DISEÑO DE UN MODELO DE GESTIÓN DE RIESGOS APLICABLE A PROYECTOS DE NATURALEZA TI DE LA ALCALDÍA DISTRITAL DE CARTAGENA DE INDIAS.

ING. CHRISTIAN SARAVIA MARTÍNEZ

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA
MAESTRÍA EN GERENCIA DE PROYECTOS
CARTAGENA-BOLÍVAR
2018

DISEÑO DE UN MODELO DE GESTIÓN DE RIESGOS APLICABLE A PROYECTOS DE NATURALEZA TI DE LA ALCALDÍA DISTRITAL DE CARTAGENA DE INDIAS.

ING. CHRISTIAN SARAVIA MARTÍNEZ

TESIS DE GRADO PARA OBTENER EL TÍTULO DE MAGISTER EN GERENCIA DE PROYECTOS

Directora:
MGTR. BEATRIZ ELENA LÓPEZ VALENCIA

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA
MAESTRÍA EN GERENCIA DE PROYECTOS
CARTAGENA-BOLÍVAR
2018

CARTA DE ACEPTACIÓN

El Trabajo de Grado “Diseño de un modelo de Gestión de Riesgos aplicable a proyectos de naturaleza TI de la Alcaldía Distrital de Cartagena de Indias.”, presentado para obtener el título de Magister en Gerencia de Proyectos, cumple con los requisitos establecidos y recibe nota aprobatoria.

_____

Firma del director del Trabajo de Grado

_____

Firma del Jurado 1

_____

Firma del Jurado 2

Cartagena de Indias, Marzo de 2019.

DEDICATORIA

Una vez que terminé mi carrera de pregrado siempre tuve en mente como reto profesional ser Magister, hoy después de 2 años logro este reto. Agradezco primero a Dios, por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación.

A mi mamá, mi abuelo y mi tía abuela, por ser los pilares más importantes y por demostrarme siempre su cariño y apoyo incondicional. A mi ángel en el cielo, mi abuela, la cual me guía y acompaña en cada paso; a mi pareja que sin importar nuestras pequeñas diferencias siempre me apoyó y estuvo en todo momento aconsejándome y dándome ánimos.

A los que me han ayudado a crecer a nivel profesional y personal. A quienes enriquecieron mis experiencias y aprendizaje y, aprendieron conmigo, incluyendo a mis docentes, muy especialmente a mi tutora la profesora Beatriz por su apoyo y por haberme guiado en la elaboración de este trabajo, al profesor Alfonso por sus consejos y apoyo, de igual forma a Yicet por siempre estar muy pendiente de nosotros en este proceso y estar dispuesta a colaborarnos; por último a mis compañeros y amigos incondicionales de este proceso, especialmente Yaneth, David, Sr. Nando, Joko, Romi, Julieth y Yohanna porque sin el equipo que formamos, no hubiéramos logrado esta meta.

Muchas Gracias

TABLA DE CONTENIDO

GLOSARIO

Con el fin de tener un conocimiento más amplio, se hace una descripción de las definiciones de los conceptos más relevantes que componen el entorno en cual se desarrolla el tema de investigación, de la siguiente forma:

1. **Acción de riesgo:** Es una de las tareas detalladas que implementa en su totalidad o en parte, una estrategia de respuesta para hacer frente a un riesgo individual o al riesgo global del proyecto (Project Management Institute, 2013).
2. **Amenaza:** Es una condición o situación desfavorable para el proyecto, una serie de circunstancias negativas, una serie de acontecimientos negativos, el riesgo de que tendrá un impacto negativo sobre un objetivo del proyecto de que si éste ocurre, o la posibilidad de cambios negativos. La amenaza contrasta con el término de oportunidad (Project Management Institute, 2013).
3. **Apetito de riesgo:** Grado de incertidumbre que una organización o un individuo están dispuestos a aceptar con miras a una recompensa (Project Management Institute, 2017, p.736).
4. **Buenas prácticas:** Son aquellas prácticas profesionales que resultan ser las mejores de entre todas las que los profesionales realizan para lograr los resultados esperados.[1]
5. **Categoría de riesgo:** Es un grupo de posibles causas de riesgo. Las causas de riesgo pueden ser agrupadas en categorías como: técnicas, externas, de la organización, ambientales o de la gestión de proyecto. Una categoría puede incluir subcategorías como la madurez técnica, condiciones climáticas o la estimación agresiva (Project Management Institute, 2013).
6. **Ciclo de vida del proyecto:** Es un conjunto de fases del mismo, generalmente secuenciales y en ocasiones superpuestas, cuyo nombre o número se determinan por las necesidades de

[1] CORUJO, Rosa. MANUAL DE BUENAS PRÁCTICAS EN LA GESTIÓN DE PROYECTOS DE I+D+i. En: CRUE REDUGI Red de Unidades de Gestión de la Investigación. Septiembre, 2016. Vol. 2. Pág. 4-46.

gestión y control de la organización u organizaciones que participan en el proyecto, la naturaleza propia del proyecto y su área de aplicación. El ciclo de vida proporciona el marco de referencia básico para dirigir el proyecto, independientemente del trabajo específico involucrado (Project Management Insitute, 2013, p. 15).

7. **Condiciones de activación:** Es una definición de las circunstancias en las que se considera que un riesgo se ha producido, o sobre los cuales se iniciará una acción de reproceso (Association for Project Management, 2004).
8. **Estrategia de respuesta:** Es un enfoque de alto nivel para hacer frente a un riesgo individual o el riesgo global del proyecto, desglosado en un conjunto de acciones de riesgo (Project Management Institute, 2013).
9. **Evento de riesgo secundario:** Es un evento de riesgo que puede ocurrir como resultado de la aplicación de una respuesta al riesgo o el plan de reserva (Association for Project Management, 2004).
10. **Exposición al riesgo:** Es una medida del riesgo global del proyecto que describe el efecto total de los riesgos identificados sobre los objetivos (Project Management Institute, 2013).
11. **Fases del proyecto:** Son divisiones dentro del mismo proyecto, donde es necesario ejercer un control adicional para gestionar eficazmente la conclusión de un entregable mayor. Las fases del proyecto suelen completarse de manera secuencial, pero en determinadas situaciones de un proyecto pueden superponerse (Project Management Insitute, 2013, p. 18).
12. **Gestión de riesgos del proyecto:** Incluye los procesos relacionados con llevar a cabo la planificación de la gestión, la identificación, el análisis, la planificación de respuesta a los riesgos, así como su seguimiento y control en un proyecto. Los objetivos de la gestión de los riesgos del proyecto son aumentar la probabilidad y el impacto de eventos positivos, y disminuir la probabilidad y el impacto de eventos negativos para el proyecto (Project Management Insitute, 2013, p. 273).
13. **Impacto:** Es la medida del efecto de un riesgo en uno o más objetivos si se produce. (Project Management Institute, 2013).

14. **Lecciones aprendidas:** Conocimiento adquirido durante un proyecto que muestra cómo se abordaron o deberían abordarse en el futuro los eventos del proyecto, a fin de mejorar el desempeño futuro (Project Management Insitute, 2013, p. 715).
15. **Metalenguaje de riesgo:** Es una descripción estructurada de un riesgo que separa la causa, el riesgo y el efecto. Una descripción de riesgo típica que utiliza el metalenguaje de riesgo podría ser en la siguiente forma: "A consecuencia de la <Causa>, el <Riesgo> puede ocurrir, lo que llevaría al <Efecto>" (Project Management Institute, 2013).
16. **Plan de Gestión de Riesgos:** Es un documento que define la forma de gestión de riesgos que ha de aplicarse en el contexto del proyecto específico (Association for Project Management, 2004).
17. **Probabilidad:** Es una medida de la posibilidad de que un riesgo individual se va a producir. También es conocida como verosimilitud (Project Management Institute, 2013).
18. **Propietario de la acción del riesgo**: Es la persona responsable de llevar a cabo las acciones de riesgos aprobadas para responder a un riesgo determinado. También conocido como "Propietario de la respuesta" cuando el contexto lo permite (Project Management Institute, 2013).
19. **Proyecto:** Es un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único. La naturaleza de los proyectos indica un principio y un final definidos. El final se alcanza cuando se logran los objetivos del proyecto o cuando se termina el proyecto porque sus objetivos no se cumplirán o no pueden ser cumplidos, o cuando ya no existe la necesidad que dio origen al proyecto (Project Management Insitute, 2013).
20. **Registro de riesgos:** Es un conjunto de información que contiene todos los riesgos identificados del proyecto; también explica la naturaleza de cada riesgo y contiene la información pertinente de su evaluación y gestión (Association for Project Management, 2004).
21. **Riesgo:** Es un evento o condición incierta que, si sucede, tiene un efecto en por lo menos uno de los objetivos del proyecto (Project Management Institute, 2013, p. 275).

22. **Sistema de Gestión de Seguridad de la Información (SGSI):** Parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información. (NTC-ISO/IEC 27001, 2006, p. 11)
23. **Software:** Es la parte intangible del computador, es decir el conjunto de programas que permiten al computador realizar determinadas tareas.
24. **Tecnologías de la información y la comunicación (TIC):** Conjunto de dispositivos, herramientas, equipos y componentes electrónicos, capaces de manipular información que soportan el desarrollo y crecimiento económico de cualquier organización. Cabe destacar que en ambientes tan complejos como los que deben enfrentar hoy en día las organizaciones, sólo aquellos que utilicen todos los medios a su alcance, y aprendan a aprovechar las oportunidades del mercado visualizando siempre las amenazas, podrán lograr el objetivo de ser exitosas. (Thompson y Strickland, 2004)
25. **Umbral de riesgo:** Nivel de exposición al riesgo por encima del cual los riesgos se abordan y por debajo del cual los riesgos pueden aceptarse (Project Management Institute, 2017, p. 762).

RESUMEN DE LA TESIS

El Trabajo de grado titulado “Diseño de un modelo de Gestión de Riesgos aplicable a proyectos de naturaleza TI de la Alcaldía Distrital de Cartagena de Indias.”, contiene el modelo de gestión de riesgo propuesto a fin de mejorar la gestión de aquellos eventos que pueden llegar a afectar el cumplimiento de los objetivos de los proyectos TI.

Como punto de partida, se utilizó como base las buenas prácticas sugeridas en los principales marcos de referencia de gestión de tecnología, normativas, metodologías y estándares de la gerencia de proyectos como lo son COBIT5, ITIL, PRINCE2, PMI, APM e ISO, para el diseño del modelo para la gestión de riesgos.

La metodología definida y aplicada en el desarrollo de la investigación, está compuesta por cuatro etapas:

- Recopilación y análisis de información objeto de la investigación.
- Análisis comparativo de los enfoques metodológicos de gestión de riesgos.
- Construcción de modelo para la gestión de riesgos en proyectos TI de la Alcaldía de Cartagena.
- Implementación del modelo de gestión de riesgo propuesto.

Como resultado final se plantea un nuevo modelo de apoyo para la gestión de riesgos con sus respectivos componentes (Procesos, Actividades y Técnicas de apoyo a los procesos); de esta manera, se logra obtener una herramienta que servirá de apoyo para la gestión de eventos de riesgos en los proyectos de TI desarrollados por la Alcaldía de Cartagena.

Palabras Claves: Gestión de riesgos, riesgos en proyectos TI, modelo de gestión de riesgos.

INTRODUCCIÓN

El Trabajo de grado titulado “Diseño de un modelo de Gestión de Riesgos aplicable a proyectos de naturaleza TI de la Alcaldía Distrital de Cartagena de Indias.”, constituye un requerimiento para la obtención del título de Magister, y se encuentra contemplado dentro del programa de Maestría en Gerencia de Proyectos de la Universidad Tecnológica de Bolívar, perteneciendo a la línea de investigación de Gestión de Riesgos en Gerencia de Proyectos.

El presente documento es el resultado de un trabajo de investigación realizado con base en la problemática mostrada en los proyectos de naturaleza T.I ejecutados por la Alcaldía de Cartagena, cuyos resultados se han visto afectados por la materialización de diferentes eventos de riesgo, debido a una inadecuada gestión de los mismos.

Ante la situación anterior, se plantea diseñar un modelo de gestión de riesgos que sirva de apoyo en la gestión de los proyectos T.I de la Alcaldía, ejecutados por las distintas dependencias que la conforman, a fin de mejorar la gestión de los eventos que pueden llegar a afectar el cumplimiento de los objetivos de los proyectos y los intereses de la Alcaldía.

En el desarrollo de la investigación se aplicaron cuatro etapas, en la primera se realizó una recopilación y análisis de información, en la cual se buscó información sobre investigaciones de diversos autores que han trabajado incesantemente en la identificación y gestión de riesgos en proyectos T.I, tales como Anudhe & Mathew, 2009; Bannerman, 2008; Boehm, 1989; Costa et al., 2007; Dash & Dash, 2010; Dey et al., 2007; Keil y otros, 2004; Oz & Sosik, 2000, Ropponen y Lyytinen, 2000, entre otros.

En la segunda etapa se realiza un análisis comparativo de los enfoques metodológicos de gestión de riesgos, entre los cuales destacan estándares orientados a procesos T.I, metodologías orientados a los proyectos y normas de seguridad informática, entre otros; identificándose las fortalezas de cada uno desde la óptica de los procesos, actividades y técnicas sugeridas.

Posteriormente se tomaron los resultados generados en las etapas anteriores para establecer el modelo para la gestión de riesgos con sus respectivos componentes: procesos, actividades y técnicas de apoyo.

De esta forma, se logra tener una herramienta que servirá de apoyo para la gestión de los eventos de riesgos de los proyectos ejecutados por la Alcaldía de Cartagena.

1. GENERALIDADES

En el presente capítulo se plantean los aspectos relacionados con el tema principal del caso de estudio, iniciando con el planteamiento del problema; el cual se divide en la descripción del problema y la justificación, y por último se detallan los objetivos del estudio.

1.1. PLANTEAMIENTO DEL PROBLEMA

Con el fin de dar a conocer la situación que se tiene en el entorno, se expone a continuación: la descripción y justificación del problema.

1.1.1. DESCRIPCIÓN DEL PROBLEMA

Anteriormente, en las organizaciones existía una preocupación enfocada a la ejecución de la dirección estratégica, esto por no tener las herramientas adecuadas como soporte, ahora, en esta nueva Sociedad de la Información los avances tecnológicos y especialmente los enmarcados en el desarrollo de las Tecnologías de la Información y las Comunicaciones - TIC-, han brindado diversas herramientas y tecnologías, entre las que se encuentran la minería de datos, los sistemas inteligentes y los sistemas de información integrados.

Es evidente, la masiva utilización de las TIC como soporte a los procesos de gestión de las organizaciones, en este escenario, se produce una transformación dentro de las organizaciones, en el que la apropiación de las TIC cada vez es más frecuente, implementando, integrando y adaptando diferentes tecnologías como lo son softwares gerenciales (ERP, CRM, BI), redes virtuales, redes WAN, servicios en la nube, entre otros.

No obstante, en un estudio realizado por Piattini[2] (2007), basado en la denominada crisis de la ingeniería del software, identifico que solo el 28 por ciento de los proyectos de software tuvieron

[2] Mario Gerardo Piattini Velthuis, es un informático con diversas investigaciones en el ámbito de la ingeniería de sistemas y software, fundador del Grupo Alarcos de Investigación, es reconocido por haber realizado sobresalientes aportaciones científicas en el área de la ingeniería informática.

éxito, es decir, se completaron a tiempo y dentro del presupuesto, con todas las funciones operativas como se especificaron inicialmente.

Otro 49 por ciento de los proyectos fueron cuestionados, es decir, completados y operativos, pero con un presupuesto excesivo, sobre el tiempo estimado, y ofrecen menos características y funciones que las especificadas originalmente.

Por último, el 23 por ciento restante de los proyectos de software ha fracasado, es decir, se cancelaron antes de completarse o se entregaron y nunca se utilizaron.

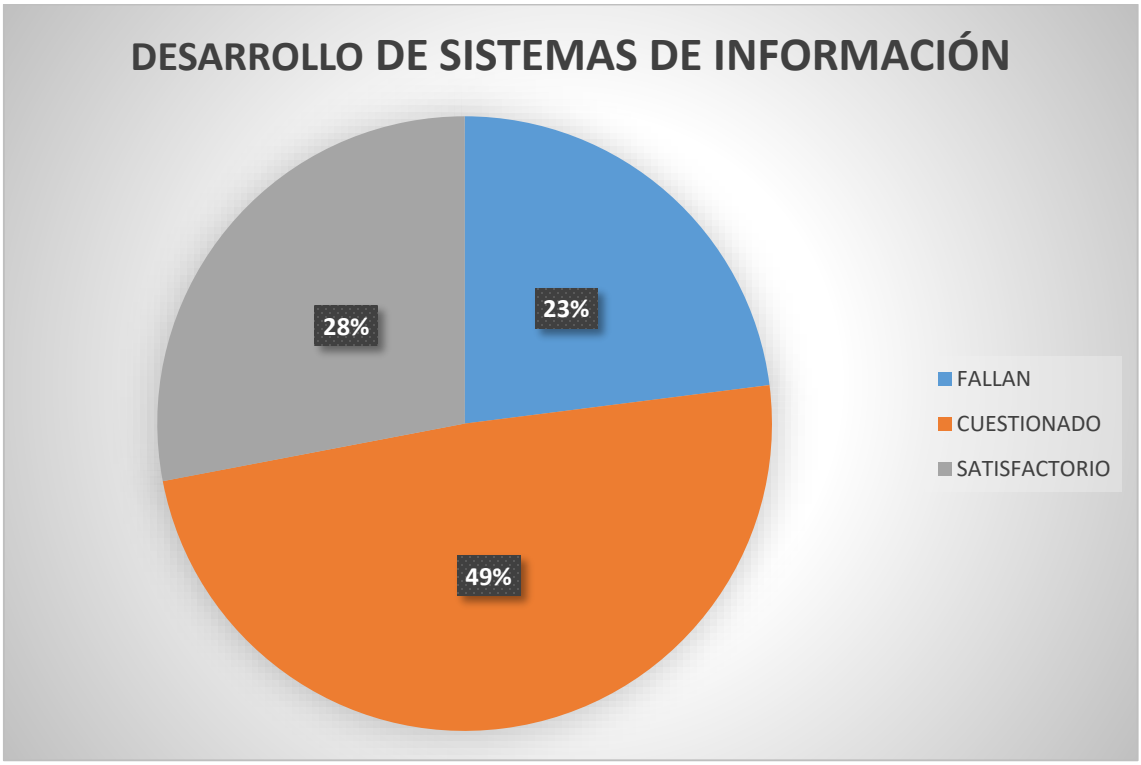


Figura 1. Estadística de Piattini desarrollo de proyectos de software, 2007.

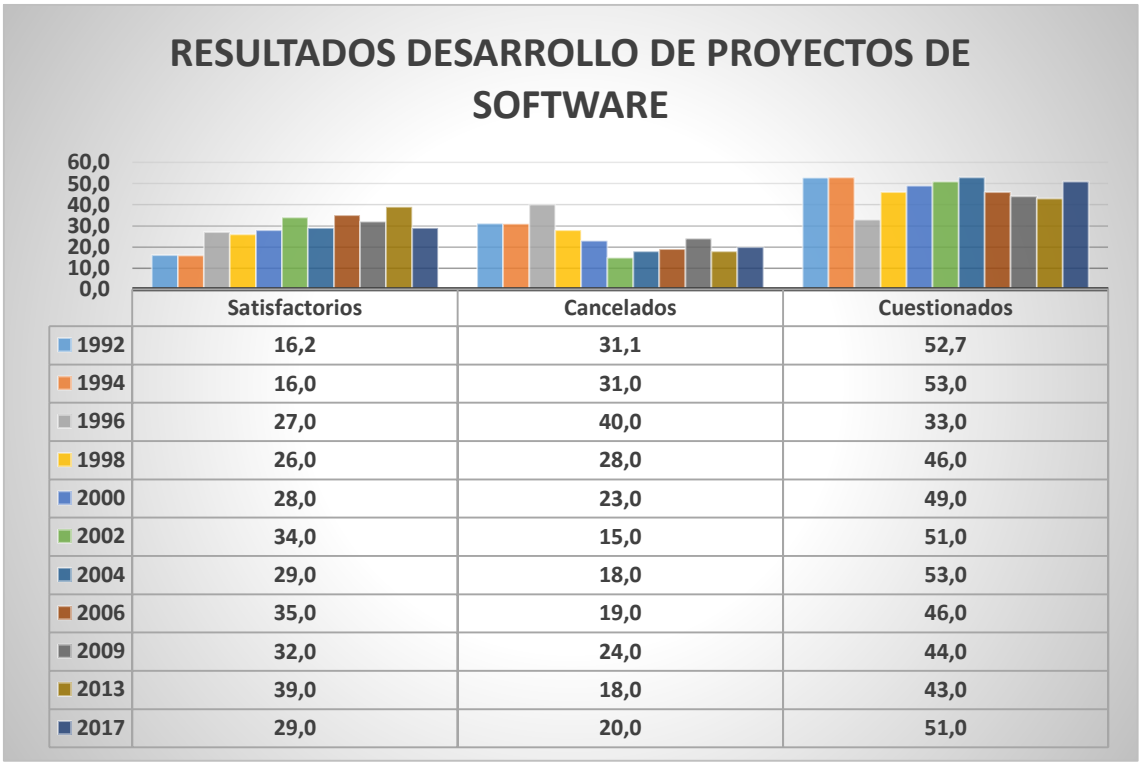
Igualmente, en la comparación realizada y presentada en el Informe del Caos (The Standish Group, 2017) entre las estadísticas de proyectos de desarrollo de software desde los años 1992 hasta 2017, arrojó un panorama similar a los resultados obtenidos por Piattini, el informe muestra que los

proyectos software tienen una tasa de éxito del 29%, frente al 39% del informe de 2013 y al 16,2% del de 1992.

El éxito de los proyectos es ligeramente peor que en 2013 (29% vs 39%). Por otra parte, el 51% de los proyectos fueron cuestionados (con retraso, por encima del presupuesto y/o con menos de los requisitos esperados) mientras que el 20% fracasaron (se cancelaron o se finalizaron pero el producto nunca se usó).

Las dos razones principales para estos resultados en ambos años fueron la materialización de dos riesgos principales, que son la falta de participación del usuario y requisitos incompletos.

Lo anterior, ha llevado a las organizaciones a preocuparse cada vez más por las pérdidas económicas acarreadas por los riesgos ocasionados tanto por la propia naturaleza de los proyectos TIC como por la falta de calidad en su desarrollo.



	Satisfactorios	Cancelados	Cuestionados
1992	16,2	31,1	52,7
1994	16,0	31,0	53,0
1996	27,0	40,0	33,0
1998	26,0	28,0	46,0
2000	28,0	23,0	49,0
2002	34,0	15,0	51,0
2004	29,0	18,0	53,0
2006	35,0	19,0	46,0
2009	32,0	24,0	44,0
2013	39,0	18,0	43,0
2017	29,0	20,0	51,0

Figura 2. Estadística Informe del Caos 2017.

Fuente: Adaptado del Informe del Caos de The Standish Group.

Tomando sólo el informe de 1994, que es el de peores resultados y el que más autores referencian, suman directamente el 31% de fracasos y el 53% de deficientes concluyendo que el 84% de los proyectos fracasan, creando, como afirma Glass[3], la sensación de que en software más del 70% de los proyectos fallan. Triste y preocupante imagen para el sector TIC, ya que los grandes proyectos de software pueden afectar negativamente a toda la empresa que los implementa.

Cabe señalar que aparte del Informe del Caos y del estudio de Piattini, en Colombia se desarrolla de forma anual La Encuesta de Gerencia de Proyectos en Tecnologías de Información[4], la cual es un referente del estado de la gerencia de proyectos, y particularmente en los proyectos de tecnología informática.

Para el año 2018 se pudo evidenciar en este informe que, en este tipo de industria es notoria la dificultad que tienen quienes lideran proyectos de estimar correctamente la duración de los mismos, esto debido a que cerca del 75% de los proyectos se planea en una duración igual o menor a un año y solo el 50% lo logra - es decir 1 de 3 proyectos planeados en un año o menos, será completado después de más de un año, y los proyectos planeados a dos años o más, crecerán en un 50% entre lo planeado y lo real. Se registra una desviación en la duración del cronograma entre el 3% y 10% para el 63% de los proyectos registrados en la encuesta.

[3] GLASS, Robert L. IT Failure Rates - 70% or 10-15%?. En: IEEE Software, vol. 22, no. , pp. 112, 110-111, 2005.

[4] Encuesta realizada por la Asociación Colombiana de Ingenieros de Sistemas – ACIS.

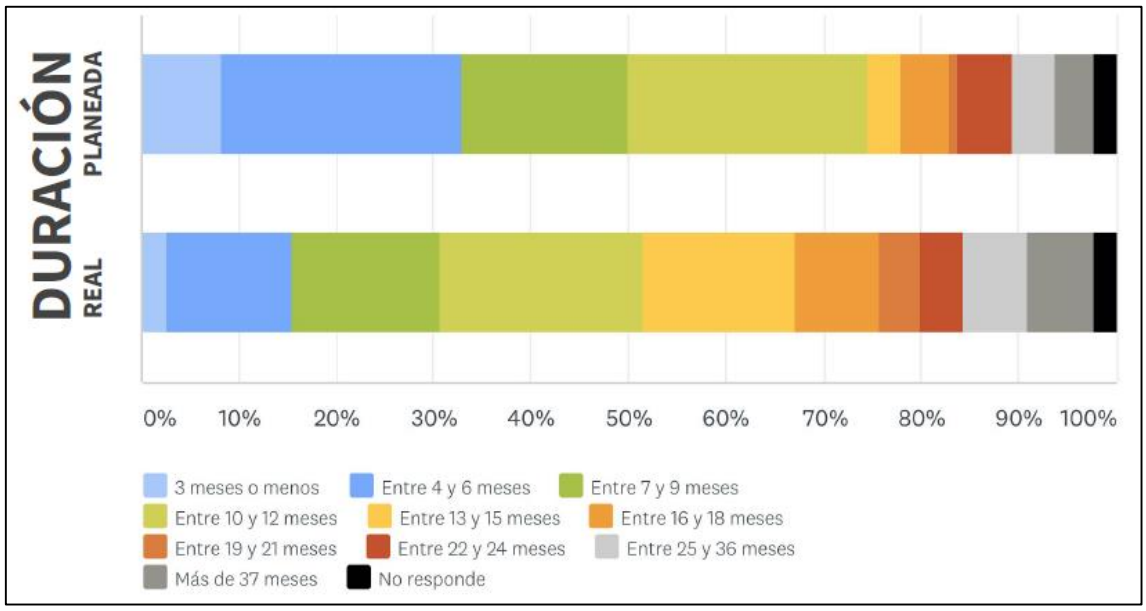


Figura 3. Duración de proyectos TI en Colombia.

Fuente: Tomado de la XVI Encuesta de Gerencia de Proyectos de TI ACIS.

A diferencia del tiempo (duración), el presupuesto no sufre mayores modificaciones a lo largo del proyecto. Esto puede ser consecuencia de la tendencia estricta del mercado Colombiano de contratar proyectos a costo fijo y la relación dominante entre los clientes y proveedores (cerca del 80% de los encuestados).

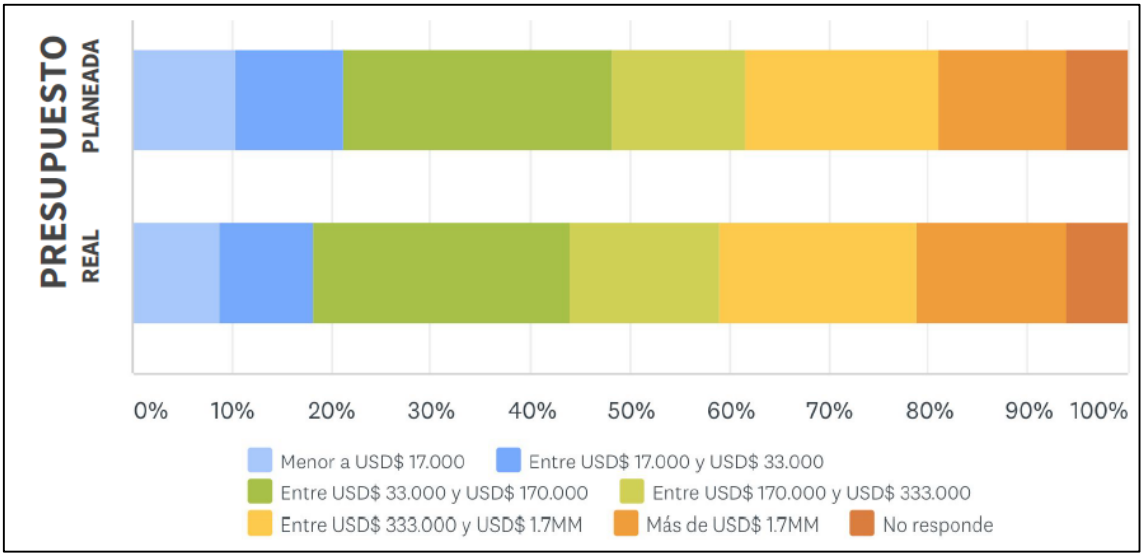


Figura 4. Presupuesto de proyectos TI en Colombia.

Fuente. Tomado de la XVI Encuesta de Gerencia de Proyectos de TI ACIS

Esta teoría se fortalece a la luz de las respuestas las desviaciones de los proyectos:

- El cronograma (tiempo) es el más afectado negativamente en los proyectos y para el que menos ahorros (adelantos) se reportan.
- El alcance y el presupuesto muestran mejores índices de desempeño y mayor capacidad de ahorro (o mejor desempeño).

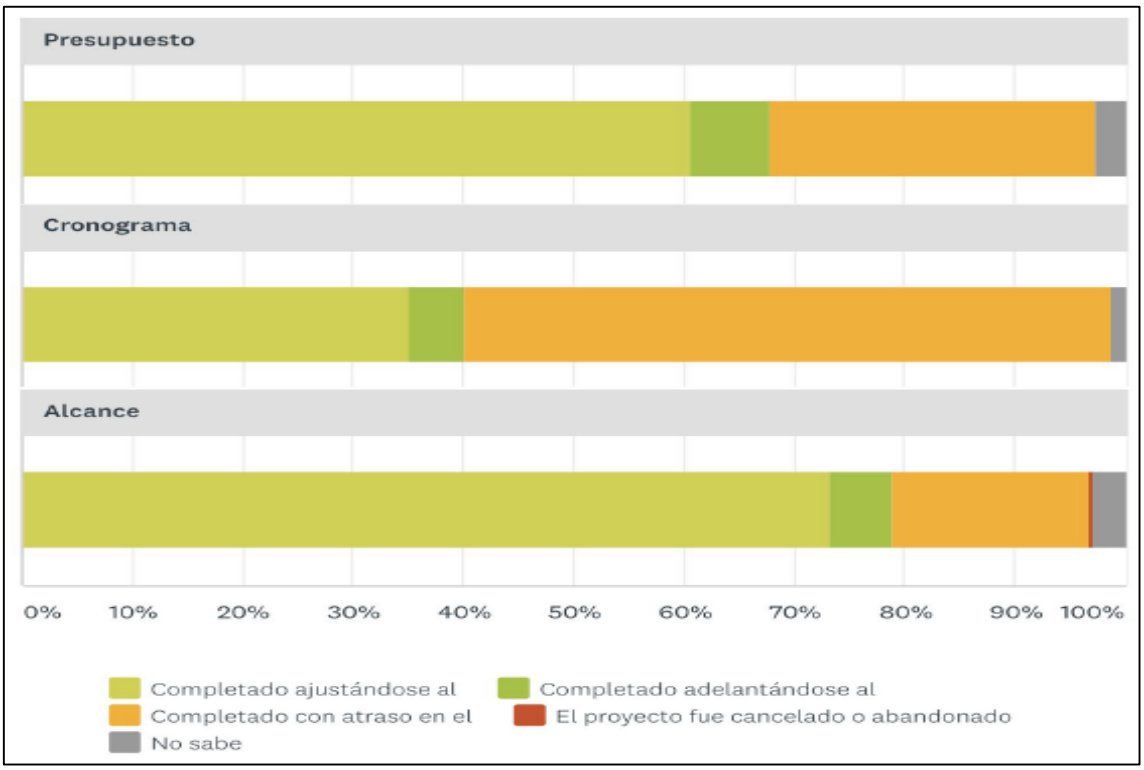


Figura 5. Variaciones de proyectos TI.

Fuente. Tomado de la XVI Encuesta de Gerencia de Proyectos de TI ACIS

El desempeño de los proyectos arroja que cerca del 60% de los proyectos no cumple las fechas objetivo propuestas y presenta retrasos, y cerca del 30% de los proyectos requiere más presupuesto del estipulado inicialmente.

Aunque no se puede concluir con certeza, es claro que existe una falta de alineación de las expectativas de los interesados y que, de una forma u otra, se sigue esperando por resultados más rápido (en menos tiempo) y más baratos (con menos presupuesto).

Por otra parte, en los últimos 10 años la Alcaldía de Cartagena de Indias ha desarrollado alrededor de 3.000 proyectos donde solo el 48,8% han terminado satisfactoriamente cumpliendo con el alcance, tiempo y costo, mientras que el 51,2% de los proyectos restantes se encuentran suspendidos o han terminado de forma anormal, es decir, con un evidente sobrecosto,

incumplimientos cronograma, del alcance e incluso afectados por la mala calidad de los entregables.

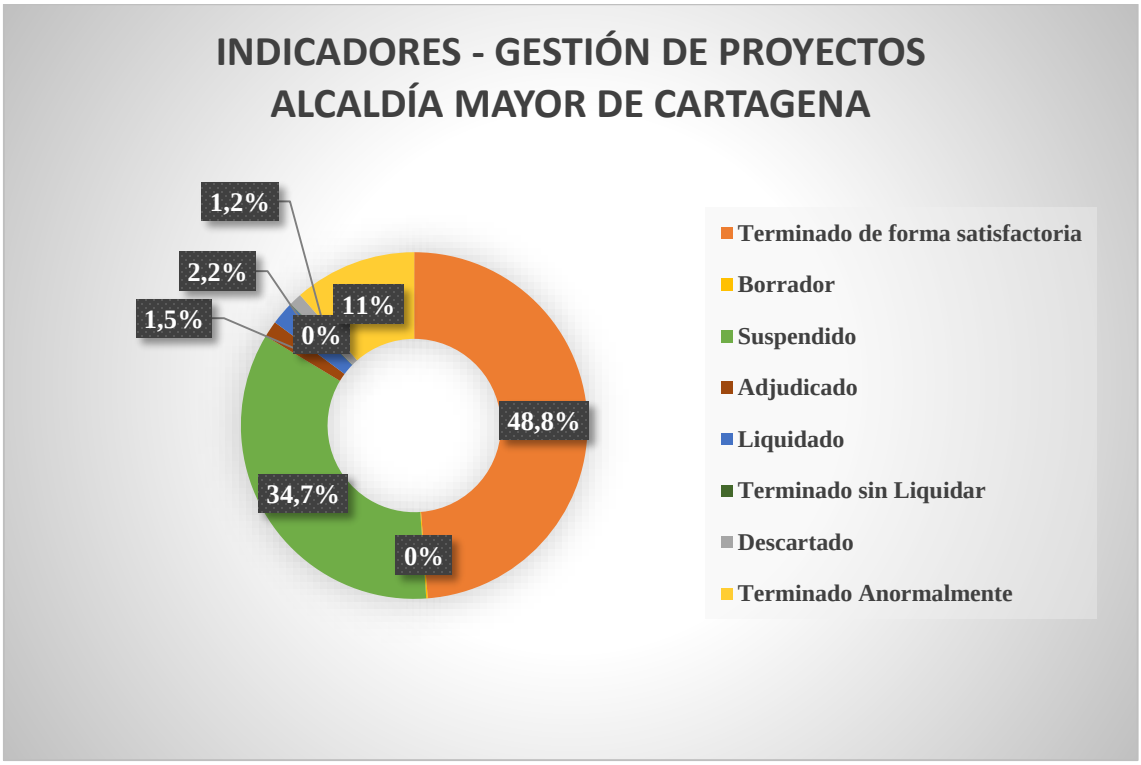


Figura 6. Proyectos desarrollados en la Alcaldía de Cartagena 2008-2018.

Fuente. Estadísticas arrojadas por SECOP.

Entre los proyectos que la Alcaldía de Cartagena ha tenido mayores desfases en cuanto a duración, costos, alcance y calidad se encuentran los de T.I, esto por la mala gestión de riesgos tales como la inadecuada captura de requerimientos, alto nivel de complejidad técnica, cambio del personal que conforma el equipo de trabajo, entre otras.

Cabe destacar que ningún proyecto de T.I ha terminado de forma satisfactoria, sino de forma anormal y a nivel de toda la Alcaldía son del tipo de proyecto que más se encuentran suspendidos.

