Instituto Tecnológico de Costa Rica
Área Académica de Administración de Tecnologías de Información

Metodología para la gestión de riesgos de TI basada en COBIT 5

Trabajo Final de Graduación para optar por el grado académico de Licenciatura en Administración de Tecnología de Información

Elaborado por:

Jean Carlo Alfaro Campos

Profesor tutor:

Ing. Laura Alpízar Chaves, M.Sc.

Cartago, Costa Rica

Junio de 2017

TEC | Tecnológico de Costa Rica

ÁREA DE ADMINISTRACIÓN DE TECNOLOGÍAS DE INFORMACIÓN
GRADO ACADÉMICO: LICENCIATURA

Los miembros del Tribunal Examinador del Área de Administración de Tecnologías de Información, recomendamos que el presente Informe Final del Proyecto de Graduación del estudiante *Jean Carlo Alfaro Campos*, sea aceptado como requisito parcial para obtener el grado académico de *Licenciatura en Administración de Tecnología de Información*.

_____

Ing. Laura Alpízar Chaves, M.Sc.
Profesora tutora

_____

Ing. Luis Chavarría Sánchez, M.Ed.
Miembro del Tribunal Examinador

_____

Lic. Pedro Leiva Chinchilla
Miembro del Tribunal Examinador

_____

Ing. Sonia Mora González, MBA
Coordinadora Trabajo Final de Graduación

Junio de 2017

Dedicatoria

Dedico este trabajo a Flora Jiménez, sin quien no habría podido completar mis estudios universitarios. Su ejemplo y su apoyo constante, hicieron de mí una mejor persona y me prepararon para la vida profesional.

También quiero dedicarlo a mi hermana, Glenda quien recién inicia la vida universitaria. Que este logro sirva como motivación y muestra de mi apoyo incondicional en el proceso que le espera.

Agradecimientos

Ante todo, agradezco a Dios, creador y dador de vida por amarme infinitamente a pesar de mis incontables defectos y mi testarudez.

A mis padres, por regalarme mis principios y velar siempre por mi educación.

A Lilliana y sus cuatro hijos, mis hermanos, por recibirme como un miembro de su familia durante mi estadía en la universidad.

A Laura mi profesora tutora por sus consejos, su apoyo y su innegable esfuerzo en el desarrollo de este trabajo.

A la firma Deloitte, especialmente a Andrés, Karol y Pablo por la oportunidad de realizar este trabajo y su apoyo.

A Larissa, Melvin, Rocío, Ronald, Yarima y mis profesores, por enseñarme más que computación o literatura, por convertirme en lo que soy hoy.

A Aarón, Gloriana, Mercedes y Yesenia por apoyarme y creer en mí hasta el final.

Resumen

La firma consultora Deloitte, mediante su departamento de *Risk Advisory*, ofrece servicios a sus clientes, relacionados con la gestión de riesgos de tecnología de información. Al igual que en los demás servicios desarrollados por Deloitte, con el desarrollo de proyectos sobre riesgos de tecnología de información, esta firma pretende generar un impacto en sus clientes y en la sociedad.

Sin embargo, la organización no cuenta con una metodología estandarizada sobre gestión de riesgos de tecnología de información. Esto ha generado algunos inconvenientes en los proyectos que la empresa desarrolla para sus clientes. Además de la creciente necesidad de estandarización, certificación y cumplimiento que presentan las empresas ya sea por cuestiones internas o por factores externos como leyes y regulaciones.

Este trabajo final de graduación, desarrollado por un consultor de Deloitte, en el marco de los esfuerzos de esta firma por aumentar la calidad de sus servicios, propone una metodología estandarizada para la gestión de riesgos de tecnología de información. Esta propuesta de metodología está basada en el marco COBIT 5 y en la norma ISO 31000. Además, considera las prácticas utilizadas actualmente por la firma consultora.

Luego del proceso investigativo desarrollado para este trabajo de graduación, se concluye que la empresa no ha utilizado al máximo los recursos de conocimiento disponibles y que las prácticas disponibles, aunque se ajustan a marcos de referencia conocidos, no son adecuadas para la realidad de la región y no siempre se utilizan de la mejor manera.

Se recomienda a la empresa, explotar el conocimiento disponible a lo interno, utilizar la propuesta de metodología en sus proyectos sobre riesgos de tecnología de información, referirse a las guías oficiales sobre mejores prácticas reconocidas y mantener su manera de trabajar actualizada y vigente.

Palabras clave: Tecnología de información, riesgo, gestión de riesgos de TI, COBIT 5.

Abstract

The consulting firm Deloitte through *Risk Advisory* offers services to its clients related to information technology risk management. Likewise other services developed by Deloitte, this firm aims to generate an impact on its customers and society with the development of projects on information technology risks.

However, the organization does not have a standardized methodology on information technology risk management generating some inconveniences in the projects that the company develops for its clients, which have an increasing need for standardization, certification and compliance for internal issues or external factors such as laws and regulations.

This thesis, developed by a Deloitte consultant, within the framework of this firm's efforts to increase the quality of its services, proposes a standardized methodology for information technology risk management based on the COBIT 5 framework and the ISO 31000 standard. Also, consider the practices currently used by the firm.

Within the investigation process, it was determined that the company has not used all the available knowledge resources to the maximum moreover the available practices, although they conform to known frames of reference, are not adequate for the reality of the region nor used in the best way.

A recommendation for the company is to exploit the knowledge available, to use the proposed methodology in its projects on information technology risks, to refer to the official guides on recognized best practices and to maintain its current and updated working practices.

Keywords: Information Technology, risk, IT risk management, COBIT 5.

Abreviaturas

A continuación, se presentan las abreviaturas utilizadas en este informe. Estos términos serán utilizados a lo largo de este documento y constituyen un componente esencial para la comprensión del mismo. Por ello, resulta de gran importancia para el lector conocerlos y consultarlos cuando sea necesario, facilitando así la comprensión del presente informe.

Término	Significado
ATI	Administración de Tecnología de Información. *Carrera impartida en el Instituto Tecnológico de Costa Rica*.
COBIT	Objetivos de Control para Información y Tecnologías Relacionadas.
COSO	*Committee of Sponsoring Organizations of the Treadway Commission.*
DTTL	*Deloitte Touche Tohmatsu Limited.*
INTECO	Instituto de Normas Técnicas de Costa Rica.
ISACA	*Information Systems Audit and Control Association.*
ISO	Organización Internacional de Normalización.
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.
OCTAVE	*Operationally Critical Threat, Asset, and Vulnerability Evaluation.*
SUGEF	Superintendencia General de Entidades Financieras de Costa Rica.
TI	Tecnología de Información.

Índice general

Índice de figuras

Índice de tablas

Introducción

1 Introducción

Este Trabajo Final de Graduación, propone una metodología para la gestión de riesgos de tecnología de información (TI) para la firma de servicios profesionales Deloitte, específicamente para la firma miembro de Centroamérica y República Dominicana. La metodología, se basa en lo sugerido por el marco de referencia COBIT 5, considerando a su vez las prácticas utilizadas por Deloitte y otros marcos de referencia como lo son la norma ISO 31000, ITIL y otros que resultan relevantes en el tema.

El presente informe, documenta el proceso investigativo que es llevado a cabo por el autor para generar la propuesta de metodología. Para ello, en este primer capítulo, se ofrece una descripción general del proyecto y de los antecedentes en la Firma Deloitte & Touche, S.A. (Deloitte), contemplando aspectos como su misión, visión y estructura organizativa. Posteriormente, se realiza el planteamiento del problema, se presentan los objetivos y el alcance del proyecto, así como los entregables tanto de producto como de gestión de proyecto. Se contemplan las restricciones y supuestos que son considerados en este trabajo, además de las limitaciones para la realización del mismo.

El segundo capítulo, presenta el marco teórico que sustenta el proceso de investigación y el desarrollo de la propuesta de metodología para la gestión de riesgos de tecnología de información. Por su parte, el tercer capítulo describe el marco metodológico que fundamenta y define, el proceso que se sigue para el desarrollo de este trabajo final de graduación.

Una vez llevado a cabo el proceso descrito en el marco metodológico, el cuarto capítulo, presenta el análisis de los resultados obtenidos. Allí se puede encontrar los resultados correspondientes con cada objetivo específico de este trabajo.

La información recopilada en el análisis de resultados es utilizada para construir la propuesta de solución. En este caso, una propuesta de metodología para la gestión de riesgos de TI. El quinto capítulo, describe la propuesta que se entrega a la organización y constituye el principal entregable producto de este trabajo final de graduación.

Finalmente, en los capítulos sexto y sétimo, se presentan las conclusiones y recomendaciones que se generan de esta investigación respectivamente. Las primeras, permiten resolver el problema de investigación en función de los objetivos establecidos y

con base en los resultados y la propuesta de solución que se generan. Mientras que las recomendaciones, son realizadas por el autor a la luz de todo el proceso investigativo, luego de presentar la propuesta de metodología a la organización y completar el trabajo de graduación.

En la sección siguiente, se ofrece una descripción general del trabajo realizado.

1.1 Descripción general

Deloitte ayuda a sus clientes a tomar decisiones inteligentes teniendo en consideración la prevención y el tratamiento de los riesgos de TI. Esto, se lleva a cabo en sintonía con las mejores prácticas y marcos de referencia que existen en la industria; además, de las normativas legales vigentes. Actualmente, esta firma está incluyendo como parte de sus servicios, la implementación de procesos de COBIT 5 relacionados con el riesgo de TI.

La ejecución de este trabajo, contempla las buenas prácticas que están vigentes actualmente y aplica conceptos y procedimientos probados e innovadores, que son utilizados por gran cantidad de organizaciones en todo el mundo y que le permitirán a Deloitte, brindar servicios de gestión de riesgos de TI, adecuados a las tendencias y necesidades de sus clientes.

La razón principal para el desarrollo de este trabajo es la necesidad de estandarizar las diferentes actividades que realiza Deloitte en sus servicios de gestión de riesgos de tecnología de información. Actualmente se lleva a cabo un proceso distinto para cada proyecto que realiza la Firma, lo que representa un desperdicio importante de horas e insumos de trabajo, espacio de oficina y, por consiguiente, una reducción del beneficio económico.

Este trabajo permite contar con una metodología definida que marca el camino a seguir para efectuar una adecuada gestión de riesgos de TI y sirve como apoyo en los servicios que brinda Deloitte. Esta metodología, además de COBIT, considera otras mejores prácticas como las normas ISO 31000 por ejemplo. Se utiliza como principal referencia, el marco COBIT 5 y lo que este presenta en relación con la gestión del riesgo de tecnología de información.

En seguida se presentan los antecedentes sobre Deloitte y sobre otros trabajos relacionados con este proyecto.

1.2 Antecedentes

Este apartado presenta una serie de aspectos importantes sobre el entorno en el que se lleva a cabo este trabajo final de graduación. Primeramente, se resume el quehacer de la organización y se resaltan algunos puntos clave como su misión, su visión y el equipo de trabajo con el que cuenta.

Además, se hace un resumen de los trabajos o proyectos, realizados en la firma, que sean similares a este o tengan relación alguna con el mismo. Esto, con el objetivo de fundamentar, y contextualizar esta investigación.

1.3 Descripción de la organización

Deloitte es la red de servicios profesionales privada más grande del mundo y presta servicios en auditoría, consultoría, asesoría financiera, gestión de riesgo, servicios fiscales y otros en más de 150 países y territorios; para lo cual, cuenta con aproximadamente 245,000 profesionales, de los cuales 45% son mujeres. Deloitte fue fundada en 1845 en Londres por William W. Deloitte, la primera persona en ser reconocida como un auditor externo.

> “Deloitte” es la marca bajo la cual decenas de miles de profesionales comprometidos en firmas independientes alrededor del mundo, colaboran para otorgar servicios de auditoría, consultoría, asesoría financiera, gestión de riesgo, servicios fiscales para sus clientes. No todas las firmas miembro de Deloitte brindan todos los servicios. Estas firmas son miembros de Deloitte Touche Tohmatsu Limited (DTTL), sociedad privada de limitada por garantía en el Reino Unido. Cada firma miembro brinda servicios en un área geográfica específica y está sujeta a las leyes y regulaciones profesionales del país o países específicos en los que opere (Deloitte & Touche, S.A., 2017).

En el sitio web de Deloitte, además del texto citado, se indica que todas las firmas que son miembro de DTTL, se estructuran de acuerdo con las leyes, reglamentos y normas de sus respectivos países o regiones. De esta forma, según se afirma en la página, se asegura la prestación de servicios profesionales en una zona específica mediante subsidiarias y filiales asociadas. Se hace la salvedad de que algunas de las firmas miembro, no ofrecen todos los servicios de Deloitte (Deloitte & Touche, S.A., 2017).

Según muestra el mismo sitio en Internet, DTTL y todas sus firmas miembro, son entidades independientes y únicas ante la Ley. Por ello, según se indica, cada firma es responsable por su actuar y sus omisiones, sin que esto comprometa a las demás entidades miembro. Así mismo, se aclara que Deloitte & Touche, S.A. es una afiliada de *Deloitte Latin American Countries Organization Regional Services Limited* (Deloitte LATCO). Y que Deloitte LATCO, a su vez es una firma miembro de DTTL (Deloitte & Touche, S.A., 2017).

Debido a la rápida evolución del mercado latinoamericano, se estableció Deloitte LATCO como organización regional que unifica las firmas de Argentina, Paraguay, Uruguay, Perú, Ecuador, Colombia, Venezuela, Panamá, Guatemala, Costa Rica, Honduras, El Salvador, República Dominicana y Nicaragua. Deloitte LATCO cuenta con alrededor de 6000 profesionales, los cuales trabajan de manera articulada, conformando equipos homogéneos para agregar mayor valor a su trabajo, garantizando el correcto balance de habilidades y conocimientos (Deloitte & Touche, S.A., 2017).

En Costa Rica, Deloitte & Touche, S.A. y sus afiliadas, cuentan con más de 450 profesionales. Esta firma es miembro de DTTL desde 1973 y fue fundada en 1964. Deloitte Costa Rica, lidera un clúster que conforma en conjunto con Honduras, Nicaragua y República Dominicana. Además, en el país se sitúa un Centro de Servicios Compartidos que soporta la gestión y las operaciones de Deloitte en Costa Rica, Guatemala, Honduras, El Salvador, Nicaragua y República Dominicana.

La filosofía de Deloitte Costa Rica es prestar servicios de la más alta calidad y ser reconocida en Costa Rica como la mejor firma en servicios de auditoría, consultoría gerencial, servicios gerenciales (*outsourcing*), asesoría tributaria y administración del riesgo empresarial e informático. En esta última línea es que se lleva a cabo este proyecto.

En seguida se muestran la misión, visión, valores y estructura de la organización.

1.3.1 Misión

La misión de Deloitte es la siguiente:

"Generar impactos que trascienden"

(Deloitte & Touche, S.A., 2017)

1.3.2 Visión

Por otra parte, la visión de la Firma consiste en:

"Ser el líder global indiscutido del sector de servicios profesionales"

(Deloitte & Touche, S.A., 2017)

1.3.3 Valores

Así mismo, los valores que guían el trabajo en Deloitte son los siguientes:

- Integridad.
- Aportamos valor a nuestros clientes y a los mercados.
- Compromiso mutuo.
- Fortaleza basada en la diversidad cultural.

(Deloitte & Touche, S.A., 2017)

1.3.4 Estructura organizacional

Como insumo para el proyecto, resulta importante conocer la estructura organizativa de la Firma. La Figura 1, muestra el organigrama resumido de la organización.

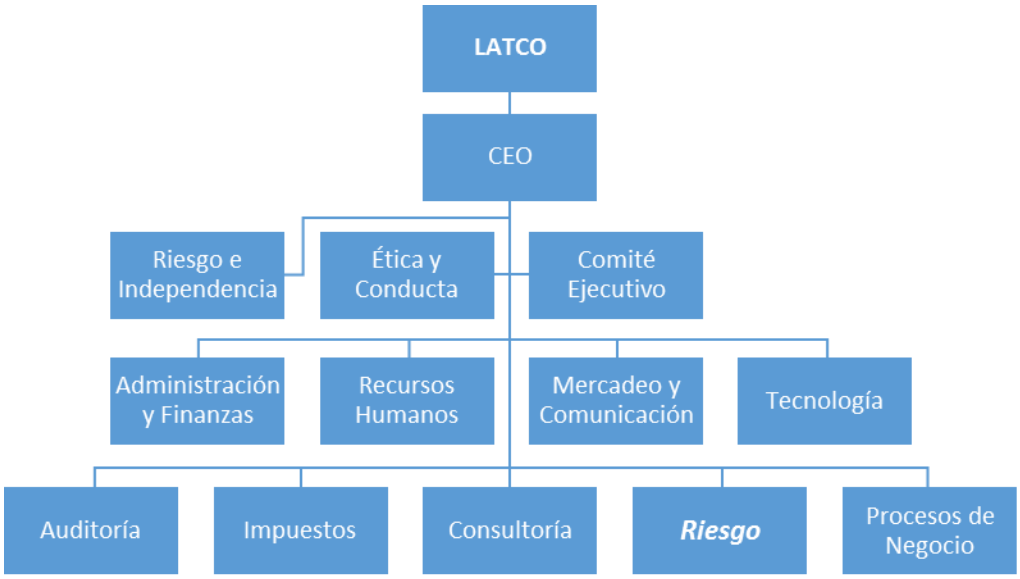


Figura 1. Organigrama de la Firma
Fuente: (Deloitte & Touche, S.A., 2017)

1.3.5 Servicios de riesgo

Específicamente en el área de *Risk Advisory* o Servicios de Riesgo, la cual se resalta en la Figura 1, se cuenta con 44 colaboradores en Costa Rica, 13 en República Dominicana y cinco entre Honduras y Nicaragua. De estos, 10 son Gerentes, tres son Socios, una es secretaria y los restantes son consultores.

Risk Advisory, como su nombre lo indica, brinda servicios en el área de riesgo. Para ello, ofrece cuatro líneas de servicio: Sistemas de Gestión, Auditoría Interna, Aseguramiento de Controles y Ciberseguridad. En todas estas áreas, hay un componente muy importante de Tecnología de Información, de hecho, una parte importante de los colaboradores son profesionales en ingeniería de sistemas o computación y actualmente, hay cuatro que son de Administración de Tecnología de Información (ATI). Otros seis egresados de ATI han trabajado en el departamento y también se cuenta con colaboradores de ingeniería industrial y administración de negocios.

A continuación, se resume lo que la organización ha venido haciendo, en relación con el tema de este trabajo final de graduación.

1.4 Trabajos similares dentro de la organización

En años anteriores, algunos consultores de Deloitte propusieron una metodología para gestionar los riesgos de TI como parte de un proyecto específico para un cliente. Desde entonces, ese trabajo se ha utilizado para guiar los servicios que la Firma ofrece a sus clientes y ha servido como referencia en procesos de gestión de riesgos que Deloitte facilita.

Ese trabajo, logra un alineamiento entre lo que el cliente venía haciendo y los principales aspectos sugeridos por el marco COBIT 4.0. Adicionalmente, considera el ciclo de gestión de riesgos que se propone en las normas ISO 31000. Dicha metodología, ofrece una descripción de las etapas a seguir para la gestión de riesgos de TI y muestra las consideraciones que se deben tener en cada una de ellas. Además, identifica los responsables de ejecutar las tareas para cada etapa.

Esta metodología tiene diversas oportunidades de mejora. Cuando se desarrolló, el cliente no tenía bien definidos ni el apetito ni la tolerancia de riesgos, por tanto, no se garantiza que los insumos son adecuados para continuar con el ciclo de gestión de riesgos. Así mismo, no se incluye ningún mecanismo para promover o garantizar el involucramiento de las instancias superiores de la organización.

El trabajo, también contempla el tema del riesgo inherente y riesgo residual. Esto, mediante la evaluación de efectividad de los controles aplicados para mitigar los riesgos y un nuevo análisis del riesgo que permanece después del tratamiento. Así mismo, contempla el proceso para la definición de una política de riesgos en la organización cliente.

Aunque este artefacto está documentado y disponible para que Deloitte lo utilice en distintos proyectos, no es estándar ni fue concebido pensando en adaptarlo para diferentes proyectos o servicios de la Firma. Esto, aunado con el hecho de que no se alinea con COBIT 5 ni satisface completamente las necesidades de Deloitte o de sus clientes, lo hace insuficiente ante las condiciones actuales.

Fuera del trabajo mencionado, no se ha realizado ninguna investigación, herramienta, metodología o similar, para la gestión de riesgos de tecnología de información en esta firma miembro de Deloitte.

A continuación, se plantea formalmente el problema que pretende solventar este proyecto.

1.5 Planteamiento del problema

Esta sección, presenta la situación actual en relación con proyectos o servicios de gestión de riesgos de TI en la organización. Esto, con el objetivo de identificar el problema que da paso a la realización de este trabajo final de graduación.

Como se indicó anteriormente, el área de *Risk Advisory* ofrece servicios de consultoría en diversos aspectos relacionados con la optimización del riesgo. Como parte de los servicios de Sistemas de Gestión, se realizan proyectos de implementación de COBIT, ITIL, normas ISO y otros estándares relacionados; además de planes de continuidad de TI y planes estratégicos de TI que también requieren la consideración del riesgo asociado. Así mismo, se realizan evaluaciones de cumplimiento de normativas nacionales como las de SUGEF y las Normas Técnicas de la Contraloría General de la República.

A pesar de lo anterior, la organización no cuenta con una metodología actualizada para la implementación de proyectos de riesgos de TI o bien, para utilizarla como parte de otros proyectos que deban contemplar el tema de riesgos de TI. Esto, da pie a que Deloitte experimente la situación problemática que se describe a continuación.

1.6 Situación problemática

Actualmente, muchas de las empresas clientes de Deloitte, o bien, aquellas a las que potencialmente se les podría brindar servicios, están comenzando a utilizar COBIT 5 como marco de gestión para su tecnología de información. Esto, ocasiona que los procesos que la Firma venía utilizando queden desactualizados y no se ajusten a la realidad actual. Las organizaciones buscan la implementación de los procesos y prácticas más actualizados con el objetivo de optar por una certificación, o bien porque deben cumplir con alguna normativa legal o empresarial. Deloitte, en concordancia con sus valores, debe permanecer a la vanguardia en los métodos utilizados para brindar sus servicios.

Existen versiones anteriores de COBIT como la 4.1, sin embargo, este trabajo final de graduación se basa específicamente en el marco COBIT 5. Lo anterior, se debe a los cambios sustantivos que fueron introducidos en la última versión del marco, el cual, pasó de ser una herramienta para auditar y controlar, a un marco con un enfoque integral para la gobernanza, administración y operación de las TI. Así mismo, por temas de certificación y cumplimiento, las organizaciones deben garantizar que se utilizan las prácticas de una versión específica de COBIT. En este caso, se requiere que dicha versión sea COBIT 5, como es el caso del Acuerdo SUGEF 14-17 que requiere la implementación de un marco de gestión y gobierno estructurado en 34 procesos de Tecnologías de Información.

Otro aspecto relevante en la situación problemática de la organización es que las tendencias actuales de gestión, están orientadas a la gestión basada en riesgos. Esto no es algo exclusivo para la industria de tecnología de información, si no que aplica también para la gestión operativa, la gestión financiera y otros procesos de negocio. No obstante, la tecnología de información constituye un componente de gran importancia cuando de riesgos se trata. Las TI pueden ser un gran aliado para la optimización y tratamiento de riesgos, pero al mismo tiempo, su uso conlleva diferentes riesgos que podrían afectar negativamente a las organizaciones.

Deloitte, actualmente no cuenta con una metodología estructurada que funcione de apoyo en la gestión de riesgos de TI y que, por tanto, pueda ser utilizada en los diferentes servicios relacionados que esta Firma ofrece. La ausencia de dicha metodología, ocasiona que el trabajo realizado por la organización para brindar servicios relacionados con la gestión del riesgo de TI, sea más costoso en términos de recursos como tiempo y personal. Al no existir un marco de trabajo estandarizado, en cada proyecto debe realizarse una investigación y

una adaptación de las prácticas y conocimientos identificados, a las necesidades de los diferentes clientes, considerando también el enfoque de cada proyecto.

En el apartado siguiente, se resumen los beneficios del presente trabajo final de graduación.

1.7 Beneficios esperados del proyecto

Este apartado, presenta los beneficios que se obtendrán como resultado de realizar este trabajo final de graduación. Los mismos, se listan a continuación.

- El establecimiento de una metodología estandarizada para la gestión de riesgos de TI, que está basada en COBIT 5, que se puede adecuar a clientes de distintas industrias a los que Deloitte presta sus servicios y que se adapta a la realidad y los requerimientos propios del entorno actual de las TI.
- La creación de una metodología integral y asertiva en cuanto a la gestión de riesgos de TI, que permite contemplar todos los riesgos relacionados con TI como son los de seguridad, los de continuidad y los de proveedores. Actualmente, no hay una metodología o herramienta de este tipo, que permita contemplar todos los tipos de riesgos asociados con la tecnología de información.
- La propuesta de metodología que ofrece este trabajo, permite generar conciencia, en las esferas más altas de las organizaciones, sobre la importancia de la gestión de riesgos de TI. De esta forma, podrá estructurarse un Sistema de Gestión de Riesgos de TI que sea integral y cuente con el apoyo de los directivos de la organización. La falta de involucramiento de los niveles gerenciales representa, según Deloitte, uno de los principales inconvenientes y contratiempos en la implementación de proyectos relacionados con el riesgo de TI.

1.8 Objetivos

Esta sección, declara los objetivos planteados para el desarrollo del trabajo final de graduación. Primeramente, se presenta el objetivo general y en seguida los objetivos específicos del proyecto.

1.8.1 Objetivo general

El objetivo general del trabajo, consiste en:

Proponer una Metodología de Gestión de Riesgos de Tecnología de Información para la firma costarricense Deloitte & Touche, S.A., que esté basada en COBIT 5 y se ajuste a otras mejores prácticas de la industria de tecnología de información, contemplando los aspectos estratégicos y de gestión de estos riesgos.

1.8.2 Objetivos específicos

Los objetivos específicos de este trabajo final son:

- Comprender las prácticas que Deloitte ha utilizado en el desarrollo de proyectos sobre gestión de riesgos de TI.
- Examinar las mejores prácticas relevantes en la industria de TI, sobre la gestión de riesgos.
- Construir una metodología para la gestión de riesgos de TI, que considere las prácticas de Deloitte y se alinee con las mejores prácticas existentes.

1.9 Alcance del proyecto

Esta sección, describe las actividades desarrolladas como parte de este trabajo final de graduación. Ofrece una visión general y completa que permite comprender con claridad de qué trata el proyecto. Además, ofrece información sobre sus actividades, el fundamento de las mismas y el orden lógico para efectuarlas y alcanzar así el resultado final del proyecto.

A través de esta sección, el lector podrá identificar las macro actividades del proyecto y cómo estas generan valor para la organización y contribuyen con la consecución de la Propuesta de Metodología, que constituye el resultado principal de este proyecto. Del mismo modo, podrá estar al tanto de los aspectos que se incluyen y aquellos que no se toman en cuenta como parte del proceso para generar la Propuesta de Metodología supra citada.

Para ello, se hace un repaso sobre qué es la Metodología y lo que se pretende alcanzar con la misma. Esta Metodología se divide en dos ámbitos principales guiados por dos procesos de COBIT, el primer ámbito está relacionado con la definición de los lineamientos organizacionales para la gestión del riesgo de TI y el segundo, se trata más bien del ciclo o procedimiento que se debe utilizar para llevar a cabo la gestión de dichos riesgos. Por ello, este alcance también describe en qué consisten tales ámbitos y cuáles son los aspectos que se desarrolla en cada uno de ellos. Finalmente, se incluye un apartado con aquellos aspectos que no se toman en cuenta durante el desarrollo del proyecto.

La Metodología que propone este trabajo final de graduación es un mecanismo que establece el proceso que va desde la comprensión de la realidad de una organización y definición de su estrategia de riesgos de TI, hasta la implementación del ciclo de gestión de riesgos con todas las actividades que este conlleva.

Es importante recalcar que este trabajo no busca definir la estrategia de gestión de riesgos de TI ni implementar el ciclo de gestión de riesgos de TI en una organización específica. La Metodología propuesta viene a ser, más bien, un apoyo y una guía para realizar tales actividades de la forma óptima según lo que indican las mejores prácticas conocidas en la industria de las Tecnologías de Información. En palabras más sencillas, no se trata de "hacerlo" si no de "cómo hacerlo", en referencia a la gestión de los riesgos de TI.

Debido a la naturaleza de la organización en la que se desarrolla el proyecto, el resultado final obtenido, permitirá brindar servicios de gestión de riesgos de TI de una manera estructurada y adaptados a la realidad de las diferentes organizaciones a las que Deloitte brinda servicios. La Metodología, permitirá a la Firma, guiar a sus clientes en la implementación de una adecuada gestión de riesgos de TI. Este resultado será, además, un apoyo importante en proyectos más ambiciosos relacionados con el cumplimiento de normativas o estándares en el campo de la tecnología de información, proyectos en los cuales, la gestión adecuada de los riesgos es un componente fundamental.

Para el desarrollo de la Propuesta de Metodología, se establece una base o marco teórico con las mejores prácticas e investigaciones relacionadas con la gestión del riesgo de TI. El sustento teórico principal, tal como el título del trabajo lo indica es lo que se propone en COBIT 5 para llevar a cabo la gestión de los riesgos de tecnología de información. Tanto los procesos atinentes de COBIT, como la demás teoría identificada, constituyen el principal sustento para el desarrollo del proyecto.

El contenido de la Metodología propuesta, se ha estructurado en dos etapas con base en dos procesos presentados por COBIT 5. Tal y como se mencionó anteriormente, el primero de ellos atiende aspectos de nivel estratégico en relación con las políticas y lineamientos para la gestión de los riesgos de TI. Mientras tanto, el segundo proceso se enfoca propiamente, en llevar a cabo las actividades necesarias para la gestión de los riesgos de TI. La Figura 2, muestra cuáles son estos procesos y el orden lógico que siguen.

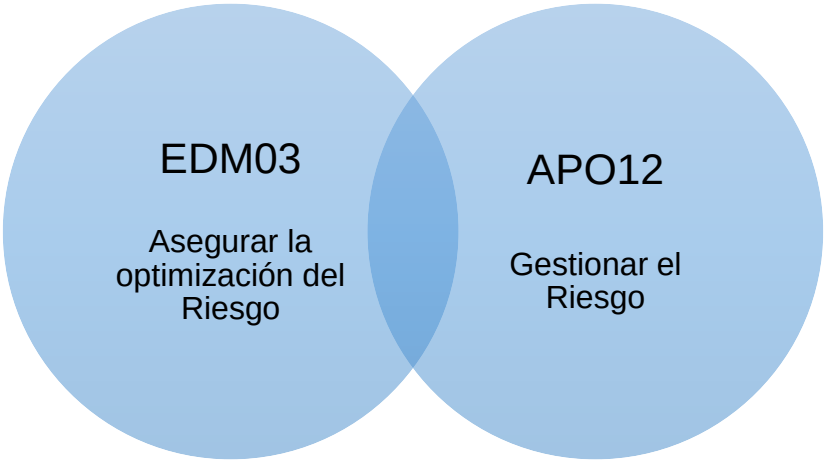


Figura 2. Procesos COBIT 5 para la gestión de riesgos de TI
Fuente: Elaboración propia. Adaptado de COBIT 5.

Aunque los procesos presentados, son distintos y pertenecen a dominios de COBIT independientes; lo cierto es que son complementarios uno con el otro y que, juntos, permiten cubrir los aspectos esperados sobre la gestión de riesgos de Tecnología de Información. En los dos apartados siguientes, se detalla cómo se abordan las etapas propuestas en la Metodología y se detalla los aspectos tomados en cuenta para cada una de ellas. En un tercer apartado, se abordan los aspectos que no se consideran como parte de la Propuesta de Metodología.

Antes de adentrarse en el detalle de las etapas que contempla la Propuesta de Metodología es de importancia agregar que estas etapas se refieren a los dos grandes procesos que la Metodología permitirá implementar. Es decir, como resultado de este trabajo de graduación, la firma Deloitte, obtendrá una herramienta de conocimiento que le permita implementar en sus proyectos, los dos aspectos principales de la gestión de riesgos de TI según COBIT 5, a saber: la definición de lineamientos sobre los riesgos de Tecnologías de Información y el ciclo de gestión de los mismos.

1.9.1 Etapa 1: Lineamientos organizacionales sobre riesgos de TI

Esta primera etapa, se basa en el proceso EDM03 de COBIT 5, proceso denominado "Asegurar la optimización del Riesgo" y que pertenece al área de procesos de Gobierno de TI propuestos en COBIT 5, específicamente al dominio "Evaluar, Orientar y Supervisar".

De acuerdo con lo indicado en COBIT 5, el proceso EDM03, consiste en asegurar que los aspectos relevantes sobre los riesgos de TI en una organización, como lo son el apetito de riesgo y la tolerancia al riesgo, se entiendan adecuadamente, se encuentren articulados y sean comunicados en la organización. Además, permite asegurar que el riesgo asociado con el uso de tecnologías de información en una organización, sea debidamente identificado y que se realice la correcta gestión del mismo.

Para la implementación de este proceso, COBIT 5 sugiere tres Prácticas Clave de Gobierno, las cuales se muestran en la Figura 3. Estas prácticas, permiten a las organizaciones llevar a cabo una evaluación de la gestión de riesgos de TI, orientar dicha gestión cuando se identifiquen desviaciones y mantener un monitoreo constante para garantizar la adecuada gestión de los riesgos relacionados con la tecnología de información.

Figura 3. Prácticas de Gobierno EDM03
Fuente: Elaboración propia. Adaptado de COBIT 5.

La primera etapa de la Propuesta de Metodología, considera transversalmente las Prácticas de Gobierno sugeridas por COBIT 5, sin embargo, se realiza una agrupación de las actividades que integran dichas prácticas con el objetivo de satisfacer tres aspectos primordiales que, según Deloitte, generan un mayor valor agregado en las organizaciones. La Tabla 1, presenta esos aspectos, los define e introduce lo que se incluye para cada uno de ellos, en el alcance de este trabajo final de graduación.

Tabla 1. Aspectos primordiales de la Etapa 1

Aspecto	Detalle	Abordaje en la Propuesta de Metodología
Apetito de Riesgo de TI.	Es una estimación de alto nivel que indica cuánto riesgo está dispuesta la organización a aceptar.	Se creará algún mecanismo que permita definir el Apetito de Riesgo de TI en una organización. El mecanismo que se defina, deberá contemplar las actividades que sugiere COBIT en relación con este aspecto. Además, debe tener un balance entre especificidad y adaptabilidad, esto con el objetivo de que Deloitte lo pueda utilizar en sus diferentes proyectos.
Tolerancia al Riesgo de TI.	Es el nivel máximo de riesgo, en términos medibles, que la organización puede resistir, para conseguir un objetivo específico.	Al igual que en el caso anterior se debe proponer un mecanismo determinado que permita establecer, para una organización, el nivel de Tolerancia al riesgo de TI. Del mismo modo, el mecanismo que se incluya en la Metodología, deberá basarse en lo que indica COBIT 5 y además, sin ser demasiado general, debe permitir ser adaptado para diferentes organizaciones.
Política de Riesgos de TI.	Son los lineamientos de nivel directivo en una organización, sobre la gestión de los riesgos.	Se contemplará las principales actividades necesarias para la definición de una Política Organizacional de Riesgos de TI, siempre en concordancia con lo que indica COBIT 5. El mecanismo que se proponga como parte de la Metodología, deberá permitir su utilización en distintas organizaciones.

Fuente: Elaboración propia.

Los aspectos contemplados en la Etapa 1, descritos en la tabla anterior, forman parte de la Propuesta de Metodología que resulta de este trabajo de graduación. Aportan un enfoque estratégico a la gestión de riesgos de TI, alineándola con las necesidades y políticas organizacionales. Luego de esta etapa de Lineamientos sobre Riesgos de TI, corresponde definir las actividades necesarias para gestionar los riesgos y el ciclo o procedimiento respectivo. Para esto, se contempla la Etapa 2, detallada a continuación.

1.9.2 Etapa 2: Ciclo de gestión de riesgos de TI

La segunda etapa, se basa en el proceso APO12 de COBIT 5, proceso denominado "Gestionar el Riesgo" y que pertenece al área de procesos de Gestión de TI propuestos en COBIT 5, específicamente al dominio "Alinear, Planificar y Organizar".

