Cómo citar este artículo: P. A. Arias-Murcia, R. Ferro-Escobar, A. Abuchar-Porras, "Metodología para la mitigación de riesgos en el mejoramiento de vías terciarias en Cundinamarca, Colombia" Revista Ingeniería, Investigación y Desarrollo, vol. 19 (2), pp. 29-40, julio. 2019.

DOI: https://doi.org/10.19053/1900771X.v19.n2.2019.12879

ANÁLISIS DE METODOLOGÍAS APLICADAS A LA GESTIÓN DE RIESGOS EN PROYECTOS DE DESARROLLO DE SOFTWARE EN COLOMBIA

Analysis of methodologies applied to risk management in software development projects in Colombia

Paola Andrea Arias Murcia[1], Roberto Ferro Escobar[2], Alexandra Abuchar Porras[3]
[1]Universidad ECCI, docente del programa de Ingeniería Mecatrónica, Colombia.
[2]Universidad Distrital Francisco José de Caldas, docente del programa Especialización en Telecomunicaciones Móviles, Colombia.
[3]Universidad Distrital Francisco José de Caldas, docente del programa Especialización en Ingeniería del Software, Colombia.
Email: [1]pariasm@ecci.edu.co, [2]rferro@udistrital.edu.co, [3]aabuchar@udistrital.edu.co

(Recibido Junio 22 de 2019 y aceptado Octubre 5 de 2019)

Resumen

La Gestión del Riesgo es un factor muy importante que debe ser abordada desde el inicio de cualquier tipo de proyecto, este es uno de los aspectos fundamentales que permite ver desde diferentes puntos de vista diversas variables que pueden traer múltiples problemas en la ejecución del proyecto, en este artículo se hace un énfasis en la realización de proyectos de software debido a la importancia que han tenido en los últimos años y debido a los altos índices de fallas en la realización de los mismos. Esta investigación tiene en cuenta en su fase metodológica el uso de la Gestión de riesgos propuesta por el PMBOK, el ciclo PHVA y la metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, el uso de estas metodologías permitirá usar y aplicar las mejores prácticas propuestas para definir las amenazas, riesgos, vulnerabilidades y a futuro sentará las bases para formular políticas de mejora continua y de esta forma evitar que estos proyectos fracasen.

Palabras clave: *gestión de riesgo, metodología PMBOK deming, desarrollo de software.*

Abstract

Risk Management is a very important factor that must be addressed from the beginning of any type of project, this is one of the fundamental aspects that allows us to see from different points of view different variables that can bring multiple problems in the execution of the project, This article emphasizes the realization of software projects due to the importance they have had in recent years and due to the high failure rates in their realization. This research considers in its methodological phase the use of Risk Management proposed by the PMBOK, the PHVA cycle and the methodology of Analysis and Risk Management of Information Systems, the use of these methodologies will allow the use and application of Proposed best practices to define threats, risks, vulnerabilities and in the future will lay the groundwork for formulating policies for continuous improvement and thus prevent these projects from failing.

Key words: *risk managment, PMBOK methodology, deming, software developement.*

1. INTRODUCCIÓN

Los proyectos de software son iniciativas que poseen variables complejas y son susceptibles de presentar muchos problemas como lo presento Bannerman [1]. Uno de los posibles problemas puede ser originado

en no administrar los riesgos presentes en el proyecto de desarrollo de software. Según Pinna y Carvalho [2], si los riesgos no se abordan de forma adecuada, la calidad del producto final puede verse comprometida; los intereses del cliente no se cumplen; y el personal, durante el ciclo de vida del proyecto, puede disminuir la productividad y cometer errores garrafales. Desde el punto de vista de la teoría relacionada con la perspectiva organizacional, el riesgo surge cuando las organizaciones buscan oportunidades frente a la incertidumbre y están limitadas por la capacidad y los costos asignados al proyecto [1]. Algunos directores o gerentes de proyectos de software ven las actividades y procesos de gestión de riesgos como trabajo y gastos adicionales innecesarios, lo que causa que sea eliminado del alcance del proyecto cuando se retrasa un proyecto.

Algunos autores afirman que muchos profesionales e ingenieros de desarrollo de software perciben la gestión y el control de riesgos como un inhibidor de la creatividad. Las altas tasas de fracaso asociadas con los proyectos de sistemas de información sugieren que las organizaciones necesitan mejorar no solo su capacidad para identificar los riesgos asociados con estos proyectos, sino también para gestionar los mismos [3].

De acuerdo con la revisión del estado del arte, este artículo tiene como objetivo presentar una revisión, de la Gestión de Riesgos en proyectos de desarrollo de software bajo los lineamientos del PMBOK 6 y dos metodologías que permite el uso de estos aspectos de forma adecuada.

Esta investigación tiene en cuenta en su fase la Gestión de riesgos propuesta por el PMBOK, la metodología del uso del ciclo Deming (PHVA) y la metodología MAGERIT ("Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información"). El uso de estas metodologías permitirá tener en cuenta las mejores prácticas propuestas para definir las amenazas, riesgos, vulnerabilidades y a futuro sentara las bases para formular políticas de mejora continua. De acuerdo a lo establecido debemos definir los siguientes aspectos:

Análisis de Riesgos: Identificación de activos informáticos relacionados con el desarrollo y producción de software sus vulnerabilidades y amenazas a los que se encuentran expuestos así como su probabilidad de ocurrencia y el impacto de las mismas, a fin de determinar los controles adecuados para aceptar, disminuir, transferir o evitar la ocurrencia del riesgo, para establecer un correcto diagnóstico del riesgo que se está presentando se debe realizar un análisis donde se establece la siguiente relación:

Riesgo Total = Probabilidad * Impacto promedio (1)

Ley estatutaria 1581 de 2012: La cual tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido

Auditoría: Proceso para diagnosticar los sistemas de información de una empresa u organización, que proporciona metodologías para tomar decisiones sobre los sistemas auditados, por lo tanto, debe tenerse en cuenta que no todas las empresas manejan y manipulan la información de la misma manera.