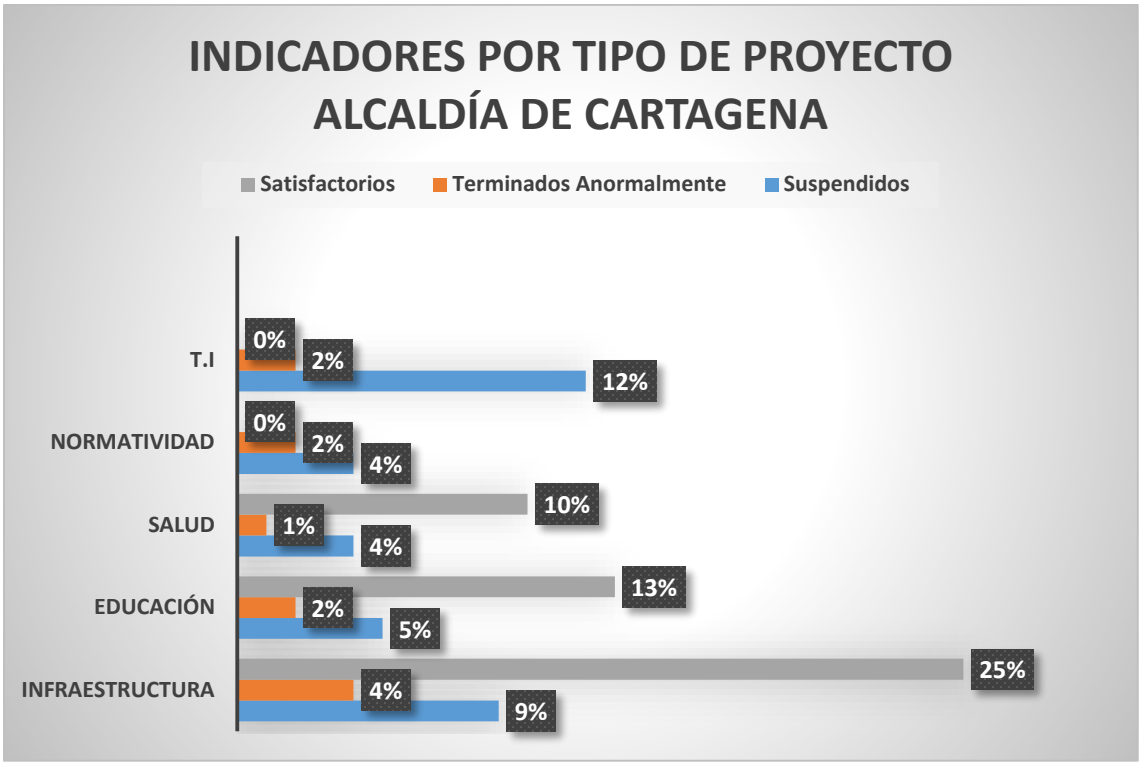


Figura 7. Indicadores por tipo de proyecto desarrollado en la Alcaldía de Cartagena 2008-2018.

Fuente: Adaptado de informe de auditoría de Control Interno, Alcaldía de Cartagena.

Es claro entonces, que los proyectos T.I no son exitosos en términos generales, fundamentalmente debido al poco conocimiento en la gestión de los riesgos que se presentan, éstos deben ser objeto de una gestión adecuada la cual debe ser iniciativa por la gerencia, supervisada y controlada por cada uno de los jefes de las áreas importantes involucradas en el proyecto.

Debido a esta realidad que vive la Alcaldía, el presente estudio busca dar respuesta al siguiente interrogante ¿Es posible que al implementar un modelo de gestión de riesgos se incremente el logro de los objetivos de los proyectos de T.I?

1.1.2. JUSTIFICACIÓN DEL PROBLEMA

El éxito de los proyectos TI es bastante subjetivo y está sujeto a muchos riesgos, cuya percepción varía de individuo a individuo y depende en gran medida de las características del proyecto.

Estos riesgos pueden marcar la diferencia entre un proyecto cancelado, uno que logra culminar con deficiencias (cuestionado) o uno culminado de forma satisfactoria. Es por esto, que al comenzar el proyecto también lo deben hacer las tareas orientadas a gestionar sus riesgos, para que de esta forma se pueda prevenir la materialización de ellos o bien poder estar preparados para afrontar la situación adversa que se presente.

Se ha escrito mucho sobre la gestión de riesgos y existen métodos bien documentados y probados en la práctica. Sin embargo, los proyectos TI cuentan con características particulares que lo distancian mucho de cualquier otro tipo de proyecto, como pueden ser su complejidad y abstracción. Por ejemplo, a nivel de un proyecto de desarrollo de software, a los ojos del cliente el software es moldeable, y nunca es demasiado tarde para modificarlo. En un proyecto de Redes de Comunicación, el cliente piensa que cualquier dispositivo de red funcionaría igual. Entre otros escenarios.

Si bien existen algunas propuestas metodológicas específicas para ciertos proyectos TI, no es fácil encontrar en la literatura un análisis de las fortalezas y debilidades de estos métodos en su aplicación en proyectos concretos.

Por tal motivo, contar con un modelo que permita Gestionar los Riesgos de proyectos TI puede generar un panorama importante para la administración de proyectos de la Alcaldía de Cartagena, ya que estará preparada proactivamente para enfrentar las amenazas que afecten el resultado final de dichos proyectos.

Este trabajo de grado, estará orientado a la investigación sobre las mejores prácticas, normatividad y herramientas disponibles para la Gestión de Riesgos, con el fin de construir un modelo que se

adapte a las necesidades de la Alcaldía de Cartagena y pueda además introducir una cultura de control del Riesgo que se pueda ver reflejada en el éxito de los proyectos a desarrollar.

Es una necesidad para la Alcaldía de Cartagena implantar la Gestión de Riesgos por dos situaciones que marcaran diferencias a los resultados actuales, primero asegurar mayor cumplimento en los objetivos estratégicos que se miden a través de indicadores de cumplimiento de tiempo, costo y calidad, y segundo en la documentación del conocimiento de la entidad, pues actualmente no hay un repositorio que almacene información de riesgos de este tipo de proyectos, lecciones aprendidas, oportunidades de mejora y que a través de este modelo se permitirá la generación de una base de información para referenciación de futuros proyectos.

El modelo propuesto le permitirá a la Alcaldía de Cartagena contar con una serie de herramientas para documentar y controlar los riesgos a los que están expuestos los proyectos de TI, mejorar la comunicación con los responsables de los planes de acción y verificar la efectividad en las acciones tomadas, considerando desde medidas preventivas hasta las acciones correctivas a implementar, posterior a la materialización de los riesgos. De esta manera ver resultados tangibles en la reducción de la probabilidad de materialización de eventos negativos que afecten el costo, tiempo o calidad de este tipo de proyectos.

1.2. OBJETIVOS

Dentro del presente estudio se plantea un objetivo general en el cual se expone el propósito principal del proyecto; de igual forma, se establecen unos objetivos específicos por medio de los cuales se detalla de manera estructurada la forma como será desarrollado el proyecto para cumplir con el objetivo general del mismo.

1.2.1. OBJETIVO GENERAL:

Diseñar e implementar la propuesta de un modelo práctico para la Gestión de Riesgos basado en las mejores prácticas de estándares existentes, en proyectos de naturaleza TI de la Alcaldía Distrital de Cartagena de Indias.

1.2.2. OBJETIVOS ESPECÍFICOS:

- Elaborar el estado del arte sobre la gestión de riesgos comúnmente utilizadas en proyectos de T.I, mediante una revisión bibliográfica que permita identificar las mejores prácticas en la gestión y valoración de riesgos en este tipo de proyectos.

- Realizar un análisis comparativo de los enfoques metodológicos de gestión de riesgos que permita establecer sus principales fortalezas y debilidades en la gestión de riesgos.

- Construir los componentes y estructura del modelo de gestión de riesgos con base al estado del arte y el análisis comparativo y aplicarlo a un proyecto TI de la Alcaldía Distrital de Cartagena de Indias.

2. ASPECTOS METODOLÓGICOS

En el presente capítulo se muestra el diseño metodológico bajo el cual se desarrolló el trabajo de investigación; al igual se describe la metodología de estudio relacionada con el tipo de investigación, las fuentes de información utilizadas y los límites del trabajo de investigación.

2.1. DISEÑO METODOLÓGICO DE LA INVESTIGACIÓN.

Para cumplir con los establecidos en la presente investigación, se plantea una investigación compuesta por 4 etapas, las cuales se describen tabla No 14, con sus respectivas actividades.

N°	Descripción de la etapa	Actividades
1	Recopilación y análisis de información objeto de la investigación.	1.1. Revisar antecedentes bibliográficos en libros y artículos de investigación de los principales investigadores que han trabajado en la identificación y gestión de riesgos en proyectos T.I.
		1.2. Revisar documentación de los principales marcos de referencia de gestión de tecnología, normativas, metodologías y estándares de la gerencia de proyectos.
2	Análisis comparativo de los enfoques metodológicos de gestión de riesgos.	2.1. Establecer los criterios (procesos, actividades y técnicas de apoyo) comunes y diferentes de los enfoques metodológicos seleccionados.
		2.2. Identificar fortalezas en cada uno de los criterios analizados de los enfoques metodológicos seleccionados.

3	Construcción de modelo para la gestión de riesgos en proyectos TI de la Alcaldía de Cartagena.	3.1. Identificar las variables (procesos, actividades, técnicas de apoyo y documentos asociados) del modelo a proponer para la gestión de riesgos.
		3.2. Establecer la estructura del nuevo modelo propuesto para la gestión de riesgos.
4	Implementación del modelo de gestión de riesgo.	4.1. Seleccionar proyecto TI de la Alcaldía de Cartagena e implementar el modelo propuesto.

Tabla 13. Metodología para el desarrollo de la investigación.

Fuente: Elaboración propia.

2.2. TIPO DE INVESTIGACIÓN.

El Trabajo de grado pertenece al ámbito de la Formulación de Proyectos: Gestión de Riesgos; se plantea cómo una investigación con la siguiente naturaleza:

- **Enfoque de investigación:** Cualitativo.
- **Alcance de investigación:** Descriptivo.
- **Diseño de investigación:** No experimental de tipo transversal.

Esto, debido a que se realizaran descripciones y mediciones de conceptos o variables y sus propiedades inmersas en la gerencia de proyectos y la gestión de riesgos, sin necesidad de manipularlas y en un tiempo único, para analizar así su incidencia.

2.3. ESTRATEGIA DE INVESTIGACIÓN.

La estrategia de investigación utilizada en el presente trabajo de grado serán a través de investigación de archivos y documentales; la cual según Baena (1985), es una técnica que consiste en la selección y compilación de información a través de la lectura y crítica de documentos y materiales bibliográficos, bibliotecas, bibliotecas de periódicos, centros de documentación e información.

En virtud de lo anterior, se separará la documentación consultada de la siguiente manera:

Fuentes Primarias: Se consultará información relacionada con el tema de investigación, a través de documentos disponibles como estándares, guías, normas y artículos asociados, tanto físicos como en medios electrónicos disponibles en portales web, de los cuales destacan los siguientes:

Journal	Cuartil
Project Management Journal	Q1
International Journal of Project Management	Q1
Journal of Systems and Software	Q1
Computer Standards and Interfaces	Q2
Information and Software Technology	Q2
International Journal of Information Systems and Project Management	Q2
International Journal of Managing Projects in Business	Q2
Journal of Ambient Intelligence and Humanized Computing	Q2
Journal of Information Systems	Q2
Polish Journal of Management Studies	Q2

Fuentes Secundarias: Se consultará información secundaria relacionada al diagnóstico actual de la Alcaldía en la gestión de los proyectos y más en el tema de la gestión de riesgos por lo cual se revisará los informes de auditoría gubernamental de la Contraloría General de la Nación, los informes de auditoría de la Oficina Asesora de Control Interno, entre otros.

2.4. LIMITES DE LA INVESTIGACIÓN.

Se consideran dos limitaciones principales:

- La primera es que al tratarse del sector de tecnologías de la información y la comunicación (TIC) de proyectos públicos en una entidad territorial del Caribe Colombiano, que es la Alcaldía de Cartagena, se debe tener cuidado con su uso en contextos fuera de este ámbito sin una validación adicional de la aplicabilidad de los resultados y las herramientas propuestas.

- En segundo lugar, la implementación del modelo aunque proporciona un enfoque estructurado, por sí solo no garantiza el éxito, es vital que se articule con otros elementos entre los cuales está la cultura, tiempo, la gestión del cambio y el sentido de pertenencia.

3. MARCO REFERENCIAL

En el presente capítulo se hizo una profundización de la temática sobre uso y apropiación de las TIC y de la gestión de riesgos en proyectos en diversas metodologías, destacando conceptos técnicos y procedimientos, a fin de ofrecerle al lector una contextualización del entorno bajo el cual se desarrollará el trabajo de investigación.

3.1. MARCO TEÓRICO

El marco teórico de este trabajo de grado está conformado por los antecedentes sobre el uso y apropiación de las Tecnologías de la Información y la Comunicación, los cuales son necesarios para caracterizar el sector y por las diferentes metodologías y estándares que son usadas por las Empresas para la gestión de riesgos en proyectos T.I

El desarrollo y competitividad de un país en una economía globalizada, está fuertemente correlacionados con la sensibilización, uso y apropiación adecuada de las Tecnología de Información y Comunicación (TIC), tal como se evidencia en la determinación de los índices del

Foro Económico Mundial, respecto al ranking de competitividad global (Global Competitiveness Report, GCR) y en el índice de preparación de las naciones para un mundo interconectado (Network Readiness Index, NRI).

RANKING	PAIS	PUNTAJE
1	Singapur	6
2	Finlandia	6
3	Suecia	5.8
4	Noruega	5.8
5	Estados Unidos	5.8
38	Chile	4.6
43	Uruguay	4.5
44	Costa Rica	4.5
55	Panamá	4.3
68	Colombia	4.1
72	Brasil	4
76	México	4
82	Ecuador	3.9
89	Argentina	3.8
90	Perú	3.8
105	Paraguay	3.4
108	Venezuela	3.4
111	Bolivia	3.3
137	Haití	2.5
138	Burundi	2.4
139	Chad	2.2

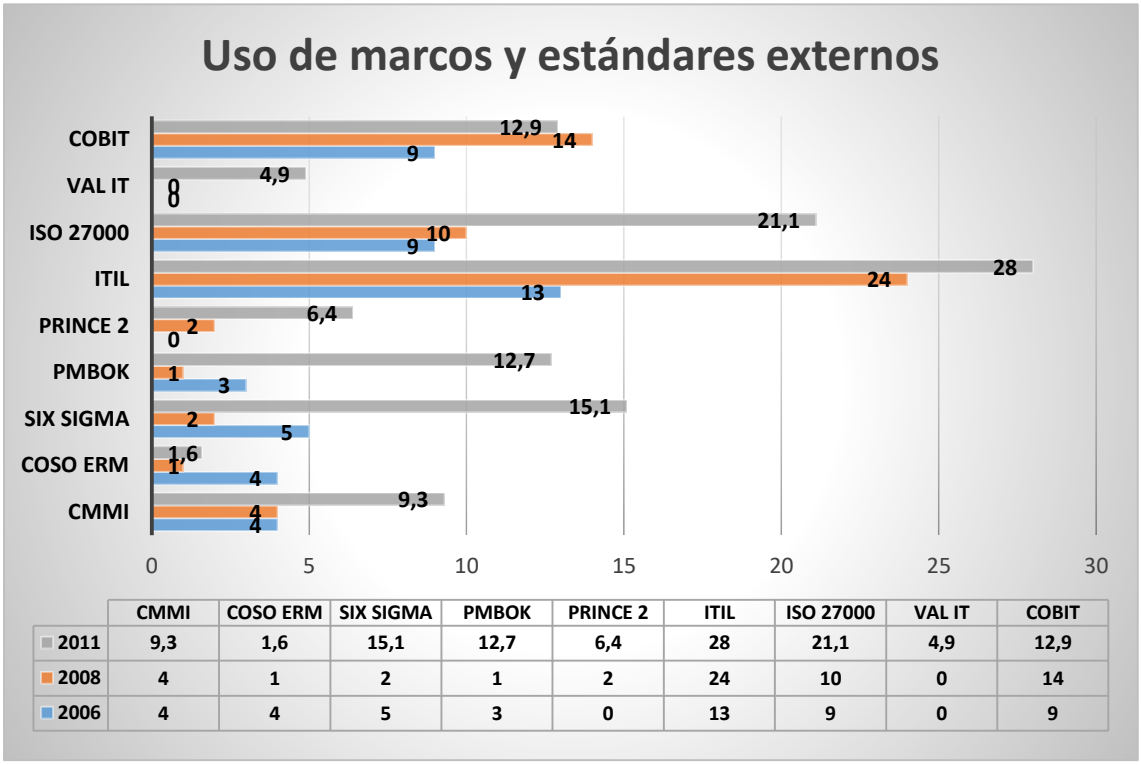
Tabla 1. Ranking 2016 de Network Readiness Index (NRI)

El Network Readiness Index (NRI), analiza cuán preparados están los países para utilizar las TIC de forma eficaz en tres dimensiones: el entorno empresarial, normativo y de infraestructura de las TIC, en general; la preparación de los tres principales interesados (individuos, empresas y gobiernos) para utilizar las TIC y beneficiarse de ellas; y el uso real de las más recientes tecnologías de la información y las comunicaciones disponibles. Y el informe The Global Competitiveness Report 2008-2009 que publica el World Economic Forum mide el grado de competitividad que tienen los países analizando una serie de componentes como Tamaño del

gobierno, Estabilidad macroeconómica, Infraestructuras, Educación, Eficiencia del mercado laboral, Innovación, Estructura legal y seguridad de los derechos de propiedad, etc.

Colombia tiene un índice de preparación para utilizar las TIC de 4.1 que lo sitúa en el puesto 68 de 139 a nivel mundial (bajando 4 puestos a comparación del ranking del año anterior) y en el quinto puesto en Latinoamérica. Con estos informes se evidencia la importancia de la TIC para lograr un país competitivo y Colombia debe incrementar la aplicación de estas siempre con estándares de calidad que logren posicionar a Colombia como líder en Latinoamérica y luego a nivel mundial

El auge de las TIC, trajo consigo el desarrollo de buenas prácticas en la industria para la administración de servicios de Tecnologías de Información. Según IT Governance Global Status Report – 2011 entre 834 organizaciones encuestadas a nivel mundial, los marcos de referencia más utilizados son ITIL o ISO 2000, ISO 27000 y COBIT y entre las buenas prácticas de proyectos están PRINCE y PMI.



	CMMI	COSO ERM	SIX SIGMA	PMBOK	PRINCE 2	ITIL	ISO 27000	VAL IT	COBIT
2011	9,3	1,6	15,1	12,7	6,4	28	21,1	4,9	12,9
2008	4	1	2	1	2	24	10	0	14
2006	4	4	5	3	0	13	9	0	9

Figura 8. Tendencias en el uso de marcos y estándares externos.

Fuente. Adaptado del Global Status Report on the Governance of Enterprise IT (Geit)

En Colombia entre los marcos de referencia, estándares y metodologías más utilizados según La Encuesta de Gerencia de Proyectos en Tecnologías de Información, se encuentra el estándar de fundamentos PMBoK® del Project Management Institute (PMI®).

Es de resaltar que los proyectos gestionados bajo una metodología ágil aparecen con un 7.6% pasando de casi 20% en 2017, tal vez como resultado de incluir una nueva opción sobre esquemas híbridos que obtuvo cerca del 18%.

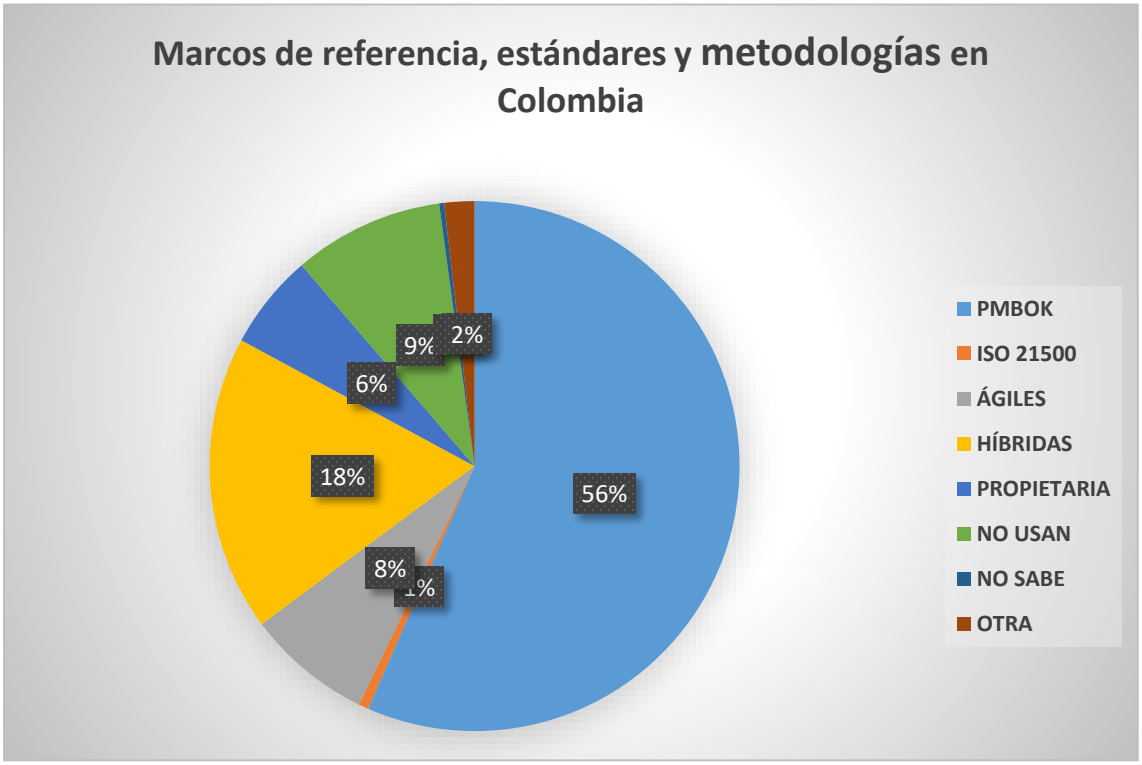


Figura 9. Marcos de referencia, estándares y metodologías en Colombia.

Por otro lado, la encuesta de certificaciones ISO 2017 refleja el número de certificados válidos que tienen las diferentes empresas a nivel mundial a corte 31 de diciembre de 2017, identificando lo siguiente:

RANKING	PAIS	PUNTAJE
1	Japón	9161
2	China	5069
3	Reino Unido de Gran Bretaña e Irlanda del Norte	4503
4	India	3272
5	Estados Unidos de América	1517
23	México	315
34	Brasil	170
35	Colombia	148
50	Chile	64
52	Argentina	57
57	Perú	43
64	Uruguay	31
73	Costa Rica	21
87	Ecuador	8
88	Panamá	8
89	Bolivia	7
107	Venezuela	4
128	Paraguay	2
158	Tayikistan	1
159	Uzbekistan	1
160	Vanuatu	1

Tabla 2. Número de certificaciones en ISO 27000 por país.
Fuente. Adaptado The ISO Survey of Management System Standard Certifications

A nivel mundial se cuenta con un total de 39501 certificaciones en la norma ISO 270001, de las cuales a nivel Latinoamérica, Colombia ocupa el tercer puesto con 148 certificaciones y el puesto 35 a nivel mundial, lo que ni equivale al 1% de certificaciones.

3.2. ESTADO ACTUAL.

El estado actual de este trabajo de grado tiene el propósito de describir la forma en la cual la Alcaldía de Cartagena realiza el proceso de gestión de riesgos dentro de sus proyectos.

La Alcaldía de Cartagena posee una taxonomía de riesgos predeterminada que utiliza en todos sus proyectos sin tener en cuenta la naturaleza y/o tipo de proyecto. Esta taxonomía está conformada de la siguiente forma:

- ✓ **RIESGOS CREDITICIOS:** Estos son los efectos favorables y desfavorables de la alteración de las condiciones de financiación como consecuencia de la variación del mercado y la obtención de recursos para adelantar el objeto contractual –100% para el contratista.
- ✓ **RIESGOS CAMBIARIOS:** Pueden darse en caso de que los bienes o servicios objeto del futuro proceso contractual deban ser importados y/o el oferente adjudicatario plantee su rentabilidad en otra divisa. En estas ocasiones el oferente adjudicatario deberá asumir el ciento por ciento (100%) de las pérdidas ocasionadas por la fluctuación en las tasas de cambio correspondientes.
- ✓ **RIESGOS DE OPERACIÓN:** El riesgo de operación hace referencia al no cumplimiento de parámetros de desempeño, calidad y originalidad de los bienes y servicios especificados y al incremento abrupto de los costos del servicio y de los insumos, mayores a los proyectados. Adicionalmente puede presentarse el riesgo de ser sujeto activo de un hecho que ocasione responsabilidad civil extracontractual o daño a terceros o bienes ajenos por parte del contratista, con bienes de la entidad contratante.
- ✓ **PERDIDA DEL MATERIAL:** La pérdida, destrucción, deterioro o robo de los elementos requeridos para desarrollar el objeto contractual y dentro de la ejecución del futuro contrato u orden de compra, correrá a cargo del contratista adjudicatario hasta el recibo final a entera satisfacción de los bienes 100% para el contratista.
- ✓ **OTROS RIESGOS:** En general, los efectos, favorables o desfavorables, de las variaciones de los componentes económicos y técnicos necesarios para cumplir con las obligaciones del Contratista necesarias para la cabal ejecución de este Contrato, relacionadas con la consecución de la financiación, la contratación de personal, las labores administrativas, los procedimientos utilizados, los equipos y materiales requeridos, entre otros.

MATRIZ DE RIESGOS								
TIPIFICACIÓN DEL RIESGO			ASIGNACIÓN DEL RIESGO		CATEGORIZACIÓN DEL RIESGO			PORCENTAJE DE RIESGO A ASUMIR DE ACUERDO CON EL MONTO DEL EVENTO PRESENTADO
					PROBABILIDAD	MAGNITUD	DURACIÓN	
o.	DESCRIPCIÓN	OBSERVACIONES	DISTRITO	PROPONENTE Y/O CONTRATISTA	EVALUADA	EVALUADA	EVALUADA	
	RIESGOS							
	Paros ocasionados por los trabajadores y personal a cargo del Contratista por la no cancelación oportuna de salarios y prestaciones sociales y demás beneficios a que tengan derecho.	Riesgo que asume el Contratista, es quien tiene la obligación de cubrir las obligaciones laborales de sus trabajadores a que haya lugar.		X	Baja	Baja	Baja	100%
	Errores involuntarios que hayan quedado en el pliego de condiciones, unidades, Cantidades, especificaciones, descripción del proyecto y/o estudios previos, operaciones aritméticas, etc.	Responde el DEPARTAMENTO.	X		Baja	Baja	Baja	100%
	Errores cometidos en la elaboración de la propuesta presentada por el Contratista. Errores cometidos en documentos elaborados por el Contratista durante la ejecución del contrato.	Riesgo que asume el Contratista.		X	Baja	Baja	Baja	100%
	Precios artificialmente bajos en la propuesta de la Contratista.	Riesgo que asume el contratista.		X	Baja	Baja	Baja	100%
	No pago oportuno, por parte del Contratista, a toda clase de proveedores en relación con compras, alquileres, servicios, contratos, etc.	Riesgo que asume el Contratista.		X	Baja	Baja	Baja	100%

	Problemas presentados entre socios y/o consorciados y/o integrantes de uniones temporales y/o familiares de las empresas y/o firmas que conforman al Contratista y que contratan con EL DISTRITO.	Riesgo que asume el Contratista.		X	Media	Media	Media	100%
	Demora y errores en la legalización del contrato, en la radicación oportuna de las actas y/o cuentas con su soportes (correctamente diligenciadas y firmadas).	Riesgo que asume el Contratista, dado que le corresponde tener la debida diligencia y cuidado en la presentación y/o elaboración de los documentos.		X	Baja	Baja	Baja	100%
	Demora involuntaria en la revisión y trámite de actas y/o cuentas por parte de supervisores de contrato y/o funcionarios del DISTRITO.	Riesgo que asume el Contratista, teniendo en cuenta el alto volumen de trabajo que tienen estos funcionarios.		X	Baja	Baja	Baja	100%
	Cambios de normatividad aplicable durante la ejecución del contrato.	Riesgo compartido.	X	X	Baja	Baja	Baja	50%
0	Prórrogas al contrato	Según las circunstancias que amparan la prórroga, es compartido este riesgo.	X	X	Media	Media	Media	50%
1	Variación Tributaria	Riesgo del Contratista, que asume las cargas impositivas vigentes a la fecha de suscripción del contrato y asume el riesgo tributario por creación de nuevos impuestos.		X	Media	Alta	Media	100%
2	Daños por terceros	El Contratista asume el riesgo por daños, perjuicios ó pérdida		X	Media	Alta	Media	100%

		de los bienes de su propiedad causados por terceros						
3	Fuerza Mayor y Caso fortuito	El Contratista asume el riesgo por efectos favorables o desfavorables de eventos inesperados. En general los riesgos por las variaciones de los componentes económicos, legales y técnicos, necesarios para cumplir con las obligaciones de la Contratista durante la ejecución del contrato, relacionadas con las labores administrativas, son asumidos por el Contratista.		X	Media	Alta	Baja	100%

Tabla 3. Distribución y Asignación de Riesgos.

De lo anterior, se identifica que el contratista es el que responde por la gran mayoría de la materialización de riesgos. En el informe de auditoría modalidad especial vigencia 2017 realizado por la Contraloría Distrital de Cartagena de Indias a proyectos T.I de la Alcaldía, identificó que la taxonomía utilizada para la gestión de riesgos no es la adecuada; ya que al materializarse diferentes riesgos las dependencias del Distrito no cuentan con ningún plan de contingencia y/o plan de acción.

De igual forma identificó la materialización de riesgos similares en diferentes proyectos T.I de diferentes dependencias que no encajan en la taxonomía usada. Estos riesgos son:

- No se define ni se documenta la arquitectura de los sistemas de información.

- No se define una metodología formal para el desarrollo y mantenimiento de software, que oriente los proyectos de construcción o evolución de los sistemas de información que se desarrollen a la medida, ya sea internamente o a través de terceros, lo que ocasiona que no se realice de forma correcta los análisis de requerimientos técnicos y funcionales necesarios para la definición del software a nivel de sistema y del diseño del software.
- Nula participación de los involucrados tanto al interior como exterior de la dependencia.
- Los sistemas de información quedan obsoletos de forma muy rápida debido a que no establecen criterios de aceptación ni se definen Acuerdos de Nivel de Servicio (ANS) el cual abarque el mantenimiento de los sistemas de información.
- Atentados contra la disponibilidad, integridad y confidencialidad de la información (ataques a los dispositivos activos y pasivos de la red).

Como observación final, la Contraloría Distrital estableció que la Alcaldía no garantiza la continuidad y la disponibilidad de los servicios Tecnológicos, asimismo identificó que el Distrito no posee la capacidad de atención y resolución de incidentes para ofrecer continuidad de la operación y la prestación de todos los servicios T.I utilizados, por tal motivo aconsejó al distrito que debe realizar el análisis y gestión de los riegos asociados a su infraestructura tecnológica haciendo énfasis en aquellos que puedan comprometer la seguridad de la información o que puedan afectar la prestación de un servicio de T.I.

3.3. ESTADO DEL ARTE

3.3.1. REVISIÓN BIBLIOGRÁFICA.

En busca de elementos que permitan orientar el presente estudio, se realiza un recorrido por los diferentes soportes teóricos y aportes de diferentes autores, quienes desarrollaron supuestos que en la actualidad han enmarcado los diferentes lineamientos y estrategias que posibilitan la gerencia de proyectos, así como también la determinación y fortalecimiento de la gestión de riesgos en las organizaciones.

Numerosos estudios se han llevado a cabo sobre la identificación y el manejo de los factores de riesgo del software. Estos estudios datan de 1975, cuando Brooks citó las causas del fracaso del proyecto sobre la base de su experiencia en IBM. A partir de entonces, muchos investigadores han estado trabajando en la identificación y gestión de riesgos de proyectos de naturaleza T.I.

Dey et al. (2007), a través de un estudio de caso en la Oficina de Planificación de Town and Country (TCPO) en Barbados, identificó la falta de disponibilidad de personal clave, rotación de personal y requisitos incorrectos / incompletos como los riesgos que afectan el desarrollo de software. El estudio también desarrolló un marco integrado para la gestión del riesgo en el desarrollo de software con la participación de los interesados en el TCPO.

Verner, Evanco y Cerpa (2007) realizaron análisis estadísticos exploratorios tanto de los desarrolladores de software como de la alta dirección para identificar sus percepciones sobre los factores determinantes del éxito del proyecto y utilizaron la regresión logística para predecir el éxito del proyecto. En consecuencia, las perspectivas de los desarrolladores sugieren que es más probable que el éxito suceda si el gerente del proyecto participa en las negociaciones del cronograma; que la información de requisitos esté disponible cuando se hacen las estimaciones; el permiso del personal se toma en cuenta; y no se agregue más personal al final del proyecto para cumplir con un cronograma agresivo.

Zhou, Vasconcelos y Nunes (2008) analizaron diez casos de estudio en el Reino Unido, los Estados Unidos y Nueva Zelanda para identificar factores de riesgo críticos en las etapas de pre-implementación e implementación del proyecto de software, dando como resultado la fluencia del alcance, falta de voluntad del cliente para aceptar sistemas finales, mala gestión del proyecto, entre otros.

Bannerman (2008) realizó un estudio en agencias gubernamentales en Australia para investigar las prácticas de un gobierno estatal cuando se trata de proyectos de software. El análisis del estudio descubrió diez categorías de factores de riesgo: gobernanza del proyecto, configuración del proyecto, compromiso del socio, propiedad empresarial, gestión del proyecto, gestión del cambio, gestión de proyectos, reconocimiento de señales de alerta, gestión de riesgos y realización de beneficios.

Iacovou y Nakatsu (2008) utilizaron el método de encuesta de Delhi en 57 profesionales senior de TI e identificaron falta de compromiso de la alta dirección, el conjunto original de requisitos mal comunicados, barrera idiomática en las comunicaciones del proyecto, falta de conocimiento técnico requerido por el equipo offshore y fracaso en considerar todos los costos como los principales factores de riesgo. El estudio tuvo como objetivo proporcionar una idea de los riesgos que afectan a los proyectos de desarrollo subcontratados en el extranjero.

Anudhe y Mathew (2009), utilizando una metodología basada en casos y entrevistas estructuradas y semi estructuradas con altos directivos de varias compañías de software indias, describieron diversos factores de riesgo que afectan los proyectos de software. Programar y administrar el presupuesto (desarrollar una cultura de trabajo colaborativo con los clientes), expectativas del cliente (educar al cliente para involucrar a un nivel profundo de participación con el cliente), captura de requisitos (recopilación de datos elaborados y análisis proactivo), personal (mantener recursos de búfer, involucrar el cliente en la contratación de recursos) y los cambios en la estructura corporativa del cliente (transparencia y comunicación adecuada) son algunos de los factores de riesgo, y su mitigación se menciona en dicho estudio.

Javani y Rwelamila (2016) realizaron un estudio con el objetivo de identificar el reconocimiento, la aplicación y la comprensión de la gestión de riesgos en proyectos de tecnología de la información (TI) en el sector público sudafricano y así contribuir a la brecha de investigación, concluyendo que se debe implementar bases de datos y herramientas para administrar el riesgo en proyectos de TI. Estos actuarán como herramientas para comunicar los riesgos de los proyectos de TI durante la implementación del proyecto, aumentando así la probabilidad de éxito del proyecto.

Curcio, Navarro, Malucelli y Reinehr (2018) identificaron que cinco de los ocho factores principales de cancelación de proyectos TI están relacionados con los requisitos. Los requisitos incompletos, la baja participación del cliente, las expectativas poco realistas, los cambios en los requisitos y los requisitos innecesarios se enumeraron como los principales factores, estableciendo la necesidad de investigaciones futuras, entre las que se incluyen la obtención de requisitos, la gestión de cambios, los requisitos de medición, las herramientas de requisitos de software y los estudios comparativos entre los requisitos tradicionales y los ágiles. En esta investigación, también se identificaron algunos obstáculos que enfrentan los profesionales al tratar con la ingeniería de requisitos en un contexto ágil. Están relacionados con el medio ambiente, las personas y los recursos.

3.3.2. ESTÁNDARES Y METODOLOGÍAS ANALIZADAS

En virtud de lo anterior, se puede afirmar que los modelos de gestión de riesgos se pueden aplicar a un sector, una industria, una organización, una unidad de negocio o un equipo para proporcionar una hoja de ruta para el cumplimiento de los objetivos. Por lo tanto, también se puede aplicar a los proyectos T.I de la Alcaldía de Cartagena.

Del universo de marcos de referencia, estándares y metodologías en gestión de proyectos referenciados en el marco teórico de esta investigación, se seleccionaron aquellos modelos más utilizados. Además de lo anterior, los modelos finalmente seleccionados para la construcción del nuevo modelo deben ser de carácter genérico y de fácil implementación, también se descartan aquellos que son propios de una industria o de un área en específico y que apliquen solo a

programas o portafolios, en otras palabras, se seleccionarán aquellos que posibiliten iniciar un proceso de identificación de debilidades y fortalezas en materia de gestión de proyectos.

A partir de lo anterior se analizan y seleccionan los modelos que servirán de base para el diseño del nuevo modelo basado en los elementos teóricos pertinentes para la aplicación y desarrollo de la presente investigación.

