo para un proceso adecuado de gestión de riesgos de tecnologías de información? (S/N)

- En su caso particular, ¿Cuenta o contaría con el apoyo del comité directivo en la implementación de una gestión de riesgos de tecnologías de información? (S/N)
- ¿Existe un proceso de gestión de riesgos corporativos implementado en su organización? (S/N)
- ¿Existe un proceso de gestión de riesgos de tecnologías de información implementado en su organización? (S/N)

En caso que tuviese un proceso de gestión de riesgos de T.I. implementado:

- ¿El proceso de gestión de riesgos de T.I. implementado en su organización sigue alguna norma o marco de trabajo reconocido a nivel nacional o mundial? (S/N)

  En caso de ser afirmativa la pregunta anterior,
  - ¿Cuál es el nombre de la norma o el marco de trabajo que fue implementado? (Texto)
- ¿Cada cuánto se actualiza o revisa el proceso de gestión de riesgos de tecnologías de información en su organización? (Número, en meses)
- ¿Qué estrategias o actividades establece el proceso para realizar la definición de los riesgos de tecnologías de información? (Texto)
- ¿El proceso de gestión de riesgos cómo realiza la evaluación y priorización de los riesgos de tecnologías de información? (Texto)
- ¿Qué estrategia define el proceso para tratar los riesgos de tecnologías de información identificados y evaluados? (Texto)
- ¿Qué hace el proceso referente a la ejecución de planes de acción de riesgos de tecnologías de información? (Texto)
- ¿El proceso de gestión de riesgos de tecnologías de información tiene un proceso de seguimiento para evaluar la efectividad de la aplicación de los planes de acción? (Texto)
- ¿El proceso de gestión de riesgos de tecnologías de información incluye un componente de mejoramiento continuo? (Texto)
- ¿El proceso de gestión de riesgos de tecnologías de información incluye un modelo de madurez? (Texto)
- ¿El proceso de gestión de riesgos tiene en cuenta los objetivos organizacionales? (Texto)
- ¿Qué importancia tiene el proceso de gestión de riesgos de tecnologías de información frente a los demás procesos del área de T.I.? (Texto)
- ¿Quiénes están involucrados en el levantamiento de la información de los riesgos? (Texto)
- ¿Cuántas personas conforman el equipo de trabajo que hace frente a la gestión del riesgo de tecnologías de información? (Texto)
- ¿Existen roles o responsabilidades definidas dentro del proceso de gestión de riesgos? (Texto)

- ¿Tiene influencia el proceso de gestión de riesgos de tecnologías de información dentro de la cultura organizacional? (Texto)
- ¿Qué alcance tiene el proceso de gestión de riesgos de tecnologías de información dentro de las políticas o directrices organizacionales? (Texto)
- ¿El proceso de gestión de riesgos de tecnologías de información considera los “riesgos positivos”? (Texto)
- ¿El proceso de gestión de riesgos está integrado a otros procesos de gestión de riesgos de la organización? (Texto)
- ¿El proceso de gestión de riesgos de tecnología es usado y aplicado en la operación del departamento de T.I.? (Texto)
- ¿Qué falencias considera que tiene el proceso de gestión de riesgos implementado en su organización? (Texto)

En caso que no tuviese un proceso de gestión de riesgos de T.I. implementado:

- ¿Por qué no es implementado el proceso de gestión de riesgos de T.I. en la operación del departamento? (Texto)
- ¿Por qué razón considera que no se implementa un proceso de riesgos de tecnologías de información en su organización? (Texto)
- ¿Quiénes deberían tomar las decisiones relacionadas con el proceso de riesgos de tecnologías de información? (Texto)
- ¿Cuáles serían los criterios para establecer los riesgos más relevantes para la organización? (Texto)
- ¿Considera importante el concepto de "riesgo positivo", es decir, aquellos que puedan generar una oportunidad a explorar? (S/N)
- ¿Considera que un proceso de gestión de riesgos tecnologías de información debe estar alineado a los objetivos organizacionales? (S/N)
- ¿Considera que un proceso de gestión de riesgos de tecnologías de información debe involucrar a toda la organización o debe ser sólo un esfuerzo del área de T.I.?(Texto)
- ¿Considera que una gestión de riesgos de tecnologías de información debe estar integrada a otros procesos de gestión de riesgos de la organización? (S/N)
- ¿Considera que el proceso de gestión de riesgos de tecnologías de información debe tener un proceso de seguimiento para evaluar la efectividad de la aplicación de los planes de acción? (S/N)
- ¿Considera que el proceso de gestión de riesgos de tecnologías de información debería contar con un proceso de mejoramiento continuo? (S/N)
- ¿Considera que el proceso de gestión de riesgos de tecnologías de información debería contar con un modelo de madurez para evaluar el proceso frente a las demás instituciones? (S/N)
- ¿Considera que el proceso de gestión de riesgos de tecnologías de información debe estar integrado a otros procesos de gestión de riesgos de la organización? (S/N)

ANEXO 2. ENCUESTA PARA OBTENER EL JUICIO DE EXPERTOS

Correo electrónico enviado a los expertos

Estimado/a (nombre del experto), cordial saludo.

Nos es grato dirigirnos a Usted para saludarle y a la vez requerir de su valiosa colaboración como experto, con la finalidad de solicitar la validez y confiabilidad del instrumento "Propuesta de guía de implementación de mejores prácticas en gestión de riesgos de tecnologías de información en entidades privadas de educación superior", el cual es un trabajo de grado de la maestría de gerencia de informática y telecomunicaciones de la Universidad Icesi.

Basándonos un marco común de mejores prácticas ofrecidas por los marcos de trabajo y normas de referencia de mayor uso a nivel mundial y nacional, hemos realizado una propuesta de guía de implementación de mejores prácticas en gestión de riesgos de tecnologías de información orientada a las universidades privadas de la ciudad de Cali. La propuesta consta de dos componentes:
- La guía como tal, la cual podrá encontrar en la siguiente dirección: (Se incluyó una URL donde aparecía la propuesta de guía plasmada en el capítulo 3)
- Las plantillas de apoyo, las cuales puede encontrar en la siguiente dirección: (Se incluyó una URL donde aparecían las plantillas de apoyo correspondientes a los anexos 2-7 de este documento)

Con base en la información antes presentada, hemos elaborado un breve cuestionario que nos permitirá obtener la retroalimentación de usted como experto, el cual podrá encontrar en la siguiente dirección: (Se incluyó una URL donde aparecía la encuesta que se mostrará a continuación).

Le damos las gracias de antemano por su atención prestada y por su valiosa colaboración.

Encuesta enviada a los expertos

Estimado experto, cordial saludo.

En la actualidad se está desarrollando un trabajo de grado de la maestría de gerencia de informática y telecomunicaciones de la Universidad Icesi, titulado "Propuesta de guía de implementación de mejores prácticas en gestión de riesgos de tecnologías de información en entidades de educación superior".
La propuesta la puede encontrar en el siguiente enlace: (Se incluyó una URL donde aparecía la propuesta de guía plasmada en el capítulo 3)

Las plantillas de apoyo las puede encontrar en el siguiente enlace: (Se incluyó una URL donde aparecían las plantillas de apoyo correspondientes a los anexos 2-7 de este documento)

Esta encuesta servirá para validar la pertinencia del proceso propuesto por la guía de acuerdo a los lineamientos y estándares en el tema, regidos por normas como la familia de ISO 27000. A continuación, le presentamos una serie de preguntas referidas a un conjunto de procesos relacionados con la gestión de riesgos de tecnología, los cuales son similares a lo largo de los marcos y normas más representativas del área. La encuesta está compuesta por 50 preguntas y responderla le tomará aproximadamente 30 minutos.

Las preguntas con calificación numérica tienen la siguiente escala de evaluación:

1 - Muy en desacuerdo
2 - En desacuerdo
3 - Ligeramente de acuerdo
4 - De acuerdo
5 - Muy de acuerdo

Agradecemos de antemano su participación en esta investigación. De la veracidad de sus respuestas y de su valioso aporte depende el éxito de nuestro proyecto.