• Auditoría Interna: Según el Instituto de Auditores Internos (The Institute of Internal Auditors - IIA), definieron la auditoría interna como "La actividad independiente y objetiva de aseguramiento y consulta concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de gestión de riesgos, control y gobierno".

• Auditoría Externa: La auditoría externa son los métodos utilizados por una compañía externa para examinar sistemáticamente las herramientas que respaldan la administración de la compañía, aquellos sistemas que respaldan algún procedimiento que puede auditarse para determinar la integridad del estado actual de los documentos, archivos e información. Eso causó la entrada de información. Como resultado, se emite un concepto independiente

de sistemas de información y se harán sugerencias de acuerdo con los hallazgos y la evidencia encontrada, para dar fe pública sobre el procedimiento desarrollado para examinar los procesos, validar la evidencia ante terceros y formular los procedimientos para la mejora continua.

2. MARCO NORMATIVO EN COLOMBIA SOBRE DESARROLLO DE SOFTWARE

Ley 1341 de 2009 Define principios y conceptos sobre la sociedad de la información y la organización de las TIC, constituyendo en el marco general para la formulación de las políticas públicas que rigen el sector de las Tecnologías de la Información y las Comunicaciones, su ordenamiento genera [4].

Sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en su artículo 20. Asimismo, los principios y disposiciones contenidos en esta ley son aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de ser tratados por entidades de naturaleza pública o privada [5].

Ley Estatutaria 1266 de 2008 tiene como disposiciones generales del Habeas Data y regulación del manejo de la información contenida en bases de datos personales, especialmente financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones [6].

Ley 603 de 2000 (Derechos de Autor) Es a través de la cual se modifica el artículo 47 de la Ley 222 de 1995 donde se establece que los informes de gestión deben contener una presentación fiel sobre la evolución de los negocios y la situación económica, administrativa y legal de la empresa [7].

Ley 1712 de 2017 Mediante la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y otras disposiciones que se emiten [8].

Por medio del decreto 1377 DE 2013 se reglamenta parcialmente la Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales. De la misma forma, indica lo que está relacionado con el procesamiento de datos en el ámbito personal o doméstico, definiciones, autorización, políticas de tratamiento, ejercicio de los derechos de los propietarios, transferencias y transmisiones internacionales de datos personales y responsabilidad demostrada hacia el procesamiento de datos personales [9].

3. METODOLOGÍAS PROPUESTAS

A continuación se realiza una descripción de las tres metodologías propuestas y los aspectos que se destacan para su aplicación en la investigación propuesta:

3.1 Metodología PMBOK

Planificar la gestión de los riesgos es el proceso organizacional que pretende realizar identificación, análisis, planificación de respuesta al riesgo, para así aumentar la probabilidad y el impacto de las oportunidades, y disminuir la probabilidad y el impacto de las amenazas.

Figura 1. Mapa de riesgos de un proyecto de software

Si bien existen varios modelos de gestión del riesgo, uno de los más utilizados en proyectos es la guía de los

los fundamentos para la dirección de proyectos [10].

Los objetivos de la gestión de los riesgos del proyecto consisten en aumentar la probabilidad y el impacto de los eventos positivos y disminuir la probabilidad y el impacto de los eventos negativos.

De acuerdo a la descripción y definición del PMBOK se plantean seis actividades a realizar en cuanto a la gestión del riesgo: planificar la gestión de riesgos, identificar los riesgos, realizar el análisis cualitativo de los riesgos, realizar el análisis cuantitativo de los riesgos, planificar la respuesta a los riesgos y monitorear y controlar los riesgos.

