



POSGRADOS

MAESTRÍA EN ADMINISTRACIÓN DE EMPRESAS

RPC-SO-30-No.502-2019

OPCIÓN DE
TITULACIÓN:

PROPUESTAS METODOLÓGICAS Y TECNOLÓGICAS AVANZADAS

TEMA:

PROPUESTA DE UN MODELO DE GESTIÓN DE RIESGOS
PARA PROYECTOS DE DESARROLLO DE SOFTWARE
BAJO UNA METODOLOGÍA ÁGIL

AUTORES:

ERNESTO MAURICIO GARZÓN QUITO

DIRECTOR:

CÉSAR XAVIER AYALA SALGUERO

CUENCA - ECUADOR

2021

Autor:***Ernesto Mauricio Garzón Quito***

Ingeniero de Sistemas

Candidato a Magíster en Administración de Empresas, Mención en Gestión de Proyectos por la Universidad Politécnica Salesiana – Sede Cuenca.

egarzonq@est.ups.edu.ec

Dirigido por:***César Xavier Ayala Salguero***

Ingeniero de Sistemas

Magíster en Administración de Empresas, Universidad del Azuay

Candidato a Magíster en Dirección de Proyectos, Aden Business School

cayala@ups.edu.ec

Todos los derechos reservados.

Queda prohibida, salvo excepción prevista en la Ley, cualquier forma de reproducción, distribución, comunicación pública y transformación de esta obra para fines comerciales, sin contar con autorización de los titulares de propiedad intelectual. La infracción de los derechos mencionados puede ser constitutiva de delito contra la propiedad intelectual. Se permite la libre difusión de este texto con fines académicos investigativos por cualquier medio, con la debida notificación a los autores.

DERECHOS RESERVADOS

©2021 Universidad Politécnica Salesiana.

CUENCA – ECUADOR – SUDAMÉRICA

GARZÓN QUITO ERNESTO MAURICIO

PROPUESTA DE UN MODELO DE GESTIÓN DE RIESGOS PARA PROYECTOS DE DESARROLLO DE SOFTWARE BAJO UNA METODOLOGÍA ÁGIL.

RESUMEN

En el presente trabajo se elaboró una propuesta metodológica para gestionar riesgos dentro de proyectos de desarrollo de software bajo un entorno de trabajo ágil, cuya finalidad es mejorar la probabilidad de éxito de los proyectos, y en consecuencia el crecimiento de las organizaciones.

La metodología planteada consta de tres procesos genéricos que son la identificación, evaluación y respuesta a los riesgos, los cuales están esquematizados dentro del marco de trabajo Scrum, en donde a su vez se determinaron los eventos y artefactos en los cuales es fundamental realizar una adecuada y oportuna gestión de riesgos.

El modelo propone adicionalmente un tablero de control y monitoreo de riesgos, con la finalidad de que los interesados y equipo de proyecto tengan siempre la visibilidad del estado actual de los riesgos, lo cual facilitará sin duda la toma de decisiones a la hora de dar respuesta a los riesgos dentro de los proyectos.

Palabras clave: Modelo de gestión de riesgos, gestión de riesgo en proyectos de desarrollo de software, gestión ágil de riesgos.

ABSTRACT

In the presented work, a methodological proposal was elaborated to manage risks within software development projects under an agile work environment, the purpose of which is to improve the probability of success of the projects, and consequently the growth of the organizations.

The proposed methodology consists of three generic processes which are the identification, evaluation and response to risks, which are schematized within the Scrum framework, where the events and artifacts in which it is fundamental to carry out adequate and timely risk management were determined.

The model additionally proposes a control panel and risk monitoring dashboard, with the goal that those interested as well as the project team always have the visibility over the current state of the risks, which will undoubtedly facilitate decision making when responding to risks within the projects.

Keywords: Risk management model, risk management in software development projects, fast risks management.

Tabla de Contenidos

CAPITULO I: INTRODUCCIÓN	10
1.1. Situación Problemática. Antecedentes	10
1.2. Formulación del Problema	13
1.3. Justificación.....	16
1.4. Objetivo General	17
1.5. Objetivos Específicos	17
CAPITULO II: MARCO TEÓRICO	18
2.1. Conceptos Generales	18
2.2. Marco de Trabajo Scrum.....	25
2.3. Metodologías de Gestión de Riesgos	34
2.3.1. Gestión de Riesgos bajo el Marco de Trabajo CCMI.....	35
2.3.2. Metodología CRAMM: (Risk Analysis and Management Method)	38
2.3.3. Marco de Referencia ISO 31000-2018:.....	39
2.3.4. Guía PMBOK – Dominio de desempeño de la Incertidumbre.....	44
CAPITULO III: METODOLOGÍA	57
3.1. Unidad de Análisis	58
3.2. Población.....	58
3.3. Tamaño de la muestra	58
3.4. Selección de la muestra	59
3.5. Métodos a emplear	60
3.6. Identificación de las necesidades de información. Fuentes primarias y secundarias.	61
3.7. Técnicas de recolección de datos	62
3.8. Herramientas utilizadas para el análisis e interpretación de la información	62
CAPITULO IV: RESULTADOS Y DISCUSIÓN	63
4.1. Análisis, Interpretación y discusión de resultados	63
4.1.1. Fiabilidad de la encuesta.....	63
4.1.2. Análisis y resultados de la encuesta	64
4.1.3. Análisis comparativo de metodologías existentes	77
4.2. Propuesta Metodológica.....	82
4.2.1. Estructura planteada	82
4.2.2. Puntos de gestión de riesgos dentro Scrum	84

4.2.3. Procedimiento de gestión de riesgos con Scrum	84
4.2.4. Cuadro de mando para control y monitoreo de riesgos	86
4.2.5. Premisas o Supuestos.....	87
4.2.6. Objetivo de la propuesta metodológica	88
4.2.7. Objeto de la propuesta	88
4.2.8. Responsables de la implementación y control.....	88
4.2.9. Fases para su puesta en práctica	89
4.2.10. Indicadores de evaluación.	89
CONCLUSIONES	91
RECOMENDACIONES.....	92
AGRADECIMIENTOS	93
REFERENCIAS BIBLIOGRÁFICAS.....	94
ANEXOS	96

Lista de tablas

Tabla 1 Modelos, Métodos y Artefactos Dominio de desempeño de la Incertidumbre	48
Tabla 2 Área de Conocimiento Gestión de los Riesgos del Proyecto.....	49
Tabla 3 Estrategias para dar respuesta a los riesgos	54
Tabla 4 Valores Z y e, para muestreo aleatorio simple sin conocer el tamaño de la población. ..	59
Tabla 5 Contraste tamaño de empresas vs giro de negocio	65
Tabla 6 Nivel de Complejidad de Proyectos vs Percepción de la Importancia de gestionar los riesgos	68
Tabla 7 Nivel de Complejidad de Proyectos vs nivel de conformidad del tiempo invertido para gestionar los riesgos.....	70
Tabla 8 ¿En su empresa se aplica alguna de las siguientes metodologías y/o normas para la gestión de riesgos en los proyectos de desarrollo de software?	74
Tabla 9 Metodologías de gestión de riesgos seleccionadas	78
Tabla 10 Comparación Metodologías de Riesgos según su propósito y estructura.....	79
Tabla 11 Ventajas y Desventajas modelos de Gestión de Riesgos	81
Tabla 12 Descripción de Actividades de gestión de Riesgos dentro de Scrum	85

Lista de figuras

Figura 1 Resultado Proyectos	10
Figura 2 Resultado Proyectos Según Metodología utilizada	12
Figura 3 Razones para no adoptar una metodología de gestión de riesgos	13
Figura 4 Principales causas que provocaron el fracaso en sus proyectos	14
Figura 5 Árbol de problemas	16
Figura 6 Pilares de Scrum	26
Figura 7 Valores de Scrum	27
Figura 8 Roles de Scrum.....	28
Figura 9 Eventos de Scrum	30
Figura 10 Artefactos de Scrum	31
Figura 11 Descripción proceso de Scrum	33
Figura 12 Practicas Gestión de Riesgos según CMMI	36
Figura 13 Fases de la metodología CRAMM	38
Figura 14 Principios, marco de referencia y proceso.....	40
Figura 15 Principios ISO 31000-2018	41
Figura 16 Marco de referencia ISO 31000-2018	42
Figura 17 Proceso ISO 31000-2018.....	44
Figura 18 Relación entre los principios de la dirección de proyectos y los dominios de desempeño del proyecto.....	45
Figura 19 Entorno VUCA.....	46
Figura 20 Aspectos que pueden ser adaptados según la naturaleza de los proyectos.....	47
Figura 21 Entradas, herramientas, técnicas, y salidas para Planificar la Gestión de los Riesgos. 50	
Figura 22 Entradas, herramientas, técnicas, y salidas para Identificar los Riesgos.....	51
Figura 23 Entradas, herramientas, técnicas, y salidas para Realizar el Análisis Cualitativo de Riesgos.....	52
Figura 24 Entradas, herramientas, técnicas, y salidas para Realizar el Análisis Cuantitativo de Riesgos.....	53
Figura 25 Entradas, herramientas, técnicas, y salidas para Planificar la Respuesta a los Riesgos.	55
Figura 26 Entradas, herramientas, técnicas, y salidas para Implementar la Respuesta a los Riesgos.	56
Figura 27 Entradas, herramientas, técnicas, y salidas para Monitorear los Riesgos.	56
Figura 28 Fases metodología de trabajo	57
Figura 29 Resultado prueba de fiabilidad de Alta de Cronbach	63
Figura 30 ¿Con cuántos empleados cuenta la empresa en la que actualmente presta sus servicios?	64
Figura 31 ¿Qué rol usted desempeña dentro de los proyectos de desarrollo de software de su empresa?	65
Figura 32, ¿Qué nivel de complejidad usted considera que tuvieron los proyectos que se ejecutaron en su empresa en los últimos 12 meses?.....	66
Figura 33 Nivel de Complejidad Alta de Proyectos vs Percepción de la Importancia de gestionar los riesgos.....	67

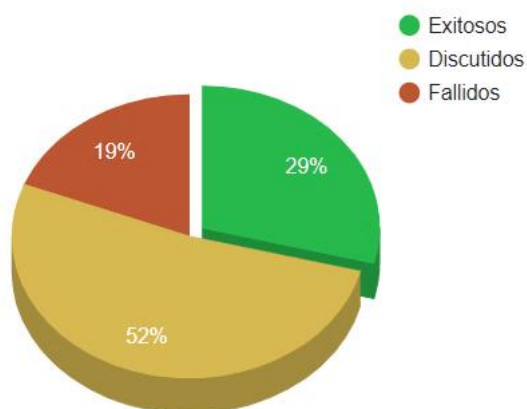
Figura 34 Nivel de Complejidad de Proyectos Muy Alta, y Alta vs nivel de conformidad del tiempo invertido para gestionar los riesgos.....	69
Figura 35 En su experiencia, ¿Qué se debe mejorar o fortalecer para una adecuada gestión de riesgos en los proyectos de desarrollo de software de su empresa?	71
Figura 36 ¿En su empresa al momento de abordar un nuevo Proyecto de desarrollo de Software, se aseguran de cumplir con alguna metodología para gestionar los riesgos?	72
Figura 37 Sector de las empresas en las que trabajan los encuestas que siempre y casi siempre utilizan una metodología para gestionar los riesgos dentro de los proyectos de desarrollo de software.....	73
Figura 38 ¿En qué medida considera usted que es necesario adoptar una metodología ágil para la gestión de riesgos en los proyectos de desarrollo de software de su empresa?	75
Figura 39 ¿Qué factor considera usted que es el principal limitante para no adoptar una metodología de gestión de riesgos en sus proyectos de desarrollo de software?.....	75
Figura 40 Contraste de preguntas de necesidad de implementar una metodología versus las limitaciones.	76
Figura 41 ¿A su criterio, en qué medida afectó No gestionar oportunamente los riesgos en los últimos proyectos de desarrollo de software de su empresa?	77
Figura 42 Estructura propuesta para la gestión de riesgos en proyectos de desarrollo de Software	82
Figura 43 Identificación de puntos o eventos en donde se debe gestionar los riesgos.	84
Figura 44 Tablero de control y monitoreo de riesgos	86

CAPITULO I: INTRODUCCIÓN

1.1. Situación Problemática. Antecedentes

La constante evolución tecnológica e innovación son dos factores decisivos que las empresas de cualquier tipo deben considerar para competir con productos y servicios de acorde a las necesidades y la exigente demanda actual de los mercados y usuarios de hoy en día, en este punto los proyectos de desarrollo de software juegan un papel primordial para atender con soluciones personalizadas a cualquier línea de negocio. Según Standish Group Internacional, que es una organización internacional independiente de tecnología de la información especialista en software de misión crítica, en su informe Chaos del año 2015, presenta el resultado de estudio de 50 mil proyectos de tecnología de todo el mundo, de dicho universo el 29% de los proyectos culminaron con éxito, el 19% proyectos fueron proyectos fallidos, mientras que el 52% fueron proyectos sobre los cuales hay dudas sobre su éxito o fracaso (Gómez, 2016).

Figura 1 Resultado Proyectos



Fuente: Tomada del portal el laboratorio de las TI

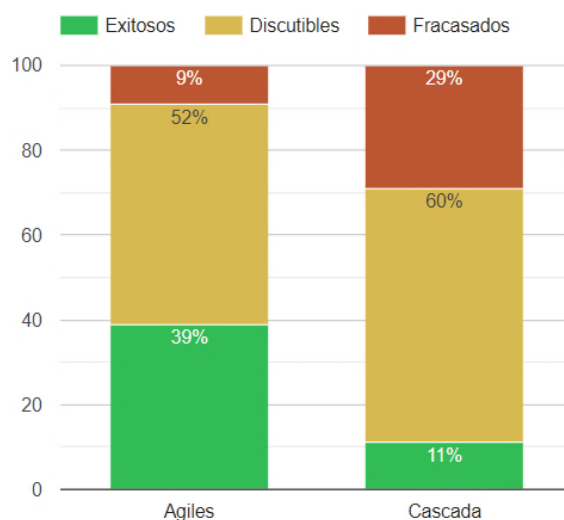
En tal virtud, aunque no se puede especificar una por una las razones del éxito o fracaso de cada uno de los proyectos del estudio en mención, se puede deducir en términos generales que existen

eventos y condiciones dentro de los proyectos de desarrollo de software, que sin duda impactan ya sea en el éxito o fracaso de los mismos, según Project Management Institute (PMI) en su libro Project Management Body of Knowledge (PMBOK), estos eventos pueden ser riesgos individuales que, si se producen en los proyectos, tienen un efecto positivo o negativo en uno o más objetivos del proyecto (PMI, 2017).

Por otro lado, según las mejores prácticas, dirigida al control y supervisión de tecnología de la información COBIT por sus siglas en inglés Control Objectives for Information and related Technology define al riesgo como cualquier amenaza sobre las metas u objetivos de la organización, causado por un evento no planificado (ISACA, 2012).

Otro resultado importante dentro del informe de Standish Group International hace referencia al éxito o fracaso de los proyectos en función de la metodología utilizada para el desarrollo del software, comparando así las metodologías tradicionales versus las metodologías ágiles en donde se concluye que del 100% de proyectos que utilizaron un metodología ágil el 39% de ellos fueron proyectos exitosos, por su parte del 100% de proyectos que utilizaron una metodología tradicional(Cascada), el 11% fueron proyectos exitosos, dando la pauta para inferir que los proyectos de desarrollo de software que utilizan una metodología ágil tienen una mayor probabilidad de éxito, sin embargo de acuerdo al mismo análisis la brecha de proyectos fracasados más los proyectos en discusión superan en los dos casos el 50%, lo cual advierte que es necesario gestionar los eventos positivos y/o negativos que suceden dentro de los proyectos ya sean estos de carácter técnico u organizacional.

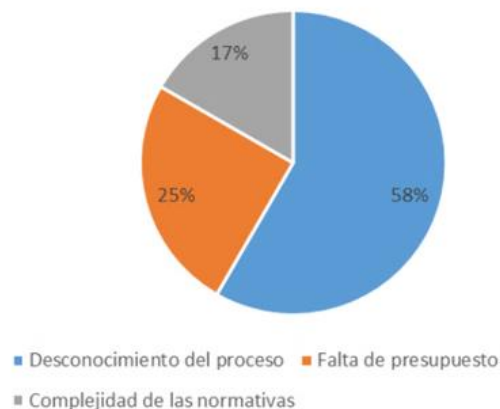
Figura 2 Resultado Proyectos Según Metodología utilizada



Fuente: Tomada del portal el laboratorio de las TI

Por otro lado, según la revista Enfoque de la Universidad UTE en su artículo “Ecu@Risk, Una metodología para la gestión de Riesgos aplicada a las MPYMEs” (Martinez, 2017), en donde se realizó una encuesta a 50 empresas de la región austral del Ecuador para determinar las razones por las que no se adopta un modelo de gestión de riesgo de información, que aunque no está enfocada específicamente a la gestión de riesgos en el desarrollo de software, proporciona la pauta para determinar el nivel de importancia y aplicabilidad en cuestión de riesgos que actualmente tienen las empresas de la zona, es así que del total de encuestados, el 58% manifiesta desconocer el proceso de gestión de riesgos, el 17% manifiesta la complejidad de las normativa ISO para la gestión de riesgos, y el 25% en la falta de presupuesto,

Figura 3 Razones para no adoptar una metodología de gestión de riesgos



Fuente: Tomada de la revista *EnfoqueUTE*

1.2. Formulación del Problema

Las empresas de desarrollo de software y las áreas de ID+i dentro de las diferentes industrias enfrentan retos importantes en referencia a la entrega temprana de productos y servicios de software que cumplan con los requisitos de calidad de los clientes bajo las restricciones de los proyectos, lo cual implica adoptar y estar en una constante evolución y aplicación de metodologías ágiles de desarrollo de software que les permitan agilizar sus procesos de construcción, para así aumentar la tasa de cumplimiento de sus proyectos, por lo tanto es importante en este punto considerar todo tipo de riesgo potencial que afecte al proyecto, para ello de acuerdo a lo planteado por el estándar para la administración del riesgo en proyectos, programas y portafolios del PMI es fundamental apoyarse en una estructura de desglose del riesgo o RBS (Risk Breakdown Structure) que es un marco jerárquico de fuentes de riesgos potenciales que contempla al menos los riesgos de tipo técnico, administrativos, comerciales y riesgos externos (PMI, 2019), que sin duda impactan en el cumplimiento de las actividades planificadas afectando comúnmente las principales aristas de un proyecto como lo son el alcance, el tiempo, el costo, la calidad y satisfacción del

cliente, lo que a su vez trasciende en pérdidas financieras, degradación de imagen reputacional, o acciones legales que afectan a las instituciones.

En base a un estudio realizado por el PMI, en su revista “pulse of the profession” en su edición del año 2018 se realizó una encuesta a 4.455 profesionales de dirección de proyectos, de una diversidad de sectores, que incluyen gobierno, tecnologías de la información (TI), telecomunicaciones, energía, manufactura, asistencia sanitaria y construcción. Los encuestados pertenecen a las regiones de América del Norte, Asia y el Pacífico, Europa, Medio Oriente y África (EMEA), América Latina y el Caribe, en donde se preguntó cuáles son las principales causas que provocaron el fracaso en sus proyectos iniciados en los últimos 12 meses. De esta encuesta, como se puede observar en la siguiente figura, el 29% coinciden en no haber definido las oportunidades o riesgos de los proyectos (PMI, 2018).

Figura 4 Principales causas que provocaron el fracaso en sus proyectos



Fuente: Tomado de Pulse of the Profession 2018

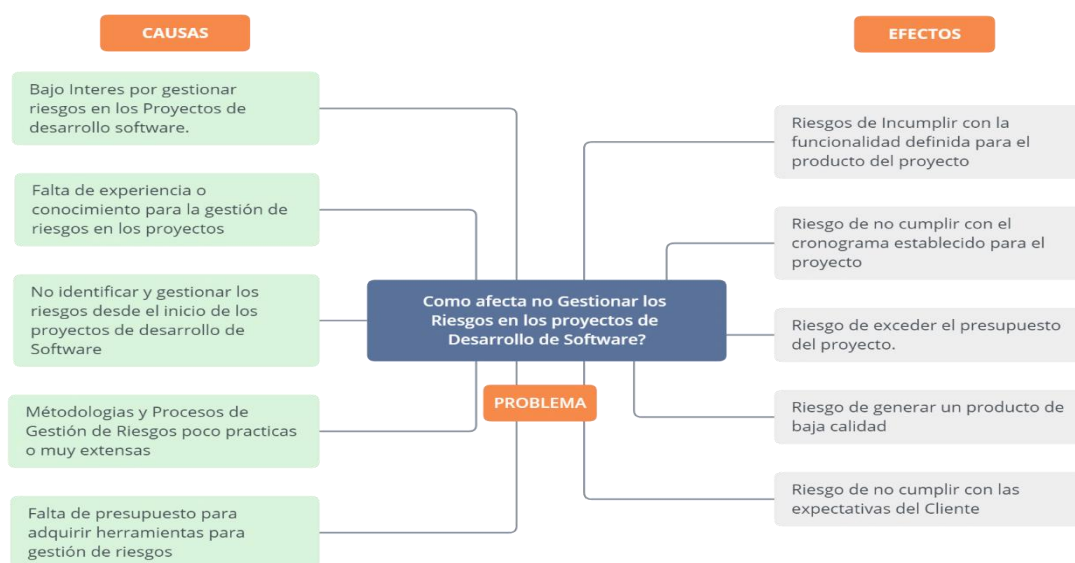
En este contexto y en base a estadísticas reales un factor que no se puede dejar de considerar en la ejecución de los proyectos de desarrollo de software es la gestión de riesgos, para lo cual existen en el mercado varios métodos estándar y procesos formales, entre los más populares se pueden mencionar la metodología creada por el PMI, que contiene un área de conocimiento específica para la gestión de riesgos en los proyecto, o el estándar ISO 31000:2018 que tiene el objetivo de integrar, diseñar, implementar, valorar y mejorar la gestión del riesgo a lo largo de las organizaciones. (Organización Internacional de Normalización 31000, 2018).

En consecuencia, las variables pertinentes para evaluar los riesgos de un proyecto deben diseñarse sobre la base de los requisitos del proyecto y la situación real de la empresa. (Wong, Kwai, & Tang, 2010)

Por su parte, según artículo titulado “Metodología Ágil para la Gestión de Riesgos Informáticos”, de la revista Killkana Técnica, presenta una metodología integral para la gestión de riesgos informáticos basándose en los estándares mundialmente aceptados como son ISO 31000 e ISO/IEC 27005, los mismos que indican los requerimientos para una gestión adecuada de riesgos; sin embargo, no indican, al menos de manera clara, como se puede realizar dicha gestión. (Arévalo et al, 2017) , así mismo un trabajo previo de (Buitrago, 2014), realiza un análisis descriptivo de las metodologías CCMI, Microsoft Solutions Framework, Rational Unified Process (RUP), Norma ISO 31000 y concluye con una discusión para definir los riesgos más comunes de su empresa dentro de la fase de desarrollo de software, pero no trasciende al uso general de gestión de riesgos en el ciclo de desarrollo de software.

En la siguiente figura 5, se ilustran las principales causas y efectos identificados dentro del presente estudio en torno al problema de no gestionar los riesgos en los proyectos de desarrollo de software.