- **Establecimiento de contexto**

¿La guía propuesta...
... establece una visión/contexto de los riesgos de T.I.?
Respuesta: [1 2 3 4 5]
... da pautas para definir los criterios de evaluación de los riesgos de T.I.?
Respuesta: [1 2 3 4 5]
... alinea el proceso de gestión de riesgos de T.I. con los objetivos de la empresa?
Respuesta: [1 2 3 4 5]

¿Considera usted que el proceso de establecimiento de contexto tal y como se formuló en la guía…
... es relevante? [S/N]
... es coherente? [S/N]
... es claro? [S/N]

¿Tiene algún comentario con respecto al proceso de establecimiento de contexto?

- **Identificación de riesgos**

¿La guía propuesta...

... define un universo de los riesgos de T.I. existentes en la organización?
Respuesta: [1 2 3 4 5]
... realiza una priorización de los riesgos de T.I.?
Respuesta: [1 2 3 4 5]
... identifica los riesgos de TI mayor probabilidad de ocurrencia?
Respuesta: [1 2 3 4 5]
... identifica las consecuencias de los riesgos de TI ?
Respuesta: [1 2 3 4 5]

¿Considera usted que el proceso de identificación de riesgos tal y como se formuló en la guía…
... es relevante? [S/N]
... es coherente? [S/N]
... es claro? [S/N]

¿Tiene algún comentario con el proceso de identificación de riesgos?

- **Análisis de riesgos**

¿La guía propuesta...
... da pautas para la evaluación de controles existentes?
Respuesta: [1 2 3 4 5]
... define el método de evaluación de los riesgos de T.I.?
Respuesta: [1 2 3 4 5]
... da pautas para la estimación del nivel de riesgo de los riesgos de T.I.?
Respuesta: [1 2 3 4 5]

¿Considera usted que el proceso de análisis de riesgos tal y como se formuló en la guía…
... es relevante? [S/N]
... es coherente? [S/N]
... es claro? [S/N]

¿Tiene algún comentario con respecto a este proceso?

- **Evaluación de riesgos**

¿La guía propuesta...
... evalúa los riesgos de T.I. según su impacto y probabilidad?
Respuesta: [1 2 3 4 5]
… da pautas para la interpretación del resultado de la evaluación de los riesgos de T.I.?
Respuesta: [1 2 3 4 5]

¿Considera usted que el proceso de evaluación de riesgos tal y como se formuló en la guía…
... es relevante? [S/N]
... es coherente? [S/N]
... es claro? [S/N]

¿Tiene algún comentario con respecto al proceso de evaluación de riesgos?

- **Tratamiento del riesgo**

¿La guía propuesta...
... define las estrategias para tratamiento de los riesgos de T.I.?
Respuesta: [1 2 3 4 5]
... prepara e implementa los planes de acción de riesgos de T.I.?
Respuesta: [1 2 3 4 5]

¿Considera usted que el proceso de tratamiento de riesgos tal y como se formuló en la guía…
... es relevante? [S/N]
... es coherente? [S/N]
... es claro? [S/N]

¿Tiene algún comentario con respecto al proceso de tratamiento de riesgos?

- **Monitoreo y revisión**

¿La guía propuesta...
... evalúa constantemente el proceso completo de la gestión de riesgos de T.I. dependiendo de los cambios externos e internos relevantes para la organización?
Respuesta: [1 2 3 4 5]
... evalúa el cambio sobre los factores de riesgos de T.I. sobre los cuales se definen los mismos?
Respuesta: [1 2 3 4 5]

¿Considera usted que el proceso de monitoreo y revisión tal y como se formuló en la guía…
... es relevante? [S/N]
... es coherente? [S/N]
... es claro? [S/N]

¿Tiene algún comentario con respecto al proceso de monitoreo y revisión?

- **Comunicación y consulta**

¿La guía propuesta...

... define un plan de comunicaciones involucrando todos los interesados del proceso de gestión de riesgos de T.I.?
Respuesta: [1 2 3 4 5]
... define un nivel de comunicación claro y relevante a la naturaleza de los diferentes niveles jerárquicos de los interesados?
Respuesta: [1 2 3 4 5]

¿Considera usted que el proceso de comunicación y consulta tal y como se formuló en la guía…
... es relevante? [S/N]
... es coherente? [S/N]
... es claro? [S/N]

¿Tiene algún comentario con respecto al proceso de comunicación y consulta?

