La gestión del riesgo en proyectos de TI

Risk Management in IT Projects

Harry Aguiño Cardenas[1]
Harry.aguino00@usc.edu.co

Douglass Noé Mejía Hernández[1]
Douglass.mejia00@usc.edu.co

Edgar Alirio Restrepo Castillo[2]
Edgar.restrepo01@usc.edu.co

Universidad Santiago de Cali, Facultad de Ingeniería, Programa de Ingeniería de Sistemas (1)
Universidad Santiago de Cali, Facultad de Ingeniería, Programa de Ingeniería de Sistemas (2)

Resumen
Este artículo tiene como objetivo, realizar una revisión bibliográfica de la gestión del riesgo orientada a los proyectos de Tecnología de la Información (TI). Las compañías en la actualidad son cada vez más conscientes del gran impacto que pueden ocasionar los riesgos relacionados con TI, identificando que diferentes sectores de la economía son víctimas frecuentes de fallas y ataques sobre sus servicios internos, afectando de manera relevante su reputación y área financiera. Por medio de la gestión y el análisis exhaustivo de los riegos se busca incentivar a la comunidad corporativa a implementar en todos sus proyectos y emprendimientos, metodologías y buenas prácticas relacionadas con la gestión del riesgo como un proceso vital para todo el desarrollo de los mismos, y no solo como una etapa olvidada en las fases del proyecto, garantizando así incrementar de manera significativa la tasa de éxito en todas sus ejecuciones.

Palabras Clave: Gestión del riesgo, Gestión de proyectos, Proyectos de TI.

Abstract
The objective of this article is to carry out a bibliographic review of risk management oriented to information technology (or IT) projects. Companies today are more and more frequent of the great impact that IT-related risks can cause, identifying that different sectors of the economy are frequent victims of failures and attacks on their internal services, significantly affecting their reputation and financial area. Through the management and the exhaustive analysis of the risks, the corporate community is encouraged to implement, in all its projects and ventures, methodologies and good practices related to risk management as a vital process for all their development, and not only as a forgotten stage in the project phases, thus significantly guaranteeing the success rate in all its executions.

Keywords: Risk management, Project management, IT projects.

1. INTRODUCCIÓN

En la actualidad, las compañías están implementando de manera exponencial el tema del desarrollo de los sistemas de información en el área de TI, esto trae consigo un apoyo en los negocios, mejoramiento del procesamiento y administración de la información interna de las empresas, lo que conlleva a tener mejores posibilidades para relacionarse con clientes, proveedores y empleados, también con los tiempos de respuesta que giran en torno a las compañías y sus socios (Guerrero & Gómez, 2011).

El objetivo de este artículo está directamente relacionado con el concepto de gestión de riesgos en el entorno tecnológico de las organizaciones, donde es vital que se entienda como proceso y no como un fin último, además de tener en claro la certeza de que la gestión de riesgos implica una gestión para reducir el riesgo existente y una gestión que predice eventualidades futuras, que pueden llegar a materializarse (Corda, Viñas & Coria, 2017).

La gestión de proyectos es una actividad clave en las organizaciones que buscan implementar nuevas tecnologías e innovaciones. Identificar fallas en cada una de las actividades pueden ocasionar costos muy elevados (Vega, Garcia & Cervantes, 2018). Por ejemplo, para la mayoría de planes y proyectos en los cuales emprenden las compañías dependen de

una correcta identificación de tecnologías apropiadas para su desarrollo, lo cual es un paso muy importante a momento tomar decisiones en la fase de planeación, debido a que estas tecnologías no siempre son tan conocidas, por lo que sus utilizaciones en muchas ocasiones no logran los beneficios esperados (Hidalgo, 2004).

En la industria, se estima que solo una cuarta parte de los proyectos, en especial los de software por ser de alto riesgo, tienen un éxito total o logran completarse según lo planeado, traduciéndose en muchas pérdidas financieras, impactando de esta manera al sector público y privado por igual (Bannerman, 2008). Desde este punto de vista, las actividades tecnológicas de una organización que buscan lograr un gran proyecto, debe tener en cuenta que pueden verse alteradas por eventualidades inesperadas (riesgos), cuya aparición modifica o impide el éxito del proyecto e influye directamente en el plazo y coste de todas fases identificadas. (Hidalgo, 2004). Ese éxito dependerá en gran parte en la experiencia y las habilidades de los gerentes de riesgos y proyectos, así como las estrategias diseñadas sobre cómo se aborda el riesgo (Masso, Pino, Pardo, García & Piattini, 2020).

No poder realizar una buena gestión de estas eventualidades hacen parte de las mayores razones de fracaso en los proyectos. Según un estudio reciente realizado por el PMI, relacionado con los profesionales involucrados en la gestión de proyectos, se demuestra que la mala gestión del riesgo es un factor determinante en no poder lograr el objetivo de un proyecto; además de este motivo, existe una falta de capacidad por parte de los gerentes de proyecto y la organización para abordar los desafíos que surgen. Identificando, que al ser un proceso complejo, requiere muy buenas habilidades y experiencias para realizar de manera correcta la toma de decisiones, y de igual forma lograr descifrar la información que se utilizará, para predecir riesgos nuevos que puedan alterar el resultado del proyecto, debido que al ignorar estos eventos puede generar riesgos y costos adicionales que influyan negativamente en la comunicación y armonía de los interesados (Masso et al., 2020).

A mediados de los 80, las empresas entendieron la necesidad de incluir el riesgo dentro de sus planes de los proyectos y empezaron a desarrollar metodologías que se enfocaron en la gestión del riesgo (Hidalgo, 2004).

En las compañías existen limitaciones como el alcance, tiempo, costo y calidad, esto hace que el fracaso siempre esté presente y más cuando se habla de gestión de proyectos. Los proyectos pequeños tienen un 70% de éxito, mientras que los grandes proyectos tienen mayores restricciones y menos posibilidades de ser terminados. Para que haya éxito de la gestión de proyectos por lo general hay que basarse en comprender las barreras o inconvenientes que puede haber dentro del mismo, escoger una buena metodología para la gestión de riesgos que sea efectiva y se ajuste a las necesidades, también un liderazgo dinámico que pueda evitar tropiezos en el camino, mantener una buena actitud en los trabajadores, obtener los recursos adecuados y necesarios, cultura organizacional y que la alta gerencia tenga una mayor participación y entrega (Dandage, Mantha, Rane & Bhoola, 2018).