Figura 5 Árbol de problemas



Fuente: Investigación propia elaborada por el autor

1.3. Justificación

El presente trabajo se enfoca en determinar los principales obstáculos y dificultades que tienen los profesionales de tecnología de la información a la hora de gestionar los riesgos dentro de un proceso ágil de desarrollo de software, así como también realizar un estudio comparativo basándose en los principales estándares y métodos de gestión de riesgos existentes en el mercado de los cuales se toman los conceptos más importantes, buenas prácticas, y se realizan adaptaciones y especificaciones pertinentes para proporcionar un método más específico que se pueda aplicar de una forma integral, natural y simple dentro del ciclo de vida del desarrollo de software en un contexto de agilidad, utilizando como base el marco de referencia Scrum de tal forma que el modelo propuesto tenga la flexibilidad de adaptarse al entorno de las organizaciones y a las necesidades de los equipos de trabajo de desarrollo de software con la intención de introducir o fortalecer una cultura de control de riesgos en proyectos de desarrollo de software que aporte a la

probabilidad de éxito de los proyectos, lo cual a su vez se convierte en beneficios financieros, técnicos y estratégicos de las organizaciones.

El modelo propuesto cuenta con herramientas que permiten llevar el registro y control de los riesgos a los que están expuestos los diferentes proyectos de desarrollo de software con la finalidad de que estos sean debidamente comunicados tanto a nivel de equipos de trabajo, así como a patrocinadores y altas gerencias involucradas, para de esta manera establecer planes de acción, ya sean preventivos y/o correctivos que permitan reducir, mitigar, transferir o eliminar la probabilidad de ocurrencia de eventos negativos que desvíen los objetivos de los proyectos de desarrollo de software.

1.4. Objetivo General

Proponer un modelo de gestión de riesgos específico para proyectos de desarrollo de software bajo una metodología ágil con la finalidad de que las empresas que así lo deseen puedan gestionar oportunamente cualquier evento que pueda afectar los objetivos de los proyectos.

1.5. Objetivos Específicos

1. Identificar las principales razones y dificultades por las cuales las organizaciones de nuestro medio, no gestionan los riesgos dentro de los proyectos de desarrollo de software.
2. Identificar ventajas y desventajas de métodos o marcos de referencia de gestión de riesgos existentes más utilizados.
3. Crear procedimientos, procesos y plantillas necesarios para la gestión ágil de riesgos en los proyectos de desarrollo de software.
4. Implementar un cuadro de mando para el monitoreo y control de los riesgos más comunes dentro de proyectos de construcción de software.

CAPITULO II: MARCO TEÓRICO

Para el planteamiento y creación de un modelo, es necesario apoyarse en conceptos sobre gestión de proyectos, ingeniería de software, metodologías ágiles, gestión de riesgos, y demás teorías relacionadas al objetivo de estudio las cuales se describen a continuación.

2.1. Conceptos Generales

A continuación, se describen los conceptos netamente necesarios y claves para el desarrollo del presente trabajo de investigación y propuesta metodológica.

Proyecto:

Cuando se escucha la palabra proyecto, la misma dicta un sentido de hacer algo nuevo para alcanzar un objetivo específico, o a su vez hacer cambios o mejoras importantes en algo existente para optimizar o alcanzar nuevos o mejores beneficios, todo esto enmarcado en las preguntas de, ¿Cuánto me costará?, y ¿Qué tiempo tomará?. Bajo esta realidad podemos aducir que un proyecto nunca es igual a otro pues siempre estarán presentes principalmente las restricciones de alcance, tiempo, y costo, y a su vez dependerá de su naturaleza, equipo de trabajo, riesgos, calidad, y una diversidad de factores ambientales de las empresas o instituciones en las que se desarrollará el proyecto. Según el Instituto de Administración de Proyectos por sus siglas en inglés PMI, un proyecto se puede definir como: “Un proyecto es un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único” (PMI, 2017).

Por su parte, PRINCE2, que es un estándar para la gestión de proyectos en varios países de Europa, especialmente del Reino Unido, define a un proyecto como: “una organización temporal que se

crea con el propósito de entregar uno o más productos comerciales de acuerdo a un Business Case convenido” (Turley, 2010) .

Como podemos notar en las definiciones anteriores, se menciona un punto importante de temporalidad, y de entrega de productos, de ahí y como una primera aproximación al tema de estudio del presente trabajo, se puede concluir que un proyecto, independientemente de su naturaleza y/o restricciones o suposiciones, siempre tiene el riesgo de fracasar o ser exitoso, en tal virtud es de suma importancia gestionar dichos riesgos desde el mismo instante en que nace el proyecto.

Gestión:

De acuerdo a la definición de la real academia de la lengua española en su actualización 2020 se define gestión como: “Ocuparse de la administración, organización y funcionamiento de una empresa, actividad económica u organismo”, trasladando este concepto general al ámbito práctico de proyectos de desarrollo de software se podría decir que la gestión en sí, son las diferentes actividades y/o diligencias que debe ejecutar el equipo de trabajo para el logro de los objetivos de un proyecto específico.

Gestión de Proyectos:

Una vez definido que es un proyecto, y teniendo presente el concepto de gestión, podemos unir estas dos definiciones para referir que la gestión de proyectos está dirigida o tiene la finalidad de hacer que se cumplan las actividades específicas de principio a fin para así alcanzar los objetivos preestablecidos de un proyecto y entrega de beneficios a una empresa. El PMI por su parte presenta el símil a la gestión de proyectos enfocándose a la administración o dirección de

proyectos, lo cual define como: “La dirección de proyectos es la aplicación de conocimientos, habilidades, herramientas y técnicas a las actividades del proyecto para cumplir con los requisitos del mismo” (PMI, 2017).

En concordancia con lo expuesto, la gestión de proyectos implica la supervisión de equipos de trabajo que se espera que trabajen conjuntamente durante o parte de la duración del proyecto para alcanzar un objetivo común, de ahí el reto de los directores o gerentes de proyecto para coordinar de una manera efectiva las diferentes aristas de un proyecto como alcance, tiempos, costos, riesgos, calidad y demás factores para poder entregar un proyecto exitoso.

Stakeholder (Interesados)

Por el hecho que los proyectos siempre se dan o existen dentro de un entorno cualquiera que este sea, los mismos están relacionados con personas, clientes, empleados, socios y demás sujetos que tienen un interés particular en el resultado del proyecto a lo que se le llama interesado o en inglés stakeholder. Según la guía PMBOK en su versión 6, se define como: “individuo, grupo u organización que puede afectar, verse afectado o percibirse a sí mismo como afectado por una decisión, actividad o resultado de un proyecto, programa o portafolio” (PMI, 2017).

Metodología Ágil:

Se puede definir una metodología ágil como un conjunto de procesos y tareas para gestionar proyectos cuya finalidad es, en esencia, incorporar cambios de un manera rápida y flexible para entregar en períodos cortos de tiempo partes de un software funcionando, satisfaciendo así las necesidades de los clientes. Este concepto está basado en el desarrollo iterativo e incremental en donde los requerimientos van madurando y entregándose en el tiempo de acuerdo a las necesidades

del proyecto. En la actualidad existen una variedad de metodologías ágiles, entre las más conocidas se puede mencionar a: Programación Extrema (XP), Scrum, Kanban; todas estas cumplen con el manifiesto ágil el cual consta de 12 principios agrupados en cuatro valores fundamentales:

1. Individuos e interacciones sobre procesos y herramientas.
2. Software funcionando sobre documentación extensiva.
3. Colaboración con el cliente sobre negociación contractual.
4. Respuesta ante el cambio sobre seguir un plan.

Historia de Usuario:

De acuerdo a Alaimo:

Los clientes o especialistas de negocio se comunican con los equipos de desarrollo a través de extensos documentos conocidos como especificaciones funcionales. A su vez, las especificaciones funcionales son la documentación de supuestos y están sujetas a interpretaciones, lo que causa malos entendidos y que finalmente el software construido no se corresponda con la realidad esperada (2013, p.87).

En respuesta a esta complejidad nace el concepto de historia de usuario, que dicho en palabras simples es una representación de un requisito del usuario en forma escrita bajo un lenguaje propio del usuario. Un formato común para redactar una historia de usuario en la práctica, es que se describa el rol, la funcionalidad requerida y el beneficio que se espera alcanzar, ejemplo: Como (Rol) Necesito (funcionalidad) Para (beneficio).

Riesgo:

Partiendo de un concepto básico dado por la Real Academia de la Lengua Española, en su actualización 2020, en donde define al riesgo como “contingencia o proximidad de un daño”, en donde, a su vez, contingencia se define como la “posibilidad de que algo suceda o no suceda”. Ante esta definición, y en un contexto práctico, se puede decir que un riesgo es un evento imprevisto que puede o no suceder afectando o beneficiando los objetivos de un proyecto. Desde este punto de vista, el riesgo es un factor muy importante a considerar sobre todo en el ámbito de desarrollo de software en donde generalmente existen varias aristas internas y externas que pueden afectar la conclusión de los objetivos.

Por su parte, el PMI, define al riesgo como "un evento o una condición de inciertos que, si ocurren, tienen un efecto positivo o negativo en uno o más de los objetivos de un proyecto" (PMI, 2017).

Otro concepto de riesgo interesante se puede encontrar en la norma ISO 31000:2018, en donde se define al riesgo como el “efecto de la incertidumbre sobre los objetivos” y un efecto es una desviación respecto a lo previsto, la cual puede ser positiva, negativa, o ambas, lo cual a su vez puede resultar en oportunidades y amenazas (Organización Internacional de Normalización 31000, 2018).

Amenazas:

De la forma más general se puede definir una amenaza como un evento externo que puede poner en peligro a alguien o a algo, según la norma Margerit v3.0 menciona que la amenaza es el “Causal potencial de un incidente que puede causar daños a un sistema de información o a una organización” (Ministerio de Hacienda y Administraciones Públicas, 2012).

Así mismo, según la guía PMBOK v7 define la amenaza como: “Evento o condición que, si se produce, tiene un impacto negativo en uno o más de los objetivos” (PMI, 2021).

Oportunidades:

De acuerdo a la Guía PMBOK v7, define la oportunidad como: “Evento o condición que, si se produce, tiene un impacto positivo sobre uno o más de los objetivos de un proyecto” (PMI, 2021).

Vulnerabilidad:

De acuerdo a la norma Magerit v3.0, “se denomina vulnerabilidad a toda debilidad que puede ser aprovechada por una amenaza; o más detalladamente, a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial” (Ministerio de Hacienda y Administraciones Públicas, 2012).

Impacto:

El impacto son las consecuencias que se pueden llegar a presentar si un riesgo se materializa, en consecuencia, es un indicador de qué puede suceder cuando ocurren las amenazas, siendo la medida del daño causado por una amenaza cuando se materializa sobre un activo (Miranda, 2015).

Probabilidad:

La probabilidad es la posibilidad de que un riesgo se materialice en el tiempo, de acuerdo a la norma ISO 31000-2018:

En la terminología de administración/gestión de riesgos, la palabra “probabilidad” se utiliza para indicar la posibilidad de que algo suceda, esté definida, medida o determinada objetiva o subjetivamente, cualitativa o cuantitativamente, y descrita utilizando términos generales o matemáticos (como una probabilidad matemática o una frecuencia en un periodo de tiempo determinado) (2018, p.2).

Gestión del Riesgo:

Bajo los conceptos de riesgo y gestión que se dieron por separado en los párrafos anteriores, nos podemos referir en términos generales a la gestión de riesgos como una serie de actividades que buscan manejar adecuadamente los riesgos. Según la norma ISO 31000:2018, define la gestión de riesgos como: “actividades coordinadas para dirigir y controlar la organización con relación al riesgo”, (Organización Internacional de Normalización 31000, 2018) de aquí la necesidad e importancia de contar con un marco de trabajo para poder identificar, analizar y controlar los riesgos para lograr los objetivos de una manera eficaz.

Gestión de Riesgos de un Proyecto:

De una manera más específica en el contexto de desarrollo de software, es importante entonces tener presente que la gestión de riesgos debe enfocarse en buscar, de manera estructurada y ordenada, las diferentes actividades que se deben ejecutar para manejar los riesgos dentro del ciclo de vida de desarrollo, esto con el objetivo de minimizar la probabilidad de que los riesgos se vuelvan un problema que afecte al proyecto.

Según el PMI:

Los objetivos de la gestión de los riesgos del proyecto son 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 (2017, p.395).

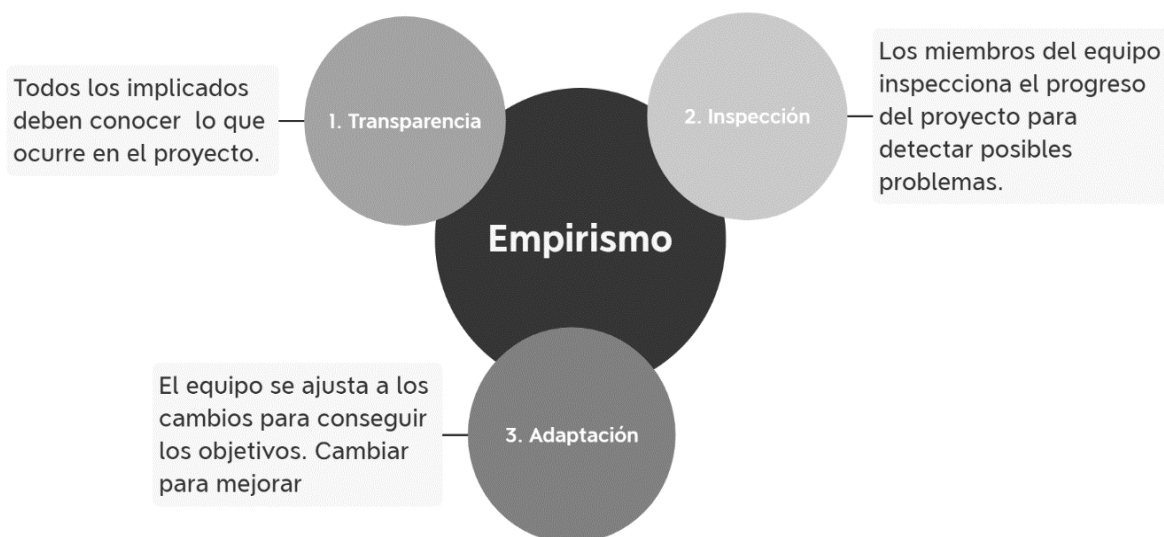
2.2. Marco de Trabajo Scrum

Scrum es un marco de trabajo que se adapta al tipo de proyecto, es decir Scrum se puede aplicar de diferente forma de una empresa a otra, o de un proyecto a otro. Scrum es aplicado en su mayoría para el desarrollo de proyectos tecnológicos y más específicamente en proyectos desarrollo de software, su propósito es justamente crear un marco de trabajo para que las personas puedan abordar y ejecutar problemas y proyectos de una alta complejidad, todo basado en un equipo Scrum con sus roles, eventos, artefactos y reglas asociadas, con la finalidad de generar entregas tempranas que agreguen valor a los objetivos buscados en los proyectos.

2.2.1. Pilares de Scrum

Scrum se basa en el concepto de empirismo es decir en el conocimiento que procede de la experiencia lo cual esta a su vez esta soportado por 3 pilares que son la transparencia, la inspección y la adaptación lo cual se resumen en la siguiente figura 6:

Figura 6 Pilares de Scrum



Fuente: Figura basada en la guía definitiva de Scrum: “Las reglas del juego” (Schwaber & Sutherland, 2017)

2.2.2. Valores de Scrum

Para que Scrum tenga éxito es necesario que el equipo scrum se consolide conforme vaya trabajando en el proyecto; en este punto, los cinco valores propuestos por scrum ayudan a modular las decisiones del equipo. Es así que el valor “foco” permite que el equipo se centre en el trabajo y en las metas del equipo scrum, el “coraje” ayuda para que las cosas se hagan bien sobre todo al afrontar problemas complejos; así mismo el equipo scrum y de sus interesados acuerdan tener la “apertura” para lograr todo el trabajo y los desafíos que se les presente en el camino, todo esto bajo el “compromiso” y “respeto” entre cada uno de los miembros del equipo scrum. A continuación, se presenta la figura 7 en donde consta un resumen de los valores scrum.

Figura 7 Valores de Scrum



Fuente: Figura basada en la guía definitiva de Scrum: “Las reglas del juego” (Schwaber & Sutherland, 2017)

2.2.3. Equipo Scrum

Los equipos scrum están diseñados para optimizar la flexibilidad, la creatividad y la productividad con el fin de entregar productos de forma iterativa e incremental para asegurar que siempre esté disponible una versión potencialmente útil y funcional del producto. Para ello es necesario que el equipo scrum sea autoorganizado es decir que los miembros del equipo no requieran o dependan de la dirección de una persona externa al equipo, sino más bien que lleven su trabajo de una forma autónoma, ordenada y proactiva. Adicional el equipo scrum debe ser multifuncional lo que facilita llevar a cabo el trabajo sin depender de competencias de otras personas que no son parte del equipo.

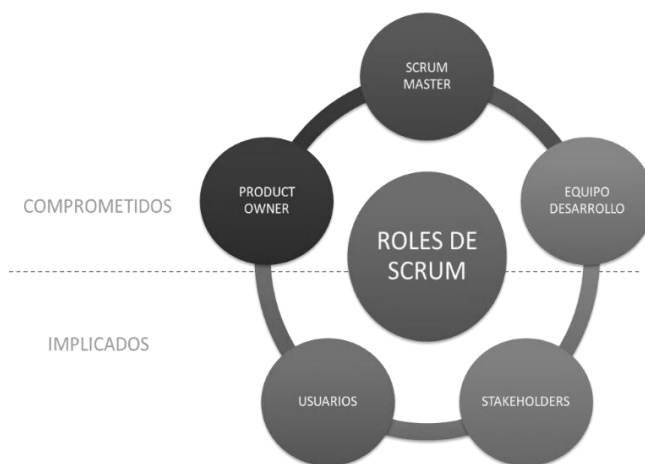
2.2.4. Roles de Scrum

Dentro de scrum hay dos grupos de personas: los comprometidos y los implicados los cuales intervienen de forma directa o indirecta dentro de los proyectos.

Para entender de una mejor manera estos dos grupos en varios artículos y libros en donde se explican los roles de scrum se hace referencia a la metáfora de la gallina y el cerdo que cuenta que una gallina y un cerdo paseaban por la carretera, cuando la gallina le preguntó al cerdo: “¿Quieres abrir un restaurante conmigo?”, a lo que el cerdo consideró la propuesta y respondió: “Sí, me gustaría. ¿Y cómo lo llamaríamos?”, la gallina respondió: “huevos con jamón”, entonces el cerdo se detuvo, hizo una pausa y contestó: “Pensándolo mejor, creo que no voy a abrir un restaurante contigo, porque Yo estaría realmente comprometido, mientras que tu estarías sólo implicada” (Palacio, 2008).

En la siguiente figura 8 se presentan los roles de scrum de acuerdo a estos dos grupos mencionados en el párrafo anterior:

Figura 8 Roles de Scrum



Fuente: Figura basada en la guía definitiva de Scrum: “Las reglas del juego” (Schwaber & Sutherland, 2017)

Comprometidos. - Personas que forman parte del Equipo y proceso Scrum

- Product Owner: El propietario del producto es quien conoce el negocio y posee la visión sobre el producto, se encarga de interpretar las ideas del cliente, ordenarlas y priorizarlas para agregar valor al producto.
- Scrum Master: Es el responsable de comprobar que el modelo y la metodología se cumpla asegurando siempre que la organización entiende y que se trabaja conforme a lo establecido en las reglas de scrum. Es además quien se encarga de eliminar cualquier obstáculo que exista en medio el proceso, siendo el nexo entre el equipo de desarrollo y el dueño del producto.
- Equipo de Desarrollo: Está conformado por profesionales autoorganizados y multifuncionales que tienen un mismo propósito bajo un espíritu de colaboración y solidaridad entre sí. La principal responsabilidad del equipo es entregar un incremento del producto que potencialmente se pueda poner en producción al final de cada Sprint. Es recomendable que un equipo scrum este conformado entre 3 a 9 personas, ya que resulta más sencilla la comunicación directa entre los miembros, evitando así problemas que habitualmente se empiezan a presentar en equipos de más de 6 personas.

Implicados. - Personas que no forman parte del proceso scrum, pero se les debe considerar ya que su retroalimentación es necesaria con respecto a la salida del proceso a fin de revisar y planear cada sprint.

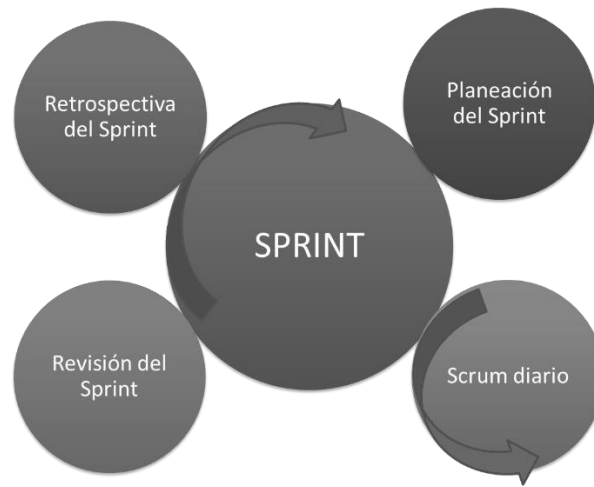
- Usuarios: Destinatario final del producto.
- Interesados: Personas a las que el proyecto les producirá algún beneficio, generalmente deben participar en las revisiones del sprint.

- Gerentes, administradores: Toma las decisiones finales participante en la selección de los objetivos y los requisitos.

2.2.5. Eventos

En Scrum hay eventos de tiempo preestablecidos con la finalidad de crear disciplina en el trabajo, optimizando así el tiempo del equipo ya que todos los miembros tienen en mente el objetivo del evento. A continuación, en la figura 9 la descripción de cada evento de Scrum:

Figura 9 Eventos de Scrum



Fuente: Figura basada en la guía definitiva de Scrum: “Las reglas del juego” (Schwaber & Sutherland, 2017)

Sprint: Es un ciclo de trabajo y es el evento principal de Scrum sobre el cual se dan el resto de eventos. El resultado del sprint son los productos intermedios que son solicitados por el dueño del producto.

El objetivo de un Sprint es crear entregables potencialmente listos para ser entregados, o presentar incrementos de producto que cumplan con los criterios de aceptación definidos por el cliente y el product owner (VM Edu, Inc., 2013).

Planeación del Sprint: Es la reunión para iniciar el sprint en donde se hace la planificación y se establece el objetivo a alcanzar en el sprint.

Scrum diario: Es una reunión que generalmente se la hace de pie, dura pocos minutos y el objetivo de este evento es organizar el trabajo de cada día.

Revisión del Sprint: Este evento se realiza al finalizar cada sprint y es donde se revisan y analizan los resultados y se muestra al cliente el producto alcanzado.

Retrospectiva del Sprint: Es un evento que se debe realizar antes de realizar un nuevo sprint cuyo objetivo es mejorar los procesos del equipo de desarrollo potenciando lo que se hizo bien y evitando que se repitan aspectos negativos.