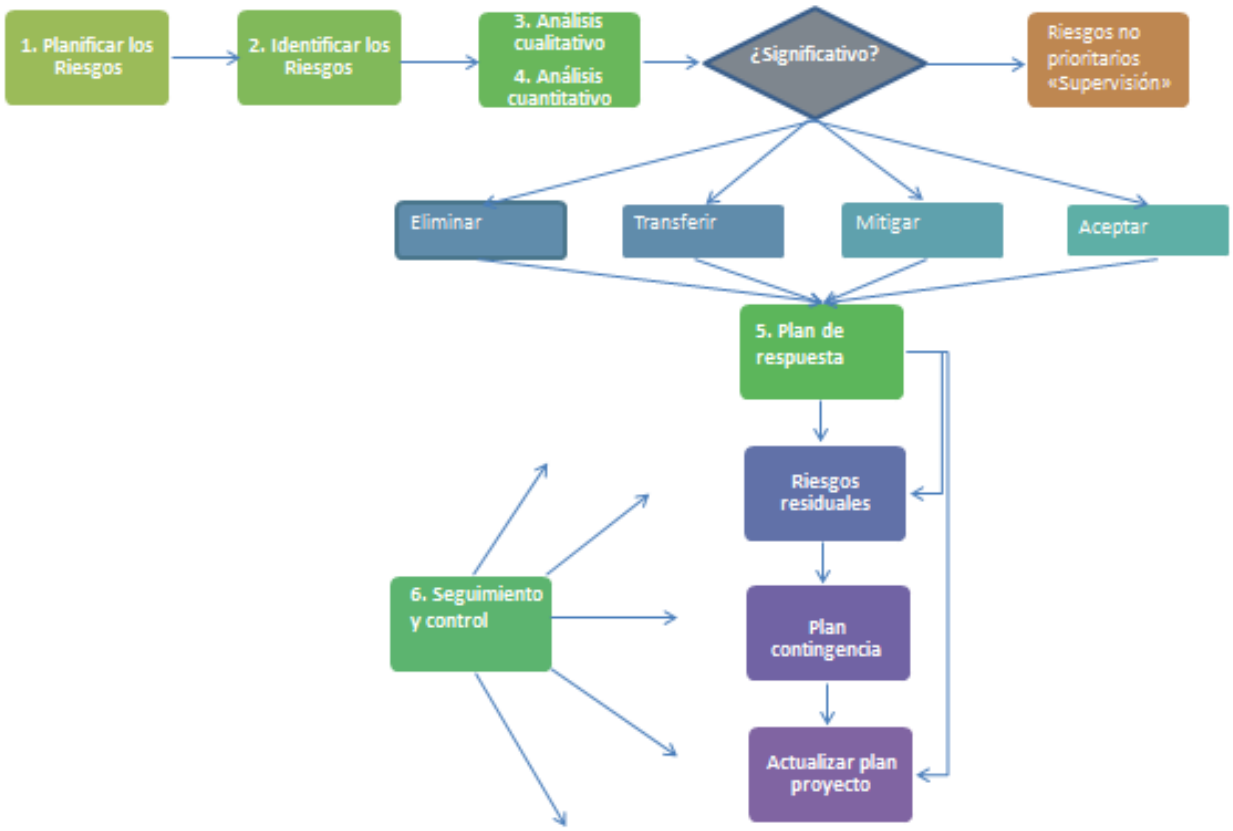

Figura 2. Actividades de gestión del riesgo

3.1.1 Planificar la gestión de los riesgos. Es el proceso de definir como realizar las actividades de gestión de riesgos de un proyecto relacionado con software.

3.1.2 *Identificar los Riesgos.* Consiste en determinar los riesgos que pueden afectar el proyecto y documentar sus características los cuales se establecerán en la matriz de riesgos en la etapa de identificación del proyecto.

3.1.3. Realizar el análisis de riesgos cuantitativos. Consiste en analizar numéricamente el efecto de los riesgos identificados en el proyecto, los cuales se manejarán en la matriz de riesgos identificando el impacto, la probabilidad, valoración del riesgo.

3.1.4. Realizar análisis de riesgos cualitativos. Consiste en priorizar los riesgos para llevar a cabo las acciones

posteriores, evaluar y combinar la probabilidad de ocurrencia y el impacto de dichas acciones que se establecerán en la matriz de riesgos, en la etapa de análisis cualitativo.

3.1.5. Planificar los riesgos. Comiste en desarrollo opciones y acciones para mejorar las oportunidades y reducir las amenazas a los objetivos del proyecto, los cuales se identificarán en la matriz de riesgos en la periodicidad de la gestión de los riesgos.