De acuerdo con lo indicado en COBIT 5, el proceso APO12, consiste en realizar la identificación, evaluación y reducción de aquellos riesgos que estén relacionados con la tecnología de información. Lo anterior, de forma continua y siempre en sintonía con los niveles de tolerancia y las políticas de la dirección ejecutiva definidas previamente; este último aspecto, entrelaza la Etapa 1 con la Etapa 2 requiriéndose, para la implementación esta última, información que se obtiene de la primera.

Para la gestión de este proceso, COBIT 5 sugiere seis Prácticas Clave de Gestión, las cuales se muestran en la Figura 4. Dichas prácticas facultan a las organizaciones, para realizar una recopilación de datos sobre los riesgos y llevar a cabo un análisis de los mismos, así como mantener un perfil de riesgos y acciones definidas para responder ante estos.

Figura 4. Prácticas de Gestión APO12
Fuente: Elaboración propia. Adaptado de COBIT 5.

Al igual que la Etapa 1, la Propuesta de Metodología, considera las Prácticas de Gestión sugeridas por COBIT 5 de manera transversal y se realiza una reorganización de las actividades incluidas en dichas Prácticas. Esto, en aras de crear un Ciclo de Gestión de Riesgos con los pasos que proponen las normas ISO 31000. Deloitte, solicitó utilizar este enfoque pues los pasos se adaptan a diferentes marcos de referencia y normativas aplicables; además, utilizar este ciclo podría facilitar un proceso de certificación en la Norma mencionada. La Figura 5, muestra el ciclo de gestión de riesgos solicitado por la organización.

Figura 5. Ciclo de gestión de riesgos de TI
Fuente: Elaboración propia. Adaptado de ISO 31000.

En el ciclo que ilustra la figura anterior, no se contempla la primera actividad que indica ISO 31000, referente al establecimiento del contexto. Este paso se queda fuera de la Etapa 2, dado que en la Etapa 1 de la Metodología, se contemplan los aspectos de estrategia y contexto de los riesgos de TI.

La Tabla 2, presenta los pasos que tendrá el Ciclo de Gestión de Riesgos de TI, define cada uno y presenta lo que este trabajo final de graduación contempla para cada uno de ellos.

Tabla 2. Pasos solicitados para la Etapa 2

Paso	Detalle	Abordaje en la Propuesta de Metodología
Identificación de Riesgos.	Consiste en la identificación de los riesgos para la organización, derivados del uso de las TI.	Se generará un método o técnica que permita realizar una identificación exhaustiva de las fuentes de riesgo relativas a TI. El método entregado, debe considerar incluso los riesgos cuya fuente no esté bajo el control de la organización. Y deberá poder adaptarse a distintas organizaciones.

Paso	Detalle	Abordaje en la Propuesta de Metodología
	Escenarios de Riesgo.	Con el apoyo de *COBIT 5 para Riesgos*, se incluirá en la Propuesta de Metodología, el tema de los escenarios posibles de riesgo para las distintas áreas relacionadas con TI. Se debe generar un mecanismo que permita definir los escenarios de riesgo en una organización para, con esa base, identificar los riesgos relativos a TI.
Análisis de Riesgos.	Consiste en comprender el riesgo, genera elementos de entrada para la evaluación y permite visualizar si es necesario tratar el riesgo y cómo hacerlo.	Se diseñará y propondrá una o varias actividades para llevar a cabo el análisis de un riesgo. La propuesta contemplará el análisis de tipo cualitativo, cuantitativo, o bien, una combinación de estos dos. Las actividades propuestas deberán ser adaptables para la realidad de distintas organizaciones.
Evaluación de los Riesgos.	Pretende determinar cuáles riesgos se deben tratar y cuál es la prioridad para hacerlo. Realiza una comparación entre lo que se definió en la Etapa 1 y el análisis del riesgo del paso anterior.	La Propuesta de Metodología contemplará la guía para efectuar la comparación del análisis de un riesgo con los lineamientos de la Etapa 1. De esta forma, será posible decidir cuáles riesgos se ubican en los diferentes rangos de apetito y tolerancia, para proceder según la Política de Riesgos de TI establecida. La metodología deberá considerar la implementación de las sugerencias en diferentes tipos de organizaciones.
Tratamiento de los Riesgos	La organización, debe seleccionar e implementar una o varias opciones para atender los riesgos que se han identificado, analizado, evaluado y requieren tratamiento.	Se generará una propuesta de atención o tratamiento de los riesgos, de manera que pueda utilizarse en diversas organizaciones. La propuesta generada, deberá seguir el orden lógico mostrado a continuación: • Valorar un tratamiento. • ¿El riesgo residual es aceptable? ○ Si no, valorar un nuevo tratamiento. • Evaluar la eficacia del tratamiento.

Paso	Detalle	Abordaje en la Propuesta de Metodología
	Estrategias para Riesgo.	Se propondrá un conjunto de posibles estrategias y se indicará para cuáles casos son aplicables las mismas. Por ejemplo, modificar la probabilidad o compartir un riesgo.
Seguimiento y Revisión.	Se trata de dar seguimiento y revisar el estado de los riesgos que requirieron tratamiento.	Se propondrá un mecanismo que permita vigilar de manera periódica o cuando sea necesario, el avance en la implementación del tratamiento seleccionado para un riesgo. Además, en el paso de Tratamiento de los Riesgos se contemplará la planificación del seguimiento y las revisiones. La propuesta debe considerar su posible uso en distintos tipos de organizaciones.
Comunicación y Consulta.	Esta parte, más que un paso es una actividad que debe realizarse durante todo el proceso de gestión de riesgos. Se trata de enviar, atender y recibir, comunicaciones y consultas de las partes interesadas.	La Propuesta de Metodología incluirá el desarrollo de un Plan de Comunicación para la Gestión de Riesgos. Este Plan puede tener distintos enfoques, abarcará las comunicaciones internas y externas y uno de sus principales beneficios será que los intereses de las distintas partes sean comprendidos y se tomen en cuenta. La propuesta debe permitir que se desarrolle un Plan para diferentes tipos de organizaciones.

Fuente: Elaboración propia.

Como se evidenció en la tabla anterior, para el desarrollo de la Propuesta de Metodología, además de lo indicado en COBIT 5 e ISO 31000, se tomará como referencia el marco COBIT 5 para Riesgos, que ofrece un mayor nivel de detalle sobre cómo utilizar COBIT 5 para la gestión de riesgos de TI.

Con esta segunda etapa, la Propuesta de Metodología permite completar una gestión efectiva del riesgo asociado al uso de las TI. La Metodología debe abarcar todos los aspectos mencionados en esta sección, así como aquellos asuntos que, durante el desarrollo del proyecto, resulten necesarios para alcanzar alguno de los puntos declarados anteriormente. Los aspectos que no se contemplan, se presentan en el siguiente apartado.

1.9.3 Exclusiones

En este apartado, se listan los aspectos que no son tomados en cuenta en la Propuesta de Metodología. Dichos aspectos, no forman parte de los resultados esperados ni de los entregables del proyecto. Por tanto, la Propuesta de Metodología, no necesariamente debe incluir aspectos relacionados con lo que aquí se define, exceptuando los que hayan sido declarados en apartados anteriores.

Antes de listar los aspectos excluidos es importante aclarar, que el estudiante y el Instituto Tecnológico de Costa Rica, están exentos de cualquier responsabilidad por daños o pérdidas ocasionadas por el uso de la Metodología resultante de este trabajo final de graduación. Así mismo, el proyecto se realiza para la empresa costarricense Deloitte & Touche, S.A. y no para otras firmas miembro de DTTL. El uso de la Metodología por parte de otras entidades de Deloitte, queda bajo responsabilidad de Deloitte & Touche, S.A.

Además, la Propuesta de Metodología está dirigida a colaboradores de Deloitte que tengan conocimiento en principios de administración, en tecnología de información y que, además, estén familiarizados con el tema de gestión de riesgos. El proyecto no garantiza que la Metodología pueda ser utilizada adecuadamente por personas que no satisfagan las características indicadas.

No se incluirán como parte del proyecto, los siguientes aspectos:

- El desarrollo, recomendación o implementación de herramientas tecnológicas para soportar la gestión de riesgos de TI. Deloitte considera que este aspecto puede representar un proyecto independiente y la organización planea desarrollarlo en el futuro.
- La elaboración de cualquier plan, procedimiento o similar, para el mantenimiento o actualización de la Propuesta de Metodología que se entrega a Deloitte o de cualquiera de sus componentes, anexos y otros.
- La implementación del proceso o las actividades de gestión de riesgos de TI en Deloitte o alguno de sus clientes; así como pruebas o planes piloto. Si la Firma desea realizar algún tipo de prueba sobre lo que se esté desarrollando, el trabajo necesario para efectuar tales pruebas será cubierto por la empresa y la información obtenida podría ser utilizada para realimentar este trabajo si así lo acuerda el equipo de proyecto.

- La implementación de cualquier proceso COBIT, de Normas ISO o de otros estándares y marcos relacionados con la gestión y gobierno de TI.
- La consideración de recomendaciones o solicitudes de organizaciones distintas a Deloitte o de profesionales internos que no formen parte del equipo de trabajo del proyecto.
- Todo tipo de capacitaciones o formación en el uso de la Propuesta de Metodología o de los procesos y marcos referenciales utilizados para su elaboración.
- Todo tipo de manuales o guías para el uso de la Metodología.
- Proveer recursos humanos, materiales, financieros, etc., para la implementación, uso o actualización de la Metodología.

Estas exclusiones, así como lo declarado en toda la sección de Alcance del proyecto, representan el trabajo que se desarrolla como parte del trabajo final de graduación. Este alcance, incluye todos los aspectos que la empresa espera del proyecto y se basa en las mejores prácticas, solicitadas también por Deloitte y que serán analizadas en el capítulo correspondiente con el Marco Teórico.

Las secciones siguientes, presentan los entregables, supuestos y limitaciones del proyecto.

1.10 Entregables del proyecto

Esta sección, presenta los principales entregables que se generan como parte del trabajo de graduación. Para ello se contemplan tres categorías, los entregables académicos, los de producto y los de gestión del proyecto.

1.10.1 Entregables académicos

Estos entregables están dirigidos al Tecnológico de Costa Rica, específicamente a la Coordinación del Trabajo Final de Graduación y a la profesora tutora del trabajo de graduación.

Estos entregables se dividen en:

- Avances solicitados por la profesora tutora o por la coordinación.
- Informe final del trabajo de graduación.
- Presentación final y defensa del trabajo de graduación.

1.10.2 Entregables de producto

Los entregables de producto, representan el resultado del trabajo final de graduación, son los que se entregan a la organización y generan valor con su contenido.

Para este proyecto, el entregable de producto consiste en la Propuesta de Metodología para la gestión de riesgos de TI basada en COBIT 5, la cual, se encuentra en el quinto capítulo de este documento.

1.10.3 Entregables de gestión del proyecto

Estos entregables, representan una serie de documentación que se genera durante el proyecto y pretenden brindar información sobre los acuerdos, cambios, estado, entre otros aspectos relacionados con la gestión del proyecto.

Los principales entregables de gestión son los presentados a continuación, no obstante, se pueden presentar otros si son solicitados por la profesora tutora, por la coordinación del trabajo o por la organización.

- Minutas de reunión.
- Solicitudes de cambio.
- Informes de avance.

1.11 Supuestos del proyecto

Esta sección presenta algunos aspectos que se asume, estarán presentes o serán aportados para el desarrollo del proyecto. A continuación, se presenta la lista de dichos supuestos.

- Disposición de la organización para brindar información, atender consultas y dar retroalimentación al desarrollo del TFG.
- Estimación adecuada del tiempo y la carga de trabajo de las actividades necesarias.
- Disponibilidad de las herramientas y recursos necesarios para la elaboración de la Propuesta de Metodología.
- Las personas representantes de la organización, cuentan con conocimientos en el área de gestión de riesgos de TI.
- Canales adecuados de comunicación entre las partes involucradas en el proyecto.

- La profesora asignada por el Tecnológico de Costa Rica, asesora y brinda apoyo en la gestión del trabajo final de graduación.

1.12 Limitaciones

Esta sección, presenta las principales restricciones o limitaciones que fueron previstas para el proyecto. Dichas restricciones son consideradas durante el desarrollo del proyecto, para evitar conflictos y para lograr una correcta gestión de las distintas actividades del proyecto y los recursos que estas requieren.

Si las restricciones no se gestionan adecuadamente, pueden afectar negativamente al trabajo de graduación. Las principales restricciones, son las presentadas a continuación.

- Complicaciones con la integración de COBIT 5 y otros marcos para la gestión de riesgos de TI.
- Poca experiencia y documentación en la organización, por causa de lo reciente que es COBIT 5.
- Disponibilidad limitada del equipo de trabajo para el proyecto.
- La Propuesta de Metodología debe considerar diferentes tipos de organización, por tanto, puede no incluir aspectos específicos para determinados tipos de organizaciones.

Marco Teórico

2 Marco Teórico

Este capítulo contiene la teoría que se utiliza como fundamento teórico principal para el presente trabajo final de graduación.

En primera instancia, se introducen el concepto de riesgo y otros términos relacionados que resultan de vital importancia, tanto para el desarrollo de la investigación como para la propuesta de solución resultante de este trabajo.

Más adelante, se contempla una serie de mejores prácticas, normas y marcos de referencia relevantes para la gestión de riesgos de TI. Algunos de estos, como COBIT 5 e ISO 31000 son, por solicitud de la firma consultora Deloitte, los que guían y sustentan el desarrollo de la Metodología para la gestión de riesgos de TI. Otros de los marcos, por su parte, complementan el conocimiento presentado en los dos anteriores, este es el caso de COBIT 5 para Riesgos.

Adicionalmente, se mencionan otros marcos y trabajos académicos relacionados con la gestión de riesgos de tecnología de información a lo largo del capítulo. El objetivo de incluir esta información, consiste en ampliar el conocimiento utilizado para el trabajo. Del mismo modo, se busca documentar una visión integral de la gestión de riesgos de TI, considerando para esto distintas fuentes de información como parte del proceso investigativo.

2.1 Riesgo

Esta sección, busca contextualizar los marcos y teorías considerados para el presente trabajo a través de la definición del término riesgo y más específicamente el riesgo de tecnología de información. Así mismo, se presentan algunos conceptos importantes relacionados con el riesgo.

El riesgo, se ha definido de diferentes maneras que, sin ser totalmente correctas o erróneas, permiten abstraer algunos puntos en común (Cienfuegos, 2013). Según concluye Cienfuegos, aunque no se puede hallar en la literatura una definición estandarizada de riesgo, se pueden mencionar algunas características comunes. Algunas de estas características presentadas por Cienfuegos son las siguientes:

- Riesgo es la probabilidad de un resultado adverso.
- Riesgo es una medida de la probabilidad y la severidad de los efectos adversos.

- Riesgo es la combinación de la probabilidad de un evento y sus consecuencias.
- Riesgo está definido como un conjunto de escenarios, cada uno de los cuales tiene una probabilidad y una consecuencia.
- Riesgo es igual a la combinación bidimensional de eventos/consecuencias y sus incertidumbres asociadas.
- Riesgo se refiere a la incertidumbre del resultado de las acciones y eventos.

Para Alvarado y Zumba "el ***riesgo*** es la probabilidad de que un evento ocurra y cause consecuencias (daños o pérdidas) que afecten la habilidad de alcanzar los objetivos" (2015). Además, estas autoras indican que "Dentro de la entidad el riesgo siempre estará presente aun cuando no se lo haya reconocido o detectado" (Alvarado & Zumba).

De acuerdo con lo anterior, el riesgo parece ir de la mano con el término de incertidumbre. Sin embargo, el riesgo puede ser explicado como "no saber con seguridad qué va a ocurrir", mientras que incertidumbre se refiere a "no saber ni siquiera las probabilidades de lo que va a ocurrir". Por lo tanto, en ese sentido, la incertidumbre sería inmedible e incalculable mientras que el riesgo se puede medir utilizando la fórmula: riesgo = probabilidad x impacto (Cienfuegos, 2013).

En función de los objetivos de este trabajo de graduación, conviene definir el término riesgo desde el punto de vista de la gestión de riesgos. En esta misma línea, se define riesgo como "la distribución de posibles desviaciones de los resultados esperados y los objetivos causadas por eventos de incertidumbre, que podrían ser internos o externos a la organización" (Cienfuegos, 2013).

2.1.1 Riesgo de TI

Este concepto se refiere al riesgo asociado con el uso de tecnología de información y comunicación en las organizaciones. Los riesgos de TI resultan de la incertidumbre que rodea a las operaciones de tecnología de información, de la probabilidad de pérdidas en el negocio y de resultados negativos provenientes del entorno interno o externo (Kumsuprom, 2010).

Los riesgos típicos incluyen pérdida de productividad o negocios debido al tiempo de inactividad, responsabilidad por brechas de seguridad que exponen la información de los clientes, multas por violaciones de normas y la imposibilidad de defenderse de demandas debido a la conservación inadecuada de registros (Alvarado & Zumba, 2015).

Este tipo de riesgos se puede clasificar en tres categorías (Alvarado & Zumba, 2015).

Riesgo de generación de valor de TI (estratégico)

Volver a enfocarse en los riesgos para consideraciones tales como cuan bien alineada esta la capacidad de las TI con las estrategias de negocio y su aprovechamiento con el fin de mejorar la eficiencia o efectividad de los procesos del negocio (Alvarado & Zumba, 2015).

Riesgo en la entrega de programas y proyectos de TI (proyecto)

La administración de riesgos necesita enfocarse en la habilidad para comprender y gestionar proyectos complejos de manera que no exista una deficiente contribución de las TI para las nuevas soluciones o mejoras (Alvarado & Zumba, 2015).

Riesgo en la entrega de servicios y operaciones de TI (operacional)

Aquellos riesgos que podrían comprometer la efectividad de los servicios soportados por TI y la infraestructura de apoyo. Se debe recordar que el rendimiento y disponibilidad de los servicios de TI pueden influir directamente en el valor de la empresa llegando a reducirlo e inclusive destruirlo (Alvarado & Zumba, 2015).

Actualmente, la tecnología de información permite convertir los datos en información y de esta, obtener conocimiento; creando así valor en las organizaciones (Valencia, Marulanda, & López, 2016). Así mismo, se indica que las TI apoyan la toma de decisiones en una organización en tres niveles distintos: operativo, táctico y estratégico (Valencia et al.). Lo anterior es congruente con la clasificación del riesgo de TI descrita más arriba. Es natural que, al estar la tecnología de información presente en tres niveles distintos, se generen también riesgos en cada uno de ellos.

Por otra parte, Kumsuprom indica que los riesgos de TI se pueden clasificar en estratégicos, técnicos y operativos (2010). Así mismo, este autor propone una serie de fuentes de riesgo y factores clave para cada categoría de riesgos de TI (Kumsuprom). La Tabla 3 presenta el detalle de las fuentes y factores clave para cada tipo de riesgo.

Tabla 3. Fuentes de riesgo y factores clave asociados

Tipo de riesgo TI	Fuentes de riesgo	Factores clave
Operacional y riesgos técnicos asociados.	• Pérdida de activos informáticos. • Registro inexacto de datos. • Aumento del riesgo de fraude. • Pérdida o robo de datos. • Interrupción del negocio. • Violaciones de privacidad. • Brechas informáticas. • Protección insuficiente de la información o los sistemas. • Roles y responsabilidades pocos claros. • Faltas técnicas y humanas. • Vulnerabilidades de sistemas. • Fraude o eventos externos.	• Gestión de activos. • Gestión del recurso humano. • Gestión de seguridad de la información. • Gestión de tecnología de información.
Estratégico.	• Falta de estrategia. • Falta de gestión específica para riesgos de TI. • La naturaleza de la perspectiva de gestión. • Fallos en los procesos de gestión. • La responsabilidad de la auditoría y el control de las TI. • La complejidad de los sistemas. • Plan estratégico poco claro. • Plan operativo poco claro. • Fallos en la gestión de proyectos de TI.	• Estrategia organizacional. • Política organizacional. • Planificación en relación con planes estratégicos y planes operativos.

Fuente: (Kumsuprom, 2010)

Del mismo modo, Alvarado y Zumba indican que no todos los riesgos de TI provienen de sucesos inevitables como desastres naturales, sino también de incidentes operativos, procesos inadecuados, normativas u otros factores controlables (2015). En la Tabla 4 estas autoras muestran ejemplos de amenazas, vulnerabilidades y riesgos de TI asociados, con base en COBIT 5.

Tabla 4. Ejemplo de amenazas, vulnerabilidades y riesgos de TI con base en COBIT 5

Amenazas	Vulnerabilidad	Riegos
Maliciosa Ingeniería Social.	Falencias en capacitación del personal respecto a los nuevos métodos utilizados para una intrusión.	Información sensible sea revelada.
Natural Inundación.	Ubicación incorrecta de servidores y ausencia de copias de respaldo para la información.	Destrucción de la infraestructura e información.
Falla	Ausencia de un plan de continuidad de aquellos procesos críticos para la entidad.	Interrupción de servicios.
Accidental	Ineficiencia en los controles internos para el manejo de dispositivos.	Pérdida de un dispositivo portátil con información sensible.

Fuente: (Alvarado & Zumba, 2015)

2.1.2 Gestión del riesgo de TI

> Los riesgos de TIC han estado presentes en la evolución de los diferentes modelos de negocio y reglamentaciones que han surgido a través del tiempo, […], lo que pone de manifiesto que cualquier riesgo tecnológico no puede ser analizado al margen del contexto organizacional dado su efecto dominó sobre sus procesos, metas y objetivos. Ello conlleva un proceso de articulación entre las actividades de riesgo organizacional y riesgo de TIC, y en particular [a] desarrollar iniciativas de [gobierno y gestión de riesgos de TI] (Valencia et al., 2016).

Valencia et al., aclaran que “El concepto de gobierno y gestión de riesgos de TIC surge a partir de la noción de gobierno y gestión de TIC. Entendido el gobierno de TI, […] como un sistema por el que se dirige y controla la utilización actual y futura de las TIC” (2016).

La gestión de TI, por su parte, “se centra en administrar e implementar la estrategia tecnológica del día a día, y su enfoque está más orientado al suministro interno de TI” (Valencia et al., 2016). Además, se define la gestión de TI como “el sistema de controles y procesos requeridos para lograr los objetivos estratégicos establecidos por la dirección de la organización” (Valencia et al.).

Como parte de su investigación, Valencia et al. concluyen que algunas fases son comunes en cualquier proceso de gestión de riesgos. Estos autores, afirman que las fases se pueden resumir en:

- Establecimiento del contexto.
- Identificación de riesgos.
- Análisis de riesgos.
- Valoración de riesgos.
- Plan de tratamiento de riesgos.
- Comunicación y consulta.
- Monitoreo.

Estas fases, son congruentes con lo que se indica en las mejores prácticas relacionadas a la gestión de riesgos de TI. Más adelante, en este mismo capítulo, se detalla lo indicado por dichas prácticas. Los apartados siguientes muestran algunos aspectos clave en la gestión de riesgos de TI, las principales diferencias con una gestión de riesgos organizacional y algunos principios importantes para un enfoque estructurado de gestión de riesgos de TI.

2.1.2.1 Aspectos clave en la gestión de riesgos de TI

En (Kumsuprom, 2010), Se describen algunos aspectos clave para la gestión de riesgos de TI. En seguida se resumen dichos aspectos según lo indicado por este autor.

Gestión de recursos humanos

La gestión de riesgos de TI se encuentra inmersa en la estructura organizacional de la empresa o entidad en la que se desarrolle. Para garantizar una gestión de riesgos eficaz, la organización debe tener el conocimiento y establecer los procedimientos adecuados. Así mismo, la arquitectura organizacional, debe permitir que los colaboradores desempeñen sus responsabilidades en la gestión de riesgos de TI (Kumsuprom, 2010).

Gestión de TI

La importancia de la gestión de TI para una adecuada gestión de riesgos, radica en que la primera permite conocer los recursos y la capacidad de TI (Kumsuprom, 2010). Los recursos de TI están directamente ligados con el riesgo, pues pueden ser factores causantes de riesgo o bien, pueden verse afectados por la ocurrencia de riesgos. La capacidad de TI, por su parte, es un concepto al que se debe prestar atención en pro de disminuir el nivel de riesgo asociado.

Gestión de la seguridad de la información

La seguridad de la información, tanto física como lógica, es un aspecto relevante para la gestión de riesgos de TI. Permite asegurar que los datos y la información están protegidos con identificación/autenticación, autorización, confidencialidad, integridad y no repudio. Los controles de seguridad que establezca la organización son aliados importantes para la gestión de los riesgos; tanto aquellos asociados con vulnerabilidades propias de los activos como los que son causados por el hombre (Kumsuprom, 2010).

Controles para riesgos de TI

Tanto los controles que se haya establecido para los objetivos de negocio como los relacionados con los objetivos de TI, deben adaptarse al modelo de gestión de riesgos de TI. Adaptarse de manera que aseguren el diseño de políticas, procedimientos, prácticas y de una estructura organizacional que permita prevenir, detectar y corregir los riesgos de TI oportunamente (Kumsuprom, 2010).

2.1.2.2 Aspectos diferenciadores entre la gestión de riesgos general y la de TI

Los activos objeto del análisis de riesgo y los parámetros utilizados para medir el impacto del riesgo, son los principales aspectos diferenciadores entre un proceso de gestión del riesgo organizacional y uno específico para la gestión de riesgos de TI (Valencia et al., 2016). En los apartados siguientes, se resume lo indicado por los autores al respecto de estos dos aspectos.

Activos objeto del análisis de riesgo

Según Valencia et al., los principales objetos que se debe considerar para el análisis de riesgos de TI son la información y los activos tecnológicos (2016). Sin embargo, estos autores indican que debido a la evolución que ha experimentado la función de TI en las organizaciones, se debe agregar el concepto de servicios de TI. Pues esta función ha pasado de gestionar simplemente recursos tecnológicos, a realizar una gestión integral de servicios que soportan los procesos de una organización (Valencia et al.).

Del párrafo anterior es posible resumir que, para una gestión integral de riesgos de TI, el análisis debe considerar tres áreas fundamentales: la información, los activos tecnológicos y los servicios de TI. En congruencia con estas tres áreas, Valencia et al., proponen un modelo de 12 capas interdependientes que deben ser consideradas por una gestión integral de riesgos, ya que podrían generar un efecto dominó en caso de falla en alguna de ellas

(2016). La Tabla 5 presenta las capas que, según (Valencia et al.), se debe considerar en el análisis de riesgos de TI.

Tabla 5. Capas de tecnologías de información y comunicaciones

1	Procesos de negocio.
2	Servicios de TI.
3	Datos, información, conocimiento.
4	Sistemas de información transaccionales.
5	Sistemas de información de soporte.
6	Motores de bases de datos.
7	Sistemas operativos.
8	Computadoras personales de escritorio e impresoras.
9	Servidores.
10	Centros de redes y cableado.
11	Centros de cómputo.
12	Sistemas de energía.

Fuente: (Valencia et al., 2016)

Parámetros para la medición del impacto

Según (Valencia et al., 2016), el impacto de cualquier tipo de riesgo afecta directamente los objetivos de una organización, sin embargo, el impacto de los riegos de tecnología de información se mide generalmente en tres términos: Confidencialidad, Integridad y Disponibilidad. A continuación, se presenta un resumen de estos tres aspectos.

Confidencialidad hace referencia la propiedad de la información dolo ser accesible a individuos, entidades o procesos que tengan la respectiva autorización y que requieran conocer dicha información (Valencia et al., 2016).

Integridad es la propiedad de salvaguardar y garantizar la exactitud y la completitud de los datos (Valencia et al., 2016).

Disponibilidad se refiere a que, tanto la información como los activos tecnológicos, deben estar disponibles en el momento en que así sea requerido por los procesos de negocio (Valencia et al., 2016).

2.1.2.3 Enfoque estructurado para la gestión de riesgos de TI

El desarrollo de las tecnologías de información y comunicación, ha crecido dramáticamente para soportar los procesos de negocio (Kumsuprom, 2010). Esto da paso al surgimiento de estructuras de gestión como lo son las siguientes.

Gobierno de TI

Para la adecuada gestión del riesgo de tecnología de información, se debe contar con una estructura de Gobierno de TI, que sea parte integral del Gobierno Corporativo. Una estructura de gobierno de este tipo, es capaz de definir lineamientos y responsabilidades para la adecuada gestión de riesgos, así como un proceso de evaluación de controles. Además de velar por el alineamiento de la gestión de riesgos con las aspiraciones del negocio (Kumsuprom, 2010).

Gobierno de seguridad de la información

La seguridad de la información, no solamente es un tema técnico, también incluye aspectos relevantes para el negocio. Una estructura de Gobierno de Seguridad de la Información tiene entre sus principales funciones proveer a la organización de una estrategia general para la seguridad de la información (Kumsuprom, 2010). Dicha estrategia, según (Kumsuprom, 2010), debe incluir:

- El entendimiento de la información y de la seguridad de la información que son críticas para la organización.
- La revisión de la inversión en seguridad de la información para asegurar el alineamiento con la estrategia y el perfil de riesgo de la organización.
- Apoyar el desarrollo y la implementación de un programa integral de seguridad de la información.

De acuerdo con (Kumsuprom, 2010) el liderazgo, así como los procesos organizacionales son fundamentales en el gobierno de seguridad de la información y sus principales beneficios son:

- Mayor previsibilidad y menor incertidumbre en las operaciones de negocio mediante la reducción del riesgo relacionado con la seguridad de la información a niveles aceptables.
- Aseguramiento de una política efectiva de seguridad de la información y del cumplimiento de dicha política.

- Una base sólida para la gestión eficiente y efectiva de riesgos, la mejora en el proceso y la rápida respuesta a incidentes relacionados con seguridad de la información.

2.2 COBIT 5

El primer y principal marco de referencia para este trabajo, es COBIT 5. Esta sección presenta una serie de aspectos generales sobre dicho marco, incluyendo una descripción del mismo, un resumen de la evolución que ha experimentado y su estructura. En los dos últimos apartados se profundiza en dos de los procesos del marco. Estos procesos serán utilizados como fundamento principal de la Propuesta de Metodología para la gestión de riesgos de TI.

La principal razón de utilizar este marco es la solicitud directa de la firma Deloitte & Touche, S.A., sin embargo, existen diferentes condiciones que hacen a COBIT 5, un marco óptimo para ser considerado en la gestión de riesgos de TI. Una de ellas es que “COBIT 5 se alinea con una variedad de estándares reconocidos y aceptados globalmente, como son: ISO 27000, COSO ERM, ISO 9001, ISO 31000, PMBOK […], CMMI […], etc., los cuales se usan como herramientas por auditores y administradores de negocios” (Alvarado & Zumba, 2015).

Considerando que Deloitte es una firma internacional que busca generar valor a sus clientes mediante la implementación de prácticas aceptadas (Deloitte & Touche, S.A., 2017), resulta de gran valor diseñar un modelo de gestión de riesgos de TI que se encuentre alineado con los estándares mencionados en el párrafo anterior.

En los objetivos específicos de este trabajo, se indica que la Propuesta de Metodología debe adecuarse a distintos tipos de organizaciones que sean o puedan ser clientes de Deloitte. Por su parte, COBIT 5 es genérico y útil para empresas de todos los tamaños, tanto comerciales, como sin ánimo de lucro o del sector público (Information Systems Audit and Control Association [ISACA], 2012).

Otro aspecto importante es que COBIT 5 provee un marco de trabajo integral que ayuda a las organizaciones en el gobierno y la gestión de las TI corporativas (Vanegas, 2013). Según cita Vanegas, este marco ayuda a las empresas a mantener el equilibrio entre la generación de beneficios desde TI, el nivel de riesgo asociado y el uso de recursos. Para

ello, COBIT 5 se basa en cinco principios claves para el gobierno y la gestión de riesgos empresariales (Vanegas). La Figura 6 muestra estos cinco principios.

Figura 6. Principios de COBIT 5
Fuente: (ISACA, 2012)

De los principios mostrados en la Figura 6, hay dos que resultan particularmente importantes en el contexto de este trabajo. En los dos apartados siguientes se detalla esta idea.

2.2.1 Un marco de referencia integrado

El primer principio que sobresale para el desarrollo de este trabajo es el principio número tres, Aplicar un Marco de Referencia Único Integrado. Esto pues parte del valor que genera este trabajo de graduación para la firma Deloitte, se debe a la estandarización de prácticas y procedimientos utilizados para la gestión de riesgos de TI.

Según (ISACA, 2012), hay muchos estándares y buenas prácticas relativos a TI, ofreciendo cada uno ayuda para un subgrupo de actividades de TI. COBIT 5 se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las TI de la empresa.

Por lo anterior, el uso de COBIT 5 como base para la Propuesta de Metodología; permite además de alcanzar los objetivos planteados para el trabajo, garantizar la compatibilidad con otras prácticas y marcos utilizados en la industria de tecnología de información.

2.2.2 Gobierno de TI y gestión de TI

Por otra parte, el principio número cinco, Separar el Gobierno de la Gestión es de importancia para el trabajo pues, como se indicó en el Alcance del proyecto, se contempla la Etapa 1: Lineamientos organizacionales sobre riesgos de TI (Gobierno) y la Etapa 2: Ciclo de gestión de riesgos de TI (Gestión).

"El marco de trabajo COBIT 5 establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos" (ISACA, 2012). A continuación, se citan las definiciones de ambos aspectos expuestas en COBIT 5.

2.2.2.1 Gobierno

El Gobierno asegura que se evalúan las necesidades, condiciones y opciones de las partes interesadas para determinar que se alcanzan las metas corporativas equilibradas y acordadas; estableciendo la dirección a través de la priorización y la toma de decisiones; y midiendo el rendimiento y el cumplimiento respecto a la dirección y metas acordadas (ISACA, 2012).

2.2.2.2 Gestión

"La gestión planifica, construye, ejecuta y controla actividades alineadas con la dirección establecida por el cuerpo de gobierno para alcanzar las metas empresariales." (ISACA, 2012).

2.2.3 Versiones de COBIT

En el año de 2012 ISACA, realiza la publicación de COBIT 5, el cual contiene el gobierno y la gestión de las TI de la empresa (Vanegas, 2013). Sin embargo, esta no es la única versión existente del marco. El nivel de madurez que le permite diferenciar entre gobierno y gestión como se indica en el apartado anterior, se ha alcanzado a través de un proceso de mejora que COBIT ha atravesado. De acuerdo con Vanegas, este modelo ha venido evolucionando desde su primera aparición en 1996 hasta su quinta versión lanzada en el 2012. La Tabla 6 presenta las diferentes versiones existentes del marco.

Tabla 6. Evolución de COBIT a través del tiempo

Versión	Año de publicación	Propósito o alcance
COBIT 1	1996	Auditoría.
COBIT 2	1998	Directrices de gestión.
COBIT 3	2000	Gestión.
COBIT 4	2005	Gobierno de TI.
COBIT 4.1	2007	Gobierno de TI.
COBIT 5	2012	Gobierno de la empresa.

Fuente: (Vanegas, 2013)

COBIT 4.1 define la gestión de riesgos partiendo de una conciencia de los riesgos por parte de los altos ejecutivos, un claro entendimiento del deseo de riesgo que tiene la organización, comprender los requerimientos de cumplimiento, y la transparencia de los riesgos significativos, incluyendo las responsabilidades de administración de riesgos dentro de la organización (Vanegas, 2013).

COBIT 5 amplía esta visión indicando que la gerencia en todos los niveles de la organización debería tener una adecuada comprensión del apetito del riesgo, requerimientos de cumplimiento y el impacto de los riesgos significativos de TI y otras operaciones en la gestión de riesgos que podrían impactar en forma individual o en toda la compañía en su conjunto (Alvarado & Zumba, 2015).

2.2.4 Estructura de COBIT 5

COBIT 5 es un marco de referencia, esto quiere decir que no es absoluto o prescriptivo, más bien permite ser adaptado por las diferentes organizaciones a la hora de implementarlo. El propio Marco de COBIT 5 indica que “una empresa puede organizar sus procesos como crea conveniente, siempre y cuando las metas de gobierno y gestión queden cubiertas. Empresas más pequeñas pueden tener pocos procesos; empresas más grandes y complejas pueden tener numerosos procesos, pero todos con el ánimo de cubrir las mismas metas” (ISACA, 2012). Las áreas fundamentales, que deben estar cubiertas se muestran en la Figura 7.