2.2.6. Artefactos

En Scrum se manejan tres principales artefactos que son los elementos físicos que se generan como resultado de la aplicación de la metodología. Estos artefactos cumplen la función de proporcionar transparencia al equipo del proyecto e interesados de tal manera que todos tengan el mismo entendimiento. A continuación, en la figura 10, la descripción de cada uno de los artefactos.

Figura 10 Artefactos de Scrum



Fuente: Figura basado en la guía definitiva de Scrum: “Las reglas del juego” (Schwaber & Sutherland, 2017)

Lista de Producto (Product Backlog): Es una lista dinámica que cambia conforme el producto y su entorno van evolucionando. Esta lista contiene todas las características, funcionalidades, requisitos, mejoras y correcciones que constituyen cambios a realizarse sobre el producto. Cada uno de los elementos de la lista debe tener un orden, una estimación y el valor que agrega al producto.

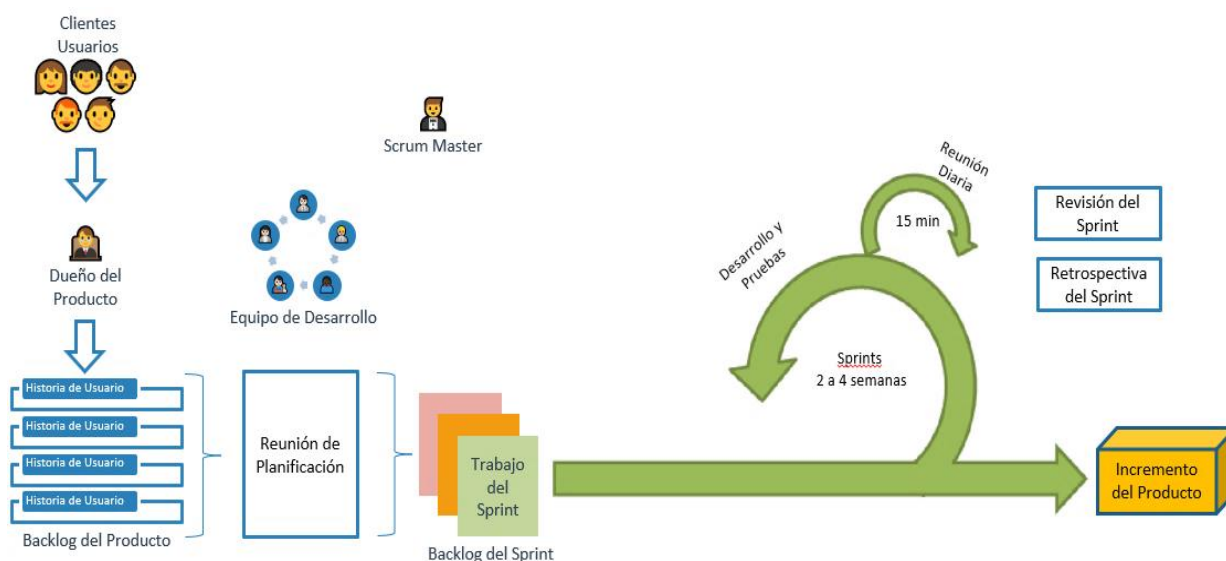
Lista de pendientes del Sprint (Sprint Backlog): Son los elementos seleccionados de la lista de producto para trabajarlo en el sprint actual, lo cual constituirá el objetivo a alcanzar al finalizar el tiempo del sprint.

Incremento: Es un entregable totalmente funcional, listo para presentarle al cliente luego de terminado un sprint.

2.2.7. Descripción del proceso Scrum

En scrum normalmente un proyecto se ejecuta en ciclos o iteraciones de duración fija (sprints) cuyo tiempo de duración es definido por el equipo dependiendo de la naturaleza y alcance del proyecto; sin embargo, se puede mencionar que generalmente esta duración va de 2 a 4 semanas. Al final de cada iteración el objetivo es presentar al cliente un incremento del producto final, el cual debe ser funcional de acuerdo a la definición de hecho que se haya llegado con el equipo Scrum. En la siguiente figura 11 se encuentra representado el proceso que sigue Scrum.

Figura 11 Descripción proceso de Scrum



Fuente: Figura basada en la guía definitiva de Scrum: “Las reglas del juego” (Schwaber & Sutherland, 2017)

Una vez que el dueño del producto haya priorizado las diferentes historias de usuario en función del valor que estas agregan al objetivo u objetivos del producto, el proceso de scrum inicia con:

Reunión de planificación de la iteración: en donde el cliente y dueño del producto presentan al equipo la lista de requisitos que priorizaron para que a su vez se solvete cualquier inquietud y el equipo tenga claro los detalles de los requerimientos y el orden de prioridad. Con este punto resuelto, el equipo selecciona los requisitos que podrían completar en la iteración de acuerdo a la definición de hecho (definition of done) y elabora la lista de tareas necesarias (backlog del sprint) con su respectiva estimación de esfuerzo que tomará el desarrollo y se autoasignan las tareas al equipo.

Ejecución del Sprint: Todos los días el equipo realiza la reunión de sincronización en donde se revisa el progreso del trabajo para cumplir con el objetivo del sprint y determinar soluciones a posibles obstáculos que impidan alcanzar el objetivo del sprint actual. En esta reunión cada miembro del equipo debe responder a 3 preguntas claves:

1. ¿Qué ha hecho desde la última reunión de sincronización para alcanzar el objetivo del sprint?
2. ¿Qué voy a hacer hoy para ayudar al equipo a cumplir con el objetivo del sprint?
3. ¿Existe algún obstáculo que me impida ejecutar el trabajo previsto para alcanzar el objetivo del sprint?

En este punto, el Scrum Master tiene que asegurarse de eliminar cualquier dificultad externa u obstáculo que pueda distraer la atención del equipo y afectando los tiempos y productividad del mismo, lo cual impactaría en el cumplimiento del objetivo del sprint.

Revisión del Sprint: Al finalizar el Sprint, el equipo presenta al cliente y/o al dueño del producto los requerimientos cumplidos como un incremento a la funcionalidad del producto, y en función de los resultados alcanzados el cliente puede solicitar adaptaciones que sean necesarias para el producto y objetivo que deben ser tomadas en cuenta en las siguientes iteraciones.

Retrospectiva del Sprint: Por otra parte, el equipo debe analizar lo bueno y lo malo del sprint que acaba de finalizar, para así detectar posibles mejoras en el proceso para optimizar su productividad en las siguientes iteraciones.

2.3. Metodologías de Gestión de Riesgos

En el apartado de conceptos generales del presente trabajo se presentaron algunos conceptos de riesgos los cuales deben ser aterrizados dependiendo de la rama o disciplina en la que se aplique la gestión riesgos, es decir en áreas como ingenieras, salud, áreas financieras y demás siempre existirán variaciones y particularidades a la hora de implementar la gestión de riesgos, en este

contexto dentro de este apartado se expondrán las metodologías que en base a la investigación se pueden alinear con el propósito de desarrollo de software.

2.3.1. Gestión de Riesgos bajo el Marco de Trabajo CMMI

CMMI (Capability Maturity Model Integration) o “Integración de los modelos de madurez de capacidades”, es un marco de trabajo norteamericano subsidiado por ISACA que describe buenas prácticas que se deben aplicar en la industria de desarrollo, mantenimiento y adquisición de productos y servicios para ayudar a las empresas a mejorar sus procesos. Es así que, en base a estas buenas prácticas, se puede evaluar el nivel de madurez de una organización para detectar puntos de mejoras y fomentar una cultura productiva y más eficiente.

Los niveles de madurez se refieren a la consecución de la mejora de procesos de una organización en múltiples áreas de proceso (Carnegie Mellon University, 2010).

Dentro del ámbito de desarrollo de software, este marco de trabajo se ha convertido en un estándar para evaluar la calidad de los procesos de desarrollo de software en donde una arista importante a considerar es el manejo de los riesgos. En tal sentido, una de sus áreas prácticas, que está bajo la categoría de gestión, es justamente la “administración de riesgos y oportunidades” la cual tiene como finalidad identificar tempranamente problemas para planificar las respectivas actividades de respuesta, ya sea para evitar y/o mitigar los impactos de posibles problemas o en su defecto detectar a tiempo posibles oportunidades para explotarlas adecuadamente para el beneficio del proyecto.

CMMI en referencia a “Administrar los riesgos y oportunidades” plantea un enfoque sistemático y continuo para planear, anticipar, y mitigar riesgos de una manera proactiva y minimizar el impacto en el proyecto, o en su defecto maximizar los beneficios en función de las oportunidades, para ello CMMI plantea unas prácticas para gestión de riesgos que se deben alcanzar las cuales se describen a continuación en la siguiente figura 12.

Figura 12 Practicas Gestión de Riesgos según CMMI



Fuente: Figura basada en el marco de trabajo CMMI v2.

Definir la estrategia para manejar los riesgos y oportunidades.

Es necesario definir una estrategia de cómo se llevará internamente la gestión de riesgos y oportunidades. Es decir, definir las acciones, procesos, y/o formatos que se deben considerar para la identificación de los riesgos y oportunidades, esquema para su clasificación y los parámetros que se utilizarán para evaluar y controlar los riesgos. En este punto es importante que el plan de gestión de riesgos y oportunidades, a más de quedar documentado, se dé a conocer a todos los miembros de la organización o equipos que se están administrando.

Identificar y analizar los riesgos u oportunidades.

Identificar y analizar los riesgos y oportunidades es fundamental hacerlo desde el inicio de los proyectos en donde es oportuno detectar amenazas u oportunidades potenciales que puedan afectar negativa o positivamente los esfuerzos del trabajo y plan del proyecto, lo que a su vez permitirá monitorearlos durante la ejecución del proyecto. Sobre este punto es importante además que los

riesgos u oportunidades se identifiquen y describan lo más comprensiblemente posible para su posterior análisis, de tal forma que los mismos puedan gestionarse adecuadamente en el contexto y condiciones particulares de cada proyecto.

Establecer planes de mitigación y contingencia de los riesgos.

Una vez identificados y analizados los riesgos ya sabemos a qué peligros nos afrontamos y su nivel de impacto, en tal virtud es necesario monitorearlos continuamente para ejecutar las actividades correspondientes cuando un riesgo sobrepasa el umbral definido, por lo tanto el plan de mitigación lo que busca es reducir de forma proactiva el impacto potencial de ocurrencia del riesgo, el cual a su vez puede venir acompañado de un plan de contingencia en caso de que el riesgo se materialice a pesar de los intentos de mitigación.

Establecer planes para aprovechar las oportunidades.

Por otro lado, es necesario fijar qué planes o acciones se deben ejecutar para lograr que las oportunidades identificadas se materialicen, es decir buscar los caminos necesarios para alcanzar los beneficios de las oportunidades en bienestar del proyecto.

Implementar los planes para el manejo de riesgos u oportunidades.

La implementación de los planes para el manejo de riesgo u oportunidades, de acuerdo a lo planteado por CMMI, debe mantenerse durante todo el proyecto; en el caso puntual de desarrollo de software, durante todas sus etapas y no únicamente al inicio del proyecto. Esto permitirá gestionar y controlar adecuadamente el estado de cada uno de los riesgos u oportunidades según los umbrales establecidos, o en su defecto nuevas formas de tratar los mismos para mitigar y/o evitar un riesgo, o concretar una oportunidad. Así mismo, al ser un proceso continuo en el camino

o ejecución del proyecto, se pueden identificar nuevos riesgos u oportunidades los cuales tendrán que analizarse, evaluarse y planificarse de acuerdo al procedimiento establecido dentro de este marco de trabajo.

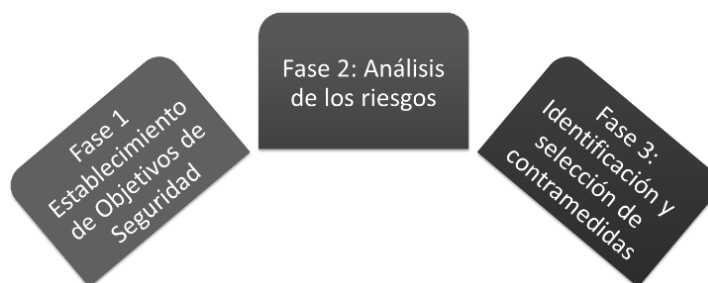
2.3.2. Metodología CRAMM: (Risk Analysis and Management Method)

Metodología creada por la agencia de cómputo y telecomunicaciones del Reino Unido; traducida al español significa “Método de análisis y gestión de riesgos”, y está orientada a proteger la confidencialidad, integridad y disponibilidad de un sistema y de sus activos iniciando desde el análisis de los riesgos hasta la propuesta de contramedidas incluyendo informes y resultados para el aseguramiento de la continuidad de los sistemas y sus activos. El ciclo de CRAMM consiste primero en identificar los riesgos y luego estimar la frecuencia de presentación de los mismos (Crespo Martínez & Cordero Torres, 2016).

Por otra parte, la metodología CRAMM ayuda a las organizaciones demostrar la eficiencia del costo invertido en materia de riesgos y está soportada por una herramienta informática que ayuda a la recopilación de datos, cálculo de los riesgos y generación de informes de gestión de riesgos.

En la siguiente figura 13, se presenta la estructura de CRAMM:

Figura 13 Fases de la metodología CRAMM



Fuente: Figura basada en la metodología CRAMM v5

Fase 1: Establecimiento de Objetivos de Seguridad

En la primera fase se establecen los objetivos generales de Seguridad, para ello se define el alcance, se identifican y evalúan los activos de hardware y de software que forman parte del sistema, y se identifica y determina el valor de los datos e información en cuanto al impacto en el negocio en caso de destrucción, modificación, indisponibilidad o divulgación de la información.

Fase 2: Análisis de los riesgos

En la segunda fase se identifican los diferentes tipos de amenazas que afectan los sistemas de información, así como se debe realizar el análisis y valoración de las vulnerabilidades ante las dichas amenazas identificadas para finalmente realizar el cálculo de la medida de los riesgos en base a las amenazas y vulnerabilidades identificadas.

Fase 3: Identificación y selección de contramedidas

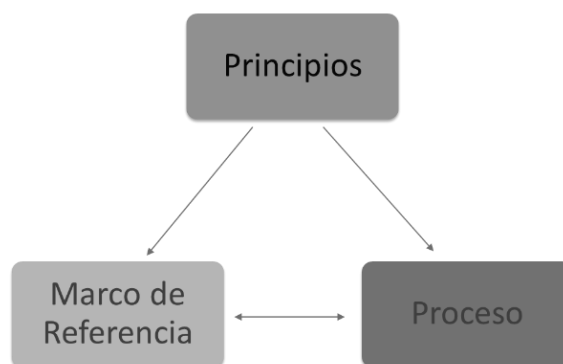
En la tercera fase la metodología sugiere que se implemente un plan de seguridad y su respectiva estrategia para la mitigación de riesgos en función de la valoración realizada en la fase uno, sin embargo, cabe destacar que la metodología también contiene procedimientos que permiten evaluar la relevancia los riesgos para decidir si es preciso o no implementar un plan para aplicar las contramedidas necesarias para la mitigación.

2.3.3. Marco de Referencia ISO 31000-2018:

La norma técnica de Gestión de Riesgos ISO 31000, en su versión 2018 está basada en el modelo PHVA (Planear, Hacer, Verificar y Actuar) y provee las directrices para la gestionar el riesgo al que se enfrentan las organizaciones. Estas directrices son adaptables a cualquier tipo de

organización y contexto, por lo que se puede implementar en cualquier tipo de industria o negocio. La ISO 31000-2018 está basada en principios que son las directrices generales del sistema de gestión, un marco de referencia que es la estructura que soporta el sistema, y los procesos que son los pasos o metodología para gestionar los riesgos; estas tres aristas se ilustran y explican a continuación en la siguiente figura 14.

Figura 14 Principios, marco de referencia y proceso



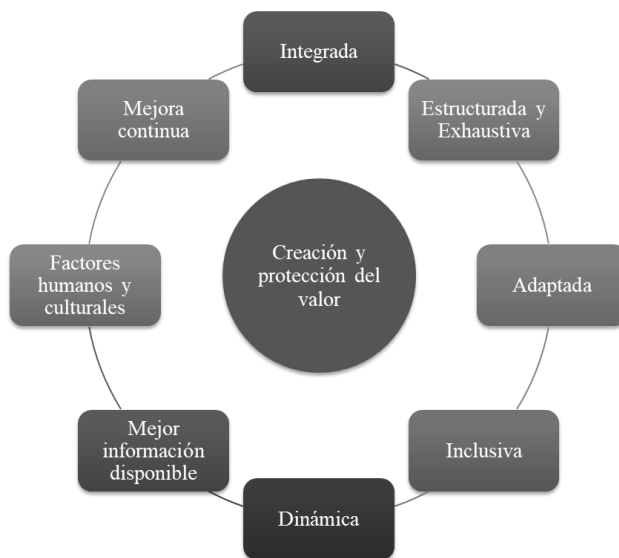
Fuente: Figura basada en la norma ISO 31000-2018

Principios:

La ISO 31000-2018, establece ocho principios rectores clave para la gestión de riesgos con el propósito de mejorar el desempeño, fomentar la innovación y contribuir en el logro de los objetivos de la organización. Estos principios establecen que la gestión de riesgos debe estar integrada a todos los procesos de la organización, debe tener un enfoque estructurado y exhaustivo para contribuir con resultados coherentes y comparables, debe ser adaptable al contexto y objetivos de la organización, debe ser inclusiva en el sentido de involucrar a todas las partes interesadas ya sean de la organización o externas, debe ser dinámica para soportar la modificación y/o aparición de nuevos riesgos de acuerdo al contexto cambiante de la organización o factores externos, debe contar una mejor información disponible como información histórica y expectativas futuras como

base para gestionar limitaciones e incertidumbres, debe considerar factores humanos y culturales que afecten o impactan en la gestión del riesgo, y finalmente la mejora continua en base al aprendizaje y experiencia. En la siguiente figura 15 se presentan los principios de la ISO 31000,2018.

Figura 15 Principios ISO 31000-2018



Fuente: Figura basada en la norma ISO 31000-2018

Marco de Referencia ISO 31000-2018:

Como se mencionó en el apartado anterior, uno de los principios rectores de la ISO 31000-2018 es integrar la gestión del riesgo en todas las actividades y procesos de la organización, lo cual depende de factores clave como: la cultura organizacional, la toma de decisiones y sobre de todo si existe o no el apoyo de la alta gerencia quien debe transmitir y comprometer a toda la organización.

El marco de referencia, como se explica e ilustra en la siguiente figura 16, implica entonces:

- Integrar de tal manera que se cubran todas las áreas, personas y procesos de la organización.
- Diseño alineado al contexto real de la organización asignando roles y canales de comunicación.

- La Implementación, mediante un plan con plazos y recursos, que especifique cuándo, cómo, dónde y quién toma las decisiones en la organización y en función de esto hacer ajustes al sistema para la gestión de riesgos.
- La Valoración, mediante la visualización y medición de los indicadores de desempeño y alineamiento a la estrategia de la organización.
- La Mejora, para contribuir al fortalecimiento de la gestión del riesgo en la organización.

Figura 16 Marco de referencia ISO 31000-2018



Fuente: Figura basada en la norma ISO 31000-2018

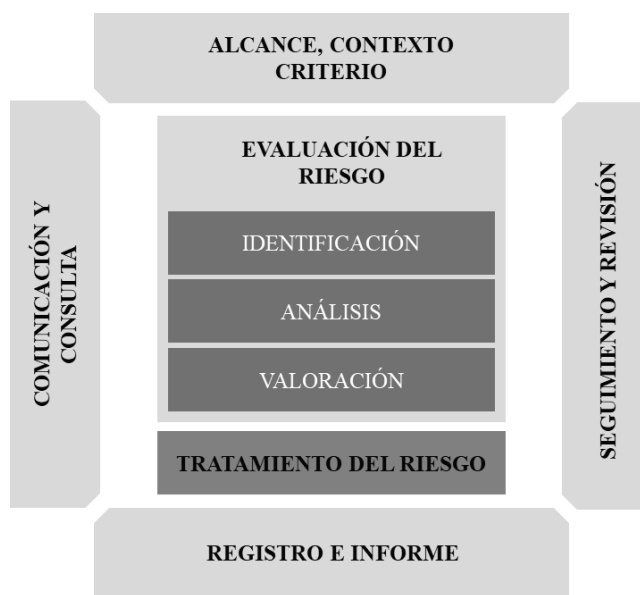
Proceso:

Según la ISO 31000-2018 el proceso de gestión de riesgos implica la aplicación sistemática de políticas, procedimientos y prácticas a las actividades de comunicación y consulta, establecimiento del contexto y evaluación, tratamiento, seguimiento, revisión, registros y reportes de los riesgos (Organización Internacional de Normalización 31000, 2018).

Estas actividades que presenta la norma, establecen los pasos o metodología que se debe aplicar para la gestión de los riesgos en la organización, lo se encuentra ilustrado en la siguiente figura 17, y son explicados de una manera resumida a continuación:

- Comunicación y Consulta, debe mantenerse durante todas las etapas del proceso para que quede siempre comprendido el riesgo y las bases para la toma las decisiones.
- Alcance, criterios y contexto, con el propósito de realizar una correcta evaluación del riesgo, para así, realizar un apropiado tratamiento al riesgo.
- Evaluación del riesgo, que es el proceso integral y sistemático para la identificación, análisis y valoración del riesgo.
- El tratamiento del riesgo, de acuerdo a la norma, tiene como propósito seleccionar e implementar opciones para abordar el riesgo, que implica evitar el riesgo, aceptar el riesgo, eliminar la fuente del riesgo, modificar la probabilidad del riesgo, modificar la consecuencia del riesgo, compartir el riesgo o retener el riesgo.
- El seguimiento y revisión, debe darse en todas las etapas del proceso de la gestión del riesgo con la finalidad de proporcionar retroalimentación en base a resultados obtenidos.
- El Registro e Informe, se refiere a dejar documentado el proceso de la gestión de riesgos y los resultados obtenidos, lo cual debe ser oportunamente comunicado a las partes interesadas.

Figura 17 Proceso ISO 31000-2018



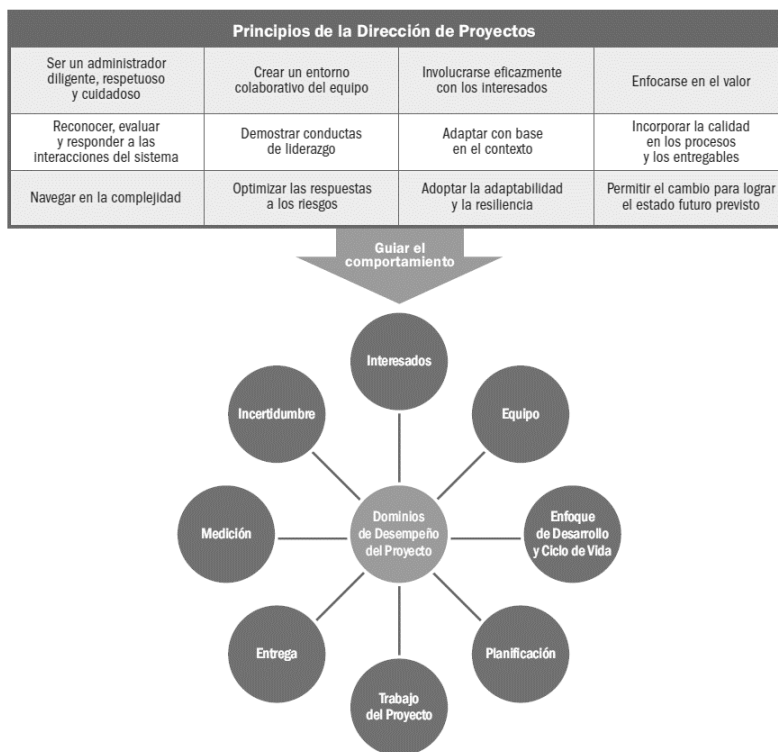
Fuente: Figura basada en la norma ISO 31000-2018

2.3.4. Guía PMBOK – Dominio de desempeño de la Incertidumbre

EL PMBOK, en su séptima edición publicada en el presente año 2021, contempla, como se ilustra en la siguiente figura 18, doce principios rectores para la entrega de proyectos los cuales guían el comportamiento de ocho dominios de desempeño, a estos últimos, la guía PMBOK les define como: “Los dominios de desempeño del proyecto son áreas de énfasis interactivas, interrelacionadas e interdependientes que funcionan al unísono para conseguir los resultados deseados del proyecto” (PMI, 2021).