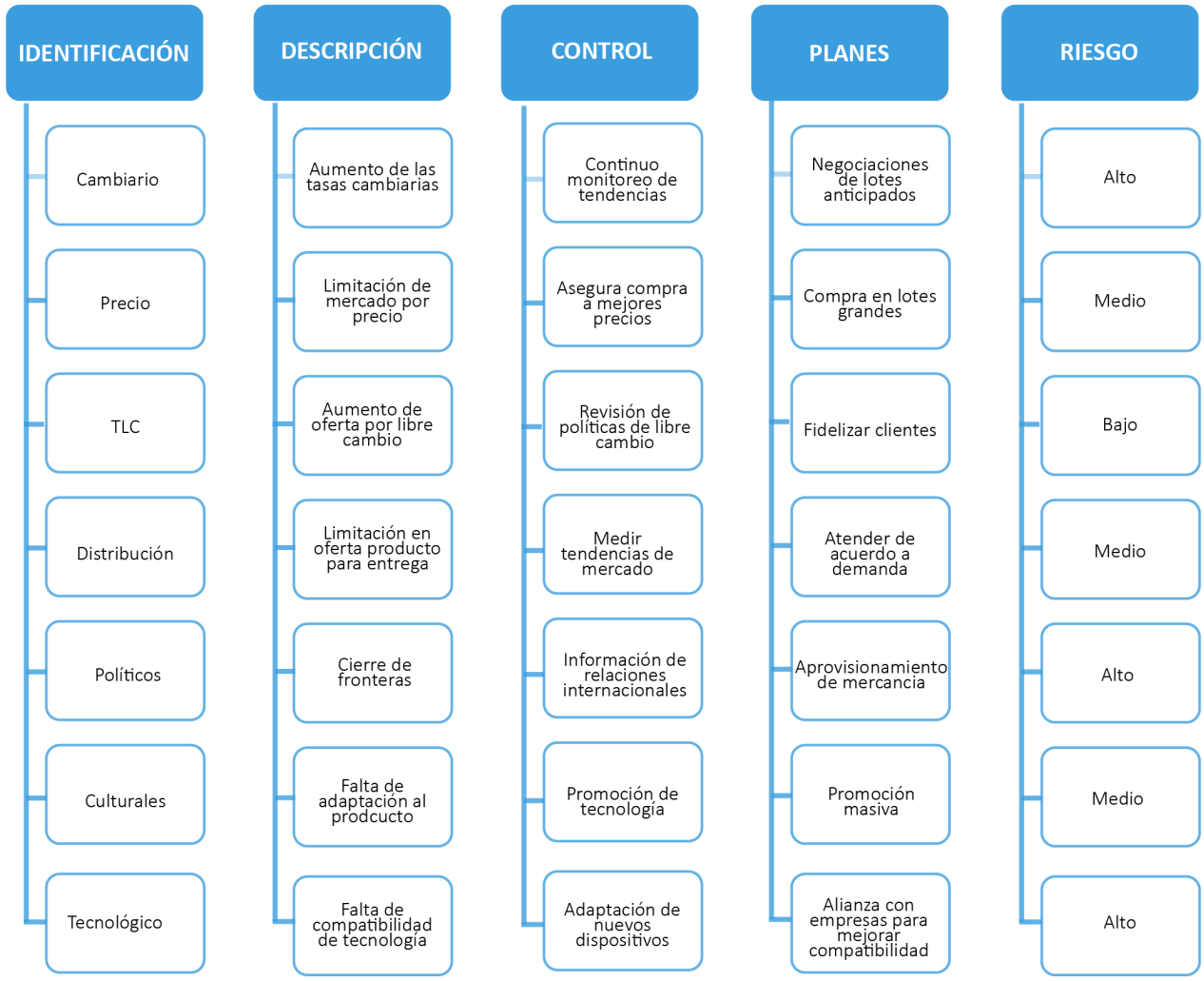

Figura 3. Matriz temática de posibles riesgos de un proyecto.

3.1.6. Dar respuesta a los riesgos. Consiste en implementar la respuesta al riesgo, para que los riesgos identificados sean rastreados y monitoreados, esto permite identificar nuevos riesgos y evaluar la efectividad del proceso contra los riesgos a través del proyecto, que se identificarán en la matriz de riesgos en el control y periodicidad de riesgos.

						EVALUCION DE RIESGO		
						CALIFICACION	SEVERIDAD	
No.	TIPO DE RIESGO	RIESGO	EFECTO	IMPACTO	PROBABILIDAD		VALOR	NIVEL
1	CAMBIARIO	AUNMENTO EN LAS TASA DE CAMBIO DE LA MONEDA DE ADQUISICION (Proveedores)CON RESPECTO A LA MONEDA LOCAL	MAYOR PRECIO PARA EL PAIS DE DESTINO DE LOS PROVEEDORES	3	2	6	3	ALTO
2	PRECIO	LIMITACIONES DE MERCADO POR PRECIO	MANOR INTENSION DE COMPRA DEL CONSUMIDOR FINAL	2	1	2	2	MEDIO
3	TLC	AUMENTO DE LA OFERTA POR LIBRE CAMBIO	DISMINUCION DE IMPACTO EN EL MERCADO	1	2	2	1	BAJO
4	DISTRIBUCION	LIMITACION DE OFERTA PDE PRODUCTO PARA LA ENTREGA AL CONSUMIDOR	MALA IMAGEN DEL PRODUCTO E INAPETENCIA DEL CONSUMIDOR	2	2	4	2	MEDIO
5	POLITICOS	CAMBIO DE POLITICAS DEL GOBIERNO NACIONAL	FALTA DE INVENTARIO PARA VENTA	3	2	6	3	ALTO
6	CULTURALES	FALTA DE ADAPTACION DE USO DE PRODUCTO POR NO SABER COMO HACERLO	POCO ISO DE LOS BENEFICIOS TECNOLOGICOS	2	2	4	2	MEDIO
7	TECNOLOGICOS	FALTA DE COMPATIBILIDAD DE TECNOLOGIA CON MEDIOS LOCALES	USO INADECUADO DEL PRODUCTO	3	2	6	3	ALTO

NIVEL DE SERVICIO		
CALIFICACION	VALOR	RIESGO
9	3	ALTO
6	3	ALTO
4	2	MEDIO
2	2	MEDIO
3	1	BAJO
1	1	BAJO

Figura 4. Matriz de valoración de riesgos de un proyecto

3.1.6. Identificación y monitoreo de riesgos.

Riesgos técnicos o calidad: Relacionados con el rendimiento tanto del software como de las TIC

1. No contar con la suficiente experiencia para desarrollar el proyecto.
2. Fallas en la ingeniería de requerimientos.
3. No disponer de dispositivos de última tecnología.
4. Desconocimiento sobre licenciamiento.
5. No conocer temas de derechos de autor.

Riesgos en la gerencia de proyecto:

1. Diseño adecuado de los ETL y cronogramas con tiempos de holgura.
2. Identificar a los expertos adecuados que apoyen el proyecto.
3. Diseño y calidad de los entregables que estén acorde sal acta de constitución y sus entregables.

Riesgos externos:

1. Cambio de políticas de gobierno o nuevos estándares de desarrollo de software.
2. Problemas relacionados con virus o malware.
3. Cambio de las partes interesadas definidas al inicio del proyecto.
4. Cambios de la TRMN alzas de moneda exterior.
5. No levantamiento de la cultura empresarial destino.

Después de entrevistar a 10 líderes de tecnología de

universidades, empresas privadas y del sector gobierno es posible identificar que existen diferentes riesgos en el proceso de desarrollo de software, autores como Bannerman indican que es necesario usar diferentes metodologías para realizar la gestión de riesgos [1].

3.2 Ciclo PHVA

El movimiento de calidad japonés trajo consigo el ciclo de mejoramiento PHVA también conocido como el ciclo de Shewhart, creado por Walter Shewhart que posteriormente fue Popularizado y efectivamente aplicado por Edward Deming, [11]. Este ciclo ha sido la base de estándares de calidad y modelos de mejora continua como ISO 9000, Six Sigma y BPM.