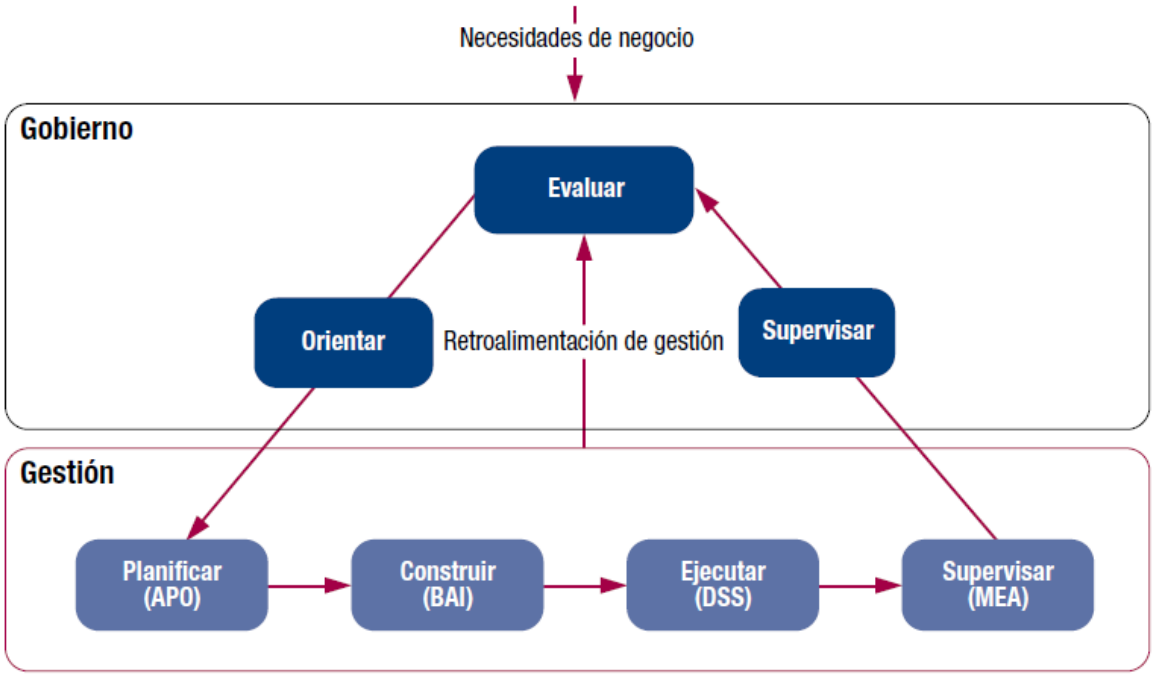


Figura 7. Áreas Clave de Gobierno y Gestión de COBIT 5
Fuente: (ISACA, 2012)

"COBIT 5 incluye un modelo de referencia de procesos que define y describe en detalle varios procesos de gobierno y de gestión. […]. El modelo de proceso propuesto es un modelo completo e integral, pero no constituye el único modelo de procesos posible (ISACA, 2012).

De acuerdo con lo que se muestra en la Figura 7, el modelo de referencia de procesos de COBIT 5 divide los procesos de gobierno y los de gestión de TI empresarial en dos categorías (ISACA, 2012). La organización de los procesos en dominios responde a la siguiente estructura de acuerdo con (ISACA):

- Gobierno.
  - Evaluar, Orientar y Supervisar (EDM).
- Gestión.
  - Alinear, Planificar y Organizar (APO).
  - Construir, Adquirir e Implementar (BAI).
  - Entregar, dar Servicio y Soporte (DSS).
  - Supervisar, Evaluar y Valorar (MEA).

La Figura 8 presenta el modelo completo de referencia de procesos de COBIT 5. Incluyendo los 37 procesos de gobierno y gestión que incluye el marco.

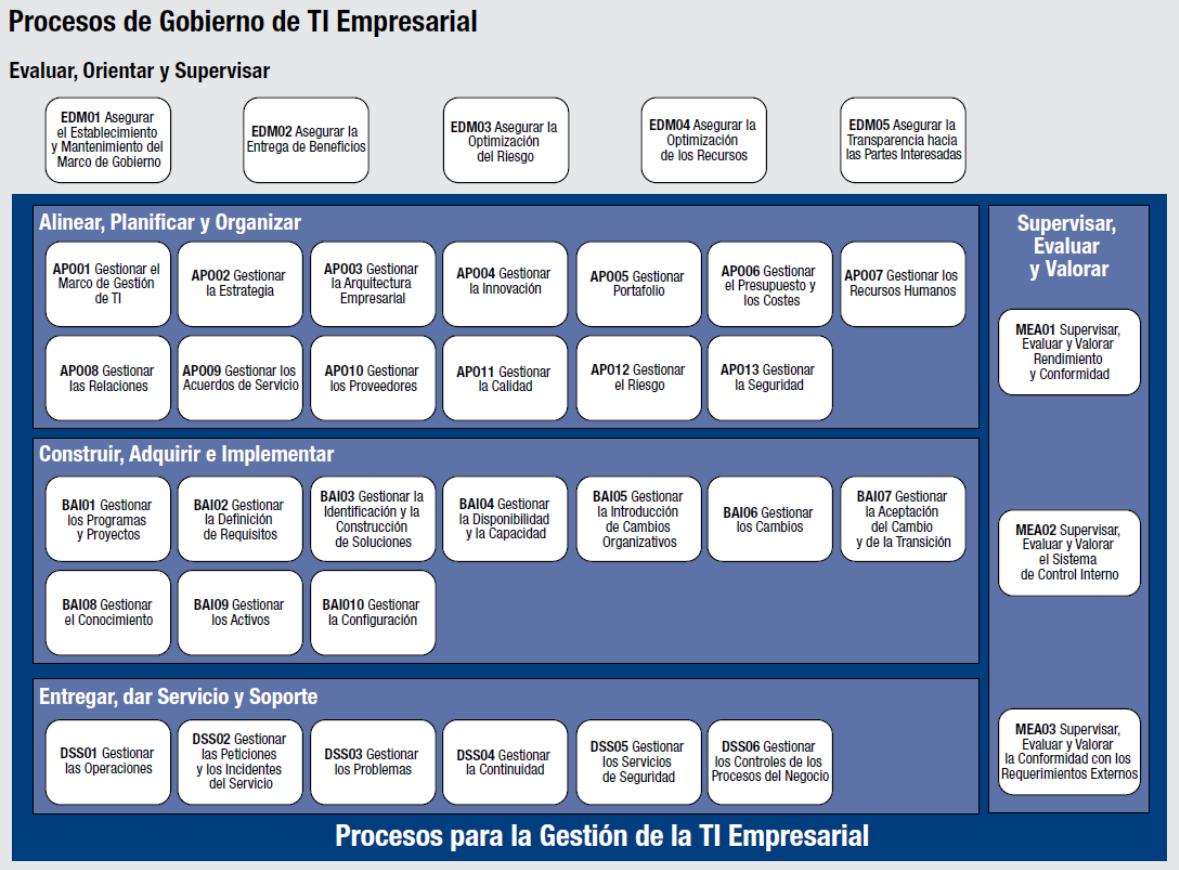


Figura 8. Modelo de Referencia de Procesos de COBIT 5
Fuente: (ISACA, 2012)

COBIT 5 […] es considerado actualmente uno de los principales referentes en materia de gobierno y gestión de tecnologías de información, de allí que contemple desde la perspectiva tanto de gobierno como de gestión de TI, el componente de riesgos (Valencia et al., 2016). Los procesos de COBIT 5 que tratan el tema de gestión de riesgos desde la perspectiva de gobierno y gestión son el EDM03 y el APO12 respectivamente. Como se define en el Alcance del proyecto, para efectos de este trabajo final de graduación, interesa conocer y analizar en detalle estos dos procesos. En seguida se detallan ambos procesos.

2.2.4.1 Proceso EDM03 Asegurar la optimización del riesgo

Este proceso, corresponde con el riesgo de tecnología de información desde la perspectiva de gobierno de TI. El mismo, se describe según (Valencia et al., 2016) como un proceso requerido para asegurar que el apetito y la tolerancia al riesgo de una organización es

entendido, articulado y comunicado y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado.

Así mismo, el propósito del proceso consiste en asegurar que los riesgos relacionados con TI de la empresa no exceden ni el apetito ni la toleración de riesgo, que el impacto de los riesgos de TI en el valor de la empresa se identifica y se gestiona y que el potencial fallo en el cumplimiento se reduce al mínimo (ISACA, 2012).

La guía de referencia de procesos de COBIT 5, sugiere tres prácticas de gobierno para el proceso EDM03. Estas prácticas, se describen en seguida.

EDM03.01 Evaluar la gestión de riesgos

Examinar y evaluar continuamente el efecto del riesgo sobre el uso actual y futuro de las TI en la empresa. Considerar si el apetito de riesgo de la empresa es apropiado y el riesgo sobre el valor de la empresa relacionado con el uso de TI es identificado y gestionado (ISACA, 2012).

EDM03.02 Orientar la gestión de riesgos

Orientar el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que son apropiadas para asegurar que riesgo TI actual no excede el apetito de riesgo del Consejo (ISACA, 2012).

EDM03.03 Supervisar la gestión de riesgos

Supervisar los objetivos y las métricas clave de los procesos de gestión de riesgo y establecer cómo las desviaciones o los problemas serán identificados, seguidos e informados para su resolución (ISACA, 2012).

Con estas tres prácticas de gobierno, se satisface lo que una organización debe considerar para el gobierno de los riesgos relacionados con tecnología de información. Adicionalmente, (ISACA, 2012) indica que el proceso EDM03 se relaciona con otras guías y marcos para riesgos de TI como lo son COSO/ERM e ISO/IEC 31000.

Hay dos términos que resulta importante considerar para las prácticas sugeridas en el proceso EDM03, la tolerancia y el apetito de riesgo. De acuerdo con Alvarado y Zumba, la tolerancia al riesgo es el nivel aceptable de fluctuación del apetito de riesgo que inicialmente ha sido definido para el logro de los objetivos de la entidad. Mientras que el apetito de riesgo es el riesgo que ha sido definido por los administrativos de la entidad como normal dentro

de las operaciones de la misma, es decir, cuánto riesgo está dispuestos a aceptar como un medio para lograr los objetivos (2015).

2.2.4.2 Proceso APO12 Gestionar el riesgo

Con este proceso, COBIT 5 considera el riesgo de la perspectiva de gestión de tecnología de información. Este proceso permite identificar, evaluar y reducir los riesgos de TI de forma continua, dentro de los niveles de tolerancia establecidos por la dirección de la empresa (Valencia et al., 2016).

Según lo indica (ISACA, 2012), el propósito del proceso APO12 consiste en integrar la gestión de riesgos empresariales relacionados con TI con la gestión de riesgos empresarial general (ERM) y equilibrar los costes y beneficios de gestionar riesgos empresariales relacionados con TI.

Para el proceso APO12, la guía de referencia de procesos de OCBIT 5 sugiere seis prácticas de gestión. Cada una de ellas se presenta a continuación de acuerdo con lo que define COBIT 5.

APO12.01 Recopilar datos

Identificar y recopilar datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI (ISACA, 2012).

Según Alvarado y Zumba, la información y el conocimiento constituyen un elemento base para la realización de la gestión de riesgos, […]. Por ello, se considera necesario definir todo respecto a: procesos claves y secundarios, un método apropiado que permita recoger los datos para su posterior clasificación y análisis, datos relevantes sobre el ambiente en el cual se desenvuelve la entidad, información de eventos pasados que causaron problemas y en general datos históricos que sirvan de retroalimentación (2015).

APO12.02 Analizar el riesgo

Desarrollar información útil para soportar las decisiones relacionadas con el riesgo que tomen en cuenta la relevancia para el negocio de los factores de riesgo (ISACA, 2012).

Uno de los objetivos del gobierno es optimizar el riesgo, lo que representa una parte esencial para la creación de valor, […], es por ello, que el riesgo de TI requiere ser visualizado como un riesgo del negocio [y] por tal motivo [se] aspira a una óptima gestión [de] riesgos, la cual le permita a la entidad reconocer y tener conciencia de cuáles son los

riesgos potenciales a los cuales se enfrenta y contrarrestarlos o prevenirlos mediante el planteamiento de estrategias efectivas de gestión evitando pérdidas o daños irreparables que imposibiliten el cumplimiento de los objetivos planteados (Alvarado & Zumba, 2015).

APO12.03 Mantener un perfil de riesgo

Mantener un inventario del riesgo conocido y atributos de riesgo (incluyendo frecuencia esperada, impacto potencial y respuestas) y de otros recursos, capacidades y actividades de control actuales relacionados (ISACA, 2012).

Este proceso de apoya en el proceso EDM03 que permite la definición y comunicación de la tolerancia y el apetito de riesgo en una organización (Alvarado & Zumba, 2015).

APO12.04 Expresar el riesgo

Proporcionar información sobre el estado actual de exposiciones y oportunidades relacionadas con TI de una forma oportuna a todas las partes interesadas necesarias para una respuesta apropiada (ISACA, 2012).

Una oportuna comunicación de los riesgos y la exposición de los activos organizacionales, permite la formulación de un plan de respuesta adecuado. Esto con la colaboración de individuos internos y externos a la organización (Alvarado & Zumba, 2015).

APO12.05 Definir un portafolio de acciones para la gestión de riesgos

Gestionar las oportunidades para reducir el riesgo a un nivel aceptable como un portafolio (ISACA, 2012).

Según Alvarado y Zumba, una vez expresado el riesgo y sus atributos, se puede definir un portafolio con propuestas para enfrentar los riesgos, considerando el nivel de riesgo y siempre priorizando los riesgos para atender aquellos que representen una mayor pérdida o tengan más impacto en la consecución de los objetivos (2015).

APO12.06 Responder al riesgo

Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI (ISACA, 2012).

Luego de analizar el riesgo con base en los niveles de apetito y tolerancia definidos, además de definir el portafolio de acciones, se debe establecer la respuesta que ejecutará la organización si se materializa el riesgo en cuestión (Alvarado & Zumba, 2015). Las

respuesta al riesgo pueden ser: evitar, compartir/transferir, aceptar o mitigar según (Alvarado & Zumba).

Con estas las seis prácticas de gestión presentadas, COBIT 5 abarca los aspectos que cualquier organización debería considerar para una adecuada gestión de los riesgos de TI. Algunas otras guías o marcos que apoyan y complementan lo indicado en el proceso APO12 son ISO/IEC 31000 y la familia ISO/IEC 27000 (ISACA, 2012).

Como complemento a los procesos descritos de COBIT 5, ISACA emitió en el 2013 la guía COBIT 5 para Riesgo, la cual explica en detalle cómo utilizar los principios de COBIT 5 para alcanzar una óptima gestión del riesgo de TI. En una sección posterior se presenta esta guía como uno más de los marcos referenciales utilizados para este trabajo.

2.3 INTE/ISO 31000:2011

Al igual que en el caso de COBIT 5, esta norma se utiliza como referencia pues así lo solicitó la firma Deloitte. No obstate, la norma consiste en el estándar internacional de principios y directrices genéricas para la gestión de riesgo (Instituto de Normas Técnicas de Costa Rica, 2011). Por lo anterior, resulta de gran valor para el desarrollo de este trabajo final de graduación. Así mismo, “esta norma nacional es equivalente a la norma ISO 31000:2009” (INTECO, 2011), por lo que es la versión oficial que se debe utilizar en Costa Rica.

> Aunque esta norma proporciona directrices genéricas, no tiene como objetivo promover la uniformidad en la gestión del riesgo a través de las organizaciones. El diseño y la implementación de planes y marcos de referencia de gestión del riesgo necesitarán tener en cuenta las diversas necesidades de una organización específica, sus objetivos particulares, contexto, estructura, operaciones, procesos, funciones, proyectos, productos, servicios, o activos y prácticas específicas utilizadas (INTECO, 2011).

Según lo indicado por INTECO en el párrafo anterior, esta norma se ajusta a lo planteado como parte de este trabajo de graduación, que pretende generar una metodología que se adapte a distintos tipos de organización. Del mismo modo, INTECO indica que “Esta norma puede utilizarse por cualquier empresa pública, privada o social, asociación, grupo o individuo. Por tanto, esta norma no es específica de una industria o sector” (2011).

El principal objetivo de esta norma, según lo indica (INTECO, 2011), es ser utilizada para los procesos de gestión de riesgo establecidos en distintas normas. Además, se indica que

proporciona un enfoque común en el apoyo de las normas que tratan riesgos y/o sectores específicos sin sustituir dichas normas.

De acuerdo con lo indicado en (Posada & Gómez, 2012), cuando la gestión de riesgos, se implementa y mantiene de acuerdo con la norma ISO 31000, permite entre otros aspectos:

- Mejorar la probabilidad de alcanzar los objetivos.
- Conocer 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.

Esta norma ISO está constituida por tres grandes pilares que son los principios para una gestión eficaz de riesgos, el marco de referencia para que la información de riesgos se utilice en la toma de decisiones y responsabilidades; y el proceso con las actividades que debe contemplar la gestión de riesgos en una organización. La Figura 9 muestra estos tres componentes de la norma y la relación entre ellos.

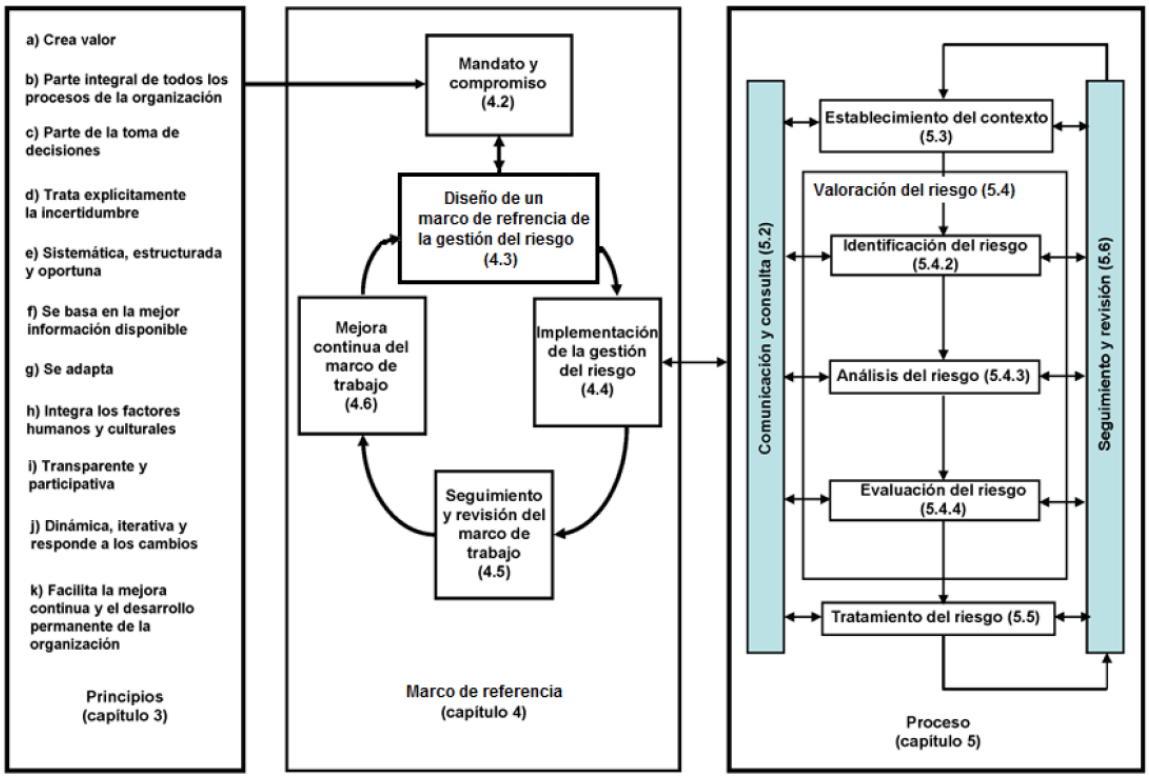


Figura 9. Relación entre los principios, el marco de referencia y el proceso de gestión del riesgo
Fuente: (INTECO, 2011)

En los siguientes apartados, se presentan los principios que indica la norma INTE/ISO 31000:2011 para la gestión de riesgos, así como la descripción del marco de referencia propuesto y el proceso de gestión de riesgos.

2.3.1 Principios

La norma INTE/ISO 31000:2011, presenta 11 principios que las organizaciones deben cumplir en todos sus niveles para alcanzar una gestión de riesgos eficaz. Dichos principios se pueden observar en la primera parte de la Figura 9 y en seguida se define cada uno de los principios de la gestión de riesgo, según se indica en (INTECO, 2011).

La gestión del riesgo crea y protege el valor

“La gestión del riesgo contribuye de manera tangible al logro de los objetivos y a la mejora del desempeño” (INTECO, 2011).

La gestión del riesgo es una parte integral de todos los procesos de la organización

“La gestión del riesgo es parte de las responsabilidades de gestión y una parte integral de todos los procesos de la organización, incluyendo la planificación estratégica y todos los procesos de la gestión de proyectos y de cambios” (INTECO, 2011).

La gestión del riesgo es parte de la toma de decisiones

“La gestión del riesgo ayuda a las personas que toman decisiones a realizar elecciones informadas, a definir las prioridades de las acciones y a distinguir entre planes de acción alternativos” (INTECO, 2011).

La gestión del riesgo trata explícitamente la incertidumbre

“La gestión del riesgo tiene en cuenta explícitamente la incertidumbre, la naturaleza de esa incertidumbre, y la manera en que se puede tratar” (INTECO, 2011).

La gestión del riesgo es sistemática, estructurada y oportuna

“Un enfoque sistemático, oportuno y estructurado de la gestión del riesgo contribuye a la eficacia y a resultados coherentes, comparables y fiables” (INTECO, 2011).

La gestión del riesgo se basa en la mejor información disponible

“Los elementos de entrada del proceso de gestión del riesgo se basan en fuentes de información tales como datos históricos, experiencia, retroalimentación de las partes interesadas, observación, previsiones y juicios de expertos” (INTECO, 2011).

La gestión del riesgo es a la medida

"La gestión del riesgo se alinea con el contexto externo e interno de la organización y con el perfil del riesgo" (INTECO, 2011).

La gestión del riesgo integra los factores humanos y culturales

"La gestión del riesgo permite identificar las aptitudes, las percepciones y las intenciones de las personas externas e internas que pueden facilitar u obstruir el logro de los objetivos de la organización" (INTECO, 2011).

La gestión del riesgo es transparente y participativa

"La implicación apropiada y oportuna de las partes interesadas y, en particular, de las personas que toman decisiones a todos los niveles de la organización, asegura que la gestión del riesgo se mantenga pertinente y actualizada" (INTECO, 2011).

La gestión del riesgo es dinámica, iterativa, y responde a los cambios

> La gestión del riesgo es sensible de manera continuada a los cambios y responde a ellos. Como se producen eventos externos e internos, el contexto y los conocimientos cambian, se realiza el seguimiento y la revisión de riesgos, surgen nuevos riesgos, algunos cambian y otros desaparecen (INTECO, 2011).

La gestión del riesgo facilita la mejora continua de la organización

"Las organizaciones deberían desarrollar e implementar estrategias para mejorar su madurez en la gestión del riesgo en todos los demás aspectos de la organización" (INTECO, 2011).

2.3.2 Marco de referencia

> El éxito de la gestión del riesgo dependerá de la eficacia del marco de referencia de gestión que proporcione las bases y las disposiciones que permitirán su integración a todos los niveles de la organización. El marco de referencia facilita una gestión eficaz del riesgo mediante la aplicación del proceso de gestión del riesgo […] a diferentes niveles y dentro de contextos específicos de la organización (INTECO, 2011).

Este marco de referencia, está diseñado para ayudar a que una organización logre integrar la gestión del riesgo, con su sistema de gestión global (INTECO, 2011). A continuación se describen los cinco componentes del marco de referencia que se observan en la segunda parte de la Figura 9, según lo que se presenta en (INTECO, 2011).

2.3.2.1 Mandato y compromiso

La introducción de la gestión del riesgo y el aseguramiento de su eficacia continua requieren un compromiso fuerte y sostenido de la dirección de la organización, así como el establecimiento de una planificación estratégica y rigurosa para conseguir el compromiso a todos los niveles (INTECO, 2011).

2.3.2.2 Diseño del marco de referencia de la gestión de riesgos

Comprensión de la organización y de su contexto

Antes de iniciar el diseño y la implementación del marco de referencia de la gestión del riesgo, es importante evaluar y entender el contexto externo e interno de la organización, dado que ambos pueden influir significativamente en el diseño del marco de referencia (INTECO, 2011).

Establecimiento de la política de gestión del riesgo

"La política de gestión del riesgo debería indicar claramente los objetivos y el compromiso de la organización en materia de la gestión del riesgo" (INTECO, 2011).

Rendición de cuentas

La organización debería asegurarse de que está establecida la rendición de cuentas, la autoridad y las competencias apropiadas para gestionar el riesgo, incluyendo la implementación y el mantenimiento del proceso de gestión del riesgo y asegurar la idoneidad, la eficacia y la eficiencia de todos los controles (INTECO, 2011).

Integración en los procesos de la organización

La gestión del riesgo debería estar integrada en todas las prácticas y procesos de la organización, de una manera que sea relevante, eficaz y eficiente. El proceso de gestión del riesgo debería formar parte de los procesos de la organización, y no ser independiente de ellos. En particular, la gestión del riesgo debería estar integrada en el desarrollo de la política, en la planificación y revisión estratégicas y de negocio, y en los procesos de gestión de cambios (INTECO, 2011).

Recursos

"La organización debería proporcionar los recursos adecuados para la gestión del riesgo. Se debe considerar: personas, procesos, sistemas, etc." (INTECO, 2011).

Establecimiento de los mecanismos internos de comunicación e información

"La organización debería establecer mecanismos internos de comunicación e información con objeto de apoyar y fomentar la rendición de cuentas y la responsabilidad del riesgo" (INTECO, 2011).

Establecimiento de los mecanismos externos de comunicación y de información

"La organización debería desarrollar e implementar un plan para comunicarse con las partes interesadas externas" (INTECO, 2011).

2.3.2.3 Implementación de la gestión del riesgo

Implementación del marco de referencia de la gestión del riesgo

Para la implementación del marco de referencia de la gestión del riesgo, la organización debería: definir el cronograma y estrategia apropiados para la implementación, aplicar la política y los procesos de gestión de riesgos, organizar sesiones de información, entre otros (INTECO, 2011).

Implementación del proceso de gestión del riesgo

La gestión del riesgo se debería implementar de manera que se asegure que el proceso de gestión del riesgo, se aplica mediante un plan de gestión del riesgo en todos los niveles y funciones relevantes de la organización, como parte de sus prácticas y procesos (INTECO, 2011).

2.3.2.4 Seguimiento y revisión del marco de trabajo

Con objeto de asegurar que la gestión del riesgo es eficaz y contribuye al desempeño de la organización, esta debería: medir el desempeño de la gestión, medir periódicamente el progreso del plan de gestión de riesgos y establecer informes sobre los riesgos, entre otros (INTECO, 2011).

2.3.2.5 Mejora continua del marco de trabajo

Con base en los resultados obtenidos del seguimiento y de las revisiones, se deberían tomar decisiones sobre cómo mejorar el marco de referencia, la política y el plan de gestión del riesgo. Estas decisiones deberían conducir a mejoras en la gestión del riesgo por parte de la organización, así como a mejoras de su cultura de gestión del riesgo (INTECO, 2011).

2.3.3 Proceso

En la tercera parte de la Figura 9 se puede apreciar el proceso de gestión de riesgo sugerido por la norma ISO 31000. El proceso de gestión de riesgos debería ser una parte integral de la gestión, que se integre en la cultura y las prácticas; y se adapte a los procesos de negocio de la organización (INTECO, 2011).

Los apartados siguientes describen las etapas del proceso de gestión de riesgo, según lo indicado en la norma.

2.3.3.1 Comunicación y consulta

Las comunicaciones y las consultas con las partes interesadas externas e internas se deberían realizar en todas las etapas del proceso de gestión del riesgo. Por esto, en una de las primeras etapas se deberían desarrollar planes de comunicación y consulta que traten temas relativos al riesgo en sí mismo, a sus causas, a sus consecuencias y a las medidas para tratarlo (INTECO, 2011).

Se deberían realizar comunicaciones y consultas externas e internas efectivas para asegurarse de que las personas responsables de la implementación del proceso de gestión del riesgo y las partes interesadas comprenden las bases que han servido para tomar decisiones (INTECO, 2011).

Las comunicaciones y consultas con las partes interesadas son importantes, ya que estas pueden emitir juicios sobre el riesgo basados en sus percepciones de riesgo. Estas percepciones pueden variar debido a diferencias en los valores, las necesidades, las hipótesis, los conceptos y las inquietudes de las partes interesadas (INTECO, 2011).

2.3.3.2 Establecimiento del contexto

Según se indica en (INTECO, 2011), “Mediante el establecimiento del contexto, la organización articula sus objetivos, define los parámetros externos e internos a tener en cuenta en la gestión del riesgo, y establece el alcance y los criterios de riesgo para el proceso restante”. Aunque estos aspectos son similares a lo considerado en el marco de referencia, en este punto del proceso debe considerarse la relación con el alcance del proceso particular para la gestión de riesgos (INTECO).

Establecimiento del contexto externo

"El contexto externo es el entorno externo en el cual la organización busca conseguir sus objetivos" (INTECO, 2011).

> La comprensión del contexto externo es importante para asegurarse de que los objetivos e inquietudes de las partes interesadas externas se tienen en cuenta cuando se desarrollan los criterios de riesgo. Este contexto se basa en […] toda la organización, pero con detalles específicos de requisitos legales y reglamentarios, con las percepciones de las partes interesadas y otros aspectos de riesgos específicos del alcance del proceso de gestión del riesgo (INTECO, 2011).

Establecimiento del contexto interno

"El contexto interno es el entorno interno en el cual la organización busca conseguir sus objetivos" (INTECO, 2011).

> El proceso de gestión del riesgo debería alinearse con la cultura, los procesos, la estructura y la estrategia de la organización. El contexto interno lo constituye todo aquello que en el seno de la organización puede influir en la manera en la que una organización gestionará el riesgo (INTECO, 2011).

Establecimiento del contexto del proceso de gestión del riesgo

> Se deberían establecer los objetivos, las estrategias, el alcance y los parámetros de las actividades de la organización, o de aquellas partes de la organización donde será aplicado el proceso de gestión del riesgo. La gestión del riesgo debería ser emprendida teniendo en cuenta todo lo necesario para justificar los recursos que se han de utilizar para llevarla a cabo la gestión del riesgo. También se deberían especificar los recursos requeridos, las responsabilidades y autoridades, y los registros que se deben conservar (INTECO, 2011).

Definición de los criterios de riesgo

> La organización debería definir los criterios que se aplican para evaluar la importancia del riesgo. Los criterios deberían reflejar los valores, los objetivos y los recursos de la organización. Algunos criterios pueden estar impuestos o derivarse de requisitos legales o reglamentarios, o de otros requisitos suscritos por la organización. Los criterios de riesgo deberían ser coherentes con la política de gestión del riesgo de la

> organización […], definidos al comienzo de cualquier proceso de gestión del riesgo, y revisados continuamente (INTECO, 2011).

2.3.3.3 Valoración del riesgo

"La valoración del riesgo es el proceso global de identificación, de análisis y de evaluación del riesgo" (INTECO, 2011).

Identificación del riesgo

Según se indica en (INTECO, 2011), se debe identificar las fuentes de riesgo y áreas de impacto, así como los eventos con sus causas y consecuencias. El objetivo de esta etapa es crear una lista de riesgos exhaustiva, lo cual, es crítico pues un riesgo no identificado será omitido en las posteriores etapas del análisis.

Además de identificar los eventos de riesgo que podría ocurrir, es necesario considerar un amplio rango de escenarios y consecuencias, así como los efectos en cadena o acumulativos. Adicionalmente, se debe considerar las posibles causas que ocasionen el evento de riesgo, aunque dichas causas no sean evidentes o no estén bajo el control de la organización (INTECO, 2011).

> La organización debería aplicar herramientas y técnicas de identificación del riesgo que se adapten a sus objetivos y aptitudes, así como a los riesgos a los que está expuesta. Para la identificación de los riesgos es esencial disponer de información relevante y actualizada. Siempre que sea posible, esta información debería ir acompañada de antecedentes apropiados. En la identificación de los riesgos deberían intervenir personas con conocimientos apropiados (INTECO, 2011).

Análisis del riesgo

De acuerdo con lo que se indica en (INTECO, 2011), en esta etapa se realiza una comprensión del riesgo. El análisis de riesgo genera insumos para la evaluar el riesgo y tomar decisiones sobre el tratamiento de los mismos, así como las estrategias y métodos más apropiados.

El riesgo se analiza considerando la posibilidad o **probabilidad** de las causas, así como las consecuencias y su **afectación** a diferentes objetivos de la organización. También se deben considerar los **controles** existentes y su eficacia. La forma en que se expresan y combinan estos elementos para determinar un **nivel de riesgo**, debería corresponder al tipo de riesgo,

a la información disponible y al objetivo de la valoración del riesgo. Todos estos datos deberían ser coherentes con los criterios de riesgo establecidos y se debe considerar la interdependencia de los diferentes riesgos y de sus fuentes (INTECO, 2011).

Factores como diferencias de opinión entre expertos, la incertidumbre, la disponibilidad, la calidad, la cantidad y la validez de la información; se deberían considerar en el análisis y comunicar de manera eficaz a quienes se encarguen de tomar decisiones y a otras partes interesadas. El nivel de detalle del análisis, dependerá del riesgo, de la finalidad del análisis y de la información disponible (INTECO, 2011).

El análisis puede ser cualitativo, semi-cuantitativo, cuantitativo, o una combinación de estos, dependiendo de las circunstancias. Las consecuencias se pueden expresar en términos de impactos tangibles o intangibles. En algunos casos, se requiere más de un valor numérico o descriptor para especificar las consecuencias y su posibilidad para diferentes escenarios (INTECO, 2011).

Evaluación del riesgo

Una vez realizado el análisis, la evaluación del riesgo pretende ayudar a la toma de decisiones, determinando los riesgos a tratar y la prioridad para implementar el tratamiento. En esta fase se debe comparar el nivel de riesgo con los criterios del Establecimiento del contexto. Con base en dicha comparación, se determina la necesidad o no de realizar el tratamiento de un riesgo (INTECO, 2011).

Para la toma de decisiones se debería tener en cuenta el contexto más amplio del riesgo y considerar la tolerancia al riesgo de terceros interesados. Las decisiones, además, deben cumplir con requisitos legales y reglamentarios entre otros. La decisión puede ser realizar un análisis en mayor profundidad o no tratar el riesgo y mantener únicamente los controles existentes. La toma de decisiones estará influenciada por la actitud ante el riesgo en la organización y por los criterios de riesgo establecidos (INTECO, 2011).

2.3.3.4 Tratamiento del riesgo

Según lo indicado en (INTECO, 2011), en esta fase se realiza la selección e implementación de una o varias opciones para tratar el riesgo, lo que brinda o modifica los controles para dicho riesgo. La Figura 10 muestra el proceso cíclico para el tratamiento de riesgos que propone esta norma ISO.

Las opciones para el tratamiento de riesgos no son excluyentes entre sí y pueden incluir evitar el riesgo no realizando alguna actividad, aceptar o aumentar el riesgo, eliminar la fuente del riesgo, modificar la posibilidad o las consecuencias, compartir el riesgo o retener el mismo mediate una decisión informada (INTECO, 2011).

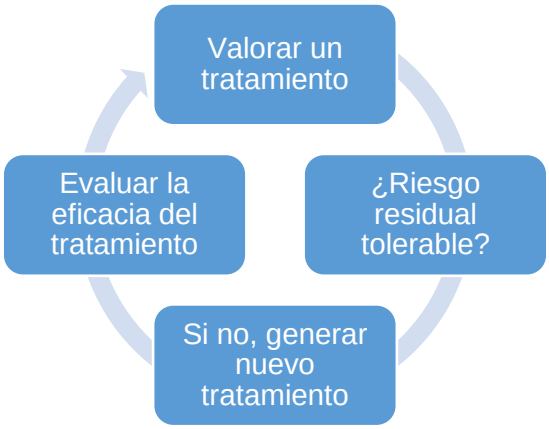


Figura 10. Ciclo de tratamiento de riesgo
Fuente: Elaboración propia con base en (INTECO, 2011)

Así mismo, en (INTECO, 2011), se describe una serie de actividades para el tratamiento de riesgo. A continuación, se muestran dichas descripciones.