En la siguiente figura 18, se ilustra la relación entre los principios de la dirección de proyectos y los dominios de desempeño del proyecto.

Figura 18 Relación entre los principios de la dirección de proyectos y los dominios de desempeño del proyecto

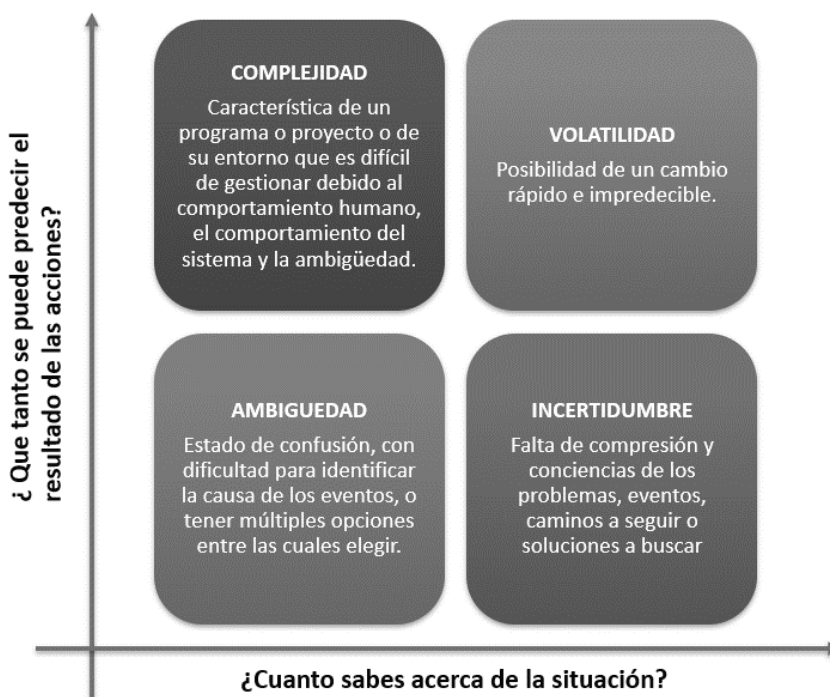


Fuente: Figura tomada de la guía PMBOK séptima edición, Sección 1-Introducción pág. 5.

Dentro de estos dominios desempeño, consta justamente el dominio de desempeño de la incertidumbre, el cual en específico se ocupa de las actividades y funciones asociadas con el riesgo y la incertidumbre que existen en los diferentes contextos y realidades cambiantes en los que se ejecutan los proyectos para anticipar amenazas y aprovechar oportunidades, esto implica conocer a su vez, el nivel de volatilidad, incertidumbre, complejidad, y ambigüedad, que se presentan en los proyectos por una serie de realidades y factores, como por ejemplo requisitos altamente complejos o ambiguos, complejidad en el manejo del factor humano, ya sea de los interesados o del mismo equipo del proyecto, volatilidad en referencia a cambios en los requisitos que se pueden presentar en cualquier momento durante la ejecución del proyecto, o a su vez, eventos externos o internos inciertos que se presentan en forma de oportunidades o amenazas que deben ser gestionadas a tiempo.

Dentro de este contexto y bajo el dominio de desempeño de la incertidumbre presentado por la guía PBMOK v7, es sustancial hablar de los entornos VUCA, por sus siglas en ingles de **V**olatility, **U**ncertainty, **C**omplexity, **A**mbiguity, cuyo concepto inició en la década de los noventa por la escuela de guerra del ejército de los Estados Unidos como respuesta para describir el mundo incierto, complejo y ambiguo, multilateral, resultante del fin de la guerra fría. Dicho concepto con el pasar del tiempo se fue adoptando y aplicando a empresas de diversas industrias para guiar el liderazgo y planificación estratégica de los negocios y por ende de los proyectos. Bajo este esquema y de acuerdo a lo planteado por la guía PMBOK v7 el riesgo general del proyecto depende en qué medida estos factores de incertidumbre, complejidad, ambigüedad y volatilidad afecten a un proyecto en específico, concluyendo que, si el riesgo general es demasiado alto, la organización puede optar por cancelar el proyecto (PMI, 2021). En la siguiente figura 19 se ilustra el entorno VUCA.

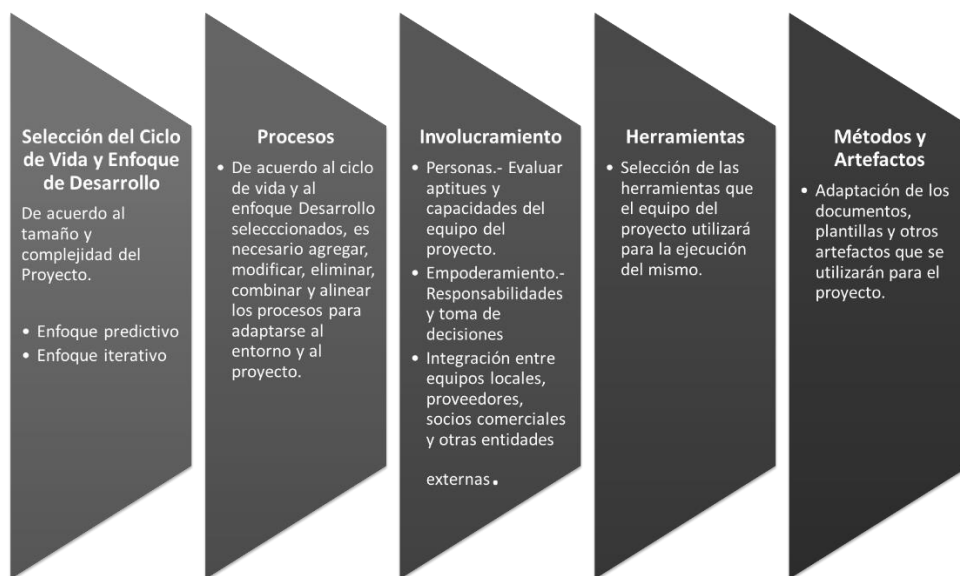
Figura 19 Entorno VUCA



Fuente: Figura basada en los conceptos de la guía PMBOK séptima edición, Sección 2-Dominios de desempeño del proyecto pág. 117.

Adaptación: Bajo el conocimiento de los diferentes entornos cambiantes en los que se ejecutan los proyectos, y en referencia a la figura anterior, es importante que se realicen ajustes y adaptaciones para la gestión y entrega de cada proyecto, pues no es igual ejecutar un proyecto de largo alcance como la construcción de una planta hidroeléctrica, que ejecutar un proyecto pequeño que tiene como entregable una página web. En este sentido la guía PMBOK v7 determina que no existe un enfoque único que pueda ser aplicado a todos los proyectos todo el tiempo (PMI, 2021), sino que, establece algunos aspectos que se pueden adaptar según la naturaleza del proyecto, cultura organizacional de la empresa, tamaño, duración, complejidad de cada proyecto, necesidad de comunicación, entre otros factores. Dichos aspectos que se deben adaptar son resumidos en la siguiente figura 20.

Figura 20 Aspectos que pueden ser adaptados según la naturaleza de los proyectos



Fuente: Figura basada en los conceptos de la guía PMBOK séptima edición, Secciones 3.3.1 a 3.3.4, pág. 134.

Modelos, Métodos y Artefactos guía PMBOK v7

En consideración que el uso de modelos, métodos y artefactos dentro los proyectos también deben adaptarse al entorno de las organizaciones y las características del proyecto, es importante que el equipo del proyecto evite el uso de cualquier modelo, método y/o artefacto que genere esfuerzos innecesarios que no agregan valor al equipo del proyecto o a sus interesados. En este sentido para el dominio de desempeño de la incertidumbre la guía PMBOK v7 sugiere algunos modelos, métodos y artefactos de uso común que son útiles a la hora de gestionar los riesgos y oportunidades del proyecto, en la siguiente tabla 1 un resumen de los mismos.

Tabla 1 Modelos, Métodos y Artefactos Dominio de desempeño de la Incertidumbre

DOMINIO DE DESEMPEÑO INCERTIDUMBRE	
MODELOS	Marco de referencia de Cynefin
	Matriz de Stacey
MÉTODOS	Análisis de alternativas
	Análisis de supuestos y restricciones
	Matriz de probabilidad e impacto
	Análisis FODA
	Análisis de escenarios ¿Qué pasa sí.?
	Revisión del riesgo
ARTEFACTOS	Registro de supuestos
	Lista de trabajo pendiente ajustada al riesgo
	Registro de riesgos
	Plan de gestión de riesgos
	Estructura de desglose del riesgo
	Diagrama de causa y efecto

Fuente: Tabla basada en los conceptos de la guía PMBOK séptima edición, Sección 4.

Área de conocimiento Gestión del Riesgos PMBOK v6

En línea con la búsqueda de las bases conceptuales para posteriormente plantear un método específico para la gestión de riesgos en proyectos de desarrollo de software, a continuación se describe el área de conocimiento de gestión de los riesgos del proyecto que plantea la guía PMBOK en su sexta edición, la cual está estructurada por los procesos que se muestran en la tabla 2 a continuación:

Tabla 2 Área de Conocimiento Gestión de los Riesgos del Proyecto

ÁREA DE CONOCIMIENTO	GRUPO DE PROCESO		
	Grupo de Procesos de Planificación	Grupo de Procesos de Ejecución	Grupo de Procesos de Monitoreo y Control
Gestión de los Riesgos del Proyecto	1. Planificar la gestión de los Riesgos	6. Implementar la respuesta a los riesgos	7. Monitorear los riesgos
	2. Identificar los Riesgos		
	3. Realizar el Análisis Cualitativo de Riesgos		
	4. Realizar el Análisis Cuantitativo de Riesgos		
	5. Planificar la Respuesta a los Riesgos		

Fuente: Tabla basada en los conceptos de la Guía PMBOK sexta edición, pág. 25.

Planificar la Gestión de los Riesgos.

Este proceso de planificación para la gestión de los riesgos, debe llevarse a cabo una única vez al inicio del proyecto tan pronto este sea concebido, así como también en puntos previamente establecidos en la planificación del proyecto, y debe contener cómo se estructurarán y realizarán las actividades de gestión de riesgos que se deben ejecutar durante el ciclo de vida del proyecto, de tal manera que se pueda proporcionar oportunamente el tiempo y los recursos necesarios para

la gestión de los riesgos y así establecer una base sobre la cual se evaluarán posteriormente los riesgos. En la siguiente figura 21, se muestran las entradas, herramientas, técnicas, y salidas de este proceso.

Figura 21 Entradas, herramientas, técnicas, y salidas para Planificar la Gestión de los Riesgos.



Fuente: Figura tomada de la guía PMBOK sexta edición, pág. 401.

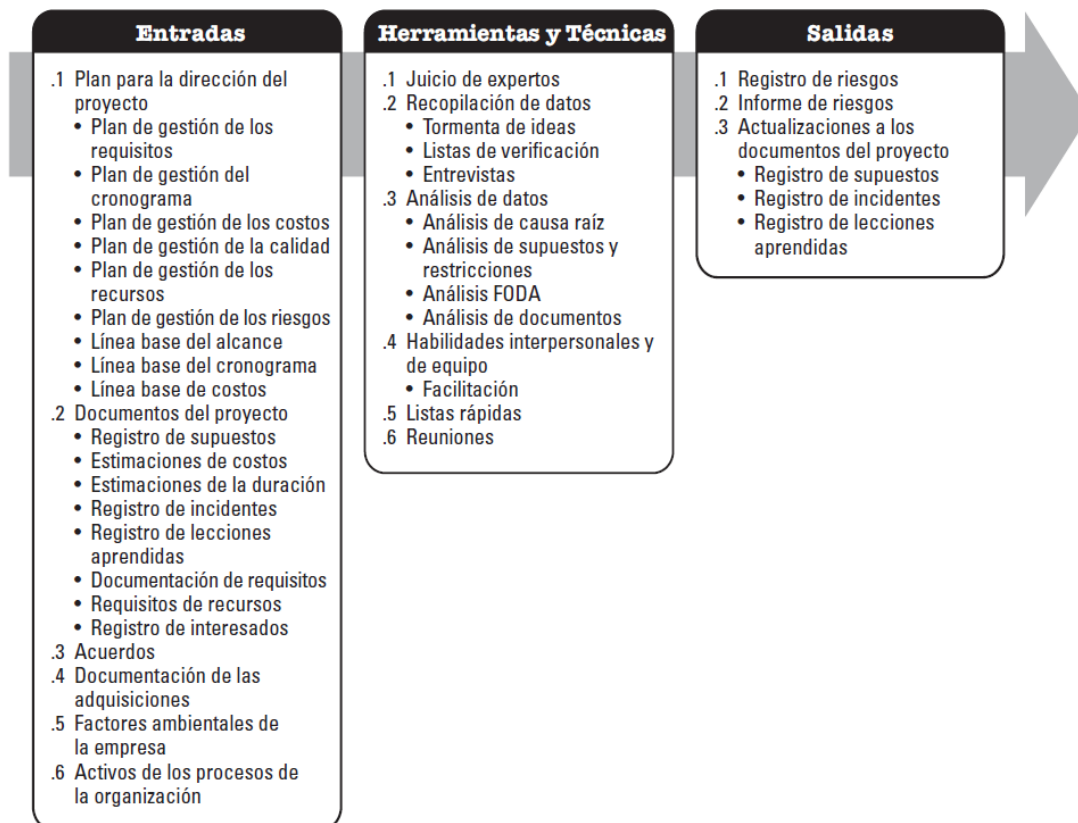
Identificar los Riesgos.

Este proceso debe tomar en cuenta, tanto los riesgos locales del proyecto, así como las fuentes del riesgo general del proyecto, y se lo debe ejecutar de una manera iterativa durante todo el ciclo de vida, ya sea para identificar nuevos riesgos que pueden afectar al proyecto, o porque los riesgos identificados inicialmente fueron evolucionando durante la ejecución y avance del proyecto. Es por eso que la frecuencia de iteración y los participantes para el proceso de identificación deben estar definidos dentro del plan de gestión de los riesgos.

Dentro de este proceso es importante la participación activa del equipo del proyecto de tal manera que se genere un sentido de propiedad y responsabilidad para ejecutar las acciones y respuestas asociadas a los riesgos identificados.

En la siguiente figura 22, se muestran las entradas, herramientas, técnicas, y salidas de este proceso.

Figura 22 Entradas, herramientas, técnicas, y salidas para Identificar los Riesgos.



Fuente: Figura tomada de la guía PMBOK sexta edición, pág. 409.

Realizar el Análisis Cualitativo de Riesgos

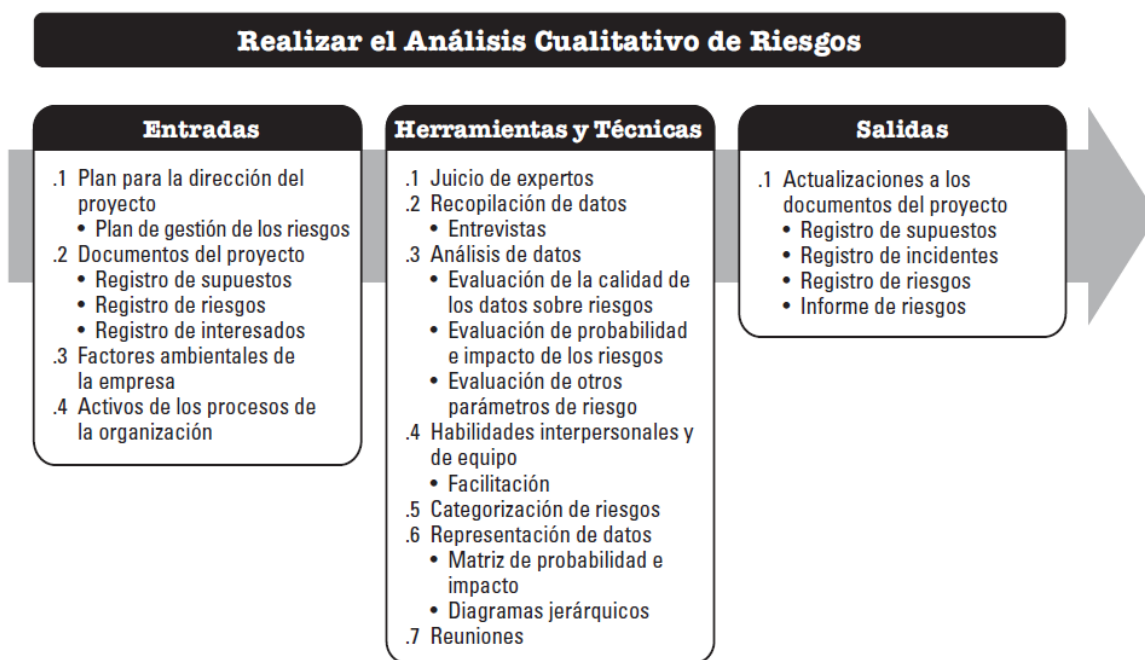
Según el PMBOK v6, “Realizar el Análisis Cualitativo de Riesgos es el proceso de priorizar los riesgos individuales del proyecto para análisis o acción posterior, evaluando la probabilidad de ocurrencia e impacto de dichos riesgos, así como otras características” (PMI, 2017, p.419).

De acuerdo al concepto anterior, la importancia de este proceso radica en la priorización de los diferentes riesgos del proyecto, ya que esto permite enfocarse principalmente en los riesgos de

alta prioridad, lo cual a su vez mejora la gestión y desempeño del proyecto. Este proceso se lo debe ejecutar de una manera periódica a lo largo de todo el ciclo de vida del proyecto en donde, a más de priorizar cada riesgo identificado, se debe asignar un responsable que tenga la capacidad de dar una respuesta adecuada y oportuna al riesgo.

En la siguiente figura 23, se muestran las entradas, herramientas, técnicas, y salidas de este proceso.

Figura 23 Entradas, herramientas, técnicas, y salidas para Realizar el Análisis Cualitativo de Riesgos.



Fuente: Figura tomada de la guía PMBOK sexta edición, pág. 419.

Realizar el Análisis Cuantitativo de Riesgos

Este proceso de análisis cuantitativo, se realiza sobre los riesgos priorizados mediante el análisis cualitativo, así como en los riesgos generales del proyecto, con el objetivo de cuantificar numéricamente la exposición al riesgo en general. De acuerdo a la guía PMBOK v6, este proceso

no es requerido para cada proyecto, pero, en los que se utiliza se lleva a cabo durante todo el proyecto (PMI, 2017).

En la siguiente figura 24, se muestran las entradas, herramientas, técnicas, y salidas de este proceso.

Figura 24 Entradas, herramientas, técnicas, y salidas para Realizar el Análisis Cuantitativo de Riesgos.



Fuente: Figura tomada de la guía PMBOK sexta edición, pág. 428.

Planificar la Respuesta a los Riesgos

El proceso de planificar la respuesta a los riesgos se ejecuta luego de los procesos de análisis cualitativo y cuantitativo de los riesgos, y busca establecer estrategias para dar una respuesta adecuada para reducir al mínimo las amenazas individuales, y maximizar las oportunidades individuales, para así llegar a reducir la exposición global del riesgo del proyecto. En la siguiente

tabla 3, se muestran las estrategias para tomar acción sobre las amenazas y oportunidades, así como sobre el riesgo general del proyecto.

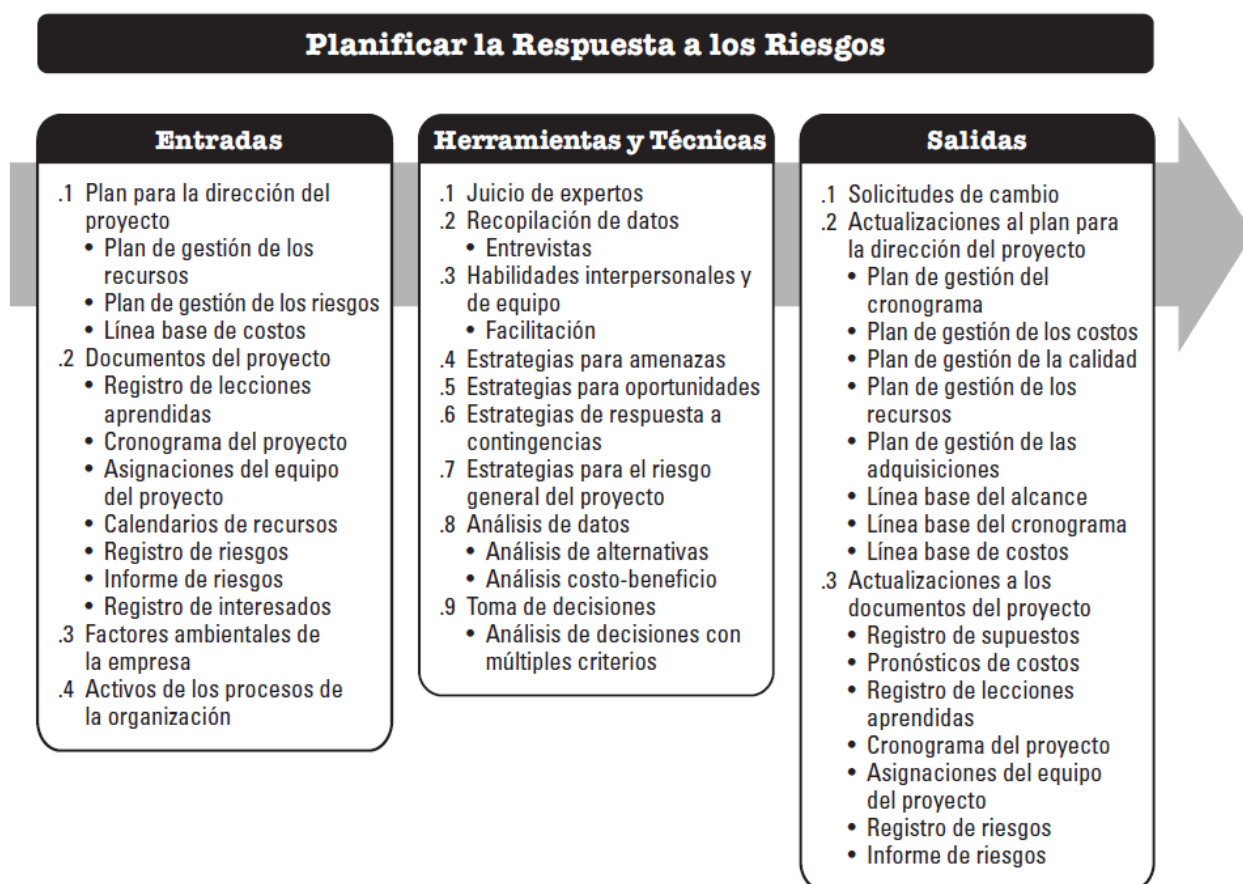
Tabla 3 Estrategias para dar respuesta a los riesgos

Ámbito	Estrategias
Amenazas Individuales	Escalar
	Evitar
	Transferir
	Mitigar
	Aceptar
Oportunidades Individuales	Escalar
	Explotar
	Compartir
	Mejorar
	Aceptar
Riesgo General del Proyecto	Evitar
	Explorar
	Transferir / Compartir
	Mitigar/Mejorar
	Aceptar

Fuente: Tabla basada en los conceptos de la guía PMBOK sexta edición, páginas de la 442 a la 446

Es importante que todas las respuestas a los riesgos sean acordadas por los interesados e involucrados en el proyecto y sobre todo que tenga un responsable asignado. En la siguiente figura 25, se muestran las entradas, herramientas, técnicas, y salidas de este proceso.