Se argumentan que las empresas de proyectos de software son propensas al fracaso y se mencionan dos clases de riesgo de proyectos de software que serían: riesgos comunes que se presentan en todo proyecto y riesgos específicos, si bien algunos son fáciles de identificar y lograr gestionar. Otros son más complicados de encontrar y predecir su probabilidad y/o impacto. Con esto se quiere llegar a que la gestión de riesgos en proyectos de software es importante porque ayuda a evitar desastres, el "retrabajo" y equilibrio de esfuerzo entre los implicados (Bannerman, 2008).

Por lo anterior, los autores del presente artículo, decidieron optar por hacer una revisión bibliográfica, en la que se hace énfasis inicialmente en el reconocimiento de las definiciones propuestas por algunos autores sobre proyectos, proyectos de TI y riesgos aplicados a los proyectos de TI. Posteriormente, revisar los conceptos fundamentales sobre proyectos en general, para finalmente enfocarse en una revisión de artículos orientados específicamente a proyectos de TI. Lo que permitirá a los autores y lectores de este artículo tener un panorama más amplio sobre la importancia de la Gestión de Riesgos en proyectos de TI como elemento clave dentro de las organizaciones.

2. DEFINICIONES

Aceptación de Riesgo: "decisión generada por la entidad de aceptar las consecuencias y probabilidad de un riesgo en particular, sin adelantar acciones de reducción y control" (COLCIENCIAS, 2015).

Administración de Riesgos: "proceso efectuado por la Alta Dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos" (COLCIENCIAS, 2015).

Amenazas: "situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización" (Cadena, 2020).

Gestión de Riesgos: Según Carvalho y Junior (2009), "se definen los enfoques apropiados para cada organización, para la identificación, gestión y categorización de los diversos tipos de riegos: riegos técnicos, riesgos de gestión de proyectos, riesgos de proyectos, organización y riesgos externos" (Lima, 2016).

Gestión de riesgos de software: se define como "una disciplina que tiene como objetivo identificar, abordar y eliminar elementos de riesgo antes de que se conviertan en una amenaza para un proyecto de software exitoso o se conviertan en las principales fuentes de trabajo del software" (Wan, Yahya, Mohd, Amir, Chuprat & Azmi., 2019).

Identificación de riesgos: "es un proceso para establecer el alcance de la gestión de riesgos y los objetivos del proyecto. El alcance de la gestión de riesgos debe estar alineado con los objetivos del proyecto" (Wan et al., 2019).

Interesado: "una persona o grupo de personas que pueden representar a un cliente, patrocinador, organización o público y que están involucrados activamente en el proyecto, o cuyos intereses pueden verse afectados positiva o negativamente por la ejecución o finalización del proyecto" (Gillespie, 2014).

Plan de gestión de riesgos: "Componente del plan para la dirección del proyecto, programa o portafolio que describe el modo en que las actividades de gestión de riesgos serán estructuradas y llevadas a cabo" (PROJECT MANAGEMENT INSTITUTE, 2017).

Prevención: en el contexto del ciberespacio significa "Reducir el riesgo de ocurrencia del crimen y la gravedad potencial del crimen y de eventos desordenados que pueden ocurrir, tanto en línea, como fuera de línea" (Acevedo & Satizábal, 2016).

Proyecto: "puede definirse como una tarea que debe completarse a una especificación definida dentro de un tiempo acordado y por un precio específico" (Jahn, Cook & Graham, 1998).

Proyecto de Software: Según Caper Jones, especialista en metodologías de ingeniería de software, define lo que es un proyecto como: "Una determinada implementación de software satisfaciendo un conjunto coherente de requisitos preestablecidos por los ámbitos de negocios y técnicos" (Arias, 2010).

Riesgo: "El riesgo es el impacto negativo neto debido a una vulnerabilidad considerando su probabilidad y el impacto de ocurrencia" (Acevedo & Satizábal, 2016).

Riesgo en proyectos de software: "consisten de una serie de factores o condiciones que pueden representar una amenaza grave para la finalización exitosa del proyecto. Implican cuantificar la importancia de tales riesgos, evaluar su

frecuencia y su impacto potencial en el desempeño del proyecto" (Neves, Da silva, Salomon, Da Silva & Sotomonte 2014).

Riesgos de acceso: "se enfocan en lo que es el acceso inapropiado a sistemas, datos e información. Estos riesgos suponen tanto los riesgos de segregación inapropiada de trabajo, así como los riesgos asociados con la integridad de la información de sistemas de bases de datos y los riesgos asociados a la confidencialidad de esa información" (Corda et al., 2017).

Tecnología de la Información (TI): "Sinónimo de sistemas de información; implica el uso de sistemas computarizados, hardware, software u otros recursos técnicos, lo que resulta en el soporte o la creación de un producto o servicio tangible, que beneficia al público, patrocinador u otra parte interesada" (Gillespie, 2014).

Vulnerabilidad: "la debilidad de un activo o grupo de activos que puede ser explotada por una o más amenazas" (Cadena, 2020).

3. PROYECTO

Se puede determinar que los proyectos constan de un factor de tiempo bien definido, desde su inicio hasta poder lograr el objetivo y terminarlo, aunque en muchos de los casos este tiempo no es exacto, debido al tamaño y complejidad de las variaciones y cambios que puedan sufrir los proyectos en su desarrollo (Arias, 2010).