Selección de opciones de tratamiento de riesgo

"La selección de la opción más apropiada de tratamiento del riesgo implica obtener una compensación de los costos y los esfuerzos […] en función de los beneficios […], teniendo en cuenta los requisitos legales, reglamentarios y otros" (INTECO, 2011).

Puede resultar beneficiosa la implementación de varias opciones conjuntamente. En la selección, se debe considerar los valores de las partes interesadas. Del mismo modo, cuando una opción pueda impactar en otra parte de la organización o de las partes interesadas, se debe involucrar a las mismas en la decisión. Algunos tratamientos pueden ser igual de eficaces, pero más o menos aceptables que otros por sus efectos secundarios (INTECO, 2011).

El plan de tratamiento debería identificar con claridad el orden de prioridad en que se deberían implementar los tratamientos de riesgo individuales. Además de considerar como parte del mismo plan original, aquellos riesgos que pudieran surgir como consecuencia de los tratamientos aplicados (INTECO, 2011).

Preparación e implementación de los planes de tratamiento de riesgo

De acuerdo con (INTECO, 2011), el objetivo de un plan de tratamiento de riesgo, consiste en documentar la forma de implementar el tratamiento seleccionado. Para ello, el plan debe proporcionar las razones de la selección, los responsables de aprobación e implementación del plan, las acciones propuestas, la necesidad de recursos, las medidas de desempeño, los requisitos de información, la programación, entre otros.

> Los planes de tratamiento deberían integrarse en los procesos de gestión de la organización y discutirse con las partes interesadas apropiadas. Las personas que toman decisiones y las otras partes interesadas deberían estar enteradas de la naturaleza y amplitud del riesgo residual (INTECO, 2011).

2.3.3.5 Seguimiento y revisión

"El seguimiento y la revisión deberían planificarse en el proceso de tratamiento del riesgo y someterse a una verificación o una vigilancia regular. Esta verificación o vigilancia puede ser periódica o *ad hoc*" (INTECO, 2011). Además, las responsabilidades de seguimiento y revisión deberían estar claramente definidas y que el seguimiento debe abarcar todos los aspectos del proceso de gestión de riesgo (INTECO).

Según (INTECO, 2011), el avance en la implementación de los planes de tratamiento representa una medida de su funcionamiento y los resultados del seguimiento y revisión, deben documentarse en informes internos y externos según corresponda. Y al mismo tiempo, funcionar como insumos para revisar el Marco de referencia.

2.4 COBIT 5 para Riesgos

De acuerdo con lo indicado por (Alvarado & Zumba, 2015), COBIT 5 para Riesgos permite un mejor entendimiento de cómo los riesgos de TI impactan en una organización. Estas autoras describen el marco como una guía de extremo a extremo para la forma de gestionar los riesgos de TI.

COBIT 5 para Riesgos, se basa en el marco COBIT 5 enfocándose en el tema de riesgos y proveyendo una guía más detallada y práctica para los profesionales de riesgos y otras partes interesadas en todos los niveles de la organización (ISACA, 2013).

Según (ISACA, 2013), esta guía incrementa las capacidades organizacionales relacionadas con riesgos de TI con beneficios como la identificación más acertada de riesgos y medición

de la eficacia en la gestión de los mismos, un mejor entendimiento del impacto, conocimiento sobre inversiones en gestión de riesgos de TI, facilidades de integración con la gestión de riesgos organizacional, mejor comunicación en toda la empresa y un perfil de riesgo completo para una mejor utilización de recursos.

COBIT 5 para Riesgos “Provee una guía de alto nivel en cómo identificar, analizar y responder a los riesgos utilizando procesos de COBIT 5 y con el uso de escenarios de riesgo” (Peña & Rico, 2013).

Esta guía se basa en los principios de COBIT 5, sus catalizadores y la cascada de metas son la plataforma para identificar, analizar, responder y comunicar el riesgo a las partes interesadas (Alvarado & Zumba, 2015). Adicionalmente, COBIT 5 para Riesgos presenta los principios para la gestión de riesgos como puede observarse en la Figura 11.

Figura 11. Principios de la Gestión de Riesgos
Fuente: (ISACA, 2013)

COBIT 5 para Riesgos define dos perspectivas en relación con el riesgo de TI, la Función del Riesgo y la Gestión del Riesgo (Alvarado & Zumba, 2015). La primera de ellas describe los catalizadores de COBIT 5 que son necesarios para construir y mantener una adecuada función de riesgo en las organizaciones. La segunda como el proceso principal de gestión

de riesgo: identificar, analizar y responder al riesgo; puede ser apoyado por los catalizadores de COBIT 5 (ISACA, 2013).

La Figura 12 muestra estas dos perspectivas presentadas por COBIT 5 para Riesgos. Mientras que la Figura 13 presenta el alcance de dicha guía.

Figura 12. Las dos perspectivas del riesgo
Fuente: (ISACA, 2013)

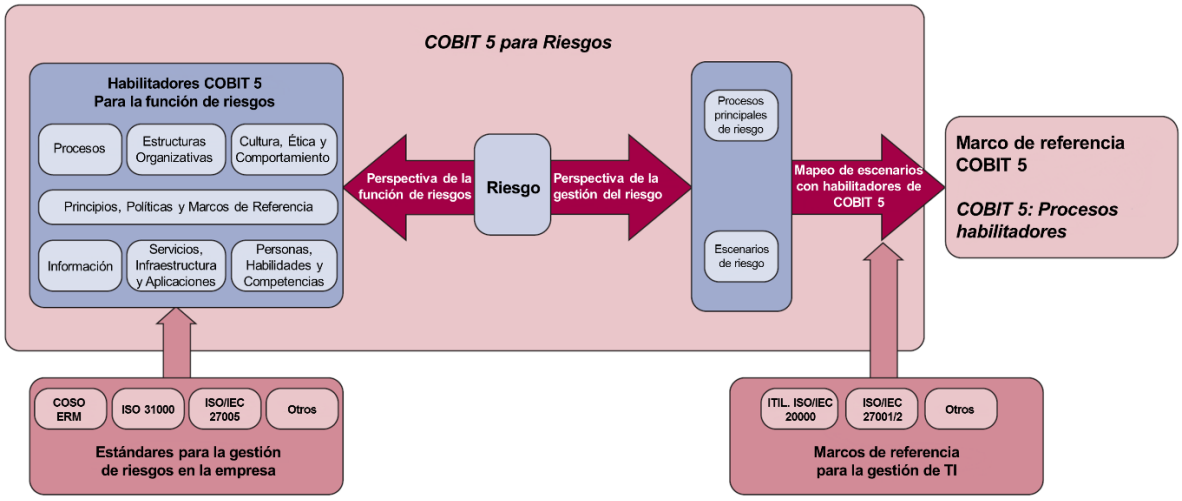


Figura 13. Alcance de COBIT 5 para Riesgos
Fuente: (ISACA, 2013)

Esta guía se enfoca en aplicar los procesos de COBIT 5 a la gestión de riesgos, provee una guía de alto nivel sobre cómo identificar, analizar y responder al riesgo mediante la aplicación de los procesos COBIT 5 y el uso de escenarios de riesgo; se alinea con marcos de referencia en la industria y provee un enlace entre los escenarios de riesgo y los catalizadores de COBIT 5 (ISACA, 2013).

A continuación, se describen las dos perspectivas de riesgo que presenta la guía COBIT 5 para Riesgos.

2.4.1 Perspectiva de la Función de Riesgo

En esta perspectiva, COBIT 5 para Riesgos, describe cómo los catalizadores de COBIT 5 pueden ser aplicados en situaciones prácticas para la implementación de un gobierno de riesgos y una gestión de riesgos efectivas y eficientes (ISACA, 2013).

En otra definición, se dice que esta perspectiva "describe lo que se necesita en una empresa para construir y sostener actividades efectivas de gobierno y gestión de riesgos" (Peña & Rico, 2013).

La Tabla 7 resume las principales anotaciones que presenta el marco COBIT 5 para Riesgos sobre la aplicación de los catalizadores de COBIT 5 para establecer y mantener la función de riesgos.

Tabla 7. Catalizadores de COBIT 5 en la Función de Riesgo

Catalizador	Enfoque en Riesgos
Principios, Políticas y Marcos de referencia.	Los principios de riesgo mostrados en la Figura 11, proveen un enfoque sistemático y estructurado para la gestión de riesgos, contribuyendo a la obtención de resultados consistentes y confiables. Los principios de riesgo formalizan y estandarizan la implementación de políticas de riesgo. Las políticas ofrecen una guía más detallada de cómo poner en práctica los Principios y cómo estos influencian la toma de decisiones. No todas las políticas deben estar a cargo de la Función de riesgos, dependiendo de la organización pueden estar en otras dependencias o incluidas en otras políticas organizacionales. Algunas políticas mencionadas por el marco son: • Política principal de riesgo. • Política de seguridad de información. • Política de continuidad de negocio. • Política de administración de proyectos. • Políticas de RRHH. • Políticas de cumplimiento. • Política de control interno. • Política de privacidad de los datos.

Catalizador	Enfoque en Riesgos
Procesos.	Los dos procesos principales para el gobierno y la gestión de riesgos: EDM03 y APO12, se consideran en la Perspectiva de gestión de riesgo. Adicionalmente, hay otros procesos que soportan la Función de riesgos. • EDM01. El gobierno y la gestión de riesgos requieren un marco de gobierno adecuado. • EDM02. Para gestionar e valor que genera la función de riesgos. • EDM05. La función de riesgo requiere medidas de rendimiento transparentes y aprobadas. • APO02. La estrategia de riesgos debe estar definida y alineada con la estrategia organizacional. • APO06. Presupuesto para la función de riesgos. • APO07. La gestión de riesgos requiere personas, habilidades y experiencia. • APO08. Se debe mantener la relación entre la función de riesgos y el negocio. • APO11. La calidad es parte importante en la gestión de riesgos. • BAI08. La función de riesgo requiere conocimiento para soportar sus actividades. • MEA01. El riesgo es un punto clave en el monitoreo y evaluación del negocio y de TI. • MEA02. El control interno es fundamental en la prevención de riesgos. • MEA03. El cumplimiento de leyes, regulaciones y contratos supone riesgos.
Estructuras organizativas.	El marco presenta las estructuras o roles principales para el gobierno y gestión de riesgos, en un modelo de tres líneas de defensa. Primera línea de defensa: • Operaciones. Los gerentes de operación son los primeros dueños de la gestión de riesgos. • Grupo empresarial de riesgo. Este grupo considera y analiza el riesgo en mayor detalle y asesora al Comité de Gestión de Riesgo Empresarial.

Catalizador	Enfoque en Riesgos
	Segunda línea de defensa: • Función de riesgo. Unidad responsable y que rinde cuentas de la gestión de riesgos en toda la empresa. Se puede establecer una filial de esta función en TI. • Departamento de cumplimiento. Responsable del riesgo relacionado con regulaciones, directrices legales y políticas/estándares internos. Tercera línea de defensa: • Auditoría interna. Unidad responsable de identificar riesgos asociados con la brecha en los controles establecidos. De manera trasversal en la segunda y tercera líneas de defensa, se ubica el Comité de Gestión del Riesgo Empresarial. El grupo de ejecutivos de negocio responsable por crear consenso y colaboración en toda la empresa. Dicha colaboración es necesaria para soportar las actividades y decisiones de gestión de riesgo. Un Consejo de riesgos de TI puede asesorar a este Comité.
Cultura, Ética y Comportamiento.	La guía presenta los aspectos de comportamiento y cultura deseados para alcanzar una gestión de riesgo eficaz y eficiente. Estos se agrupan en tres niveles: Comportamiento general: • Cultura consciente del riesgo. • Políticas definidas y comunicadas que orientan el comportamiento. • Reconocer la importancia del riesgo. • El negocio acepta la propiedad del riesgo. • Se permite la aceptación de riesgos como una opción válida. Comportamiento de los profesionales de riesgo: • Esfuerzo por entender las implicaciones de riesgo para cada interesado y cómo se impacta a sus objetivos. • Crear conciencia y entendimiento de la política de riesgos. • Colaboración y comunicación bidireccional durante la evaluación de riesgos. • El apetito de riesgo está claro y es comunicado. • Las políticas reflejan el apetito y la tolerancia. • La cultura empresarial apoya las prácticas de riesgo.

Catalizador	Enfoque en Riesgos
	• Se usan indicadores de riesgo como alerta temprana y se actúa cuando caen fuera del apetito y la tolerancia de riesgo. Comportamiento de la administración: • Los gerentes demuestran apoyo genuino a las prácticas de riesgo. • La administración se compromete con los interesados para acordar acciones y dar seguimiento a los planes. • Se asignan recursos a ejecutar las acciones. • Se alinea las políticas y acciones con el apetito de riesgo. • Se monitorea el riesgo y los planes de acción proactivamente. • Se premia la gestión efectiva de riesgos.

Información.	Se listan loa ítems de información necesarios para establecer y mantener el gobierno y la gestión de riesgos.
	
	• Perfil de riesgo.
	  ○ Registro de riesgos.
	  ▪ Escenarios de riesgo.
	  ▪ Resultados del análisis de riesgos.
	  ○ Plan de acción de riesgos.
	  ○ Eventos de pérdida.
	  ○ Factores de riesgo.
	  ○ Hallazgos de auditoría.
	• Plan de comunicación de riesgo.
	• Reporte de riesgos.
	• Programa de concientización en riesgos.
	• Mapa de riesgos.
	• Universo de riesgos.
	• Apetito de riesgo.
	• Tolerancia de riesgo.
	• Indicadores clave de riesgos.
	• Asuntos emergentes de riesgos.
	• Taxonomía de riesgos.
	• Reporte de Análisis de Impacto de Negocio.
	• Eventos de riesgo.
	• Matriz de controles y actividades de riesgo.
	• Proceso de identificación y evaluación de riesgos.

Catalizador	Enfoque en Riesgos
Servicios, Infraestructura y Aplicaciones.	El marco describe los servicios, infraestructura y aplicaciones que el proceso de gestión de riesgo debe proveer. Servicios: • Asesoría en riesgo de proyectos/programas. • Gestión de incidentes. • Asesoría en arquitectura. • Inteligencia de riesgo. • Gestión de riesgo. • Gestión de crisis. Infraestructura: • Datos de riesgo. • Repositorios de conocimiento. • Arquitectura para integración de conocimiento. Aplicaciones: • Herramientas de gobierno, riesgo y cumplimiento. • Herramientas de análisis. • Reporte/comunicación de herramientas para riesgo. • Repositorios de conocimiento. • Herramientas de continuidad del negocio.
Personas, Habilidades y Competencias.	La guía de ISACA presenta las competencias necesarias para soportar la función de riesgo. • Habilidades de liderazgo. • Capacidad analítica. • Pensamiento crítico. • Capacidades interpersonales. • Comunicación. • Influencia/persuasión. • Pensamiento “fuera de la caja”. • Entendimiento técnico. • Conciencia organizacional y del negocio. • Experiencia en riesgos. • Capacitación y entrenamiento.

Fuente: Elaboración propia con base en (ISACA, 2013)

2.4.2 Perspectiva de la Gestión de Riesgo

En esta segunda perspectiva, se presentan los procesos centrales para la gestión de riesgos que aparecen en COBIT 5. Además, se trata el tema de escenarios de riesgo y la respuesta al riesgo con base en los catalizadores de COBIT (ISACA, 2013).

Vista según (Peña & Rico, 2013), esta perspectiva describe como los procesos *core* de gestión de riesgos que son identificación, análisis y respuesta de riesgos; pueden ser apoyados con los habilitadores de COBIT 5.

2.4.2.1 Procesos principales para riesgos

Los procesos principales que ofrece el marco COBIT 5 para el gobierno de riesgos y para la gestión de riesgos son el Proceso EDM03 Asegurar la optimización del riesgo y el Proceso APO12 Gestionar el riesgo, respectivamente (ISACA, 2013).

Estos procesos fueron contemplados anteriormente en el apartado Estructura de COBIT 5, en este mismo documento. COBIT 5 para Riesgos, presenta una guía para el gobierno y la gestión eficaz del riesgo, asumiendo para ello que los procesos EDM03 y APO12 se encuentran implementados en la organización (ISACA, 2013).

2.4.2.2 Escenarios de riesgo

Durante la implementación del proceso APO12, un elemento de información clave son los escenarios de riesgo. Los mismos son la representación tangible y medible de la ocurrencia y el impacto de un riesgo (ISACA, 2013).

Un escenario de riesgo es la descripción de un posible evento que, al ocurrir, tendrá un impacto incierto en el logro de los objetivos del negocio. Mantener escenarios de riesgo bien diseñados soporta la identificación, análisis y respuesta a riesgos (ISACA, 2013). La Figura 14 presenta una vista de alto nivel sobre los escenarios de riesgo.

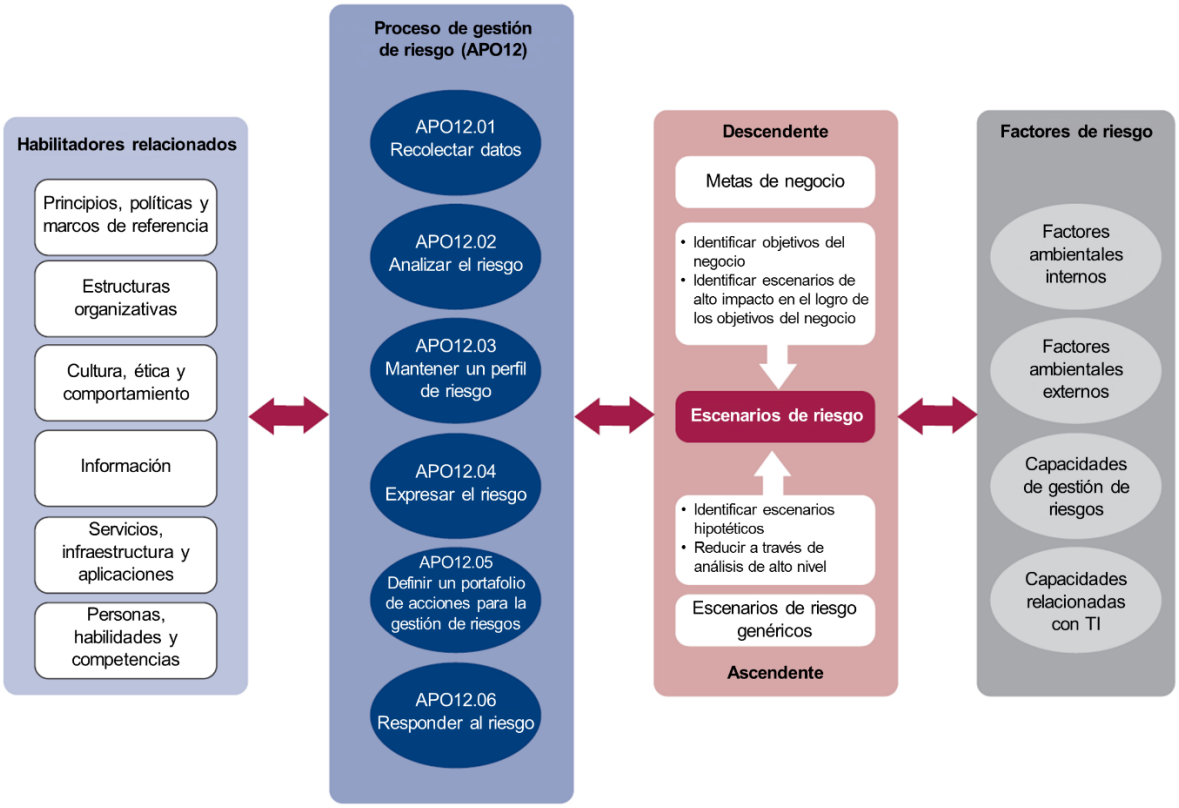


Figura 14. Resumen escenarios de riesgo
Fuente: (ISACA, 2013)

Desarrollando escenarios de riesgo

De acuerdo con (ISACA, 2013), hay dos enfoques para el desarrollo de escenarios de riesgo, enfoques complementarios que las organizaciones deben combinar para obtener el mejor resultado. Dichos enfoques se pueden observar en la Figura 14.

El enfoque descendente o *top-down* inicia con las metas y objetivos del negocio. Posteriormente, se debe llevar a cabo el análisis de los riesgos de TI más probables y relevantes que podrían afectar el cumplimiento de los objetivos del negocio. El enfoque ascendente o *bottom-up* consiste en utilizar escenarios genéricos definidos previamente tratando de identificar los más relevantes para cada organización (ISACA, 2013).

Factores de riesgo

Los factores de riesgo son aquellas condiciones que pueden influenciar la probabilidad y el impacto de los escenarios de riesgo. Dichos factores pueden ser clasificados en dos grandes categorías, factores contextuales y factores de capacidad (ISACA, 2013). La Figura 15 presenta los factores de riesgo incluidos en COBIT 5 para Riesgos.

Figura 15. Factores de riesgo
Fuente: (ISACA, 2013)

Estructura de un escenario de riesgo de TI

Un escenario de riesgo de TI, es una descripción de los eventos relacionados con TI que podrían desencadenar un impacto en el negocio. Para que un escenario de riesgo sea completo y usable para la toma de decisiones, debe contener al menos el actor, el tipo de amenaza, el evento, los activos o recursos y la información de tiempo (ISACA, 2013).

En seguida, la Figura 16 resume la estructura de los escenarios de riesgo.

Figura 16. Estructura de un escenario de riesgo
Fuente: (ISACA, 2013)

2.4.2.3 Respuesta a riesgos

El propósito de definir una respuesta a los riesgos, es acercar el nivel de riesgo al apetito de riesgo definido en la organización. Cuando se establece una respuesta, el principal objetivo es reducir el nivel de riesgo residual hasta que quede en los límites de la tolerancia de riesgo (ISACA, 2013).

Para llevar a cabo este proceso, se requiere conocer tres parámetros clave. En seguida se describe cada uno de ellos según lo presentado en COBIT 5 para Riesgos.

Apetito de riesgo

Es la cantidad de riesgo que, a nivel directivo, una organización está dispuesta a aceptar en búsqueda de sus objetivos (ISACA, 2013).

Tolerancia al riesgo

Es el nivel de variación aceptable que la gerencia está dispuesta a permitir para un riesgo en particular cuando permita alcanzar un objetivo (ISACA, 2013).

Capacidad de riesgo

Es la cantidad de pérdidas que se puede soportar sin poner en riesgo la continuidad o existencia de la organización (ISACA, 2013).

La guía detallada de las actividades de respuesta al riesgo, se puede encontrar en las prácticas EDM03.02 y APO12.02. Por su parte, la evaluación de respuestas de riesgo, no es un esfuerzo único, sino que forma parte del ciclo de gestión de riesgo. Una vez identificados los escenarios se debe analizar el riesgo versus los posibles beneficios de cada uno. Cuando el nivel de riesgo no se ajuste a los parámetros de apetito y tolerancia establecidos, se debe generar una respuesta al riesgo (ISACA, 2013). La Figura 17 presenta el flujo de actividades de respuesta al riesgo.

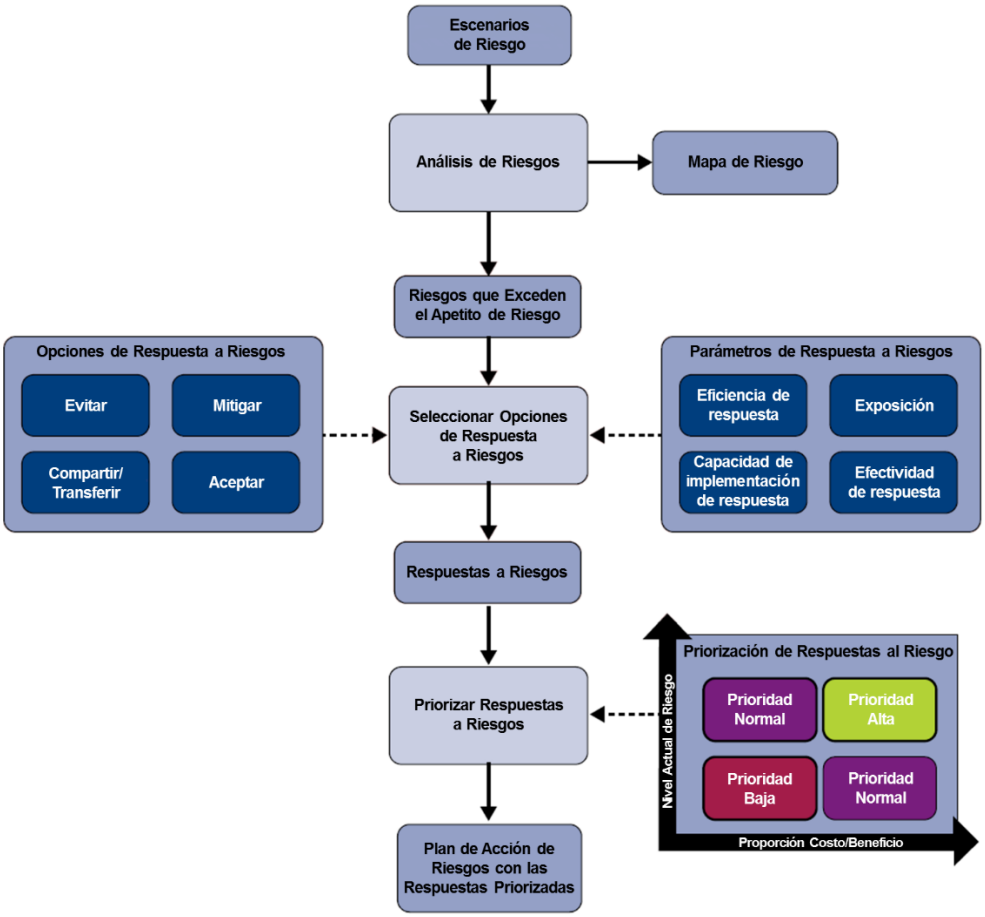


Figura 17. Flujo de actividades de respuesta a riesgos
Fuente: (ISACA, 2013)

2.4.2.3.1 Opciones de respuesta a riesgos

De acuerdo con (ISACA, 2013), las opciones de respuesta al riesgo que las organizaciones deben analizar son las siguientes:

Evitar el riesgo

Consiste en no realizar las actividades que dan espacio al riesgo. Aplica cuando ninguna otra respuesta al riesgo es adecuada. Por ejemplo, cuando las posibles respuestas no son costo efectivas o la exposición al riesgo es demasiado inaceptable para el negocio (ISACA, 2013).

Aceptar el riesgo

La exposición a pérdidas es reconocida y aceptada. No se toma acción alguna para atender un riesgo específico y las pérdidas serán aceptadas cuando ocurran. La decisión de aceptar un riesgo corresponde a los altos niveles de la organización y debe quedar documentada y ser comunicada (ISACA, 2013).

Compartir/transferir el riesgo

Significa reducir la probabilidad o el impacto de un riesgo transfiriendo o compartiendo una parte del riesgo con otra entidad. Algunas técnicas comunes son la adquisición de pólizas de seguro o bien, tercerizar las operaciones o proyectos que implican riesgos relevantes (ISACA, 2013).

Mitigar el riesgo

Se refiere a tomar acciones de mitigación para reducir le frecuencia o el impacto de un riesgo. Formas comunes de mitigación incluyen reforzar los procesos de gestión de TI, implementar controles con ayuda de COBIT 5 o utilizar otras prácticas conocidas y marcos de referencia (ISACA, 2013).

2.4.2.3.2 Selección y priorización de respuesta

Una vez identificados los riesgos ante los que la organización debe responder, se debe seleccionar y priorizar las estrategias para responder al riesgo (ISACA, 2013). Dichas estrategias se deben seleccionar de las opciones de respuesta al riesgo mencionadas en el apartado anterior. Este proceso se puede observar en la Figura 17.

Para llevar a cabo este proceso se debe tomar en cuenta algunos parámetros importantes. De acuerdo con (ISACA, 2013), se debe considerar:

- Eficiencia de la respuesta. Se puede comparar con otras respuestas.
- Exposición o posición del riesgo atendido en el mapa de riesgos.
- Capacidad de la organización para implementar la respuesta.
- Efectividad de la respuesta, cómo reducirá el nivel del riesgo.

La suma de esfuerzos necesarios para implementar la respuesta a un riesgo, puede exceder las capacidades de la organización. Por ello, utilizando los mismos criterios para la selección de las respuestas, estas se deben priorizar y ubicarse en uno de tres niveles de prioridad como se puede ver en la Figura 17 (ISACA, 2013).

- Prioridad alta. Respuestas efectivas y muy eficientes en costo ante riesgos altos.
- Prioridad normal. Respuestas costosas o difíciles ante riesgos altos o respuestas efectivas ante riesgos de menor nivel.
- Prioridad baja. Respuestas a riesgos bajos y que pueden no ser efectivas.

COBIT 5 para Riesgos, ilustra con ejemplos y casos todos los conceptos que han sido mencionados en este resumen. Para conocer más sobre dicha guía o ampliar en algún tema específico, se puede consultar el material oficial de ISACA.

En la sección siguiente se hace referencia a otros marcos y regulaciones que se debe considerar en la gestión de riesgos de TI.

2.5 Otros marcos, prácticas y regulaciones

Gran cantidad de marcos y prácticas, así como diferentes investigaciones y trabajos académicos, discuten el tema de riesgos y riesgos de TI. En dicho material se proponen métodos y herramientas diversas para llevar a cabo una adecuada gestión de los riesgos de TI en las organizaciones. Aunque este Trabajo Final de Graduación se basa fundamentalmente en COBIT 5 e ISO 31000, resulta importante conocer otras perspectivas que complementan el conocimiento en el campo.

Esta sección presenta de manera resumida, una serie de marcos y regulaciones adicionales que complementan el marco de conocimiento considerado para el presente trabajo. Se resume, en la opinión de distintos autores, lo presentado por la norma ISO 27005, así como los marcos OCTAVE, MAGERIT y COSO. También se presenta un resumen de normas nacionales emitidas por la Superintendencia General de entidades Financieras.

Otros trabajos académicos, tesis y artículos de investigación se consideran de manera trasversal en todo este capítulo. Lo anterior, pues dichos trabajos hacen referencia y amplían lo indicado en los marcos que han sido considerados en este marco teórico.

2.5.1 ISO/IEC 27005

De acuerdo con (Vanegas, 2013), esta norma pertenece a la familia de normas ISO 27000 y proporciona las directrices para la gestión de riesgos de seguridad de la información apoyándose para ello, en un sistema de gestión de seguridad de la información. Este autor continúa indicando que la norma no establece un método específico para la gestión de dichos riesgos, sino que depende de cada organización definir un enfoque apropiado (Vanegas, 2013).

“El estándar […] contiene la descripción de los procesos y actividades de la administración de riesgos de seguridad informática. Este estándar […] está diseñado para apoyar la implementación satisfactoria de esquemas de seguridad de la información en el enfoque de la administración de riesgos” (Posada & Gómez, 2012).

El procedimiento presentado por esta norma es similar al analizado previamente en la sección INTE/ISO 31000:2011. Según (Vanegas, 2013) este procedimiento consiste en establecer el contexto, evaluar el riesgo, tratar el riesgo, si el tratamiento fue efectivo entonces aceptar el riesgo residual y finalmente, comunicar el riesgo y efectuar la revisión y monitoreo; estos dos últimos aspectos, llevados a cabo de manera transversal durante todo el proceso.

La Figura 18 presenta el proceso de gestión de riesgos indicado por esta norma.

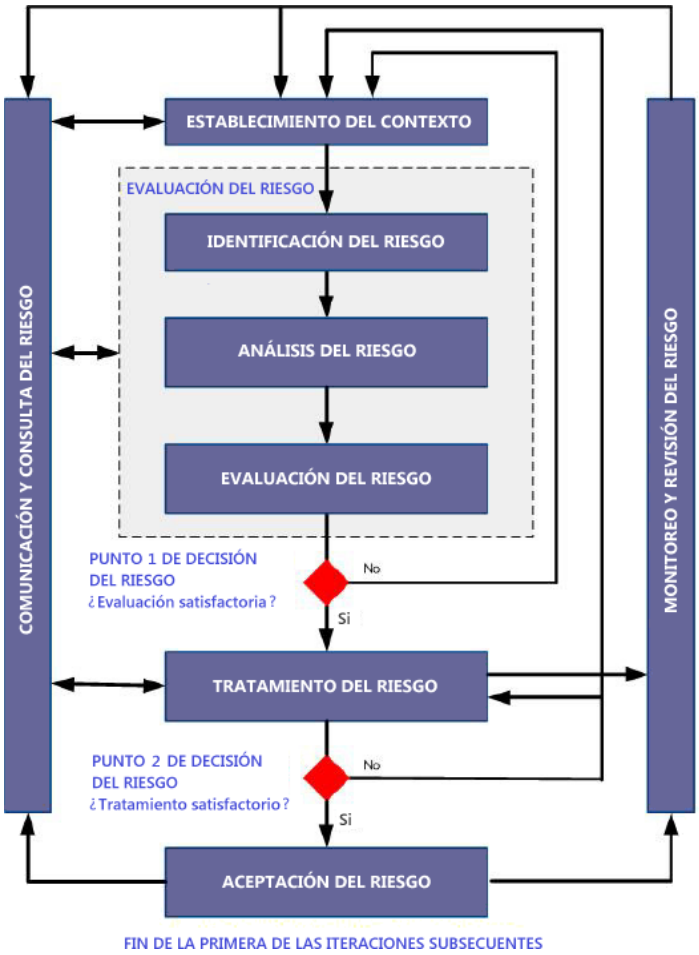


Figura 18. Proceso de gestión de riesgos de ISO 27005
Fuente: (Posada & Gómez, 2012)

2.5.2 OCTAVE

Esta es una metodología que mejora la toma de decisiones estableciendo un conjunto de herramientas, técnicas y métodos de información con base en los riesgos. Está diseñada con un enfoque auto dirigido, donde los usuarios pueden aprender y mejorar la postura de seguridad de la organización sin depender de expertos o proveedores (Vanegas, 2013).

Según (Peña J. Á., 2010) OCTAVE u *Operational Critical Threat, Asset and Vulnerability Evaluation*, es una metodología de análisis de riesgos de seguridad de TI. Metodología enfocada en que la organización sea capaz de:

- Dirigir y gestionar sus evaluaciones de riesgos.
- Tomar decisiones con base en sus riesgos.
- Proteger los activos clave de información.
- Comunicar de forma efectiva la información clave de seguridad.

Así mismo, se indica que los principales beneficios de este marco consisten en que identifica riesgos que pueden impedir la consecución de objetivos, enseña a evaluar los riesgos de seguridad de la información, crea una estrategia para reducir los riesgos de seguridad prioritarios y ayuda al cumplimiento de regulaciones (Peña J. Á., 2010).

La Figura 19 presenta las fases de la metodología OCTAVE.

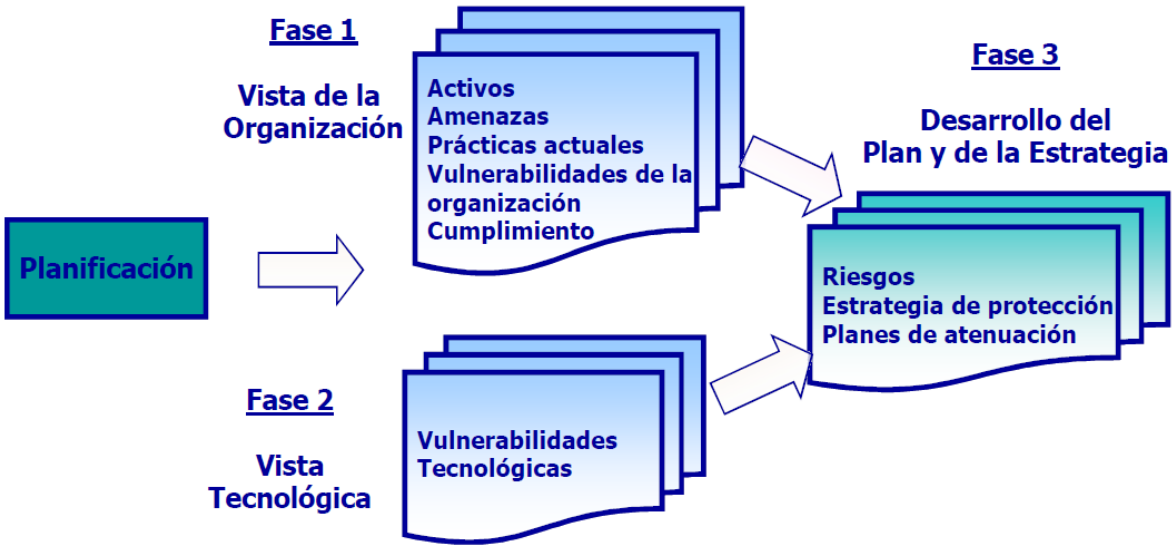


Figura 19. Fases de OCTAVE
Fuente: (Peña J. Á., 2010)

2.5.3 MAGERIT

La Metodología de Análisis y Gestión de Riesgos de TI es un referente de uso obligatorio para las entidades públicas de España (Posada & Gómez, 2012). Sin embargo, se recomienda su uso en todo tipo de organizaciones (Peña J. Á., 2010).