Figura 25 Entradas, herramientas, técnicas, y salidas para Planificar la Respuesta a los Riesgos.

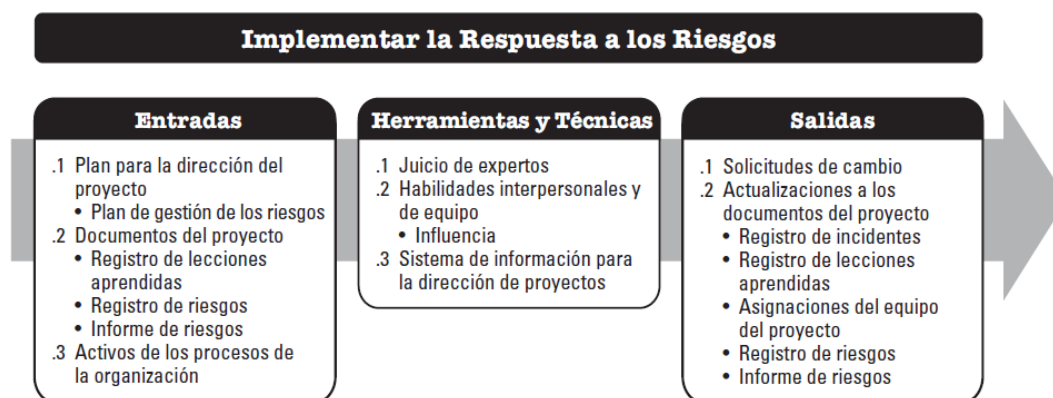


Fuente: Figura tomada de la guía PMBOK sexta edición, pág. 437.

Implementar la Respuesta a los Riesgos

Este proceso se lleva a cabo durante todo el proyecto y tiene la finalidad de asegurar que se cumplan las respuestas a los riesgos de acuerdo a lo planificado en referencia a las estrategias de respuesta al riesgo. En la siguiente figura 26, se muestran las entradas, herramientas, técnicas, y salidas de este proceso.

Figura 26 Entradas, herramientas, técnicas, y salidas para Implementar la Respuesta a los Riesgos.

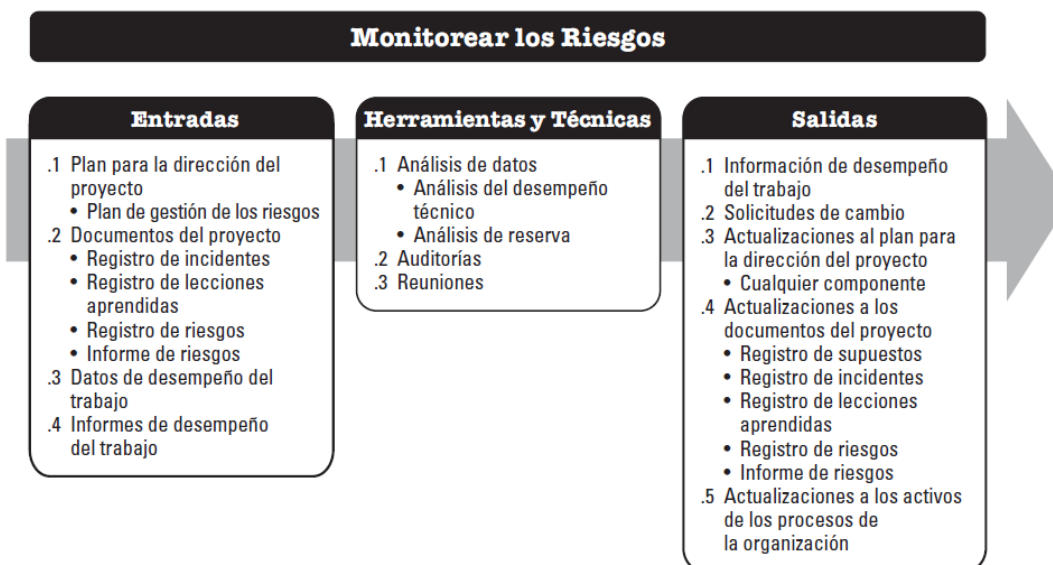


Fuente: Figura tomada de la Guía PMBOK sexta edición, pág. 449.

Monitorear los Riesgos

Este proceso se lleva a cabo durante todo el proyecto y se encarga de monitorear la implementación de los planes de respuesta acordados, dar seguimiento los riesgos identificados, identificar y analizar nuevos riesgos, así como de evaluar la efectividad del proceso de gestión de los riesgos a lo largo del proceso. En la siguiente figura 27, se muestran las entradas, herramientas, técnicas, y salidas de este proceso.

Figura 27 Entradas, herramientas, técnicas, y salidas para Monitorear los Riesgos.

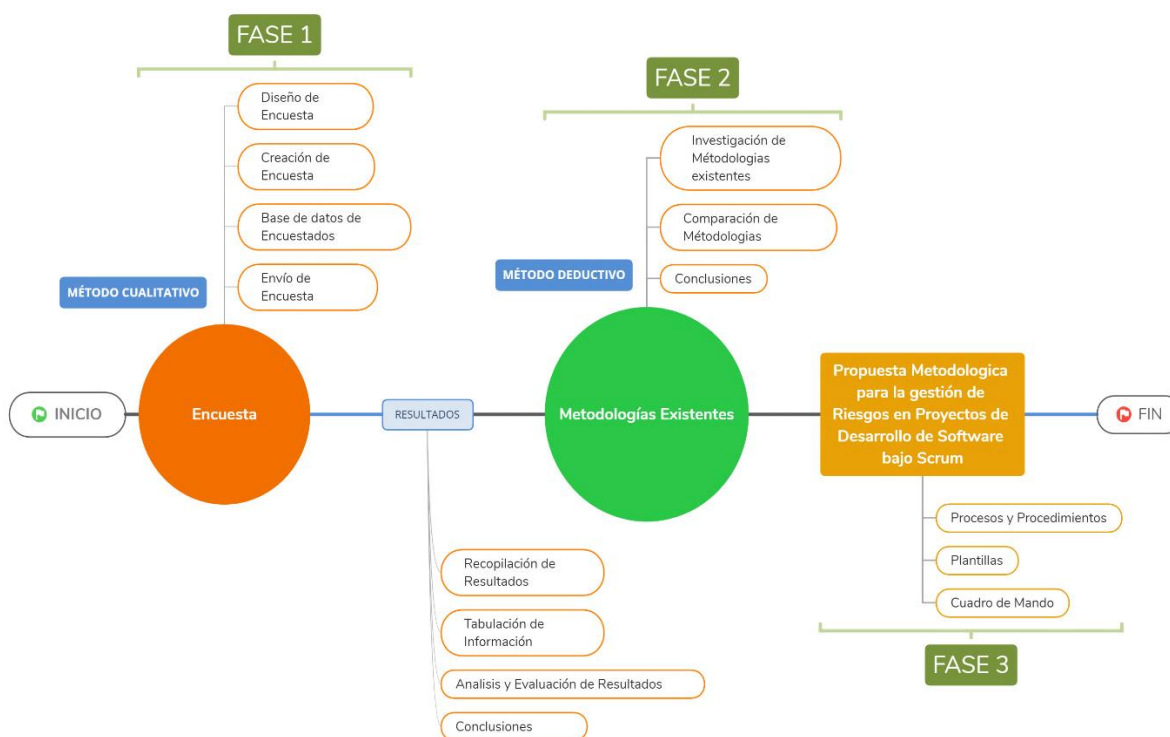


Fuente: Figura tomada de la guía PMBOK sexta edición, pág. 453.

CAPITULO III: METODOLOGÍA

Con el afán de comprender la situación actual en materia de gestión de riesgos que tienen las empresas y profesionales que se dedican al desarrollo de software, y en función de metodologías existentes, se realizó una investigación y desarrollo siguiendo las fases representadas a continuación en la figura 28.

Figura 28 Fases metodología de trabajo



Fuente: Figura de autoría propia.

Fase 1: Encuesta tipo descriptiva para recolectar información relevante a ejecución de proyectos de desarrollo de software y gestión de riesgos en empresas ecuatorianas.

Fase 2: Estudio y comparación de marcos de trabajo y/o metodologías existentes para gestionar riesgos.

Fase 3: Propuesta de un modelo para gestionar riesgos en proyectos de desarrollo de software bajo un marco de trabajo ágil.

3.1. Unidad de Análisis

La investigación está dirigida a profesionales de tecnología de la información de nuestro medio que están relacionados con la rama del desarrollo de software para así obtener información sobre, si utilizan o no en sus organizaciones una metodología de gestión de riesgos dentro de sus proyectos de desarrollo de software, y/o a su vez conocer las principales razones y dificultades por las cuales no se ha implementado ninguna metodología.

3.2. Población

Para la presente investigación, se toma como base la población de ingenieros de sistemas y/o profesionales relacionados con las tecnologías de información que actualmente trabajan en áreas de investigación, desarrollo e innovación en las diferentes organizaciones del Ecuador. Para ello se recurrió a la preparación y envío de una encuesta vía web a diferentes grupos relacionados en redes sociales.

3.3. Tamaño de la muestra

Para calcular el tamaño de la muestra se utilizó la fórmula de población infinita, en virtud que no se conoce con exactitud el tamaño de la población objeto del presente estudio:

Fórmula:

$$N = \frac{Z^2 * p * q}{e^2}$$

En donde:

- N = Tamaño de la Muestra
- Z = Nivel de Confianza
- p = Ocurrencia positiva
- q = 1 – p (Ocurrencia negativa)
- e = margen de error

Bajo un nivel de confianza del 90%, y un margen de error del 10%, siendo el nivel ocurrencia positivo el 50% porque no se tiene información previa; al aplicar la fórmula se obtiene el siguiente tamaño de la muestra:

$$N = \frac{(1.65)^2 * 0.50 * 0.50}{(0.10)^2}$$

$$N = 68$$

El valor Z, y el valor e, fueron obtenidos en función de la siguiente tabla 4, que es una porción extraída del apéndice B.1 del libro “Estadística aplicada a los negocios y la economía.” (Lind, Marchal, & Wathen, 2012)

Tabla 4 Valores Z y e, para muestreo aleatorio simple sin conocer el tamaño de la población.

Nivel de Confianza	95%	94%	93%	92%	91%	90%	80%
Valor Z	1.96	1.88	1.81	1.75	1.69	1.65	1.28

Margen de Error	13%	12%	11%	10%	9%	8%	7%
Valor e	0.13	0.12	0.11	0.1	0.09	0.08	0.07

Fuente: Libro, Estadística aplicada a los negocios y la economía, apéndice B.1.

3.4. Selección de la muestra

En consideración a las limitaciones de espacio y tiempo, y al no tener una población conocida o totalmente definida, se utilizó un muestreo aleatorio simple, cuyo concepto manifiesta, que es una

muestra seleccionada de manera que cada elemento o individuo de la población tenga las mismas posibilidades de que se le incluya (Lind, Marchal, & Wathen, 2012).

Bajo esta premisa se optó por realizar una encuesta digital de tal forma que todos los encuestados únicamente tengan la opción de contestar una sola vez el cuestionario enviado.

3.5. Métodos a emplear

La metodología utilizada en el presente trabajo fue de carácter cualitativo y deductivo, utilizando en primera instancia el método cualitativo para evaluar el nivel de conocimiento en metodologías o marcos de referencia para la gestión de riesgos y el nivel de aplicación de los mismos en proyectos de desarrollo de software. Con esta premisa y resultados lo que se busca es identificar si existe consciencia en las empresas de nuestro medio sobre la importancia de gestionar adecuadamente los riesgos en el ciclo de vida de desarrollo de software versus la facilidad o dificultad de implementar una metodología para gestionar los riesgos dentro de los proyectos de desarrollo de software.

En base a este análisis cualitativo se deriva cuáles son los principales obstáculos y/o dificultades que hoy en día tienen las empresas de nuestro medio para implementar una metodología que les ayude a gestionar apropiadamente los riesgos dentro de los proyectos de desarrollo de software.

En la segunda fase del presente trabajo se utiliza un método deductivo en donde se investigó las principales características de las siguientes metodologías de gestión de riesgos:

- Gestión de Riesgos bajo el Marco de Trabajo CCMI
- Metodología CRAMM

- Marco de Referencia ISO 31000-2018:
- PMBOK (Gestión de Riesgos)

Con la información de estas metodologías o marcos de referencia, se realiza un análisis comparativo de sus procesos, formatos, buenas prácticas y demás artefactos y particularidades de cada una, para posteriormente, como fase final, presentar una propuesta de un modelo específico para la gestión de riesgos en proyectos de desarrollo de software bajo un contexto de agilidad, que busca de alguna manera establecer un camino rápido y simple para gestionar los riesgos en el ciclo de vida de desarrollo de software dentro de las empresas que así lo requieran, sin que esto represente o garantice que dicho modelo funcione o se ajuste a las diferentes realidades de las organizaciones.

3.6. Identificación de las necesidades de información. Fuentes primarias y secundarias.

Para el presente trabajo se utilizaron fuentes de información primaria y secundarias, las cuales se describen a continuación.

Fuente Primaria: como fuente primaria se vio la necesidad de explorar los criterios y experiencia de profesionales que se encuentran en el campo del desarrollo de software para conocer en qué medida aplican o no una metodología de gestión de riesgos en sus proyectos dentro de sus organizaciones.

Fuente Secundaria: Por otro lado, se utilizó como fuente secundaria libros, revistas, normas, guías, y trabajos previos que contienen material relevante en cuestión de gestión de riesgos y ejecución de proyectos de desarrollo de software.

3.7. Técnicas de recolección de datos

Para la recolección de datos se diseñó una encuesta tipo descriptiva con una serie de preguntas en el contexto de proyectos de desarrollo de software y el uso y conocimiento de gestión de riesgos en la ejecución de los proyectos de desarrollo de software. Ver anexo 1 “Encuesta”.

3.8. Herramientas utilizadas para el análisis e interpretación de la información

En primera instancia, se utilizó la herramienta Google Forms, para el diseño y formulación de las preguntas de la encuesta, la cual fue enviada por redes sociales, utilizando principalmente las redes de Whatsapp y Telegram.

Para calcular el tamaño de la muestra, se utilizó Microsoft Excel bajo el concepto de muestreo aleatorio simple sin conocer el tamaño de la población.

Por otra parte, para comprobar la validez y fiabilidad de la encuesta se utilizó el software SPSS de IBM, sobre el cual se realizó la prueba estadística alfa de Cronbach.

Finalmente, para la recolección de información, análisis y comparación de los resultados de la encuesta realizada, se utilizó las herramientas de Google Forms, Microsoft Excel, y Microsoft Power BI como herramientas de soporte y transformación de datos.

CAPITULO IV: RESULTADOS Y DISCUSIÓN

4.1. Análisis, Interpretación y discusión de resultados

Luego de definir el tamaño de la muestra necesaria para la recolección de información, se procedió a realizar el diseño, construcción y envío de la encuesta (Anexo 1), a grupos de profesionales relacionados con el desarrollo de software.

4.1.1. Fiabilidad de la encuesta

Una vez finalizada la recolección de información se realizó una prueba de fiabilidad de la encuesta en base al concepto del alfa de Cronbach, el cual es utilizado para escalas unidimensionales entre tres y veinte ítems, y manifiesta que si el resultado de esta prueba esta entre 0,70 y 0,90 indican una buena consistencia interna. (Celina Oviedo, 2005), es decir los resultados son fiables para realizar cualquier tipo de análisis. En la siguiente figura 29, se muestra el resultado de la prueba utilizando el software SPSS de IBM.

Figura 29 Resultado prueba de fiabilidad de Alfa de Cronbach

→ **Fiabilidad**

Escala: Encuesta

Resumen de procesamiento de casos

		N	%
Casos	Válido	78	100,0
	Excluido ^a	0	,0
	Total	78	100,0

a. La eliminación por lista se basa en todas las variables del procedimiento.

Estadísticas de fiabilidad

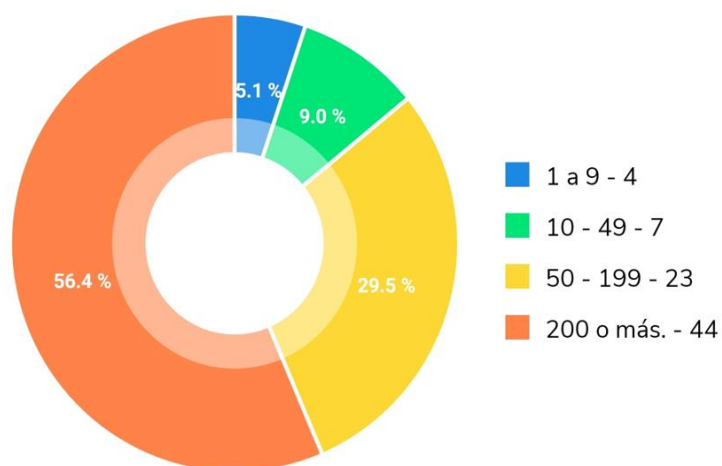
Alfa de Cronbach	Alfa de Cronbach basada en elementos estandarizados	N de elementos
,727	,729	13

Fuente: Caso práctico de autoría propia

4.1.2. Análisis y resultados de la encuesta

En primera instancia para iniciar el análisis, es importante determinar el tamaño y giro de negocio de las empresas en las cuales trabajan o prestan sus servicios los profesionales encuestados. La siguiente figura 30 muestra que la mayoría de profesionales encuestados trabajan en empresas grandes, es decir en organizaciones de 200 o más empleados, el 29.5% de encuestados trabajan en empresas medianas, el 9% en pequeñas empresas, y el 5.1% en microempresas, lo cual contrastado con el giro de negocio al que pertenecen estas empresas, podemos notar que de los 44 profesionales que trabajan en empresas grandes, la mayoría de éstas empresas pertenecen al sector financiero e industrial. En la siguiente tabla 5, se puede apreciar un resumen en base a los profesionales encuestados versus el tamaño y giro de negocio de las empresas en las cuales trabajan.

Figura 30 ¿Con cuántos empleados cuenta la empresa en la que actualmente presta sus servicios?



Fuente: Resultado Encuesta, autoría propia.

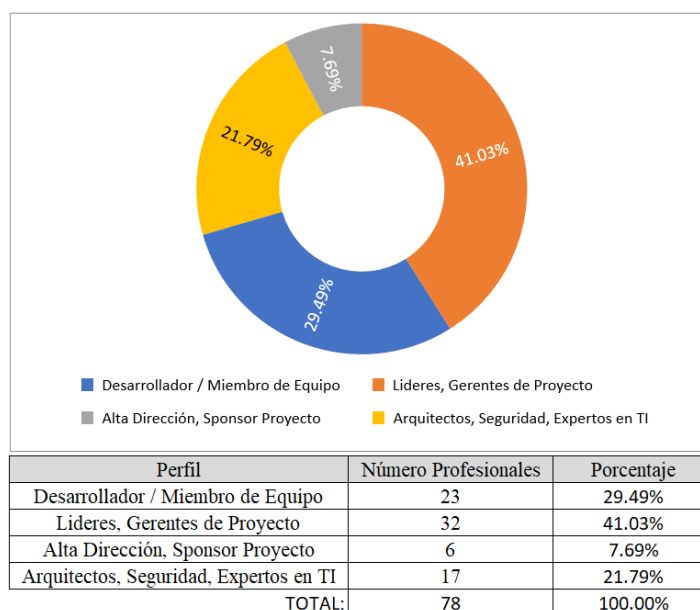
Tabla 5 Contraste tamaño de empresas vs giro de negocio

	PYMES				
	MICROEMPRESAS	PEQUEÑAS	MEDIANAS	GRANDES	
	1-9	10-49	50-199	200 o mas	
Financiero	0	1	10	26	37
Tecnologías de las información	3	4	5	2	14
Industrial	0	0	0	5	5
Servicios	1	1	2	3	7
Educación	0	1	2	2	5
Alimentos	0	0	1	0	1
Gobierno	0	0	0	1	1
otros	0	0	3	5	8
TOTALES	4	7	23	44	78

Fuente: Resultado Encuesta, autoría propia.

En la siguiente figura 31, de acuerdo al atributo del perfil de los encuestados podemos ver que el 78.21% son profesionales que están relacionados directamente con la ejecución de los proyectos, y por ende tienen la responsabilidad del éxito o fracaso de los mismos. Por otra parte, el 21.79% son profesionales de apoyo como arquitectos, jefes de seguridad de la información, y expertos de TI en general.

Figura 31 ¿Qué rol usted desempeña dentro de los proyectos de desarrollo de software de su empresa?

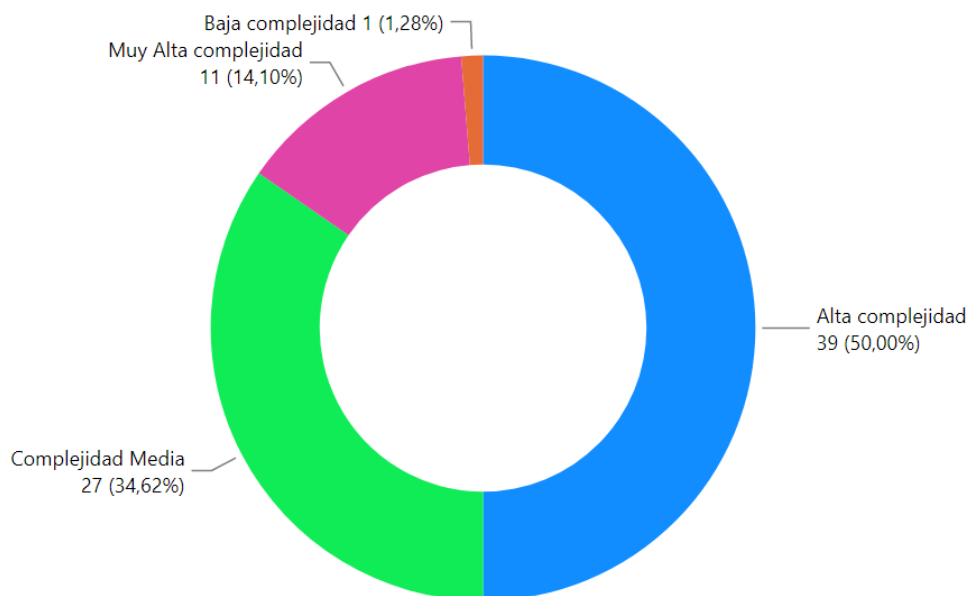


Fuente: Resultado Encuesta, autoría propia.