3.3.2.1. COSO ERM.

En el contexto empresarial actual, el estándar internacional de gestión de riesgos de mayor reconocimiento es el estándar COSO – ERM[5], publicado el año 2004 bajo el concepto integrado de gestión de riesgos. El COSO, "Enterprise Risk Management – Integrated Framework" publicado el 2004, define ERM como:

> Gestión de riesgos empresariales es un proceso efectuado por el directorio, gerentes, y otros funcionarios, aplicada en el establecimiento de la estrategia en todos los niveles de la empresa, diseñado para identificar potenciales eventos que puede afectar a la entidad, y gestionar el riesgo dentro de su apetito de riesgo, para proveer seguridad razonable en relación con el logro de objetivos empresariales. (COSO, 2004, p. 4).

El marco para la gestión integrada de riesgos COSO ERM, busca ayudar en la creación de valor para los accionistas a través de una estructura adecuada e interrelacionada enfocada en gestionar los riesgos de la organización de forma integral. El valor se maximiza en la medida en que se cuente con objetivos y estrategias establecidas para lograr un adecuado balance entre crecimiento, metas, rentabilidad, riesgos, y el uso efectivo y eficiente de los recursos de la organización. Esta estructura, fluye a través de los distintos niveles de la organización, con roles y responsabilidades establecidos enfocados en la gestión de riesgos.

[5] Es una versión mejorada y enfocada en gestión de riesgos del texto "*COSO, Control Interno – Marco Integrado",* publicado en 1992 y modificado en 1994.

Lo que se busca es contar con un único marco o metodología estándar de gestión de riesgos para ayudar a la gerencia a lograr el desempeño y rentabilidad deseados previniendo la pérdida innecesaria de recursos, o en su defecto, mantener las pérdidas en los niveles de apetito y tolerancia al riesgo (COSO ERM 2004, p. 3-9).

COSO ERM incluye cuatro categorías de objetivos y ocho componentes, indicando que el control interno es parte de la gestión integral de riesgos. A continuación se muestra el esquema general de la relación entre los objetivos y los componentes en una matriz tridimensional, llamado "cubo COSO ERM".

Figura 10. Cubo COSO ERM.

Las cuatro categorías de objetivos son los siguientes:

- **Estratégicos:** Metas de alto nivel, alineados con la visión y misión de la organización. Reflejan la elección de la alta dirección en cuanto a cómo la entidad procurará crear valor para sus grupos de interés.

- **Operativos:** Relacionados con la eficacia y eficiencia de las operaciones de la entidad, incluyendo los objetivos de rendimiento y rentabilidad y de salvaguarda de recursos frente a pérdidas.
- **Reporte:** Relacionados con la confiabilidad de la información reportada (sea interna o externa, de carácter financiero y no financiero).
- **Cumplimiento:** Relacionados al cumplimiento de las leyes y regulaciones aplicables. (COSO ERM, 2004, p. 35-36).

Los ocho componentes se describen a continuación:

- **Ambiente interno:** Abarca el entorno de la organización, es la base de todos los componentes de la gestión de riesgos, proporcionando disciplina y estructura. Influye en cómo se establecen las estrategias y los objetivos; cómo se estructuran las actividades del negocio; y cómo se identifican, evalúan y controlan / mitigan los riesgos. Está comprendido por:
  - ✓ Filosofía de gestión de riesgo.
  - ✓ Apetito por el riesgo.
  - ✓ Rol de supervisión del Directorio.
  - ✓ Integridad y valores éticos.
  - ✓ Compromiso de competencia.
  - ✓ Estructura organizacional y procesos.
  - ✓ Asignación de autoridad y responsabilidad.
  - ✓ Políticas y prácticas de Recursos Humanos.
  - ✓ Políticas y Procedimientos de Gestión de Riesgos.
  - ✓ Crear Área/Unidad de Riesgo. (COSO ERM, 2004, p. 27-34)
- **Establecimiento de objetivos:** Los objetivos son definidos a nivel estratégico alineados a la visión y misión de la organización, estableciendo la base para los objetivos operativos, de reporte y cumplimiento. Una condición previa para la efectiva identificación de eventos, evaluación de riesgos y respuesta de riesgos es el

establecimiento de objetivos. Los objetivos están alineados con el riesgo aceptado de la entidad, el cual impulsa sus niveles de tolerancia al riesgo. Está comprendido por:

- ✓ Objetivos Estratégicos.
- ✓ Objetivos de Operación.
- ✓ Objetivos de Reporte.
- ✓ Objetivos de Cumplimiento.
- ✓ Apetito por el riesgo: El monto total de riesgo que una compañía u otra entidad desea aceptar para la obtención de su misión / visión.
- ✓ Tolerancia al riesgo: La variación relativa aceptable para el logro de un objetivo (COSO ERM, 2004, p. 35-40).

- **Identificación de eventos:** Un evento es un incidente o hecho, derivado de fuentes internas o externas, que afecta la ejecución correcta de la estrategia o el logro de objetivos. Eventos con impacto negativo representan riesgos, mientras que eventos con impacto positivo representan oportunidades. Está comprendido por:
  - ✓ Eventos: positivos o negativos.
  - ✓ Factores externos: económicos, naturaleza y medio ambiente, políticos, culturales, sociales, tecnológicos.
  - ✓ Factores internos: infraestructura, personal, procesos, tecnología.
  - ✓ Técnicas de identificación de eventos.
  - ✓ Interdependencia de eventos.
  - ✓ Categorías de eventos.
  - ✓ Distinción de riesgos y oportunidades (COSO ERM, 2004, p. 41-47).
- **Evaluación de riesgos:** La evaluación de riesgos permite que la organización estime en qué medida eventos potenciales afectan el logro de sus objetivos. La evaluación de riesgos se realiza a través de dos perspectivas: impacto y probabilidad. Los enfoques cuantitativos no sustituyen necesariamente a los enfoques cualitativos, más bien se complementan. Comprende lo siguiente:
  - ✓ Riesgo inherente y residual.

- ✓ Impacto y probabilidad.
- ✓ Metodologías y técnicas:
  - Enfoques cualitativos
    - Autoevaluación.
    - Mapas de riesgo.
  - Enfoques cuantitativos
    - Distribuciones de severidad y frecuencia.
    - Procesos estocásticos (COSO ERM, 2004, p. 49-54).

➢ **Respuesta al riesgo:** Habiendo identificado los riesgos significativos, la gerencia determina como responderá para mitigarlos, eligiendo entre las estrategias alternativas de: evitar, reducir, compartir o aceptar. Se evalúa el efecto en el impacto y probabilidad del riesgo, así como el costo-beneficio, seleccionando una respuesta que lleve al riesgo residual a ubicarse dentro de la tolerancia del riesgo deseado. Comprende lo siguiente:

- ✓ Categorías de Respuestas.
- ✓ Identificar respuestas al riesgo.
- ✓ Evaluar efectos en impacto y probabilidad.
- ✓ Evaluar costo-beneficio.
- ✓ Selección de respuestas (COSO ERM, 2004, p. 55-60).

➢ **Actividades de control:** Establecimiento y revisión continua de políticas y procedimientos que ayudan a la gerencia a asegurar que las respuestas a los riesgos son llevadas a cabo; en sí mismas estas actividades pueden ser la respuesta al riesgo. Ocurren a lo largo de toda la organización, a todo nivel y función y logran cumplir con los objetivos de la entidad en todas sus categorías. Incluye lo siguiente:

- ✓ Integración con la respuesta al riesgo.
- ✓ Tipos de actividades de control:
  - Preventivas vs. Detectivas.
  - Manuales vs. Automatizadas.
- ✓ Controles en sistemas de información:

- Controles generales.
- Controles específicos (COSO ERM, 2004, p. 61-66).

- **Información y Comunicación:** Se necesita información en todos los niveles de la organización para identificar, evaluar y responder a los riesgos. La información pertinente es identificada, capturada y comunicada oportunamente, permitiendo que el personal lleve a cabo sus responsabilidades. Comprende lo siguiente:
  - ✓ Información: fuentes internas y externas, cuantitativa y cualitativa, financiera y no financiera.
  - ✓ Sistemas estratégicos e integrados.
  - ✓ Nivel de detalle y oportunidad de la información.
  - ✓ Calidad de la información.
  - ✓ Comunicación (interna y externa, vertical y horizontal) (COSO ERM, 2004, p. 67-74).
- **Monitoreo:** Consiste en determinar si el funcionamiento de la gestión de riesgos corporativos continua siendo eficaz. Se logra a través de la supervisión continua de las actividades o a través de evaluaciones independientes, o una combinación de ambos. La supervisión debe entenderse como el proceso de evaluar y monitorear la presencia y funcionamiento de los componentes de ERM. Incluye lo siguiente:
  - ✓ Evaluaciones independientes:
    - Auditores internos
    - Auditores externos
    - Especialistas
  - ✓ Evaluaciones continuas / supervisión permanente.
  - ✓ Reporte de Deficiencias (COSO ERM, 2004, p. 75-81).

3.3.2.2. ASSOCIATION FOR PROJECT MANAGEMENT –APM-.

Es una organización benéfica educativa para la profesión de proyectos, fundada en 1972 en el Reino Unido. El objetivo de APM es desarrollar y promover las disciplinas profesionales de gestión de proyectos, programas y portafolios, basándose así en cinco dimensiones para el profesionalismo en gestión de proyectos: Responsabilidad, profundidad, compromiso, logro y amplitud.

La guía de APM con el conjunto de acciones y actividades para la gestión de proyectos se conoce como Association for Project Management Body of Knowledge, el cual permite explorar las áreas esenciales en la gestión de proyectos, programas y portafolios (P3). Está estructurado en torno a cuatro secciones principales e incluye definiciones de los términos y técnicas fundamentales. Estas secciones son:

- **Contexto:** El contexto de un proyecto, programa y/o portafolio se compone de dos áreas: La gobernanza la cual se refiere al conjunto de políticas, regulaciones, funciones, procesos, procedimientos y responsabilidades que definen la gestión y control de P3. Y el área de configuración la cual es la relación del P3 con su organización, la cual aplicará la gestión estratégica para establecer sus objetivos y razón de existencia.
- **Personas:** Los P3 tienen como objetivo motivar y coordinar a las personas para lograr objetivos específicos. Esta sección cubre las habilidades interpersonales que todo gerente necesita, como lo son la comunicación, manejo de conflictos, delegación, influencia, liderazgo, negociación y trabajo en equipo.
- **Entregables:** Esta sección trata sobre la entrega de productos, resultados y beneficios; cubriendo las siguientes áreas:
  - ✓ **Alcance:** ¿Cuáles son los objetivos y el alcance del trabajo?
  - ✓ **Programación:** ¿Cuánto tiempo llevará lograr el trabajo?
  - ✓ **Finanzas:** ¿Cómo se gestionan los fondos y los costos necesarios?
  - ✓ **Riesgo:** ¿Cuáles son las amenazas y oportunidades involucradas?

- ✓ **Calidad:** ¿Cómo se garantizará la idoneidad para el propósito de los entregables y los procesos de gestión?
- ✓ **Recursos:** ¿Cómo se adquirirán, movilizaran y gestionaran los recursos necesarios?

➢ **Interfaces:** Los gerentes de proyectos, programas y portafolios deben tener una comprensión de cómo las disciplinas como la ley, la contabilidad y la gestión de recursos humanos repercuten en su trabajo.

Para la gestión de riesgos, APM posee un documento conocido como la Guía del PRAM, en esta guía se describe un enfoque sistemático y disciplinado para controlar los riesgos, la cual puede ser utilizada para ayudar a mejorar el éxito de los proyectos.

La guía PRAM plantea inicialmente unos beneficios de la gestión de riesgos a nivel del proyecto, los cuales denomina “Beneficios duros" (contingencias, decisiones, control, estadísticas y similares) y “Beneficios blandos" (personas que están implícitas en algunos de los beneficios duros, pero que no suelen expresarse como beneficios por derecho propio); estos beneficios se describen en la tabla número 4.

BENEFICIOS DUROS	BENEFICIOS BLANDOS
H1 Permite tener planes, programas y presupuestos mejor informados y creíbles.	S1 Mejora la experiencia corporativa y la comunicación general.
H2 Aumenta la probabilidad de que un proyecto cumpla con su cronograma y presupuesto.	S2 Conduce a un entendimiento común y a un mejor espíritu de equipo.
H3 Conduce a la utilización de un tipo de contrato más adecuado.	S3 Ayuda a distinguir entre la buena suerte y la buena gestión y entre la mala suerte y la mala gestión.
H4 Permite una evaluación y justificación más significativa de las contingencias.	S4 Ayuda a desarrollar la capacidad del personal para evaluar los riesgos.
H5 Desalienta la aceptación de proyectos financieramente bajos.	S5 La gestión de proyectos centra la atención en los problemas reales y más importantes.
H6 Contribuye con la acumulación de información estadística para ayudar a una mejor gestión de los proyectos futuros.	S6 Facilita una mejor aceptación de riesgos, lo que aumenta los beneficios obtenidos.

H7 Permite una comparación más objetiva de alternativas.	S7 Demuestra una actitud responsable frente a los clientes.
H8 Identifica y asigna las responsabilidades al mejor propietario de riesgo.	S8 Proporciona una nueva visión de los problemas de personal en un proyecto.

Tabla 4. Beneficios Duros y Blandos de la Gestión de Riesgos de Proyecto.
Fuente: Adaptado de Guía de Análisis y Gestión de Riesgos de Proyectos 2a. Edición - (Association for Project Management, 2004).

Adicionalmente, se definen unos beneficios a nivel de la organización registrados en la tabla número 5.

BENEFICIOS DUROS	BENEFICIOS BLANDOS
H9 Cumplimiento con los requisitos de gobierno corporativo.	S9 Mejor reputación como resultado de un menor número de fracasos de los proyectos principales.
H10 Un mayor potencial futuro de los negocios con los clientes existentes.	S10 Mejores relaciones con los clientes, debido a un mejor desempeño de los proyectos en curso.
H11 Reducción de base de costos.	S11 Un ambiente de trabajo menos estresante.

Tabla 5. Beneficios Duros y Blandos de la Gestión de Riesgos de Proyecto en toda la Organización.
Fuente: Adaptado de Guía de Análisis y Gestión de Riesgos de Proyectos 2a. Edición - (Association for Project Management, 2004).

La guía PRAM plantea un proceso de gestión de riesgo compuesto por 5 fases y una actividad denominada “Gestionar Proceso” como se describe en la figura número 12; el proceso es iterativo en sí mismo, por lo que la salida de cada fase puede requerir que una fase anterior hay sido ejecutada.

En la Figura número 12 las líneas continuas gruesas indican el ciclo iterativo importante, las líneas continuas delgadas muestran otros posibles vínculos de vuelta a fases anteriores, y las líneas punteadas representan la obligación de gestionar el proceso en todas sus etapas.

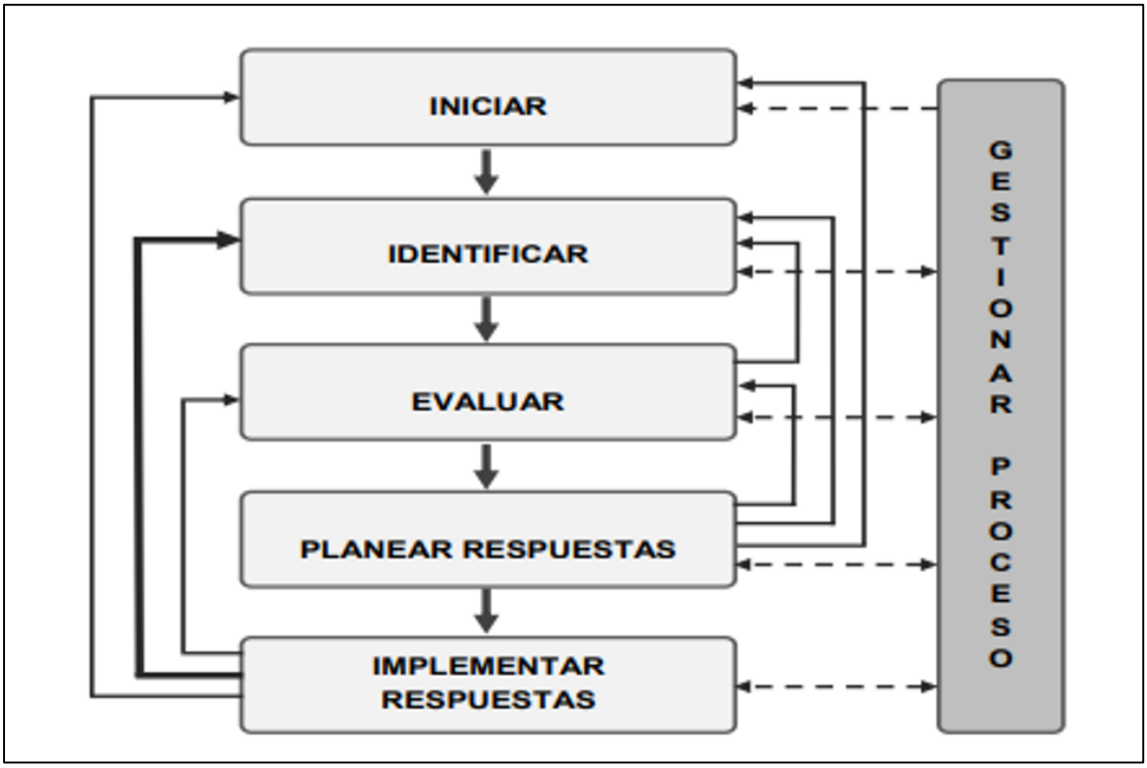


Figura 11. Proceso de Gestión de Riesgos – Guía PRAM
Fuente: Tomado de Guía de Análisis y Gestión de Riesgos de Proyectos 2a. Edición - (Association for Project Management, 2004).

El proceso de gestión de riesgos debe aplicarse durante todo el ciclo de vida del proyecto y debe estar integrado con los demás procesos de gestión del proyecto. En cuanto a la información sobre la gestión de riesgo debe notificarse a los otros procesos del proyecto, incluyendo el plan de gestión del proyecto, presupuesto, estimación de recursos, gestión de cambios, gestión de calidad y gestión de los interesados.

Las fases del proceso se pueden dividir en sub-fases como muestra en la figura número 13, dependiendo de cómo se quiera el proceso; de modo que el nivel deseado de detalle del proceso de gestión debe ser determinado por las necesidades específicas de cada proyecto o por el grado de madurez de la capacidad de gestión de riesgos de la organización en donde se vaya a aplicar.

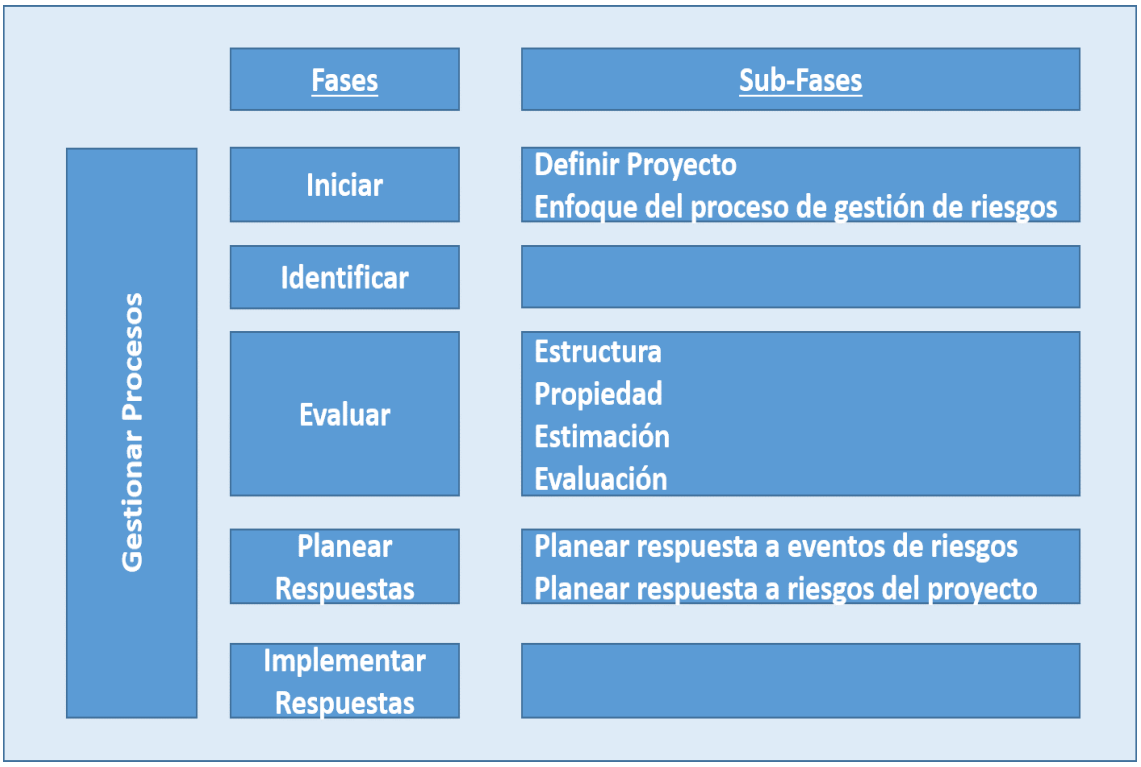


Figura 12. Estructura de las Fases y Sub-fases del Proceso Gestión de Riesgos. Fuente: Adaptado de Guía de Análisis y Gestión de Riesgos de Proyectos 2a. Edición - (Association for Project Management, 2004).

Las fases y sub-fases que componen el proceso de gestión de riesgos de proyecto definido en la guía PRAM permiten lo siguiente:

- **Iniciar:** Tiene como propósito establecer el alcance, los objetivos y el contexto para gestionar el proceso. Esta fase se divide en dos sub-fases:
  - **Definir el proyecto:** Tiene por objeto garantizar un entendimiento común del proyecto para el cual se va aplicar el proceso de gestión de riesgos, debe tener unos objetivos bien definidos que reflejen las expectativas de los interesados en el proyecto, incluidos los de la puesta en marcha del proyecto, y deben ser apoyados por los criterios cuantificables de éxito; de igual manera debe tener un alcance bien definido (que está incluido y excluido, porque se está llevando a cabo el proyecto,

relación del proyecto con otros proyectos). Se debe definir el alcance en términos de que los productos sean el resultado del proyecto.

El Proyecto debe tener una estrategia bien definida y un plan general de ejecución del proyecto, estos deben estar bien establecidos y entendidos para que una estrategia de prevención de riesgos sea adaptada a las necesidades específicas del proyecto. Si el proyecto carece de adecuada definición de objetivos, de alcance, de estrategia o del plan, esta debilidad debe corregirse antes que el proceso de gestión del riesgo descrito sea aplicado de manera eficaz.

- **Enfoque del proceso de gestión de riesgos:** Los objetivos del proceso deben ser bien comprendidos y documentados antes de su aplicación a un proyecto, así como los requisitos de alto nivel (gestión de riesgos estratégicos o procesos de gobierno corporativo). Los objetivos definidos en la aplicación del proceso deben ser revisados periódicamente durante la ejecución y actualizados en forma apropiada. La gestión de riesgos debe aplicarse desde el inicio (a ser posible antes de hacer compromisos significativos) y durante el ciclo de vida del proyecto; al igual, que la definición de la estrategia de riesgos debe establecerse desde el comienzo, teniendo en cuenta los objetivos de gestión de riesgo, políticas, procedimientos, métodos, la organización, las funciones, la infraestructura de personal, las habilidades y las herramientas a utilizar.

  Las decisiones sobre la estrategia de gestión de riesgos deben documentarse de forma adecuada (dentro de un plan de gestión de riesgos). La responsabilidad de garantizar que el proyecto cuente con las medidas adecuadas de gestión de riesgos y que éstas se apliquen en la práctica, recae en el gerente del proyecto.

  La profundidad o nivel en el que el proceso de gestión de riesgos debe aplicarse en cada etapa del ciclo de vida del proyecto y debe ser acorde con las circunstancias del proyecto. Los factores a considerar en la determinación de un nivel apropiado de intensidad son: (a) La importancia de realizar el proyecto para la organización, (b) El tamaño o el valor del proyecto, (c) La complejidad del proyecto, (d) El grado

en que el proyecto representa cambio, (e) La estabilidad percibida de la línea base del proyecto, (f) La novedad del enfoque que se planea y (g) Cualquier conocimiento previo del nivel de riesgo al que se enfrenta el proyecto En un proyecto en ejecución, la gestión de riesgos debe ser aplicada de manera cíclica, por lo que la evaluación de la exposición al riesgo del proyecto puede mantenerse al día y la respuesta del proyecto ajustada según sea necesario.

Así mismo, el proceso de gestión de riesgos debe ser una parte integral del proceso de gestión del proyecto, y debe abordar el nivel cultural de la organización. La estructura definida en la organización para apoyar la gestión de riesgos debe ser parte integral del equipo de proyecto, y con la ayuda de expertos externos del proyecto cuando sea necesario; al igual, se deben proporcionar los recursos suficientes para la práctica efectiva del proceso, en la profundidad e intensidad que justifique el proyecto.

La Información de la gestión de riesgo debe disponerse un registro de riesgos en una forma que promueva la eficiencia del proceso de gestión de riesgo y facilite cualquier actividad de revisión o auditoría. Los registros deben ser adecuados para el propósito del proyecto y deben mantenerse a fin de que las lecciones aprendidas del proyecto puedan ser aplicadas a los proyectos futuros de la organización.

Es necesario asegurar una correcta aplicación de los procedimientos de gestión de riesgos propuestos los proyectos, a través de la integración con el sistema de control de calidad y con la generación de insumos para el proceso de auditoría de la organización.

- **Identificar:** Esta fase tiene como fin evidenciar los eventos de riesgo relacionados con los objetivos del proyecto, mediante una identificación de forma amplia, práctica y rentable. Las respuestas para algunos eventos de riesgo pueden ser definidas durante esta fase, si no se establecen en este momento, deben ser establecidos en la fase "Planear Respuestas". Debe adoptarse un enfoque para la identificación de riesgos que de la confianza y capacidad al proyecto para elaborar una lista de los eventos de riesgo,

que sea lo más completa posible, que abarque todos los tipos y fuentes de evento de riesgos pertinentes, al igual se debe consultar a los interesados y buscar opiniones externas cuando sea conveniente y práctico; se deben consultar las lecciones aprendidas de experiencias anteriores en materia de gestión de riesgo de proyectos similares.

El objetivo debe estar orientado a obtener información objetiva y el método utilizado debe promover una respuesta abierta a partir de los individuos que pueden ser abordados. Después de identificar un evento de riesgo, se debe validar en la medida de lo posible la veracidad de la información inicial y la exactitud de la descripción de las características del evento de riesgo. El esfuerzo dedicado a la validación debe ser proporcional al nivel de la probabilidad o de lo contrario los datos obtenidos sobre el evento de riesgo podrían ser inexactos.

- **Evaluar:** Esta fase tiene como objetivo aumentar la comprensión de cada evento de riesgo identificado a un nivel donde se puedan tomar decisiones adecuadas y eficaces. Además de considerar los eventos de riesgo individuales, y el nivel de riesgo global del proyecto, mediante un efecto combinado de los riesgos individuales sobre el proyecto, lo cual se puede realizar mediante una evaluación cualitativa para eventos de riesgo individual y/o un enfoque cuantitativo para el riesgo global del proyecto, según sean las circunstancias del proyecto. Esta fase puede implicar una serie de sub-fases o puede ser llevada a cabo en una sola fase.

  La información recopilada sobre cada evento debe describir todas las características relevantes (naturaleza de la incertidumbre que enfrentan y la naturaleza de su potencial de impacto positivo o negativo). Por practicidad las evaluaciones deben ser hechas sobre la probabilidad de ocurrencia de un evento de riesgo y el impacto potencial. La prioridad de los eventos de riesgo identificados debe evaluarse en términos del nivel de la amenaza que representa para el logro de los objetivos del proyecto o de la oportunidad de mejorar los resultados; para ello, se debe establecer una ventana del impacto del riesgo e indicar cuando es probable que el impacto se produzca y así ayudar a priorizar los riesgos identificados esto puede estar relacionado con el plan del

proyecto, asegurando un tiempo adecuado para hacer frente a cada evento de riesgo de manera proactiva.

Así como hay un efecto potencial individual de cada evento de riesgo, puede haber efectos adicionales en una combinación de eventos de riesgo. El efecto combinado de todos los eventos de riesgo identificados debe ser evaluado, posiblemente utilizando un enfoque de modelos de simulación. Si se identifican respuestas preliminares, debe determinarse su eficacia y sus repercusiones en los costos. Cuando no se haya identificado respuestas, la evaluación (ya sea cualitativa o cuantitativa) debe ser considerada como un preliminar y debe revisarse en la fase de planear respuestas, con el fin de tener en cuenta las respuestas acordadas y evaluar su eficacia probable.

La fase de evaluación debe ser vista como una "foto instantánea" de la exposición al riesgo del proyecto en un momento en el tiempo, teniendo en cuenta los planes elaborados para el proyecto, el estado actual de los eventos de riesgo y la eficacia de las respuestas a los riesgos en ese momento. Esta evaluación debe ser utilizada como insumo para tomar las decisiones con respecto a la priorización de las respuestas a los riesgos. Se debe tener en cuenta el momento de los impactos de los eventos de riesgo y las interdependencias que puede haber entre los eventos de riesgo y sus efectos.

La fase evaluar se divide en 4 sub-fases, las cuales se denominan Estructura, Propiedad, Estimación y Evaluación, estas sub-fases pueden ser ejecutadas mínimo en un ciclo, tres o más según la naturaleza del proyecto, la guía del PRAM como tal plantea un máximo de tres ciclos, con una serie de actividades para cada ciclo, éstas actividades se detallan en la tabla número 6.

- **Planear Respuestas:** En esta fase se determinan las respuestas adecuadas a los eventos de riesgos individuales y se utiliza la evaluación para asegurar que el nivel de riesgo global del proyecto se pueda utilizar para ajustar o modificar la estrategia del proyecto; estos dos objetivos pueden ser abordados a través de dos sub-fases.

  La fase Planear Respuestas se aplicará en una iteración del proceso de gestión de riesgos. Las respuestas a los eventos de riesgo retroalimentan a las fases identificar y

evaluar, ya que actúa sobre las respuestas al riesgo que afectaran a los eventos de riesgo identificados y puede dar lugar a eventos de riesgo emergentes, así como a eventos de riesgo secundarios.

Planear Respuestas a los Riesgos del Proyecto alimenta nuevamente a la fase de iniciar, cuando el nivel de riesgo global del proyecto requiera cambios en la estrategia del proyecto o en todo el proceso de gestión de riesgos.

- **Planear respuestas a eventos de riesgos:** Las respuestas a los eventos de riesgo individuales identificados deben desarrollarse y aplicarse de manera justificada y práctica. El objetivo es evitar o reducir al mínimo las amenazas y explotar o maximizar las oportunidades, con el fin de optimizar la probabilidad de alcanzar los objetivos del proyecto.

  Esta sub-fase debe empezar por examinar las respuestas preliminares ya identificadas durante la fase de identificación y re-evaluarlas si no son las adecuadas, se identifican nuevas respuestas; así mismo, para todos los demás eventos de riesgo a los que no se le hayan previamente identificado respuestas deben ser revisados durante esta fase y generarle las respuestas apropiadas.

  La toma de decisiones sobre las respuestas a riesgos se puede basar en un análisis de sensibilidad y/o en estudios de compensación. Para determinar si una respuesta se justifica, el gerente del proyecto debe tener en cuenta lo siguiente: (a) La importancia relativa de los diferentes objetivos del proyecto, (b) La importancia del evento de riesgo en relación con los objetivos del proyecto, (c) La efectividad potencial de la respuesta al momento de abordar el evento de riesgo y la consecución de los objetivos del proyecto, (d) El efecto probable en el tiempo de ejecución del proyecto, el presupuesto y el rendimiento, (e) El costo esperado de realizar la acción (incluyendo el costo de oportunidad), en comparación con los posibles gastos posteriores si no se toman las medidas y si el evento de riesgo se produce (si es una amenaza) o si se pierde (si es una oportunidad), (f) La posibilidad de introducir eventos de riesgo secundarios en el proyecto, como resultado de la

implementación de las acciones de las respuestas y (g) La disponibilidad de los recursos para las acciones de respuesta al riesgo.

El desarrollo de una respuesta al riesgo incluye la planificación de reserva y debe haber condiciones de activación bien definidas para aplicar las acciones. Para que sean evidentes las condiciones de activación, es fundamental contar con un proceso eficaz de seguimiento a los avances del proyecto.

Después de haber definido las respuestas, se debe repetir de nuevo a la fase "Evaluar" y volver a evaluar los eventos de riesgo a la luz de las respuestas acordadas. Los planes del proyecto deben incluir un nivel de contingencia a la magnitud del riesgo global del proyecto que se enfrentan y el nivel necesario para una probabilidad aceptable de éxito del proyecto (o nivel de confianza).

- **Planear respuestas a riesgos del proyecto:** Esta sub-fase utiliza la información de las fases anteriores para mejorar la ejecución del proyecto. Esto incluye tomar en cuenta el riesgo global del proyecto en la planificación del proyecto y la planificación de la gestión de riesgos.

  Al aplicar la sub-fase de Planear Respuestas a los riesgos del proyecto se itera de nuevo la fase Iniciar del proceso, además de afectar a la estrategia global del proyecto. La primera iteración del proceso de gestión del riesgo es probable que sea en un nivel estratégico alto y los resultados son utilizados para informar la conducta actual del proyecto y luego las iteraciones del proceso de gestión de riesgos. El principio clave es la necesidad de utilizar un nivel razonable de planificación estratégica para la gestión de riesgos del proyecto con eficacia y eficiencia al principio del proyecto y en el desarrollo los detalles necesarios para la ejecución del proyecto sobre la base de la primera iteración por el proceso de gestión de riesgos.

  La separación de Planear Respuestas a los riesgos del proyecto de esta manera ahorra tiempo en la planificación detallada innecesaria y esfuerzos para el proyecto, al igual evita limitaciones graves que se plantean si la gestión del riesgo se hace a

nivel táctico detallado sin un análisis estratégico previo. Esto es fundamental para todos los proyectos, independientemente de su tamaño o complejidad. El resultado clave es un plan de proyecto eficaz, que incorpore los resultados de las fases de gestión de riesgos anteriores.

- **Implementar Respuestas:** En esta fase se asegura que se apliquen las acciones con base en las decisiones tomadas durante la fase Planear Respuestas. Esto incluye tanto las acciones para implementar respuestas a riesgos dirigidas a los eventos de riesgos individuales y a las acciones que afectan la planificación estratégica general y a la gestión del proyecto con base en la evaluación de los riesgos del proyecto.

  Las responsabilidades para la aplicación de las respuestas planificadas a los riesgos deben estar bien definidas y sin ambigüedades en la asignación de las personas responsables. Las respuestas deben ser verificables y los propietarios de las respuestas deben ser responsables por los resultados; estas personas deben estar facultadas con la información apropiada, la autoridad y los recursos, de la misma forma que las otras tareas de gestión del proyecto.

  La aplicación de las respuestas de cada evento de riesgo debe ser controlada de manera que la respuesta a los riesgos y/o contingencia puedan ser ajustadas o se apliquen en forma apropiada. Esto implica volver a aplicar el enfoque descrito en las fases anteriores en la medida que las situaciones cambian. Los criterios establecidos deben ser bien definidos para determinar en qué punto cada evento de riesgo puede ser retirado de la atención del proceso de gestión de riesgos.

  Los participantes en el proyecto deben contar con información actualizada y precisa del riesgo a un nivel y frecuencia adecuada con sus intereses y necesidades. La información sobre el riesgo debe ser proporcionada en una serie de informes de riesgo y debe abarcar aspectos tales como la naturaleza de los eventos de riesgo individuales, el efecto combinado de su impacto en los objetivos del proyecto, las prioridades para la reducción del riesgo, la situación de la reducción de riesgos y la previsión para contingencias. La estrategia y el plan del proyecto deben evolucionar de acuerdo con

las decisiones tomadas sobre las respuestas al riesgo y con los cambios en las respuestas generales de riesgo del proyecto y con los cambios en el riesgo global del proyecto.

La fase de implementar respuestas también debe abordar la eficacia del proceso de gestión de riesgos, para determinar si se cumple con el alcance y los objetivos establecidos durante la fase Iniciar; en caso de ser necesario se deben hacer modificaciones en el proceso y documentarlas en el plan de gestión de riesgos.

- **Gestionar Proceso:** La actividad Gestionar Proceso se tiene para asegurar que el proceso de gestión del riesgo sea eficaz en el tratamiento de los eventos de riesgo identificados y el riesgo del proyecto. Esta toma la entrada de cada fase del proceso de gestión del riesgo y revisa el enfoque adoptado para cada fase, así como para el proceso en su conjunto. Esta actividad abarca todos los aspectos de la implementación del proceso de gestión de riesgos, incluyendo técnicas y herramientas, la intensidad de la aplicación, los roles y responsabilidades, la comunicación y los requisitos de presentación de informes, etc. También cubre la integración del proceso de gestión de riesgos con otros procesos de gestión de proyectos y del negocio.

  Esta actividad es responsabilidad del gerente del proyecto, quien debe garantizar que la aplicación del proceso de gestión de riesgos al proyecto sea eficaz en todo momento, en términos de eventos de riesgos individuales identificados y a nivel del riesgo global del proyecto. La eficacia se define en términos del uso de los recursos, en la medida en que el proceso es proactivo en lugar de reactivo, en la oportunidad de las respuestas y así sucesivamente.