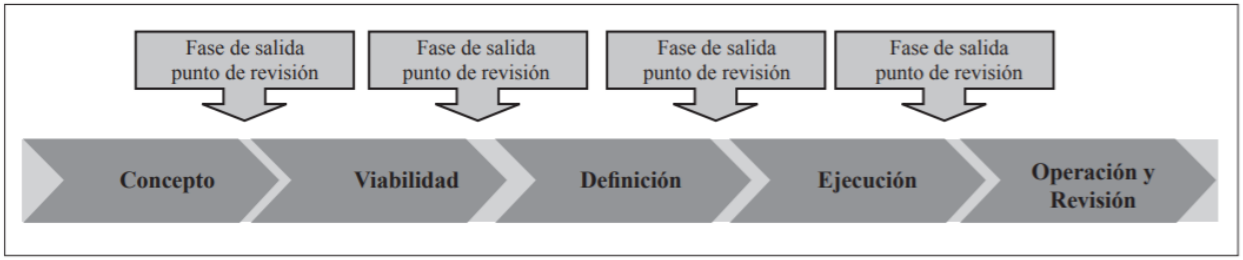
En específico, definir un proyecto de grandes magnitudes puede ser fácil, sin embargo, se requiere que muchas personas aporten diferentes habilidades, a medida que la tarea evoluciona desde la idea inicial hasta la finalización del mismo. Las grandes empresas, encuentran más manejable dividir proyectos en fases, que reflejan los requisitos de habilidades y compromiso de los recursos disponibles (Jahn et al., 1998).

Si un proyecto es viable, los recursos están disponibles y los niveles de riesgo son aceptables, se procede a continuar con el diseño inicial y estimaciones de costos, con el fin de preparar un documento con un nivel de detalle suficiente que sustente una solicitud de fondos y el apoyo de los interesados de manera total (Jahn et al., 1998).

3.1 CICLO DE VIDA DEL PROYECTO

Una gran apreciación sobre los proyectos y los emprendimientos que no lo son, es otorgada por Morris (2004) "la única cosa que distingue a los proyectos de los no proyectos es que todos los proyectos, sin importar su complejidad o trivialidad, pasan por una secuencia de desarrollo del ciclo de vida común" como se pude ver reflejado en la (figura 1) (Munz & Melissa, 2013).

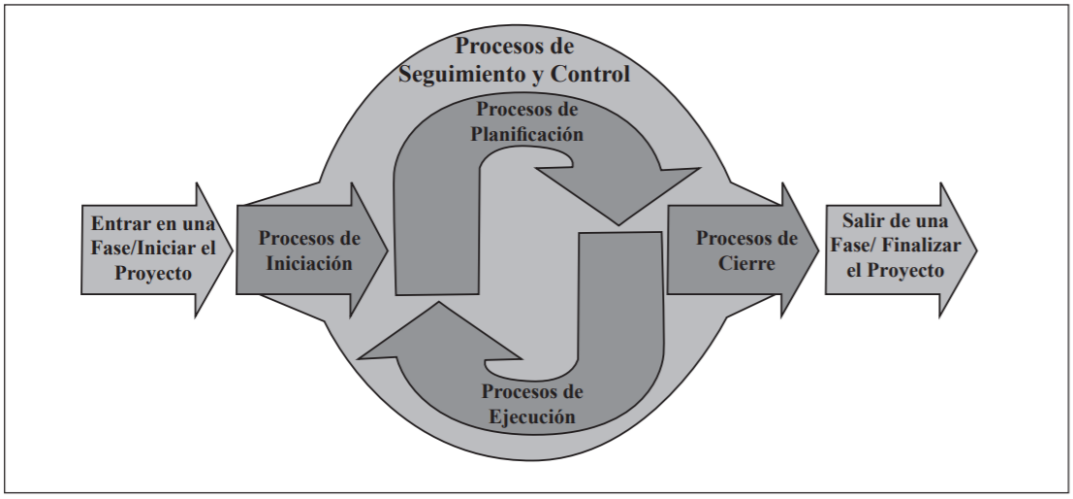
Figura 1. El ciclo de vida del proyecto



Fuente: Adaptado de (Munz & Melissa, 2013).

La noción y apreciación de Morris sobre el ciclo de vida, es sólo una de las muchas que se encuentran en la literatura de proyectos. Sin embargo, parece existir un factor común y algunas similitudes, acerca de las fases básicas entre los esquemas esbozados. Entre estas fases o etapas se reconocen: iniciación, la planificación, ejecución, seguimiento y control y cierre. Estas etapas son también incluidas por el PMI en su esquema de ciclo de vida, en el que agrupa sus procesos de gestión (figura 2) (Munz & Melissa, 2013).

Figura 2. El ciclo de vida de las etapas de un proyecto.



Fuente: Adaptado de (Munz & Melissa, 2013).

Estos esquemas brindan un panorama amplio a un alto nivel de cómo se dividen los proyectos por fases y logran organizar sus componentes en un ciclo de vida, con el fin de dar una dirección general de como un proyecto, puede lograr un objetivo determinado para un bien común, siguiendo los lineamientos referenciados e ilustrados en este caso como el PMI y Morris.

3.2 GESTIÓN DE PROYECTO

Hoy en día la gestión de proyectos es una disciplina que se considera relativamente joven. En épocas de la Segunda Guerra Mundial se empezó a hablar de la gestión de proyectos debido al esfuerzo que requería la organización de la misma. Varios métodos "típicos" surgieron en las décadas comprendidas entre los años 1940 – 1950. En la universidad de Nueva Gales del Sur en Australia, se logró inaugurar hace más de 50 años el primer curso en gestión de proyectos. En las primeras etapas, los proyectos tenían varios limitantes en ciertas industrias, así que la gestión de proyectos solo se enfocaba en mejorar el tema del cronograma y durabilidad de un proyecto, pero con el uso de técnicas cuantitativas (Silvius & Schipper, 2018).

A nivel mundial existen organizaciones importantes que se dedican a promocionar el uso de la práctica de gestión de proyectos. Estas organizaciones se relacionan con descripciones de algunas de sus principales características (tabla 1) y cuentan con publicaciones de políticas y pautas que constituyen los esquemas actuales que son requeridos para triunfar en la gestión de proyectos. El que más se destaca por ser el más reconocido y usado a nivel mundial como el estándar de gestión de proyectos es el PMI: Guía de fundamentos de la gestión de proyectos Project Management Body Of Knowledge (PMBOK®) (Munz & Melissa, 2013).