En los proyectos y para el PHVA es importante trabajar bajo el marco de la planeación estratégica es por eso la importancia que dentro del proyecto se defina el ciclo enfocado desde tres puntos de vista estratégico, táctico y operativo. El estratégico con el componente de gobernanza en cuanto a las estrategias, metas y objetivos, políticas y procedimientos; el táctico todo lo correspondiente a gestión de riesgos y en el operativo todo lo correspondiente al cumplimiento con sus procesos, controles y actividades, para que así mismo se definan los elementos del modelo de acuerdo a la normatividad y buenas prácticas mencionadas tomando el Ciclo PHVA de Deming (Planear, Hacer, Verificar, Actuar), en cada una de sus etapas.

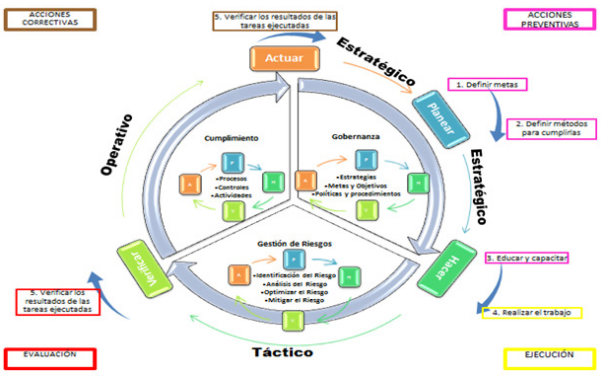

Figura 5. Ciclo PHVA ajustado a riesgos

El ciclo PHVA (Planear-Hacer-Verificar-Actuar) es de gran utilidad para estructurar y ejecutar proyectos de mejora de la calidad y la productividad en cualquier proyecto, esto se entiende como una herramienta para la mejora integral, que presenta 4 aspectos fundamentales que deben llevarse a cabo sistemáticamente para lograr la mejora continua, donde las salidas de una fase son las entradas de la siguiente fase y el ciclo de repetición debe repetirse nuevamente, de modo que las actividades se reevalúen periódicamente para incorporar nuevas mejoras, asegurando así que se forme una red de trabajo de calidad [12].

Lo anterior comprendiendo la mejora continua de la calidad en términos de (reducción de fallas, aumento de la eficacia y la eficiencia, resolución de problemas, previsión y eliminación de riesgos potenciales...); Por eso es tan importante que para proyectos de consultorías o incluyo en proyectos del diario vivir se apliquen conceptos básicos que funcionan para evitar el riesgo de pérdida de control.

3.2.1. Planear. Fase preliminar en la que se identifican problemas o actividades susceptibles de mejora y definen los objetivos y metas a alcanzar. A partir de un buen conocimiento de la situación del proyecto y los posibles puntos críticos, determinar los procesos afectados, factores clave, responsables, entre otros, que en conjunto buscan obtener los resultados esperados. En gestión de proyectos, algunas de las actividades para la planificación son:

- Tener clara las necesidades reales del cliente
- Definir el alcance del producto final.
- Definir mecanismos a seguir para realizar el seguimiento y control.
- Definir los planes necesarios para la correcta ejecución del proyecto [13].

En general como principio es definir y construir la línea base que se debe tener en cuenta en la ejecución y seguimiento y control para obtener el producto o servicio deseado, que después con la ayuda de las otras fases pueda ser transformado para el cumplimiento de los objetivos en el ejercicio de la mejora continua.

3.2.2. Hacer. En esta etapa se comienza a ejecutar lo planificado, por lo tanto Se realizará la identificación, análisis y evaluación de las vulnerabilidades, Amenazas y riesgos potenciales para definir controles para mitigarlos, para este fin, las acciones que, en base al diagnóstico previo, permiten resolver el problema o corregir las deficiencias. Es importante tener en cuenta que la ejecución de lo planeado en la fase anterior debe desarrollarse en el orden estipulado y en detalle en su totalidad para obtener los resultados esperados. Teniendo en cuenta que en la gestión de proyectos, no se deben omitir los pasos planificados, ya que se puede incurrir en riesgos de que las actividades se vean perturbadas, generalmente es aconsejable realizar una prueba piloto para probar la operación antes de realizar cambios a gran escala.

3.2.3. Verificar. Una vez implantada la mejora, se deja un periodo de prueba para verificar su correcto funcionamiento, es por eso que en esta etapa sobresale la verificación de los resultados de las acciones implementadas con las hipótesis efectuadas en el diseño de la planificación para cumplir con los requerimientos y objetivos del proyecto.

Por lo tanto, se presta especial énfasis en monitorear, revisar e interpretar los resultados obtenidos, las herramientas, controles y actividades realizadas con el fin de comprobar en qué medida se ha acertado o no en la búsqueda de la solución requerida y que tan eficientes resultaron.

3.2.4. Actuar. El equipo del proyecto trata de establecer la relación causa efecto (relación matemática entre las variables de entrada y la variable de respuesta) para predecir, mejorar y optimizar el funcionamiento del proceso. Finalmente, se determina el rango operativo de los parámetros o variables de entrada del proceso [14].

Por último, se deben estudiar los resultados obtenidos y compararlos con el funcionamiento de las actividades antes de haber sido implantada la mejora, para así poder comprobar si arrojan resultados satisfactorios o por mejorar.

Si los resultados son positivos realizan los ajustes necesarios para implementar la mejora de forma definitiva, además se documentan las mejoras que deben ser adicionadas a todo el proceso con los respectivos controles de cambios, Si por el contrario se evidencio que la mejora no cumplió las expectativas iniciales se deben establecer las acciones correctivas y modificaciones para las falencias evidenciadas en el proyecto con la finalidad de ajustar los aspectos necesarios para cumplir los objetivos esperados a fin de obtener la retroalimentación respectiva para la búsqueda de soluciones.