  La actividad de Gestionar el proceso puede llevarse a cabo a través de revisiones formales y regulares del proceso de gestión del riesgo o puede llevarse a cabo de manera informal durante todo el proyecto.

El proceso de gestión de riesgos de la guía PRAM, sugiere como mínimo una estructura iterativa en tres ciclos para gestionar los riesgos a nivel estratégico a través de las fases y sub-fases que lo componen, el detalle de esta estructura iterativa se muestra de manera resumida en la tabla número

6. La aplicación de estos ciclos se puede dar en periodo semanal, quincenal o mensual, de acuerdo con la naturaleza de los proyectos.

Fase/Sub-fase	Primer ciclo	Segundo ciclo	Tercer ciclo
Iniciar – Definir el Proyecto	Consolidar la información relevante sobre el proyecto en una forma adecuada.	Ajustar los supuestos básicos que enmarcan la definición del proyecto, con base en hallazgos encontrados en la primera iteración.	Puede conllevar una amplia y fundamental revisión de la segunda Fase Evaluar-Evaluación y de paso revelar problemas que no han sido resueltos en la planificación de respuesta durante la segunda iteración.
Iniciar – Enfoque del Proceso de Gestión de Riesgos	Elaborar planes estratégicos y planes tácticos detallados para el proceso de gestión de riesgos del proyecto, puede ejecutarse en paralelo con la definición del proyecto.	Ajustar el plan de gestión de riesgos a causa de los hallazgos encontrados de la primera iteración. El primer ciclo puede ser en gran medida sobre la cuantificación de la incertidumbre, es decir, ver sí importa, y si es de interés, donde es más relevante; en el segundo paso puede ser una cuidadosa planificación de la respuesta, es decir, las pruebas y la elección de las estrategias de respuesta, en aquellas áreas que son clave.	Puede implicar modificaciones extensas y fundamentales, si la segunda iteración ha revelado problemas importantes no resueltos. Por otro lado, podría haber modestos cambios en el proceso para la tercera iteración, como se había previsto anteriormente y sería todo lo que se necesita.

Identificar	Identificar eventos de riesgo y respuestas asociadas (tanto amenazas como oportunidades son relevantes).	Generar un conjunto de respuestas alternativas para los principales riesgos no contemplados por los cambios de supuesto en la sub-fase Iniciar- Definición del proyecto.	Buscar riesgos claves "secundarios" previamente pasados por alto o causados por la aplicación de respuestas asociadas a eventos de riesgo. Al igual que generar las respuestas necesarias.
Evaluar-Estructura	Definir la estructura con un nivel de robustez y de detalle razonable. Ej. Hay dos eventos de riesgo estrechamente relacionados en términos de una misma respuesta, ¿tratarlos como un único riesgo sería satisfactorio? o ¿un evento de riesgo realmente implica dos conjuntos diferentes de posibles problemas, que implica que lo que más útil es tratarlos como dos eventos de riesgo por separado?	Continuar con la prueba sólida de estructuración de las decisiones anteriores, pero con un conjunto más amplio de tareas; al igual, es una buena idea ordenar los riesgos por ej. Reflejando el orden en que éstos se produzcan y también es importante ordenar las respuestas en términos de preferencia.	Continuar con las pruebas en general y utilizar diagramas de riesgo y respuestas para ayudar a explicar los resultados del análisis de riesgo, cómo se ordenan las respuestas, respuestas secundarias, y de cómo se distinguen las respuestas específicas y generales. Estos diagramas son árboles de decisión en resumen, con las decisiones vinculadas a los eventos de riesgo y opciones de respuesta.
Evaluar-Propiedad	Establecer responsabilidad de lo que el cliente poseerá y gestionará y qué riesgos se espera que los contratistas posean y administren. Esto puede ser una cuestión de las políticas de la empresa para los proyectos.	Validar que la estructura de respuesta desarrollada se haya definido de acuerdo con los paquetes de trabajo, a fin de evitar problemas con un contratista en la gestión de las respuestas, debido a problemas y costos asociados con la gestión de riesgos a través de límites contractuales.	Asumiendo que es una iteración final, se debe mencionar las personas asignadas a la gestión de riesgos y asegurarse que las consecuencias financieras tienen propietarios definidos.

Evaluar-Estimación	Abordar cada uno de los eventos de riesgo identificados. Validar si el evento de riesgo se puede asociar con un proceso de cuantificación, o si es mejor manejarlo como un supuesto o condición bajo un enfoque cualitativo.	Utilizar un modelo probabilístico tradicional. Se puede tratar de reducir la incertidumbre a través de datos más apropiados o utilizando técnicas de estimación más sofisticadas.	Afinar distribuciones de probabilidad y hacer ajustes finales. Esta estimación se basa en las sub-fases anteriores para percibir lo más importante, tomar decisiones y predecir resultados asociados a valores esperados y a los riesgos de los proyectos.
Evaluar-Evaluación	Combinar la incertidumbre asociada a los eventos de riesgo individuales y decidir qué hacer con respecto a las consecuencias.	Se pueden utilizar diagramas para gestionar más iteraciones y tener una comprensión más profunda de la estructura causal de los eventos de riesgo y ayudar a tomar decisiones entre los supuestos de respuesta alternativas.	Mostrar el nivel acumulado de costo global definitivo (en tiempo, calidad). Proporcionar una base para obtener la aprobación para implementar el proyecto. Con la información acumulada se genera un diagnóstico de riesgo y las respuestas al problema, se generan los planes de base y planes de contingencia.
Planear respuesta a eventos de riesgos	Plantear "respuestas concretas" asociadas a los eventos de riesgos individuales, estas respuestas debe empezar a más tardar al final del primer ciclo a través de la sub-fase de Evaluar- Evaluación.	Se considera mejor integrar en gran medida con todas las sub-fases anteriores. Las condiciones de activación asociadas con el costo y el uso eficaz de ambas respuestas específicas y generales requieren una especial atención al	Integrar con todas las sub-fases anteriores de la tercera iteración, para garantizar la entrega de todo lo necesario para obtener la aprobación de los planes de base a nivel estratégico y los planes de contingencia asociados.

Planear respuesta a los riesgos del proyecto	Con base en el efecto del conjunto de respuestas específicas definir respuestas asociadas a la gestión colectiva del riesgo global. Es importante tener por lo menos una respuesta potente disponible.	impacto de los cambios en las pasadas las fases anteriores.	

Tabla 6. Estructura Iterativa en Tres Ciclos del Proceso de Gestión de Riesgos a Nivel Estratégico – Guía PRAM. Fuente: Adaptado de Guía de Análisis y Gestión de Riesgos de Proyectos 2a. Edición - (Association for Project Management, 2004).

Adicionalmente, en la práctica tendrán que llevarse a cabo iteraciones no planificadas; por lo tanto, se requiere un grado de gestión de riesgos reactiva, así como una gestión de riesgos proactiva.

La guía plantea una actividad complementaria denominada "Gestionar Proceso", por medio del cual integra todo el proceso de gestión de riesgos del proyecto, esto implica el seguimiento a los progresos, en sentido del control de la implementación del plan de contingencia, y en el sentido de control del ciclo para regresar a la sub-fase Iniciar - Definición del proyecto a nivel de los planes tácticos o estratégicos detallados, y ejecutando hacia adelante los planes detallados que se producen en la fase de Planear Respuestas. Asimismo, la guía PRAM define reservas de riesgo que generalmente se dividen en dos categorías:

- **Reservas del proyecto:** Reservas hechas por el proyecto para excepciones del proyecto.
- **Reservas para contingencias:** Reservas hechas específicamente para financiación de situaciones de contingencia de riesgo. El control de las reservas de riesgos debe realizarse a través del proceso de gestión del proyecto.

3.3.2.3. METODOLOGÍA DE GESTIÓN DE PROYECTOS – PRINCE2-

PRINCE 2 está orientada a proyectos en ambientes controlados, el cual "…*es un método estructurado para la gestión efectiva de proyectos, utilizado por el gobierno del Reino Unido, y ampliamente reconocido y utilizado por el sector privado. Este método es del dominio público, ofreciendo una guía de buenas prácticas en la gestión de proyectos*"[6].

Las características clave de PRINCE 2 son:

- Enfoque en una justificación de negocio.
- Una estructura de organización definida para el equipo de gestión del Proyecto.
- Una planificación basada en productos.
- Su énfasis en dividir el proyecto en fases manejables y controlables.

[6] Oficina de Comercio Gubernamental del Reino Unido, 2009.

- Su flexibilidad para ser aplicado al nivel apropiado del proyecto.

El estándar PRINCE 2 plantea ocho procesos para la gestión de los proyectos, los cuales se registran en la tabla número 7.

SIGLA	NOMBRE DEL PROCESO
SU	Proceso Preliminar (Starting Up a Project)
IP	Inicio de Proyecto (Initiating a Project)
DP	Dirección del Proyecto (Directing a Project)
CS	Control de Fase (Controlling a Stage)
MP	Gestión de Entrega de Productos (Managing Product Delivery)
B	Gestión de Límite de Fases (Managing Stage Boundaries)
CP	Cierre del Proyecto (Closing a Project)
PL	Planificación (Planning)

Tabla 7. Procesos para la Gestión de Proyectos - PRINCE 2.

Fuente: Tomado de Metodología de Gestión de Proyectos de PRINCE 2 - (Oficina de Comercio Gubernamental del Reino Unido, 2009).

Dentro de los procesos descritos en la tabla anterior, PRINCE 2 aplica una serie de componentes, detallados a continuación: Organización, Planes, Controles, Fases, Gestión del Riesgo, Calidad en el entorno del proyecto, Gestión de la Configuración y Control de Cambios. De estos componentes solo se hará la descripción de la Gestión del Riesgo.

PRINCE 2 plantea el riesgo como "…la posibilidad de exposición a consecuencias adversas de acontecimientos futuros, en donde todos los proyectos son susceptibles de sufrir cambios. Además, en ocasiones, los proyectos pueden ser largos y complejos, y deben tratar factores nuevos o poco habituales. Por este motivo, el riesgo es el factor más importante que debe ser tenido en cuenta durante la gestión de un proyecto". (Oficina de Comercio Gubernamental del Reino Unido, 2009).

La gestión de riesgos planteada por PRINCE 2 en la "metodología de gestión de proyectos" se divide en dos procesos: (a) Análisis de Riesgos y (b) Tratamiento de riesgos; a su vez, establece para cada uno de estos procesos un bloque de actividades, las cuales se detallan en la tabla número 8.

Proceso	Descripción y Actividades
Análisis del Riesgo	El Análisis del Riesgo es esencial para una Gestión del Riesgo efectiva. Necesita información de la Dirección de la Organización y ésta, a su vez, debe estar permanentemente informada por el Análisis. La comunicación es particularmente importante entre los niveles de Proyecto. El análisis comprende tres actividades:
	Identificación del Riesgo: Determina los riesgos potenciales a los que puede enfrentarse el proyecto.
	Estimación del Riesgo: Establece la importancia de cada riesgo, basándose en la valoración de su probabilidad y sus consecuencias para el proyecto y para el negocio.
	Evaluación del Riesgo: Decide si el nivel de riesgo es aceptable, y si no lo es, qué acciones deben llevarse a cabo para que lo sea. Hay cinco tipos de acciones sobre riesgos: prevención, reducción, transferencia, contingencia y aceptación
	Los resultados del Análisis deben quedar documentados en el Registro de Riesgos del proyecto, también debe es importante tener en cuenta que las actividades del Análisis del Riesgo se superponen y pueden ser iterativas, y que es un proceso que será llevado a cabo a lo largo de todo el proyecto, cuando se produzcan cambios o se tenga nueva información.
Tratamiento del Riesgo	El tratamiento del riesgo consta de cuatro actividades principales:
	Planificación: Para las acciones de contramedida realizadas durante la evaluación del riesgo, se realiza las siguientes actividades:

	• Identificar la cantidad y tipo de recursos que se necesita para realizar las acciones.
	• Desarrollar un plan de acción detallado, que se incluya en el Plan de Fase.
	• Confirmar la necesidad de continuar llevando a cabo las acciones identificadas en la evaluación del riesgo, a la luz de la información adicional conseguida.
	Asignación de Recursos: Consiste en la identificación y asignación de recursos necesarios para evitar el riesgo o disminuir su impacto.
	Monitorización: Esta actividad consiste en:
	• Comprobar si la ejecución de las acciones planificadas tiene el efecto deseado sobre el riesgo.
	• Vigilar para detectar pronto los riesgos que se puedan estar desarrollando.
	• Predecir riesgos potenciales.
	• Comprobar que la gestión de riesgos se está realizando de manera satisfactoria.
	• Informar de la situación del riesgo.
	Control: Consiste en asegurar que los eventos planificados ocurren realmente.

Tabla 8. Procesos para la Gestión de Riesgos en Proyectos - PRINCE 2.

Fuente: Metodología de Gestión de Proyectos de PRINCE 2 - (Oficina de Comercio Gubernamental del Reino Unido, 2009).

3.3.2.4. NORMA TÉCNICA COLOMBIANA NTC-ISO 31000.

La NTC-ISO 31000 es una norma publicada por el Instituto Colombiano de Normas Técnicas y Certificación (ICONTEC), esta norma suministra un enfoque genérico con una serie de principios y directrices para el proceso de gestión del riesgo, que pueden ser aplicados a toda la organización dentro de sus áreas, en cualquier nivel, a cualquier momento, así como en funciones, en los proyectos o en actividades específicas.

La norma NTC-ISO 31000 establece un proceso de gestión de riesgos con tres componentes relacionados entre sí, y nombrados de la siguiente manera:

- Principios.
- Marco de Referencia.
- Procesos.

En la figura número 13 se muestra a nivel gráfico los tres componentes definidos por la norma y se describen las relaciones que tienen entre sí. En esta norma se utilizan dos expresiones puntuales, una de "gestión del riesgo" que hace referencia a la estructura (principios, marco de referencia y proceso) para la gestión eficaz del riesgo, y la otra de "gestionar el riesgo" que se refiere a la aplicación de esa estructura a los riesgos particulares.

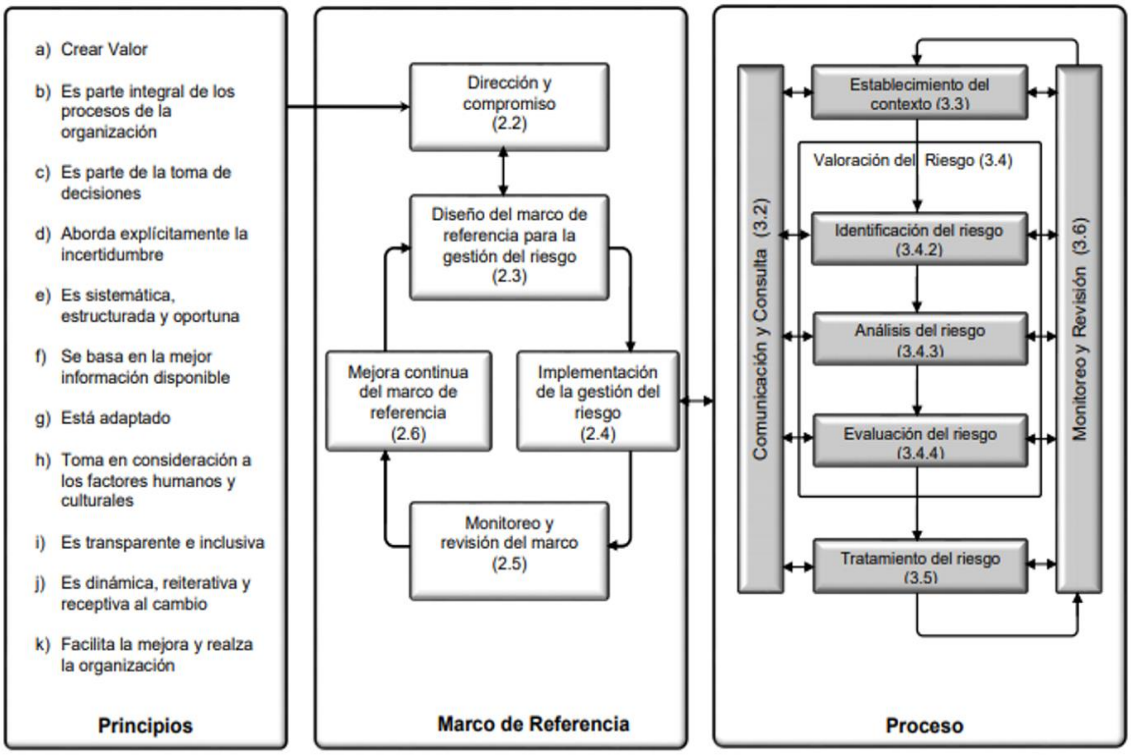


Figura 13. Relaciones entre los Principios, Marco de Referencia y Procesos para la Gestión del Riesgo – NTC-ISO 31000.
Fuente: Tomado de Norma Técnica Colombiana NTC-ISO 31000 - (ICONTEC, 2012).

A continuación, se describen a través de la tabla número 9 los principios señalados en la figura anterior:

Principio	Descripción
La gestión del riesgo crea y protege valor.	Contribuye con el logro demostrable de los objetivos y con la mejora del desempeño de los procesos de la organización.
La gestión del riesgo es una parte integral de todos procesos de la organización.	Hace parte de las responsabilidades de la dirección y es parte integral de todos los procesos (planeación estratégica, los procesos de gestión de proyectos y de cambio).
La gestión del riesgo es parte de la toma de decisiones.	Ayuda a quienes toman decisiones a hacer elecciones informadas, priorizar acciones y distinguir alternativas.
La gestión del riesgo aborda explícitamente la incertidumbre.	Toma en consideración explícitamente la incertidumbre, su naturaleza y la forma que se puede tratar.
La gestión del riesgo es sistemática, estructurada y oportuna.	Por medio de un enfoque sistemático, estructurado y oportuno contribuye a la eficiencia y a los resultados consistentes, comparables y confiables.
La gestión del riesgo se basa en la mejor información disponible.	Se basa en fuentes de información como datos históricos, experiencia, retroalimentación de las partes involucradas, observación, previsiones y exámenes de expertos.
La gestión del riesgo está adaptada.	La gestión del riesgo se alinea del contexto externo e interno y del perfil de riesgo de la organización.
La gestión del riesgo toma en consideración los factores humanos y culturales.	Reconoce las capacidades, percepciones e intenciones de individuos externos e internos, los cuales pueden facilitar o dificultar el logro de los objetivos de la empresa.
La gestión del riesgo es transparente e inclusiva.	La correcta y oportuna intervención de los involucrados, en particular aquellos que toman decisiones en todos los niveles de la

	organización, garantiza que la gestión sea pertinente y actualizada.
La gestión del riesgo es dinámica, reiterativa y receptiva al cambio.	La gestión del riesgo siente y responde continuamente al cambio.
La gestión del riesgo facilita la mejora continua de la organización.	Las empresas deberían implementar estrategias para mejorar la madurez de la gestión de riesgos.

Tabla 9. Principios para el Proceso de Gestión de Riesgos.

Fuente: Adaptado de Norma Técnica Colombiana NTC-ISO 31000 - (ICONTEC, 2012).

El marco de referencia, es el segundo componente del proceso para la gestión del riesgo definido por la norma NTC-ISO 31000, el cual a su vez está compuesto por cinco elementos descritos en la tabla número 10, estos elementos son necesarios para tener una gestión eficaz de riesgos a través de la aplicación del proceso para la gestión del riesgo en los distintos niveles y contextos de la organización.

Elemento	Descripción
Dirección y compromiso	La introducción de la gestión del riesgo y el garantizar su eficacia continua, requiere de un compromiso fuerte y sostenido por parte de la dirección de la empresa. Dentro de las responsabilidades que tiene la dirección están:
	• Definir y aprobar política para la gestión del riesgo.
	• Garantizar que la cultura organizacional y la política para la gestión del riesgo estén alineadas.
	• Definir indicadores de desempeño de la gestión del riesgo.
	• Alinear los objetivos de la gestión del riesgo con los objetivos y estrategias de la organización.
	• Garantizar la conformidad legal y reglamentaria.

	• Asignar obligaciones y responsabilidades en los niveles de la empresa.
	• Garantizar la asignación de recursos necesarios para la gestión del riesgo.
	• Comunicar los beneficios de la gestión del riesgo a todos los involucrados.
	• Garantizar que el marco de referencia para gestionar riesgos sea adecuado.
Diseño del marco de referencia para la gestión del riesgo	Para el diseño del marco de referencia se plantea tener en cuenta 7 aspectos importantes:
	• **Entender la organización y su contexto:** Antes de hacer el diseño e implementar el marco de referencia es importante evaluar y conocer el contexto tanto externo como interno de la organización, ya que esto puede influenciar en el diseño de dicho marco.
	• **Establecer la política para la gestión del riesgo:** Se debe hacer la declaración de los objetivos de la organización para la gestión del riesgo y su compromiso con esta, la cual debe ser comunicada de manera adecuada.
	• **Rendición de cuentas:** La organización debe garantizar que exista responsabilidad, autoridad y competencia adecuada para gestionar el riesgo.
	• **Integración con los procesos de la organización:** La gestión del riesgo debe estar incluida en todas las prácticas y procesos de la organización, de manera que sea pertinente y eficiente.
	• **Recursos:** La organización debe asignar los recursos (personas, procesos, herramientas, entrenamiento etc.) adecuados para la gestión del riesgo

	• **Establecer mecanismos para la comunicación interna y presentación de informes:** La organización debe establecer estos mecanismos con el fin de ayudar y fomentar la rendición de cuentas y la pertenencia del riesgo interna.
	• **Establecer mecanismos para comunicación externa y presentación de informes:** La organización debe implementar un plan sobre la forma como se comunicará con las partes involucradas externas.
Implementar la gestión del riesgo	La implementación está orientada a dos direcciones:
	Implementar el marco de referencia para gestionar el riesgo: La organización debe tener en cuenta lo siguiente: (a) Definir el tiempo ya la estrategia adecuados para implementar el marco de referencia, (b) Aplicar el proceso y la política para la gestión de riesgos a los procesos de la empresa, (c) Cumplir con los requisitos legales y reglamentarios, (d) Garantizar la toma de decisiones, incluyendo el desarrollo y establecimiento de objetivos alineados con los resultados de los procesos de gestión del riesgo y (e) Comunicar y consultar a las partes involucradas para garantizar que el marco sigue siendo adecuado.
	Implementar el proceso para la gestión del riesgo: La gestión del riesgo se debe implementar a través de un plan de gestión de riesgos en todos los niveles y las funciones de la organización como parte de sus prácticas y procesos.

Monitorear y revisar el marco de referencia	Con el fin de garantizar que la gestión del riesgo sea eficaz y continua sustentando el desempeño de la organización, esta debe gestionar las actividades de: • Medir el desempeño de la gestión del riesgo frente a los indicadores, de manera periódica. • Medir periódicamente el progreso frente al plan para la gestión del riesgo y las desviaciones con respecto a este. • Revisar periódicamente si el marco de referencia, la política y el plan para la gestión del riesgo siguen siendo adecuados según el contexto de la organización. • Presentar informes sobre el riesgo, el progreso del plan para la gestión del riesgo y sobre que tanto se cumple con la política para la gestión del riesgo. • Revisar la eficacia del marco de referencia para la gestión del riesgo.
Mejora continua del marco de referencia	Con base en los resultados del monitoreo y las revisiones, se deben tomar decisiones sobre la forma en que se podría mejorar el marco de referencia, la política y el plan para la gestión del riesgo. Estas decisiones deberían originar mejoras en la gestión del riesgo de la organización y en su cultura de gestión del riesgo.

Tabla 10. Elementos del Marco de Referencia para la Gestión del Riesgo.

Fuente: Adaptado de Norma Técnica Colombiana NTC-ISO 31000 - (ICONTEC, 2012).

El tercer y último componente para la gestión del riesgo definido por la norma NTC-ISO 31000, son los "Procesos", la cual está conformado por cinco actividades denominadas:

- **Comunicación y consulta:** La comunicación y consulta con las partes involucradas externas e internas es una actividad que se debe aplicar en todas las etapas del proceso para la gestión del riesgo, por lo tanto se sugiere que se genere tempranamente un plan de comunicación y la consulta. Es importante tener en cuenta que los puntos de vista de las partes involucradas pueden tener un impacto significativo en las decisiones que se tomen, de modo que las percepciones de los involucrados se deben identificar, registrar y tomar en consideración en el proceso de toma de decisiones; al igual, se debe facilitar los intercambios de información del proceso. (ICONTEC, 2012, p. 32-34).
- **Establecimiento del contexto:** Al establecer el contexto, la organización articula sus objetivos, define los parámetros externos e internos que se van considerar al gestionar el riesgo y establece el alcance y los criterios del riesgo para todo el proceso, esos parámetros pueden ser similares a los considerados en el diseño del marco de referencia, de modo que a este nivel es necesario considerarlos a mayor detalle. Esta etapa tiene cuatro actividades muy importantes:
    - **Establecer el contexto externo:** Es el ambiente externo en el cual la organización busca alcanzar sus objetivos, de modo que al definir los criterios del riesgo se toman en consideración las expectativas de las partes involucradas externas. El contexto externo puede incluir: el ambiente social y cultural, político, legal, económico, natural y competitivo.
    - **Establecer el contexto interno:** Es el ambiente interno en el cual la organización busca alcanzar sus objetivos. El proceso para la gestión del riesgo debe estar alineado con la cultura, los procesos, la estructura y la estrategia de la empresa.
    - **Establecer el contexto del proceso para la gestión del riesgo:** El contexto del proceso puede variar de acuerdo con las necesidades de la organización, pero es importante tener en cuenta los siguientes aspectos:

- ✓ Definir metas y objetivos de las actividades de gestión del riesgo.
- ✓ Definir responsabilidades para la gestión del riesgo.
- ✓ Definir el alcance y extensión de las actividades, incluyendo exclusiones e inclusiones específicas.
- ✓ Definir las relaciones entre el proyecto, proceso y actividad con otros procesos.
- ✓ Definir metodologías para valoración de riesgos.
- ✓ Definir la forma de evaluar el desempeño y eficacia del proceso.
- ✓ Identificar y especificar decisiones que se deben tomar.

- **Definir los criterios del riesgo:** Se deben definir los criterios que se van a utilizar para evaluar la importancia del riesgo, estos deben reflejar los valores, objetivos y recursos de la empresa, además deben ser consistentes con la política definida. Los criterios deben definirse al principio y revisarse continuamente. Al definir los criterios se deben tener en cuenta los siguientes factores:
  - ✓ Naturaleza, tipos de causa, consecuencias que se pueden presentar y la forma como se van a medir.
  - ✓ Como se va a definir la probabilidad.
  - ✓ Marcos temporales de probabilidad y las consecuencias.
  - ✓ Como se va a determinar el nivel del riesgo.
  - ✓ Puntos de vista de los involucrados.
  - ✓ El nivel en el cual se torna aceptable o tolerable.
  - ✓ Validar si se deben tener en cuenta las combinaciones de riesgo y cuáles combinaciones deberían considerarse. (ICONTEC, 2012, P.34-37).

- **Valoración del riesgo:** La valoración del riesgo es el proceso integral de la Identificación, Análisis y Evaluación del riesgo.

- **Identificación del riesgo:** La organización debe identificar las fuentes de riesgo, las áreas de impacto, los eventos, las causas y consecuencias potenciales; el objeto de esta fase es identificar una lista exhaustiva de riesgos con base en aquellos eventos que puedan afectar el logro de los objetivos; esto se puede realizar mediante el uso de herramientas técnicas de identificación e riesgos que sean adecuadas con sus capacidades, para ello es importante disponer de información actualizada e involucrar al personal con el conocimiento apropiado.
- **Análisis del riesgo:** Implica el desarrollo y la comprensión del riesgo, esté análisis implica una entrada para la evaluación del riesgo y para las decisiones de tratamiento del riesgo, al igual que para las estrategias y métodos adecuados para su tratamiento. El análisis involucra la consideración de las causas, las fuentes de riesgo, sus consecuencias positivas y negativas, y la probabilidad de que tales consecuencias puedan ocurrir; también se deben considerar los controles existentes, su eficacia y eficiencia. Se combinan las consecuencias y la probabilidad para determinar el nivel del riesgo con lo cual se determina el tipo de riesgo. El análisis puede ser cualitativo, semi-cuantitativo o cuantitativo, o una combinación de ellos, dependiendo de las circunstancias.
- **Evaluación del riesgo:** El propósito de la evaluación del riesgo es facilitar la toma de decisiones, basada en los resultados obtenidos en el análisis, acerca de cuáles riesgos necesitan tratamiento y la prioridad para la implementación del tratamiento. La evaluación del riesgo implica la comparación del nivel del riesgo obtenido en el análisis y de los criterios del riesgo establecidos al considerar el contexto, con base en esta comparación se puede considerar la necesidad de tratamiento. En las decisiones se debe incluir la tolerancia al riesgo. (ICONTEC, 2012, p. 37-39).

- **Tratamiento del riesgo:** El tratamiento del riesgo involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales opciones. Una vez implementado, el tratamiento suministra controles o los modifica. El tratamiento del riesgo implica un proceso cíclico que incluye:
    - ✓ Valoración del tratamiento del riesgo.
    - ✓ Decisión sobre si los niveles de riesgo residual son tolerables.
    - ✓ Si los niveles no son tolerables, generar un nuevo tratamiento para el riesgo.
    - ✓ Valoración de la eficacia de dicho tratamiento.

  Las opciones de tratamiento del riesgo no son necesariamente mutuamente excluyentes, ni adecuadas en todas las circunstancias, las opciones pueden ser:
    - ✓ Evitar el riesgo al decidir no iniciar o continuar la actividad que lo originó.
    - ✓ Tomar o incrementar el riesgo para perseguir una oportunidad.
    - ✓ Retirar la fuente del riesgo.
    - ✓ Cambiar la probabilidad.
    - ✓ Cambiar las consecuencias.
    - ✓ Compartir el riesgo con una o varias partes.
    - ✓ Retener el riesgo mediante una decisión informada.

  - **Selección de las opciones para el tratamiento del riesgo**: Implica equilibrar los costos y los esfuerzos de la implementación frente a los beneficios legales y financieros, al igual considerar aquellos riesgos que no ameritan porque no son justificables en términos económicos; las opciones de tratamiento pueden ser individuales o combinadas, al igual se debe identificar en el plan de tratamiento el orden de prioridad en el cual se deben implementar los tratamientos para los riesgos, estos tratamientos pueden generar otros riesgos secundarios que es necesario valorar, tratar,

monitorear y revisar, estos riesgos deben ser incluidos en el mismo plan de tratamiento definido para el riesgo original.

- **Preparación e implementación de los planes de tratamiento:** Su propósito está orientado a documentar la forma en que se van a implementar las opciones de tratamiento seleccionadas. Los planes de tratamiento deben estar integrados con los procesos de gestión de la organización. (ICONTEC, 2012, p. 39-41).

- **Monitoreo y revisión**: Las responsabilidades del monitoreo y revisión deben estar claramente definidas, por lo tanto debe hacer parte de la planificación del proceso para le gestión del riesgo, puede ser ejecutada de manera periódica o según convenga. El monitoreo está orientado a: garantizar que los controles sean eficientes tanto en el diseño como en la operación, obtener información adicional para la valoración del riesgo, analizar y aprender lecciones a partir de los eventos, detectar cambios en el contexto interno o externo e identificar riesgos emergentes. Los resultados pueden ser incorporados en las actividades globales de gestión del desempeño, medición y reporte interno y externo de la organización. (ICONTEC, 2012, P. 41-42). El monitoreo y revisión hacen parte integral de la gestión y deben estar incluidos en la cultura y las prácticas, así como también deben estar adaptados a los procesos de la organización.

Como última actividad la norma NTC-ISO 31000 sugiere el uso de un "Registro del proceso para la gestión del riesgo", debido a que las actividades de gestión deben tener una trazabilidad, y a su vez brindan una base para la mejora de los métodos y herramientas, así como el proceso global.

3.3.2.5. NORMA TÉCNICA COLOMBIANA NTC-ISO 27001.

La norma ISO 27001 es una solución de mejora continua, con la cual puede desarrollarse un Sistema de Gestión de Seguridad de la Información (SGSI) que permita evaluar todo tipo de riesgos o amenazas susceptibles de poner en peligro la información de una organización tanto propia como datos de terceros.

Por otro lado, también permite establecer los controles y estrategias más adecuadas para eliminar o minimizar dichos peligros. Esta norma está basada en el ciclo de mejora continua o modelo de Deming. Dicho ciclo consiste en cuatro procesos que son Planificar-Hacer-Verificar-Actuar, por lo que se le conoce también como ciclo PDCA (acrónimo de sus siglas en inglés Plan-Do-Check-Act).

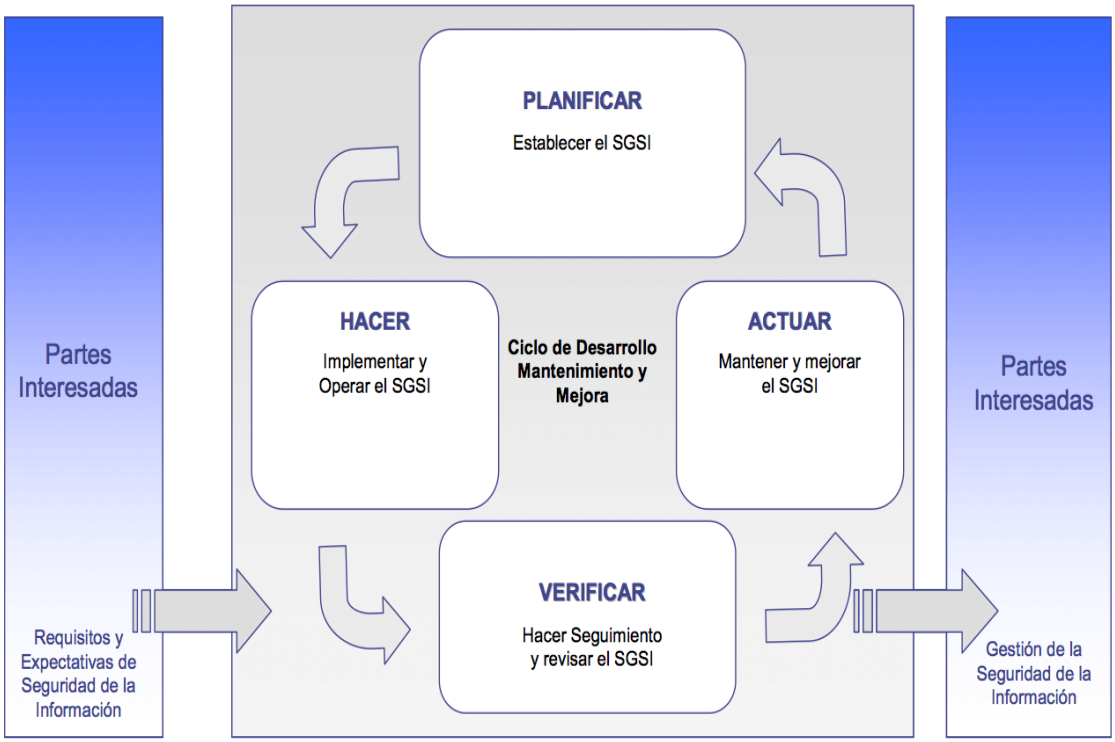


Figura 14. Modelo PHVA aplicado a los procesos de SGSI.
Fuente: Adaptado de Norma Técnica Colombiana NTC-ISO 27001 - (ICONTEC, 2006).

Trasladado a las necesidades de un SGSI, el ciclo PDCA planteado por la ISO 27001 se dividiría en los siguientes pasos, cada uno de ellos ligado a una serie de acciones:

Proceso	Actividades
	Definir la política de seguridad
	Establecer al alcance del SGSI

Planificar (establecer el SGSI)	Realizar el análisis de riesgo
	Seleccionar los controles
	Definir competencias
	Establecer un mapa de procesos
	Definir autoridades y responsabilidades
Hacer (implementar y operar el SGSI)	Implantar el plan de gestión de riesgos
	Implantar el SGSI
	Implantar los controles
Controlar (hacer seguimiento y revisar el SGSI)	Revisar internamente el SGSI
	Realizar auditorías internas del SGSI
	Poner en marcha indicadores y métricas
	Hacer una revisión por parte de la Dirección
Actuar (mantener y mejorar el SGSI)	Adoptar acciones correctivas
	Adoptar acciones de mejora

Tabla 11. Relación entre procesos y actividades ciclo PDCA ISO 27001.

Fuente: Adaptado de Norma Técnica Colombiana NTC-ISO 27001 - (ICONTEC, 2006).

3.3.2.6. BIBLIOTECA DE INFRAESTRUCTURA DE TECNOLOGÍAS DE INFORMACIÓN –ITIL V3-.

ITIL, nació en la década de 1980, a través de la Agencia Central de Telecomunicaciones y Computación del Gobierno Británico (Central Computer and Telecomunications Agency - CCTA), que ideó y desarrollo una guía para que las oficinas del sector público británico fueran más eficientes en su trabajo y por tanto se redujeran los costes derivados de los recursos TI. Sin embargo esta guía demostró ser útil para cualquier organización, pudiendo adaptarse según sus circunstancias y necesidades.

De hecho resultó ser tan útil que actualmente ITIL recoge la gestión de los servicios TI como uno de sus apartados, habiéndose ampliado el conjunto de "buenas prácticas" a gestión de la seguridad de la información, gestión de niveles de servicio, perspectiva de negocio, gestión de activos software y gestión de aplicaciones. Estas buenas prácticas provienen de las mejores soluciones posibles que diversos expertos han puesto en marcha en sus organizaciones a la hora de entregar de servicios TI, por lo que en ocasiones el modelo puede carecer de coherencia.