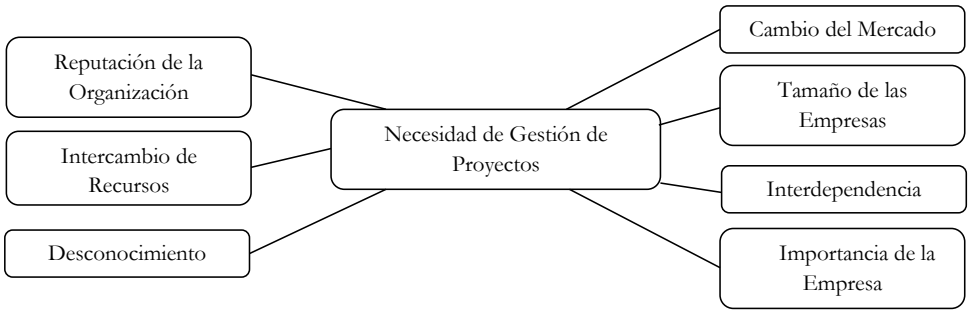
Tabla 1. Organizaciones de Gestión del Riesgo en el mundo.

Sigla	Nombre de la organización	Estándar	País	Año de Fundación	Número de miembros
PMI	*Project Management Institute*	PMBOK®	Estados Unidos	1969	Más de 500.000 en 187 países.
APM	*Association for Project Management*	*APM Body of Knowledge*	Inglaterra	1972	17.500 miembros individuales y 500 corporaciones miembros a través de todo el Reino Unido y en el exterior.
IPMA	*International Project Management Association*	ICB	Holanda	1965	Más de 110.000 en 50 países.
AIPM	*Australian Institute of Project Management*	PCSPM	Australia	1976	Más de 10.000.
PMAJ	*Project Management Association of Japan*	P2M	Japón	2005	Un poco menos de 3.000.

Fuente: Adaptado de (Munz & Melissa, 2013).

Según Cleland (1999) "Describió las posibles necesidades relacionadas con el uso de la gestión de proyectos para resolver problemas inherentes a cada tipo de organización", tal y como se indica en la (Figura 3). Existen varios componentes que pueden identificarse individualmente o en grupos (Lima, 2016).

Figura 3. Necesidad de utilizar la gestión de proyectos en las organizaciones.



Fuente: Adaptado de (Lima, 2016).

4. GESTIÓN DE RIESGO

Uno de los objetivos más relevantes de la gestión de riesgos son aumentar la probabilidad y el impacto de los eventos positivos y disminuir la probabilidad y el impacto de los eventos negativos en el proyecto (Lima, 2016). La gestión del riesgo se extiende a identificar impactos y construir planes de acción, definidos de forma general por cinco procesos relevantes necesarios para una adecuada gestión tales como: identificación, análisis, planeación, monitoreo y control (Holguín & Mejía, 2017).

Otro enfoque que se le puede dar a la gestión de riesgos independiente a los factores físicos y lógicos como los sistemas de información y los recursos materiales, son las medidas a nivel de organización haciendo referencia al factor humano (Corda et al., 2017). El cual es un elemento muy importante cuando se busca crear conciencia y cultura organizacional, logrando una mayor atención de la alta gerencia, lo cual es vital para contemplar este proceso como una aplicación total en todas las fases de un proyecto y no solo como una fase individual.

Mediante un estudio realizado en Distrito Federal México donde participaron más de 100 empresas, revelo que muchas organizaciones no han tomado un buen lineamiento con respecto al tema de gestión de riesgos, incluso en un intento fallido por cubrir este elemento, impulsaron ejercicios para impulsar los riesgos a través de matrices y cruces de probabilidad

obteniendo un entregable que en la mayoría de casos no llega a otorgar valor en el plan estratégico de las compañías (Garcia, 2013).

Por medio de la gestión de riesgos se busca crear una cultura organizacional que debería integrar parte de la cultura de gestión de una compañía; es decir, debe estar incorporada en la ideología, las prácticas y los procedimientos, más que ser considerada como una actividad separada o casual interpretada como un solo entregable (Corda et al., 2017). Sin embargo, existen algunas barreras comunes las cuales se debe tener en cuenta en este proceso de gestión de riesgos tales como: la resistencia al cambio por parte de los empleados, alto costo del procedimiento de gestión de riesgos, falta de apoyo de la alta dirección, falta de capacitación formal de los empleados diferencia cultural, falta de cooperación de la alta gerencia y los empleados, no definir claramente los riesgos (Dandage et al., 2018). Siendo conscientes de los obstáculos identificados previamente se intenta lograr y demostrar, que no se debe siempre etiquetar el riesgo como un sinónimo de pérdidas y eventualidades negativas, sino como una oportunidad que se puedan explotar positivamente en los proyectos (Garcia, 2013).

5. GESTIÓN DE RIESGO EN PROYECTOS DE TI

En la actualidad, gran cantidad de compañías a nivel global tienen basada su información en gran parte en los sistemas de software, ya que controlan infraestructuras como energía, comunicaciones, finanzas, seguridad, entre otros. El Software con el paso del tiempo ha tomado mucha fuerza en toda la economía, ya que ayuda a mejorar tiempos de producción y motiva el crecimiento a muchas industrias, pero esta dependencia trae consigo muchos riesgos que pueden estar presentes en los proyectos de software o TI (Li, Li, Wu & Song, 2012).

Las múltiples fallas en los proyectos de software son el resultado de la diversidad de riesgos que están presentes al momento de desarrollarlos. Esto conlleva lamentablemente a un historial de sobrecostos, desfase en cronograma, baja calidad y poca usabilidad. El éxito de un proyecto es complicado de predecir ya que el alcance está sujeto a cambios continuos por los requisitos que haya en el mercado, buscando una adaptación a las ultimas condiciones requeridas. Esto también aplica para los proyectos para clientes en específico ya que los requisitos pueden estar en constante cambio a petición del cliente (Kwak & Stoddard, 2004).