Una vez cumplido lo anterior es indispensable retornar al primer ciclo con cierta periodicidad para mantener la mejora continua y estudiar nuevas mejoras a implementar.
El aspecto positivo de esta metodología es que el resultado se expresa en valores económicos. Además, concientiza a los responsables de los sistemas de información de la existencia de los riesgos y de la necesidad de atajarlos a tiempo y así como dice H. James Harrington “La medición es el primer paso para el control y la mejora. Si algo no se puede medir, no se puede entender. Si no se entiende, no se puede controlar. Si no se controla, no se puede mejorar” [15].

1.3. Metodología MAGERIT

Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina “Proceso de Gestión de los Riesgos”, sección 4.4 (“Implementación de la Gestión de los Riesgos”) dentro del “Marco de Gestión de Riesgos”. En otras palabras, MAGERIT implementa el Proceso de Gestión de Riesgos dentro de Un marco para que las agencias gubernamentales tomen decisiones teniendo en cuenta los riesgos derivados del uso de las tecnologías de la información, [16].

En este sentido, fue desarrollado MAGERIT una metodología de análisis y gestión de riesgos creada por el Consejo Superior de Administración Electrónica de España, bajo la apreciación de que la administración en general crece y es

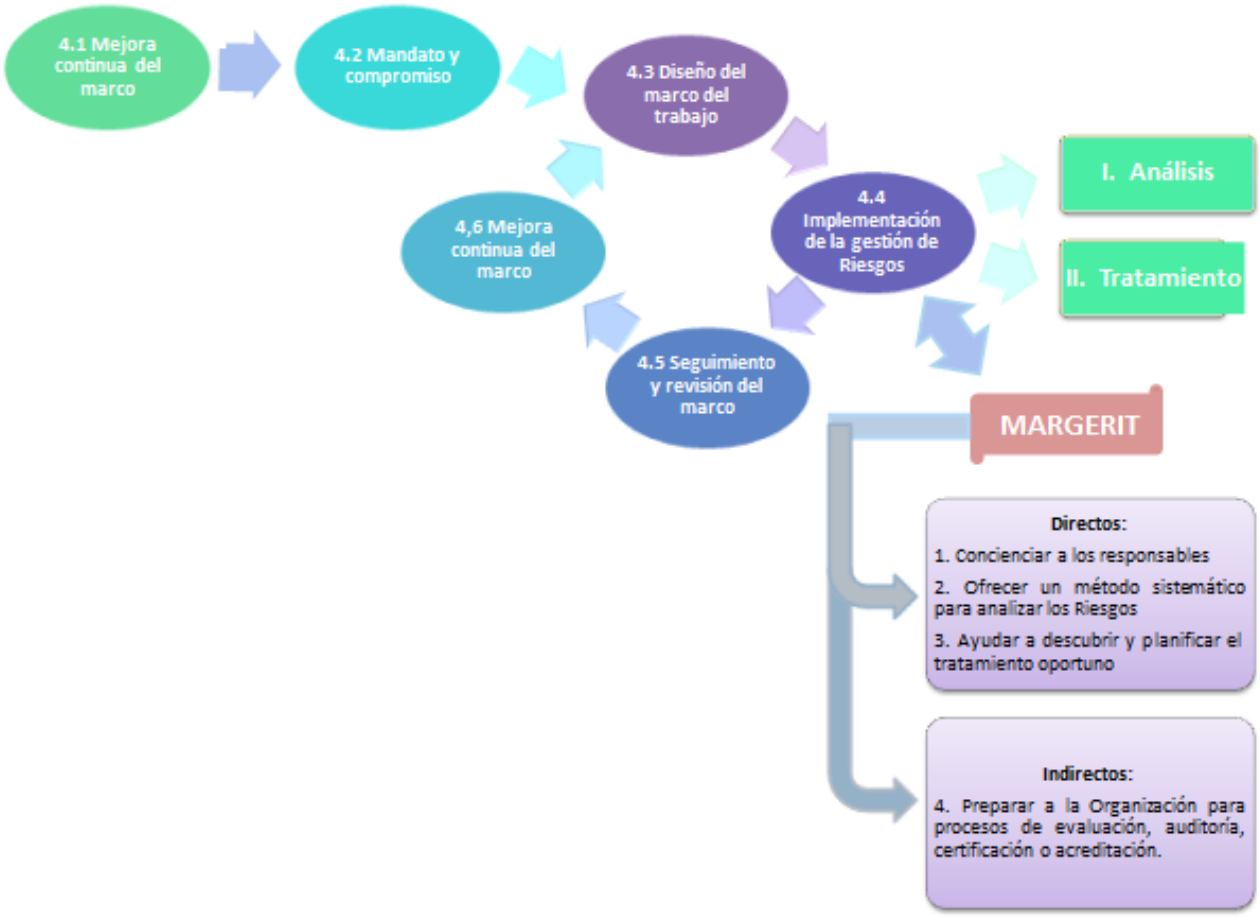

Figura 6. ISO 31000 – Marco de trabajo para la gestión de riesgos

dependiente a las tecnologías de la información para el cumplimiento en general de la administración y de las otras áreas [16].

En el preámbulo de esta metodología se pueden resaltar los riesgos que soporta un sistema de información y su entorno, concibiendo el riesgo como la probabilidad de que ocurra o se materialice un peligro, esto en una aproximación inicial se ciñe a la aceptación habitual del término, además de recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir impedir, reducir o controlar los riesgos investigados [17].