En la actualidad ITIL pertenece al Oficina de Comercio Británico (Office of Government Commerce - OGC), pero puede ser utilizado para su aplicación libremente. ITIL no comenzó a ser utilizada de manera común hasta aproximadamente 1990; desde esa fecha el crecimiento de la librería se situó en aproximadamente 30 publicaciones que hacían de su utilización un proceso complejo. Se hizo necesaria por tanto una revisión que agrupase los libros según conjuntos estructurados en los procesos que estuvieran más íntimamente relacionados, enmarcando la gran cantidad de publicaciones existente en ocho volúmenes, denominándose desde entonces como ITIL v2.

La última versión vio la luz en 2007, denominada como ITIL v3. En esta versión se ha realizado un refresco (refreshment en palabras de la OGC), agrupando los elementos principales de ITIL en 5 volúmenes, que pueden encontrarse en la actualidad con los siguientes títulos:

- Estrategia de servicios.
- Diseño de servicios.
- Transición de servicios.
- Operación de servicios.
- Mejora continua de servicios.

Estos 5 libros conforman "el ciclo de vida ITIL" (ITIL Lifecycle).

ITIL no posee ningún proceso específico de Gestión del Riesgo, de los procesos que abarca los diferentes volúmenes de ITIL el proceso donde se realiza una gestión de riesgos es en Gestión de la Continuidad, proceso que se hace parte del volumen Diseño del Servicio.

El objetivo de la Gestión de la Continuidad (IT Service Continuity Management ITSCM) es garantizar que la infraestructura y los servicios más importantes de la Organización puedan superar la ocurrencia de un desastre en el menor tiempo posible, restaurando la normalidad.

Un desastre puede ser natural (terremotos, inundaciones, tormentas, etc.), provocado por el ser humano (incendios, inundaciones, etc.) o informáticos (virus, ataques globales, hackers, etc.). El proceso de Gestión de la Continuidad se despliega sobre dos formas de actuar:

- **La preventiva:** se trata de procedimientos que tratan de impedir la ocurrencia de desastres (normalmente informáticos o humanos).
- **La activa:** es la que pone en marcha el servicio tras la ocurrencia de un desastre.

Para disponer de este tipo de actuaciones, previamente la Organización debe poner en marcha un proceso de Gestión de la Continuidad que contemple al menos las siguientes actividades:

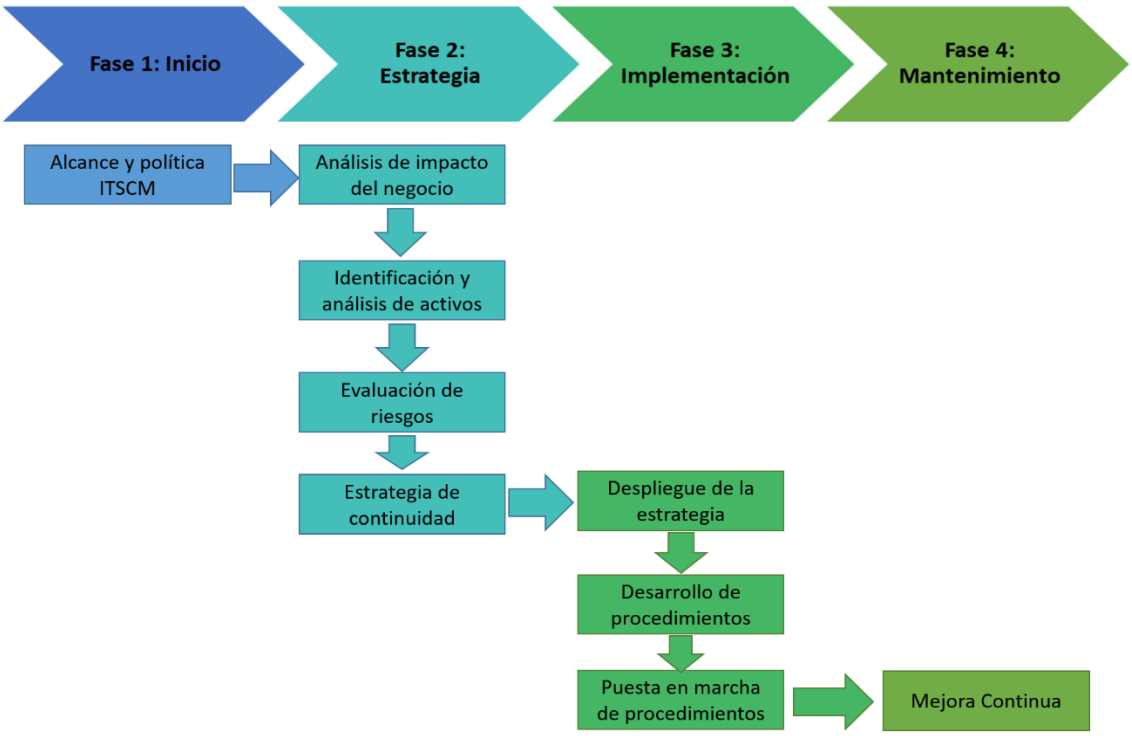


Figura 15. Proceso de Gestión de la Continuidad y despliegue de actividades.

- **Evaluación de riesgos:** El objetivo de la Evaluación de Riesgos es determinar a qué tipo de riesgos están expuestos los servicios. Para detectarlos es necesario conocer muy profundamente el Servicio, para lo que la información de entrada de la identificación previa de activos es muy importante.

  Así mismo, un análisis de estos activos, conociendo sus amenazas y vulnerabilidades posibles (y potenciales) dará fuerza a esta evaluación para comenzar a plantear medidas que aseguren la Continuidad del Servicio. Estas medidas pueden ser de prevención y de recuperación, y serán adoptadas según la posibilidad que se estime tienen de ocurrir desastres o la potencialidad de riesgos, unida a su coste en esfuerzo y económico.

- **Estrategia de continuidad:** A partir de la evaluación de riesgos se han de establecer las Estrategias de Prevención o de Recuperación. La suma de ambas será la Estrategia de Continuidad de los Servicios de la Organización.

El equilibrio de ambas se dirime por cuestiones financieras. Los planes de prevención suelen ser más caros que los de recuperación, por lo que según la Evaluación de Riesgos y la Gestión Financiera la Organización se decantará por cómo Gestionar la Continuidad de sus Servicios.

- **Planes de Prevención:** Se relacionan con otros aspectos de gestión de la organización, como la Gestión de la Continuidad del Negocio y la Gestión de la Seguridad. En ambos casos las medidas que se toman son comunes con la Gestión de la Continuidad del Servicio. Las acciones a llevar a cabo para plantear un Plan de Prevención se derivan del refuerzo de los aspectos que impiden el acceso a la infraestructura.
- **Planes de Recuperación:** Dependiendo del nivel de importancia del Servicio (de cara al cliente) a recuperar y de su importancia económica para la Organización, se pueden establecer diferentes soluciones que tienen también un coste creciente, ya que requieren mantenimiento de infraestructuras de replicación continua, alojamientos en otros lugares, equipos de mantenimiento y otros servicios contratados.

3.3.2.7. OBJETIVOS DE CONTROL PARA INFORMACIÓN Y TECNOLOGÍAS RELACIONADAS –COBIT 5-.

El IT Governance Institute (ITGI) fue creado en 1998 por ISACA para avanzar en la definición de estándares para la dirección y control de la tecnología de información en las empresas, en donde para proveer un marco de trabajo que colabore en la búsqueda de niveles adecuados de seguridad, definió COBIT (Control Objectives for Information and related Technology), en donde define unos objetivos de control asociados con la información y la tecnología relacionada.

COBIT considera fundamental el tratamiento de los riesgos asociados a los activos de información electrónica, alineada con su misión, que consiste en investigar, desarrollar, publicar y promover un conjunto internacional y actualizado de objetivos de control para tecnología de información que sea de uso cotidiano para gerentes, auditores y usuarios.

COBIT 5 proporciona un marco global que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI, o sea que ayuda a las empresas a crear valor óptimo de la misma por mantener un equilibrio entre la obtención de beneficios, la optimización de los niveles de riesgo y el uso de los recursos; adicionalmente permite el desarrollo de las políticas y buenas prácticas para el control de las tecnologías.

COBIT 5 ha integrado COBIT 4.1, Val IT 2.0[7] y Risk IT[8] contenido en un modelo de referencia de proceso, en donde reúne cinco principios que permiten a las empresas a construir un gobierno efectivo y un marco de gestión basado en siete facilitadores que optimizan la información y la inversión en tecnología y el uso para el beneficio de las partes interesadas.

Figura 16. Principios de COBIT. Fuente: Basado en Isaca, COBIT 5

[7] Val IT es un marco de referencia de gobierno que incluye principios rectores generalmente aceptados y procesos de soporte relativos a la evaluación y selección de inversiones de negocios de TI

[8] Risk IT es un marco de referencia normativo basado en un conjunto de principios rectores para una gestión efectiva de riesgos de TI.

Los principios que maneja COBIT 5 son:

1. **Entregar las necesidades a los interesados ("Meeting Stakeholder Needs"):** El sistema de gobierno debe considerar todas las partes interesadas en la toma de decisiones de beneficios, recursos y evaluación de riesgos.

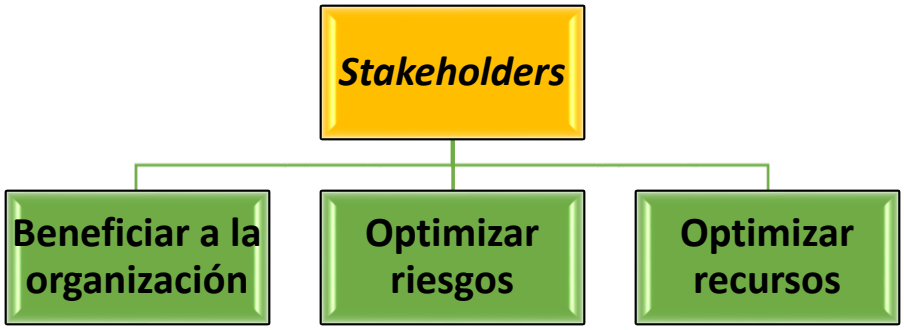


Figura 17. Necesidades de los Stakeholders.

Fuente: Basado en Isaca, COBIT 5

2. **Cubrir la Empresa de extremo a extremo ("Covering the Enterprise End-to-End"):** Se refiere al gobierno y la gestión de las TI relacionada a un nivel corporativo, de extremo a extremo.
3. **Aplicar un marco único integrado ("Applying a Single Integrated Framework):** COBIT 5 se alinea con las normas y marcos utilizados por las empresas: COSO, COSO ERM, ISO / IEC 9000, ISO / IEC 31000, ISO / IEC 38500, ITIL, ISO / IEC 27000 serie, TOGAF, PMBOK/PRINCE2, CMMI.
4. **Habilitar un enfoque holístico ("Enabling a Holistic Approach"):** COBIT 5 maneja la definición de facilitadores que son los factores que, individual y colectivamente, influyen en el gobierno y la gestión en la empresa de TI.

Figura 18. Facilitadores COBIT 5.

Fuente: Basado en Isaca, Cobit5

Estos facilitadores son:

- Principios, políticas y marcos que son las formas para traducir el comportamiento deseado en una guía práctica para la gestión del día a día.
- Procesos que es un conjunto organizado de prácticas y actividades para lograr ciertos objetivos y producir un conjunto de salidas en apoyo del logro de TI.
- Estructura de la organización que es la clave de la toma de decisiones en las entidades de una organización.
- Cultura, ética y conducta de los individuos y de la organización, muy a menudo subestimado como factor de éxito en las actividades de gobierno y gestión.

- La información que es necesaria para mantener la organización funcionando, pero en el plano operativo, la información es muy a menudo la clave del producto de la propia empresa.
- Servicios, infraestructura y aplicaciones, con la infraestructura, tecnología y aplicaciones que proporcionan a la empresa con el procesamiento de tecnología de la información y los servicios.
- Personas, habilidades y competencias, están relacionadas con las personas y son necesarios para completar con éxito todas las actividades y de tomar decisiones correctas y tomar las acciones correctivas.

5. **Separar el gobierno de la gestión ("Separating Governance from Management"):** El marco de COBIT 5 hace una clara distinción entre el gobierno y la gestión. En donde el gobierno es la responsabilidad del consejo de administración bajo el liderazgo del presidente, mientras que la gestión es responsabilidad de la dirección ejecutiva. Adicionalmente el gobierno contiene cinco procesos que son:

- Asegurar el establecimiento y mantenimiento del marco de gobierno de TI.
- Asegurar la entrega de beneficios.
- Asegurar la optimización de riesgos.
- Asegurar la optimización de recursos.
- Asegurar la transparencia de las partes interesadas.

Éstos procesos se debe evaluar, dirigir y supervisar (EDM). En cambio la gestión se basa en las áreas de planificar, construir, ejecutar y supervisar (PBRM).

COBIT 5 posee dos procesos para la gestión de riesgos, los cuales son:

- **EDM03 Asegurar la Optimización del Riesgo:** Se encarga de asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las T.I es identificado y gestionado. Este proceso posee 3 prácticas claves que son:

- **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; considera 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.
- **Orientar la gestión de riesgos:** Orientar el establecimiento de prácticas de gestión de riesgos para proporcionar una seguridad razonable de que riesgo TI actual no excede el apetito de riesgo del Consejo.
- **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.

- **APO12 Gestionar el Riesgo:** Proceso donde se identifica, evalúa y se reduce los riesgos relacionados con T.I de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa. Este proceso posee 6 prácticas claves que son:
  - **Recolectar Datos:** Identificar y recopilar datos relevantes para catalizar una identificación, análisis y notificación efectiva de riesgos relacionados con TI.
  - **Analizar 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.
  - **Mantener un perfil del 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.
  - **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.

- **Definir un portafolio de acciones para la gestión de riesgo:** Gestionar las oportunidades para reducir el riesgo a un nivel aceptable a través de un inventario de actividades de control.
- **Responder el riesgo:** Responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI.

3.3.2.8. GUÍA DE LOS FUNDAMENTOS PARA LA DIRECCIÓN DE PROYECTOS - GUÍA DEL PMBOK®-

La guía del PMBOK® es un documento desarrollado por el PMI, en donde se establece un criterio de buenas prácticas relacionadas con la gestión, la administración y la dirección de proyectos mediante la implementación de técnicas y herramientas que permiten identificar un conjunto de 49 procesos, distribuidos a su turno en 10 áreas de conocimiento; dichas áreas de conocimiento se muestran en la figura número 19, en donde a su vez se encuentra la "Gestión de Riesgos", la cual se va profundizó en el presente numeral.

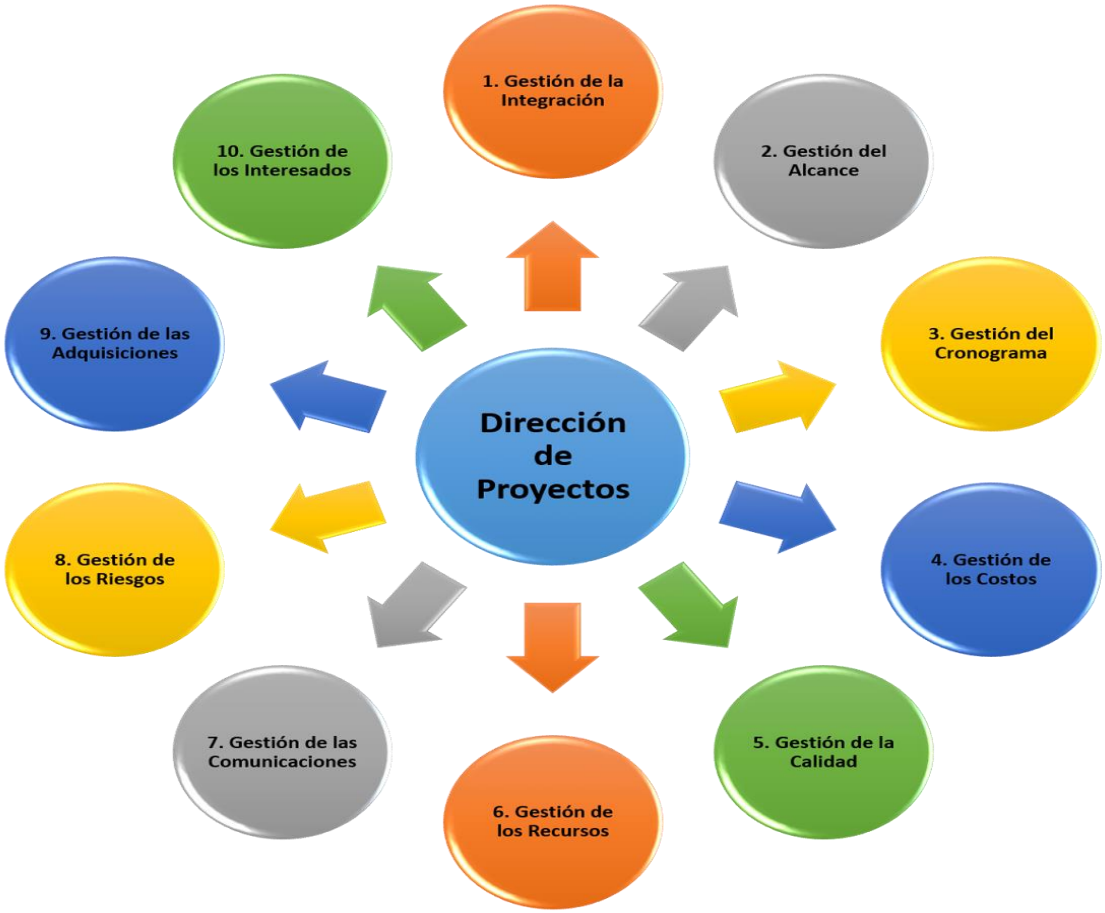


Figura 19. Áreas de conocimiento para la dirección de proyectos PMI.

Fuente: Elaboración propia.

La Gestión de Riesgos del Proyecto incluye los procesos para llevar a cabo la planificación de la gestión, identificación, análisis, planificación de respuesta, implementación de respuesta y monitoreo de los riesgos de un proyecto. Tiene como objetivo "…aumentar la probabilidad y/o el impacto de los riesgos positivos y disminuir la probabilidad y/o el impacto de los riesgos negativos, a fin de optimizar las posibilidades de éxito del proyecto" (Project Management Institute, 2017, p. 431).

Los procesos de la gestión de los riesgos interactúan entre sí y también con los procesos de las otras áreas de conocimiento. Cada proceso se ejecuta por lo menos una vez en cada proyecto y en

una o todas las fases del ciclo de vida del proyecto, los procesos de la gestión de riesgos se describen en la siguiente tabla:

PROCESO	DESCRIPCIÓN
Planificar la Gestión de Riesgos	Se define la estrategia de cómo realizar las actividades para gestión del riesgo total del proyecto y a su vez integrar esta gestión con las otras actividades dentro del plan de gestión del proyecto y con los procesos de gestión del resto de la organización. Dentro de la planificación se debe generar un presupuesto en términos de recursos, costos y tiempo para las actividades de gestión de riesgo definidas; así mismo, el costo del tratamiento de los riesgos debe incluirse en el presupuesto del proyecto. Adicionalmente, en el plan de gestión de riesgos se debe registrar la siguiente información: ▪ Como se evalúa, se aprueba, se asigna y se administra el presupuesto de riesgos. ▪ Definir los métodos de supervisión para la ejecución de los gastos de riesgos. ▪ Especificación y nivel de detalle de los riesgos que se deben abordar

	▪ Proporcionar una plantilla del registro de riesgos. ▪ Indicar la intensidad del esfuerzo y la frecuencia con la que los diferentes procesos de gestión de riesgos del proyecto deben ser aplicados. ▪ Especificar los roles y responsabilidades en la gestión de riesgos de los miembros del equipo de proyecto. ▪ Definir las expectativas correspondientes tanto para los directivos, como para el personal del proyecto. ▪ Descripción de la frecuencia y el alcance de las reuniones de gestión de riesgos y la estructura, contenido de los informes necesarios. ▪ Definición de la estructura, el contenido y la frecuencia de los documentos de rutina a recibir, así como la manera en que la información se divulgará periódicamente o por acontecimientos excepcionales.
Identificar Riesgos	Tiene como objetivo identificar todos los riesgos evidentes que pueden afectar a los objetivos del proyecto, esto no quiere decir que todos los riesgos queden contemplados, es por ello que este proceso debe ser iterativo.

	Al evidenciar los riesgos también se pueden visualizar las respuestas al mismo tiempo y registrar las acciones en el proceso de identificar riesgos, en caso que las respuestas no sean implementadas de inmediato, deben ser consideradas durante el proceso "planificar la respuesta a los riesgos". Los resultados del proceso de identificar los riesgos deben reposar en un registro de riesgos, el cual incluye una descripción estructurada del riesgo, su propietario y puede también incluir información sobre las causas y efectos del riesgo, las condiciones de activación y las respuestas preliminares.
Realizar el Análisis Cualitativo de Riesgos	Consiste en clasificar y evaluar las características de los riesgos del proyecto identificados individualmente y a su vez priorizar los riesgos basados en las características acordadas, esto consiste en evaluar la probabilidad que cada riesgo ocurrirá y el impacto de cada riesgo individual sobre los objetivos del proyecto. Como tal, no se aborda directamente el riesgo global del proyecto, el cual es el resultado del efecto combinado de todos los riesgos y sus posibles interacciones con los demás.

	Un paso importante en el análisis consiste en clasificar los riesgos en función de sus fuentes o causas, una identificación de los efectos comunes de los grupos de riesgos permite evidenciar las áreas de mayor exposición de riesgo, lo que facilitaré el enfoque de respuestas. El análisis cualitativo de riesgos se aplica a la lista de los riesgos creados o actualizados en el proceso de identificar los riesgos. Los riesgos que se evalúan como de alta prioridad serán un foco importante en el proceso Planificar la Respuesta de Riesgos. Existen unos factores que son claves para determinar la importancia del riesgo: ▪ Urgencia/Proximidad. ▪ Capacidad de administración ▪ Impacto externo al proyecto. La recopilación de información de alta calidad es muy importante, en caso de no estar disponible se debe realizar entrevistas, taller y otros medios como juicio de expertos. Los datos recopilados de personas puede tener declaraciones con sesgo intencional, si esto ocurre se debe identificar y ajustar en lo posible. El análisis cualitativo es más exitoso si se realiza

	periódicamente durante todo el proyecto, la frecuencia de esta actividad será incluida en el plan de gestión de riesgos, pero también puede depender de eventos propios del proyecto. En conclusión el proceso de análisis cualitativo de riesgos incluye los siguientes pasos: ▪ Seleccionar características del riesgo que definen la importancia de los riesgos. ▪ Recopilar y analizar los datos. ▪ Priorizar los riesgos por la probabilidad y el impacto sobre los objetivos específicos. ▪ Priorizar los riesgos por probabilidad e Impacto sobre el Proyecto Global. ▪ Categorizar las causas de riesgos. ▪ Documentar los resultados del análisis cualitativo.
Realizar el Análisis Cuantitativo de Riesgos	Este proceso proporciona una estimación numérica de los efectos globales del riesgo sobre los objetivos del proyecto, basados en los planes actuales y la información, considerando los riesgos simultáneamente. Los resultados de este tipo de análisis pueden ser utilizados para evaluar la probabilidad de éxito en el logro de los objetivos del proyecto y estimar las reservas de contingencia, por lo general en tiempo

	y costo, para que sean apropiadas a los riesgos y la tolerancia al riesgo de los participantes del proyecto. Este análisis de incertidumbre en el proyecto utiliza técnicas cuantitativas, como la simulación de Monte Carlo, la cual proporciona un mayor realismo en la estimación del costo total del proyecto o programa, a diferencia de un método no probabilístico. Sin embargo, se debe reconocer que el análisis cuantitativo de riesgos no siempre es necesario o adecuado para todos los proyectos. El enfoque principal del análisis cuantitativo de riesgos es el cálculo de la estimación del riesgo global del proyecto, para ello se requiere contar con la siguiente información: ▪ Representación completa y precisa de los objetivos del proyecto construido a partir de elementos individuales del proyecto. ▪ Identificación de riesgos sobre elementos individuales del proyecto (actividades del cronograma o elementos de línea de costos). ▪ Inclusión de los riesgos genéricos que tienen un efecto más amplio que los elementos individuales del proyecto.

	▪ Aplicación de un método cuantitativo (por ejemplo, la simulación de Monte Carlo o el análisis del árbol de decisión) que incorpora simultáneamente múltiples riesgos para determinar el impacto global sobre el objetivo general del proyecto. Los pasos que debe contener un análisis cuantitativo de riesgos son: ▪ Priorización de riesgos (generado en el análisis cualitativo de riesgos). ▪ Examinar las interrelaciones entre los riesgos. ▪ Recopilar datos del riesgo de alta calidad. ▪ Disponer del modelo del proyecto (cronograma de proyecto, estimación de costos). ▪ Realizar análisis cuantitativo de riesgos (simulación Monte Carlo, arboles de decisión). Resultados del análisis (¿Qué tan probable es el éxito?, ¿Cuánta contingencia se necesita?, ¿Qué riesgos son de alta prioridad?). La reserva de contingencia del proyecto en tiempo y costo debe reflejarse en el cronograma y presupuesto del proyecto.

	El análisis cuantitativo de riesgos proporciona información que puede ser usada para modificar el plan de proyecto.
Planificar la Respuesta a los Riesgos	Este proceso determina las acciones de respuestas eficaces para que sean apropiadas con la prioridad de los riesgos individuales y el riesgo global del proyecto. Tiene en cuenta las actitudes de los grupos de interés de riesgo y los convenios especificados en el Plan de Gestión de Riesgos, además de las limitaciones y supuestos que se determinaron cuando los riesgos fueron identificados y analizados. La especificación de la respuesta para cada riesgo deber incluir una descripción de las condiciones de activación correspondiente. La responsabilidad de la supervisión de las condiciones del proyecto y ejecución de las acciones correspondientes deben estar claramente asignadas; cada riesgo debe tener asignado un propietario en el proceso de identificar los riesgos, y a cada una de las respuestas a los riesgos se le debe asignar un propietario de la acción del riesgo específico. El propietario del riesgo es responsable de asegurar que la respuesta al riesgo sea eficaz y de planificar

	respuestas de riesgos adicionales; mientras que el propietario de acción de riesgos es responsable de asegurar que las respuestas a los riesgos acordadas se llevan a cabo como fueron previstas y de manera oportuna. El papel del propietario del riesgo y del propietario de la acción de riesgo puede ser asignado a una misma persona. Puede haber riesgos residuales que permanecen después de que las respuestas han sido implementadas. Estos riesgos residuales deben estar claramente identificados, analizados, documentados y comunicados a todos los interesados; por otra parte, todas las acciones aprobadas que surgen de la planificación de la respuesta al riesgo deben integrarse en el plan de gestión del proyecto. Una serie de factores son importantes para el éxito del proceso planificar las respuestas a los riesgos: ▪ Comunicar a las distintas partes interesadas. ▪ Definir claramente roles y responsabilidades relacionadas con los riesgos. ▪ Especificar el momento de las respuestas a los riesgos (activación).

	▪ Proporcionar recursos, presupuesto y programación de respuestas. ▪ Dirección entre la interacción y respuestas de riesgos. ▪ Asegurar respuestas apropiadas, oportunas, eficaces y acordadas. ▪ Gestión de amenazas y oportunidades. ▪ Desarrollar estrategias tácticas ante las respuestas. Para los riesgos individuales se debe definir una estrategia de respuesta: ▪ Evitar una amenaza o explotar una oportunidad. ▪ Transferir una amenaza o compartir una oportunidad. ▪ Mitigar una amenaza o mejorar una oportunidad. ▪ Escalar una amenaza o una oportunidad. ▪ Aceptar una amenaza o una oportunidad. Los pasos del proceso “planificar las respuestas a los riesgos” son: ▪ Identificar respuestas. ▪ Seleccionar respuestas. ▪ Planificar la acción (con condición de activación). ▪ Definir a los propietarios y asignar las responsabilidades.

	▪ Actualizar el registro de riesgos. ▪ Revisar la exposición residual del riesgo (si la exposición no es aceptable ajustar respuesta). ▪ Actualizar el plan de gestión del proyecto (incluyen costos, asignación de recursos, detalles de la programación, y los cambios en la documentación del proyecto).
Implementar la Respuesta a los Riesgos	Uno de los escenario más frecuentes cuando se gestiona los riegos en un proyecto es dedicar mucho esfuerzo a los procesos que comprende la planificación, desde identificarlos hasta planificar la respuesta a los mismos pero lamentablemente no siempre se implementa la respuesta a los riesgos, por tal motivo este es un proceso muy importante ya que permite implementar los planes de respuesta a los riesgos, este proceso se lleva a cabo a lo largo de todo el proyecto.
Monitorear los Riesgos	Proceso mediante el cual se monitorea la implementación de los planes acordados de respuesta a los riesgos, para garantizar que el equipo del proyecto y los principales interesados estén conscientes del actual nivel de exposición al riesgo se debe realizar un monitoreo de forma continua al trabajo del proyecto para así identificar nuevos riesgos, riesgos cambiantes y obsoletos, si el enfoque de gestión de riesgo sigue siendo

	adecuado, si las reservas para contingencias de costos o cronograma requieren modificación y la estrategia del proyecto sigue siendo válida.

Tabla 12. Estándar de Práctica para la Gestión de Riesgos de Proyecto.

Fuente: Project Management Institute, 2017

3.3.2.9. METODOLOGÍAS ÁGILES – SCRUM-.

Las metodologías ágiles son sistemas de gestión de proyectos que ayudan a usar el tiempo de manera efectiva y creativa. Son muy útiles para visualizar y organizar las tareas a realizar y para mejorar el rendimiento y el trabajo en equipo, permiten tener un seguimiento detallado de cada etapa de un proyecto, tanto a nivel personal como grupal.

Entre las metodologías ágiles existentes se encuentra la metodología SCRUM, la cual surgió para administrar de manera dinámica proyectos de desarrollo de Software fue aplicado por primera vez por Ken Schwaber y Jeff Sutherland, quienes lo documentaron en detalle en el libro Agile Software Development with Scrum. Esta metodología centra su atención en las actividades de Gerencia y no especifica prácticas de Ingeniería. Fomenta el surgimiento de equipos autodirigidos cooperativos y aplica inspecciones frecuentes como mecanismo de control. SCRUM parte de la base de que los procesos definidos funcionan bien sólo si las entradas están perfectamente definidas y el ruido, ambigüedad o cambio es muy pequeño. Por lo tanto, resulta ideal para proyectos con requerimientos inestables, ya que fomenta el surgimiento de los mismos. El ciclo de vida definido por SCRUM es incremental iterativo y se caracteriza por ser muy adaptable.

Los proyectos se realizan durante una serie de iteraciones de un mes de duración llamadas Sprints. Al comienzo de cada Sprint tiene lugar una Sprint Planning Meeting durante la cual el Product Owner prioriza el Product Backlog y el Scrum Team selecciona las tareas que serán completadas durante el Sprint que va a comenzar. Esas tareas son removidas del Product Backlog para ser llevadas al Sprint Backlog.

Durante el Sprint el equipo se mantiene en contacto a través de las Daily Meetings. Y al final del Sprint debe mostrar la funcionalidad completa en la Sprint Review Meeting.

4. DESARROLLO DE LA INVESTIGACIÓN – CONSTRUCCIÓN MODELO DE GESTIÓN DE RIESGOS –

El presente capitulo se centra en el desarrollo de la investigación de acuerdo con el planteamiento realizado por el autor, esta se llevará a cabo en los pasos descritos en la figura número 20, en donde se tiene como objetivo proponer la construcción del modelo de control y gestión de riesgos para proyectos TI.

Figura 20. Pasos aplicados en el desarrollo de la investigación

Fuente: Elaboración propia.

4.1. ANÁLISIS COMPARATIVO DE LOS ENFOQUES METODOLÓGICOS DE GESTIÓN DE RIESGOS.

En la presente sección se realiza un análisis comparativo de las variables (marco de referencia, procesos, actividades y técnicas o métodos de apoyo) que componen los enfoques metodológicos de gestión de riesgos seleccionados y que servirán como base para proponer un nuevo modelo que sirva de apoyo para la gestión de riesgos de los proyectos TI ejecutados por la Alcaldía de Cartagena.

Los criterios aplicados para la selección de los enfoques se basaron en que éstos estuvieran orientados a gestión de riesgos en proyectos o pudieran ser aplicados de acuerdo con el tema de

estudio, y que a su vez se dispusieran de documentos de referencia detallados. De acuerdo con lo anterior los enfoques seleccionados son:

- COSO ERM.
- Association For Project Management –APM-
- Metodología De Gestión De Proyectos – Prince2-
- Norma Técnica Colombiana NTC-ISO 31000.
- Norma Técnica Colombiana NTC-ISO 27001.
- Biblioteca De Infraestructura De Tecnologías De Información –ITIL V3-
- Objetivos De Control Para Información Y Tecnologías Relacionadas –COBIT 5-
- Guía De Los Fundamentos Para La Dirección De Proyectos - Guía Del PMBOK®-

La descripción detallada de cada uno de los enfoques se encuentra registrada en el numeral 2.3.2 del Estado del arte, perteneciente al Marco Referencial del Capítulo 2 de este documento. El primer análisis comparativo se realiza a nivel de los procesos o fases planteados en cada enfoque metodológico para la gestión de riesgos seleccionados, los cuales se identifica que su estructura tiene similitudes entre sí, de modo que si se hace una homologación con los términos utilizados por cada enfoque se generaría una estructura en términos genérico; de este modo el resultado del análisis se registra en las siguientes tablas:

Análisis al proceso “Comunicación”
Observación: Este proceso solo es realizado por 5 de los enfoques seleccionados los cuales son COSO ERM, la norma ISO 31000, COBIT 5, ITIL, y PRINCE 2. La guía del PMBOK, APM y la ISO 27001 no tienen planteado un proceso individual para gestionar la comunicación de los riesgos.
Análisis: COBIT 5 e ITIL V3 manejan la comunicación de forma muy sencilla; en COBIT 5 dentro de APO12 Gestionar el Riesgo se encuentra la práctica de "Expresar el riesgo" en el cual se proporciona información sobre el estado actual de exposiciones y oportunidades relacionados con TI de una forma oportuna a todas las partes interesadas necesarias para una respuesta apropiada, generando documentos como lo son los informes del perfil de riesgo. Mientras que en ITIL V3, dentro de la fase de implementación se tiene como objetivo la definición de los procedimientos de continuidad del servicio y hacer que se desplieguen por toda la Organización, este despliegue se hace través de documentación e información como lo son los planes de respuesta ante emergencias, los planes de recuperación y los planes de evaluación. La norma NTC-ISO 31000 plantea un proceso denominado “Comunicación y Consulta” con el fin de gestionar las comunicaciones con las partes interesadas, en este proceso se generar un plan de comunicación y consulta (tanto externo e como interno), y se desarrolla dicho plan para integrarlo con el plan de gestión de riesgos del proyecto y el plan de gestión del proyecto, garantizando de esta manera estar al tanto de las expectativas de los involucrados con el proceso de riesgos. PRINCE 2 y COSO ERM lleva a cabo de manera continuada el proceso de comunicación con el propósito de asegurar que la información relacionada con las amenazas y oportunidades que enfrenta el proyecto se comunican dentro y fuera del proyecto a todas las partes interesadas necesarias, PRINCE 2 utiliza además diferentes informes de gestión para comunicar la información del riesgo. Algunos de estos informes son:

- Informe del Punto de Control
- Informe de Desarrollo
- Informe al Final de Fase
- Informe al Final de Proyecto
- Informe sobre las Lecciones

Conclusión: Tanto la Guía del PMBOK como la norma APM no disponen de un proceso por separado para gestionar las comunicaciones, dentro del PMBOK en su quinta versión se establecía dentro del proceso de Planificar, sin embargo en su sexta versión omitió esta actividad. Mientas la Norma ISO 31000 y PRINCE 2, establecen un proceso independiente, para el modelo propuesto se manejará como un proceso independiente o transversal, donde se permita una comunicación en todos los niveles de la organización tanto de forma interna como externa.

Análisis al proceso "Planificar la gestión"

Observación: Este proceso solo es realizado por 4 de los enfoques seleccionados los cuales son PMBOK, APM, COSO ERM y COBIT 5

COSO ERM	PMBOK	APM	COBIT 5

Análisis: Estas 4 normas poseen procesos con actividades similares siendo el más sencillo el proceso de COSO ERM el cual es el establecimiento de los objetivos los cuales están alineados con el riesgo aceptado de la entidad, el cual impulsa sus niveles de tolerancia al riesgo, sin embargo el proceso del PMBOK (Planificar la gestión de riesgo) posee al igual el establecimiento de objetivos, y de los niveles de apetito y tolerancia al riesgo y otros factores de importancia como los roles y responsabilidades del equipo del proyecto, las reservas de contingencia y de gestión; mientras dentro del proceso Iniciar de APM como primer paso se debe consolidar la información relevante sobre el proyecto y se elaboran los planes estratégicos

y planes tácticos detallados para el proceso de gestión de riesgos del proyecto. Por último, en COBIT 5 dentro del proceso Asegurar la Optimización del Riesgo, se encuentra la práctica clave Orientar la gestión de riesgos en el cual se orientar el establecimiento de prácticas de gestión de riesgos, obteniendo como productos principales la política de gestión de riesgo y los objetivos claves a ser monitorizados por la gestión de riesgos.