"La gestión de riesgos se define como un conjunto de actividades coordinadas que permiten a la organización ser dirigida y controlada en lo que respecta al riesgo" (Masso et al., 2020a).

La gestión de riesgos con un enfoque hacia la gerencia define y documenta el comportamiento, esperado para un proyecto. Dado que los eventos aleatorios pueden afectar esta conducta y comportamiento, el gerente analiza la sensibilidad del proyecto con respecto a muchas combinaciones de los mismos, que pueden convertirse en riesgos para lograr un análisis sobre cómo estos acontecimientos pueden desafiar el éxito y objetivo del proyecto (Barros, Lima & Travassos, 2004).

La gestión de riesgo cuenta con un papel importante en la protección de los riesgos relacionados con los sistemas de información, a un nivel muy amplio a tal punto de proporcionar a las organizaciones, la capacidad de medir los niveles de riesgo y alinearlos al impacto corporativo, ayudando directamente a la toma de decisiones y minimizar las pérdidas, logrando llevar a la compañía a cumplir con su misión (Guerrero & Gómez, 2012).

El objetivo primordial dentro del proceso de gestión de riesgos en el área de desarrollo en TI, serían los siguientes: identificar y evaluar todos los riesgos que puedan llegar a afectar o influir en los proyectos que se vayan a desarrollar. Esto es de vital importancia porque este proceso se puede reutilizar en futuros proyectos en donde ya quedan identificados y documentados, para que haya una mejor fluidez y coordinación (Barros et al., 2004).

La Gestión de riesgos tecnológico busca evitar las pérdidas de información, ante fallas en los sistemas que puedan afectar

directamente los proyectos en las compañías, estas fallas pueden ser de cualquier tipo (naturales, accidentales, intencionales, etc.), como también pueden verse involucrados riesgos legales y el comportamiento ante esas amenazas (Corda et al., 2017).

Para una buena ejecución de la gestión del riesgo en proyectos de TI, requiere una buena identificación, evaluación, planificación e implementación de los riesgos presentes, también es importante la comunicación en las actividades que se vayan a desarrollar entre los implicados del proyecto (Masso et al., 2020b).

Hay que tener presente también que no solamente el área de la academia y organizaciones profesionales tienen presente el tema de la gestión de riesgos en proyectos de TI; también muchas compañías privadas como Microsoft, implementan la gestión de riesgos como una disciplina importante y fundamental, logrando elaborar lo que se conoce como MSF (Microsoft Solutions Framework). Esta metodología contiene principios y guías para tener una buena gestión de riesgo, teniendo un proceso de 5 pasos para lograr un éxito permanente en los proyectos (Del Carpio Gallegos, 2008).

6. NORMATIVIDAD

A continuación, y como parte fundamental de la revisión bibliográfica, se abordó una serie de artículos públicos por parte del gobierno nacional de la república de Colombia, los cuales tocan temas normativos de cómo el gobierno de la nación aborda los temas de gestión de proyectos y gestión de riegos relacionados con las tecnologías de la información TI.

A través del documento "MGPTI.GEN.01 – Documento Maestro del Modelo de Gestión de Proyectos TI", es brindar a las Entidades Públicas a través del Líder Estratégico de TI quien orienta para administrar sus proyectos de tecnologías de la información de forma adecuada y ofrecer mejores servicios a los ciudadanos teniendo en cuenta las políticas de gobierno digital (MINTIC, 2019).

El marco normativo al que se encuentra sujeto el Modelo de Gestión de Proyecto de TI se encuentra descrito a continuación en la (tabla 2) en donde se menciona algunas normas, las cuales deben ser tenidas en cuenta en el ejercicio de administración de proyectos que se realiza en las Entidades Públicas (MINTIC, 2019).

Tabla 2. Marco normativo del Maestro del Modelos de Gestión de Proyectos de TI.

Nombre	Descripción
Ley 1955 de 2019	Por el cual se expide el Plan Nacional de Desarrollo 2018-2022. "Pacto por Colombia, Pacto por la Equidad".
Decreto 612 de 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
CONPES 3920 de 2018.	Política Nacional de Explotación de datos.
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto número 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de Tecnologías de la Información y las Comunicaciones.

Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto 1510 de 2013	Por el cual se reglamenta el sistema de compras y contratación pública.
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Acuerdo 11 de 1996	Por el cual se establecen criterios de conservación y organización de documentos.

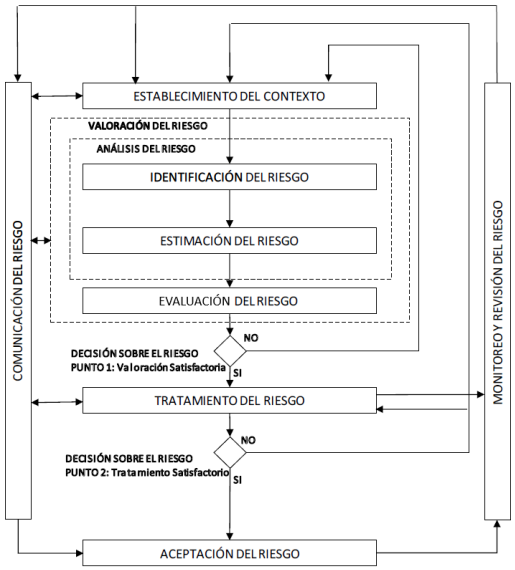
Fuente: Adaptado de (COLCIENCIAS, 2015).

Como segunda fuente se transmitirá la información suministrada por el Ministerio de Tecnologías de la Información y las Comunicaciones de la república de Colombia (MinTIC), donde se pudo obtener un lineamiento dirigido a las compañías con el fin de gestionar los riesgos de Seguridad de la información basado en los criterios de seguridad (Confidencialidad, Integridad, Disponibilidad), buscando integrar la metodología DAFP. El cual posee referencias a las políticas, definiciones o contenido publicado en la norma técnica colombiana NTC ISO/IEC 27001 vigente e ISO 27005 vigente, así como a los anexos con derechos reservados por parte de ISO/ICONTEC (MINTIC, 2016).