- **Propuesta de guía de implementación vista como un todo**

Realizando una evaluación de la guía como un todo, ¿considera usted que la guía propuesta...
... es relevante? [S/N]
... es coherente? [S/N]
... es clara? [S/N]

Finalmente, ¿tiene algún comentario con respecto al documento en general?
El producto final de la evaluación de expertos se muestra en el capítulo 5: resultados obtenidos.

ANEXO 3. HOJA DE VIDA DE JUICIO DE EXPERTO

Hoja de vida de Andrés Ricardo Almanza Junco, MSc., tomada de la página de ACIS: http://www.acis.org.co/index.php?id=1776

Ingeniero de Sistemas – Universidad Católica de Colombia.
Especialista en Seguridad de Redes – Universidad Católica de Colombia.
Máster en Seguridad Informática – Universidad Oberta de Cataluña, España.
Certificación LPIC1 - Linux Professional Institute.
Certificado ITIL v3.
Auditor Interno ISO/IEC 27001:2005.
Docente Universitario de programas de Postgrado en Seguridad de la Información.
Coordinador de Seguridad de la Información de la Cámara de Comercio de Bogotá.

ANEXO 4. PLANTILLA GRTI-00: LISTADO DE SERVICIOS DE T.I.

Universidad XYZ

GRTI-00 - Listado de servicios de T.I.

Fecha de revisión:

Servicio	Responsable	¿Crítico?	Prioridad
Asesoría en T.I.			
Soporte técnico			
Digitalización de documentos			
Matrícula académica en línea			
Pago matrícula financiera en línea			
Impresión			
Salas de cómputo			
Educación virtual (e-learning)			
Desarrollo de software			
Compra de recursos de T.I.			
Consulta de contenidos de materias			

Lecciones aprendidas:

(continúa en la siguiente página)

ANEXO 5. PLANTILLA GRTI-01: UNIVERSO DE RIESGOS DE T.I.

Universidad XYZ

GRTI-01 - Universo de riesgos de T.I.

Fecha de revisión: XX-XX-XXXX

ID	Descripción del riesgo	Servicio afectado principal	Prioridad servicio

Lecciones aprendidas:

ANEXO 6. PLANTILLA GRTI-02: ANÁLISIS DE RIESGOS DE T.I.

Universidad XYZ

GRTI-02 - Análisis de riesgos de T.I.

ID	Descripción del riesgo	Causas del riesgo	Consecuencias del riesgo	Probabilidad inicial	Impacto inicial	Evaluación inicial	Lista de controles existentes	Probabilidad final	Impacto final	Evaluación final
1										
2										
3										
4										

Lecciones aprendidas:

ANEXO 7. PLANTILLA GRTI-03: RESPUESTA A LOS RIESGOS DE T.I.

Universidad XYZ

GRTI-03 - Respuesta a los riesgos de T.I.

ID	Descripción del riesgo	Opciones de manejo sugeridas	Opción de manejo escogida	Acción ante el riesgo	Responsable	Prioridad	Fecha programada
1							
2							
3							
4							

Lecciones aprendidas:

Opciones de manejo de riesgos: Aceptar, mitigar, transferir o evitar.

ANEXO 8. PLANTILLA GRTI-04: SEGUIMIENTO AL PLAN

Universidad XYZ

GRTI-04 - Seguimiento al plan

ID	Descripción del riesgo	Acción ante el riesgo	Prioridad	Responsable	Fecha	Avance fecha 1	Avance fecha 2	Avance fecha 3
1								
2								
3								
4								

Lecciones aprendidas:

ANEXO 9. PLANTILLA GRTI-05. MEJORAMIENTO CONTINUO

Universidad XYZ

GRTI-05 - Mejoramiento continuo

Fecha revisión: DD-MM-YYYY

Proceso	Actividad	Tarea	Lección aprendida	Fecha

Cambios propuestos:

Cambio	Justificación	¿Aprobado?