Análisis al proceso "Identificar riesgo"
Observación: Este proceso es realizado por todas las metodologías.
Análisis: Dentro de la norma ISO 270001 al momento del establecimiento del SGSI la Organización debe identificar los activos dentro del alcance del SGSI y los propietarios de dichos activos, de forma paralela debe identificar las amenazas a esos activos que afecten los criterios de confidencialidad, integridad y disponibilidad. En la norma ISO 31000, la identificación del riesgo es un subproceso dentro del proceso de Valoración del riesgo, este subproceso sugiere las siguientes actividades: • Identificar los eventos de riesgo. • Identificar fuentes de los riesgos. • Identificar áreas impactadas por los riesgos identificados. • Identificar causas y consecuencias potenciales. • Describir la técnica de identificación de riesgo aplicada. • Generar lista exhaustiva de riesgos identificados con base en los eventos que pueden afectar los objetivos. La guía del PRAM define este proceso como una fase denominada "Identificar", en la cual plantea las siguientes actividades: • Identificar los riesgos de forma amplia, práctica y temprana. • Describir las características del evento de riesgo.

- Determinar los tipos y fuentes de eventos de riesgos
- Establecer respuestas asociadas que puedan ser identificadas en esta fase (sino definirlas en la fase “Planear Respuestas”
- Elaborar lista de eventos de riesgos como registro.

La guía del PMBOK plantea un bloque de actividades de gestión más amplio que la guía PRAM permitiendo:

- Identificar todos los riesgos evidentes que pueden afectar a los objetivos del proyecto.
- Definir una descripción completa y estructurada del riesgo.
- Establecer la propiedad y el nivel de detalle (asignar a un propietario único con una responsabilidad clara y rendición de cuentas de su gestión, guardando similitud con la norma ISO 27001).
- Identificar condiciones de activación de la respuesta.
- Identificar las respuestas (preliminar), al mismo tiempo registrar las acciones en el proceso de identificar riesgos, (sí las respuestas no son implementadas de inmediato, deben considerarse en el proceso posterior “Planificar la respuesta a los riesgos”).
- Registrar los resultados en un registro de riesgos.

En PRINCE 2, al igual que la norma ISO 31000, posee como subproceso la identificación del riesgo, la cual hace parte del análisis del riesgo, el cual se puede realizar de forma iterativa (como la norma APM) para poder determinar los riesgos potenciales a los que se puede enfrentar el proyecto. Por último la información queda documentada en el registro de riesgo.

En COBIT 5 la identificación se encuentra inmersa dentro del proceso APO12 Gestionar el Riesgo (Recopilar Datos), donde se registran datos sobre eventos de riesgo que han causado o pueden causar impactos al beneficio/valor facilitado por TI, a la entrega de programas y proyectos de TI y/o las operaciones y entrega de servicio de TI.

En ITIL V3 se da un proceso de identificación de activos, donde se realiza un análisis de amenazas y vulnerabilidades posibles (y potenciales) que pueden tener los servicios, esto como paso primordial para comenzar a plantear medidas que aseguren la Continuidad del Servicio (al igual que la ISO 27001, ITIL se enfoca en los criterios de disponibilidad, integridad y confidencialidad).

Análisis al proceso "Analizar riesgo"

Observación: Todos los enfoques poseen un proceso orientado al análisis y/o evaluación del riesgo, a excepción de ITIL V3 que no especifica cómo hacer la evaluación de los riesgos en los servicios.

Análisis: APM establece el análisis como una fase llamada "Evaluar" planteando las siguientes actividades:

- Validar si los eventos de riesgo identificados pueden ser cuantificados o ser manejados como supuestos bajo un enfoque cualitativo.
- Estimar la probabilidad de ocurrencia de cada evento de riesgo.
- Considerar el impacto potencial ocasionado si un evento de riesgo ocurre.
- Establecer una ventana del impacto del riesgo e indicar cuando es probable que el impacto se produzca.
- Priorizar los eventos de riesgo en términos del nivel de la amenaza que representa para el logro de los objetivos del proyecto o de la oportunidad de mejorar los resultados.
- Identificar respuestas preliminares (debe determinarse su eficacia y sus repercusiones en los costos), estas deben ser validadas en las fase Planear respuestas.
- Combinar la incertidumbre asociada a los eventos de riesgo individuales y decidir el tratamiento de consecuencias.
- Aplicar modelo probabilístico para los eventos asociados a un enfoque cuantitativo.

- Afinar distribuciones de probabilidad y hacer ajustes finales.
- Determinar nivel acumulado del costo global definitivo.
- Generar un diagnóstico de riesgo y las respuestas al problema.
- Generar planes de base y planes de contingencia.
- Actualizar la lista de eventos de riesgos.

La NTC-ISO 31000 define un proceso llamado "Valoración del Riesgo" compuesto por 3 sub-procesos: Identificación del riesgo, Análisis del riesgo y Evaluación del Riesgo, estos dos últimos se relacionan con el proceso analizado.

Análisis del riesgo. Actividades definidas:

- Considerar las causas y fuentes de los riesgos.
- Considerar las consecuencias positivas y negativas
- Considerar que la probabilidad de que las consecuencias puedan ocurrir
- Considerar los controles existentes, su eficacia y eficiencia.
- Combinar las consecuencias y la probabilidad para determinar el nivel del riesgo.
- Determinar el tipo de riesgo con base en el nivel del riesgo calculado.
- El análisis puede ser cualitativo, semi-cuantitativo o cuantitativo, o una combinación de ellos, según las circunstancias.

Evaluación del riesgo. Las actividades aplicadas son:

- Comparar el nivel del riesgo obtenido en el análisis y de los criterios del riesgo establecidos al considerar el contexto.
- Considerar el tratamiento que se dará al riesgo con base en la comparación anterior. En las decisiones se debe incluir la tolerancia al riesgo.

En cuanto al proceso de Análisis Cuantitativo la norma NTC-ISO 31000 solo nombra este proceso como una posible actividad que se puede desarrollar a mayor profundidad, pero no menciona ninguna actividad por detallado como si lo hace en el análisis cualitativo.

La norma NTC-ISO 27001 en el Establecimiento del SGSI, determina que la organización debe:

- Valorar el impacto de negocios que podría causar una falla en la seguridad, sobre la organización, teniendo en cuenta las consecuencias de la pérdida de confidencialidad, integridad o disponibilidad de los activos.
- Valorar la posibilidad realista de que ocurra una falla en la seguridad, considerando las amenazas, las vulnerabilidades, los impactos asociados con estos activos, y los controles implementados actualmente.
- Estimar los niveles de los riesgos.

COBIT 5 posee una práctica denominada "Analizar el riesgo" aquí se estima la frecuencia y magnitud de pérdida o ganancia asociada con escenarios de riesgos de TI, se compara el riesgo residual con la tolerancia al riesgo y se identifica exposiciones que puedan requerir una respuesta al riesgo. Asimismo, se analiza el coste-beneficio de las opciones de respuesta al riesgo potencial y se propone la respuesta al riesgo óptima.

COSO ERM establece un proceso denominado "Evaluación de riesgo" realizándola a través de dos perspectivas: impacto y probabilidad, esta metodología aclara que los enfoques cuantitativos no sustituyen necesariamente a los enfoques cualitativos, sino que se complementan, dentro de las metodologías y técnicas establece:

Enfoques cualitativos:

- Autoevaluación.
- Mapas de riesgo.

Enfoques cuantitativos:

- Distribuciones de severidad y frecuencia.
- Procesos estocásticos.

Por último, la guía del PMBOK separa este proceso en Análisis Cualitativo y Cuantitativo de los riesgos, de esta forma se permite tener una mejor gestión por separado de los riesgos individuales y del riesgo global del proyecto; al igual brinda la opción que si no se dispone de datos amplios históricos de los riesgos de los proyectos, se puede aplicar solo el método cualitativo para analizar los riesgos individualmente y definir sus respectivas respuestas.

El análisis cualitativo incluye las siguientes actividades:

- Seleccionar características del riesgo que definen la importancia de los riesgos.
- Recopilar y analizar los datos:
  - ✓ Evaluar la probabilidad que cada riesgo ocurrirá.
  - ✓ Determinar el impacto de cada riesgo individual sobre los objetivos del proyecto.
- Priorizar los riesgos por la probabilidad y el impacto sobre los objetivos específicos.
- Priorizar los riesgos por probabilidad e Impacto sobre el Proyecto Global.
- Categorizar las causas de riesgos.
- Documentar los resultados del análisis cualitativo.

Mientras las actividades que componen el proceso del análisis cuantitativo son:

- Disponer de la lista de priorización de riesgos (generada en el análisis cualitativo de riesgos)
- Examinar las interrelaciones entre los riesgos individuales.
- Recopilar datos del riesgo de alta calidad.
- Disponer del modelo del proyecto (cronograma de proyecto, estimación de costos).
- Realizar análisis cuantitativo de riesgos (modelos numéricos, combinación de resultados, límites de confianza y análisis de sensibilidad a través de simulación Monte Carlo o de árboles de decisión).
- Consolidar los resultados del análisis.
- Determinar qué tan probable es el éxito en el proyecto.
- Determinar la reserva de contingencia del proyecto.

- Identificar riesgos que son de alta prioridad y actualizar la lista priorizada de riesgos.
- Ajustar el plan del proyecto de acuerdo con el resultado del análisis cuantitativo.

Análisis al proceso "Planificar respuesta"
Observación: Todos los enfoques poseen un proceso orientado a la planificación de respuestas a los riesgos, a excepción de ITIL V3.
Análisis: La norma NTC-ISO 31000 plantea un proceso llamado "Tratamiento del Riesgo", es un proceso cíclico que incluye las siguientes actividades: • Valoración del tratamiento del riesgo. • Validar si los niveles de riesgo residual son tolerables. • Si los niveles no son tolerables, generar un nuevo tratamiento para el riesgo. • Valoración de la eficacia de dicho tratamiento. • Identificar el orden de prioridad en el que se deben implementar los tratamientos para los riesgos. Las opciones de tratamiento del riesgo pueden ser: • Evitar el riesgo al decidir no iniciar o continuar la actividad que lo originó. • Tomar o incrementar el riesgo para perseguir una oportunidad. • Retirar la fuente del riesgo. • Cambiar la probabilidad. • Cambiar las consecuencias. • Compartir el riesgo con una o varias partes. • Retener el riesgo mediante una decisión informada. **Nota:** Las opciones de tratamiento pueden ser individuales o combinadas. Dentro de NTC-ISO/IEC 27001 se identifica y evalúa las opciones para el tratamiento de los riesgos. Las posibles acciones incluyen:

- Aplicar los controles apropiados.
- Aceptar los riesgos con conocimiento y objetividad, siempre y cuando satisfagan claramente la política y los criterios de la organización para la aceptación de riesgos.
- Evitar riesgos.
- Transferir a otras partes los riesgos asociados con el negocio, por ejemplo: aseguradoras, proveedores, etc.

Dentro de PRINCE 2 se planifica respuestas específicas a las amenazas y oportunidades, PRINCE2 sugiere 6 tipos de respuestas para las amenazas y 4 para las oportunidades.

- Las 6 respuestas a las amenazas son: evitar, reducir, estrategia alternativa (consiste en planificar alguna acción alternativa que pueda ser llevada a cabo si el riesgo ocurre. Estas acciones ayudarán a reducir el impacto de la amenaza.), transferir, compartir y aceptar.
- Las 4 respuestas a las oportunidades son: aprovechar, incrementar, compartir o rechazar.

La norma APM plantea una fase denominada "Planificar Respuestas", dividida en dos sub-fases, éstas se describen a continuación con sus respectivas actividades:

Planificar Respuestas a Eventos de Riesgos:

- Validar respuestas identificadas en los procesos anteriores.
- Revisar los eventos de riesgo identificados y generarle una respuesta apropiada.
- Definir condiciones de activación.
- Planificar la reserva necesaria para hacer frente al evento de riesgo si este ocurre.
- Repetir la evaluación del riesgo para validar la exposición residual.

Planificar Respuestas a Riesgos del Proyecto, Las actividades planteadas son:

- Con base en el efecto del conjunto de respuestas específicas definir respuestas asociadas a la gestión colectiva del riesgo global. Es importante tener por lo menos una respuesta potente disponible.
- Integrar con los procesos anteriores.

En COSO ERM habiendo identificado los riesgos significativos, la gerencia determina como responderá para mitigarlos, eligiendo entre las estrategias alternativas de: evitar, reducir, compartir o aceptar. Se evalúa el efecto en el impacto y probabilidad del riesgo, así como el costo-beneficio, seleccionando una respuesta que lleve al riesgo residual a ubicarse dentro de la tolerancia del riesgo deseado. Comprende las siguientes actividades:

- Categorías de Respuestas.
- Identificar respuestas al riesgo.
- Evaluar efectos en impacto y probabilidad.
- Evaluar costo-beneficio.
- Selección de respuestas.

COBIT 5 establece dentro del proceso gestionar el riesgo, la practica denominada "Definir un portafolio de acciones para la gestión de riesgos" en el cual se mantiene un inventario de actividades de control que estén en marcha para gestionar al riesgo y que permitan que el riesgo que se tome esté alineado con el apetito y tolerancia al riesgo y se define un conjunto de propuestas de proyecto equilibradas diseñadas para reducir el riesgo y/o proyectos que permitan oportunidades estratégicas empresariales, considerando costes/beneficios, el efecto en el perfil de riesgo actual y las regulaciones.

La guía del PMBOK dentro de su proceso de planificar la gestión de riesgos define las siguientes actividades:

- Identificar las respuestas.
- Seleccionar las respuestas.
- Planificar la acción.
- Definir propietarios y asignar responsabilidades.
- Actualizar el registro de riesgos.

- Revisar la exposición residual del riesgo (si la exposición no es aceptable ajustar respuesta)
- Actualizar el plan de gestión del proyecto (incluye costos, asignación de recursos, detalles de la programación y cambios en la documentación del proyecto).

Para los riesgos individuales se definen las siguientes estrategias de respuesta:

- **Para las amenazas:** Evadir, transferir, mitigar y aceptar.
- **Para las oportunidades:** Explotar, compartir, mejorar y aceptar.

Con la nueva versión de la guía del PMBOK se añade la estrategia de "Escalar riesgo" tanto para las amenazas como las oportunidades. La guía PMBOK establece:

- El escalar respuesta al riesgo se realiza cuando el equipo de proyecto o el patrocinador concluyen que el riesgo está fuera del alcance del proyecto.
- También podría ocurrir que el riesgo esté en el alcance pero que las acciones de respuesta estén más allá de la autoridad del Director de proyectos, en este caso el riesgo debe ser escalado.
- Los riesgos escalados se gestionan a nivel de programa, portafolio o el área organizacional apropiada que no esté a nivel de proyecto. Es recomendable que el Gerente de proyectos obtenga la confirmación de aceptación del riesgo escalado por parte de la persona u unidad organizacional que recibe.
- El Gerente de proyecto determina quién debe ser notificado acerca de las amenazas u oportunidades, comunicando los detalles que sean necesarios.
- Los riesgos son escalados al nivel organizacional cuyos objetivos se vean más afectados si la amenaza ocurre (O se vean más beneficiados si se trata de una oportunidad).
- Las amenazas u oportunidades dejan de ser monitoreadas por el equipo de proyecto después de ser escaladas. Sin embargo, se pueden dejar documentadas en el registro de riesgos para propósitos informativos.

Análisis al proceso “Implementar respuesta”
Observación: Todos los modelos metodológicos a excepción de COSO ERM poseen un proceso encaminado a la implementación de respuesta a los riesgos.
Análisis: La norma APM establece un proceso de implementación de respuesta, ya que no tiene sentido ejecutar todas las fases anteriores en el proceso de administración de riesgos si las respuestas planificadas no se implementan. En el contexto de la gestión de riesgos del proyecto a nivel estratégico, la fase de Implementar respuestas se enfoca en asegurar que los planes estratégicos se cambien para reflejar toda la gestión de riesgos anterior, y esto se refleja completamente en cualquier proceso relacionado de sanción de proyectos y acuerdos asociados. Más adelante, si se están implementando planes detallados, la fase de Implementar respuestas puede implicar asegurar que los responsables de las respuestas específicas hagan lo que se requiere. La norma NTC-ISO 31000 plantea un proceso denominado “Tratamiento del riesgo” con el fin de realizar la selección de una o más opciones para modificar los riesgos y la implementación de tales opciones. El propósito de los planes para el tratamiento del riesgo es documentar la forma en que se van a implementar las opciones de tratamiento seleccionadas. La información suministrada en los planes de tratamiento debería incluir: • Las razones para la selección de las opciones de tratamiento, que incluyan los beneficios que se espera obtener; • Personal responsable de aprobar el plan y los responsables de implementarlo. • Acciones propuestas. • Requisitos de recursos, incluyendo las contingencias. • Medidas y restricciones de desempeño. • Requisitos de monitoreo y reporte.

- Tiempo y cronograma.

Los planes de tratamiento se deberían integrar con los procesos de gestión de la organización y se deberían discutir con las partes involucradas pertinentes. Los encargados de tomar las decisiones y otras partes involucradas deberían conocer la naturaleza y la extensión del riesgo residual después del tratamiento del riesgo. El riesgo residual se debería documentar y someter a monitoreo, revisión y, cuando así corresponda, a tratamiento adicional.

En PRINCE 2 dentro de su ciclo de gestión de riesgos se encuentra el proceso de Implementar respuestas, el objetivo de este paso es asegurarse de que las respuestas planificadas se realicen; tanto las acciones correctivas como de seguimiento. En este paso, lo principal a decidir es:

- ¿Quién realizará el seguimiento de estos riesgos? (Propietario del riesgo)
- ¿Quién será el responsable de llevar adelante las respuestas planificadas? (Ejecutor del riesgo)

El manual PRINCE2 menciona dos roles específicos, ellos son: Propietario del riesgo y Ejecutor del riesgo los cuales pueden ser la misma persona.

- El Propietario del riesgo es responsable de gestionar y realizar el seguimiento de los aspectos relacionados con el riesgo. Además, puede llevar a cabo acciones que le hayan sido asignadas.
- El Ejecutor del riesgo es alguien asignado para llevar a cabo acciones particulares además de dar apoyo al Propietario del riesgo. Por lo tanto no son responsables de gestionar ni de realizar el seguimiento.

La norma NTC-ISO/IEC 27001 posee un proceso denominado Implementación y operación del SGSI, en el cual se identifica actividades muy enfocadas al tratamiento de los riesgos, entre ellas se encuentra:

- Implementar el plan de tratamiento de riesgos para lograr los objetivos de control identificados, que incluye considerar la financiación y la asignación de funciones y responsabilidades.

- Implementar los controles seleccionados.
- Definir cómo medir la eficacia de los controles o grupos de controles seleccionados, y especificar cómo se van a usar estas mediciones con el fin de valorar la eficacia de los controles para producir resultados comparables y reproducibles.
- Implementar programas de formación y de toma de conciencia.
- Gestionar la operación del SGSI.
- Gestionar los recursos del SGSI.
- Implementar procedimientos y otros controles para detectar y dar respuesta oportuna a los incidentes de seguridad.

ITIL, dentro de la fase de implementación del proceso de Gestión de la Continuidad posee la actividad puesta en marcha de procedimientos, aquí se realizan pruebas iniciales con el fin de realizar un informe que plantee mejoras para evitar la existencia de fallos que no permitan recuperar un servicio en un tiempo acordado con el cliente y que provoque pérdidas a la Organización. Dicha actividad es lo más parecido que posee este modelo metodológico para la implementación de respuestas.

COBIT 5, establece la práctica responder al riesgo la cual hace parte del proceso Gestionar riesgo, esta práctica permite responder de una forma oportuna con medidas efectivas que limiten la magnitud de pérdida por eventos relacionados con TI.

La norma COSO ERM no establece un proceso separado para la implementación de las respuestas de los riesgos.

El PMI estableció en su nueva guía del PMBOK un proceso de gestión de proyectos dedicado a garantizar que se implemente las respuestas al riesgo.

De acuerdo a lo establecido en la nueva versión implementar la respuesta al riesgo es el proceso para implementar los planes de respuesta al riesgo que han sido acordados y documentados en el plan de gestión de riesgos. Está dirigido a garantizar que las respuestas acordadas sean

implementadas para abordar la exposición al riesgo, minimizar las amenazas y aprovechar las oportunidades.

- Los insumos para su ejecución son:
  - ✓ Plan de gestión de riesgos.
  - ✓ El registro de riesgos.
  - ✓ Registro de lecciones aprendidas.
  - ✓ Otros activos de proceso organizacional como lo son políticas, procedimientos, metodologías, entre otros.

El PMI enfatiza la necesidad que los dueños del riesgo inviertan el esfuerzo necesario en implementar las respuestas al riesgo acordadas. Solo así se puede asegurar que la exposición a las amenazas sea minimizada y se aprovechen al máximo las oportunidades.

Análisis al proceso "Monitoreo"
Observación: Todos los modelos metodológicos a excepción de APM y PRINCE 2 poseen un proceso encaminado al monitoreo de los riesgos.
Análisis: La guía del PMBOK establece este proceso, el cual se encarga de monitorear la implementación de los planes de respuesta acordados, hacer seguimiento a los riesgos identificados, identificar y analizar nuevos riesgos. Este proceso ya existía en versiones previas de la guía del PMBOK y su principal beneficio es asegurar que las decisiones del proyecto se basen en información actualizada y correcta sobre el estado de los riesgos. La razón del cambio de nombre de Controlar a Monitorear, obedece a que durante el proyecto, estos procesos se encargan de observar (monitorear) para entender que está sucediendo y ajustar la estrategia según las necesidades cambiantes. entre las actividades definidas en este proceso se encuentra: • Realizar revisiones periódicas del estado de los riesgos. • Realizar auditorías para determinar las fortalezas y debilidades en el manejo de riesgos dentro del proyecto.

- Realizar un análisis integral de la gestión de riesgos al final del proyecto: Describir al cierre de todos los riesgos en el registro de riesgos: a) Si se materializaron o no, (b) Si se produjeron, nombrar el plan de contingencia, frecuencia, las acciones aplicadas no planificadas (c) y el impacto en el proyecto (es decir, en el alcance, tiempo, costo y calidad).

La norma NTC-ISO 31000 plantea un proceso llamado "Monitoreo y Revisión" con las siguientes actividades:

- Revisar periódicamente la efectividad de los controles.
- Detectar cambios en el contexto interno o externo e identificar riesgos emergentes.
- Incluir los resultados en las actividades globales de gestión del desempeño, medición y reporte interno y externo de la organización.

La norma NTC-ISO 27001 establece un proceso de Seguimiento y revisión del SGSI, en el cual establece que la organización debe:

- Ejecutar procedimientos de seguimiento y revisión y otros controles para:
  - ✓ Detectar rápidamente errores en los resultados del procesamiento.
  - ✓ Identificar con prontitud los incidentes e intentos de violación a la seguridad, tanto los que tuvieron éxito como los que fracasaron.
  - ✓ Posibilitar que la dirección determine si las actividades de seguridad delegadas a las personas o implementadas mediante tecnología de la información se están ejecutando en la forma esperada.
  - ✓ Ayudar a detectar eventos de seguridad, y de esta manera impedir incidentes de seguridad mediante el uso de indicadores.
  - ✓ Determinar si las acciones tomadas para solucionar un problema de violación a la seguridad fueron eficaces.
- Emprender revisiones regulares de la eficacia del SGSI (que incluyen el cumplimiento de la política y objetivos del SGSI, y la revisión de los controles de seguridad) teniendo

en cuenta los resultados de las auditorias de seguridad, incidentes, medición de la eficacia sugerencias y retroalimentación de todas las partes interesadas.

- Medir la eficacia de los controles para verificar que se han cumplido los requisitos de seguridad.
- Revisar las valoraciones de los riesgos a intervalos planificados, y revisar el nivel de riesgo residual y riesgo aceptable identificado, teniendo en cuenta los cambios en:
  - ✓ La organización.
  - ✓ La tecnología.
  - ✓ Los objetivos y procesos del negocio: las amenazas identificadas, la eficacia de los controles implementados, y eventos externos, tales como cambios en el entorno legal o reglamentario, en las obligaciones contractuales, y en el clima social.
- Realizar auditorías internas del SGSI a intervalos planificados.

ITIL dentro de la fase de mejora establece actividades de seguimiento donde se realiza informes de seguimiento que arrojen información de consecución de objetivos y auditorías tanto internas como externas las cuales aportan algo más de confiabilidad al Proceso.

COSO ERM establece un proceso de monitoreo en el cual se hace supervisiones de forma continua de las actividades, Incluye las siguientes actividades:

- Auditores internos.
- Auditores externos.
- Evaluaciones continuas / supervisión permanente.
- Reporte de Deficiencias.

COBIT 5 dentro del proceso Asegurar la Optimización del Riesgo, posee una práctica denominada supervisar la gestión de riesgos, aquí se supervisa los objetivos y las métricas clave de los procesos de gestión de riesgo y establecer cómo las desviaciones o los problemas serán seguidos para su resolución, entre las actividades que se establecen es esta práctica se encuentra:

- Facilitar la revisión por las principales partes interesadas del progreso de la empresa hacia los objetivos identificados.
- Supervisar has qué punto se gestiona el perfil de riesgo dentro de los umbrales de apetito de riesgo.
- Supervisar las metas y métricas clave de gestión de los procesos de gobierno y gestión del riesgo respecto a los objetivos, analizar las causas de las desviaciones e iniciar medidas correctivas para abordar las causas subyacentes.

4.2. DISEÑO DEL MODELO PARA LA GESTIÓN DE RIESGOS.

La gestión de riesgos en proyectos de TI es un proceso iterativo que implica la identificación, análisis, evaluación y planificación, y control de la respuesta al riesgo, que se lleva a cabo a lo largo del ciclo de vida del proyecto (Brandas et al., 2012). Esto ha sido destacado por Taylor et al. (2008) y Bannerman (2008). Para administrar problemas complejos asociados con proyectos de TI, Kwak y Stoddard (2004) recomiendan la implementación de un proceso formal de administración de riesgos haciendo hincapié en los procesos de identificación y análisis como los más importantes y de mayor detalle y coordinación a realizar; de igual forma, Hubbard (2009) vincula esto con una visión que resalta que la gestión del riesgo es la identificación, evaluación y priorización de los riesgos, seguida de una aplicación de recursos efectiva y eficiente para maximizar la realización de oportunidades y reducir, controlar y monitorear la probabilidad y /o impacto de los acontecimientos. Además, Richardson (2010) destaca que este proceso debe ser proactivo a lo largo del ciclo de vida del proyecto para que siga siendo efectivo.

En virtud de lo anterior, y complementando con el análisis comparativo entre las actividades planteadas en los procesos de los enfoques metodológicos de gestión de riesgos presentados en el numeral anterior, se determina los procesos que se incluirán el modelo de gestión de riesgos propuesto los cuales son:

- Preparar la gestión de riesgos.
- Identificar riesgos.

- Analizar riesgos.
- Tratar riesgos.

Se toma el proceso de preparar la gestión de riesgos, el cual es el primer proceso establecido en la ISO31000, en el cual se identifica el contexto externo e interno del proyecto, lo cual lo hace un proceso clave y claro para el equipo del proyecto.

Por último, rescatando una característica de las metodologías ágiles se tomará para este modelo las reuniones diarias y de retrospectiva, la cuales permitirán hacer un seguimiento en tiempo real. Por cada uno de estos procesos, se define su objetivo clave a realizar para dar cumplimiento a éste, asimismo ciertos procesos tienen actividades para poder alcanzar dicho objetivo.

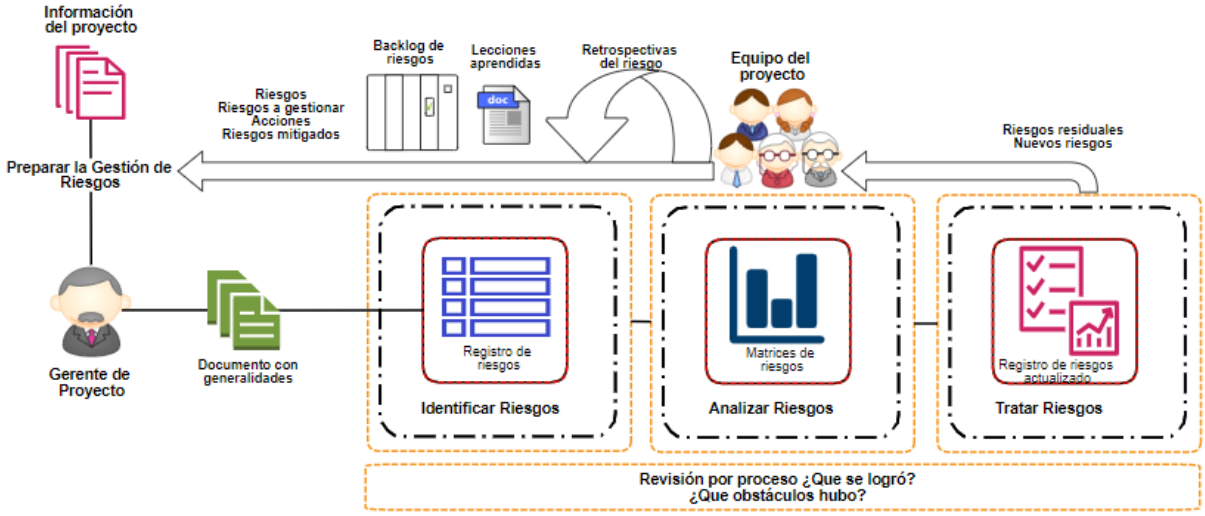


Figura 21. Procesos Modelo de Gestión de Riesgos CSM.

Fuente: Elaboración propia.

Para un mejor resultado en la aplicación del modelo, durante todo el ciclo de vida del proyecto se debe cumplir con los siguientes principios:

- Alinear con los objetivos de la organización.
- Alinear la gestión de los riesgos de los proyectos informáticos con la gestión de los riesgos de la organización.

- Promover la comunicación abierta y la documentación de la gestión de los riesgos.
- Establecer enfoque directivo y responsabilidades.
- Promover la mejora continua.

De igual forma se debe implementar el modelo de forma iterativa donde los riesgos se consideran a la hora de seleccionar el contenido de cada iteración, y los riesgos también serán identificados, analizados y gestionados durante cada iteración.

Se sugiere un mínimo de tres ciclos para gestionar los riesgos a nivel estratégico, ya que al finalizar la primera iteración y realizar la reunión de retrospectiva se obtendrá otro documento que es el Backlog de riesgos, el cual será una entrada al proceso de gestionar los riesgos y servirá de documento de comunicación para mantener informado a todo el equipo del proyecto.

4.2.1. PROCESO PREPARAR LA GESTIÓN DE LOS RIESGOS.

Objetivo: Realizar actividades concernientes a la preparación de la gestión de los riesgos. Una tarea clave del modelo para este proceso es establecer el contexto externo e interno como una actividad al inicio de este. Al establecer el contexto se definen, entre otros: los objetivos del proyecto, el entorno en el cual se conseguirán los objetivos, las partes involucradas y la diversidad de criterios de riesgo; todo en conjunto ayudará a revelar y evaluar la naturaleza y la complejidad de sus riesgos.

Actividades: Se propone 3 actividades principales en este proceso:

- **Establecer el contexto externo:** Es el ambiente externo, todo aquello fuera del proyecto que pueda influenciar sus objetivos. Tenerlos en consideración es muy importante para elaborar los criterios del riesgo. Algunos de los aspectos a tener en cuenta son: legales, normativos, tecnológicos, financieros, tendencias actuales y partes involucradas. En proyectos de naturaleza TI es muy importante este contexto, por lo que se debe tener en cuenta:
  - ✓ Ley 1816/2016 por el cual quedan exentos del IVA los computadores portátiles o de escritorio que tengan un valor máximo de $1.657.800 y tabletas y celulares cuyo valor máximo sea de $729.432.

- ✓ En proyectos de redes y telecomunicaciones WAN, es recomendable hacer visitas de campo, para así identificar las diferentes interferencias del ambiente y poder generar un plan de acción real. La Dra. Schwalbe en su libro "Information Technology Project Management" considera a las interferencias en el ambiente como uno de los riesgos que más se materializa en este tipo de proyectos.
- ✓ En proyectos que sean financiados por otros países se debe hacer seguimiento a la tasa de cambio, ya que esta podría ser un riesgo positivo (oportunidad) o negativo (amenaza), y se debe tener planes de respuesta para cuando se materialice.

- **Establecer el contexto interno:** Se refiere al ambiente interno, y está constituido por todo aquello dentro del proyecto que pueda influenciar sus objetivos. Algunos aspectos a tener en cuenta son: políticas, estrategias, recursos humanos, cultura organizacional, procesos, sistemas de información y partes involucradas internas, de igual forma tener en cuenta los hallazgos de auditorías internas los cuales pueden servir de insumo para la identificación y análisis de riesgos; en organizaciones del sector público, toda auditoría interna que haya generado hallazgos se le realiza un plan de mejoramiento, por lo cual es un documento que se debe considerar.
- **Establecer la estrategia de gestión de los riesgos:** Se refiere a la definición de la estrategia a utilizar para evaluar la importancia del riesgo. Algunos de los aspectos a tener en cuenta son: naturaleza, causas, consecuencias, apetito de riesgo, tolerancia al riesgo, el rol y la responsabilidad de cada persona en las actividades de gestión de riesgos del proyecto. Por ejemplo: "El director del proyecto será el responsable de gestionar los riesgos y de crear el plan de gestión de riesgos. También mantendrá actualizado el registro de riesgos y convocará a las reuniones de evaluación del estado de los riesgos. En la identificación de los riesgos participará todo el equipo del proyecto, el patrocinador, el cliente, y los principales interesados". Al final de la descripción del modelo se establece un gobierno de la gestión integral de los riesgos que sirva de base en la gestión de riesgos del proyecto.

Salidas: Documento con las generalidades del proyecto (valor, fechas, red de interesados, roles y responsabilidades, niveles de tolerancia al riesgo).

4.2.2. PROCESO IDENTIFICAR LOS RIESGOS.

Objetivo: Determinar, describir y documentar los riesgos que pueden afectar al proyecto, en este proceso se elabora una lista que permita determinar todos los aspectos que puedan impactar positiva o negativamente el logro de los objetivos del proyecto. Los aspectos básicos a tener en cuenta son: origen de los riesgos, impacto, causas y consecuencias; este es un proceso iterativo ya que con el avance del proyecto podrían surgir nuevos riesgos que se identifican y se agregan a la lista de riesgos.

Entradas: Para poder identificar los riesgos hay que considerar el documento con las generalidades del proyecto y complementarlo con la documentación del contrato.

Herramientas: A continuación se describen varias herramientas para identificar riesgos en los proyectos aplicando el modelo propuesto.

- **Análisis de "checklist" de riesgos:** Esta herramienta consiste en una lista con riesgos identificados en proyectos anteriores, la cual se puede usar como una lista de referencia, y recorrerlas a fin de considerar si dichos riesgos u oportunidades que se plantean se podrían presentar en el proyecto actual. Esta lista es sólo una ayuda, no se debe limitar la identificación solo al checklist, se deben considerar otros riesgos. El **anexo 1** consiste en un checklist de riesgos de proyectos informáticos identificados en el desarrollo de esta investigación el cual puede ser utilizado para este proceso.
- **Consultas a expertos:** Los expertos son personas especialistas en la materia, que conocen sobre los tipos de riesgos que se pueden presentar en un proyecto y/o han gestionado los riesgos de un proyecto similar. En todo proyecto TI, se debe tener en cuenta la experiencia u opinión de especialistas de diferentes áreas como lo son en desarrollo de software, redes y telecomunicaciones, seguridad informática entre otros.

Salidas: El resultado de identificar los riesgos es el registro de riesgos. Allí estarán listados los riesgos y su información relevante. La cantidad de columnas que se le quiera agregar a dicho

registro depende del Director de Proyecto, y de qué tanta información quiera recabar sobre los riesgos. Algunas buenas prácticas a tener en cuenta durante la consolidación de riesgos son:

- Los riesgos deberían ser expuestos claramente de tal forma que todos los miembros del equipo sean capaces de entender exactamente el riesgo cuando haya pasado un tiempo.
- En la descripción del riesgo se debería incluir el evento relacionado, el momento en que ocurrió y el impacto del mismo.

4.2.3. PROCESO ANALIZAR LOS RIESGOS.

Objetivo: Priorizar los riesgos evaluando la probabilidad de que ocurra y el impacto que tendrían dentro del proyecto si ocurren.

Entradas: Registro de riesgos que se identificó en el proceso anterior, cuando se analizan los riesgos hay que considerar, entre otras cosas, cuáles son las actitudes de los interesados del proyecto frente al riesgo. Por ejemplo, si los interesados principales son reacios al riesgo habrá que hacer un análisis más cuidadoso para evitar o minimizar la mayor cantidad de riesgos posible. Al comenzar a analizar los riesgos se discute en equipo y con los interesados, para determinar cuál es la probabilidad de que cada riesgo prioritario ocurra, y si ocurriera cuál sería su impacto.