Los factores claves para el análisis de riesgos, según Magerit son: activo, amenaza, vulnerabilidades, impacto, riesgo y salvaguardas (funciones, servicios y mecanismos) [18]. De la misma manera, el proceso de análisis de riesgos se desarrolla en las siguientes etapas: planificación, análisis de riesgos, gestión de riesgos y selección de salvaguardas [19].

Puntualmente, MAGERIT detalla la metodología desde los siguientes aspectos: describe los pasos para realizar un análisis del estado del riesgo a partir de analizar el impacto que puede tener una compañía víctima de la violación de la seguridad, identificar las amenazas que pueden llegar a afectar a la empresa y las vulnerabilidades de las cuales pueden aprovecharse las amenazas, a

continuación guía para gestionar la mitigación del riesgo, consiguiendo contar con una identificación más acertada de las medidas preventivas y correctivas más apropiadas.

Adicionalmente, determina las actividades primordiales para ejecutar un proyecto de análisis y gestión de riesgos y en uno de sus capítulos se aplica la metodología en un caso de desarrollo de Sistemas de Información (SI). Además, evidencia varios aspectos prácticos que emanan de la experiencia acumulada a lo largo del tiempo para el análisis y la gestión del riesgo de manera efectiva [20].

5. RESULTADOS

Al realizar la comparación de las metodologías propuestas se presenta la siguiente propuesta que tiene en cuenta los mejores aspectos de cada una de ellas y se presenta a continuación:

Tabla 1. Comparativo entre PMBOK, MARGERIT Y PHVA

	Metodologías de Riesgos evaluadas		
Criterio de comparación	**Project Management Institute PMBOK® para gestión de riesgos**	**MARGERIT**	**PHVA**
Definición de la metodología	La gestión de riesgos de proyecto por medio del proceso de identificación, análisis y respuesta a un riesgo, maximización de las consecuencias de los eventos positivos y la minimización de la ocurrencia de un evento negativo, permite anticipar problemas y oportunidades, asegurando el logro de metas de fechas, costos y alcance	El método MAGERIT tiene un doble objetivo, primero estudiar los riesgos que soporta un determinado sistema de información y el entorno asociable con él, entendiendo por riesgo la posibilidad de que suceda un daño o perjuicio; y segundo recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados.	PHVA (Planear, Hacer, Verificar, Actuar), por medio de una secuencia de actividades entrelazadas que le permitirá a cualquier organización involucrar la gestión del riesgo en la identificación y/o descripción de procesos en sus sistemas de gestión, realizando así una mejora continua en sus procesos.
Sector de aplicación	Todos, pero especialmente probado en proyectos de software, ingeniería y construcción.	Maneja una visión estratégica global sobre la Seguridad de los Sistemas de Información de las Administraciones Públicas.	Método de gestión se puede utilizar en cualquier tipo de empresa y se aplica principalmente para convertirlo procesos claros y ágiles para la gestión y medición de resultados.
Etapas de la gestión del riesgo	1. Gestión de riesgos y planificación. 2. Identificación de riesgos. 3. Análisis cualitativo del riesgo. 4. Análisis cuantitativo. 5. Planes de respuesta para riesgos. 6. Monitoreo y control de riesgos.	1. Definir el alcance de estudio. 2. Establecer los activos relevantes de la organización. 3. Determinar a qué vulnerabilidades y/o amenazas están expuestos esos activos. 4. Conocer cuáles son los planes de contingencia. 5. Conocer el impacto de presentarse una amenaza sobre el activo. 6. Tratar el riesgo de probabilidad de ocurrencia de esa amenaza.	1. Planificación de sus actividades basado en un enfoque de procesos con sus respectivos riesgos. 2. Ejecutar las actividades focalizando los procesos más críticos para la organización. 3. Controlar lo planificado contra lo realizado. 4. Mejora continua de los propios procesos de auditoria y las respectivas actividades.

Técnicas y herramientas para la identificación de los riesgos	• Revisiones de documentación. • Técnicas de recopilación de información. • Análisis mediante lista de control. • Análisis de asunciones. • Técnicas de diagramación.	• Técnicas específicas para el análisis de riesgos. • Técnicas generales. • Técnicas gráficas. • Sesiones de trabajo. • Valoración Delphi.	• Análisis de la información recabada del auditado. • Análisis de la información propia. • Simuladores (Generadores de datos). • Paquetes de auditoría (Generadores de programas).
Herramienta informática	No tienen un software propio para gestionar la metodología sin embargo se apoya en Project de Microsoft, así mismo se hacen presente el uso de varias herramientas informáticas.	Posee herramientas para el análisis de riesgo como PILAR, acrónimo de "Procedimiento Informático-Lógico para el Análisis de Riesgos" es una herramienta desarrollada bajo especificación del Centro Nacional de Inteligencia para soportar el análisis de riesgos de sistemas de información siguiendo la metodología Magerit.	No tienen un software propio para gestionar la metodología sin embargo se apoya en: • Software de auditoria multisitio. • Centros de competencia. • Snapshot. • Mapping. • Tracing y flujo grama de control. Software para SGSIEl Software ISOTools Excellence ISO-27001 para Riesgos y Seguridad de la Información.
Objetivos	La gestión de riesgos de proyecto por medio del proceso de identificación, análisis y respuesta a un riesgo, maximización de las consecuencias de los eventos positivos y la minimización de la ocurrencia de un evento negativo, permite anticipar problemas y oportunidades, asegurando el logro de metas de fechas, costos y alcance.	Concientizar sobre la existencia de los riesgos y de la necesidad de atajarlos a tiempo ofrecer un método sistemático para analizar los riesgos ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.	Siempre busca la optimización de las acciones por medio del análisis de: indicadores, logros obtenidos y programas de mejora ya implementados.