De acuerdo a la metodología del Departamento Administrativo de la Función Pública (DAFP) quien la entidad que se encarga de que ese servicio al público se gestione y administre de manera eficiente y transparente. La guía sugiere tener tres etapas generales para la gestión del riesgo a partir de las cuales se soportan cada una de las actividades que permiten a la compañía tener una administración de riesgos como se representa en la (figura 4) acorde con las necesidades de la misma (MINTIC, 2016).

1) Compromiso de las alta y media dirección: es muy importante tener el verdadero compromiso de los directivos de la compañía que garantizan en gran medida el éxito de cualquier proceso emprendido,
2) Conformación de un Equipo de un grupo interdisciplinario: la idea de integrar en la gestión de riesgos una visión completa de la entidad y en la cual se pueda tener el aporte de diferentes áreas analizando un mismo proceso.
3) Capacitación en la metodología: para el equipo: este punto es un poco más profundo, porque es claro que el equipo interdisciplinario debe capacitarse para poder analizar los riesgos de seguridad de la información (MINTIC, 2016).

Figura 4. Administración del riesgo en seguridad de la información



Fuente: Adaptado de (Valencia, Marulanda & Trujillo, 2015).

Así como se muestra en la figura 3 "el proceso de gestión del riesgo en la seguridad de la información puede ser iterativo para las actividades de valoración del riesgo y/o el tratamiento del mismo" (MINTIC, 2016). Cuando el proceso se realiza con un enfoque iterativo para realizar la valoración del riesgo puede incrementar la profundidad y el detalle de la valoración en cada iteración, por medio de la madurez y el análisis del contexto que puede llegar a identificarse.

Finalmente, la tercera entrega brinda una guía del Departamento Administrativo de Ciencia (COLCIENCIAS), de tipo preventivo para analizar, valorar, tratar, comunicar, monitorear, revisar y realizar el monitoreo a los riesgos, los riesgos institucionales y los del Modelo de Seguridad y Privacidad de la Información de Gobierno en Línea, a fin de optimizar y enfocar los esfuerzos institucionales en acciones estandarizadas que permitan abordar y tratar los riesgos identificados en forma eficiente y eficaz en coherencia con los objetivos y metas institucionales.

El objetivo general de esta guía es fortalecer la implementación y el desarrollo de la política de administración del riesgo y las oportunidades a través de una guía metodológica que da unos lineamientos para un adecuado tratamiento de los riesgos de corrupción, los cuales están respaldados por algunas leyes importantes dentro del marco legal vigente (tabla 3), seguridad y privacidad en la información, identificados en cada uno de los procesos que hacen parte del sistema de gestión organizacional, a fin de garantizar el cumplimiento de la misión y objetivos estratégicos de la entidad (COLCIENCIAS, 2015).

Tabla 3. Marco legal.

Nombre	Descripción
Ley 87 de 1993	Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones, artículo 2° literal a) Proteger los recursos de la organización, Buscando su adecuada administración ante posibles riesgos que los afectan. Artículo 2 literal f) Definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos.
Ley 1474 de 2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública. Artículo 73. "Plan anticorrupción y de atención al ciudadano.
Directiva Presidencial 09 de 1999	Se adoptan lineamientos para la implementación de la Política de Lucha contra la Corrupción.
Ley 1712 de 2014	Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.
Decreto 943 de 2014 MECI	Por el cual se actualiza el Modelo Estándar de Control Interno - MECI.
Decreto 1083 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública. Art. 2.2.22.1 y siguientes. Establece que el Plan Anticorrupción y de Atención al Ciudadano hace parte del Modelo Integrado de Planeación y Gestión. Art. 2.2.21.6.1. Adopta la actualización del Modelo Estándar de Control Interno para el Estado Colombiano (MECI).

Fuente: Adaptado de (COLCIENCIAS, 2015).

7. METODOLOGÍAS

Una propuesta metodológica seria la opción más viable para dar una solución a nivel de riesgos dentro de las empresas o proyectos de TI. Con esto se busca minimizar los riesgos en procesos como contratación, también ayudar a los miembros del equipo para mejorar los procesos, lo cual ayudaría a tener presente los riesgos para poderlos priorizar y así poder dar una buena gestión, para que al final se logre cumplir las metas que se diseñaron en la planificación. Muchas metodologías en la gestión del riesgo tienen como objetivo disminuir los riesgos aplicando distintos procedimientos y cada una de ellas consideran necesarios, para que así puedan atacar o prevenir riesgos en los proyectos tecnológicos. También es muy importante para dar una solución a los riesgos es que el personal contratado este calificado y relacionado con el tema legal y tecnológico que está presente en la normatividad que ejercen en Colombia, para así darle un buen uso a las mejores prácticas cuando se evidencien los riesgos (Latorre, Fiallo, Díaz & Chacon 2017).

Se tiene presente que muchas empresas no son ajenas en apoyarse en el área de TI para mejorar sus procesos, teniendo mayor productividad y eficiencia, pero esto conlleva una carga grande de responsabilidad para el negocio. En la actualidad no existe una tecnología que sea perfecta, siempre hay fallas de seguridad y vulnerabilidades, así que esto incrementa aún más los riesgos para la compañía (Andrea et al., 2010). Teniendo en cuenta esto, las empresas ya cuentan con un gobierno de TI y así mismo poder gestionar estos riesgos, pero también buscan integrar una metodología que se adapte a las buenas prácticas de la compañía y sus empleados, de acuerdo a lo anterior se hablará de las metodologías más importantes que se usan a nivel mundial.