Herramientas: El modelo propuesto utiliza como herramienta la matriz de probabilidad e impacto, una matriz por cada variable (alcance, tiempo, costo y calidad) en las cuales se realiza la priorización de los riesgos teniendo en cuenta el nivel de riesgo bajo el siguiente criterio:

- ✓ Riesgos bajos (zona verde): De 1 a 30
- ✓ Riesgos moderados (zona amarilla): De 31 a 50
- ✓ Riesgos Críticos (zona roja): Mayor que 50

Este criterio se obtiene de la siguiente escala de probabilidad e impacto:

ESCALA PARA ALCANCE:

Probabilidad	Escala de probabilidad	Descripción	Impacto	Escala de impacto	Descripción
Raro	**1**	Puede suceder en circunstancias excepcionales	**Muy Bajo**	**5**	Reducción del alcance apenas perceptible
Improbable	**2**	Es probable que NO suceda en la mayoría de las circunstancias	**Bajo**	**10**	Áreas menores del alcance son afectadas
Probable	**3**	Es posible que suceda algunas veces	**Moderado**	**15**	Áreas mayores del alcance son afectadas
Altamente Probable	**4**	Puede que suceda en la mayoría de las circunstancias	**Alto**	**20**	Reducción del alcance inaceptable para el cliente
Seguramente Suceda	**5**	Se espera que suceda en la mayoría de las circunstancias	**Crítico**	**25**	El producto final del proyecto es inservible

ESCALA PARA TIEMPO:

Probabilidad	Escala de probabilidad	Descripción	Impacto	Escala de impacto	Descripción
Raro	**1**	Puede suceder en circunstancias excepcionales	**Muy Bajo**	**5**	Variación del tiempo muy insignificante
Improbable	**2**	Es probable que NO suceda en la mayoría de las circunstancias	**Bajo**	**10**	Variación del tiempo menor a 5%
Probable	**3**	Es posible que suceda algunas veces	**Moderado**	**15**	Desviación general del proyecto de 5% a 10%

Altamente Probable	**4**	Puede que suceda en la mayoría de las circunstancias	**Alto**	**20**	Desviación general del proyecto es mayor de 10% hasta 20%
Seguramente Suceda	**5**	Se espera que suceda en la mayoría de las circunstancias	**Crítico**	**25**	Desviación general del proyecto es mayor de 20%

ESCALA PARA COSTO:

Probabilidad	Escala de probabilidad	Descripción	Impacto	Escala de impacto	Descripción
Raro	**1**	Puede suceder en circunstancias excepcionales	**Muy Bajo**	**5**	Variación del costo muy insignificante
Improbable	**2**	Es probable que NO suceda en la mayoría de las circunstancias	**Bajo**	**10**	Variación del costo menor a 5%
Probable	**3**	Es posible que suceda algunas veces	**Moderado**	**15**	Incremento del costo del proyecto entre 5% a 10%
Altamente Probable	**4**	Puede que suceda en la mayoría de las circunstancias	**Alto**	**20**	Incremento del costo del proyecto mayor al 10% hasta 20%
Seguramente Suceda	**5**	Se espera que suceda en la mayoría de las circunstancias	**Crítico**	**25**	Incremento del costo del proyecto mayor al 20%

ESCALA PARA CALIDAD:

Probabilidad	Escala de probabilidad	Descripción	Impacto	Escala de impacto	Descripción
Raro	**1**	Puede suceder en circunstancias excepcionales	**Muy Bajo**	**5**	Ningún daño relevante
Improbable	**2**	Es probable que NO suceda en la mayoría de las circunstancias	**Bajo**	**10**	Tratamiento leve, sólo aplicaciones muy específicas son afectadas
Probable	**3**	Es posible que suceda algunas veces	**Moderado**	**15**	Tratamiento leve con perdidas
Altamente Probable	**4**	Puede que suceda en la mayoría de las circunstancias	**Alto**	**20**	Reducción de la calidad inaceptable, genera pérdidas importantes
Seguramente Suceda	**5**	Se espera que suceda en la mayoría de las circunstancias	**Crítico**	**25**	Las consecuencias para la entidad serian catastróficas

Salidas: Registro de Riesgos Actualizado, al actualizar el registro de riesgos resultan dos listas de riesgos, por un lado se obtiene una lista con los riesgos a tratar en el corto plazo. Es decir, aquellos riesgos más urgentes que hay que abordar, y una lista de riesgos para supervisar, es decir, riesgos de baja prioridad que podrían cambiar su prioridad al avanzar el proyecto, y por eso se debe supervisarlos para asegurarse que todo sigue bajo control.

4.2.4. PROCESO TRATAR LOS RIESGOS.

Objetivo: Seleccionar las acciones a tomar asociadas a cada riesgo de alta prioridad. Será necesario planificar dichas acciones, realizar un seguimiento sobre las mismas y controlarlas con el objetivo de reducir el valor del riesgo (el grado de exposición del riesgo).

Entradas: Registro de riesgos actualizado.

Herramienta: Para el tratamiento de los riesgos el modelo propuesto recomienda aplicar lo siguiente:

- **Estrategia de respuesta:** El modelo propuesto propone diferentes estrategias de respuesta teniendo en cuenta si son riesgos positivos o negativos:

  Las estrategias para enfrentar los riesgos positivos son:

  - ✓ **Explotar el riesgo:** Esta estrategia busca eliminar la incertidumbre asociada con una oportunidad haciendo que la oportunidad definitivamente se concrete.
  - ✓ **Aceptar el riesgo**: El equipo del proyecto no puede o escoge no tomar ninguna acción para enfrentar el riesgo.

  Las estrategias para enfrentar los riesgos negativos son:

  - ✓ **Aceptar el riesgo**: El equipo del proyecto no puede o escoge no tomar ninguna acción para enfrentar el riesgo.
  - ✓ **Transferir el riesgo:** Trasladar el impacto negativo del riesgo hacia un tercero. Por ejemplo, contratar un seguro o colocar una penalidad en el contrato con el proveedor. La transferencia de un riesgo simplemente confiere a una tercera parte la responsabilidad de su gestión, pero no lo elimina, lo cual implica que este riesgo ha de ser observado con detalle. La transferencia de la responsabilidad de un riesgo es más eficaz cuando se trata de riesgos financieros. Las herramientas de transferencias pueden ser diversas e incluyen seguros, garantías de cumplimiento, fianzas, etc. En proyectos TI, son pocas las empresas aseguradoras que ofrece pólizas para estos proyectos.
  - ✓ **Evitar el riesgo:** Cambiar las condiciones originales de realización del proyecto para eliminar el riesgo identificado. **Ejemplo:** Si se tiene el riesgo de realizar un proyecto de desarrollo de software o de telecomunicaciones con una persona sin experiencia, ello se elimina al contratar un experto que lo reemplace, otro escenario es si en un proyecto se decide traer una tecnología importada y esta pueda traer graves problemas (conflictos) en el equipo que desarrolla el proyecto, evitar este

riesgo sería desestimar la utilización de esa tecnología y reemplazarla por alguna otra. La estrategia de evasión más drástica consiste en anular por completo el proyecto.

- ✓ **Mitigar el riesgo:** Lo que busca la estrategia de mitigación de riesgos es bajar la probabilidad de que un riesgo ocurra y/o bajar el impacto del riesgo. Se usa cuando no se puede transferir ni evitar el riesgo. Es una de las estrategias más usadas para gestionar los riesgos negativos. Se hace lo mejor que se pueda para reducir el posible daño del riesgo. **Ejemplo:** En un proyecto TI, existía un alto riesgo de que los usuarios de 20 países que usarían un sistema informático como resultado final del proyecto, no les gustara la solución o la encontraran difícil de usar. Para minimizar ese riesgo, se crea un equipo multidisciplinario de usuarios finales donde cada uno representaba a uno de los 20 países. Estas 20 personas se involucraron desde el inicio del levantamiento de los requerimientos funcionales y no funcionales, así se conocería sus opiniones sobre el alcance del sistema, para luego involucrarlos en las pruebas antes de lanzar el producto a todos los clientes. Al realizar las pruebas, estos usuarios podían hacer sugerencias, sentirse parte del proceso, y hacer comentarios válidos sobre qué cosas podrían o no funcionar en su país, además ayudaban a detectar errores temprano. Fue una forma de mitigar potenciales impactos negativos al lanzar el proyecto.
- ✓ **Investigar el riesgo:** Cuando no se posee el conocimiento sobre un riesgo, el equipo del proyecto crea un plan para investigar más el riesgo para después implementar una de las cuatro estrategias explicadas anteriormente.

- **Lluvia de ideas:** No limita la creatividad al pensar "en voz alta" sobre posibles respuestas a los distintos riesgos y permite involucrar a los interesados.

Salidas: El registro de riesgos se creó al identificar los riesgos y se actualizó en el paso de analizar los riesgos. Al ejecutar este proceso se anexa las columnas de Estrategia de Respuesta, Plan de acción, Responsable, Disparador y Estado del riesgo. Mediante ellas, se indica cómo se va a responder o tratar con cada uno de dichos riesgos.

4.2.5. REUNIONES DIARIAS Y REUNIÓN DE RETROSPECTIVA.

Los métodos ágiles proporcionan un marco ideal para introducir prácticas efectivas de gestión de riesgos, de estos métodos se adaptan las reuniones diarias que plantean problemas y bloqueadores también pueden actuar como alertas tempranas para posibles nuevos riesgos, estas reuniones se realizaran después de la ejecución de cada proceso (Identificar, Analizar y Tratar). Y al finalizar el proceso de tratar de la primera iteración del modelo se efectuará la retrospectiva.

Las retrospectivas de riesgo son revisiones periódicas del registro de riesgos y oportunidades, junto con evaluaciones de los procesos de gestión de riesgos utilizados en el proyecto. Al igual que revisamos la evolución de los procesos de productos y equipos a lo largo del proyecto, también deberíamos evaluar la efectividad del plan de gestión de riesgos y los procesos utilizados por el equipo.

N°	Preguntas retrospectiva de riesgo
1	¿Estamos eliminando o reduciendo nuestros riesgos?
2	¿Tenemos algún riesgo nuevo o creciente?
3	¿Cuáles son las causas fundamentales de nuestros riesgos, y podemos eliminar alguno de ellos?
4	¿Qué estrategias de prevención o eliminación de riesgos funcionan y cuáles no?
5	Para los riesgos que elegimos transferir, ¿cómo los administran los terceros? ¿Qué podemos aprender de ellos o sería mejor traerlos de vuelta internamente?
6	¿Cómo se están desarrollando las capacidades de gestión de riesgos de nuestro equipo?
7	¿Dónde todavía necesitamos apoyo?

4.2.6. GOBIERNO DE LA GESTIÓN INTEGRAL DE RIESGOS.

Para garantizar el buen funcionamiento del modelo propuesto, se ha definido un gobierno de riesgos, donde la responsabilidad en materia de control y gestión de riesgos y, en especial, en la fijación del apetito de riesgos para los proyectos, recae en última instancia en el consejo de administración de riesgos, el cual estará conformado por un grupo interdisciplinar de profesionales con experiencia y dominio del tema. A este consejo se le escalará los riesgos que no se han podido mitigar y/o tienen un gran impacto afectando tanto al proyecto como la imagen de la Alcaldía, asimismo se recomiendo que dentro de los grupos de proyecto se tenga personal con los siguientes roles y responsabilidades:

- **Gerente de proyecto:** Entre sus responsabilidades destaca acordar y promover el proceso de gestión de riesgos para el proyecto, aclarar el nivel aceptable de riesgo para el proyecto, reportar el estado de riesgo al cliente / alta gerencia regularmente, escalar riesgos que están por encima del umbral de riesgo o riesgos con un impacto significativo fuera del proyecto, aprobar acciones de respuesta al riesgo y el seguimiento de la efectividad de la gestión de riesgos en el equipo del proyecto.
- **Gestor de riesgos:** Es un administrador de riesgos profesional afín con la naturaleza del proyecto se responsabilice de la identificación y evaluación del riesgo y de la respuesta. Es una función que a veces se requiere para un programa de proyectos y proyectos sensibles al riesgo y se puede llevar a cabo ya sea a tiempo completo o de forma consultiva.
- **Especialista técnico:** Expertos en la materia ajenos al equipo del proyecto cuya contribución al proceso de gestión de riesgos podría ser vital. A menudo, los especialistas técnicos suelen ser las únicas personas capaces de estimar el grado de probabilidad o impacto de los riesgos identificados, asumiendo el rol temporal del propietario del riesgo. De manera similar, pueden estar en una mejor posición para recomendar acciones de tratamiento de riesgo cuando se consideran las respuestas de riesgo.

4.3. IMPLEMENTACIÓN DEL MODELO PARA LA GESTIÓN DE RIESGOS.

El proyecto escogido para implementar el modelo es "Adecuación y actualización de la plataforma MIDAS". A continuación se detalla las generalidades del proyecto:

- **Cliente del proyecto:** Secretaría de Planeación Distrital.
- **Organización ejecutora:** QUSPIDE S.A.S.
- **Modalidad de contratación:** Proceso de Mínima Cuantía.
- **Duración del proyecto:** 30 días.
- **Fecha de inicio:** 30 de Noviembre de 2016.
- **Fecha final:** 30 de Diciembre de 2016.
- **Valor:** $175.000.000
- **Objetivos:**
  - ✓ Crear un enlace permanente con las curadurías distritales para dotar a la ciudadanía y demás entes de control de una herramienta por medio de la cual puedan verificar en tiempo real el estado de la licencia de una construcción.
  - ✓ Ajustar la información de estratificación de las empresas de servicios públicos domiciliarios con la del Distrito de Cartagena de Indias.
- **Matriz de riesgos:** La matriz utilizada es la que se explica en la sección 3.2. Estado Actual.

El alcance inicial del proyecto era de dotar a la ciudad de una herramienta de verificación de licencias de construcción, para así las entidades competentes realizar el correspondiente seguimiento y poder detener las construcciones que violaban las especificaciones de la licencia e identificar las licencias falsas que fueran denunciadas por la ciudadanía. El 27 de abril del año 2017, ocurre el desplome del edificio Blas de Lezo 2, el cual era 1 de 47 edificaciones construidos con licencias falsas, licencias que no se reflejaban en la plataforma MIDAS, a raíz de esto la Contraloría Distrital de Cartagena de Indias realizó una auditoría especial a la plataforma MIDAS, arrojando los siguientes resultados:

- Se evidenció que las transacciones realizadas al log del servidor no se reflejaban en la plataforma, ya que estas apuntaban a un servidor donde se realizaron pruebas y no se realizó el cambio.
- Se evidenció fallas en el seguimiento operativo de la aplicación y comunicación entre la Secretaría y la Empresa ejecutora.
- No se entregaron manuales, ni guías, en el expediente que reposa el informe final del contrato emitido por el contratista manifiesta lo siguiente: “No se contó con el apoyo de las curadurías en el correcto cargue de la información de licencias”. Al indagar y citar a los delegados de las diferentes curadurías estos respondieron que no los capacitaron en el uso de la plataforma y no sabían utilizar la herramientas, de la misma forma solicitaron copia de manuales, sin embargo la secretaría les contestó que no tenían manuales. De esta forma se evidencia que la Secretaría de Planeación no vinculó formalmente a las curadurías en el desarrollo del proyecto, lo que causó inconvenientes en la puesta en ejecución del sistema y su posterior operatividad.
- No se observan definidos acuerdos de nivel de servicio, ni cláusulas que incluyan soporte técnico posterior a la ejecución contractual, la Secretaría no realiza una identificación de riesgos teniendo en cuenta la naturaleza del proyecto.

Al implementar el modelo se obtiene los siguientes resultados:

4.3.1. PREPARAR LA GESTIÓN DE LOS RIESGOS

Las tareas clave del modelo para este proceso es establecer el contexto externo e interno, por tal motivo lo principal es hacer la identificación de Stakeholders; el proyecto tenía dos objetivos, el primero que la ciudadanía y entes de control puedan verificar en tiempo real el estado de la licencia de una construcción. Por tal motivo los principales Stakeholders externos para este objetivo son:

- Entes de Control.
- Curadurías Urbanas.
- Ciudadanía.

El último objetivo del proyecto era ajustar la información de estratificación de las empresas de servicios públicos domiciliarios con la del Distrito de Cartagena de Indias y que ésta fuera visible en la plataforma. Por tal motivo los principales Stakeholders externos para este objetivo son:

- Empresas de Servicio Público.
- Instituto Geográfico Agustín Codazzi (I.G.A.C).

Los Stakeholders internos para el cumplimiento de los objetivos del proyecto son:

- Ingeniero de Software.
- Ingeniero Ambiental.
- Topógrafo.
- Arquitecto.
- Unidades de soporte.

De igual forma, dentro del contexto interno se debe tener en cuenta los resultados arrojados de la auditoría especial realizada por la Contraloría Distrital los cuales fueron descritos en el punto anterior. La Siguiente actividad del modelo es establecer la estrategia de gestión de los riesgos, en ésta se debe identificar los roles y responsabilidades, dentro de este modelo se propone el rol de Especialista Técnico, el cual, dentro de este proyecto para alcanzar el primer objetivo es recomendable la opinión y experiencia de un Ingeniero con especialidad en Sistemas de Información Geográfica (S.I.G). De igual forma se determina los siguientes roles:

- Director del proyecto: Adm. Luz Elena Paternina Mora (Secretaria de Planeación).
- Director de riesgos: Ingeniero de Software.

El ingeniero de software será el responsable de la gestión de riesgos y de crear el plan de gestión de riesgos. Mantendrá actualizado el registro de riesgos y convocará a las reuniones de evaluación del estado de los riesgos. En la identificación de los riesgos participará todo el equipo de gestión del proyecto, el patrocinador, el cliente y los principales interesados. Dentro de esta actividad se debe establecer la tolerancia de riesgo, para este caso el patrocinador no va a tolerar que existan riesgos que provoquen daños a la imagen de la Alcaldía. El director de proyectos no aceptará ni solicitará cambios incontrolados.

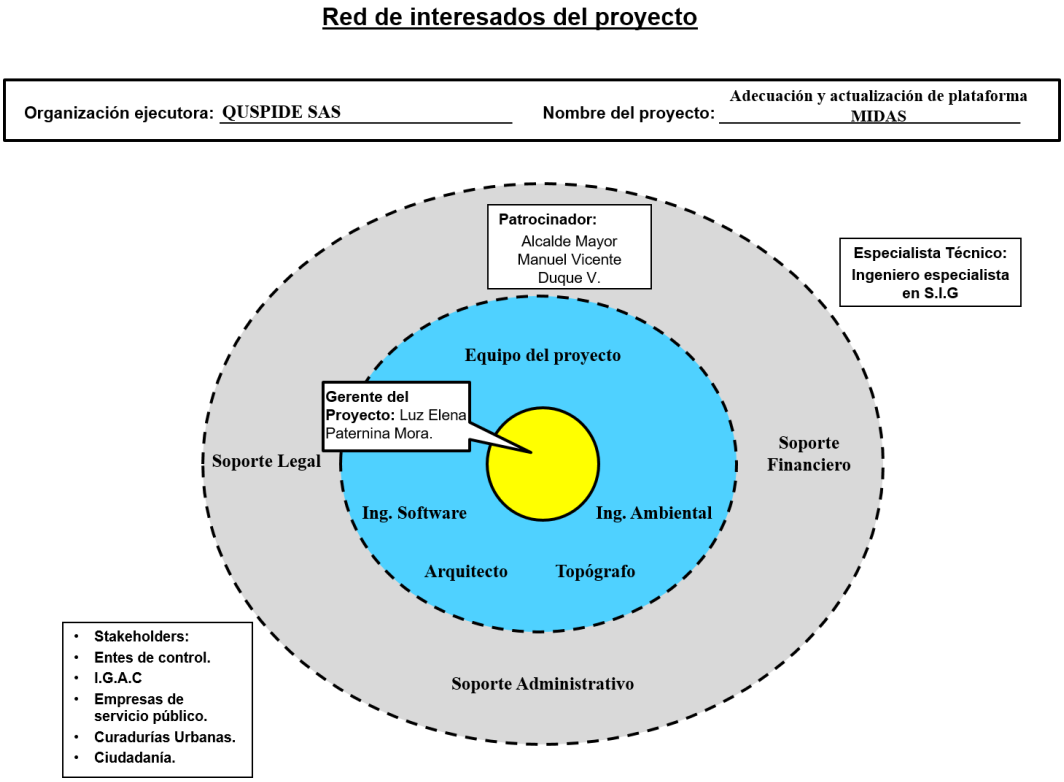


Figura 22. Red de interesados del proyecto MIDAS.

Fuente: Elaboración propia.

4.3.2. IDENTIFICAR LOS RIESGOS

Para el proceso identificar riesgos se utilizará el checklist, con el cual se establece lo siguiente:

ID RIESGO	TITULO	DESCRIPCIÓN	CATEGORÍA	CAUSA DEL RIESGO	CONSECUENCIAS	TÉCNICA DE IDENTIFICACIÓN
R01	Abandono del proyecto por parte del personal contratado	El equipo contratado desiste/renuncia a desarrollar el proyecto	Personal Contratado	Mala comunicación entre la organización ejecutora y el grupo de dirección del proyecto	Cancelación del proyecto	Checklist
R02	Afectación de la plataforma tecnológica, de canales, servidores y correo electrónico	Interrupciones que afectan la funcionalidad de canales, servidores , y correo electrónico de forma parcial	Ambiente/Infraestructura	Indisponibilidad de los: Canales (WAN, LAN), Servidores y correo electrónico	Afectación de la operación de los procesos de la entidad que se soportan en infraestructura tecnológica, por indisponibilidad de canales, servidores y correo electrónico	Checklist
R03	Apagones	Pérdida de electricidad a corto o largo plazo	Fuerzas Mayores	Fallos en una estación eléctrica, daños en las líneas de transmisión, subestaciones u otras partes del sistema de distribución, un cortocircuito o una sobrecarga de la alimentación eléctrica	Afectación de la operación de los procesos de la entidad que se soportan en infraestructura tecnológica	Checklist

R04	Ataque Informático	Ataque que tiene como objetivo infringir daños o problemas a una aplicación o el canal de transmisión o a la red informática	Ambiente/Infraestructura	Cantidad masiva de peticiones al servicio desde una misma máquina o dirección IP, consumiendo así los recursos que ofrece el servicio hasta que llega un momento en que no tiene capacidad de respuesta y comienza a rechazar peticiones	Afectación de la operación de plataformas web o redes llegando a inhabilitarlas, eliminación de información guardada, infección de archivos	Checklist
R05	Bajo rendimiento y eficiencia en el equipo de trabajo	Situación que afectan la productividad de los empleados	Personal	Mala condiciones laborales como lo es el clima organizacional, espacios y herramientas de trabajo no adecuados	Demoras en el desarrollo de actividades, mayor posibilidad de cometer errores	Checklist
R06	Cambio de estándares técnicos	Cambio del estándar o metodología que rige el desarrollo de una actividad	Normativo/Gobierno	Actualización de estándar	Demoras en el desarrollo de actividades, al tener que adaptase a la nueva actualización	Checklist

R07	Cambio en la normatividad	Cambio de norma que regulan la adquisición, uso, distribución de un elemento	Normativo/Gobierno	Cambio de gobierno	Demoras en el desarrollo de actividades, al tener que estudiar y cumplir la nueva norma	Checklist
R08	Capacitación superficial a usuarios finales	No se brinda la capacitación a actores cuyo rol es importante en la actualización de la plataforma	Usuarios finales	Falencias en la identificación de los diversos actores y/o interesados del proyecto	Plataforma desactualizada y/o sin uso	Checklist
R09	Conflicto en el equipo de trabajo	Situación en que una parte de los miembros de un grupo adopta una postura significativamente distinta al resto de los miembros, disminuyendo o anulando la cohesión del grupo	Personal	Diferencia de valores o cultura, de objetivos, de roles, de criterios, Problemas personales	Bajo rendimiento y eficiencia en el equipo de trabajo	Checklist
R10	Congestión en la red	Fenómeno por el cual la red no da cobertura o no responde a la cantidad de equipos que demandan el servicio	Ambiente/Infraestructura	Cuando a la red (o a parte de ella) se le ofrece más tráfico del que puede cursar, demasiados dispositivos móviles usando	Nodos incapaces de procesar toda la información que le llega, con lo que haría que se saturen las colas y se quede sin servicio.	Checklist

				la red por lo cual la saturan		
R11	Desarrollo de una interfaz de usuario inadecuada	Interfaces con diseños obsoletos o no prácticos	Diseño e Implementación	No validación con grupo focales de posibles diseños para las interfaces	Se debe rediseñar las interfaces generando demoras en los tiempos	Checklist
R12	El cliente no acepta el software entregado, incluso aunque cumpla todas sus especificaciones	El cliente no valida el producto	Cliente	El cliente insiste en nuevos requisitos y/o requerimientos	Demanda, cancelación del contrato	Checklist
R13	El cliente no participa en los ciclos de revisión de los planes, prototipos y especificaciones, o es incapaz de hacerlo	Nula involucración del cliente en el proyecto	Cliente	Falta de conocimiento y/o interés por la naturaleza del proyecto	No validación de los productos, nuevos requerimientos y/o diseños	Checklist
R14	El cliente y/o usuario final insiste en nuevos requisitos	Solicitud de nuevos requerimientos y/o requisitos no establecidos en el contrato	Cliente	No involucramiento del cliente en el proyecto	Conflictos entre entidad ejecutora y cliente generando demoras o cancelación del contrato	Checklist
R15	Falla en la UPS	Pérdida repentina del suministro de alimentación	Ambiente/Infraestructura	Fin de la vida útil del dispositivo	Afectación de la operación de plataformas web o redes	Checklist

R16	Falla en sistemas operativo	Anomalías y fallos en el sistema principal	Ambiente/Infraestructura	Caídas de sistemas en entornos de comunicaciones	Plataformas o dispositivos inhabilitados	Checklist
R17	Falta de documentación en el código fuente	Poca o nula ausencia de documentación de las líneas de código del software	Diseño e Implementación	No se especifica en la contratación la documentación del código	Falta de conocimiento en el funcionamiento interno de un software ya que el código no es legible	Checklist
R18	Hacking	Son aquellas personas que consiguen acceder a los datos o programas de los cuales no tienen acceso permitido	Ambiente/Infraestructura	Bajos niveles de ciberseguridad	Robo de información, pérdida de credibilidad de la entidad	Revisión histórica de proyectos similares
R19	Incendio	Ocurrencia de fuego no controlado que puede afectar un espacio	Ambiente/Infraestructura	Cortocircuitos debidos a cables gastados, tomas de corrientes defectuosas, etc.	Daños en equipos generando la no operación de plataformas, redes, etc.	Checklist
R20	Interrupción del servicio de internet	Suspensión del servicio de internet	Ambiente/Infraestructura	Falla en el suministro eléctrico o el no pago del servicio al ISP	Afectación de la operación de plataformas web o redes	Observación directa
R21	Inundación	Ocupación por parte del agua de zonas que habitualmente	Ambiente/Infraestructura	Fuertes lluvias en la zona	Equipos averiados por haberse mojado, Daños a otros elementos del datacenter originando la	Observación directa

		están libres de esta			no operación de plataformas y otras redes	
R22	La contratación tarda más de lo esperado	Proceso de contratación fuera de los términos establecidos y/o planificados	Organización y Gestión	No divulgación de los procesos de mínima cuantía o la no presentación de proponentes a la convocatoria	Demora en adjudicación del contrato o cancelación del proyecto	Checklist
R23	Las definiciones de la planificación, de los recursos y del producto han sido impuestas por el cliente o un directivo superior, y no están equilibradas	El cliente es el que establece la fecha de entrega del proyecto/producto sin tener en cuenta la opinión y/o experiencia de un experto	Cliente	Falta de conocimiento y/o interés por la naturaleza del proyecto	Producto con falencias	Checklist
R24	Las herramientas de desarrollo no funcionan como se esperaba	Software con productividad y calidad baja	Diseño e Implementación	Uso de lenguajes de programación, frameworks desactualizados u obsoletos	Producto con falencias el cual no se utilizará	Revisión histórica de proyectos similares
R25	No existe contrato de mantenimiento	Ni el cliente ni la ejecutora establecen mantenimiento de tipo correctivo y preventivo	Organización y Gestión	No se especifica en la contratación	Desactualización muy rápida de la plataforma y/o posibles errores que no se sabrán solucionar	Revisión histórica de proyectos similares

R26	Pérdida de backups	Pérdida de las copias de seguridad generadas por la plataforma	Diseño e Implementación	Error en el código fuente	Pérdida de información de respaldo	Checklist
R27	Poco espacio en el servidor	El servidor donde se alojará la plataforma no cuenta son el suficiente espacio	Ambiente/Infraestructura	Gran volumen de información alojada en el servidor	Adquirir un servicio de hosting y dominio lo cual eleva los costos del proyecto	Checklist
R28	Recursos específicos no disponible	No se cuenta con el recurso humano o equipos necesarios para el desarrollo del proyecto	Ambiente/Infraestructura	No identificación de los recursos	Sobrecostos generados por la adquisición de los recursos	Checklist

4.3.3. ANALIZAR LOS RIESGOS

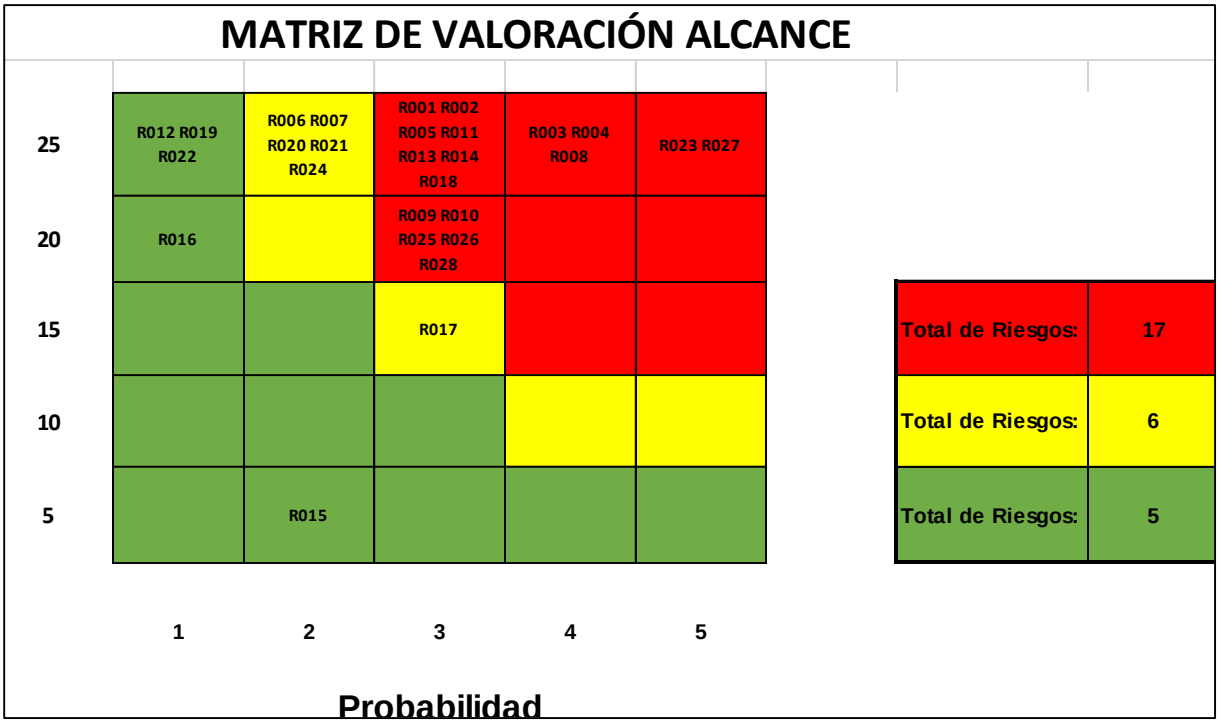
Como se explicó anteriormente, en este proceso se realiza la medición por probabilidad e impacto, obteniendo lo siguiente:

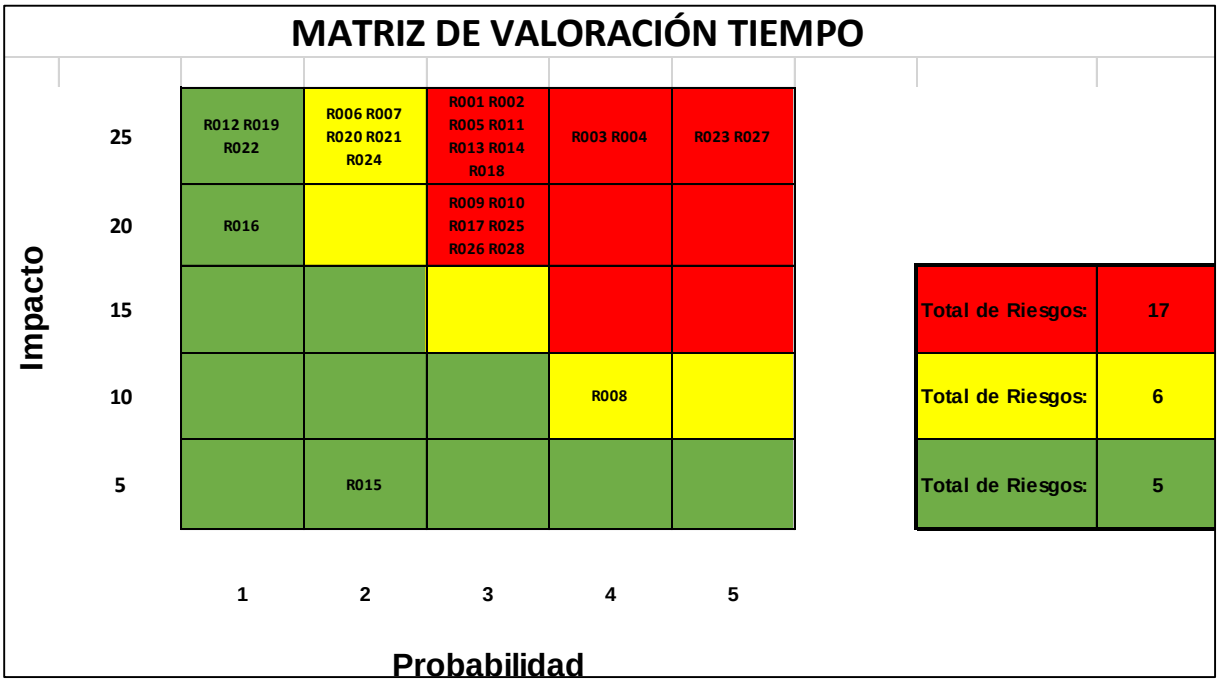
RIESGOS	ANÁLISIS DE RIESGOS									
		ALCANCE		TIEMPO		COSTO		CALIDAD		NIVEL DE RIESGO TOTAL
TITULO	ESTIMACIÓN DE PROBABILIDAD	ESTIMACIÓN DE IMPACTO	NIVEL DE RIESGO	ESTIMACIÓN DE IMPACTO	NIVEL DE RIESGO	ESTIMACIÓN DE IMPACTO	NIVEL DE RIESGO	ESTIMACIÓN DE IMPACTO	NIVEL DE RIESGO	
Abandono del proyecto por parte del personal contratado	3	25	75	25	75	25	75	25	75	300
Afectación de la plataforma tecnológica, de canales, servidores y correo electrónico	3	25	75	25	75	10	30	20	60	240

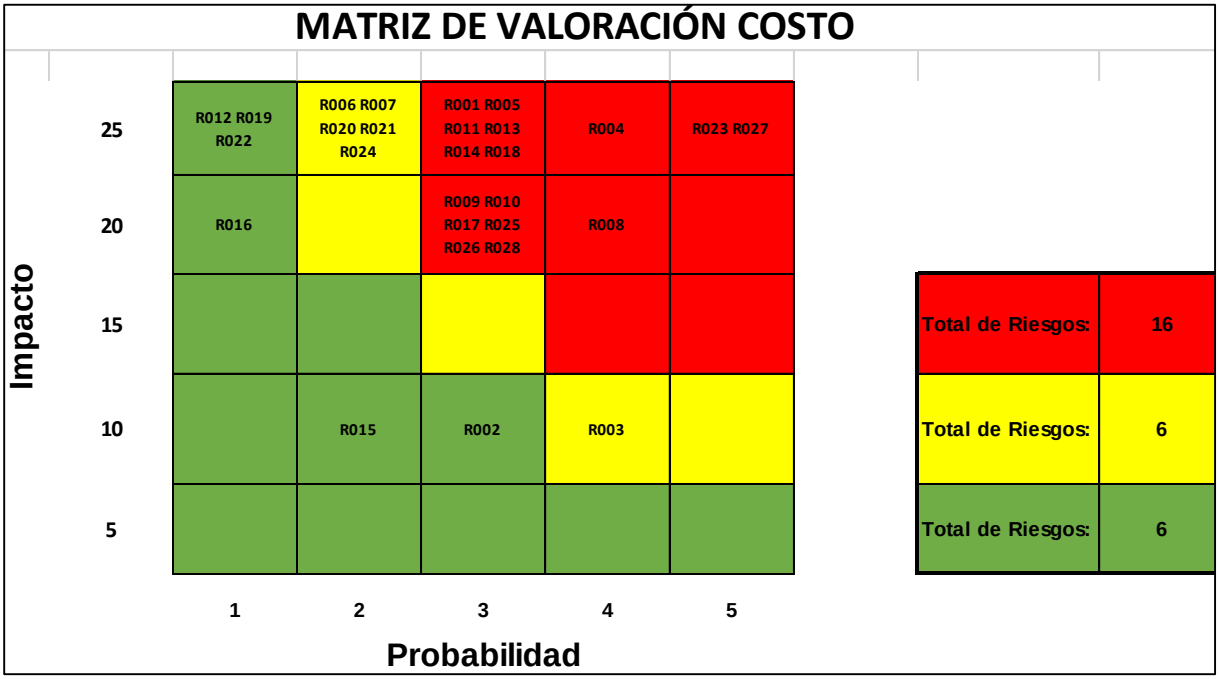
Apagones	4	25	100	25	100	10	40	25	100	340
Ataque Informático	4	25	100	25	100	25	100	25	100	400
Bajo rendimiento y eficiencia en el equipo de trabajo	3	25	75	25	75	25	75	25	75	300
Cambio de estándares técnicos	2	25	50	25	50	25	50	25	50	200