Los objetivos de esta metodología, son crear conciencia de la existencia de riesgos de TI y de la necesidad de tratarlos, ofrecer un método sistemático para el análisis de riesgos y ayudar en la planificación de medidas oportunas para controlar los riesgos (Posada & Gómez, 2012; Vanegas, 2013).

MAGERIT consta de tres volúmenes complementarios: Método, Catálogo de elementos y Guía de técnicas (Peña, 2010; Posada & Gómez, 2012; Vanegas, 2013). El primero detalla la metodología a implementar, el segundo presenta una serie de elementos genéricos para facilitar el proceso y el tercero constituye una guía con técnicas para la gestión y análisis de riesgos (Posada & Gómez, 2012; Vanegas, 2013).

De acuerdo con Peña J, Á., esta metodología consta de cuatro fases: Planificación del proyecto de riesgos, Análisis de riesgos, Gestión de riesgos y Selección de salvaguardas (2010). Una nueva versión de la metodología publicada en el año 2012, se alinea con los objetivos y el proceso de la norma ISO 31000. Contemplando la asignación de roles y funciones, el establecimiento del contexto, criterio para determinar los riesgos, evaluación de los riesgos, tratamiento de riesgos, aceptación del riesgo, comunicación y consulta, y seguimiento y revisión (Vanegas, 2013).

2.5.4 COSO

COSO (Committee of Sponsoring Organization) es un marco integrador que se puede aplicar dentro de cualquier organización indistintamente de sus características, ya que le brinda la opción de obtener mejores resultados relacionando los procesos, personas y estructuras, logrando así un mejor desempeño de la entidad y una adecuada supervisión de sus actividades (Alvarado & Zumba, 2015).

De acuerdo con Alvarado & Zumba, el marco COSO se ha convertido en una herramienta utilizada por la gerencia de miles de empresas alrededor del mundo (2015). Y su misión brinda liderazgo intelectual y orientación sobre la gestión de riesgo, control interno y disuasión del fraude (Galaz, Yamazaki, Ruiz Urquiza, S.C., 2015).

COSO establece cinco componentes del control interno que agrupan 17 principios en representación de conceptos fundamentales para el establecimiento de un efectivo Sistema de Control Interno. El segundo de esos cinco componentes es la Evaluación de Riesgos y según se indica en (Galaz, Yamazaki, Ruiz Urquiza, S.C., 2015), alberga los siguientes cuatro principios:

- La organización especifica objetivos con suficiente claridad para permitir la identificación y valoración de los riesgos relacionados a los objetivos.
- La organización identifica los riesgos sobre el cumplimiento de los objetivos, a través de la entidad y los analiza para determinar cómo esos riesgos deben administrarse.
- La organización considera la posibilidad de fraude en la evaluación de riesgos para el logro de los objetivos.
- La organización identifica y evalúa los cambios que pueden impactar significativamente al sistema de control interno.

> La *evaluación de riesgos* se considera un proceso dinámico, en el que varias personas interactúan para definir los riesgos tanto internos como externos a los cuales se expone la entidad y puede afectar la consecución de sus objetivos ya sean estos de operación, información o de cumplimiento (Alvarado & Zumba, 2015).

En dicho proceso, los involucrados deben conocer de manera integral la empresa para identificar sus puntos débiles. Conociendo dichas debilidades, se analizan sus causas y se procede con la evaluación del riesgo considerando el impacto y la probabilidad (Alvarado & Zumba, 2015).

2.5.5 Regulaciones emitidas por SUGEF

La Superintendencia General de Entidades Financieras de Costa Rica (SUGEF) tiene como objetivo:

> Velar por la estabilidad, la solidez y el funcionamiento eficiente del sistema financiero nacional, con estricto apego a las disposiciones legales y reglamentarias y de conformidad con las normas, directrices y resoluciones que dicte la propia institución, todo en salvaguarda del interés de la colectividad (Superintendencia General de Entidades Financieras, s.f.).

SUGEF emite normativas que son de acatamiento obligatorio para las entidades que regula esta institución, muchas de las cuales, son o podrán ser clientes de la firma Deloitte. Por ello, se resumen las tres normativas más relevantes para el tema de este trabajo.

2.5.5.1 SUGEF 2-10

Este acuerdo, denominado Reglamento sobre la Administración Integral del Riesgo, establece los principales aspectos de un proceso de gestión de riesgos alineado con la estrategia de negocio, su perfil de riesgo y el tamaño de sus operaciones. Este proceso contempla la identificación, medición, monitoreo, control, mitigación y comunicación de los riesgos (Acuerdo SUGEF 2-10, 2016).

Esta norma consta de siete capítulos donde describe la estructura organizacional requerida para la gestión de riesgos, contemplando un comité de riesgos y una unidad encargada de riesgos. Así mismo indica cuál es la función del gobierno corporativo en la administración integral del riesgo y dicta las pautas para la auditoría e informes de riesgo que debe realizar la organización (Acuerdo SUGEF 2-10, 2016).

2.5.5.2 SUGEF 18-16

El Reglamento sobre la Gestión del Riesgo Operativo establece los aspectos principales que las organizaciones deben observar en relación con la gestión de riesgos. Incluye políticas y procesos adecuados para identificar, cuantificar, evaluar, vigilar, informar y controlar o mitigar el riesgo operativo oportunamente (Acuerdo SUGEF 18-16, 2016).

Este reglamento indica que el riesgo operativo es un tema trasversal y que no compete únicamente a un área de la organización. El Acuerdo consta de tres capítulos los cuales contemplan la estrategia, las políticas y el proceso necesario para la gestión del riesgo operativo, incluyendo riesgos de continuidad del negocio, de seguridad de la información y de tecnologías de la información (Acuerdo SUGEF 18-16, 2016).

2.5.5.3 SUGEF 14-17

El Acuerdo 14-17 “Reglamento sobre la Gestión de Tecnología de Información”, vigente a partir de mayo 2017, es un reglamento homologado para las cuatro superintendencias de Costa Rica, la de entidades financieras, la de pensiones, la del mercado de valores y la de seguros. El reglamento fue emitido en respuesta a la creciente dependencia de las organizaciones hacia la TI y las amenazas y vulnerabilidades derivadas de este hecho.

El reglamento, indica que la gestión de riesgos de TI debe implementarse en entidades, siguiendo las mejores prácticas y estándares internacionales. Por tanto, las entidades deben declarar en su marco de gestión de TI, los procesos de TI que, por su naturaleza, complejidad y nivel de operaciones, le sean aplicables; entre ellos los procesos de riesgo. Por tratarse de buenas prácticas reconocidas en este tema, este Reglamento deja espacio abierto para que las entidades implementen marcos y estándares como COBIT 5, ISO, ITIL y PMBOK (SUGEF, 2017).

Este reglamento consta de cuatro capítulos a través de los cuales trata los objetivos de la gestión de TI y el marco de gestión que deben implementar las entidades para cubrir los riesgos operativos y tecnológicos que por la naturaleza del sistema financiero se deben controlar. Presenta la figura de la auditoría externa de TI, donde descansarán las superintendencias para que realicen evaluaciones basadas en riesgos y dictaminen la situación actual de los procesos de TI en las entidades. Así mismo, deja abierta la selección del marco para la gestión de seguridad de la información y el uso de servicios en la nube (SUGEF, 2017).

Desarrollo Metodológico

3 Desarrollo Metodológico

El marco metodológico, es el procedimiento que se sigue para lograr algo, la forma en que se realiza una investigación. Este marco, hace referencia al conjunto de técnicas e instrumentos a emplear en la recolección de datos necesarios para producir conocimiento (Casasola, 2015).

El presente capítulo, define el tipo de investigación de este trabajo final de graduación y el procedimiento metodológico utilizado para el desarrollo del mismo. Además, se incluyen las fuentes y sujetos de información, los instrumentos y técnicas para la recolección de datos, el procedimiento de análisis de dichos datos y las herramientas que apoyan el desarrollo de la propuesta de solución.

3.1 Tipo de investigación

"La **investigación** es un conjunto de procesos sistemáticos, críticos y empíricos que se aplican al estudio de un fenómeno o problema" (Hernández, Fernández, & Baptista, 2014). Así mismo, existen dos enfoques básicos de investigación: el cuantitativo y el cualitativo; además del enfoque mixto que consiste en una combinación de los dos primeros (Arias, Cuevas, León & Vasconcelos, 2012; Creswell, 2014; Hernández et al., 2014).

Para el desarrollo de este trabajo, se utiliza un enfoque cualitativo, en el cual, según Hernández et al., el proceso de investigación se mueve de manera dinámica entre los hechos y su interpretación, ocasionando que la secuencia de actividades sea distinta en cada investigación (2014). La Figura 20 representa una aproximación al proceso de investigación cualitativa.

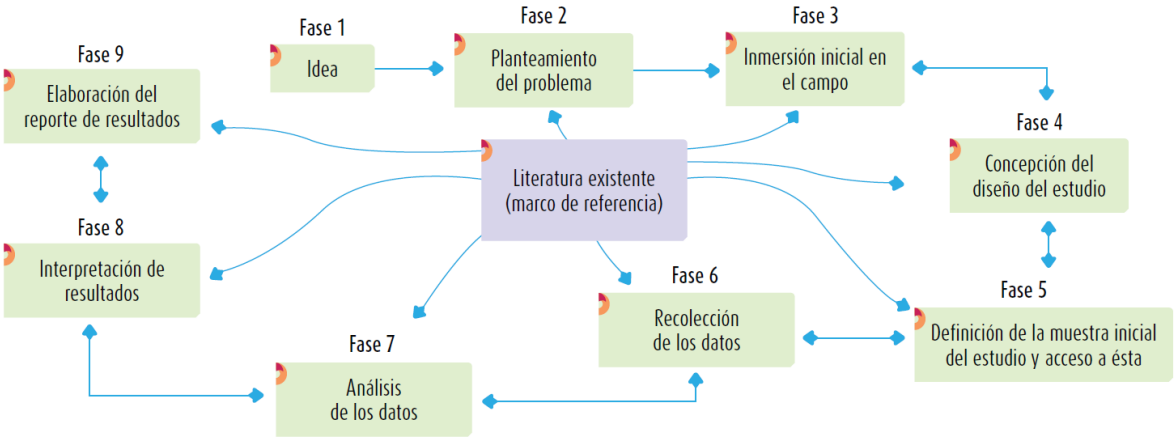


Figura 20. Proceso de investigación cualitativa
Fuente: (Hernández et al., 2014)

El enfoque de investigación cualitativo, explora en profundidad los fenómenos, afinando planteamientos abiertos durante el proceso. Los significados, en este enfoque, se extraen de los datos y el proceso se conduce principalmente en ambientes naturales, buscando conocer en detalle una realidad subjetiva, sin fundamentarse en el análisis estadístico (Hernández et al., 2014).

Según se menciona en (Abarca, Alpízar, Rojas, & Sibaja, 2012), aunque comúnmente se define la investigación cualitativa como todo aquello que no es cuantitativo, algunos autores defienden que la investigación cualitativa es un fenómeno empírico definido por su propia historia. “La metodología cualitativa se ocupa principalmente de las relaciones entre las personas en la sociedad: lo que producen, piensan, dicen y lo que hacen frente y con los demás” (Abarca et al., 2012).

La investigación cualitativa estudia aquello que produce datos descriptivos, como las palabras de la gente o la conducta observable (Taylor & Bogdan, 1996, citado en Abarca et al., 2012). Este enfoque de investigación, según Ruiz, busca la comprensión subjetiva y las percepciones de la gente, de los símbolos y de los objetos, capturando significados particulares atribuidos por los propios protagonistas y contemplando los elementos como piezas de un sistema (1999, citado en Abarca et al., 2012).

Algunas características del enfoque cualitativo presentadas por (Hernández et al., 2014) son las siguientes:

- Durante el proceso, se requiere regresar a etapas previas. El proceso aproximado se puede ver en la Figura 20.
- La definición de la muestra, así como la recolección y el análisis de datos, son etapas que se desarrollan de manera prácticamente simultánea.
- Se sigue un proceso inductivo de exploración, descripción y generación de perspectivas teóricas.
- Utiliza métodos de recolección de datos no estandarizados. No se realiza un análisis estadístico de los datos.

Del mismo modo, en (Abarca et al., 2012), se mencionan algunas características del enfoque cualitativo como se muestra a continuación:

- Utiliza múltiples métodos, busca validar la información de forma compleja, flexible e interactiva.
- Captura la información de manera flexible y desestructurada.
- Utiliza una lógica inductiva y un diseño de investigación flexible.
- Analiza a las personas y al escenario de investigación bajo una perspectiva holística.

En la siguiente sección, se define el diseño o método utilizado para llevar a cabo este trabajo final de graduación.

3.1.1 Diseño o método de la investigación

Como parte del enfoque cualitativo de investigación, se debe definir el diseño o abordaje de la investigación. Para esto, según Hernández et al., se debe decidir el abordaje de la investigación durante el trabajo de campo, es decir, durante la recolección y el análisis de datos (2014).

“La naturaleza de las cuestiones de investigación guía y orienta el proceso de indagación y, por tanto, la elección de unos métodos y otros” (Rodríguez, 1996, citado en Rojas, 2008). En este mismo sentido, Hernández et al., indican que cada estudio cualitativo es un diseño en sí mismo, que no hay dos investigaciones cualitativas iguales (2014). Las investigaciones cualitativas son “piezas artesanales del conocimiento, hechas a mano, a la medida de las circunstancias” (Hernández et al.).

Por otra parte en (Rojas, 2008), se dice que los métodos estructurales de investigación cualitativa son la forma característica de investigar, determinada por la intención sustantiva. Además, se indica que “el método brinda la posibilidad de aprehender un conocimiento a través de un procedimiento riguroso, sistemático y crítico” (Rojas).

Según se indica en (Hernández et al., 2014; Rojas, 2008), existen diferentes métodos o diseños genéricos para la investigación cualitativa, siendo los principales de ellos: teoría fundamentada, hermenéutico dialéctico, etnográficos, narrativos, fenomenológicos, investigación-acción, historias de vida y estudios de caso cualitativos.

Para este trabajo final de graduación se ha seleccionado el diseño de investigación-acción cuya finalidad es comprender y resolver problemáticas específicas de un grupo, organización o comunidad mediante la aplicación de teoría y mejores prácticas (Hernández et al., 2014). Este diseño genera insumos para la toma de decisiones para proyectos y

reformas estructurales. Pretende propiciar el cambio social, transformar la realidad y generar conciencia en las personas sobre su papel en dicha transformación (Hernández et al., 2014).

Una característica fundamental de este método es que los sujetos investigados son coinvestigadores que participan activamente pues la investigación es algo que les afecta y les interesa en profundidad (Rojas, 2008). “La investigación acción es unan forma de investigación llevada a cabo por parte de los prácticos sobre sus propias prácticas” (Kemmis, 1998, citado en Rojas, 2008). Así mismo, para Hernández et al., el diseño de investigación-acción implica la colaboración comprometida de los participantes en la detección de necesidades y su involucramiento con la estructura y el proceso a mejorar, las prácticas por cambiar y la implementación de los resultados del estudio (2014).

Las fases esenciales en los diseños de investigación acción son observar, pensar y actuar (Stringer, 1999, en Hernández et al., 2014). Sin embargo, Kurt Lewin quien es conocido como el padre de la investigación-acción (Martínez 1997, en Rojas, 2008), planteó en 1948 el ciclo presentado en la Figura 21.

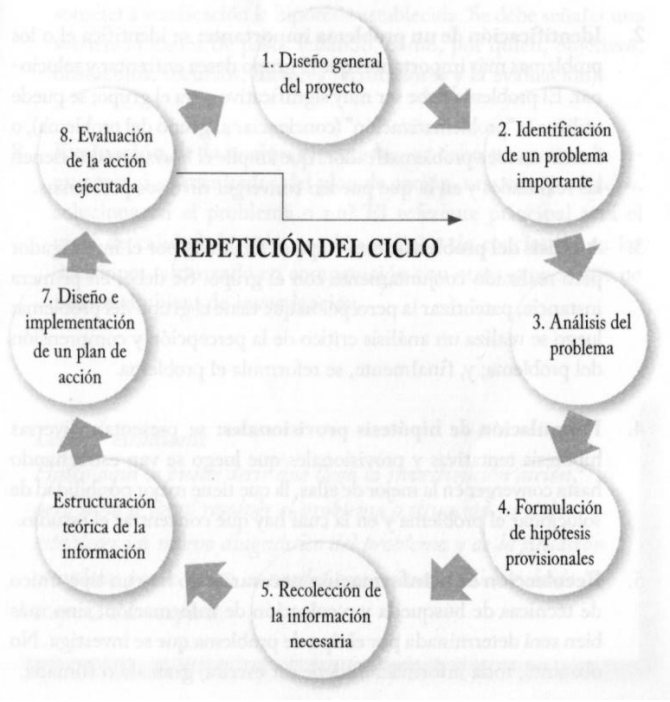


Figura 21. Etapas de la investigación-acción según Kurt Lewin
Fuente: (Rojas, 2008)

Esta investigación, por tratarse de un trabajo final de graduación que debe cumplir con requisitos de tiempo y alcance, se limita a una iteración del proceso de investigación-acción. El procedimiento específico para este trabajo se detalla más adelante en este mismo capítulo.

Existen distintos diseños o modalidades del método de investigación-acción (Hernández et al., 2014; Rojas, 2008). De ellos, la investigación-acción cooperativa o participativa, es la que mejor se adecua a este trabajo. En esta los participantes se relacionan durante todo el proceso con los datos y fungen como coinvestigadores (Hernández et al., 2014). Es "cuando algunos miembros de dos o más instituciones relacionadas deciden agruparse para resolver juntos problemas que atañen a la práctica profesional de una de las instituciones" (Rojas, 2008).

> La palabra 'participativa' le proporciona el rasgo característico a este diseño. En efecto, la problemática es identificada en conjunto por la comunidad y los investigadores. Se considera a los miembros de la comunidad como expertos en la misma, por tal motivo sus 'voces' resultan esenciales para el planteamiento y las soluciones (Hernández et al., 2014).

Algunos de los principios propuestos por estos autores para la investigación-acción participativa son:

- Cooperación y confianza entre los actores involucrados.
- El contexto es fundamental.
- El resultado debe impactar favorablemente a la población.
- Empoderar a los miembros de la comunidad.

3.2 Unidad de muestreo o análisis

La unidad de muestreo es el objeto de estudio de la investigación, en otras palabras, "los participantes, objetos, sucesos o colectividades de estudio […], lo cual depende del planteamiento […] de la investigación" (Hernández et al., 2014).

Siendo así, para este trabajo final de graduación se define como unidad de análisis al personal de Deloitte Centroamérica y República Dominicana del área de *Risk Advisory*. Así mismo, se considera como unidad de muestreo, al personal de organizaciones clientes de Deloitte.

Se aplicarán, a esta unidad de análisis, distintas técnicas y herramientas de investigación cualitativa para conocer el estado actual de y propiciar la generación de la Propuesta de Metodología para la gestión de riesgos de TI.

Según se indica en (Hernández et al., 2014), cuando se ha definido la unidad de muestreo para la investigación, se debe proceder a delimitar la población que va a ser estudiada. La siguiente sección, presenta la población establecida para este trabajo.

3.3 Población

La población, es el conjunto de todos los casos que concuerdan con una serie de especificaciones (Lepkowski, 2008, mencionado en Hernández et al., 2014).

Para este trabajo de graduación, la población es entonces el conjunto de colaboradores (consultores y gerentes) de Deloitte *Risk Advisory* ubicados en Costa Rica, que estén o hayan estado involucrados (como implementadores o como encargados) en proyectos donde se implemente o haya implementado el proceso de gestión de riesgos de TI, ya sea en su totalidad o una parte del mismo.

Por otra parte, se contemplan los encargados del proceso de gestión de riesgos de TI en organizaciones clientes de Deloitte ubicados en Costa Rica a las cuales se les esté brindando, o se les pueda brindar en el corto plazo, servicios que incluyan el proceso de gestión de riesgos de TI.

En ambos casos, los individuos contemplados deben tener conocimiento sobre gestión de tecnologías de información y sobre gestión de riesgos.

Para este trabajo de investigación cualitativa, no resulta estrictamente necesario definir una muestra estadística que permita generalizar resultados a la población analizada (Hernández et al., 2014). Al tratarse de una investigación cualitativa, el objetivo es más bien, comprender el proceso de gestión de riesgos de TI en la población y generar una propuesta de cambio en el mismo a través de los resultados de dicha investigación. No se busca generalizar ningún tipo de resultado mediante técnicas estadísticas, numéricas o similares.

3.4 Fuentes de información

Para el desarrollo de este trabajo se utilizan diversas fuentes de información, tanto para el estudio de la problemática en la organización, como para generar la Propuesta de Metodología para la gestión de riesgos de TI.

A continuación, se presentan las distintas fuentes de información contempladas para el desarrollo de este trabajo final de graduación.

3.4.1 Fuentes de información primarias

Las fuentes de información primarias para este trabajo son las siguientes:

- El Marco COBIT 5 y sus diferentes guías oficiales publicadas por ISACA.
- La norma INTE/ISO 31000:2011 y otras normas relacionadas con la gestión de riesgos y la gestión de tecnología de información.
- Documentación de proyectos realizados por Deloitte sobre la gestión de riesgos de TI.
- Tesis y publicaciones académicas sobre gestión de riesgos de tecnología de información.
- Libros sobre metodología de la investigación e investigación cualitativa.

3.4.2 Fuentes de información secundarias

Por otra parte, las fuentes secundarias de información definidas para el desarrollo de este trabajo de graduación son las siguientes:

- Repositorios de publicaciones académicas y trabajos de graduación de diferentes Universidades e instituciones, públicas o privadas, de educación superior.
- Sistema de Bibliotecas del Instituto Tecnológico de Costa Rica (SIBITEC) y su respectivo catálogo en línea.
- Bases de conocimiento, globales y locales, de la firma Deloitte.
- Libros y revistas en formato físico o electrónico.
- Páginas de internet y blogs.

3.5 Sujetos de información

Como parte del proceso de investigación para el presente trabajo, se requiere la participación de diferentes colaboradores de Deloitte, así como de individuos clave en

algunas organizaciones clientes de esta firma. Lo anterior resulta de importancia tanto durante la recolección de información, como en el momento de generar la Propuesta de Metodología para la gestión de riesgos de TI. La Tabla 8 describe los diferentes sujetos de información contemplados como parte del trabajo final de graduación.

Tabla 8. Sujetos de información

Rol / Organización	Información
Gerentes de *Risk Advisory* – Deloitte.	Información sobre la necesidad y las razones de implementar este proyecto, así como sobre el contexto en la organización y los beneficios de establecer una metodología estandarizada para los proyectos de gestión de riesgos de TI. Brindarán información relevante para la construcción y validación de las herramientas utilizadas en el proyecto, así como para la propuesta de solución. Poseen la experiencia necesaria en la implementación y dirección de proyectos relacionados con la gestión de riesgos de TI, para brindar esta información. Conocen las necesidades y requerimientos de la industria y de los clientes de la Firma en el tema de gestión de riesgos de TI, así como las tendencias y regulaciones que atañen a las organizaciones en este sentido. Se encargarán además de brindar realimentación sobre el desarrollo del proyecto y sobre la Propuesta de Metodología en desarrollo.
Consultores senior de *Risk Advisory* – Deloitte.	Conocen la necesidad de una herramienta que soporte el desarrollo de proyectos relacionados con la gestión de riesgos de TI debido a que son quienes implementan dichos proyectos y deben realizar investigaciones o levantar procesos en cada uno de ellos. Constituyen una fuente importante de información en este trabajo pues, la Metodología que se genere les traerá beneficios directos en sus labores.

Rol / Organización	Información
	Poseen información detallada sobre proyectos anteriores por lo que pueden describir las prácticas utilizadas en dichos proyectos y facilitar información relevante al respecto. Trabajan hombro a hombro con los clientes de Deloitte en el desarrollo de proyectos relacionados con la gestión de riesgos de TI. Por ello, conocen las condiciones existentes en dichas organizaciones que podrían guiar aspectos importantes en el desarrollo de la Propuesta de Metodología.
Encargados de gestión de riesgos de TI, de control interno de TI, de la seguridad de la información o de riesgo empresarial – Organizaciones clientes de Deloitte.	Brindarán datos importantes sobre los insumos y condiciones disponibles en las organizaciones que son o pueden ser clientes de Deloitte. Esta información permitirá analizar la viabilidad de implementación de la Metodología para la Gestión de Riesgos de TI resultante de este trabajo. Estos individuos son aptos para brindar la información ya que, en sus labores diarias, conocen la realidad de cada organización en relación con los insumos necesarios para una adecuada gestión del riesgo tecnológico.

Fuente: Elaboración propia

Para recopilar la información mencionada, se utilizará una serie de métodos cualitativos, los cuales se describen en la siguiente sección.

3.6 Recopilación de datos

Para el desarrollo de este trabajo final de graduación y de la Propuesta de metodología para la gestión de riesgos de TI, se utilizará una serie de métodos propuestos en la literatura para la recolección de datos cualitativos. En esta sección, se describen dichos métodos de acuerdo con lo indicado por diferentes autores con el objetivo de tener una perspectiva general y amplia de cada uno.

Es importante anotar que, para la construcción de las herramientas de recolección de datos, así como para la documentación del trabajo final de graduación, se utilizarán las

herramientas de Microsoft Office 2016 o Microsoft Office 365. Para el envío de cuestionarios a los involucrados se utilizará un gestor de encuestas digitales como Google Forms, Survey Monkey, o bien, alguna de las herramientas que utiliza Deloitte para la aplicación de este tipo de instrumentos en sus labores cotidianas.

Les métodos de recopilación de información se presentan en seguida agrupados de acuerdo con los objetivos específicos de este trabajo final de graduación.

3.6.1 Prácticas utilizadas por Deloitte

Estos métodos de recolección de datos, permitirán conocer las prácticas que ha utilizado Deloitte en proyectos anteriores, así como la experiencia adquirida por el personal en dichos proyectos.

3.6.1.1 Observación documental

Observar, en la investigación cualitativa no se refiere únicamente a la acción de ver (sentido de la vista), sino que abarca todos los sentidos e implica adentrarse profundamente en las situaciones manteniendo un papel activo (Hernández et al., 2014). Según estos autores, el investigador debe prestar atención a los detalles, suceso, eventos e interacciones. Así mismo, indicen que los propósitos esenciales de la observación consisten en explorar y describir ambientes, comprender procesos, identificar problemas y generar hipótesis para futuros estudios.

La observación generalizada, como actividad de la vida cotidiana, “puede transformarse en una poderosa herramienta de investigación […] si se efectúa: orientándola y enfocándola a un objetivo concreto de investigación” (Ruiz & Ispizua, 1989, citados en Rojas, 2008). Por lo anterior, esta autora concluye que “La observación es un proceso deliberado y sistemático que ha de estar orientado a una pregunta, propósito o problema” (Rojas, 2008).

Además, “es un procedimiento para la recopilación de datos de la realidad utilizando los sentidos en un contexto real” y se puede observar “todo el ambiente donde las personas desarrollan su vida: físico, cultural, social, personal etcétera” (Ander-Egg, 1999, citado en Abarca et al., 2012).

Por otra parte en (Creswell, 2014), se indica que un investigador puede recolectar “documentos cualitativos”, que pueden ser reportes, minutas, anotaciones o correos entre

otros. Este autor también indica que, por tratarse de información escrita, se ahorra tiempo y se conoce el lenguaje de los involucrados en la investigación.

En este trabajo final de graduación se realizará una lectura/observación de los reportes o informes correspondientes con proyectos anteriores donde se haya contemplado el tema de gestión de riesgos de TI. Para la aplicación de este método, se utilizará el instrumento incluido en el Apéndice A.

3.6.1.2 Entrevistas

Una vez analizados los documentos de proyectos anteriores, se debe obtener la opinión del personal que ha participado en dichos proyectos. El método seleccionado para este fin es la entrevista, definida por Hernández et al., como “una reunión para conversar e intercambiar información entre una persona (el entrevistador) y otra (el entrevistado) u otras (entrevistados)” (2014).

Así mismo, la entrevista cualitativa incluye preguntas no estructuradas y usualmente abiertas que buscan obtener opiniones e información de los participantes (Creswell, 2014). Abarca et al. indican que la entrevista hace referencia a la interacción entre dos o más personas donde una funge como entrevistadora (2012). La entrevista “es una conversación que tiene una estructura y un propósito” (Álvarez-Gayou, 2003, citado en Abarca et al.).

De los distintos tipos de entrevistas, las informales, las abiertas, las no estructuradas y las estandarizadas/estructuradas pero abiertas, se consideran entrevistas cualitativas (Rojas, 2008). En este trabajo final de graduación se utilizará la entrevista semiestructurada. En este tipo de entrevistas, no todas las preguntas se encuentran predefinidas y aunque se basa en un guion, el entrevistador puede agregar preguntas adicionales o solicitar información adicional (Hernández et al., 2014).

La herramienta definida para la aplicación de este método se encuentra disponible en el Apéndice B.

3.6.2 Mejores prácticas sobre riesgos de TI

Los métodos de esta segunda parte, permitirán conocer y validar las mejores prácticas y marcos de referencia para la gestión de riesgos de TI.

En primera instancia, la identificación y análisis de mejores prácticas se da mediante la revisión de literatura documentada en el marco teórico de este documento y descrita como parte del proceso investigativo en el apartado 3.7.3. Adicionalmente, se realizará un grupo focal para que los representantes de Deloitte validen la inclusión o adaptación de las prácticas identificadas como parte de la Propuesta de Metodología para la gestión de riesgos de TI. Este último método se describe a continuación.

3.6.2.1 Grupo focal

Hernández et al., definen un grupo de enfoque o grupo focal como una reunión con un grupo de personas que conversan en profundidad sobre uno o varios temas específicos en un entorno informal y relajado con la guía de un experto (2014). Según estos autores, los grupos focales se utilizan como método de recopilación de información para la investigación cualitativa, en diversas disciplinas. Su objetivo principal, es generar interacciones entre los participantes y evaluar o analizar dicha interacción además de generar información y conocimiento de manera grupal (Hernández et al.).

La aplicación de este método, se limita a analizar un tema o un número reducido de estos. El moderador debe encargarse de que los demás participantes no se desvíen del conjunto de temas establecido. Así mismo, los detalles logísticos y de organización como el tiempo disponible, el propósito de la sesión y las reglas de participación, se definen previamente y se prepara una guía para la discusión.

Utilizar esta técnica en el desarrollo de este trabajo final de graduación responde al cumplimiento de dos de sus objetivos específicos pues posee un propósito dual. En primera instancia, servirá para validar con los representantes de la organización, el resultado de la revisión literaria efectuada sobre las mejores prácticas, estándares, marcos y normativas aplicables a la gestión de riesgos de TI. Además, pretende la generación conjunta de la Propuesta de metodología, pues los participantes indicarán cuáles aspectos de la literatura analizada son aplicables o no a la solución esperada y se les presentará una propuesta para su validación y para que generen observaciones.

La guía desarrollada para el grupo focal se puede consultar en el Apéndice C.

3.6.3 Propuesta de Metodología

Finalmente, los métodos descritos en este apartado permitirán satisfacer el tercer objetivo específico del trabajo, ayudando a generar la Propuesta de Metodología.

El primer método a utilizar es el grupo focal descrito anteriormente, el cual tiene un doble propósito según se indica en el apartado 3.6.2.1. La aplicación de este método, permitirá dar forma a la propuesta con la ayuda de los interesados de la empresa. Durante la sesión se presentará un borrador de la propuesta de metodología, con el objetivo de que los participantes den su opinión al respecto, hagan cambios o mejoras y de esta forma crear conjuntamente la base para la propuesta de solución final.

Se aplicará un cuestionario para conocer la situación en las empresas clientes de Deloitte donde se ejecutarían proyectos que utilizarán la metodología resultante de este trabajo. A continuación, se describe dicha herramienta.

3.6.3.1 Cuestionario

El cuestionario, es “el conjunto de preguntas que se utilizan para interrogar a la gente sobre asuntos muy variados” (Abarca et al., 2012). Según estos autores, en la literatura se hace referencia al término “cuestionario de la investigación cualitativa” para hacer diferenciación con el instrumento encuesta que se utiliza en la investigación cuantitativa.

Abarca et al., también indican que es posible distinguir cuestionarios abiertos, cerrados y mixtos en los cuales se incluyen preguntas cerradas, abiertas o una combinación de ambas, según las necesidades de la investigación (2012). También se dice que los cuestionarios cerrados implican un amplio conocimiento previo de la situación de los participantes y las posibles respuestas, pues estas deben estar preestablecidas (Abarca et al.).

La utilización del cuestionario en este trabajo final de graduación permitirá conocer las condiciones de las organizaciones clientes de Deloitte, para la implementación o utilización de la Propuesta de metodología resultante de este trabajo; además de conocer la existencia o no de ciertos documentos, lineamientos, estructuras y otros, que son necesarios para implementar dicha metodología.

Por estas razones, es resulta conveniente la utilización de un cuestionario mixto, donde algunas preguntas tienen respuestas predefinidas y algunos otras permiten que el participante ofrezca más detalle ajustando la respuesta a la realidad de su organización. El instrumento a utilizar en el desarrollo de este trabajo, se encuentra disponible en el Apéndice D.

3.7 Procedimiento metodológico

El desarrollo de este trabajo final de graduación, sigue el proceso investigativo representado en la Figura 22. Debido a que todas las investigaciones cualitativas son distintas y se adaptan a la realidad que estudian, el proceso utilizado en este trabajo fue creado por el autor con base en distintas fuentes bibliográficas.

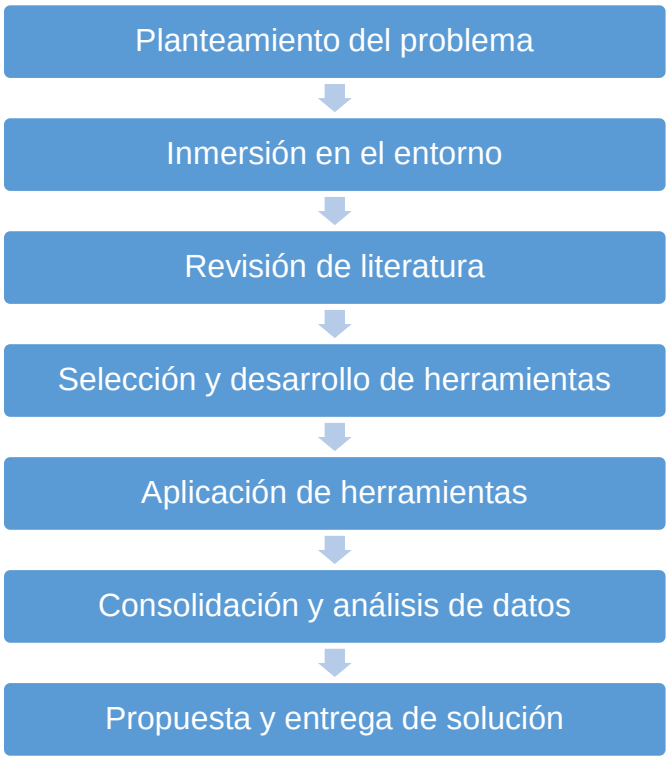


Figura 22. Proceso investigativo del trabajo final de graduación
Fuente: Elaboración propia

Es importante anotar que la investigación cualitativa es un proceso iterativo y recurrente (Hernández et al., 2014; Rojas, 2008), por tanto, los pasos descritos en esta sección no necesariamente serán ejecutados en orden. En otras palabras, la secuencia de la Figura 22 representa más bien una aproximación al orden de las actividades. Sin embargo, durante el desarrollo del proceso, el mismo puede regresar a las actividades anteriores o bien, más de una actividad podría llevarse a cabo al mismo tiempo (Creswell, 2014).

En los apartados siguientes se describe cada uno de los pasos correspondientes con el proceso establecido para el desarrollo de este trabajo.