Luego de identificar el perfil de los encuestados, una parte primordial de la encuesta, está dirigida a conocer la importancia que le dan las empresas y profesionales a la gestión de riesgos en proyectos de desarrollo de software. Es así que para este análisis se recogen en primera instancia las respuestas del nivel de complejidad de los proyectos ejecutados en los últimos 12 meses, para contrastar con la percepción de la importancia de gestionar los riesgos en los proyectos de desarrollo de software y el nivel de conformidad del tiempo invertido en base a la experiencia de los encuestados.

En la siguiente figura 32, podemos ver el resultado de la categorización del nivel de complejidad que los 78 encuestados les dan a sus proyectos.

Figura 32, ¿Qué nivel de complejidad usted considera que tuvieron los proyectos que se ejecutaron en su empresa en los últimos 12 meses?

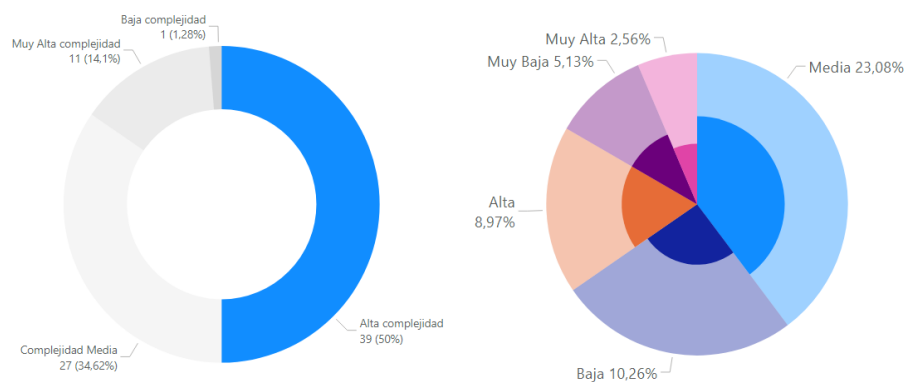


Fuente: Resultado Encuesta, autoría propia.

En donde vemos que existe una concentración del 50.00% de proyectos de Alta complejidad, lo cual, contrastando con la calificación de la percepción sobre la importancia de gestionar los riesgos

en sus proyectos vemos que el resultado obtenido va entre Media y Baja del 23.08%, y 10.26% respectivamente, (ver figura 33).

Figura 33 Nivel de Complejidad Alta de Proyectos vs Percepción de la Importancia de gestionar los riesgos



Fuente: Resultado Encuesta, autoría propia.

De lo cual podemos inferir que, a pesar de que los proyectos tengan una complejidad alta, en donde generalmente existe una mayor probabilidad de que los riesgos se materialicen, el nivel de conciencia sobre la importancia de gestionar los riesgos dentro de los proyectos es aún baja. En la siguiente tabla 6, se presenta la relación entre la categorización de complejidad de los proyectos versus la percepción en la importancia de gestionar los riesgos.

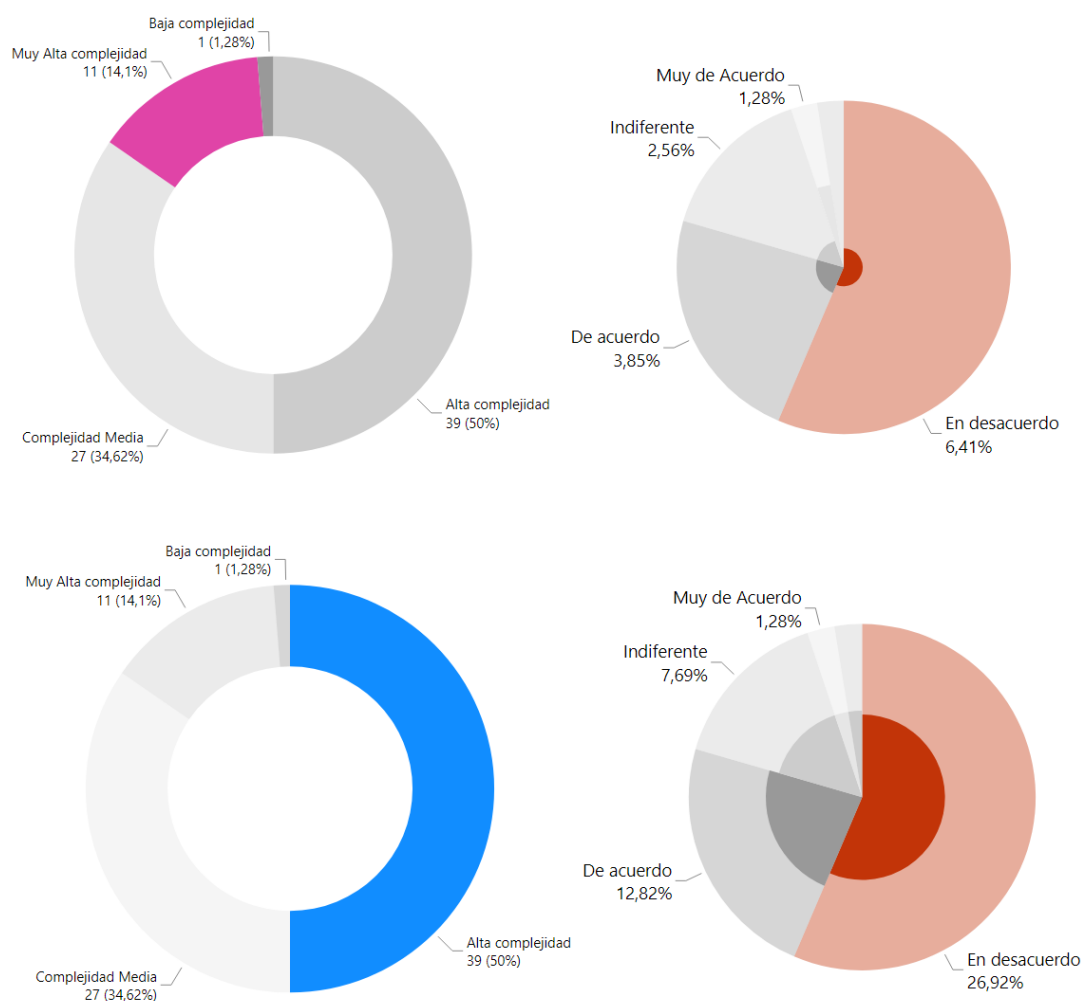
Tabla 6 Nivel de Complejidad de Proyectos vs Percepción de la Importancia de gestionar los riesgos

Nivel de Complejidad de los Proyectos		Percepción de la Importancia de gestionar los Riesgos en los Proyectos	
14.10%	Muy Alta	3.85%	Muy Alta
		3.85%	Alta
		2.56%	Media
		2.56%	Baja
		1.28%	Muy Baja
50.00%	Alta	2.56%	Muy Alta
		8.97%	Alta
		23.08%	Media
		10.26%	Baja
		5.13%	Muy Baja
34.60%	Media	0.00%	Muy Alta
		5.13%	Alta
		14.10%	Media
		12.82%	Baja
		2.56%	Muy Baja
1.30%	Baja	0.00%	Muy Alta
		0.00%	Alta
		0.00%	Media
		0.00%	Baja
		1.28%	Muy Baja

Fuente: Resultado Encuesta, autoría propia.

Por otra parte, vemos que el 64.10% de los encuestados dicen que sus proyectos están en nivel de complejidad Muy Alta y Alta, lo cual, contrastado con el nivel de conformidad de los tiempos invertidos para la gestión de riesgos en los proyectos, vemos que para una complejidad Muy Alta y Alta el 6.41% y 26.92%, respectivamente están en desacuerdo con los tiempos invertidos, (ver figura 34)

Figura 34 Nivel de Complejidad de Proyectos Muy Alta, y Alta vs nivel de conformidad del tiempo invertido para gestionar los riesgos.



Fuente: Resultado Encuesta, autoría propia

lo cual hace pensar que existe la apertura, y disposición de los diferentes gerentes de proyecto, líderes, y miembros de equipo, para invertir el tiempo que sea necesario para gestionar adecuadamente los riesgos en los proyectos.

En la siguiente tabla 7 se presenta la relación entre la categorización de complejidad de los proyectos versus el nivel de conformidad del tiempo invertido para la gestión de riesgos.

Tabla 7 Nivel de Complejidad de Proyectos vs nivel de conformidad del tiempo invertido para gestionar los riesgos.

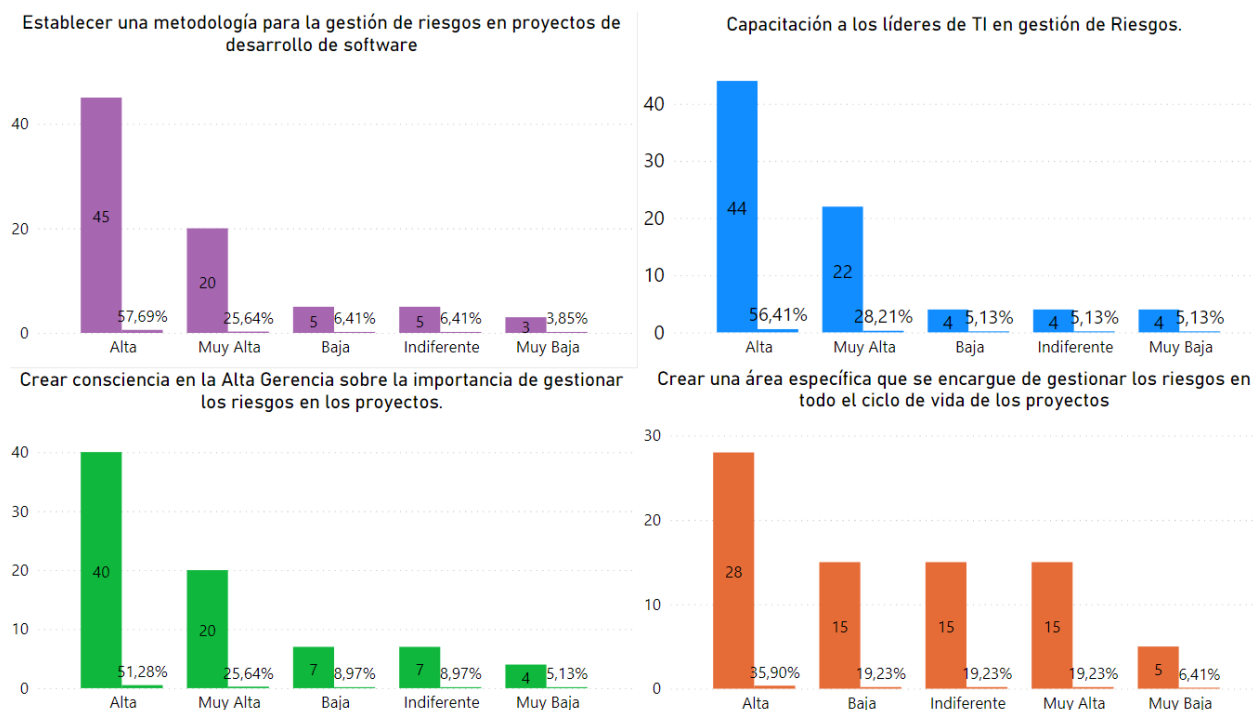
Nivel de Complejidad de los Proyectos		Nivel de Conformidad del tiempo invertido para gestionar los riesgos en los Proyectos	
14.10%	Muy Alta	0.00%	Muy en Desacuerdo
		6.41%	En desacuerdo
		2.56%	Indiferente
		3.85%	De acuerdo
		1.28%	Muy de acuerdo
50.00%	Alta	1.28%	Muy en Desacuerdo
		26.92%	En desacuerdo
		7.69%	Indiferente
		12.82%	De acuerdo
		1.28%	Muy de acuerdo
34.60%	Media	0.00%	Muy en Desacuerdo
		23.08%	En desacuerdo
		5.13%	Indiferente
		6.41%	De acuerdo
		0.00%	Muy de acuerdo
1.30%	Baja	1.28%	Muy en Desacuerdo
		0.00%	En desacuerdo
		0.00%	Indiferente
		0.00%	De acuerdo
		0.00%	Muy de acuerdo

Fuente: Resultado Encuesta, autoría propia.

Por otro lado, es de interés conocer, en base a la experiencia de los profesionales encuestados, qué factores se deben fortalecer o mejorar dentro de sus empresas para una adecuada gestión de los riesgos en los proyectos de desarrollo de software. Es así que, como se muestra en la siguiente figura 35, el 57.69% de los encuestados consideran de Alta importancia el establecer una metodología para la gestión de riesgos en proyectos de desarrollo de software, luego de ello y con un porcentaje del 56.41% se puede notar una necesidad Alta de capacitación a los líderes de proyectos en cuestión de gestión de riesgos, así mismo el crear consciencia en la alta gerencia sobre la importancia de gestionar los riesgos tiene un porcentaje Alto del 51.28%, finalmente el

35.90% manifiesta que crear un área específica que se encargue de gestionar los riesgos en todo el ciclo de vida de los proyectos es de importancia Alta.

Figura 35 En su experiencia, ¿Qué se debe mejorar o fortalecer para una adecuada gestión de riesgos en los proyectos de desarrollo de software de su empresa?

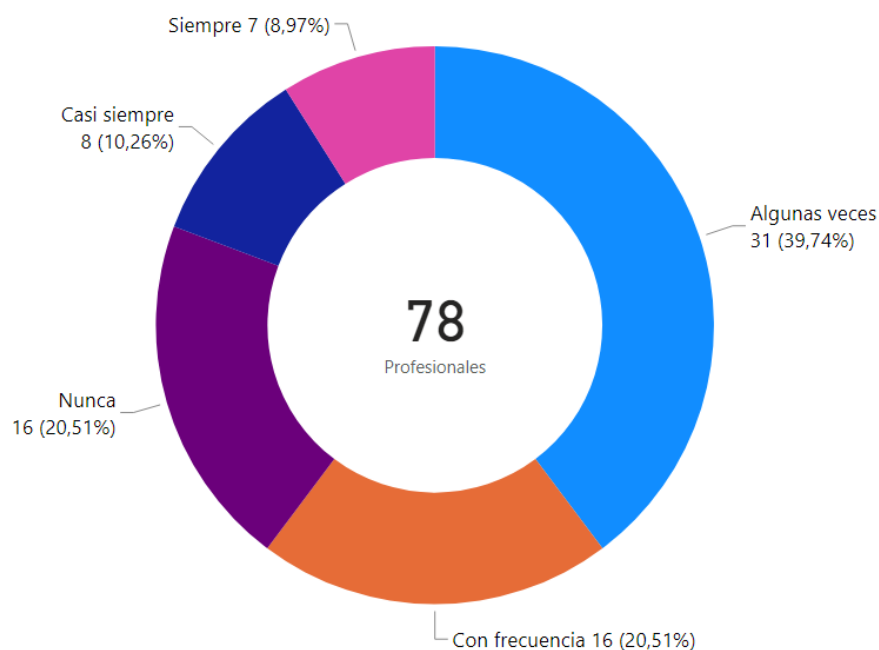


Fuente: Resultado Encuesta, autoría propia.

La siguiente figura 36, recoge resultados sobre si los profesionales encuestados se aseguran o no de utilizar alguna metodología de gestión de riesgos al momento de abordar nuevos proyectos.

Es así que, de los 78 encuestados, apenas el 8.97%, y el 10.25% aseguran que siempre, o casi siempre, utilizan una metodología de gestión de riesgos en sus proyectos, con lo cual se puede concluir que una mínima parte de las empresas a las que pertenecen los encuestados tienen procesos o metodologías establecidas y formales para la gestión de riesgos dentro del ciclo de vida de desarrollo de software de sus proyectos.

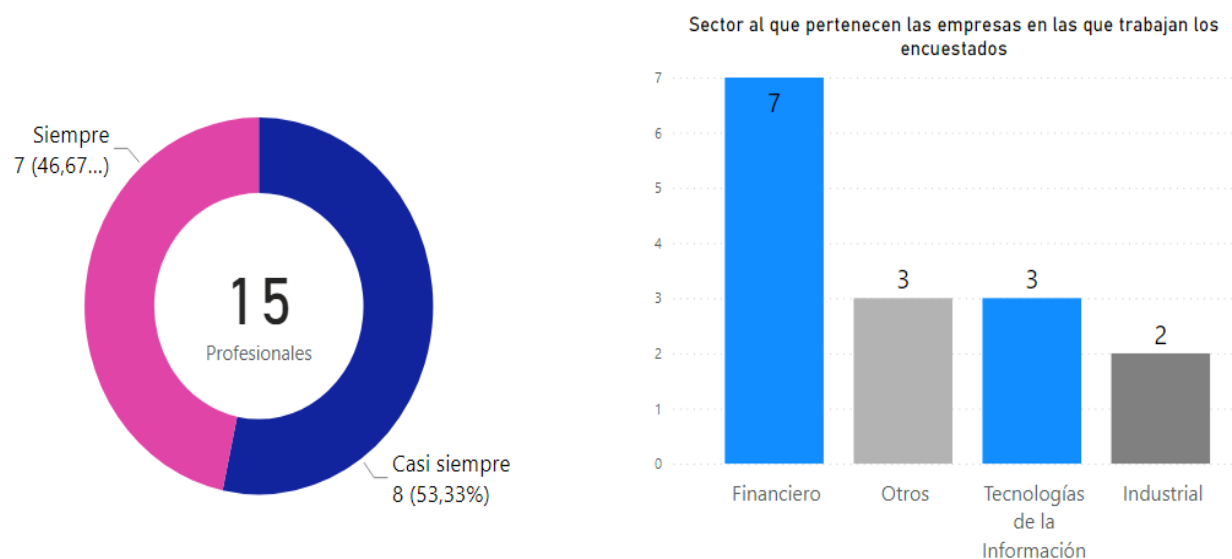
Figura 36 ¿En su empresa al momento de abordar un nuevo Proyecto de desarrollo de Software, se aseguran de cumplir con alguna metodología para gestionar los riesgos?



Fuente: Resultado Encuesta, autoría propia.

Sobre las respuestas anteriores, contrastándolas con el sector o giro de negocio al que pertenecen las empresas en donde prestan sus servicios los profesionales encuestados, podemos notar que siempre y casi siempre se utiliza una metodología de gestión de riesgos en los proyectos de desarrollo de software sobre todo en el sector financiero y sector de las tecnologías de la información. (Ver figura 37).

Figura 37 Sector de las empresas en las que trabajan los encuestados que siempre y casi siempre utilizan una metodología para gestionar los riesgos dentro de los proyectos de desarrollo de software.



Fuente: Resultado Encuesta, autoría propia.

Profundizando en la experiencia de los profesionales encuestados, una pregunta obligada y necesaria, fue conocer qué metodología de gestión de riesgos están utilizando dentro de los proyectos de desarrollo de software. En la siguiente tabla 8, se presentan los resultados ordenados decentemente por la metodología más utilizada, excluyendo las respuestas de, ninguna de las anteriores y otras.

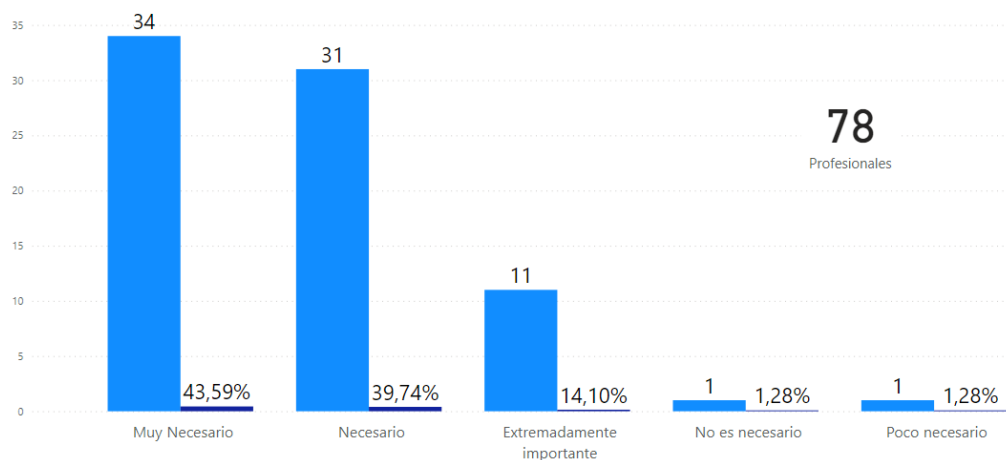
Tabla 8 ¿En su empresa se aplica alguna de las siguientes metodologías y/o normas para la gestión de riesgos en los proyectos de desarrollo de software?

METODOLOGÍA	Número de Profesionales que usan la metodología	Porcentaje
PMBOK.- Gestión de Riesgos de la guía de fundamentos para la dirección de proyectos.	27	34.62%
ISO 31000.- Estándar para la gestión del riesgo en cualquier organización.	6	7.69%
CRAMM. - Método de análisis y gestión de riesgos	3	3.85%
Gestión de Riesgos bajo el Marco de Trabajo CCMI	1	1.28%
MAGERIT.- Metodología de análisis y gestión de riesgos de las tecnologías de Información	0	0.00%
OCTAVE.- Conjunto de herramientas, técnicas y métodos para la evaluación del riesgo	0	0.00%
Otras	5	6.41%
Ninguna de las anteriores	36	46.15%
TOTALES:	78	100.00%

Fuente: Resultado Encuesta, autoría propia.

Sobre la necesidad de implementar o no una metodología ágil de gestión de riesgos en los proyectos de desarrollo de software, un 14.10% le ve extremadamente necesario, mientras que el 43.59%, y 39.74% le ve entre Muy Necesario y Necesario, respectivamente, lo cual evidencia que dentro de las empresas en las que trabajan los profesionales encuestados, existe la conciencia y necesidad mayoritaria de implementar una metodología para gestionar los riesgos en los proyectos de desarrollo de software. En la siguiente figura 38, se muestran los resultados obtenidos sobre esta pregunta.

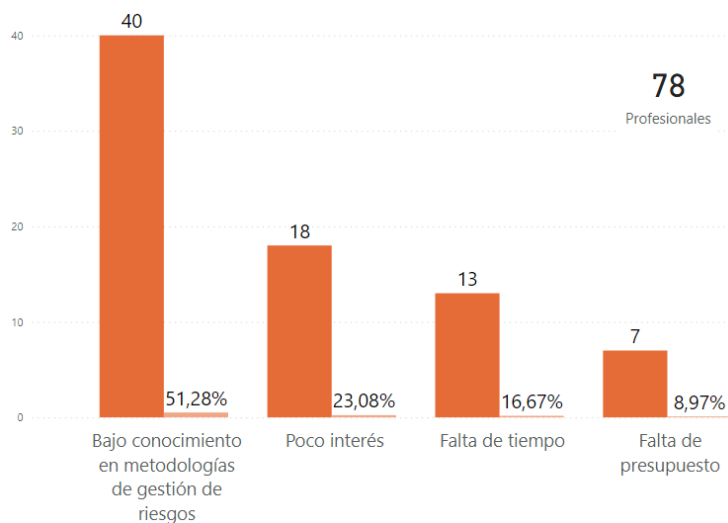
Figura 38 ¿En qué medida considera usted que es necesario adoptar una metodología ágil para la gestión de riesgos en los proyectos de desarrollo de software de su empresa?