7.1 ITIL

Information Technology Infrastructure Library [ITIL]. Esta metodología está más encaminada para el área de TI, en donde su estándar está desarrollado para dar un manejo especializado a las buenas practicas, implementa planes de prevención y captación de los riegos encontrados. Tiene presente temas como la infraestructura, amenazas, fallos y/o vulnerabilidades, para lograr esto, hace un análisis del golpe que puede dar los riesgos en la compañía, también evalúa como mitigar los riegos y por ultimo hace un control para verificar la mejor forma de concluir todo el proceso. Teniendo en cuenta todo esto, ITIL busca mejorar la calidad, la plataforma tecnológica y mejorar la relación con los clientes (Latorre et al., 2017).

7.2 MAGERIT

Su acrónimo Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información [MAGERIT]. Se formó en el Consejo Superior de Administración Electrónica de España en el 2012 con el fin de realizar una estructura para hacer una gestión en el análisis de los riesgos en el área de TI, basado en la norma ISO/IEC 27000. Cuadro etapas propone esta metodología. La etapa uno inicia con un plan de análisis de los riesgos para tener una visión del proyecto de gestión. La etapa dos se encarga de analizar los riesgos, identificarlos en las diferentes áreas y hacer estimaciones de que tanto puede abarcar el riesgo. La etapa tres gestiona los riesgos, identificándolos y revisar si hay mecanismos que sean lo potentes para mitigar los riegos y por último la etapa cuatro, se encarga de seleccionar las métodos que se van a usar para darle un control optimo a los riegos, también se hace la entrega de los documentos que recopilan toda la información obtenida durante las etapas (Acevedo & Satizábal, 2016).

7.3 OCTAVE

Esta metodología fue desarrollada por la Universidad Carnegie Mellon 2001, su acrónimo viene de "*Operationally Critical Threat, Asset and Vulnerability Evaluation"*. Se enfoca en analizar y estudiar los riesgos con tres principios fundamentales que serían disponibilidad, integridad y confidencialidad. El Departamento de Defensa de Estados Unidos entre otros entes gubernamentales usan esta metodología. Las 3 fases o principios mencionadas anteriormente iniciaría con el tema de los activos de la compañía, en donde se enfoca en identificar tanto activos como los riesgos que se puedan presentar y fallas en políticas , para luego construir perfiles de las amenazas, la segunda fase se enfoca en las fallas a nivel de infraestructura en las tecnologías de TI y la tercera fase analiza toda la información recolectada anteriormente, para hacer las estrategias y

planes de seguridad, además de crear estrategias de protección para los riesgos de más alta procedencia (Acevedo & Satizábal, 2016).

7.4 COBIT

Control Objectives for Information Systems and related Technology [COBIT]. Esta metodología se basa más que todo en la gestión de riesgos de contratación que todo proyecto debe tener en cuenta para dar un buen manejo, esto incluye procesos que son vitales para la planificación como lo son, selección de proveedores, rigurosa contratación del personal, darle una buena gestión al contrato y así mismo hacer un buen cierre. Para lograr alcanzar las metas en TI manejando esta metodología, se usan una serie de normas ISO como la ISO 27002, ISO 20000, ISO 9000 y la ISO 15504, ya que hacen parte de la de la gestión de riesgos porque hacen uso del Valor/beneficio, entrega de programas y proyectos, entrega de servicios TI, buscando con esto, tener presente todos los riesgos en cada proceso (Latorre et al., 2017).

7.5 ANI

La Agencia nacional de infraestructura (ANI) en Colombia. El 31/01/2020 presenta un plan de lineamientos y una metodología a seguir para el análisis, valoración y tratamiento de riesgos, alineados con las políticas de seguridad y privacidad de la información (Cadena, 2020).

La identificación y tratamiento de los riesgos de seguridad de la información, como lineamiento de la alta gerencia de la ANI, serán aplicados por parte de todos los funcionarios, contratistas y terceros que presten sus servicios o tengan algún tipo de relación en cualquier proceso de la compañía (Cadena, 2020).

Las etapas de la metodología ANI, para la gestión del riesgo se encuentran alineadas con la norma ISO 31000, que brinda una serie de principios y directrices a un nivel estratégico y operativo, definiendo las fases de este plan de la siguiente manera:

1) La identificación del riesgo.
2) Valoración del riesgo.
3) Identificación de amenazas.
4) Identificación de las vulnerabilidades.
5) Análisis de riesgo direccionado a la seguridad de la información.
6) Evaluación de controles se pueden implementar para la mitigación del riesgo.
7) Seguimiento y revisión de planes de acción (Cadena, 2020).

8. CONCLUSIONES

La gestión de riegos se presenta como una actividad global clave, para el resguardo de los activos de información y de los sistemas informáticos de una compañía y mostrándose como un proceso constante en todo el desarrollo de los proyectos, no solo como un entregable único que busque suplir un requisito administrativo.

Las compañías usan de manera directa la tecnología en sus actividades diarias y como parte de todos sus procesos. Lo que puede ocasionar que se presenten eventualidades que pueden afectar los activos internos y ser fuente de pérdidas y daños considerables. Hay que crear conciencia y generar valor del concepto de riesgo y buscar estrategias para obtener el apoyo de la dirección corporativa con el fin de cumplir con los objetivos y asegurar la información relevante en la compañía.

En esta revisión se identificaron ciertas metodologías, dirigidas a la gestión de riesgos que hacen ver un esfuerzo por lograr disminuir los riesgos y sus impactos, aplicando procedimientos que cada una de ellas considera necesarios, para así mitigar y controlar los riesgos presentes o futuros que puedan aparecer en los proyectos tecnológicos y reducir su tasa de

éxito.

Es importante contar con un equipo en el proceso de gestión de riesgos, que conozca todo lo relacionado con la parte legal y tecnológica presente en la normatividad de Colombia, con el fin de a aplicar las mejores prácticas una vez se generen los riesgos y se definan planes de acción.

Este proceso de gestión de riesgos es responsabilidad de todas las personas que se desempeñan en el entorno organizacional, lo que es esencial es crear y desarrollar una cultura de la seguridad, en la compañía aplicando una serie de políticas, procedimientos y buenas prácticas que permite indirectamente controlar de forma muy eficiente los riesgos.