3.7.1 Planteamiento del problema

Esta fase corresponde con la definición inicial del problema de investigación, el cual, según (Hernández et al., 2014) debe incluir aspectos como el propósito de la investigación, sus objetivos, la justificación, las deficiencias y necesidades relacionadas con el problema; así como el contexto o ambiente. Estos temas se contemplaron en el primer capítulo de este documento y en el Anteproyecto de Graduación presentado a la instancia académica correspondiente antes de iniciar este trabajo.

3.7.2 Inmersión en el entorno

De acuerdo con (Hernández et al., 2014), en esta fase corresponde al investigador entrar al espacio en donde se realizará la investigación, así como identificar a las personas importantes para brindar acceso a los recursos, espacio físico e información necesaria para el estudio. Según estos autores, es válido hacer uso de diversas técnicas que van desde mostrar interés y convencer del beneficio de la investigación, hasta explotar las habilidades sociales, dar favores y transportar personas (Hernández et al.).

Para llevar a cabo esta fase, el estudiante ha trabajado como un miembro más del equipo de *Risk Advisory* en Deloitte Centroamérica y República Dominicana desde antes de iniciar con el desarrollo de este trabajo final de graduación, ver Anexo A. De esta forma, se logra conocer el ambiente y el entorno de la organización, así como obtener acceso a la infraestructura, los recursos y la información necesarios para la realización del presente trabajo.

Así mismo, se logró identificar a las personas clave para facilitar el acceso a documentos y otros recursos necesarios, así como para brindar apoyo en la ejecución del trabajo. Coordinar reuniones, revisar el avance del trabajo, dar retroalimentación sobre los resultados y propuestas, son solo algunos de los aspectos que requieren colaboración de alguien en Deloitte y que se ven beneficiados con la inmersión en el ambiente.

3.7.3 Revisión de literatura

La tercera fase en el desarrollo de este trabajo final de graduación consiste en revisar la literatura sobre las mejores prácticas disponibles y relevantes para la metodología de gestión de riesgos de TI.

Debido a la solicitud explícita de la empresa, se revisa el marco COBIT 5 y la norma ISO 31000. Adicionalmente se considera la guía COBIT 5 para Riesgos, la normativa de la Superintendencia General de Entidades Financieras, así como algunos marcos adicionales relacionados con la gestión de riesgos de TI. También se revisan trabajos de investigación, libros y artículos sobre el tema de riesgos, riesgos de TI y la gestión de ambos.

Con base en la revisión de literatura efectuada se construye el Marco Teórico del trabajo de graduación, el cual puede encontrarse en el segundo capítulo de este documento.

3.7.4 Selección y desarrollo de herramientas

Una vez que se ha planteado el problema, y se conocen la organización y lo que indican las mejores prácticas relacionadas con gestión de riesgos de TI, el siguiente paso en el desarrollo del trabajo final de graduación, consiste en desarrollar las herramientas de recolección de datos que permitirán continuar con la investigación.

Estas herramientas, se plantean en la sección 3.6 de este mismo capítulo y con la aplicación de cada una de ellas se contribuye a alcanzar uno o más de los objetivos específicos establecidos para este trabajo. En dicha sección, se describe el objetivo de las herramientas, en qué consiste cada una y su aporte a la investigación. Por otra parte, en el apartado siguiente se describe la aplicación de dichos instrumentos.

3.7.5 Aplicación de herramientas

Para ejecutar la recolección de datos mediante las herramientas definidas, se coordinarán las sesiones o envíos necesarios con la persona encargada de la supervisión del trabajo por parte de la empresa.

La aplicación de herramientas a lo interno de Deloitte, se llevará a cabo con los sujetos de información definidos en la sección 3.5 de este documento. Es importante agregar que todas las sesiones se realizarán en las oficinas principales de Deloitte en Costa Rica.

En el caso de la información proveniente de clientes de Deloitte, la aplicación del cuestionario será coordinada con el apoyo de un gestor de desarrollo del negocio de esta Firma consultora, quien posee los contactos necesarios y el nivel de autorización para tal fin.

3.7.6 Consolidación y análisis de datos

Esta fase corresponde con la integración de los datos obtenidos, al informe del trabajo final de graduación. La información sobre las prácticas utilizadas por Deloitte, sobre proyectos anteriores y sobre las condiciones en las organizaciones clientes, será un importante insumo para el desarrollo de la Propuesta de Metodología para la gestión de riesgos de TI.

De acuerdo con (Hernández et al., 2014), en las investigaciones cualitativas, el análisis de datos no se efectúa necesariamente después de la recolección de los mismos. Por el contrario, la recolección y el análisis se realizan prácticamente al mismo tiempo. Además, como es típico en lo cualitativo, el análisis de los datos varía entre un estudio y otro.

La consolidación y análisis de resultados se presentan en el cuarto capítulo de este documento.

3.7.7 Propuesta y entrega de solución

En esta última fase, se entregará a la organización la Propuesta de Metodología, contenida en el quinto capítulo de este documento; las herramientas utilizadas en la recopilación de datos y la información resultante del proceso.

También se realizará una presentación al equipo de *Risk Advisory* en Deloitte para dar a conocer los aspectos más relevantes sobre la Propuesta de Metodología generada. Esta es además la etapa en la que se presenta el informe del trabajo a la Universidad.

En el siguiente capítulo, se presenta el análisis de resultados del trabajo final de graduación.

Análisis de Resultados

4 Análisis de Resultados

Este capítulo, presenta los resultados obtenidos con la ejecución del proceso investigativo descrito en la sección 3.7. Dichos resultados, así como los datos e información que han sido recopilados, representan un pilar fundamental para el cumplimiento de los objetivos planteados en este trabajo final de graduación.

Los resultados obtenidos con la aplicación de dichas herramientas, constituyen el fundamento principal para la construcción de la Propuesta de Metodología. Dichos resultados se encuentran agrupados en tres secciones de acuerdo con los objetivos específicos y el esquema de recolección de información planteado para este trabajo.

4.1 Prácticas utilizadas por Deloitte

Para conocer las prácticas que la firma consultora había utilizado en proyectos anteriores relacionados con la gestión de riesgos de tecnología de información, se realizaron dos actividades principales.

En primer lugar, se realizó una revisión documental a proyectos realizados anteriormente por la firma Deloitte, ver Apéndice E. Para cada proyecto, se recopiló datos básicos y extrayendo la información que el autor consideró relevante para este trabajo de graduación. Con la revisión de estos documentos se logró identificar las prácticas utilizadas por la organización para sus proyectos de gestión de riesgos de TI.

La entrevista se aplicó a una Consultora Senior con más de cuatro años de experiencia con Deloitte en proyectos de gestión de riesgos de TI, ver Apéndice F. El objetivo de la entrevista realizada, consistió en obtener información sobre la experiencia en la implementación de proyectos anteriores, contemplando el contexto de los proyectos, la estructura de gestión de riesgos utilizada y la necesidad de una metodología estandarizada para la gestión de riesgos de TI.

En los dos siguientes apartados se analizan los resultados obtenidos con la aplicación de las herramientas descritas.

4.1.1 Contexto de los servicios brindados

Para contextualizar este análisis y los servicios mismos ofrecidos anteriormente por la firma, es necesario entender que la mayoría de los clientes contaban previamente con alguna

estructura organizacional o esquema definido para la gestión de riesgos. Sin embargo, en gran parte de los casos, no existía una metodología especializada o adecuada para los riesgos de TI en particular.

Además, es notorio que, en relación con la gestión de riesgos de TI, se presenta cierto grado de duplicidad entre las tareas de diferentes unidades de negocio. Por ejemplo, el departamento de tecnología de información, mantiene un control independiente sobre algunos riesgos ya considerados por el ente gestor del riesgo a nivel organizacional.

Del mismo modo, se puede observar que las entidades del sector público, mantienen un esquema mejor definido y una serie de controles más estrictos sobre los riesgos de TI, si se les compara con empresas privadas. Esto debido, principalmente, a las regulaciones y a la normativa existente en relación con los riesgos y la gestión de TI.

En la empresa privada, por el contrario, se observa un menor interés en la gestión de riesgos general y de TI. En los clientes de carácter transnacional, normalmente se les presta mayor atención a los riesgos en la casa matriz, dejando de lado los controles y la estructura necesarios en las sucursales; en este caso en la región de Centroamérica y en la República Dominicana.

En general, se observa que los manuales o procedimientos utilizados en las organizaciones para la gestión de riesgos de TI, son una copia de lo indicado por alguna normativa o práctica. Por tanto, el trabajo de Deloitte muchas veces consistió en desarrollar desde cero un marco para este tipo de riesgos o bien, en reestructurar las prácticas existentes para satisfacer las necesidades específicas de los riesgos de tecnología de información. En algunos casos, el desarrollo del proyecto terminó convirtiéndose en un ordenamiento de la documentación y las tareas preexistentes para ajustarlas a las mejores prácticas o requerimientos establecidos.

Es importante añadir que en muchos casos la contratación de estos servicios a la firma Deloitte, se origina únicamente en un requisito de cumplimiento y no representa un interés real, por parte de las organizaciones, en atender los riesgos de tecnología de información.

4.1.2 Metodología de la firma para la gestión de riesgos de TI

DTTL cuenta con una biblioteca de recursos electrónicos sobre riesgos. Sin embargo, a nivel local no se conoce una guía definida para la gestión de riesgos de TI que se adapte a la realidad de los clientes en la región.

En el área de *Risk Advisory*, se conoce el ciclo de gestión de riesgos a nivel general, pero no específicamente para riesgos de TI. Este ciclo, contempla la identificación, análisis, evaluación, tratamiento, mitigación, monitoreo y comunicación de los riesgos.

El conocimiento utilizado por la firma se basa principalmente en el ciclo sugerido por la norma ISO 31000 y en el marco COBIT 4.1. En algunos casos específicos, se sigue también lo indicado por las normativas o regulaciones gubernamentales según la naturaleza y las necesidades del cliente.

Al no existir una plantilla genérica o un documento base que permita llevar a cabo todos los proyectos siguiendo un mismo método, se utiliza información y documentación de proyectos anteriores como guía o como plantilla para el trabajo a realizar en nuevos proyectos.

4.1.3 Necesidad de una metodología específica

Según la consultora entrevistada es necesario establecer una metodología que organice estandarice el trabajo de gestión de riesgos de TI realizado por el equipo de consultores. Se entiende por sus comentarios, que cuando los consultores tienen poco tiempo de trabajar en este tipo de proyectos, resulta complicado generar productos de calidad debido a la falta de conocimiento sobre las prácticas adecuadas. En el proceso de inmersión en el entorno, se constató que existe una alta rotación de personal en la firma. Precisamente, esta es la razón de aplicar la entrevista solamente a una persona. Los demás consultores con experiencia en el área habían dejado de trabajar para la firma al momento de este estudio.

Además, se comenta que la metodología establecida, debe estar disponible para su consulta, accesible y que todo el equipo debería conocer sus principios fundamentales y saber cómo acudir fácilmente a la documentación de apoyo. Aunque existen a nivel global distintas metodologías para los servicios ofrecidos por Deloitte, muchas veces los consultores no conocen los medios adecuados para acceder a las mismas. O bien, el conocimiento no está totalmente disponible, documentado o definido para utilizarlo en los proyectos.

Se identifica que, en algunos proyectos, ha sido necesario “armar” una solución con base en la documentación de otros proyectos. Esto ocasiona una disminución en la calidad de los servicios prestados, pues el resultado no se ajusta en un cien por ciento a la realidad y las necesidades del cliente específico. De igual manera, se afectan negativamente la calidad, el tiempo y el costo de los servicios, pues se debe invertir recursos en el aprendizaje de los consultores.

Aunque los proyectos desarrollados por la firma consultora, siempre han finalizado de manera exitosa, muchas veces conllevan un esfuerzo no planificado debido a la brecha existente entre las necesidades de los proyectos y el conocimiento o la metodología disponibles para la realización de los mismos. Una metodología estructurada y estandarizada permitirá, desde el momento de la oferta, estimar con mayor exactitud los recursos necesarios para completar un proyecto de forma óptima.

4.2 Mejores prácticas sobre riesgos de TI

Para examinar las mejores prácticas presentes en la industria, así como las normativas y tendencias relacionadas con la gestión de riesgos de TI, se efectuó una revisión de literatura. Esta revisión de literatura, dio origen al segundo capítulo de este documento.

El desarrollo del marco teórico es fundamental pues permitió identificar las mejores prácticas adecuadas para el desarrollo de este trabajo final de graduación. En el marco teórico se incluyeron los siguientes marcos de referencia:

- COBIT 5.
- ISO 31000.
- COBIT 5 para Riesgos.
- ISO 27005.
- OCTAVE.
- COSO.
- MAGERIT.
- Normativas SUGEF.

Además, en este marco se amplían los conceptos de riesgo, gestión de riesgos y algunos enfoques existentes en la literatura académica sobre metodologías para la gestión de riesgos de TI.

4.3 Propuesta de metodología

Para el desarrollo de la propuesta de metodología se obtuvo información a través de dos métodos distintos. Primeramente, el desarrollo del grupo focal permitió valorar la aplicación de las mejores prácticas sobre riesgos de TI. Así mismo, esta herramienta permitió la creación conjunta de una base para la Propuesta de Metodología. Al poner sobre la mesa las expectativas, anotaciones y recomendaciones de los principales interesados en la organización, el autor obtuvo un importante insumo para la definición de una propuesta de solución basada en las mejores prácticas y adecuada a la realidad de Deloitte.

Por otra parte, se aplicó un cuestionario a un grupo de organizaciones clientes de Deloitte. Este método fue aplicado mediante la herramienta web *Google Forms* y permitió recopilar información de organizaciones en distintos sectores, a saber: financiero, tecnológico, gobierno y educación superior.

En los dos apartados siguientes, se analizan los resultados de la sesión con los interesados en Deloitte y del cuestionario aplicado a las organizaciones cliente respectivamente.

4.3.1 Observaciones y expectativas del patrocinador

Para validar la aplicación de las prácticas sugeridas y la estructura de la propuesta de solución, se realizó un grupo focal con los representantes de la organización. En esta sesión (ver Apéndice G), participaron los siguientes integrantes:

- Socio Director regional de *Risk Advisory.*
- Una Gerente *senior* de *Risk Advisory.*
- Dos Gerentes de *Risk Advisory.*
- Un gestor de desarrollo del negocio de *Risk Advisory.*

Los comentarios realizados y la información recolectada en el grupo focal apoyaron la aplicación de las mejores prácticas sugeridas por el estudiante. Por tanto, el resultado de esta actividad refuerza la decisión de utilizar la guía COBIT 5 para Riesgos como eje central de la Propuesta de metodología.

Los participantes estuvieron de acuerdo en que el entregable del trabajo final de graduación se base en las prácticas presentadas y contemple las actividades y factores que fueron revisados en el grupo focal.

4.3.2 Condiciones en las empresas clientes de Deloitte

Para validar la aplicación de la Propuesta de Metodología en las organizaciones clientes de Deloitte, así como los principales aspectos que deben ser considerados en el contenido de dicha propuesta, se aplicó un cuestionario a 12 empresas de diferentes sectores, ver Apéndice H. Los resultados del cuestionario aplicado, se pueden resumir en los siguientes aspectos:

- Más del 90% de las empresas cuenta con un área o función encargada de la gestión de riesgos y un 75% cuenta con un comité organizacional de riesgos. Esto representa un factor ventajoso en la implementación de la Propuesta de Metodología, pues para la gestión de riesgo se requiere que la organización haya definido lineamientos y parámetros para riesgos.
- Existe en más del 90% de las empresas, una política organizacional sobre gestión de riesgos. Por tanto, se debe dar un mayor enfoque a la etapa de gestión de riesgos, aprovechando los recursos con los que ya cuentan las organizaciones cliente a nivel de gobierno de riesgos.
- Solo en la tercera parte de las organizaciones se han definido el apetito y la tolerancia de riesgo por un órgano directivo o junta de administración y en más del 40%, estos parámetros no se encuentran definidos en ningún nivel. Este tema debe contemplarse y detallarse en la propuesta de solución para apoyar a las organizaciones clientes y fortalecer la estructura de gobierno de riesgos con que cuentan actualmente.
- Los escenarios de riesgo, aspecto fundamental en la aplicación de COBIT 5 para la gestión de riesgos, no se utilizan en más del 58% de las empresas. Por tanto, la solución que este trabajo proponga, debe contemplar los aspectos necesarios para utilizar escenarios de riesgo de TI.
- Dos terceras partes de las organizaciones analizadas, no cuentan con un portafolio de estrategias o acciones definidas para el tratamiento de los riesgos de tecnología de información. Este aspecto, deberá ser considerado en la Propuesta de Metodología para la gestión de riesgos de TI.
- Existen otras vulnerabilidades en aspectos como la consideración de riesgos en proyectos de TI o el seguimiento a la gestión de riesgos de TI, que refuerzan la necesidad de establecer una metodología estándar para la gestión de riesgos de TI.

Propuesta de Solución

5 Propuesta de Solución

Este capítulo presenta la Propuesta de Metodología para la gestión de riesgos de TI que se formula como resultado de este trabajo final de graduación. Esta metodología se basa principalmente en el marco COBIT 5, siguiendo para ello las recomendaciones de la guía "COBIT 5 para Riesgos". Así mismo, la propuesta utiliza el ciclo de gestión de riesgos sugerido por la norma ISO 31000, esto de acuerdo con una solicitud expresa de la firma consultora Deloitte. Adicionalmente, la propuesta de metodología atiende las recomendaciones de otros marcos de referencia y normativas incluidos en el Marco Teórico de este documento.

La solución que se propone en este capítulo, es el resultado del proceso desarrollado durante el periodo del trabajo final de graduación y contempla tanto las prácticas utilizadas en proyectos anteriores implementados por de Deloitte, como las mejores prácticas disponibles en materia de gestión de riesgos de TI. La propuesta incluida en este capítulo, contempla los principales aspectos de la gestión de riesgos de TI sin ser demasiado exhaustiva. De tal manera, se convierte en una herramienta completa y a la vez genérica, que puede ser utilizada en diferentes tipos de organización y colaborar al establecimiento de un adecuado proceso de gestión de riesgos de tecnología de información.

A continuación, se presenta la metodología propuesta para la firma consultora Deloitte como resultado de este trabajo final de graduación.

5.1 Metodología para la gestión de riesgos de TI

5.1.1 Introducción

Esta metodología, define los pasos a seguir para gestionar los riesgos de tecnología de información, de manera que se facilite la toma de decisiones oportuna ante eventos que limiten o afecten los objetivos de TI y que puedan impactar el logro de los objetivos del negocio.

Es importante aclarar, que el presente documento no se apega a la metodología de riesgos de una organización en específico. Por el contrario, representa una guía genérica que se puede utilizar en diferentes empresas y contiene los aspectos principales recomendados por las mejores prácticas para la gestión de riesgos de tecnología de información; principalmente por el marco COBIT 5.

Lo anterior, no significa que con la implementación de esta metodología se cumplen las normas o estándares aplicables en la gestión de riesgos de TI, aunque sí se establece una sólida base para tal fin. La implementación definitiva de una metodología para la gestión de riesgos en cualquier organización; debe considerar el entorno, los objetivos, y las regulaciones aplicables en cada caso.

Con la implementación de un modelo de gestión de riesgos, se busca llevar a cabo evaluaciones periódicas sobre los riesgos y sobre las acciones establecidas a nivel de TI para la gestión de los mismos. De este modo, se pueden consolidar los resultados obtenidos para así conocer los riesgos más importantes de TI y definir los planes de acción necesarios para tomar decisiones al respecto.

5.1.2 Objetivo

Definir un modelo para la gestión de riesgos de TI, que se encuentre alineado con las mejores prácticas en la materia, que facilite el cumplimiento y asegure un adecuado control para minimizar los efectos adversos y que genere valor a la organización mediante la identificación, valoración y atención de riesgos.

5.1.3 Alcance

Esta metodología no pretende duplicar ni sustituir los procedimientos utilizados para la gestión de riesgos en la organización. Se enfoca más bien en alinear la gestión efectuada sobre los riesgos específicos de TI, con la gestión de riesgos organizacional y con las mejores prácticas o normativas aplicables. Por ello, para la adecuada implementación de esta metodología, se requiere conocer los lineamientos y políticas establecidas en el negocio para la gestión de riesgos.

El procedimiento contemplado en esta metodología para la gestión de riesgos de TI sigue los pasos sugeridos por la norma ISO 31000, los cuales se describen más adelante. En cada uno de los pasos se utiliza como base lo sugerido por el marco COBIT 5, principalmente en sus procesos referidos a la gestión de riesgos, el EDM03 y el APO12.

5.1.4 Definiciones y términos

Amenaza

Riesgo negativo; un evento adverso incierto o condición que, de llegar a ocurrir resultaría en efectos desfavorables tales como daños al ambiente, comunidades, accionistas, reputación, retrasos o pérdidas económicas.

Análisis cualitativo

Descripción de la magnitud de las consecuencias potenciales, la probabilidad de que esas consecuencias ocurran y el nivel de riesgo asociado.

Análisis cuantitativo

Estimación numérica o cuantificable de la magnitud de las consecuencias potenciales, de la probabilidad de que esas consecuencias ocurran y del nivel de riesgo asociado.

Apetito de riesgo

Nivel de riesgo que una organización está preparada para aceptar, tolerar o soportar en un momento determinado de tiempo (cuantitativo o cualitativo).

Consecuencia

El resultado de un riesgo si este ocurre. En el caso de una amenaza, las consecuencias son desfavorables y si se trata de una oportunidad las consecuencias son favorables.

Control

Políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable de que los objetivos de negocio se alcanzarán y los eventos no deseados serán prevenidos o detectados y corregidos.

Dueño del riesgo

Individuo, miembro del personal quien está cercanamente asociado con el riesgo y está dispuesto o le corresponde a monitorearlo.

Efecto

Un hecho que ocurre como consecuencia de otro que le antecede.

Evaluación de riesgos

Actividades para determinar el nivel de exposición de un proceso frente a sus riesgos, con el propósito de desarrollar estrategias de mitigación, a través de la instauración y fortalecimiento de controles.

Gestión de riesgos

Cultura, procesos y estructuras que están dirigidas hacia la administración efectiva de oportunidades potenciales y efectos adversos con el ambiente de la organización.

Impacto

Conjunto de efectos derivados de la materialización de un evento, expresado cualitativa o cuantitativamente ya sean pérdidas, prejuicios, desventajas o ganancias.

Indicadores de riesgo

Proporciona al dueño del riesgo con alertas previas para tomar acciones que mitiguen el riesgo a través de controles internos más fuertes y mantenerlos monitoreados. Estos indicadores deben ser medibles y apuntalados con datos.

Interesados (*stakeholders*)

Se refiere a las partes interesadas de la organización, que pueden incluir a la Junta Directiva, Gerencia de TI, Dirección de Riesgo, las áreas funcionales de TI y los dueños de los procesos dependiendo específicamente de la organización. También se refiere a todas las partes participantes o posiblemente afectadas por el proceso de gestión de riesgos.

Nivel de riesgo

Grado de exposición al riesgo que se determina a partir del análisis de la probabilidad de ocurrencia del evento y de la magnitud de su consecuencia potencial sobre la realización de los objetivos fijados. El nivel de riesgo permite establecer su importancia relativa sobre los objetivos.

Nivel de riesgo aceptable

Nivel de riesgo que la organización está dispuesta y en capacidad de retener para cumplir con sus objetivos, sin incurrir en costos ni efectos adversos excesivos en relación con los beneficios esperados y sin ser incompatible con las expectativas de las partes interesadas.

Objetivo de control

Es una declaración del resultado o fin que se desea lograr al implantar procedimientos de control en una actividad de TI en particular.

Oportunidad

Riesgo positivo; evento beneficioso incierto o condición que de llegar a ocurrir resultaría en un efecto favorable como una mejora de seguridad, ahorro de tiempo o costo, mejora en las relaciones con comunidades y miembros de la organización, alcance de objetivos, reputación, entre otros.

Probabilidad

Medida o descripción de la posibilidad de ocurrencia de un evento.

Proceso

Sucesión de acciones continuas regulares, que ocurren o se llevan a cabo de una forma definida y que llevan al cumplimiento de algún resultado; una operación continua o una serie de operaciones.

Riesgo

La posibilidad de que, si algo sucede, tenga un impacto en el cumplimiento de los objetivos de la organización. El riesgo es medido en términos de consecuencias y probabilidad.

Riesgo materializado

Es la ocurrencia del evento que fue identificado en un inicio, es decir, cuando la probabilidad del riesgo se concreta, se hace real y hace que el riesgo se cumpla.

Riesgo operativo

Es la posibilidad de una pérdida económica debido a fallas o debilidades de procesos, personas, sistemas internos y tecnología, así como eventos imprevistos.

Riesgo de tecnología de información (TI)

El riesgo de TI es la posibilidad de pérdidas económicas derivadas de un evento relacionado con el acceso o uso de la tecnología, que afecta el desarrollo de los procesos del negocio y la gestión de riesgos de la entidad, y que puede atentar contra la confidencialidad, integridad, disponibilidad, eficiencia, confiabilidad y oportunidad de la información.

Riesgo Inherente

El riesgo originalmente identificado antes de que alguna acción de control haya sido implementada.

Riesgo Residual

Nivel resultante del riesgo, después de tomar las medidas con pertinencia y eficacia combinadas con todos los controles asociados al riesgo.

Tolerancia al riesgo

Tolerancia al riesgo es el nivel aceptable de variación en el rendimiento en relación con el logro de los objetivos. Operar dentro de la tolerancia al riesgo proporciona una gestión con mayor confianza en que la entidad alcance sus objetivos.

5.1.5 Política y gobierno de riesgos

Para una llevar a cabo la gestión de riesgos, se requiere que el negocio haya establecido una política sobre riesgos. En esta política se deben definir las responsabilidades de los diferentes roles involucrados en el proceso, así como los lineamientos necesarios para asegurar que los procedimientos de gestión de riesgos se efectúen de la forma correcta.

5.1.5.1 Definición del apetito y la tolerancia de riesgos

Como parte del gobierno de riesgos, el nivel directivo debe definir el apetito y la tolerancia de riesgos. De esta forma, cuando se lleve a cabo el procedimiento de gestión de riesgos de TI, se pueden tomar como referencia para la evaluación de dichos riesgos, los lineamientos que el negocio ha definido y los niveles de aceptabilidad establecidos.

Los niveles de aceptabilidad de riesgos son definidos por el negocio y se comparan con el nivel de riesgo resultante de la valoración de riesgos. Según sea el resultado de esa comparación, cada riesgo se ubica en una de dos categorías: aceptable o no aceptable. En la Tabla 9 se presenta un ejemplo de las categorías definidas por la organización para la aceptabilidad de los riesgos.

En el caso que se presenta, los riesgos aceptables para la organización son aquellos que sean calificados con un nivel de riesgo bajo, moderado o medio. Por el contrario, los riesgos que sean valorados con un nivel alto o muy alto se categorizan como riesgos no aceptables y, por tanto, deben ser atendidos o tratados según se defina en el proceso de gestión de riesgos de TI.

Tabla 9. Categorías del apetito de riesgo

Categoría	Nivel de riesgo
No aceptable	Muy Alto
	Alto
Aceptable	Medio
	Moderado
	Bajo

Adicionalmente, el dueño de cada riesgo puede justificar la retención o no de un riesgo en una categoría determinada. Esto, tomando en cuenta diferentes factores como la relación costo - beneficio de atender un riesgo no aceptable, la efectividad estimada de las acciones que puedan tomarse para tender el riesgo, la capacidad y disponibilidad de la organización para llevar a cabo las acciones de atención del riesgo y cualquier otro factor relevante que la organización defina en correspondencia con sus objetivos de negocio.

El conocimiento experto del dueño del riesgo y los involucrados en la gestión de riesgos son un aspecto importante para tomar decisiones óptimas sobre este tema. El buen juicio y la experiencia, así como el conocimiento del entorno y las condiciones particulares del riesgo juegan un papel relevante en las decisiones sobre retención de riesgos.

5.1.5.2 Periodicidad de seguimiento de riesgos

Por otra parte, el gobierno de riesgos debe definir la periodicidad de revisión o seguimiento de los distintos riesgos según sea el nivel de cada uno. Esto, con el fin de priorizar las medidas, controles y planes de contingencia que han de elaborarse en cada caso, de manera que se consigan oportunamente las metas y los objetivos de negocio.

Adicionalmente, se podrán establecer frecuencias de seguimiento para algunos riesgos específicos a criterio de la unidad encargada de la gestión de riesgos o del Comité de Riesgos de la organización.

La Tabla 10, muestra un ejemplo de cómo la organización define la periodicidad de seguimiento para los diferentes niveles de riesgo resultantes de la valoración de riesgos.

Tabla 10. Periodicidad de seguimiento a riesgos

Seguimiento	Nivel de riesgo
Mensual	Muy Alto
	Alto
	Medio
Trimestral	Moderado
Semestral	Bajo

5.1.6 Proceso de gestión de riesgos de TI

Este apartado describe el proceso principal de esta metodología, el proceso para la gestión de riesgos de TI. Como se mencionó anteriormente, el contenido de esta metodología está basado en el marco COBIT 5 y se encuentra organizado según los pasos sugeridos por la norma ISO 31000.

Tal como se muestra en la Figura 23, el proceso incluye: comunicación y consulta, establecimiento del contexto, valoración de riesgos, tratamiento de riesgos, monitoreo y revisión.

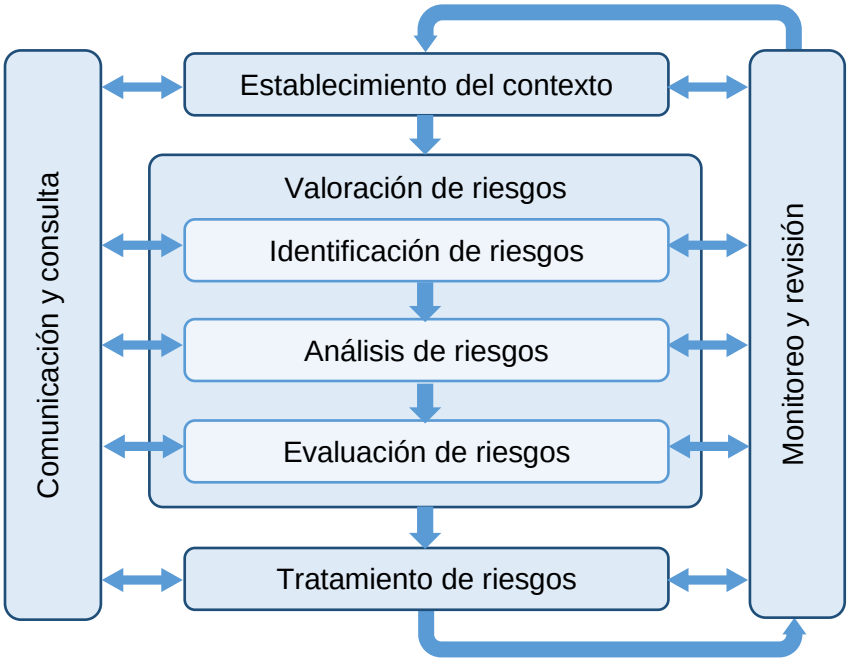


Figura 23. Proceso de la propuesta de metodología
Fuente: Elaboración propia con base en (INTECO, 2011)

En los siguientes apartados, se detalla cada uno de los pasos contemplados como parte de esta metodología de gestión de riesgos de TI.

5.1.6.1 Comunicación y consulta

Esta es una actividad trasversal que se encarga de la comunicación y consulta con los interesados ya sean internos o externos del proceso de gestión de riesgos o alguna de sus etapas en particular. El objetivo de esta actividad consiste en definir los parámetros y medios de comunicación para que los interesados obtengan la información necesaria en el momento preciso.

Con el desarrollo de esta actividad se garantiza que la documentación generada, así como su recopilación, distribución y almacenamiento, son adecuados y oportunos. Para ello, se debe seleccionar la información que se comunicará a cada uno de los interesados. De esta forma, se podrá documentar y comunicar la información relevante para cada uno de los *stakeholders* según sus intereses, su participación y el nivel de influencia o impacto que tengan en el proceso.

En la Tabla 11 se sugiere un esquema para la matriz de comunicaciones. En la columna de información se incluyen algunos documentos importantes en la gestión de riesgos de TI, aunque cada organización podría agregar la información que se requiera para las comunicaciones del proceso. Así mismo, se debe definir cuáles interesados recibirán qué información, por cuál canal o medio y con qué frecuencia. Es importante resaltar que el flujo de información es bidireccional, por lo que la organización debe establecer los medios necesarios para tal efecto y ponerlos a disposición de los interesados.

Tabla 11. Comunicaciones sobre gestión de riesgos

Información	Canal	Destinatarios	Periodicidad
Metodología de riesgos			
Matriz de valoración de riesgos			
Matriz de controles de riesgos			
Planes de acción			
Reporte de indicadores claves			

5.1.6.2 Establecimiento del contexto

Esta etapa consiste en definir los parámetros dentro de los cuales se deben gestionar los riesgos, además de establecer el alcance para el proceso de gestión de riesgos. El establecimiento del contexto se debe ajustar a los objetivos de valoración de riesgos que haya definido el negocio y debe considerar la información sobre el contexto y los factores de riesgo que conozca la organización.

Los factores de riesgo sugeridos en el marco COBIT 5 se agrupan en cuatro categorías como se describe a continuación:

Factores ambientales externos

- Factores económicos y de mercado.
- Tasa de cambio del mercado/ciclo de vida del producto.
- Industria y competencia.
- Situación geopolítica.
- Ambiente regulatorio.
- Estado de la tecnología y su evolución.
- Panorama de amenazas.

Factores ambientales internos

- Metas y objetivos de la empresa.
- Importancia estratégica de TI para la empresa.
- Complejidad de TI.
- Complejidad de la empresa y grado de cambio.
- Capacidad de gestión del cambio.
- Modelo operativo.
- Prioridades estratégicas.
- Cultura de la empresa.
- Capacidad financiera.

Capacidades de gestión de riesgos

- Gobierno del riesgo.
- Gestión del riesgo.

Capacidades relacionadas con TI

- Evaluar, dirigir y supervisar (EDM).
- Alinear, planificar y organizar (APO).
- Construir, adquirir e implementar (BAI).
- Entregar, dar servicio y soporte (DSS).
- Supervisar, evaluar y valorar (MEA).

5.1.6.3 Valoración de riesgos

Esta etapa incluye la identificación, el análisis y la evaluación de los riesgos. A continuación, se detalla cada una de estas actividades que la organización debe llevar a cabo como parte fundamental de la gestión de riesgos de TI.

5.1.6.3.1 Identificación de riesgos

Esta actividad se trata de identificar eventos potenciales que afectarán a la organización si llegan a ocurrir. El propósito fundamental es tener conocimiento de los riesgos asociados con la tecnología de información. Esta identificación permite que más adelante, se defina el nivel de riesgo al que se encuentran expuestos los procesos y actividades relacionados con las TI.

Los eventos con impacto negativo representan riesgos que exigen la evaluación y respuesta de la organización. Los eventos con impacto positivo representan oportunidades, que se deben conducir hacia la estrategia y el cumplimiento de los objetivos de negocio y de TI.

Para la identificación de riesgos, la organización puede utilizar uno o varios enfoques teniendo en cuenta que, a mayor cantidad de fuentes de información, mayor certeza habrá en el listado de riesgos resultante. Algunos de los mecanismos o enfoques para obtener información sobre posibles eventos de riesgo son los siguientes:

- Conferencias sectoriales o técnicas.
- Sitios Web de empresas afines y campañas publicitarias.
- Grupos de presión política.
- Encuentros sobre gestión de riesgos internos.
- Resultados de benchmarking.
- Procesos legales de competidores.
- Índices externos clave.

- Índices internos clave / Medidas de riesgo y rendimiento / Cuadros de mando.
- Nuevas decisiones legales.
- Informes en los medios.
- Informes mensuales de la dirección.
- Informes de analistas.
- Publicaciones sectoriales, comerciales y profesionales.
- Calendario del lanzamiento de nuevos productos frente al de la competencia.
- Perfil de las llamadas de servicio al cliente.
- Información en tiempo real sobre la actividad de los mercados financieros.
- Informes de auditoría.

Para la identificación de riesgos se utiliza, además de los mecanismos anteriores, la información recopilada sobre el contexto y los factores de riesgo, además, se construyen escenarios de riesgo como se muestra en seguida.