Fuente: Resultado Encuesta, autoría propia.

Cuando preguntamos a los encuestados sobre las principales limitaciones que les impiden adoptar una metodología de gestión de riesgos en sus proyectos de desarrollo de software, se nota que el 51.28%, es decir la mayoría de profesionales, consideran que existe un bajo conocimiento en metodologías de gestión de riesgos, y apenas 7 profesionales que representa el 8.97% dicen no tener el presupuesto suficiente. En la siguiente figura 39, se muestran los resultados obtenidos sobre esta pregunta,

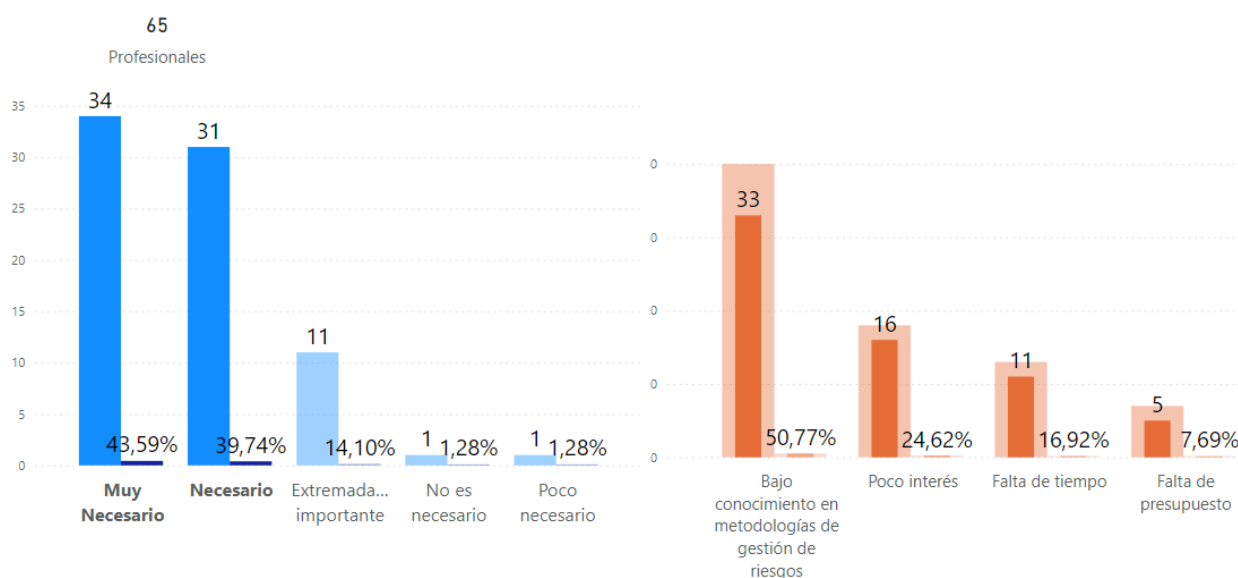
Figura 39 ¿Qué factor considera usted que es el principal limitante para no adoptar una metodología de gestión de riesgos en sus proyectos de desarrollo de software?



Fuente: Resultado Encuesta, autoría propia.

lo cual, contrastado con la necesidad de implementar una metodología de gestión de riesgos podemos ver que de los 65 encuestados que respondieron como Muy Necesario, y Necesario, el 50.77% considera que el conocimiento en metodologías de gestión de riesgos es el principal impedimento para adoptar una metodología. En tal virtud, se puede concluir que, aunque la necesidad es alta, hace falta trabajar mucho en adquirir conocimiento en gestión de riesgos. En la siguiente figura 40, se encuentran los resultados de esta relación.

Figura 40 Contraste de preguntas de necesidad de implementar una metodología versus las limitaciones.



Fuente: Resultado Encuesta, autoría propia.

En la siguiente figura 41, se recogen las respuestas de los encuestados en referencia a las consecuencias de no gestionar oportunamente los riesgos dentro los proyectos de desarrollo de software, en donde se puede notar que la arista del tiempo es la más afectada con un 41.03% que la califican como crítica, mientras que, en el alcance el 33.33% manifiesta una afectación grave, así también, en lo que se refiere al costo se ve que el 32.05% ha tenido consecuencias graves, finalmente en la arista de la calidad el 29.49% ha tenido afectaciones críticas. Con lo que podemos concluir que, el no gestionar adecuadamente los riesgos dentro de los proyectos de desarrollo de

software puede principalmente traer consecuencias graves y críticas en lo que respecta en primer lugar, al tiempo de entrega de los proyectos, seguido de cambios en el alcance, aumento de costo del proyecto y afectación de la calidad de los entregables.

Figura 41 ¿A su criterio, en qué medida afectó No gestionar oportunamente los riesgos en los últimos proyectos de desarrollo de software de su empresa?



Fuente: Resultado Encuesta, autoría propia.

4.1.3. Análisis comparativo de metodologías existentes

En la segunda fase del presente estudio, al identificar una variedad de normas, estándares, metodologías y marcos de referencia existentes relacionados con la gestión de riesgos, se tuvo que hacer un primer filtro, eligiendo como parámetro de selección, debido a su importancia y orientación de la investigación al enfoque, alcance y/o aplicación de cada una de las metodologías.

Así mismo, y con el sentido de contar con las metodologías más importantes, se decidió establecer como segundo factor, el hecho de saber si las metodologías son reconocidas a nivel internacional. En la siguiente tabla 9 se muestra las metodologías seleccionadas luego de aplicar los filtros mencionados.

Tabla 9 Metodologías de gestión de riesgos seleccionadas

METODOLOGÍA	DESCRIPCIÓN	PAIS ORIGEN	ENFOQUE, ALCANCE, APLICACIÓN
CRAMM	Metodología creada por la agencia de cómputo y telecomunicaciones del Reino Unido, traducida al español significa “Método de análisis y gestión de riesgos”	Reino Unido	Aplicable a todo tipo de sistemas y redes de información y se puede aplicar en todas las etapas del ciclo de vida del sistema de información, desde la planificación y viabilidad, a través del desarrollo e implementación.
CMMI	Marco de trabajo norteamericano subsidiado por ISACA que describe buenas prácticas que se deben aplicar en la industria de desarrollo, mantenimiento y adquisición de productos y servicios para ayudar a las empresas a mejorar sus procesos.	Estados Unidos	Dentro del ámbito de desarrollo de software, este marco de trabajo se ha convertido en un estándar para evaluar la calidad de los procesos de desarrollo de software en donde una arista importante es el manejo de los riesgos.
PMBOK	Guía de conocimiento para la gestión de proyectos del Instituto de Administración de proyectos PMI.	Estados Unidos	Administración y Ejecución de Proyectos
ISO 31000 2018	Norma de referencia aceptada mundialmente para la gestión del riesgo en cualquier tipo de organización.	Participación de miembros de más de 70 países	Cultura Organizacional, Planificación Estratégica
MAGERIT	Metodología de Análisis y Gestión de riesgos de las tecnologías de Información	España	Sistemas de Información digital
OCTAVE	Metodología de Evaluación de Amenazas Operacionalmente Críticas, Activos y Vulnerabilidades para agilizar y optimizar el proceso de evaluación de riesgos de seguridad de la información.	Estados Unidos	Enfocada en Seguridad de la Información

ISO 27001	Norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.	Ultima versión España, Asociación Española de Normalización (UNE)	Sistema de Gestión de Seguridad de la Información (SGSI)
-----------	----------------------------------------------------------------------------------------------------------------------------------------------------------------	-------------------------------------------------------------------	----------------------------------------------------------

Fuente: Tabla basada en las metodologías seleccionadas para el caso de estudio del presente trabajo.

Luego de clasificadas las metodologías por su alcance de aplicación y reconocimiento a nivel internacional, se compararon con los resultados de la encuesta (Ver tabla 8), para determinar cuáles son las metodologías más utilizadas o reconocidas por los profesionales encuestados a nivel local, con lo cual, finalmente, se seleccionaron cuatro metodologías sobre las cuales se realizó la investigación y el respectivo análisis comparativo.

En la siguiente tabla 10, como parte inicial del análisis, se presenta el propósito de cada una de las metodologías seleccionadas, juntamente con su estructura, fases o proceso para la gestión de riesgos.

Tabla 10 Comparación Metodologías de Riesgos según su propósito y estructura

METODOLOGÍA	PROPOSITO	FASES / ESTRUCTURA / PROCESOS
Guía PMBOK - Gestión de los riesgos del proyecto	El propósito se centra en aumentar la probabilidad y el impacto de los eventos o riesgos positivos, y disminuir la probabilidad y el impacto de eventos negativos en un proyecto.	<ol style="list-style-type: none"> 1. Planificar la Gestión de los Riesgos. 2. Identificar los Riesgos. 3. Realizar el Análisis Cualitativo de Riesgos. 4. Realizar el Análisis Cuantitativo de Riesgos 5. Planificar la Respuesta a los Riesgos 6. Implementar la Respuesta a los Riesgos 7. Monitorear los Riesgos
Marco de Referencia ISO 31000-2018:	Integrar, diseñar, implementar, valorar y mejorar la gestión del riesgo a lo largo de toda la organización	<p>El Proceso de Gestión de Riesgos está estructurado por:</p> <ol style="list-style-type: none"> 1. Establecer el Contexto 2. Evaluación de los Riesgos <ol style="list-style-type: none"> 2.1. Identificar los Riesgos 2.2. Análisis de los Riesgos 2.3. Valoración de los Riesgos 3. Tratamiento de los Riesgos

<p>Metodología CRAMM: (Risk Analysis and Management Method)</p>	<p>Metodología orientada a proteger la confidencialidad, integridad y disponibilidad de un sistema y de sus activos. Ayuda a las organizaciones a identificar los riesgos y sus propietarios, evaluar y definir niveles aceptables de los riesgos, identificar e implementar respuestas al riesgo.</p>	<p>Fase 1: Establecimiento de Objetivos de Seguridad Fase 2: Evaluación de riesgos Fase 3: Identificación y selección de contramedidas</p>
<p>Gestión de riesgos bajo el Marco de Trabajo CCMI</p>	<p>Evaluar la madurez de los procesos de una organización y proporcionar una orientación referente a cómo mejorar los procesos, y adoptar prácticas útiles para alcanzar los objetivos de negocio.</p>	<ol style="list-style-type: none"> 1. Definir la estrategia para manejar los riesgos y oportunidades. 2. Identificar y analizar los riesgos u oportunidades. 3. Establecer planes de mitigación y contingencia de los riesgos. 4. Establecer planes para aprovechar las oportunidades. 5. Implementar los planes para el manejo de riesgos u oportunidades.

Fuente: Tabla basada en las metodologías seleccionadas para el caso de estudio del presente trabajo.

Semejanzas y diferencias principales.

Dentro de la revisión y análisis se puede notar, que las cuatro metodologías presentadas tienen una estructura semejante, pues todas definen procesos y métodos para la identificación, evaluación, análisis, y planes de respuesta o tratamiento para gestionar los riesgos, sin embargo, la finalidad y objetivos que persiguen cada una, son diferentes, es así que la guía PMBOK se centra en el ciclo de vida de los proyectos en donde presenta una serie de procesos con sus entradas, herramientas y salidas, por su parte el principal objetivo de CRAMM es asegurar la continuidad del negocio salvaguardando los activos y sistemas relacionados.

Por otro lado, están los modelos CMMI y el estándar ISO 31000, de los cuales se podría decir que persiguen un objetivo común ya que los dos presentan modelos para evaluar y mejorar los procesos de gestión de riesgos con un alcance hacia toda la organización. Sin embargo, el concepto de cada una de ellas marca una diferencia muy importante, pues CMMI es un modelo de proceso para evaluar y calificar cual es el nivel de madurez de la organización, y está centrado únicamente en el desarrollo de software, no así ISO 31000 que puede ser aplicado a cualquier industria y es una

guía de principios y directrices genéricas que valida que los procesos se ajustan a los estándares establecidos.

En la siguiente tabla 11, se presenta una recopilación de varias ventajas y desventajas de cada uno de los modelos.

Tabla 11 Ventajas y Desventajas modelos de Gestión de Riesgos

METODOLOGÍA	VENTAJAS	DESVENTAJAS
Guía PMBOK - Gestión de los riesgos del proyecto	<ul style="list-style-type: none"> - Abarca todo el ciclo de vida del proyecto. - Alto grado de detalle en la descripción de sus procesos, lo cual facilita el entendimiento e implementación de la metodología. - Presenta un gran número de recomendaciones sobre herramientas y técnicas que se pueden aplicar para la gestión de riesgos - La identificación de riesgos es permanente, cíclica, desde inicio a fin del proyecto. 	<ul style="list-style-type: none"> - Para proyectos pequeños puede resultar demasiado engorroso y burocrático su implementación. - El proceso obliga a recorrer en su totalidad las actividades del proyecto, lo cual puede resultar una gestión redundante o excesiva.
Marco de Referencia ISO 31000-2018:	<ul style="list-style-type: none"> - Mejorar la eficiencia operativa. - Mejora la gobernabilidad interna de la organización. - Aumenta la confianza de partes externas. - Mejora el rendimiento y la sostenibilidad. - Reducir los costos. 	<ul style="list-style-type: none"> - No ofrece taxonomías de riesgos, mapas de calor, u otras herramientas de gestión. - Es una norma ISO no certificable.
Metodología CRAMM: (Risk Analysis and Management Method)	<ul style="list-style-type: none"> - Es aplicable a todo tipo de sistemas de información. - Posee una variedad de herramientas para aplicación de la metodología. - Esta soportada por una herramienta informática con una base de datos de: <ul style="list-style-type: none"> - Más de 400 tipos de Activos. - Más de 25 tipos de Impacto. - Mas de 38 tipos de Amenaza. - 7 Tipos de medida del Riesgo, y Más de 3500 salvaguardas. 	<ul style="list-style-type: none"> - No contempla elementos como procesos y recursos. - Alto costo de implementación y licencias de la herramienta.
Gestión de riesgos bajo el Marco de Trabajo CCMI	<ul style="list-style-type: none"> - Proporciona lenguaje lo cual mejora la comunicación entre clientes y empleados. - Aumenta la calidad de productos y servicios y reduce los tiempos de entrega. - Ayuda a reducir costos. - Ofrece un camino trazado para la mejora continua. 	<ul style="list-style-type: none"> - El modelo es complejo y es más utilizado en grandes empresas. - Especifica para empresas de software. - Indica las actividades que se deben de realizar, pero no define la forma de hacerlas.

Fuente: Tabla basada en las metodologías seleccionadas para el caso de estudio del presente trabajo.

4.2. Propuesta Metodológica

En función de toda la información recolectada y analizada, tanto del instrumento de encuesta, así como de la comparación de las metodologías existentes y seleccionadas en el presente trabajo, se expone el siguiente método genérico para gestionar riesgos dentro del ciclo de vida de los proyectos de desarrollo de software, el mismo que está orientado para que pueda ser utilizado en cualquier organización que desarrolle software bajo un marco de trabajo de agilidad, como lo es scrum.

4.2.1. Estructura planteada

En base al análisis comparativo realizado, en donde se vio que las metodologías seleccionadas presentan una estructura similar, se concluye planteando tres procesos genéricos para cubrir la gestión de riesgos dentro del ciclo de vida de desarrollo de software, estos son: proceso de identificación de riesgos, proceso de evaluación de riesgos, y un último proceso de respuesta a los riesgos. En la siguiente figura 42, se ilustra la estructura planteada, y a continuación se explica cada una.

Figura 42 Estructura propuesta para la gestión de riesgos en proyectos de desarrollo de Software



Fuente: Investigación propia elaborada por el autor.

Proceso Identificación de riesgos

En la identificación de los riesgos se debe considerar cualquier factor que influya sobre las actividades de los proyectos sean estos de carácter organizacional, político, legal, económico, tecnológico, etc. Para ello, se debe recurrir a diferentes fuentes de información externa y/o interna existente como informes públicos, factores económicos, lecciones aprendidas, documentación histórica, entre otros, así como también generar entrevistas, grupos focales, reuniones de trabajo para recoger opiniones y juicios de expertos.

Como parte primordial de esta fase se vio la necesidad de clasificar los riesgos identificados, ya que esto podría ayudar a buscar posibles soluciones para mitigar más de un riesgo a la vez, en tal virtud se plantea que la clasificación este dirigida a las restricciones básicas de un proyecto, estas son, alcance, tiempo, costo y calidad.

Proceso de Evaluación de Riesgos

En la evaluación de riesgos se debe llegar a establecer la probabilidad e impacto en base a la información obtenida en el proceso de identificación con el objetivo de establecer el nivel de riesgo, determinando así los peligros potenciales y sus posibles consecuencias. En esta fase es importante dejar marcados los riesgos de mayor probabilidad e impacto para que sean atendidos con mayor prioridad.

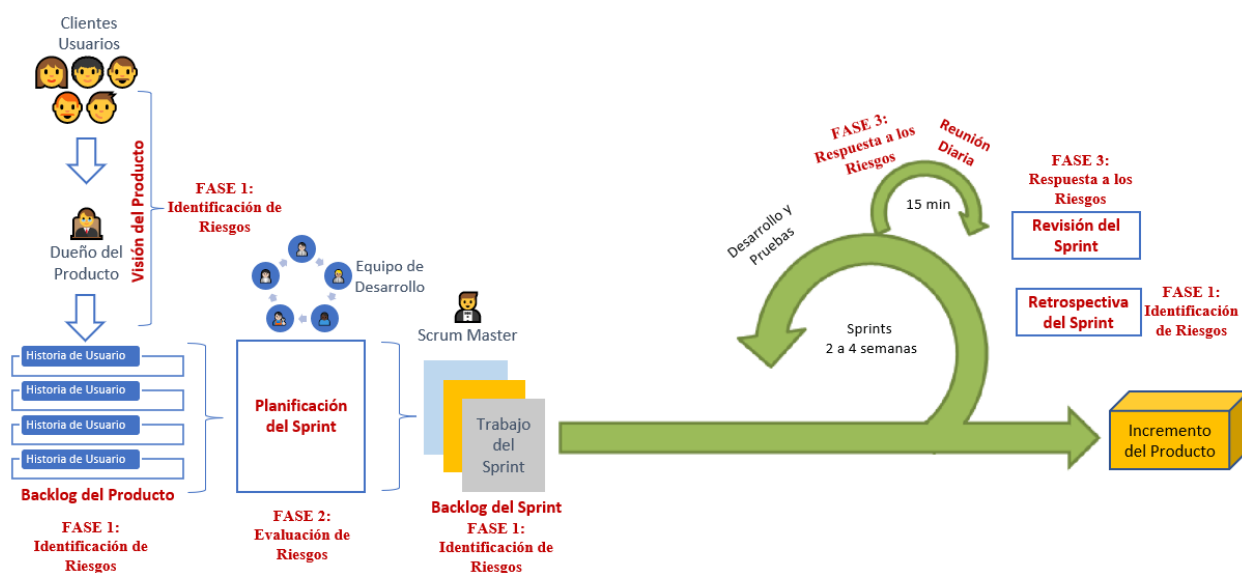
Proceso de Respuesta al Riesgo

Posibles acciones a implementar en donde se deberán tomar decisiones sobre aceptar los riesgos, mitigarlos o transferirlos según cada caso, con el objetivo de mejorar las oportunidades y disminuir las amenazas.

4.2.2. Puntos de gestión de riesgos dentro Scrum

En línea con el objetivo de plantear un modelo ágil para gestionar los riesgos en el desarrollo de software, a continuación, se explica cómo la estructura genérica planteada para gestionar los riesgos se relaciona con los eventos que se manejan dentro del marco de trabajo Scrum. Para ello, en primera instancia, se identificaron los puntos dentro del proceso Scrum en donde se debe tomar acción para gestionar los riesgos. En la siguiente figura 43, se ilustra los puntos mencionados en donde, además, se especifica la fase de gestión de riesgos que se debe ejecutar.

Figura 43 Identificación de puntos o eventos en donde se debe gestionar los riesgos.



Fuente: Investigación propia elaborada por el autor.

4.2.3. Procedimiento de gestión de riesgos con Scrum

Antes que nada, y previo a comenzar con los trabajos de desarrollo, es de suma importancia que todo el equipo del proyecto conozca la visión del negocio sobre el producto del proyecto y los objetivos que se quieren lograr con la ejecución del mismo, ya que esto, a más de crear una sinergia de equipo, facilita la toma de decisiones y retroalimentación. Visto desde la perspectiva de riesgos y del modelo planteado, es importante identificar los riesgos potenciales a un alto nivel desde un inicio, lo cual permitirá mitigar malos entendidos en referencia a las características y funcionalidades que debe cumplir el producto. Consecuentemente, y luego de tener definido los puntos en donde se debe cumplir una determinada acción para gestionar los riesgos dentro del marco de trabajo Scrum, en la siguiente tabla 12 se describe las actividades del procedimiento y sus beneficios.