6. AGRADECIMIENTOS

Los autores agradecen las investigaciones previas realizadas en los grupos de investigación gracias a los aspectos publicados fue posible abordar las temática expuesta.

REFERENCIAS

[1] Bannerman, P. L. (2008). "Risk and risk management in software projects: a reassessment. Journal of Systems and Software", 81(12), 2118-2133. [Online]. Disponible en: http://dx.doi.org/10.1016/j.jss.2008.03.059.

[2] Pinna, C. C. A., & Carvalho, M. M. (2008). Gestão de escopo em projetos de aplicações web. Revista Produção OnLine, v. 8, n. 1, p. 1-8. [Online]. Disponible en: http://dx.doi.org/10.14488/1676- 1901.v8i1.25.

[3] Jiang, J. J., Klein, G., & Discenza, R. (2001). Information System Success as Impacted by Risks and Development Strategies IEEE. Transactions on Engineering Management, 48(1), 46-55. [Online]. Disponible en: http://dx.doi.org/10.1109/17.913165.

[4] Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) (2009, Jul, 30). "Normatividad - Ley 1341 30 de jul de 2009" [Online].

Disponible en: https://mintic.gov.co/portal/604/articles-8580_PDF_Ley_1341.pdf

[5] Presidencia de la República de Colombia (2012, Oct, 17). "Normativa de la Presidencia - Ley Estatutaria 1581 de 2012" [Online]. Disponible en: http://wsp.presidencia.gov.co/Normativa/Leyes/Documents/LEY%201581%20DEL%2017%20DE%20OCTUBRE%20DE%202012.pdf

[6] Alcaldía Mayor de Bogotá (2008, Dic, 31). "Compilación de Normatividad, Doctrina y Jurisprudencia - Ley Estatutaria 1266 de 2008" [Online]. Disponible en: http://www.alcaldiabogota.gov.co/sisjur /normas/Norma1.jsp?i=34488#0

[7] Alcaldía Mayor de Bogotá (2000, Jul, 27). "Compilación de Normatividad, Doctrina y Jurisprudencia - Ley 603 de 2000 Nivel Nacional" [Online]. Disponible en: https://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=13960&dt=S

[8] Observatorio de Transparencia y Anticorrupción (2014, Mar, 06). "Normatividad- Ley 1712 de 2017" [Online]. Disponible en: http://www.anticorrupcion.gov.co/SiteAssets/Paginas/Publicaciones/ley-1712.pdf

[9] Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC) (2013, Jun, 26). "Normatividad- Decreto 1377 de 2013" [Online]. Disponible en: https://www.mintic.gov.co/portal/inicio/4274:-Decreto-1377-de-2013

[10] PMI. Project Management Institute. INC. (2017) "Guía de los fundamentos para la dirección de proyectos- Guía del PMBOK". Sexta Edición.

[11] STRATEC (2013, Ago). "PHVA automatizado" [Online]. Disponible en: https://www.stratecsoluciones.com/blog/pdca-automatizado-2/

[12] ISO. (Dic, 2003). Orientación sobre el concepto y uso del "Enfoque basado en procesos" para los sistemas de gestión, Documento: ISO/TC 176/SC 2/N 544R2

[13] G.L. Idrobo Burbano y I. L. Jojoa López, "Proceso para gerenciar proyectos de pruebas de software en empresas especializadas de servicios de aseguramiento de la calidad de software" trabajo de fin de máster, Facultad de Ingeniería Departamento Académico de Tecnologías de Información y Comunicaciones, Maestría En Gestión Informática Y Telecomunicaciones, Universidad ICESI, Santiago de Cali, 2012.

[14] M. M. Pérez riquett y l. J. Plata silva, "Diseño de un modelo para el mejoramiento de la productividad y competitividad de la línea de comedor Houston en la empresa arte & estilo basado en la metodología lean seis sigma" Tesis de Ingeniería, Master en Ingeniería, Facultad de Ingeniería, Ingeniería Industrial, universidad de la costa CUC, barranquilla, 2013.

[15] Eficiente (2019, Ago, 22). "Medir para mejorar, la apuesta como valor diferencial de CP Grupo" [Online]. Disponible en: http://www.cpeficiente.com/medir-para-mejorar-la-apuesta-como-valor-diferencial-de-cp-grupo/

[16] Ministerio de Hacienda y Administraciones Públicas, "MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información", Madrid, NIPO: 630-12-171-8, 2012. [En línea]. Disponible en: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

[17] M. Juan. Planes de Contingencia: La Continuidad del Negocio en las Organizaciones, España: Ediciones Díaz de Santos, 2006.

[18] Ministerio de Admisiones Públicas, "Magerit Versión 2- Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información", Madrid, NIPO: 326-05-047-X, 2006. [En línea]. Disponible en: https://www.ar-tools.com/doc/magerit/v2/meth-es-v11.pdf

[19] Ministerio de Admisiones Públicas, "MAP- Metodología MAGERIT Versión 1.0- Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, Guía para responsables del dominio protegible", Madrid. [En línea]. Disponible en: http:// dis.um.es/~barzana/Curso03_04/MAGERIT.pdf

[20] Instituto nacional de tecnologías de la comunicación, "Guía Avanzada de Gestión de Riesgos" (2008, Diciembre), Madrid. [En línea]. Disponible en: https://docplayer.es/5994322-Guia-avanzada-de-gestion-de-riesgos-lncs.html