5.1.6.3.1.1 Escenarios de riesgo

Un aspecto importante que COBIT 5 incorpora en la gestión de riesgos es la definición de escenarios de riesgo. Un escenario de riesgo permite representar la ocurrencia de un riesgo y la afectación que tal evento podría causar en el negocio. La organización debe identificar y mantener conocimiento de los escenarios de riesgo relevantes según sus necesidades y los factores de riesgo identificados.

La definición y documentación de los escenarios de riesgo debe incluir la siguiente información:

Actor

- Internos como colaboradores o consultores.
- Externos como competidores o entidades reguladoras.

Tipo de amenaza

- Maliciosa.
- Accidental.
- Error.
- Falla.
- Natural.

- Requerimiento externo.

Evento

- Divulgación.
- Interrupción.
- Modificación.
- Robo.
- Destrucción.
- Diseño inefectivo.
- Ejecución inefectiva.
- Reglas y regulaciones.
- Uso inapropiado.

Activos o recursos

- Personas y habilidades.
- Estructuras organizacionales.
- Procesos.
- Infraestructura (facilidades).
- Infraestructura de TI.
- Información.
- Aplicaciones.

Tiempo

- Duración.
- Calendario de incidencias (críticas o no críticas).
- Detección.
- Retraso.

Para la definición de escenarios de riesgo, la organización puede seleccionar un enfoque descendente, uno ascendente o utilizar una mezcla de ambos si se considera adecuado para la realidad de la organización y el cumplimiento de sus objetivos.

En el enfoque ascendente, se inicia la definición de escenarios de riesgo, a partir de escenarios genéricos. Con base en dichos escenarios genéricos se deben identificar los escenarios hipotéticos que pueden afectar a la organización y se efectúa una reducción de

los mismos mediante un análisis de alto nivel identificando aquellos que resulten más relevantes para la gestión de riesgos en la organización.

Por otra parte, en el enfoque descendente, el punto de partida son las metas de negocio establecidas. Se deben identificar los escenarios de alto impacto que pueden afectar los objetivos de negocio. Finalmente, se realiza una comparación con los escenarios genéricos sugeridos para dar paso a la gestión de riesgos con base en soluciones conocidas.

Para ambos enfoques resulta de vital importancia apoyarse en los escenarios de riesgo genéricos que se definen en la guía “COBIT 5 para Riesgos” publicada por ISACA en el año 2013. Adicionalmente, si se desea ahondar más en el tema de escenarios de riesgo, ISACA emitió una guía adicional en el año 2014 denominada “Escenarios de riesgo utilizando COBIT 5 para Riesgos”.

En las dos guías mencionadas, se muestra cómo utilizar los habilitadores de COBIT 5 para llevar a cabo una adecuada gestión de riesgos que se alinee con los objetivos del negocio. Las guías mencionadas presentan un catálogo completo de escenarios genéricos detallando sus componentes y sugiriendo distintas opciones para responder a cada escenario.

5.1.6.3.2 Análisis de riesgos

El objetivo del análisis de riesgos se basa en determinar la probabilidad e impacto de los riesgos identificados a través de escalas de calificación cualitativa y cuantitativa. Esto facilita la posterior asignación de valores que permiten clasificar los riesgos en el nivel correspondiente y así determinar las prioridades en la atención de riesgos. Para este fin, se colocan los valores de los riesgos analizados en un mapa de calor.

Asimismo, se debe llevar a cabo la identificación y valoración de los controles existentes. Esta identificación, se realiza para determinar si la organización o las unidades de TI, cuentan con puntos de control sobre los riesgos de TI actuales. Luego, la valoración se encarga de determinar si los controles actuales son efectivos.

Un aspecto importante que debe ser considerado son las capacidades y la experiencia que debe tener el personal encargado de ejecutar cada uno de los pasos del análisis de riesgos. Lo anterior, con el objetivo de contar con información precisa para el análisis de riesgos y que la respectiva evaluación se efectúe de manera objetiva y fundamentada.

Para llevar a cabo el análisis de riesgos, se debe realizar una serie de talleres con los dueños de los procesos relacionados con tecnología de información. En estos talleres, los participantes deben asignar una calificación cualitativa de probabilidad e impacto a cada uno de los riesgos considerados. Una vez que se obtenga la información de estas variables, el análisis se habrá completado y se podrá determinar el nivel de riesgo para cada caso.

A continuación, se describen los principales aspectos que forman parte del análisis de riesgos.

5.1.6.3.2.1 Probabilidad

Se trata de la posibilidad de que un riesgo ocurra. Se puede medir con base en los criterios de frecuencia y factibilidad de ocurrencia del riesgo.

Frecuencia

Número de veces que sucede un evento. Por ejemplo, número de veces que se descompone el equipo, número de veces que no hay información disponible o número de veces que hubo ataques de virus. Para determinar la frecuencia del riesgo, es importante preguntarse: ¿Cuántas veces al año se presenta este riesgo?

Factibilidad

Se refiere a la presencia de factores internos y externos que pueden propiciar la aparición u ocurrencia del riesgo, aunque este no se haya materializado anteriormente.

Para establecer el nivel de probabilidad de los riesgos, la organización debe definir una escala que contemple la calificación cuantitativa y la cualitativa. Esto, con el objetivo de que los participantes puedan ubicar el riesgo en una de las calificaciones y que dicha calificación sea útil en la determinación del nivel de riesgo. La Tabla 12 presenta una sugerencia de la escala que debe utilizarse en el análisis de probabilidad de riesgo. Sin embargo, esta escala puede variar dependiendo de la organización.

Algunas consideraciones adicionales que influyen en la calificación de la probabilidad de un riesgo son las siguientes:

- Frecuencia anticipada: que el riesgo se materialice antes de lo previsto.
- Ambiente externo: una variación inesperada (leyes, competencia, eventos de la naturaleza).

- Los procedimientos, herramientas y habilidades que se tienen actualmente: deficiencias en los controles, falta de capacitación, ausencia de recursos tecnológicos, entre otros.
- El compromiso del personal: la moral, la actitud, grado de identificación y participación en el desarrollo de las funciones que han sido asignadas.
- Historia de eventos previos: registro de datos sobre eventos ocurridos en el pasado.

Tabla 12. Escala de probabilidad

Probabilidad	Calificación cuantitativa	Calificación cualitativa
Altamente probable	5	Puede ocurrir al menos una vez al día
Muy probable	4	Puede ocurrir varias veces en un mes.
Probable	3	Puede ocurrir al menos una vez al año.
Poco probable	2	Puede ocurrir alguna vez entre uno y cinco años.
Improbable	1	Puede ocurrir al menos una vez en periodos superiores a cinco años.

5.1.6.3.2.2 Impacto

Se refiere a las consecuencias que podría ocasionar el riesgo en el logro del objetivo de TI y de negocio si llega a materializarse. Por ejemplo, que una tarea o servicio no se pueda efectuar, que se afecten la imagen y la credibilidad institucional o que exista una sanción legal.

Para valorar el nivel de impacto de los riesgos, la organización debe definir una escala que contemple la calificación cuantitativa y la cualitativa. La calificación cualitativa permitirá a los participantes del análisis, ubicar el riesgo en una de las categorías de impacto. La calificación cuantitativa, en este caso, corresponde exclusivamente al negocio pues se trata de una estimación de las pérdidas económicas que podría generar el riesgo.

El personal de TI encargado de riesgos o los dueños de los riesgos, deben proporcionar al negocio la información necesaria para que sea definido el nivel de impacto cuantitativo de los riesgos. La Tabla 13 presenta un ejemplo de la escala a utilizar en el análisis de impacto. Esta tabla, sirve de base para que la organización defina su propia escala de calificación de acuerdo con sus lineamientos de riesgo y el contexto en que opere.

Tabla 13. Escala de impacto

Impacto	Valor	Calificación cuantitativa	Calificación cualitativa
Muy alto	5	Pérdida económica mayor a $250.000.	No se tendría acceso a recursos críticos por más de una hora. Afecta a uno o más servicios críticos / A dos o más servicios no críticos / A una o más oficinas / Afecta el servicio a muchos clientes. Repercusiones gubernamentales a nivel político y pérdida de confianza del público. Multas por parte de entidades reguladoras.
Alto	4	Pérdida económica menor a $250.000 y mayor a $75.000.	No se tendría acceso a recursos críticos por entre una y cuatro horas. Afecta a uno o más servicios críticos / A dos o más servicios no críticos / A una o más oficinas / Afecta el servicio al cliente. Suspensión prolongada de servicios críticos. Reportajes en múltiples medios de comunicación por más de un día. Apercibimientos por parte de entidades reguladoras.
Medio	3	Pérdida económica menor a $75.000 y mayor a $10.000.	No se tendría acceso a recursos críticos por entre 4 y 24 horas. Afecta a uno o más servicios / A dos o más servicios no críticos / A una o más oficinas. Repercusiones significativas sobre los clientes. Artículos de prensa, televisión o internet. Divulgación significativa por máximo un día. Se presentan comunicados por parte de entidades reguladoras pero no sujetas a multas.
Moderado	2	Pérdida económica menor a $10.000 y mayor a $5.000.	No se tendría servicio por entre uno y tres días. Posibilidades de suspensión del servicio sin impacto significante sobre los clientes. Circulaciones por internet y propaganda menor por medios de comunicación. Comentarios adversos sin intervención de entidades reguladoras.
Bajo	1	Pérdida económica menor a $5.000.	No se tendría servicio por más de una semana. No impacta a los clientes. No hay divulgación de problemas ni propaganda del suceso por medios de comunicación. No intervienen entidades reguladoras.

5.1.6.3.2.3 Nivel de riesgo y mapa de calor

El nivel de riesgo, también conocido como severidad, representa el grado de exposición al riesgo. Este valor se determina a partir del análisis de la probabilidad de ocurrencia del evento y de la magnitud de sus consecuencias potenciales sobre el cumplimiento de los objetivos.

Cada organización debe establecer, en sus políticas, los niveles adecuados para su proceso de gestión de riesgos. En la Tabla 14 se presenta un modelo sugerido con cinco niveles de riesgo. Los valores asociados con cada nivel de riesgo se obtienen al multiplicar la calificación asignada a cada riesgo en el análisis de probabilidad por la calificación asignada en el análisis de impacto.

Es importante aclarar que los valores de referencia mostrados en la Tabla 14, corresponden con el modelo de cinco niveles que se ha utilizado para ejemplificar el análisis de probabilidad y de impacto. Si la organización define una escala distinta para la valoración de dichos parámetros, se deberán realizar los ajustes respectivos en los niveles de riesgo.

Tabla 14. Niveles de riesgo

Nivel de riesgo =	Probabilidad x Impacto
Muy alto	Mayor o igual que 20.
Alto	Mayor o igual que 10 y menor que 20.
Medio	Mayor o igual que 5 y menor que 10.
Moderado	Mayor o igual que 3 y menor que 5.
Bajo	Menor que 3.

Una vez definido e nivel de riesgo, es posible ubicar los riesgos en un mapa de calor o matriz de exposición al riesgo. Esta herramienta, permite determinar gráficamente el valor del riesgo donde se han considerado los valores asignados al impacto y a la probabilidad. Estos conceptos, se incluyen en una tabla de doble entrada para obtener la relación y Así establecer el nivel de riesgo para los diferentes escenarios.

La Tabla 15 presenta el mapa de calor asociado con la propuesta de niveles de riesgo definida en este mismo apartado.

Tabla 15. Mapa de calor

Mapa de Calor		Impacto				
		Bajo	Moderado	Medio	Alto	Muy alto
Probabilidad	**Valor**	**1**	**2**	**3**	**4**	**5**
Altamente probable	5					
Muy probable	4					
Probable	3					
Poco probable	2					
Improbable	1					

El valor del riesgo obtenido de multiplicar los valores de probabilidad e impacto, se conoce como **riesgo inherente.** Este valor representa el nivel de riesgo antes de considerar cualquier método de control que haya implementado la organización para gestionar el riesgo.

Dependiendo de las prácticas utilizadas para la gestión de riesgo en la organización, este valor puede ser modificado para que se ajuste a la escala organizacional y así facilitar el proceso de comunicación de resultados y valoración de controles. Por ejemplo, en algunos casos el riesgo residual se calcula como la raíz cuadrada del nivel de riesgo, obteniendo de esta forma un valor normalizado en relación con los valores del impacto y probabilidad.

Posteriormente, se debe calcular el **riesgo residual** que se refiere al nivel de riesgo que permanece al considerar los controles que la organización haya definido con anterioridad. Para ello, se debe llevar a cabo la valoración de los controles existentes, actividad que se describe en el siguiente apartado.

5.1.6.3.2.4 Valoración de controles existentes

El proceso a seguir para la identificación de controles consiste en las siguientes actividades:

- Levantar un borrador de los controles clave por medio de una sesión de lluvia de ideas de escritorio y una revisión de las distintas fuentes de información enlistadas.
- Verificar y analizar el comportamiento de los controles para determinar la efectividad de los mismos.
- Listar las debilidades encontradas en los controles existentes. En el caso de controles con poco tiempo de implementados donde no se haya identificado debilidades, se debe revisar cómo están operando.

Una vez que se han determinado los controles clave, las áreas dueñas de los procesos deben considerar los siguientes aspectos:

- ¿Cuáles son los puntos principales del control dentro de su proceso, actividad o función que previenen que ocurran pérdidas?
- En la ausencia del control, ¿los impactos del riesgo diferirían en severidad?
- ¿La Gerencia está dispuesta a tolerar el impacto si el control identificado falla y el riesgo se manifiesta? Si la respuesta es no, el control probablemente es clave.
- ¿Cuántos controles se han identificado?
- Verificar que los riesgos comunes o genéricos y los controles definidos para tales riesgos, han sido considerados.

Las áreas deberán asegurarse de contar con los expertos de las áreas de negocio pertinentes, con el fin de identificar los controles clave. Esto, considerando que muchas veces los servicios de TI repercuten en distintas áreas de negocio y por ello la efectividad de los controles impacta a dichas áreas. En algunos casos, puede resultar de utilidad, consultar los procesos de gestión de riesgos de las áreas involucradas y verificar la efectividad de los controles de los que dichas áreas son responsables.

Para cada uno de los controles identificados se debe registrar información importante que ayuda a la evaluación de la efectividad del control. La información que debe considerarse para este fin se describe a continuación:

- Título del control: Titulo corto que describa el control.

- Descripción del control: ¿por qué se implementa?, ¿quién o qué lo implementa? y ¿cómo se implementa? El control debe ser descrito específicamente, por ejemplo, no es suficiente establecer “Manual de procedimientos” como el control, la descripción debe especificar el procedimiento de control utilizado de forma detallada.
- Dueño del control: puede ser un individuo o un área específica que pueda proporcionar información detallada sobre el diseño y operación del control. Se debe ser tan específico como sea posible, considerando nombres de puestos y de las personas encargadas.
- Descripción amplia sobre el monitoreo del control: se debe especificar la forma en que se valida que el control se cumpla y la periodicidad con que se hace.
- Dueño del monitoreo del control: puede ser un individuo o un área específica que proporcione información detallada sobre el monitoreo y seguimiento que se da al control. Se debe ser tan específico como sea posible, considerando nombres de puestos y de las personas encargadas.
- Efectividad del control: Efectivo, Inefectivo, Necesita Mejorar.
- Tipo de control: Preventivo, Limitativo, Detectivo.
    - Preventivo. Es el que se lleva a cabo para evitar un incidente. Anticipa y reduce los errores, elimina los problemas potenciales desde el origen. Ejemplo: cifrado, autenticación, entre otros.
    - Limitativo. Se lleva a cabo para reducir el impacto de un incidente, una vez producido.
    - Detectivo. Se lleva a cabo para identificar / avisar cuando se produce un incidente. Detecta errores o incidentes que son difíciles de predecir. Detecta un incidente que está ocurriendo. Ejemplo: bitácoras o reportes.

Una vez que se han identificado los controles existentes y se ha registrado la información necesaria para cada uno de ellos, se debe expresar la valoración de cada control en términos numéricos. Para ello, se sugiere utilizar la escala de efectividad presentada en la Tabla 16.

Tabla 16. Escala de valoración de los controles

Descripción del control	Valor
Documentado y sujeto a revisión periódica	5
Se realiza formalmente y está documentado	4
Se realiza informalmente en forma total	3
Se realiza parcial e informalmente	2
No se realiza	1

Asignado el valor a los controles, este valor minimizará el nivel de riesgo establecido anteriormente y permitirá el cálculo del nivel de riesgo residual. La forma en que se combina el nivel de riego inherente con la valoración de los controles para definir el nivel de riesgo residual, dependerá del modelo de gestión de riesgos establecido por la organización.

En términos generales, al nivel de riesgo inherente, se le disminuye el valor de la efectividad de los controles y la diferencia corresponde con el riesgo residual, por ser el riesgo que permanece después de considerar los controles. Sin embargo, en algunas ocasiones el valor de los controles se promedia y se normaliza para coincidir con la escala de nivel de riesgo, mientras que en otros casos se aplica alguna fórmula especial para calcular el nivel de riesgo residual.

Este aspecto dependerá de lo indicado en la política de gestión de riesgos o bien, de las regulaciones a las que la organización esté sujeta.

5.1.6.3.3 Evaluación de riesgos

La evaluación de los riesgos consiste en comparar los valores producto del análisis de riesgos, con los parámetros establecidos en el contexto del riesgo. Esta etapa se ocupa de verificar si el nivel de riesgo se encuentra o no, dentro de los límites definidos por la organización.

En el caso de los riesgos que exceden el apetito de riesgo definido por el negocio, se debe continuar con el tratamiento de riesgos. Esta etapa se describe en el siguiente apartado.

5.1.6.4 Tratamiento de riesgos

Se enfoca en desarrollar un proceso de respuesta a los riesgos y aplicar un adecuado manejo y control de la exposición del riesgo en forma continua. Incluye la identificación de las estrategias para responder a cada uno de los riesgos.

El tratamiento de riesgos es un proceso iterativo que busca reducir el nivel de riesgo hasta que este sea aceptable para el negocio. Cuando se ha seleccionado una respuesta para un riesgo específico, se debe valorar dicho riesgo nuevamente y decidir si está listo para ser aceptado o si requiere la aplicación de una nueva respuesta o un cambio en la estrategia.

Para el tratamiento de los riesgos, con base en la guía COBIT 5 para Riesgos, se puede optar por alguna de las siguientes estrategias:

Evitar el riesgo

Consiste en no realizar las actividades que dan espacio al riesgo. Aplica cuando ninguna otra respuesta al riesgo es adecuada. Por ejemplo, cuando las posibles respuestas no son costo efectivas o la exposición al riesgo es demasiado inaceptable para el negocio (ISACA, 2013).

Aceptar el riesgo

La exposición a pérdidas es reconocida y aceptada. No se toma acción alguna para atender un riesgo específico y las pérdidas serán aceptadas cuando ocurran. La decisión de aceptar un riesgo corresponde a los altos niveles de la organización y debe quedar documentada y ser comunicada (ISACA, 2013).

Compartir/transferir el riesgo

Significa reducir la probabilidad o el impacto de un riesgo transfiriendo o compartiendo una parte del riesgo con otra entidad. Algunas técnicas comunes son la adquisición de pólizas de seguro o bien, tercerizar las operaciones o proyectos que implican riesgos relevantes (ISACA, 2013).

Mitigar el riesgo

Se refiere a tomar acciones de mitigación para reducir le frecuencia o el impacto de un riesgo. Formas comunes de mitigación incluyen reforzar los procesos de gestión de TI, implementar controles con ayuda de COBIT 5 o utilizar otras prácticas conocidas y marcos de referencia (ISACA, 2013).

Para la selección de una respuesta de riesgos, la organización debe considerar los siguientes factores:

- Eficiencia de la respuesta. Se puede comparar con otras respuestas.
- Exposición o posición del riesgo atendido en el mapa de riesgos.
- Capacidad de la organización para implementar la respuesta.
- Efectividad de la respuesta, cómo reducirá el nivel del riesgo.

La organización, no siempre estará en capacidad de implementar las respuestas más efectivas para el tratamiento de riesgos. Es por esto que las respuestas identificadas deben priorizarse según los criterios establecidos por la organización. Un modelo sugerido de categorías para la priorización de respuestas es el siguiente:

- Prioridad alta. Respuestas efectivas y muy eficientes en costo ante riesgos altos.
- Prioridad normal. Respuestas costosas o difíciles ante riesgos altos o respuestas efectivas ante riesgos de menor nivel.
- Prioridad baja. Respuestas a riesgos bajos y que pueden no ser efectivas.

5.1.6.5 Monitoreo y revisión

Es la planeación y supervisión del sistema de gestión del riesgo y cualquier cambio que pueda afectarlo. Para administrar los riesgos es conveniente que se prepare en el área o unidad un plan de manejo de riesgos y en caso de estar en presencia de riesgos intolerables debe, además, tener un plan de contingencia.

La revisión de riesgos consiste en el seguimiento sobre el comportamiento de los riesgos, así como el seguimiento a la eficacia y eficiencia de las medidas para su administración que se estén ejecutando.

Se realiza analizando el avance del plan de monitoreo o seguimiento. Es necesario que cada colaborador monitoree los riesgos identificados en su área o unidad, de manera continua, teniendo en cuenta que éstos no dejan de representar una amenaza para la organización, aunque tengan un perfil bajo.

Esta etapa es esencial para asegurar que las acciones se están llevando a cabo y para evaluar la eficiencia en su implementación, adelantando revisiones sobre la marcha para

evidenciar todas las situaciones o factores que pueden estar influyendo en la aplicación de las acciones preventivas.

La organización además deberá definir indicadores clave para medir el desempeño de la gestión de riesgos. Estos indicadores varían dependiendo de los lineamientos organizacionales o de la normativa a la que se encuentre ligada la empresa.

5.1.7 Registro y documentación de riesgos

Es una actividad permanente del proceso de gestión de riesgos de TI que consiste en el registro y la sistematización de la información asociada con los riesgos y el análisis realizado. Esta documentación incluye los informes periódicos de seguimiento.

El objetivo es que la organización cuente con información de respaldo y que además sirva como base de conocimiento sobre la gestión de riesgos de TI que se realiza. Registrar y documentar adecuadamente el proceso y las acciones tomadas para la gestión de riesgos, creará un procedimiento más limpio, que pueda ser recordado y repetido por los colaboradores con mayor facilidad.

Se documentan o registran todos los datos, informaciones o reportes relacionados con los riesgos y las medidas que se generan en cada actividad de la gestión de riesgos. Desde el principio, se deben registrar de forma continua los distintos componentes del proceso de gestión de riesgos de TI (contexto, identificación, análisis, evaluación, tratamiento, informes de seguimiento, entre otros).

Conclusiones

6 Conclusiones

Con el desarrollo de este trabajo final de graduación, se determina el estado de los objetivos planteados inicialmente. Completado el procedimiento metodológico del trabajo, es posible concluir respecto a los objetivos del mismo, que:

1. Deloitte global cuenta con una base de conocimiento y con información disponible para el desarrollo de proyectos relacionados con la gestión de riesgos de tecnología de información. La información de esta base de conocimiento, está basada principalmente en mejores prácticas y estándares internacionales. Sin embargo, se determinó que la información disponible en esta base de conocimiento, no se utiliza en la totalidad de los servicios ofrecidos por la Firma. En ninguno de los proyectos revisados hay evidencia de que se haya utilizado esta base de conocimientos.

2. Los proyectos relacionados con gestión de riesgos de TI que son desarrollados por la Firma y que fueron analizados como parte de este trabajo, no siguen un esquema estandarizado que se base en una metodología o proceso definido. Más bien, se utiliza información de diferentes proyectos anteriores, para articular soluciones, ocasionando en algunos casos, la presencia de errores o inconsistencias en la solución entregada.

3. Para identificar los marcos de referencia y mejores prácticas a utilizar en el desarrollo de la Propuesta de Metodología, se indagaron y analizaron marcos de referencia y estándares COBIT 5, ISO 31000, COBIT 5 para Riesgos, ISO 27005, OCTAVE, COSO, MAGERIT y Normativas SUGEF, cuyas prácticas y actividades de riesgos cimentaron la base de la Propuesta de este Trabajo Final de Graduación.

4. Del análisis de marcos de referencia, mejores prácticas y estándares, se concluye que el marco de referencia COBIT 5 contempla prácticas de gobierno y gestión de tecnología de información que abarcan las organizaciones de extremo a extremo, reconociendo las responsabilidades de la gestión de TI a todos los involucrados del negocio; y su enfoque permite la gestión de riesgos con responsabilidades más allá de los gestores de TI; y que el estándar internacional ISO 31000, engloba el ciclo de gestión de riesgos mayormente utilizado por gran cantidad de marcos y prácticas internacionales, debido a su estandarización y conceptualización de las actividades de ese ciclo de riesgos.

5. Producto del análisis y conceptualización de las mejores prácticas de la industria y estándares internacionales se concuerda, con la empresa contratante, que los marcos COBIT 5 e ISO 31000, sugeridos para la propuesta de la metodología de riesgos, efectivamente cumplen con los requerimientos de estandarización y las demás necesidades expuestas por la Firma.

6. COBIT 5 para Riesgos, es una guía adecuada para la creación de una metodología de gestión de riesgos basada en COBIT 5. Esta guía considera el uso de los principios y mecanismos definidos por COBIT 5, para garantizar los aspectos necesarios de una adecuada gestión de riesgos de TI según el mismo marco COBIT 5, la norma ISO 31000 y los demás marcos y prácticas analizados.

7. Se propuso una Metodología de gestión de riesgos de TI, que considera las prácticas que Deloitte utilizó en proyectos anteriores, que está basada en el marco de referencia COBIT 5 y el ciclo de gestión de riesgos de ISO 31000 y que constituye una herramienta para el cumplimiento de las necesidades de la región y de la Firma específicamente.

Recomendaciones

7 Recomendaciones

Como resultado de realizar el trabajo final de graduación, este capítulo presenta una serie de recomendaciones que se brindan a la organización para que cuente con un enfoque adecuado en sus proyectos relacionados con gestión de riesgos de TI.

1. Utilizar en los proyectos de gestión de riesgos de TI, prácticas actualizadas y vigentes en relación con la base de conocimiento que posee la Firma a nivel global. Esto, con el objetivo de aprovechar ampliamente los recursos disponibles y mantener los estándares de calidad en el desarrollo de proyectos para los clientes.

2. Aplicar una metodología de gestión de riesgos estandarizada, como la propuesta en este trabajo final de graduación, en los distintos proyectos que realiza la Firma para sus clientes. De esta forma, todos los proyectos seguirán un enfoque metodológico definido, reduciendo las inconsistencias en las soluciones entregadas a los clientes.

3. Velar por que las actualizaciones futuras que se realicen a la metodología de riesgos propuesta en este trabajo, consideren los marcos de referencia seleccionados por Deloitte. Esto, con el fin de obtener el máximo provecho en la implementación de la metodología con los clientes de la Firma y conservar una metodología de riesgos actualizada y en congruencia con las mejores prácticas de la industria a lo largo del tiempo.

4. Preferir siempre los marcos de referencia y mejores prácticas reconocidos en la industria y que son desarrollados a partir del conocimiento, la experiencia y las recomendaciones de una gran cantidad de profesionales además de considerar otros marcos conocidos y probados.

5. Estar pendiente de los cambios y actualizaciones que se presenten en los marcos de referencia utilizados. Lo anterior con el propósito de validar si dichos marcos, continúan siendo los más adecuados para la organización. De esta forma, además, se mantendrá vigente la metodología propuesta en este trabajo en relación con las mejores prácticas utilizadas.

6. Aprovechar las guías oficiales adicionales sobre mejores prácticas o normas que son emitidas por las organizaciones propietarias de los marcos de referencia. Un ejemplo de esto, es la guía COBIT 5 para Riesgos, utilizada como parte fundamental de este trabajo de graduación. Estas guías, incluyen información de gran importancia y complementan la implementación de mejores prácticas en la metodología de la organización.

7. Utilizar la Metodología de gestión de riesgos de TI, entregada como resultado de este trabajo, en todos los proyectos de la firma que contemplen la gestión de riesgos de tecnología de información. La metodología propuesta, considera las mejores prácticas aplicables, las prácticas realizadas anteriormente por la Firma y se ajusta a los distintos requerimientos de los sus clientes.

Apéndices y Anexos

8 Apéndices

En este capítulo, se presenta una serie de herramientas, plantillas e instrumentos desarrollados como parte del trabajo final de graduación. Estos artefactos, permiten llevar a cabo las actividades de la investigación como las sesiones para recolectar información.

En cada apéndice se encuentra definido el objetivo del mismo y cualquier otra información necesaria para su uso.

Apéndice A: Formulario para la observación de documentos

Este apéndice presenta el formulario utilizado para la revisión de documentos generados por Deloitte en proyectos anteriores relacionados con la gestión de riesgos de tecnología de información. La información recopilada, permitirá conocer la forma en que se ha atendido los proyectos anteriormente.

Revisión de documentos de proyectos realizados en Deloitte

Esta herramienta permite recopilar la información sobre documentos de proyectos relacionados con gestión de riesgos de TI. Esta información representa un insumo importante en el desarrollo de una propuesta para la gestión de riesgos de TI. La herramienta se debe completar una vez por cada proyecto que sea analizado.

Para la revisión de cada proyecto se contemplan dos tipos de información. La primera, consiste en información general del proyecto. Esta se debe recopilar de manera estructurada y uniforme, es decir, se debe incluir la misma información para cada proyecto. El segundo tipo de información, puede variar para cada uno de los proyectos, pues pretende extraer, de cada documento revisado, los aspectos relevantes para la Propuesta de Metodología para la gestión de riesgos de TI.

Información general del proyecto

Se debe completar la siguiente tabla con la información general del proyecto que se revisa.

Nombre del proyecto:	
Descripción breve:	Relevancia para la investigación:

Resumen de documentos revisados

Para cada uno de los documentos revisados, se debe anotar en la siguiente tabla los aspectos relevantes que el investigador considere relevantes para el desarrollo de su trabajo.

Documento revisado	**Consideraciones para el trabajo**
Anotar el nombre de documento	Resumir aquí los aspectos del documento que resultan relevantes para la investigación.

Apéndice B: Guía para entrevistas

En este apéndice, se presenta la guía para la entrevista semiestructurada a realizar con consultores que han trabajado en proyectos anteriores. Con la realización de esta entrevista, se obtendrá información sobre las prácticas que la firma ha utilizado al brindar servicios relacionados con la gestión de riesgos de TI. Así mismo, la entrevista permitirá obtener información de utilidad para la Propuesta de Metodología, con base en la experiencia del personal de Deloitte.

Entrevista semiestructurada sobre prácticas utilizadas por Deloitte en proyectos de gestión de riesgos de TI

En esta entrevista se solicitará información, de forma abierta, sobre la experiencia en proyectos de gestión de riesgos de TI. Es de utilidad la información sobre la situación encontrada en las empresas clientes, las necesidades encontradas y lo que Deloitte ha hacho para solventarlas. Además, resulta importante conocer los vacíos o brechas que presenta la metodología de Deloitte, en relación con las necesidades de los clientes y de los consultores para atender adecuadamente los proyectos.

La entrevista, que tiene una duración estimada de 30 minutos, será aplicada en las oficinas centrales de Deloitte Costa Rica y la información brindada por los entrevistados será utilizada únicamente para el desarrollo de este Trabajo Final de Graduación.

Al tratarse de una investigación cualitativa, se debe anotar las observaciones y detalles que indique el entrevistado. Además, el entrevistador y el entrevistado pueden conversar sobre los temas discutidos, y tomar esto como parte de la información recopilada.

A continuación, se presentan las preguntas utilizadas como guía para el desarrollo de la entrevista.

Preguntas

Las preguntas que guiarán la entrevista son las siguientes:

1. ¿Cuál es el procedimiento o metodología que utiliza Deloitte actualmente para la gestión de riesgos de TI?
    a. ¿Cuál es el ciclo de gestión de riesgos de TI utilizado?
    b. ¿El proceso o metodología está basado en alguna mejor práctica o marco de referencia? ¿Cuál?

2. ¿Cuál es la situación de los clientes que usted ha atendido, en relación con la gestión de riesgos de TI?
    a. ¿Los clientes que usted ha atendido contaban con una metodología establecida para la gestión de riesgos de TI?
    b. ¿Qué necesidades presentaron esos clientes en relación con la gestión de riesgos de TI?

3. ¿Es necesaria una metodología de gestión de riesgos de TI para facilitar y potenciar la labor de los consultores en este tipo de proyectos?
    a. ¿En algunos de los proyectos atendidos, fue necesario “inventar” o desarrollar algo desde cero?
    b. ¿Se ha dado una afectación negativa a los proyectos, en temas de alcance, tiempo, costo, etc.; debido a la ausencia de una metodología?

4. ¿Considera que existe una brecha entre las necesidades de los clientes o lo que se ofrece en los contratos y la metodología que utiliza la firma? ¿Por qué?

Apéndice C: Guía para realización de grupo focal

Este apéndice presenta la guía para llevar a cabo un grupo focal con personal de la firma Deloitte que resulte relevante para la investigación. Con la aplicación de esta herramienta se podrá validar la teoría a utilizar en la Propuesta de Metodología, así como los aspectos principales de dicha propuesta de acuerdo con las necesidades y la experiencia de la organización.

Grupo focal sobre Propuesta de Metodología para la Gestión de riesgos de TI

Esta herramienta consiste en la guía para efectuar una discusión enfocada sobre el tema de gestión de riegos de TI con los principales interesados de la firma Deloitte. Durante la aplicación de esta herramienta, se podrá validar la aplicabilidad de la información recopilada sobre mejores prácticas en el desarrollo de la Propuesta de Metodología. Así mismo, la información generada con la aplicación de esta herramienta (opiniones, correcciones, conclusiones, recomendaciones, entre otras) permitirá dar forma a la Propuesta de Metodología para la gestión de riesgos de TI.

A continuación, se muestra la presentación de diapositivas a utilizar con los participantes del grupo focal. Para el desarrollo de la presentación se utilizó el programa *Microsoft Power Point 2016*. La presentación se encuentra estructurada en dos partes: una serie de aspectos generales y un conjunto de preguntas relacionadas con la teoría identificada y la Propuesta de Metodología. Estas preguntas serán las que guíen la discusión sobre qué aspectos de la teoría se ajustan a las necesidades de la organización y cómo deberían reflejarse en la Propuesta de Metodología.

Presentación de diapositivas para el grupo focal

Contenido

01 Aspectos generales
- Descripción
- Alcance
- Tiempo
- Reglas

02 Mejores prácticas
- Gobierno vs Gestión
- Perspectivas de riesgo
- Habilitadores de COBIT
- Ciclo de gestión de riesgos
- Factores de riesgo
- Escenarios de riesgo
- Respuesta a riesgos

03 Consideraciones adicionales

Grupo focal gestión de riesgos de TI – Trabajo Final de Licenciatura en Adm. de TI 2

Aspectos generales

Descripción

Esta herramienta pretende compartir el conocimiento identificado en la revisión de literatura, validar su aplicabilidad en los proyectos de la Firma y generar insumos para la propuesta de metodología.

Alcance

El trabajo de esta sesión contemplará únicamente el conocimiento identificado en la revisión de literatura que se efectuó como parte del Trabajo Final de Graduación.

Para participar en la sesión de trabajo se toma en cuenta únicamente a colaboradores de *Risk Advisory* de Deloitte Costa Rica. En concreto, se pueden involucrar gerentes, directores o socios.

Grupo focal gestión de riesgos de TI – Trabajo Final de Licenciatura en Adm. de TI 5

Tiempo

Para el desarrollo de la sesión se cuenta con un tiempo máximo de dos horas. En este tiempo, el moderador guiará la discusión para mantenerla centrada en el propósito de la sesión.

Grupo focal gestión de riesgos de TI – Trabajo Final de Licenciatura en Adm. de TI 6

Algunas reglas

El moderador solo es un guía, su opinión no debe tener efecto en las opiniones e intervenciones de los participantes.

Se debe acatar las indicaciones del moderador, no adelantarse ni atrasarse.

La idea es mantener un ambiente de discusión más bien informal.

No hacer preguntas al moderador sobre el contenido.

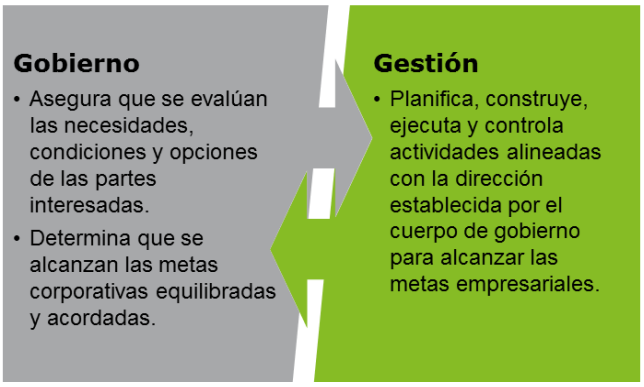
Se debe trabajar en equipo, todos son igual de importantes.