Tabla 12 Descripción de Actividades de gestión de Riesgos dentro de Scrum

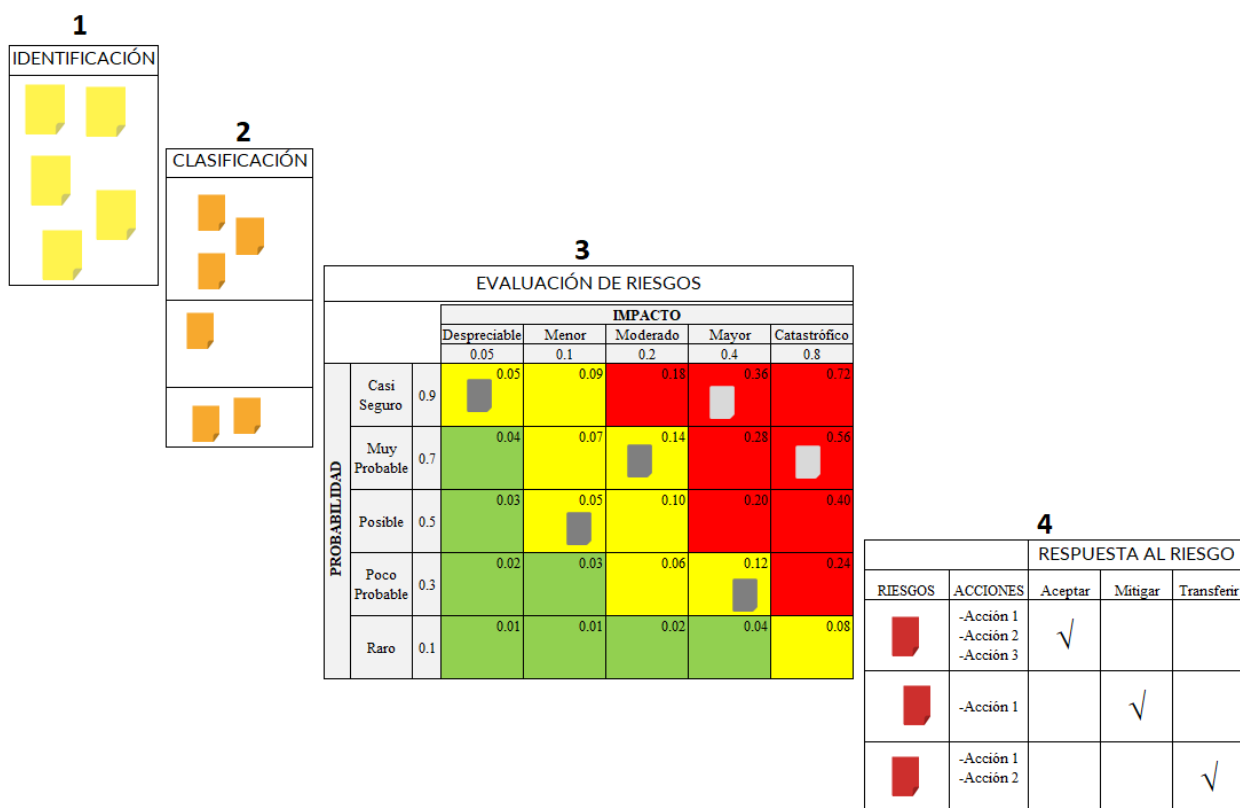
PROCESO	EVENTO / ARTEFACTO	ACTIVIDADES PROCEDIMIENTO	BENEFICIO
IDENTIFICACIÓN DE RIESGOS	Requisitos del cliente y Visión del Producto	- Entendimiento completo de la visión del producto. - Identificar riesgos potenciales de Alto Nivel. - Clasificar los riesgos en base a sus características.	- Identificación de posibles riesgos a nivel de Negocio, técnicos, comerciales, etc. (Ver Anexo 2 RBS). - Evitar tempranamente malas interpretaciones de las características y funcionalidad del producto.
	Backlog del Producto	- Identificación detalla de los riesgos sobre las Historias de Usuario. - Identificación de nuevos riesgos conforme cambie y/o se priorice el Backlog del producto.	- Prevenir posibles desvíos en el trabajo del proyecto. - Evitar confusiones en los conceptos o las características del producto que se va a construir. - Contar con un registro de riesgos actualizado para gestionar acciones oportunamente.
	Retrospectiva del Sprint	- Analizar riesgos materializados en el Sprint actual e identificar nuevos riesgos en base a la experiencia.	- Evitar que los riesgos se conviertan en problemas en los siguientes Sprints.
	Backlog del Sprint	- Identificar posibles riesgos dentro de unidades funcionales mas pequeñas.	- Gestionar de una manera rápida y sencilla riesgos pequeños.
EVALUACIÓN DE RIESGOS	Planificación del Sprint	- Analizar los riesgos que están relacionados a las funcionalidades que se realizarán en el Sprint Actual. - Determinar la probabilidad e Impacto de cada uno de los riesgos que se trabajarán en el Sprint Actual. (Ver Anexo 3 Matriz de Probabilidad e Impacto). - Determinar responsables de los riesgos. - Priorizar los riesgos.	- Enfocar el esfuerzo de la gestión de riesgos para evitar y/o mitigar los riesgos de mayor relevancia. - Determinar acciones oportunas con los responsables de los riesgos.
RESPUESTA A LOS RIESGOS	Reunión diaria	- Revisión diaria de riesgos identificados en las etapas anteriores. - Determinar posibles riesgos que se puedan materializar. - Determinar la estrategia de respuesta para los riesgos materializados.	- Tomar acciones inmediatas sobre los riesgos que están generando problemas.
	Revisión del Sprint	- Presentar riesgos que no se hayan podido mitigar completamente durante el Sprint, y definir la estrategia de respuesta.	- Asegurar que el producto cumpla con las expectativas.

Fuente: Investigación propia elaborada por el autor.

4.2.4. Cuadro de mando para control y monitoreo de riesgos

El objetivo primordial que se persigue con la gestión de riesgos es mantener controlados los riesgos para que estos no se conviertan en problemas que impidan alcanzar los objetivos del proyecto. Para cumplir con lo mencionado, es necesario contar con una herramienta que nos permita el registro de la identificación, análisis y respuesta a los riesgos, de tal manera que la gestión y estado de los riesgos siempre estén visibles para el equipo del proyecto y sus interesados, con la finalidad de que sea un insumo útil al momento de tomar decisiones. Para ello dentro del modelo propuesto, se sugiere el siguiente tablero de control el cual, se ilustra y explica a continuación.

Figura 44 Tablero de control y monitoreo de riesgos



Fuente: Investigación propia elaborada por el autor

Como se puede notar en la figura 44 anterior, la finalidad de contar con una herramienta de monitoreo y control de riesgos, es identificar en un solo vistazo, cuál es el estado de los riesgos, y cómo se están gestionando dentro del proyecto. En tal sentido, podemos notar que algunos riesgos estarán identificados, pero no clasificados, otros riesgos estarán en la fase de evaluación, o incluso en la fase de respuesta a los riesgos; todo esto con la premisa de atender siempre en primera línea a los riesgos de mayor probabilidad e impacto.

4.2.5. Premisas o Supuestos

Con el planteamiento de la metodología, se espera que los profesionales involucrados entorno a proyectos de desarrollo de software, puedan tener un entendimiento completo del modelo y en consecuencia, puedan implementar de una manera simple y transparente la gestión de riesgos en sus proyectos. En este punto es fundamental dejar explícito que, en el modelo, a pesar de estar planeado de una manera genérica, puede existir la respectiva personalización de acuerdo a la complejidad, tamaño y alcance de los proyectos, así como a la realidad de cada organización; esto implica que los responsables, a la hora de la implementación del modelo, puedan realizar ajustes ya sea en sus fases o artefactos propuestos.

Otra premisa importante que necesariamente debe quedar explícita, es que el modelo planteado está construido con el afán de mejorar o incluir la gestión de riesgos en proyectos de desarrollo de software, sin que eso implique o garantice el éxito o fracaso de los proyectos, ya que esto depende de varios factores dentro de cada organización.

Un supuesto que debe manejarse es que, para la implementación del modelo, debe existir la decisión y apoyo de los involucrados en la gestión de proyectos de la organización, pues de ellos dependerá el entendimiento, socialización y ejecución de las fases planteadas.

4.2.6. Objetivo de la propuesta metodológica

El objetivo de la propuesta metodológica es plantear un modelo de gestión de riesgos para proyectos de desarrollo de software bajo un marco de trabajo ágil, de tal manera que sea fácil de implementar y que aporte significativamente a la posibilidad de éxito de los proyectos que se ejecutan en las diferentes organizaciones.

4.2.7. Objeto de la propuesta

La propuesta está dirigida principalmente a equipos de desarrollo de software independientemente del giro de negocio de la organización, en consecuencia, la adaptación e implementación del modelo planteado dependerá totalmente y en primer orden de los procesos y gobierno de cada organización, así como de la visión y mejora continua que tienen los equipos de desarrollo de software.

4.2.8. Responsables de la implementación y control

La responsabilidad directa de la implementación cae sobre los gerentes de proyectos, líderes y equipo de desarrollo de software, así como también de patrocinadores de proyectos y gerencias interesadas y relacionadas con los proyectos de la organización.

El control del modelo y mejoras que se puedan realizar es responsabilidad de los gerentes de proyectos y líderes de equipos de desarrollo, quienes pueden adaptar el modelo planteado a las necesidades y características particulares de cada institución y equipo.

4.2.9. Fases para su puesta en práctica

La puesta en práctica del método planteado dependerá sin duda de la madurez de la organización y del equipo de desarrollo de software, para ello se sugiere seguir las siguientes fases:

1. Fase de entendimiento. - comprende una revisión de la estructura del modelo planteado y los puntos de gestión de riesgos que se deben ejecutar dentro del marco de referencia Scrum.
2. Fase de adaptación. - una vez comprendido la propuesta del modelo, los responsables de la implementación, deberán realizar las adaptaciones necesarias de acuerdo a la realidad de cada equipo de desarrollo y su entorno. En este punto es importante considerar la automatización de la herramienta de control y monitoreo de riesgos propuesta en el presente modelo.
3. Fase de Prueba y Evaluación. - para afinar el uso del modelo de gestión de riesgos dentro del marco de trabajo Scrum, necesariamente se debe ejecutar ya sea un proyecto piloto completo, o varios Sprints de prueba de cualquier proyecto de desarrollo de software, esto con la finalidad de validar que el modelo agregue valor al momento de la gestión.

4.2.10. Indicadores de evaluación.

En vista de que, el modelo planteado está dirigido para ser utilizado en un ambiente ágil y dinámico, en donde se depende de factores ambientales de la organización, equipo de trabajo,

complejidad y demás aristas propias de los proyectos de desarrollo de software, se consideran los siguientes indicadores de evaluación para una adopción y uso del modelo.

Grado de Aceptación. - Número de participantes del equipo de proyecto que aceptan la propuesta del modelo, dividido para el total de participantes del equipo de proyecto.

Grade de Satisfacción. - Número de participantes del equipo de proyecto satisfechos con la aplicación del modelo, dividido para el total de participantes del equipo de proyecto.

Debiendo en los dos casos cumplir con una mayoría relativa, es decir que al menos la mitad más uno de los participantes de los proyectos debería estar de acuerdo, en tal situación estos indicadores deberían evaluarse antes de iniciar un nuevo proyecto.

CONCLUSIONES

Una vez finalizado el presente trabajo, a continuación, se señalan las siguientes conclusiones:

- En línea con la realidad actual de las organizaciones, que cada vez más dependen de la tecnología, y en específico, de las áreas de desarrollo de software, es importante que las mismas cuenten con herramientas y métodos de gestión de riesgos específicos que les permita comunicar y transparentar los riesgos hacia la organización.
- Los riesgos e incertidumbre siempre estarán presentes en los proyectos de desarrollo de software por lo cual es necesario contar con una metodología que le permita al equipo de desarrollo gestionarlos de una manera sencilla y transparente sin que ello desvíe la concentración y esfuerzo del equipo.
- Aunque hay una conciencia clara de la importancia de gestionar los riesgos en proyectos de desarrollo de software, el interés y conocimiento por parte de los profesionales para adoptar y aplicar una metodología es baja, cuyo efecto inmediato es que no se gestionen los riesgos oportunamente.
- La Guía del PMBOK y su área de conocimiento de gestión de riesgos es la más conocida entre los profesionales encuestados quienes afirman aplicarla dentro de sus proyectos de la organización.
- La mayoría de metodologías analizadas en el presente trabajo, presentan una estructura similar a la hora de gestionar los riesgos, lo cual permitió plantear un método genérico que consta de tres procesos principales: identificación, evaluación y respuesta a los riesgos.
- En base a la estructura planteada para la gestión de riesgos, se identificaron los puntos en referencia a eventos y artefactos dentro del marco de trabajo Scrum, en donde se deben ejecutar diferentes acciones para la gestión de riesgos dentro del desarrollo de software.
- Se elaboró una plantilla que sirve de herramienta para que los interesados y equipo de proyecto puedan tener una visión completa de la gestión que se está realizando sobre los riesgos identificados.

- Al ser la metodología propuesta sobre un marco de trabajo ágil, la misma queda expuesta a adecuaciones y adaptaciones de acuerdo a la realidad de los equipos de proyectos y realidades empresariales.
- Finalmente, aunque la metodología propuesta no es oficial, está soportada por las actividades que están descritas en los procesos de gestión de riesgos de normas y estándares certificados y seleccionados en el presente trabajo, por lo que podría aplicarse a un caso real.

RECOMENDACIONES

- Previo a adoptar una nueva metodología de trabajo es fundamental contar con el apoyo de la alta gerencia o directivos claves que soporten la decisión e impulsen el cambio.
- Para las empresas, cuya decisión sea adoptar el modelo propuesto se sugiere realizar un análisis previo de su realidad, tanto organizativa como de equipo de proyecto, y seguir los pasos establecidos para la adopción y prueba del modelo.
- Se sugiere implementar una herramienta que permita automatizar la gestión de riesgos desde su identificación hasta el tratamiento y repuestas.
- La metodología está planteada sobre un ambiente de agilidad y equipos de trabajo pequeños, por lo cual, y en caso de requerir su implementación en otros escenarios, la misma deberá ser evaluada desde su estructura.
- Es recomendable evaluar periódicamente la aceptación y conformidad del equipo de proyecto frente al uso de la metodología establecida para la gestión de riesgos, lo cual permitirá mantener un constante cambio y mejora continua.

AGRADECIMIENTOS

Agradezco a Dios por darme la vida y presentarme siempre nuevas oportunidades de mejorar, tanto a nivel espiritual como profesional.

Un agradecimiento especial y de corazón a mis seres queridos principalmente a mi padres, esposa e hijos, que son el motor e inspiración diaria para alcanzar nuevos objetivos.

Un agradecimiento sincero a mi director de tesis el Ing. César Ayala, por su tiempo, dedicación y orientación para concluir con éxito el presente trabajo.

REFERENCIAS BIBLIOGRÁFICAS

- Alaimo, D. (2013). *Proyectos ágiles con Scrum Flexibilidad, aprendizaje, innovación y colaboración en*. Buenos Aires: Ediciones kloor. Obtenido de <http://www.kloor.la>
- Arévalo et al. (2017). Metodología Ágil para la Gestión de Riesgos Informáticos. *Killkana Técnica*, 31.
- Buitrago, R. A. (2014). *Metodologías para la gestión de riesgos en proyectos de software y su adaptación en Stefanini, Univeridad Militar Nueva Granada*. Respositorio Institucional. Obtenido de <https://es.slideshare.net/fredleyton/metodologas-para-la-gestin-de-riesgos-en-proyectos-de-software>
- Carnegie Mellon University. (2010). *Mejora de los procesos para el desarrollo de mejores productos y servicios*. Obtenido de www.sei.cmu.edu/library
- Celina Oviedo, H. y. (2005). Aproximación al uso del coeficiente alfa de Cronbach. *Revista Colombiana de Psiquiatría*, 572-580.
- Crespo Martínez, E., & Cordero Torres, G. (2016). ESTUDIO COMPARATIVO ENTRE LAS METODOLOGÍAS CRAMM Y MAGERIT PARA LA GESTIÓN DE RIESGO DE TI EN LAS MPYMES. *UDA AKADEM*.
- ISACA, COBIT 5. (2012). *COBIT 5 (Objetivos de control para la información y tecnologías relacionadas)*. EEUU. Obtenido de <https://www.isaca.org/>
- Lind, Marchal, & Wathen. (2012). *Estadística aplicada a los negocios y la economía*. México, D.F.: McGRAW-HILL.
- Martinez, C. (2017). Ecu@Risk, Una metodología para la gestión de Riesgos aplicada a las MPYMES. *Enfoque UTE*, 8(1), 107-121. Obtenido de <https://doi.org/10.29019/enfoqueute.v8n1.140>
- Ministerio de Hacienda y Administraciones Públicas. (2012). *MAGERIT – versión 3.0* (Vol. 1). Madrid: Subdirección General de Información, Documentación y Publicaciones. Obtenido de <http://administracionelectronica.gob.es/>
- Miranda, M. F. (2015). *PROPUESTA DE UN PLAN DE GESTIÓN DE RIESGOS DE TECNOLOGÍA APLICADO EN LA ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL*. ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL, Guayaquil, Guayas, Ecuador.
- Organización Internacional de Normalización 31000. (2018). *ISO 31000:2018*. (G. d. 262, Trad.) Organización Internacional de Normalización. Obtenido de <https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:es>
- Palacio, J. (2008). *Gestión de proyectos Scrum Manager*. Obtenido de <https://www.safecreative.org/work/0808180903131-scrummanager-gestion-de-proyectos>
- PMI Guía de los Fundamentos para la dirección de Proyectos (PMBOK. 6ª Edición). (2017). *Guía de los Fundamentos para la dirección de Proyectos (PMBOK. 6ª Edición)*. Filadelfia, Estados Unidos: Project Management Institute (PMI).

- PMI Guía de los fundamentos para la dirección de Proyectos (PMBOK. 7ª Edición). (2021). *Guía de los fundamentos para la dirección de Proyectos Séptima Edición*. Pennsylvania: Project Management Institute, Inc.
- PMI Pulse of the profession. (2018). El éxito en tiempos de disrupción. *Pulse of the profession*.
- PMI The standard for risk management in portfolios, programs and projects. (2019). *Estándar para la administración de riesgos en portafolios, programas y proyectos*. Pensilvania: PMI. Obtenido de www.pmi.org
- Schwaber, K., & Sutherland, J. (2017). *La Guía Definitiva de Scrum: Las Reglas del Juego*.
- Standish Group. (2015). *Informe Chaos 2015*. Standish Group. Obtenido de <https://www.infoq.com/articles/standish-chaos-2015/#anch128452>
- Turley, F. (2010). *El Modelo de Procesos PRINCE2® Una magnífica introducción a PRINCE2*. (A. B. Academy, Ed., & J. L. Ramírez, Trad.) Obtenido de <https://jlfpr-prince2.blogspot.com/>
- VMedu, Inc. (2013). *Una guía para el CONOCIMIENTO DE SCRUM (GUÍA SBOK™)*. Arizona: SCRUMstudy™. Obtenido de www.scrumstudy.com
- Wong, S., Kwai, S., & Tang, D. (2010). Strengthening Risk Evaluation in Existing Risk Diagnosis Method. *Industrial Engineering and Management Systems*, 41-53.

ANEXOS

Anexo 1: Encuesta

Formato utilizado para recolectar información de profesionales de tecnología de la información.

Metodologías de Gestión de Riesgos en Proyectos de Desarrollo de Software.

Estimad@ profesional, la presente encuesta tiene el objetivo de recoger información relacionada a la gestión de riesgos en proyectos de desarrollo de software. Todas las respuestas proporcionadas serán tratadas bajo una estricta confidencialidad y serán utilizadas únicamente para fines netamente investigativos.

Correo electrónico *

Correo electrónico válido

Este formulario recopila correos electrónicos. [Cambiar la configuración](#)

1. ¿Con cuántos empleados cuenta la empresa en la que actualmente presta sus servicios? *

- 1 a 9
- 10 - 49
- 50 - 199
- 200 o más.



2. ¿Seleccione el principal giro de negocio al que pertenece su empresa? *

1. Industrial
2. Financiero
3. Tecnologías de la Información
4. Salud
5. Servicios
6. Educación
7. Gobierno
8. Alimentos
9. Otros



3. ¿Qué rol usted desempeña dentro de los proyectos de desarrollo de software de su empresa? *

- Jefe de Proyecto
- Sponsor - Alta Dirección
- Líder Técnico
- Arquitecto
- Miembro del Equipo
- Especialista de Calidad
- Especialista de Seguridad
- Otra...



4. ¿Qué nivel de complejidad usted considera que tuvieron los proyectos que se ejecutaron en su empresa en los últimos 12 meses? *

- Muy Baja complejidad
- Baja complejidad
- Complejidad Media
- Alta complejidad
- Muy Alta complejidad



5. ¿Dentro de su empresa, cómo usted percibe la importancia que le dan a la gestión de riesgos en proyectos de desarrollo de software? *

1. Muy Baja
2. Baja
3. Media
4. Alta
5. Muy Alta

6. ¿ En su experiencia, cree que los tiempos que son empleados para gestionar los riesgos en los ^{*} proyectos de desarrollo de software de su empresa son suficientes?

1. Muy de Acuerdo
2. De acuerdo
3. Indiferente
4. En desacuerdo
5. Muy en desacuerdo

⋮

7. ¿En su experiencia, qué se debe mejorar o fortalecer para una adecuada gestión de riesgos ^{*} en los proyectos de desarrollo de software de su empresa?

	Muy Baja	Baja	Indiferente	Alta	Muy Ata
Crear conscien...	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Capacitación a ...	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Establecer una ...	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Crear una área ...	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

8. ¿En su empresa al momento de abordar un nuevo Proyecto de desarrollo de Software, se aseguran de cumplir con alguna metodología para gestionar los riesgos? *

- Nunca
- Algunas veces
- Con frecuencia
- Casi siempre
- Siempre

:::

9. ¿En su empresa se aplica alguna de las siguientes metodologías y/o normas para la gestión de riesgos en los proyectos de desarrollo de software? *

- CRAMM. - Método de análisis y gestión de riesgos
- PMBOK.- Gestión de Riesgos de la guía de fundamentos para la dirección de proyectos.
- Gestión de Riesgos bajo el Marco de Trabajo CCMI
- ISO 31000.- Estándar para la gestión del riesgo en cualquier organización.
- MAGERIT.- Metodología de análisis y gestión de riesgos de las tecnologías de Información
- OCTAVE.- Conjunto de herramientas, técnicas y métodos para la evaluación del riesgo
- Ninguna de las anteriores
- Otra...



10. ¿En qué medida considera usted que es necesario adoptar una metodología ágil para la gestión de riesgos en los proyectos de desarrollo de software de su empresa? *

- No es necesario
- Poco necesario
- Necesario
- Muy Necesario
- Extremadamente importante



11. ¿Qué factor considera usted que es el principal limitante para no adoptar una metodología de gestión de riesgos en sus proyectos de desarrollo de software? *

- Poco interés
- Falta de presupuesto
- Bajo conocimiento en metodologías de gestión de riesgos
- Falta de tiempo



12. ¿A su criterio, en qué medida afectó No gestionar oportunamente los riesgos en los últimos proyectos de desarrollo de software de su empresa? *

	Marginal	Grave	Crítico	Desastroso	Catastrófico
En Tiempo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
En Costo	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
En Alcance	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
En Calidad	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Anexo 2:

Extracto de una Estructura de Desglose de los Riesgos (RBS) de Muestra.

NIVEL 0 de RBS	NIVEL 1 de RBS	NIVEL 2 de RBS
0. TODAS LAS FUENTES DE RIESGO DEL PROYECTO	1. RIESGO TÉCNICO	1.1 Definición del alcance
		1.2 Definición de los requisitos
		1.3 Estimaciones, supuestos y restricciones
		1.4 Procesos técnicos
		1.5 Tecnología
		1.6 Interfaces técnicas
		Etc.
	2. RIESGO DE GESTIÓN	2.1 Dirección de proyectos
		2.2 Dirección del programa/portafolio
		2.3 Gestión de las operaciones
		2.4 Organización
		2.5 Dotación de recursos
		2.6 Comunicación
		Etc.
	3. RIESGO COMERCIAL	3.1 Términos y condiciones contractuales
		3.2 Contratación interna
		3.3 Proveedores y vendedores
		3.4 Subcontratos
		3.5 Estabilidad de los clientes
		3.6 Asociaciones y empresas conjuntas
		Etc.
	4. RIESGO EXTERNO	4.1 Legislación
4.2 Tasas de cambio		
4.3 Sitios/Instalaciones		
4.4 Ambiental/clima		
4.5 Competencia		
4.6 Normativo		
Etc.		

Fuente: Tabla tomada de la Guía PMBOK sexta edición, pág. 406.

Anexo 3:

Matriz de Probabilidad e Impacto para determinar el nivel del Riesgo

			IMPACTO				
			Despreciable	Menor	Moderado	Mayor	Catastrófico
			0.05	0.1	0.2	0.4	0.8
PROBABILIDAD	Raro	0.9	0.05	0.09	0.18	0.36	0.72
	Poco Probable	0.7	0.04	0.07	0.14	0.28	0.56
	Posible	0.5	0.03	0.05	0.10	0.20	0.40
	Muy Probable	0.3	0.02	0.03	0.06	0.12	0.24
	Casi Seguro	0.1	0.01	0.01	0.02	0.04	0.08

Fuente: Tabla tomada de la Guía PMBOK sexta edición, pág. 408.