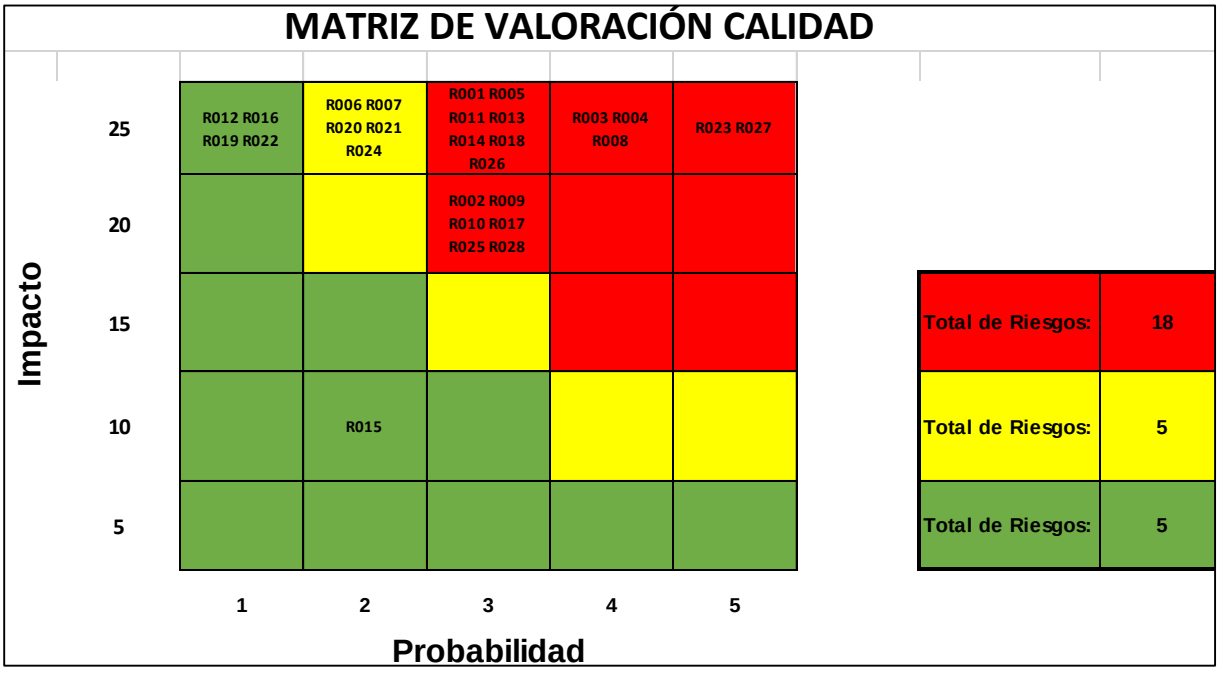
Cambio en la normatividad	2	25	50	25	50	25	50	25	50	200
Capacitación superficial a usuarios finales	4	25	100	10	40	20	80	25	100	320
Conflicto en el equipo de trabajo	3	20	60	20	60	20	60	20	60	240
Congestión en la red	3	20	60	20	60	20	60	20	60	240
Desarrollo de una interfaz de usuario inadecuada	3	25	75	25	75	25	75	25	75	300
El cliente no acepta el software entregado, incluso aunque cumpla todas sus especificaciones	1	25	25	25	25	25	25	25	25	100
El cliente no participa en los ciclos de revisión de los planes, prototipos y especificaciones, o es incapaz de hacerlo	3	25	75	25	75	25	75	25	75	300
El cliente y/o usuario final insiste en nuevos requisitos	3	25	75	25	75	25	75	25	75	300
Falla en la UPS	2	5	10	5	10	10	20	10	20	60
Falla en sistemas operativo	1	20	20	20	20	20	20	25	25	85
Falta de documentación en el código fuente	3	15	45	20	60	20	60	20	60	225
Hacking	3	25	75	25	75	25	75	25	75	300

Incendio	1	25	25	25	25	25	25	25	25	100
Interrupción del servicio de internet	2	25	50	25	50	25	50	25	50	200
Inundación	2	25	50	25	50	25	50	25	50	200
La contratación tarda más de lo esperado	1	25	25	25	25	25	25	25	25	100
Las definiciones de la planificación, de los recursos y del producto han sido impuestas por el cliente o un directivo superior, y no están equilibradas	5	25	125	25	125	25	125	25	125	500
Las herramientas de desarrollo no funcionan como se esperaba	2	25	50	25	50	25	50	25	50	200
No existe contrato de mantenimiento	3	20	60	20	60	20	60	20	60	240
Pérdida de backups	3	20	60	20	60	20	60	25	75	255
Poco espacio en el servidor	5	25	125	25	125	25	125	25	125	500
Recursos específicos no disponible	3	20	60	20	60	20	60	20	60	240


MATRIZ DE VALORACIÓN ALCANCE
25
20
15
10
5
R012 R019 R022
R006 R007 R020 R021 R024
R001 R002 R005 R011 R013 R014 R018
R003 R004 R008
R023 R027
R016
R009 R010 R025 R026 R028
R017
R015
1
2
3
4
5
Probabilidad
Total de Riesgos: 17
Total de Riesgos: 6
Total de Riesgos: 5


MATRIZ DE VALORACIÓN TIEMPO
Impacto
25
20
15
10
5
R012 R019 R022
R006 R007 R020 R021 R024
R001 R002 R005 R011 R013 R014 R018
R003 R004
R023 R027
R016
R009 R010 R017 R025 R026 R028
R008
R015
1
2
3
4
5
Probabilidad
Total de Riesgos: 17
Total de Riesgos: 6
Total de Riesgos: 5


MATRIZ DE VALORACIÓN COSTO
Impacto
25
20
15
10
5
R012 R019 R022
R006 R007 R020 R021 R024
R001 R005 R011 R013 R014 R018
R004
R023 R027
R016
R009 R010 R017 R025 R026 R028
R008
R015
R002
R003
1
2
3
4
5
Probabilidad
Total de Riesgos: 16
Total de Riesgos: 6
Total de Riesgos: 6


MATRIZ DE VALORACIÓN CALIDAD
Impacto
25
20
15
10
5
R012 R016 R019 R022
R006 R007 R020 R021 R024
R001 R005 R011 R013 R014 R018 R026
R003 R004 R008
R023 R027
R002 R009 R010 R017 R025 R028
R015
1
2
3
4
5
Probabilidad
Total de Riesgos: 18
Total de Riesgos: 5
Total de Riesgos: 5

Para realizar la priorización de los riesgos, se tomará como los más urgentes aquellos riesgos en zona crítica, es decir la zona de color rojo. Esto equivale a riesgos cuyo nivel superan los 50:

- ✓ **Priorizados por alcance:** R1, R2, R3, R4, R5, R8, R9, R10, R11, R13, R14, R18, R23, R25, R26, R27, R28.
- ✓ **Priorizados por tiempo:** R1, R2, R3, R4, R5, R9, R10, R11, R13, R14, R17, R18, R23, R25, R26, R27, R28.
- ✓ **Priorizados por costo:** R1, R4, R5, R8, R9, R10, R11, R13, R14, R17, R18, R23, R25, R26, R27, R28.
- ✓ **Priorizados por calidad:** R1, R2, R3, R4, R5, R8, R9, R10, R11, R13, R14, R17, R18, R23, R25, R26, R27, R28.

La salida de este proceso es el registro actualizado de riesgos y dos listados, una de riesgos a supervisar y la de riesgos a tratar; esta última lista está conformada por la unión de los riesgos priorizados por alcance, tiempo, costo y calidad, en este caso la lista de riesgos de calidad abarca las lista de alcance, tiempo y costo, dando como resultado final:

- ✓ **Lista de riesgos a tratar:** R1, R2, R3, R4, R5, R8, R9, R10, R11, R13, R14, R17, R18, R23, R25, R26, R27, R28.
- ✓ **Lista de riesgos a supervisar:** R6, R7, R12, R15, R16, R19, R20, R21, R22, R24.

La lista de riesgos a tratar es la entrada del siguiente proceso que es tratar los riesgos, y la lista de riesgos a supervisar entrar al Backlog enfocado a riesgos.

4.3.4. TRATAR LOS RIESGOS

ID	TITULO	DESCRIPCIÓN	CATEGORÍA	CAUSA DEL RIESGO	CONSECUENCIAS	TÉCNICA DE IDENTIFICACIÓN	NIVEL DE RIESGO TOTAL	ESTRATEGIA DE RTA	PLAN DE ACCIÓN	RESPONSABLE	ESTADO
R01	Abandono del proyecto por parte del personal contratado	El equipo contratado desiste/renuncia a desarrollar el proyecto	Personal Contratado	Mala comunicación entre la organización ejecutora y el grupo de dirección del proyecto	Cancelación del proyecto	Checklist	300	Mitigar	Acudir a un espacio de arbitraje para llegar a un acuerdo	Director de proyecto	Mitigado
R02	Afectación de la plataforma tecnológica, de canales, servidores y correo electrónico	Interrupciones que afectan la funcionalidad de canales, servidores , y correo electrónico de forma parcial	Ambiente/Infraestructura	Indisponibilidad de los: Canales (WAN, LAN), Servidores y correo electrónico	Afectación de la operación de los procesos de la entidad que se soportan en infraestructura tecnológica, por indisponibilidad de canales, servidores y correo electrónico	Checklist	240	Mitigar	Implementar mecanismos de seguimiento a la disponibilidad de los servicios que componen la plataforma tecnológica de canales de red, servidores y correo	Director de riesgos	Latente
R03	Apagones	Pérdida de electricidad a corto o largo plazo	Fuerzas Mayores	Fallos en una estación eléctrica, daños en las líneas de transmisión, subestaciones u otras partes del sistema de	Afectación de la operación de los procesos de la entidad que se soportan en infraestructura tecnológica	Checklist	340	Mitigar	Uso de plantas de energía para mantener la disponibilidad del servicio	Director de proyecto	Mitigado

				distribución, un cortocircuito o una sobrecarga de la alimentación eléctrica							
R04	Ataque Informático	Ataque que tiene como objetivo infringir daños o problemas a una aplicación o el canal de transmisión o a la red informática	Ambiente/Infraestructura	Cantidad masiva de peticiones al servicio desde una misma máquina o dirección IP, consumiendo así los recursos que ofrece el servicio hasta que llega un momento en que no tiene capacidad de respuesta y comienza a rechazar peticiones	Afectación de la operación de plataformas web o redes llegando a inhabilitarlas, eliminación de información guardada, archivos infectados	Checklist	400	Evitar	Implementar sistemas de autenticación y verificación al momento de que un usuario realice la solicitud, y mantener actualizado el firewall y antivirus	Director de riesgos	Evitado
R05	Bajo rendimiento y eficiencia en el equipo de trabajo	Situación que afectan la productividad de los empleados	Personal	Mala condiciones laborales como lo es el clima organizacional, espacios y herramientas de trabajo no adecuados	Demoras en el desarrollo de actividades, mayor posibilidad de cometer errores	Checklist	300	Mitigar	Generar talleres de coaching para mejorar las relaciones del equipo de trabajo	Director de proyecto	Mitigado
R08	Capacitación superficial a usuarios finales	No se brinda la capacitación a actores cuyo rol es importante en la actualización de la plataforma	Usuarios finales	Falencias en la identificación de los diversos actores y/o interesados del proyecto	Plataforma desactualizada y/o sin uso	Checklist	320	Evitar	Establecer sesiones de capacitación a todos los interesados y usuarios finales del producto y publicar en	Director de proyecto	Evitado

									sitio web y/o redes sociales tips o video tutorial para la utilización del producto		
R09	Conflicto en el equipo de trabajo	Situación en que una parte de los miembros de un grupo adopta una postura significativamente distinta al resto de los miembros, disminuyendo o anulando la cohesión del grupo	Personal	Diferencia de valores o cultura, de objetivos, de roles, de criterios, Problemas personales	Bajo rendimiento y eficiencia en el equipo de trabajo	Checklist	240	Mitigar	Generar talleres de coaching para mejorar las relaciones del equipo de trabajo	Director de proyecto	Mitigado
R10	Congestión en la red	Fenómeno por el cual la red no da cobertura o no responde a la cantidad de equipos que demandan el servicio	Ambiente/Infraestructura	Cuando a la red (o a parte de ella) se le ofrece más tráfico del que puede cursar, demasiados dispositivos móviles usando la red por lo cual la saturan	Nodos incapaces de procesar toda la información que le llega, con lo que haría que se saturen las colas y se quede sin servicio.	Checklist	240	Mitigar	Implementar programas sniffer para realizar el monitoreo y control de las redes	Director de riesgos	Mitigado
R11	Desarrollo de una interfaz de usuario inadecuada	Interfaces con diseños obsoletos o no prácticos	Diseño e Implementación	No validación con grupo focales de posibles diseños para las interfaces	Se debe rediseñar las interfaces generando demoras en los tiempos	Checklist	300	Evitar	Desarrollar diagramas de UML como documento anexo a los pliegos para que el contratista tenga una base para el diseño de interfaces	Director de riesgos	Evitado

R13	El cliente no participa en los ciclos de revisión de los planes, prototipos y especificaciones, o es incapaz de hacerlo	Nula involucración del cliente en el proyecto	Cliente	Falta de conocimiento y/o interés por la naturaleza del proyecto	No validación de los productos, nuevos requerimientos y/o diseños	Checklist	300	Evitar	Disponer de un enlace entre el cliente y la organización ejecutora que tenga la experiencia y participe en el desarrollo del proyecto	Director de riesgos	Evitado
R14	El cliente y/o usuario final insiste en nuevos requisitos	Solicitud de nuevos requerimientos y/o requisitos no establecidos en el contrato	Cliente	No involucramiento del cliente en el proyecto	Conflictos entre entidad ejecutora y cliente generando demoras o cancelación del contrato	Checklist	300	Evitar	Establecer dentro de los estudios previos todos los requisitos y un número máximo de solicitudes de cambio para poder implementar nuevos requisitos	Director de proyecto	Evitado
R17	Falta de documentación en el código fuente	Poca o nula ausencia de documentación de las líneas de código del software	Diseño e Implementación	No se especifica en la contratación la documentación del código	Falta de conocimiento en el funcionamiento interno de un software ya que el código no es legible	Checklist	225	Evitar	Establecer dentro de los estudios previos como condición para la aceptación del producto manuales de usuario y la documentación interna dentro del código fuente	Director de proyecto	Evitado

R18	Hacking	Son aquellas personas que consiguen acceder a los datos o programas de los cuales no tienen acceso permitido	Ambiente/Infraestructura	Bajos niveles de ciberseguridad	Robo de información, pérdida de credibilidad de la entidad	Revisión histórica de proyectos similares	300	Mitigar	Implementar antivirus licenciados, firewall y configuración de protección en los dispositivos de red	Director de riesgos	Mitigado
R23	Las definiciones de la planificación, de los recursos y del producto han sido impuestas por el cliente o un directivo superior, y no están equilibradas	El cliente es el que establece la fecha de entrega del proyecto/producto sin tener en cuenta la opinión y/o experiencia de un experto	Cliente	Falta de conocimiento y/o interés por la naturaleza del proyecto	Producto con falencias	Checklist	500	Mitigar	Establecer junto al contratista cronogramas reales teniendo en cuenta la naturaleza del proyecto	Director de riesgos	Mitigado
R25	No existe contrato de mantenimiento	Ni el cliente ni la ejecutora establecen mantenimiento de tipo correctivo y preventivo	Organización y Gestión	No se especifica en la contratación	Desactualización muy rápida de la plataforma y/o posibles errores que no se sabrán solucionar	Revisión histórica de proyectos similares	240	Evitar	Establecer dentro de los estudios previos como condición para la aceptación del producto un número de mantenimientos dentro de cierto periodo de tiempo	Director de proyecto	Evitado
R26	Pérdida de backups	Pérdida de las copias de seguridad generadas por la plataforma	Diseño e Implementación	Error en el código fuente	Pérdida de información de respaldo	Checklist	255	Transferir	Implementar servidores espejos que almacenen las copias de seguridad y configurarlo	Director de riesgos	Transferido

									s para que sean enviados a un correo institucional		
R27	Poco espacio en el servidor	El servidor donde se alojará la plataforma no cuenta son el suficiente espacio	Ambiente/Infraestructura	Gran volumen de información alojada en el servidor	Adquirir un servicio de hosting y dominio lo cual eleva los costos del proyecto	Checklist	500	Transferir	Adquirir servicio de hosting por periodos de tiempo para el funcionamiento de la plataforma, mientras se adecúa el servidor principal	Director de proyecto	Transferido
R28	Recursos específicos no disponible	No se cuenta con el recurso humano o equipos necesarios para el desarrollo del proyecto	Ambiente/Infraestructura	No identificación de los recursos	Sobrecostos generados por la adquisición de los recursos	Checklist	240	Mitigar	Realizar inspecciones para identificar la disponibilidad de los recursos	Director de proyecto	Mitigado

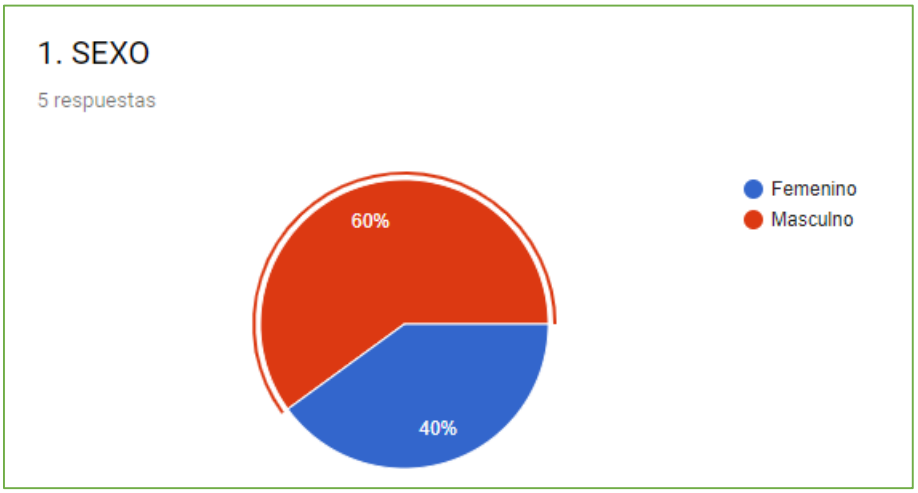
4.3.5. VALIDACIÓN DEL MODELO

Para la validación del modelo se realizó una revisión por parte de expertos (profesionales TI), con el siguiente perfil:

EXPERTO	PERFIL
E1	Ingeniero de sistemas, magister en educación virtual y redes sociales. Asesora TIC de la Secretaría de Educación (Alcaldía de Cartagena) con amplia experiencia en manejo de plataformas virtuales de aprendizaje.
E2	Doctor en Ingeniería de Software y Especialista en Gerencia de Sistemas de Información, con experiencia en la aplicación de técnicas de Inteligencia de Negocios, Minería de Datos y Planificación Estratégica Informática en las organizaciones.
E3	Ingeniera de Sistemas, Especialista en Informática para la educación en Red. Docente en Instituciones de Educación Superior, experiencia en la construcción de proyectos educativos institucionales en TIC, Configuración, administración y montaje de OVAs en LMS; Desarrollo de OVAs en varias herramientas.
E4	Ingeniero de Sistemas, especialista en Sistemas de telecomunicaciones.

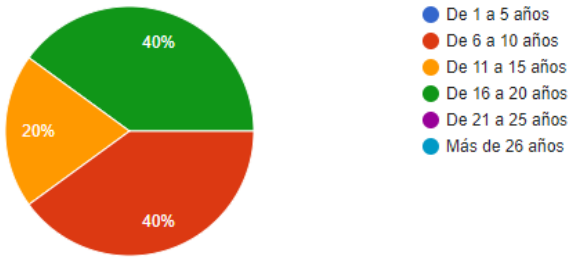
E5	Ingeniero de sistemas, especialista en auditoria informática, asesor externo en Alcaldía Mayor de Cartagena y Gobernación de Bolívar.

Los expertos tuvieron la oportunidad de revisar el expediente original del proyecto MIDAS, revisar lo propuesto en el modelo y los resultados obtenidos, seguido a esto se aplicó una encuesta donde se obtuvo los siguientes resultados:



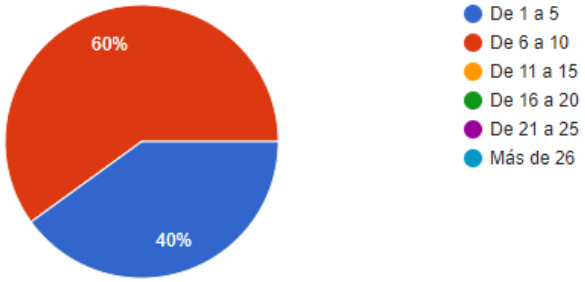
3. ¿Cuántos años de experiencia tiene en proyectos de naturaleza TI?

5 respuestas



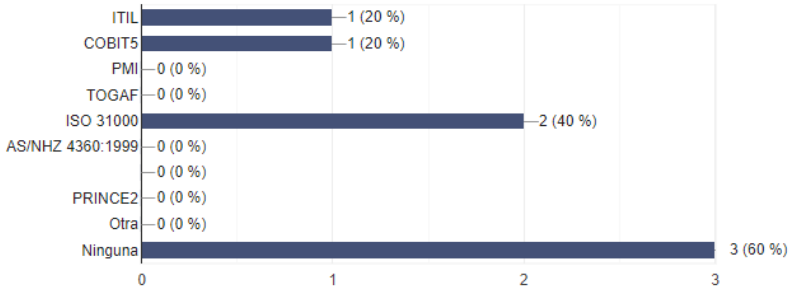
5. ¿Cuántos proyectos TI implementa al año?

5 respuestas



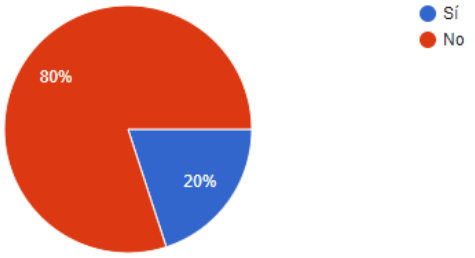
6. ¿Con cuál o cuáles marcos, normativa, estándar ha trabajado?

5 respuestas



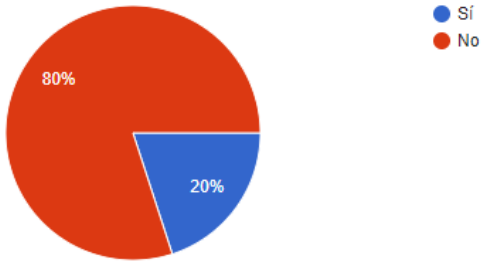
7. En su grupo de trabajo se utiliza alguna herramienta para la gestión de riesgos

5 respuestas



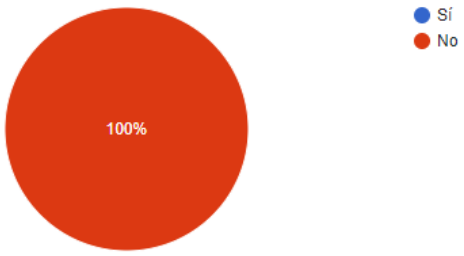
8. En sus proyectos tiene disponible información de riesgos de proyectos pasados de la organización, cómo listas, buenas prácticas, estadísticas, etc.

5 respuestas



9. Al acabar un proyecto, se lleva a cabo algún informe del desarrollo donde puedan indicarse problemas aparecidos y su impacto, o cómo se combatieron.

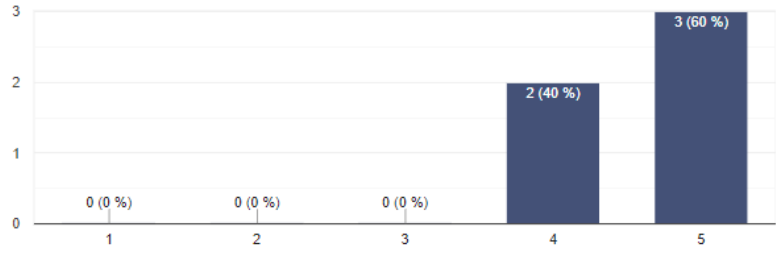
5 respuestas



Las preguntas de la 10 a la 12 constan de una escala del 1 al 5, con la siguiente equivalencia: 1. Completamente en desacuerdo 2. En desacuerdo 3. Neutral 4. De acuerdo 5. Completamente de acuerdo

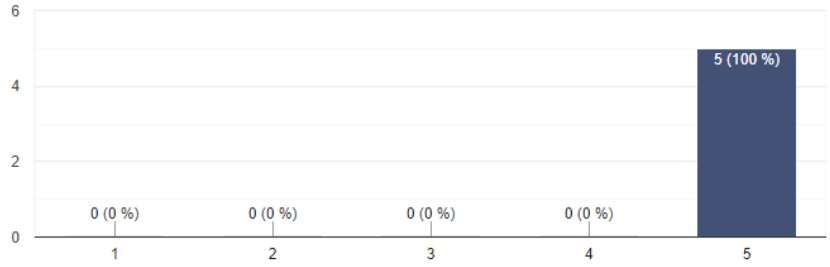
10. Al comparar el expediente del proyecto MIDAS con los resultados arrojados por el modelo propuesto, considera usted si ¿el modelo identifica los aspectos más relevantes del proyecto que pueda influenciar los objetivos de este?

5 respuestas



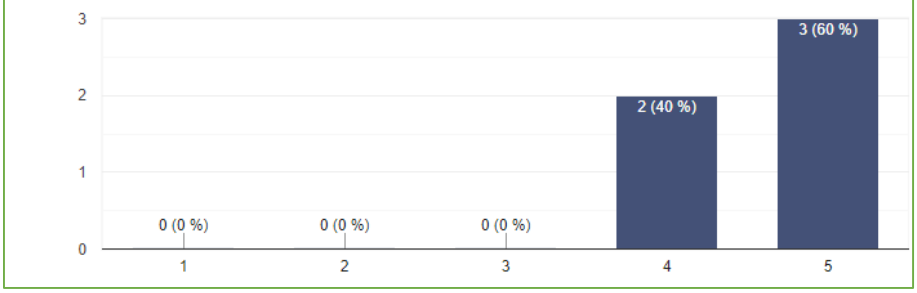
11. Al analizar y evaluar el modelo propuesto, considera usted que con el modelo se realiza una identificación, análisis y gestión de riesgos de forma eficiente

5 respuestas



12. De acuerdo a su experiencia, ¿sería útil implementar el modelo propuesto para gestionar riesgos en proyectos TI?

5 respuestas



¿Qué valoración y/o recomendaciones le da al modelo propuesto?

5 respuestas

Me parece una buena herramienta, ya que actualmente en la Alcaldía no disponemos de este tipo de recursos que permitan gestionar los incidentes y/o riesgos en los proyectos tic de las diferentes dependencias.
Tener en cuenta indicadores claves de riesgos y una estrategia de comunicación interna en el grupo de trabajo.
Considero que es un instrumento interesante, en mi experiencia trabajando en el sector público en proyectos de tecnologías no llevamos una adecuada gestión de riesgos lo cual se vería impactado de forma positiva al implementar dicho instrumento.
Se recomienda socializar con las demas dependencias el modelo propuesto para su implementacion en toda la Administracion distrital.
me gustaria que para proximos estudios se tenga en cuenta proyectos de la Gobernacion de Bolivar.

5. CONCLUSIONES

De acuerdo con los resultados obtenidos en el desarrollo de la investigación, se concluye que:

- La Alcaldía de Cartagena no realiza una eficiente gestión de los riesgos al implementar una matriz genérica en todos sus proyectos, y no tener en cuenta la naturaleza de dichos proyectos.
- Mediante la revisión de los antecedentes bibliográficos en libros y artículos de investigación de los principales investigadores se logró identificar una lista de riesgos la cual será utilizada como un "checklist" y facilitará el proceso de identificación de riesgos definido en el modelo de gestión de riesgos propuesto, de igual forma se identificó que no hay muchas investigaciones de fondo en temáticas de riesgos en este tipo de proyectos.
- Se evidencia que la Alcaldía no realiza identificación de Stakeholders, ni un involucramiento de ellos en el desarrollo del proyecto; sabiendo que la gestión de riesgos debe tratarse como un esfuerzo de equipo y, para ser eficaz, requiere una interacción regular entre las distintas partes de la organización. Por tal motivo, dentro del proceso de preparar la gestión de los riesgos del modelo propuesto, como actividad principal se realiza la identificación de Stakeholders tanto externos como internos que tendrán lugar dentro del proyecto.
- Al realizar la priorización de riesgos teniendo en cuenta su impacto en el alcance, costo, tiempo y calidad se podrá desarrollar planes de respuesta claros, actualizados y efectivos, que permitan el control y un adecuado manejo de esos riesgos para reducir la probabilidad y/o impacto de ocurrencia.
- Se evidencia que la Alcaldía no realiza una identificación de riesgos de forma eficiente, al imponer la matriz de riesgos (detallada en la sección 3.2) dejan por sentado todos los riesgos de un proyecto; y en casos como lo fue el Proyecto MIDAS, se pudieron identificar con la implementación del modelo un total de 28 riesgos; de los cuales 14 impactan de forma crítica al proyecto en sus variables de Alcance, Tiempo, Costo y Calidad, estos fueron los riesgos R001, R004, R005, R009, R010, R011, R013, R014, R018, R023, R025, R026, R027 y R028, aparte de éstos el riesgo R017 tiene un impacto crítico sobre las

variables de Tiempo, Costo y Alcance, y los riesgos R002, R003 y R008 tienen el mismo impacto sobre las variables Alcance, Costo y Calidad; para un total de 18 riesgos críticos a tratar dentro del proyecto y 10 riesgos a supervisar (R6, R7, R12, R15, R16, R19, R20, R21, R22, R24) correspondientes a bajos y moderados.

- La Alcaldía de Cartagena impone las definiciones de la planificación, de los recursos y del producto lo que lo convierte en un riesgo de gran impacto, y este tiende a ser casi seguro que ocurra debido a que los equipos de proyectos de entidades públicas constantemente están bajo presión para cumplir con los resultados del proyecto, en consecuencia rara vez tienen tiempo para invertir en actividades adicionales que carecen a su juicio de valor inmediato (Paranagamage, Carrillo, Ruikar, & Fuller, 2012).

6. RECOMENDACIONES Y TRABAJO FUTURO

Con el fin de sacar mejor provecho al trabajo ya realizado, se dejan bases para el inicio de futuras investigaciones asociadas al objetivo principal de la investigación:

- Realizar estudios comparativos con información reciente, explorar otro tipo de industrias para buscar nuevas ideas y nuevas aplicaciones para los servicios prestados.
- Establecer umbrales que puedan generar alertas de advertencia si se alcanza un punto de control para que se puedan tomar medidas antes de que los servicios se vean afectados.
- Implementar un proceso para facilitar la trasmisión de conocimiento, informaciones, actualizaciones, experiencias y habilidades entre los integrantes de la Alcaldía, de una manera sistemática y eficiente, asimismo organizar entrevistas y revisiones a los expedientes de los proyectos para rescatar toda la información con respecto a riesgos que sirvan de base de conocimiento y/o lecciones aprendidas para futuros proyectos.
- Comprender la estrategia de negocio y las metas establecidas del negocio para así implementar indicadores clave de riesgos (KRIs) que permitan detectar el nivel de exposición de un riesgo y tomar medidas oportunas.
- Diseñar e implementar el plan de gestión del cambio para la adopción exitosa del modelo, en el cual se incluya un plan de sensibilización y de capacitación.
- Fortalecer los conocimientos de los gerentes de los proyectos en el tema de gestión de riesgos por medio de capacitaciones y entrenamiento, para que éstos a su vez repliquen a los demás miembros de equipo de los proyectos.
- Tener en cuenta la gestión de riesgos positivos (oportunidades) para su aplicación dentro del modelo.
- Implementar dentro del Backlog orientado a riesgos herramientas que permitan llevar control en aspectos relacionados a costos y cronogramas, como lo puede ser la técnica de valor ganado y cronograma ganado.

7. BIBLIOGRAFÍA

- Anudhe, M. D., & Mathew, S. K. (2009). Risks in offshore IT outsourcing: A service provider perspective. European Management Journal, 27, 418–428.
- Association for Project Management. (2004). Guía de Análisis y Gestión de Riesgos de Proyectos. Gran Bretaña: APM Group.
- Bannerman, P. L. (2008). Risk and risk management in software projects: A reassessment. Journal of Systems and Software, 81, 2118–2133.
- Cocho, J. M. & Adam, M. R. (2003). Estudio exploratorio sobre los métodos de gestión de proyectos de alto riesgo. Primer Congreso Soporte del Conocimiento con la Tecnología, SOCOTE, Valencia, España.
- Chamoun, Y. (2002). Administración profesional de proyectos. La Guía. México D. F., México: McGraw-Hill.
- Comité de Organizaciones Patrocinantes de la Comisión Treadway (COSO). (29 de Septiembre de 2004). COSO Enterprise Risk Management – Integrated Framework.
- Dey, P. K., Kinch, J., & Ogunlana, S. O. (2007). Managing risk in software development projects: A case study. Industrial Management and Data Systems, 107(2), 284–303.
- Fletcher, S.K.; Jansma, R.M. & Murphy, M.D. Managing risk in software systems, article, July 1, 1995; Albuquerque, New Mexico. (digital.library.unt.edu/ark:/67531/metadc793951/: accessed May 5, 2018), University of North Texas Libraries, Digital Library, digital.library.unt.edu; crediting UNT Libraries Government Documents Department.
- Gasca-Hurtado, G. P., & Losada, B. M. (2013). Taxonomía de riesgos de outsourcing de software. INGENIARE - Revista Chilena De Ingeniería, 21(1), 41-53.
- Graham, R. & Englund, R. (1999). Administración de proyectos exitosos. México D.F., México: Pearson, Addison Wesley.

- Instituto Colombiano de Normas Técnicas y Certificación. [ICONTEC] (2011). Norma Técnica Colombia para la Gestión del Riesgo ISO 31000. Colombia.
- Instituto Colombiano de Normas Técnicas y Certificación. [ICONTEC] (2006). Norma Técnica Colombia para las tecnología de la información. técnicas de seguridad. sistemas de gestión de la seguridad de la información (SGSI) ISO 27001. Colombia.
- Iversen, J. H., Mathiassen, L., & Nielsen, P. A. (2004). MANAGING RISK IN SOFTWARE PROCESS IMPROVEMENT: AN ACTION RESEARCH APPROACH. MIS Quarterly, 28(3), 395-433.
- Luis Fernández Sanz, & Pedro Bernad Silva. (2014). Gestión de riesgos en proyectos de desarrollo de software en España: Estudio de la situación. Revista Facultad De Ingeniería Universidad De Antioquia, (70), 233-243.
- Marcelo, J. & Rodenes, M. (2003). Estudio exploratorio sobre los métodos de gestión de proyectos de alto riesgo. Primer Congreso Soporte del Conocimiento con la Tecnología, SOCOTE, Valencia, España.
- Marlene Lucila Guerrero Julio, & Luis Carlos Gómez Flórez. (2012). Gestión de riesgos y controles en sistemas de información: Del aprendizaje a la transformación organizacional. Estudios Gerenciales, 28(125), 87-95.
- Neves, Sandra Miranda, Da Silva, Carlos Eduardo Sanches, Salomon, Valério Antonio Pamplona, Da Silva, Aneirson Francisco, & Sotomonte, Bárbara Elizabeth Pereira. (2014). Risk management in software projects through Knowledge Management techniques: Cases in Brazilian Incubated Technology-Based Firms. International Journal of Project Management, 32(1), 125-138.
- Oficina de Comercio Gubernamental del Reino Unido. (2009). MANUAL PRINCE 2 - Metodología Gestión de Proyectos (Quinta ed.). Reino Unido.
- Project Management Insitute. (2017). Guía de los Fundamentos para la Dirección de Proyectos (Guía del PMBOK®) (Sexta ed.). Newtown Square, Pennsylvania, USA: PMI Publications.

- Vrhovec, Hovelja, Vavpotic, & Krisper. (2015). Diagnosing organizational risks in software projects: Stakeholder resistance. International Journal of Project Management, 33(6), 1262-1273.
- Verner, J. M., Evanco, W. M., & Cerpa, N. (2007). State of the practice: An exploratory analysis of schedule estimation and software project success prediction. Information and Software Technology, 49(2), 181–193.
- Zhou, L., Vasconcelos, A., & Nunes, M. (2008). Sorting decision making in risk management through an evidence-based information systems project risk checklist. Information Management and Computer Security, 16(2), 166–186.