9. REFERENCIAS

Acevedo, N., & Satizábal, C. (2016). Risk management and prevention methodologies: a comparison. *Sistemas y Telemática*, *14*(36), 39–58. https://doi.org/10.18046/syt.v14i36.2214

Andrea, Ricardo, G., Diego, P., Yesid, D., & Herrera. (2010). *Metodología y gobierno de la gestión de riesgos de tecnologías de la información*. 109–118.

Arias, C. M. (2010). *Marco conceptual de la administración de proyectos* (pp. 543–559).

Bannerman, P. L. (2008). Risk and risk management in software projects: A reassessment. *Journal of Systems and Software*, *81*(12), 2118–2133. https://doi.org/10.1016/j.jss.2008.03.059

Barros, D. O., Lima, M., & Travassos, G. H. (2004). *Supporting risks in software project management*. *70*, 21–35.

Cadena, G. (2020). *Plan de tratamiento de riesgos de seguridad digital* (pp. 1–17). ANI.

Colciencias. (2015). *Guia para la gestión del riesgo y las oportunidades*. *02*, 1–43.

Corda, M. C., Viñas, M., & Coria, M. K. (2017). Gestión del riesgo tecnológico y bibliotecas: una mirada transdisciplinar para su abordaje. *Palabra Clave (La Plata)*, *7*(1), 032. https://doi.org/10.24215/18539912e032

Dandage, R. V, Mantha, S. S., Rane, S. B., & Bhoola, V. (2018). Analysis of interactions among barriers in project risk management. *Journal of Industrial Engineering International*, *14*(1), 153–169. https://doi.org/10.1007/s40092-017-0215-9

Del Carpio Gallegos, J. F. (2008). *Gestión de riesgos en proyectos de tecnología de información en el Perú*. *11*(2003).

Garcia, G. D. (2013). *Inteligencia de riesgos: agregando valor a la estrategia empresarial* (pp. 149–170).

Gillespie, S. J. (2014). *Correlational study of risk management and success of the information technology*. 1–92.

Guerrero, Julio, M. L., & Gómez, Flórez, L. C. (2012). Gestión de riesgos y controles en sistemas de información: del aprendizaje a la transformación organizacional. *Estudios Gerenciales*, *28*(125), 87–95. https://doi.org/10.1016/s0123-5923(12)70011-6

Guerrero, J. L. M., & Gómez, L. C. (2011). *Revisión de estándares relevantes y literatura de gestión de riesgos y controles en sistemas de información*. 195–215.

Hidalgo, A. (2004). *Una Introducción a la Gestión de Riesgos Tecnológicos*. 35.

Holguín, D. M., & Mejía, A. C. (2017). Comparación de metodologías para la gestión de riesgos en los proyectos de las Pymes. *Revista Ciencias Estratégicas*, *25*(38), 319–338. https://doi.org/10.18566/rces.v25n38.a4

Jahn, F., Cook, M., & Graham, M. (1998). Project and contract management. *Developments in Petroleum Science*, *46*(C), 291–301. https://doi.org/10.1016/S0376-7361(98)80014-9

Kwak, Y. H., & Stoddard, J. (2004). *Project risk management: lessons learned from software development environment*. *24*, 915–920.

Leonardo, J., Jaimes, L., Augusto, O., Soto, F., Gerardo, J., & Rangel, C. (2017). *Propuesta metodológica para analizar y evaluar los riesgos presentados en el proceso de contratación en proyectos tecnológicos*. 356–386.

Li, J., Li, M., Wu, D., & Song, H. (2012). An integrated risk measurement and optimization model for trustworthy software process management. *Information Sciences*, *191*(15), 47–60. https://doi.org/10.1016/j.ins.2011.09.040

Lima, A. S. (2016). *Un método difuso para el análisis cualitativo de riesgos en proyectos de desarrollo de software*. 7–38.

Masso, J., Pino, F. J., Pardo, C., García, F., & Piattini, M. (2020a). Risk management in the software life cycle: A systematic literature review. *Computer Standards and Interfaces*, *71*. https://doi.org/10.1016/j.csi.2020.103431

Masso, J., Pino, F. J., Pardo, C., García, F., & Piattini, M. (2020b). Risk management in the software life cycle: A systematic literature review. *Computer Standards and Interfaces*, *71*. https://doi.org/10.1016/j.csi.2020.103431

MINTIC. (2016). Guía de gestión de riesgos. *Mintic*, *7*, 39. http://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

MINTIC, M. de las T. y las T. (2019). MGPTI.G.GEN.01 – Documento Maestro del Modelo de Gestión de Proyectos TI. *Diario Oficial*, *V.1 2019*, 1–44. https://www.mintic.gov.co/arquitecturati/630/articles-9401_pdf_01.pdf

Munz, S., & Melissa, I. (2013). *El enfoque de gestión de proyectos en las organizaciones dedicadas a proyectos de investigación*. 152–161.

Neves, S. M., da Silva, C. E. S., Salomon, V. A. P., da Silva, A. F., & Sotomonte, B. E. P. (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. https://doi.org/10.1016/j.ijproman.2013.02.007

PROJECT MANAGEMENT INSTITUTE, I. (2017). *La guía de los fundamentos para la dirección de proyectos (Guía del PMBOK) ®*.

Silvius, G., & Schipper, R. (2018). *Exploring Responsible Project Management Education*. 1–13.

Valencia, J., Marulanda, C., & Trujillo, M. (2015). Gobierno y gestión de riesgos de tecnologías de información y aspectos deferenciadores con el riesgo organizacional. *Revista Gerencia Tecnológica Informática*, *15*(November), 65–77.

Vega, M., García, A., & Cervantes, H. (2018). A survey on the Software Project Scheduling Problem. *International Journal of Production Economics*, *202*, 145–161. https://doi.org/10.1016/j.ijpe.2018.04.020

Wan Husin, W. S., Yahya, Y., Mohd Azmi, N. F., Amir Sjarif, N. N., Chuprat, S., & Azmi, A. (2019). Risk management framework for distributed software team: A case study of telecommunication company. *Procedia Computer Science*, *161*,

178–186. https://doi.org/10.1016/j.procs.2019.11.113