Grupo focal gestión de riesgos de TI – Trabajo Final de Licenciatura en Adm. de TI 7

Mejores prácticas

Gobierno versus gestión

¿Son los siguientes aspectos adecuados para la metodología de Deloitte?
¿Se puede prescindir de alguno o realizar alguna variante?



Grupo focal gestión de riesgos de TI – Trabajo Final de Licenciatura en Adm. de TI 9

Perspectivas de Riesgo (COBIT 5 para Riesgos)

¿Estas perspectivas representan adecuadamente lo que Deloitte debe desarrollar con sus clientes? A nivel general ¿Qué aspectos se deben contemplar en cada una de ellas?

Grupo focal gestión de riesgos de TI – Trabajo Final de Licenciatura en Adm. de TI 10

Habilitadores COBIT para la Función de riesgo

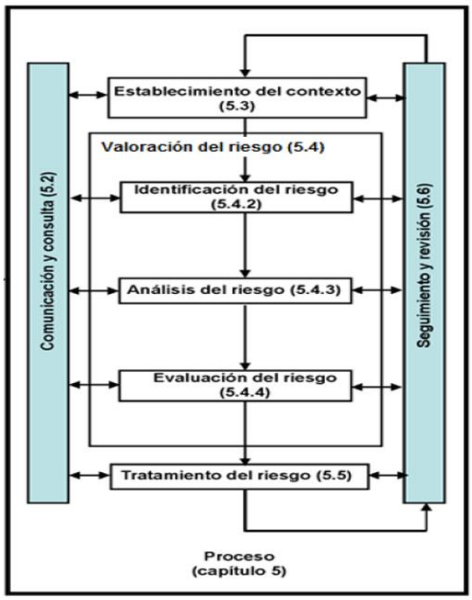
¿Es esta la forma correcta de utilizar los habilitadores de COBIT en la función de riesgos? ¿Qué recomendaciones se pueden efectuar?

Grupo focal gestión de riesgos de TI – Trabajo Final de Licenciatura en Adm. de TI 11

Ciclo de gestión de riesgos

¿Es adecuado el ciclo de gestión de riesgos?

¿En qué aspectos se concentra el aporte de la Firma?



Grupo focal gestión de riesgos de TI – Trabajo Final de Licenciatura en Adm. de TI 12

Factores de riesgo

¿Son adecuadas las categorías?
¿Se debe agregar o eliminar algunos factores?

Grupo focal gestión de riesgos de TI – Trabajo Final de Licenciatura en Adm. de TI 13

Escenarios de riesgo

¿Es adecuada la estructura propuesta para los escenarios de riesgo?
¿Se debe recomendar una lista genérica de escenarios de riesgo en las organizaciones?

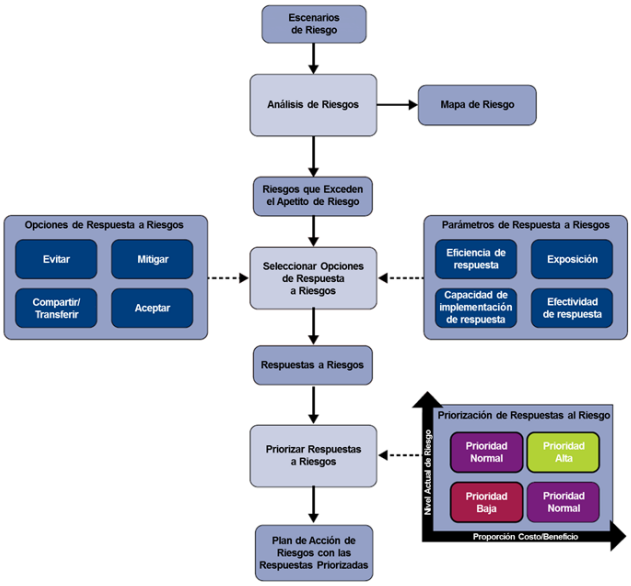
Grupo focal gestión de riesgos de TI – Trabajo Final de Licenciatura en Adm. de TI 14

Respuesta a riesgos. Opciones, parámetro priorización.

¿El flujo de respuesta a riesgos que se muestra es adecuado para el trabajo de la firma?

¿Cómo se deben gestionar las opciones y los parámetros de selección de respuestas?

¿Cuál es el mecanismo más adecuado para la priorización de respuestas?



Grupo focal gestión de riesgos de TI – Trabajo Final de Licenciatura en Adm. de TI 15

Comentarios adicionales, validación y cierre

¿Algo más qué agregar?

En resumen

Deloitte.

Apéndice D: Cuestionario para empresas clientes de Deloitte

Este apéndice consiste en un cuestionario desarrollado para aplicarlo a los sujetos de información de las empresas clientes de Deloitte. Su principal objetivo es identificar si los clientes o potenciales clientes de proyectos relacionados con gestión de riesgos de TI, cuentan con estructuras organizacionales, con una gobernanza claramente definida o con un marco normativo que permita la utilización de la Propuesta de Metodología.

Cuestionario sobre Gestión de Riesgos de TI

Este cuestionario es parte de un estudio que realiza la firma Deloitte con el objetivo de mejorar sus servicios relacionados con la Gestión de Riesgos de TI. Su participación es de gran importancia, porque permite a la Firma conocer mejor sus necesidades actuales y así brindar servicios que generen un impacto en las organizaciones, en la industria y en la sociedad.

El cuestionario está organizado en tres secciones y no le llevará más de 5 minutos completarlo. Sírvase seleccionar una o más de las respuestas disponibles según se indique en cada pregunta.

Gobierno empresarial de riesgos

En esta sección se evalúa la existencia de estructuras y políticas relacionadas con el gobierno de riesgos en su organización. Sus respuestas nos permitirán medir la importancia de realizar un análisis previo a la puesta en marcha de los proyectos o bien, de proponer una reestructuración que facilite el gobierno de los riesgos.

1. ¿Hay una función de riesgos en su empresa?
   Puede ser un departamento, unidad o rol dependiendo del tamaño de la organización.

   SÍ ( ) NO ( )

2. ¿Cuáles de las siguientes políticas relacionadas con riesgos de TI existen en su organización?
   Seleccione todas las que apliquen

   ( ) Política organizacional sobre riesgos.
   ( ) Política de seguridad de la información.
   ( ) Política de continuidad del negocio.
   ( ) Política de administración de proyectos.
   ( ) Política de privacidad de los datos.

3. ¿Hay un comité organizacional de riesgos?
   Usualmente este grupo se encarga de las decisiones estratégicas sobre riesgos y del gobierno de los mismos.

   SÍ ( ) NO ( )

4. ¿Se encuentran definidos el apetito y la tolerancia de riesgo en la organización? ¿Quién se encargó de definir esos conceptos?

   ( ) No se encuentran definidos.
   ( ) Definidos por el equipo directivo o junta de administración.
   ( ) Definidos por un comité organizacional de riesgos.
   ( ) Definidos por el gestor o encargado de riesgos.

Gobierno de Tecnología de Información

En esta sección se evalúa la existencia de estructuras, políticas y procesos relacionados con la tecnología de información en su empresa. La información brindada permitirá conocer la robustez de la función de TI en las organizaciones y por tanto qué tan flexible debiera ser la metodología utilizada por la Firma en sus servicios de riesgo de TI.

5. ¿Hay un comité o grupo directivo de TI en su empresa?
   Usualmente este grupo se encarga de las decisiones estratégicas y del gobierno de TI.

   SÍ ( ) NO ( )

6. ¿Hay un proceso implementado para el control interno de TI?
   Marque con una X la opción que mejor describa el proceso de control interno de TI.

   ( ) No hay un proceso de control interno establecido.
   ( ) Hay un proceso de control interno basado en COBIT 5 (Proceso MEA02).
   ( ) Hay un proceso de control interno basado en otras prácticas y/o normativas.
   ( ) Hay un proceso de control interno empírico, creado en la empresa.

7. ¿Existe un esquema de clasificación de la información o privacidad de los datos?

   SÍ ( ) NO ( )

8. ¿En los proyectos de TI se presupuestan aspectos relacionados con la gestión de riesgos?

   SÍ ( ) NO ( )

Gestión de riesgos

En esta sección se pretende conocer la forma de gestionar el riesgo tecnológico en las organizaciones. La información que usted nos brinde, facilitará el diseño de un proceso óptimo para la gestión de riesgos de TI.

9. ¿Se conocen los escenarios de riesgo que podrían afectar a TI y a la organización?

   SÍ ( ) NO ( )

10. ¿Hay un ciclo o proceso establecido para la gestión de riesgos de TI en su empresa?

    SÍ ( ) NO ( )

11. ¿Los riesgos de TI identificados, son evaluados para determinar si deben atenderse?

    SÍ ( ) NO ( )

12. ¿Hay un portafolio de acciones definidas para atender los diferentes riesgos relacionados con TI?

    SÍ ( ) NO ( )

13. ¿Se da seguimiento y se realiza un monitoreo de la gestión de riesgos de TI?

    SÍ ( ) NO ( )

Se ha completado el cuestionario.

Gracias por su participación.

Apéndice E: Resultados de la observación documental

En este apéndice se incluyen las principales anotaciones y apreciaciones recopiladas por el investigador en el proceso de observación efectuado a documentos de la empresa sobre proyectos anteriores. Los resultados incluidos en este apéndice, facilitan el entendimiento de las prácticas utilizadas por la empresa en proyectos anteriores de gestión de riesgos de TI.

Bitácora de revisión documental

Durante la revisión de documentos se utilizó una bitácora para registrar las principales observaciones y aspectos relevantes identificados en los documentos.

La documentación revisada pertenece a distintos proyectos realizados por la firma Deloitte, por tanto, el formulario de revisión se completó una vez por cada proyecto. De esta forma, la información se encuentra organizada por proyectos. A continuación, se puede revisar el detalle de cada proyecto revisado.

Es importante anotar que, debido a las políticas de privacidad y confidencialidad a las que se encuentran sujetos los proyectos que realiza la firma Deloitte, alguna información no se puede incluir en esta bitácora.

Proyecto I

Este proyecto inició en el año 2015 y finalizó a principios de 2017. Se realizó para un cliente del sector bancario/financiero.

Nombre del proyecto:	
Implementación de COBIT 4.1 para *un cliente del sector financiero*	
Descripción breve:	Relevancia para la investigación:
El proyecto consistió en implementar los procesos del marco COBIT 4.1 para la gestión de TI en un banco privado. El proyecto inició debido a la necesidad de la entidad bancaria de cumplir con la normativa nacional sobre gestión de TI que sugiere la implementación de los procesos de COBIT 4.1.	Como parte del proyecto se implementó el proceso de gestión de riesgos de TI y se estableció una metodología para la gestión de riesgos en el cliente.

Documento revisado	Consideraciones para el trabajo
Ficha del Proceso PO09 (Evaluar y administrar riesgos de TI).	Este documento contiene un resumen de la estructura y el proceso establecido para la administración de riesgos de TI. Incluye los indicadores de desempeño, una matriz de responsabilidades y los riesgos que debe considerar la organización sobre el proceso. Un detalle importante de este documento es que se utilizan los lineamientos sugeridos por la mejor práctica, pero siempre considerando la realidad de la organización. Por ejemplo, la matriz RACI definida es similar a la que sugiere el marco COBIT, pero considera los roles existentes en la organización en lugar de nombres genéricos de roles o puestos.

Documento revisado	Consideraciones para el trabajo
Procedimiento creado para la gestión de riesgos de TI.	Este documento contiene el procedimiento desarrollado para la administración de riesgos de TI en el cliente. El procedimiento entregado como parte del proyecto, considera las tareas sugeridas por el marco COBIT 4.1: • Marco de trabajo de Administración de Riesgos • Establecimiento del Contexto de Riesgos • Identificación de Eventos • Evaluación de Riesgos de TI • Respuesta a los Riesgos • Mantenimiento y Monitoreo de un Plan de Acción de Riesgos
Informe de evaluación del Proceso PO09.	Este documento consiste en una evaluación que se realiza una vez implementado el proceso por parte un consultor o auditor de Deloitte, para verificar que el trabajo efectuado cumple con los lineamientos establecidos. En el informe de evaluación se verifica la implementación de cada una de las tareas sugeridas por COBIT para el proceso PO09 y se concluye que estas tareas se encuentran documentadas y acorde con lo que establece el marco de referencia.

Apéndice F: Resultados de la entrevista sobre prácticas utilizadas por Deloitte

Este apéndice contiene los resultados de la entrevista a aplicada a una consultora senior de *Risk Advisory* sobre su experiencia y las prácticas utilizadas por la Firma en proyectos relacionados con gestión de riesgos de TI. Los resultados incluidos en este apéndice, facilitan el entendimiento de las prácticas utilizadas por la empresa en proyectos anteriores de gestión de riesgos de TI.

Minuta de la entrevista

Minuta de Reunión | TEC-TFG-RiesgosDeloitte-2017

Minuta de Reunión D07

Tema: Entrevista sobre las prácticas que venía utilizando la firma para los proyectos relacionados con gestión de riesgos de TI.

Fecha: 15 de mayo de 2017

Modalidad de la reunión: Presencial en Deloitte

Inicia: 15:45

Finaliza: 16:15

Participantes	Departamento/Organización	Firma
Diana Ramírez Cascante	Consultora Senior Risk Advisory - Deloitte	
Jean Carlo Alfaro Campos	Estudiante - TEC	

Agenda de la Reunión
• Entrevista sobre la gestión de riesgos de TI en los proyectos/servicios que brinda la firma.

Temas y Acuerdos Tomados
• El estudiante explica de qué se trata la entrevista y cuál es su principal objetivo. • La entrevistada comprende los objetivos y la mecánica de la entrevista. • Se procede con el desarrollo de la entrevista. Es una entrevista semi-estructurada con 4 preguntas guía que se subdividen en un máximo de dos temas o enfoques por pregunta. • Durante el desarrollo de la entrevista surgen algunas cuestiones y aclaraciones adicionales que son resueltas por el entrevistador o por la entrevistada. • Se acuerda aclarar cualquier duda adicional a través de la plataforma de comunicación de la empresa o de manera presencial de ser posible.

Tarea	Responsable
Preparar y enviar la Minuta de la reunión.	Jean Carlo Alfaro

Página 1 de 1

Apéndice G: Resultados del grupo focal

En este apéndice contiene los resultados obtenidos producto del grupo focal realizado a funcionarios de Deloitte. Los resultados del grupo focal permitirán identificar el criterio y dirección de la Firma para la escogencia de las mejores prácticas recomendadas para la elaboración de la Propuesta de metodología de gestión de riesgos.

Minuta del grupo focal

Minuta de Reunión | TEC-TFG-RiesgosDeloitte-2017

Minuta de Reunión D09

Tema: Grupo focal sobre la teoría identificada en la revisión de literatura y su aplicabilidad en la Propuesta de Metodología para la Gestión de riesgos de TI.
Fecha: 19 de mayo de 2017
Lugar: Oficinas de Deloitte en Costa Rica
Inicia: 15:00
Finaliza: 17:00

Participantes	Departamento/Organización	Firma
Andrés Casas	Socio líder - Risk Advisory - DTT	
Karla Robles	Gerente senior - Risk Advisory - DTT	
Karol Rojas	Tutora de TFG Gerente - Risk Advisory - DTT	
Daniel Gómez	Gerente - Risk Advisory - DTT	
Pablo Vásquez	Desarrollo del negocio - Risk Advisory - DTT	
Jean Carlo Alfaro	Estudiante - TEC	

Agenda de la Reunión

- Aspectos generales sobre la dinámica de trabajo, los objetivos de la sesión y algunas reglas.
- Presentación y validación de los distintos aspectos considerados a partir de las mejores prácticas.
- Comentarios adicionales y cierre.

Temas y Acuerdos Tomados

- Aspectos generales sobre la dinámica de trabajo, los objetivos de la sesión y algunas reglas.
  - Se presenta la descripción, el alcance, tiempo y reglas para el desarrollo de la sesión.
- Presentación y validación de los distintos aspectos considerados a partir de las mejores prácticas. Se analizan los siguientes aspectos:
  - Gobierno vs Gestión
  - Perspectivas de riesgo
  - Habilitadores de COBIT
  - Ciclo de gestión de riesgos
  - Factores de riesgo
  - Escenarios de riesgo
  - Respuesta a riesgos
- Comentarios adicionales y cierre.
  - Los participantes están de acuerdo con los aspectos discutidos y dan su aprobación.
  - Recomiendan considerar las posibles variantes al proceso de gestión de riesgos.
- Los resultados detallados de la sesión grupal, se podrán encontrar en el documento Informe del Trabajo Final de Graduación.

Tarea	Responsable
Preparar y enviar la Minuta de la reunión.	Jean Carlo Alfaro

Página 1 de 1

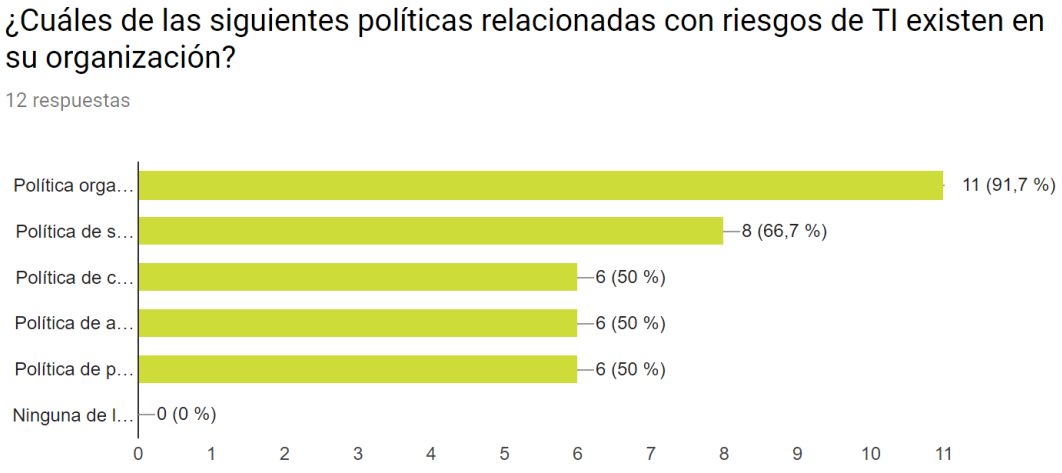
Apéndice H: Resultados del cuestionario a empresas clientes

Este apéndice presenta los resultados del cuestionario que fue aplicado a las organizaciones clientes de Deloitte. La información comprendida en este apéndice, facilita la comprensión del contexto en donde se aplicará la Propuesta de Metodología.

Respuestas de las organizaciones al cuestionario sobre gestión de riesgos de TI

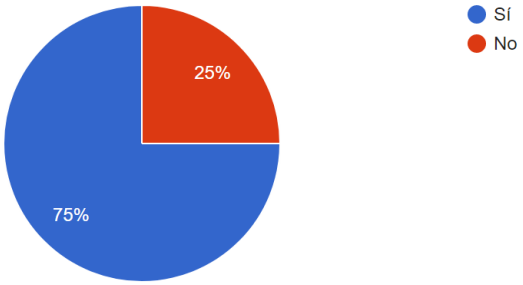
El cuestionario aplicado como parte de este trabajo final de graduación, fue contestado por un total de 12 organizaciones del sector financiero, educativo, gubernamental y tecnológico. Por motivos de confidencialidad y políticas propias de DTTL, no se puede presentar ningún dato que identifique o permita suponer la identidad de alguna de las organizaciones que completaron el cuestionario.

El cuestionario fue aplicado mediante la herramienta *Google Forms* y en seguida se muestran los resultados generados por esta herramienta.



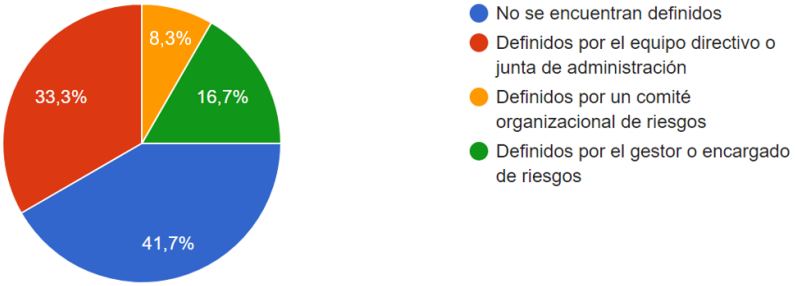
¿Hay un comité organizacional de riesgos?

12 respuestas



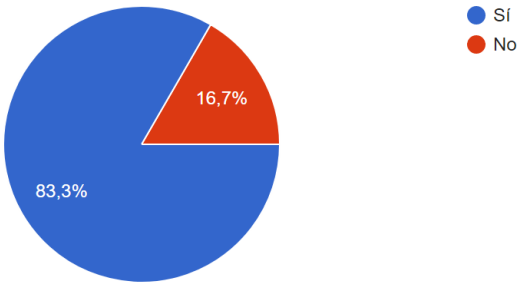
¿Se encuentran definidos el apetito y la tolerancia de riesgo en la organización? ¿Quién se encargó de definir esos conceptos?

12 respuestas



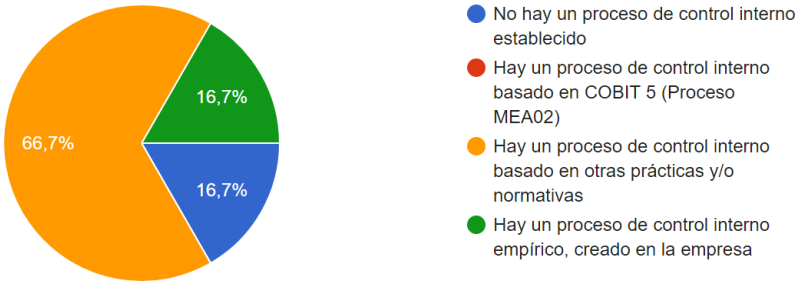
¿Hay un comité o grupo directivo de TI en su empresa?

12 respuestas



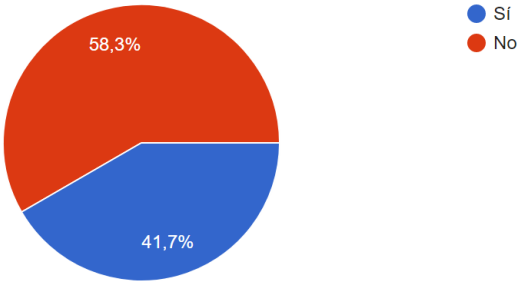
¿Hay un proceso implementado para el control interno de TI?

12 respuestas



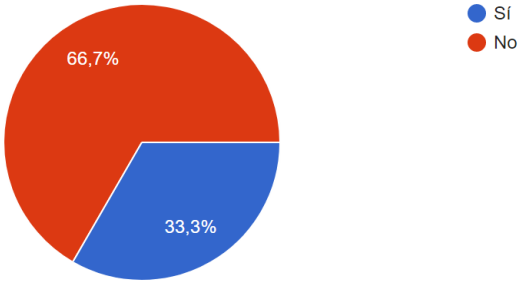
¿Existe un esquema de clasificación de la información o privacidad de los datos?

12 respuestas



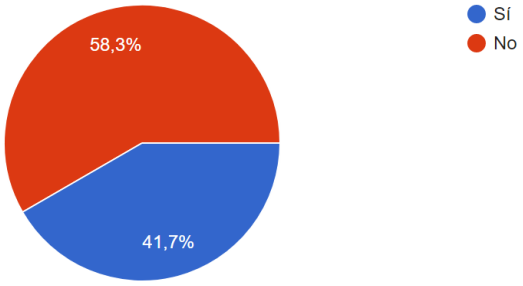
¿En los proyectos de TI se presupuestan aspectos relacionados con la gestión de riesgos?

12 respuestas



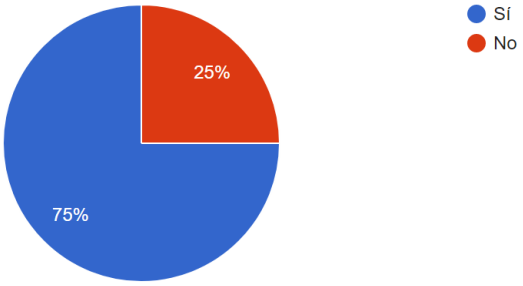
¿Se conocen los escenarios de riesgo que podrían afectar a TI y a la organización?

12 respuestas



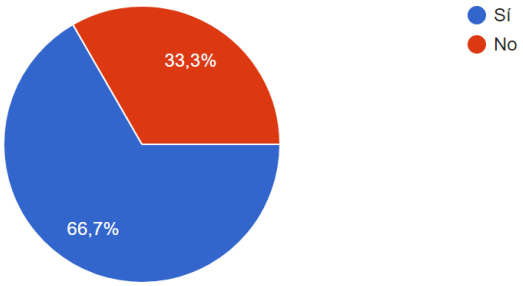
¿Hay un ciclo o proceso establecido para la gestión de riesgos de TI en su empresa?

12 respuestas



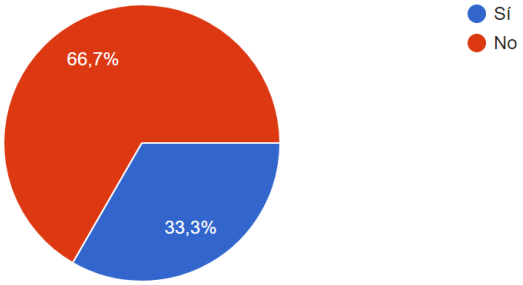
¿Los riesgos de TI identificados, son evaluados para determinar si deben atenderse?

12 respuestas



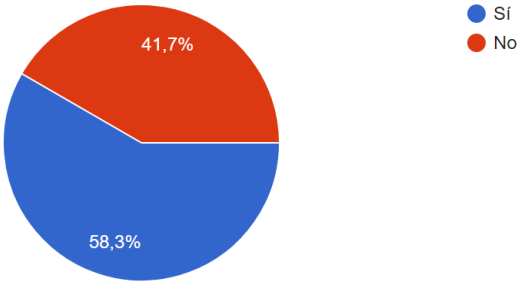
¿Hay un portafolio de acciones definidas para atender los diferentes riesgos relacionados con TI?

12 respuestas



¿Se da seguimiento y se realiza un monitoreo de la gestión de riesgos de TI?

12 respuestas



9 Anexos

Este capítulo presenta los documentos relacionados con el trabajo final de graduación, que sustentan, soportan o amplían alguna información necesaria para el desarrollo de dicho trabajo.

Cada uno de los anexos incluye una breve descripción de su contenido y propósito.

Anexo A: Constancia de trabajo en Deloitte

Este anexo contiene una constancia de que el estudiante ha estado trabajando para la firma consultora Deloitte desde antes de iniciar el proceso de trabajo final de graduación. Con este documento se respalda la etapa del proceso metodológico del trabajo denominada Inmersión en el entorno.

Deloitte.

Deloitte & Touche, S.A.
Centro Corporativo El Cafetal
Edificio B, piso 2
La Ribera, Belén, Heredia
3667-1000 San José
Costa Rica

Tel: (506) 2246 5000
Fax: (506) 2246 5100
www.deloitte.com

A QUIEN INTERESE

Por este medio hago constar que **Jean Carlo Alfaro Campos,** portador de la cédula de identidad número 207010441, labora para esta Firma desde el 26 de Julio del 2016.

Desempeña el puesto de Asistente en el área de ERS.

Se extiende la presente a solicitud del interesado el veinticuatro de Mayo del dos mil diecisiete.

Atentamente,

Deloitte & Touche, S.A.
Fiorella Arroyo Lobo
Analista Junior Talento

Deloitte & Touche, S.A.
Cédula Jurídica
N° 3-101-020162

Anexo B: Aval para la entrega del documento académico

Este anexo contiene el documento con el aval para la entrega del documento académico del trabajo final de graduación. Con este documento se garantiza que el profesor tutor del trabajo, lo ha revisado y avala la entrega del mismo.

Aval de Entrega del Documento de Trabajo Final de Graduación

Nota aclaratoria:
Este documento se redacta de acuerdo a las disposiciones actuales de la Real Academia Española con relación al uso del género inclusivo (https://goo.gl/ITVYiN).
Al mismo tiempo se aclara que estamos a favor de la igual de derechos entre los géneros.

Responsabilidad del Profesor Tutor:

1. A solicitud del estudiante, completar el formulario de Aval de Entrega del Documento de Trabajo Final de Graduación.
2. Devolver una respuesta al estudiante que realizó la solicitud de Aval de Entrega del Documento de Trabajo Final de Graduación. La respuesta debe ser por correo.

Formulario de Aval de Entrega del Documento de Trabajo Final de Graduación:

Yo Laura Alpízar Chaves Profesor Tutor del Estudiante Jean Carlo Alfaro Campos carne **201025382,** hago constar que he revisado exhaustivamente el documento académico final del Trabajo Final de Graduación. Asimismo, he verificado la atención de las correcciones realizadas en mi condición de Profesor Tutor. Por lo tanto, autorizo entregar este documento a la Coordinación de Trabajos Finales de Graduación para que se realicen las gestiones correspondientes para la programación de la defensa.

Responsabilidades del estudiante:

1. Solicitar al Profesor Tutor el Aval de Entrega del Documento de Trabajo Final de Graduación. Esta solicitud se debe realizar por correo al Profesor Tutor.

2. Enviar a la Coordinación de Trabajos Finales de Graduación la respuesta otorgada por el Profesor Tutor según el formato indicado en este documento. Para esto, debe realizar un reenvío del correo a smora@itcr.ac.cr con copia:
   a. El correo del Profesor Tutor y
   b. Al correo soniamora0407@gmail.com

   No se requiere la firma del Profesor Tutor, dado que el reenvío del correo del Profesor Tutor garantiza la identidad del Profesor.

10 Referencias bibliográficas

Abarca, A., Alpízar, F., Rojas, C., & Sibaja, G. (2012). *Técnicas cualitativas de investigación* (1 ed.). San José, Costa Rica: Editorial Universidad de Costa Rica.

Albinson, N., Blau, A., & Chu, Y. (2016). *The future of risk. New game, new rules.* Recuperado el 24 de Marzo de 2017, de Sitio web de Deloitte: https://www2.deloitte.com/us/en/pages/risk/articles/future-of-risk-ten-trends.html

Alvarado, D. F., & Zumba, L. A. (2015). *Elaborar un Plan de Gestión de Riesgos de las Tecnologías de Información y Comunicación basada en el Marco COBIT 5 para Riesgos aplicado a la Universidad de Cuenca.* Tesis de Licenciatura, Universidad de Cuenca, Facultad de Ciencias Económicas y Administrativas, Cuenca. Recuperado el 21 de Marzo de 2017, de http://dspace.ucuenca.edu.ec/handle/123456789/22342

Arias, N., Cuevas, E., León, S., & Vasconcelos, K. (2012). *Desarrollo de un trabajo de investigación apoyo metodológico* (1 ed.). San José, Costa Rica: Loyola Ediloy S.A.

Casasola, W. (2015). *El taller de la investigación: cómo realizar facilmente una investigación documental* (1 ed.). San José, Costa Rica: Ediciones Didácticas Nexo.

Cienfuegos, I. (2013). Risk Management theory: the integrated perspective and its application in the public sector [Teoría de la gestión de riesgos: una perspectiva integrada y su aplicación en el sector público]. *Estado, Gobierno, Gestión Pública*(21), 89-126. doi:10.5354/0717-8980.2013.29402

Creswell, J. W. (2014). *Research design: qualitative, quantitative, and mixed methods approaches* (4 ed.). Thousand Oaks, California, EE.UU.: SAGE Publications, Inc.

Deloitte & Touche, S.A. (2017). *Acerca de Deloitte*. Obtenido de Sitio web de Deloitte: https://www2.deloitte.com/cr/es/pages/about-deloitte/articles/about-deloitte.html

Deloitte Touche Tohmatsu Limited. (2 de Marzo de 2017). *Global risk management survey, 10th edition.* (E. Hida, Ed.) Recuperado el 24 de Marzo de 2017, de Deloitte University Press: https://dupress.deloitte.com/dup-us-en/topics/risk-management/global-risk-management-survey.html

Galaz, Yamazaki, Ruiz Urquiza, S.C. (2015). *COSO Marco de referencia para la implementación, gestión y control de un adecuado Sistema de Control Interno.* Obtenido de Sitio web de Deloitte: https://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/COSO-Sesion1.pdf

Hernández, R., Fernández, C., & Baptista, M. (2014). *Metodología de la investigación* (6 ed.). México D.F.: Mc Graw Hill.

INTECO. (2011). *INTE/ISO 31000:2011.* INTECO.

ISACA. (2012). *COBIT 5: Procesos Catalizadores.* Rolling Meadows, Illinois, EE.UU.: ISACA.

ISACA. (2012). *COBIT 5: Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa.* Rolling Meadows, Illinois, EE.UU.: ISACA.

ISACA. (2013). *COBIT 5 for Risk.* Rolling Meadows, Illinois, EE.UU.: ISACA.

Kumsuprom, S. (2010). *Structured approach to organisational ICT risk management: An empirical study in Thai businesses.* Tesis PhD, RMIT University, School of Business Information Technology and Logistics. Recuperado el 21 de Marzo de 2017, de http://researchbank.rmit.edu.au/view/rmit:7515

Peña, J. Á. (02 de marzo de 2010). *Metodologías y Normas para el Análisis de Riesgos: ¿Cuál debo aplicar?* Obtenido de Sitio web de ISACA Capítulo Monterrey: http://www.isaca.org/chapters7/Monterrey/Events/Documents/20100302%20Metodolog%C3%ADas%20de%20Riesgos%20TI.pdf

Peña, J., & Rico, S. (31 de octubre de 2013). *Un vistazo general de COBIT 5 for Risk.* Obtenido de Sitio web de ISACA Capítulo Monterrey: http://www.isaca.org/chapters7/Monterrey/Events/Documents/20133110_COBIT_5_for_Risk.pdf

Posada, A. M., & Gómez, S. (2012). *Propuesta de guía de implementación de mejores prácticas en gestión de riesgos de tecnologías de información en universidades*

privadas. Tesis de Maestría, Universidad ICESI, Facultad de Ingeniería, Santiago de Cali. Recuperado el 21 de Marzo de 2017, de http://hdl.handle.net/10906/70787

Rojas, L. (2008). *Elementos conceptuales y metodológicos de la investigación cualitativa: módulo de autoinstrucción* (1 ed.). San José, Costa Rica: Editorial Universidad de Costa Rica.

SUGEF. (9 de agosto de 2016). *Acuerdo SUGEF 18-16.* Obtenido de Sitio web de SUGEF: https://www.sugef.fi.cr/normativa/normativa_vigente/documentos/SUGEF%2018-16%20(v4%20Agosto%202016).pdf

SUGEF. (20 de mayo de 2016). *Acuerdo SUGEF 2-10.* Obtenido de Sitio web de SUGEF: https://www.sugef.fi.cr/normativa/normativa_vigente/documentos/SUGEF%202-10%20Adm%20Riesgos.pdf

SUGEF. (17 de abril de 2017). *Acuerdo SUGEF 14-17.* Obtenido de Sitio web de SUGEF: https://www.sugef.fi.cr/normativa/normativa_vigente/documentos/SUGEF%2014-17%20(v2_%2017abr2017).pdf

SUGEF. (s.f.). *Sobre SUGEF*. Recuperado el abril de 2017, de Sitio web de SUGEF: https://www.sugef.fi.cr/sobre_sugef/

Valencia, F. J., Marulanda, C. E., & López, M. (Enero de 2016). Gobierno y gestión de riesgos de tecnologías de información y aspectos diferenciadores con el riesgo organizacional. (R. Llamosa Villalba, Ed.) *Gerencia Tecnológica Informática, 15*(41), 65-77. Recuperado el 21 de Marzo de 2017, de http://revistas.uis.edu.co/index.php/revistagti/article/view/5911

Vanegas, G. A. (2013). *Armonización de múltiples modelos para el análisis de riesgos de las tecnologías de la información y desarrollo de software.* Trabajo de grado, Universidad de San Buenaventura Cali, Facultad de Ingeniería, Santiago de Cali. Recuperado el 21 de Marzo de 2017, de http://hdl.handle.net/10819/2153