

**UNIVERSIDAD NACIONAL DE LA AMAZONIA PERUANA**



**FACULTAD DE INGENIERIA DE SISTEMAS  
E INFORMÁTICA**



**“Determinación de una metodología para la gestión de Riesgos en  
Proyectos de Desarrollo de Software”**

**INFORME DE TRABAJO PRÁCTICO DE SUFICIENCIA**

**PARA OPTAR EL TITULO PROFESIONAL DE:  
INGENIERO DE SISTEMAS E INFORMATICA**

**PRESENTADO POR EL BACHILLER:  
JEAN PIERRE PEREZ MEDINA**

**ASESOR:  
ING. RUIZ HIDALGO, FRANCISCO MIGUEL**

**IQUITOS –PERÚ  
2014**

## **DEDICATORIA**

A Dios, por permitirme llegar a este momento tan especial en mi vida. Por los triunfos y los momentos difíciles que me han enseñado a valorarlo cada día más, A mi madre por ser la persona que me ha acompañado durante todo mi trayecto estudiantil y de vida, A mi padre quien con sus consejos ha sabido guiarme para culminar mi carrera profesional. A mis amigos, que gracias al equipo que formamos logramos llegar hasta el final del camino y que hasta el momento, seguimos siendo amigos. A mis profesores, gracias por su tiempo, por su apoyo así como por la sabiduría que me transmitieron en el desarrollo de mi formación profesional.

**Bach. Jean Pierre Pérez Medina**



## 2. RESUMEN

Mediante este proyecto se pretende determinar una metodología que permite gestionar los riesgos de proyectos de desarrollo de software, aplicando dicha metodología a la empresa IquitosPlay, así mismo se aplica la metodología propuesta a uno de los proyectos que desarrolla la empresa.

La administración de proyectos, cuenta hoy en día, con una serie de herramientas tecnológicas a disposición de los profesionales en la materia, así como una serie de pautas, resultado de la puesta en ejecución de los principios de la administración de proyectos, esto permite realizar análisis bien fundamentados.

En el presente proyecto, se aplicaran las técnicas sugeridas en la Guía PMBOOK del Project Management Institute (PMI), donde se establecen una serie de pautas para la elaboración de un plan de gestión de riesgos bien estructurado. El proceso de la Gestión de Riesgos comienza por una Planificación de la Gestión de Riesgos, seguido de la Identificación de riesgos e incertidumbres para luego realizar análisis de riesgos, que puede ser cualitativa o cuantitativa. Posteriormente, una vez definidas la probabilidad, el impacto y la vulnerabilidad en la etapa de análisis, se procede a planificar la respuesta a los riesgos. En el caso de tratarse de amenazas, el tipo de respuesta puede ser transferir, evitar, absorber o mitigar. Luego, los riesgos son monitoreados para observar su evolución, y si ocurre algún cambio en las condiciones o en las circunstancias del proyecto, se procede al punto inicial, es decir, identificar y analizar los riesgos y sus nuevas condiciones.

Como resultado del proyecto se definieron los pasos de la metodología propuesta, y la forma como se debería integrar los procesos de la gestión de riesgos, involucrando las necesidades que ciertos procesos requieran para finalizar correctamente un proyecto de desarrollo de software. Como herramientas se crearon plantillas de Identificación de riesgos, plan de respuestas a los riesgos e informe de monitoreo de riesgos. Las categorías de riesgos quedaron definidas como riesgos técnicos, riesgos de proyectos y Riesgos de Negocio.

Por último se desarrolló un proyecto piloto, que consiste en aplicar la metodología propuesta a un proyecto que ejecuta la empresa IquitosPlay, pues este desarrolla proyectos de desarrollo de software.



### 3. ABSTRACT

This project aims to determine a methodology to manage the risks of software development projects, applying this methodology to the company IquitosPlay, also the proposed methodology one of the projects that the company applies.

Project management, has today, with a range of technology available to professionals in the field tools as well as a set of guidelines, a result of the implementation of the principles of project management, this allows well-founded analysis.

In this project, the techniques suggested in the PMBOOK Guide Project Management Institute (PMI), where a set of guidelines established for the development of a management plan well structured risks apply. The process of risk management begins with a Planning Risk Management, followed by the identification of risks and uncertainties and then perform risk analyzes, which may be qualitative or quantitative. Later, once the probability, impact and vulnerability in the analysis stage defined, we proceed to plan risk response. In the case of hazards, the type of response can be transferred, prevent, absorb or mitigate. Then risks are monitored to observe its evolution, and if any change occurs in the conditions or circumstances of the project, proceed to the starting point, ie, to identify and analyze the risks and their new conditions.

As a result of the project were defined steps of the proposed methodology, and how it should integrate the processes of risk management requirements involving certain processes required to complete a software development project properly. As tools templates Hazard identification, plan risk responses and risk monitoring report were created. The categories of risks were defined as technical risks, project risks, and Business Risk.

Finally a pilot project, which is to apply the proposed methodology to a project that is running the company IquitosPlay because this develops software development projects are developed.



## INDICE

<b>2. Resumen.....</b>	<b>2</b>
<b>3. Abstract.....</b>	<b>3</b>
<b>4. Índice.....</b>	<b>4</b>
4.1. Índice de Contenidos.....	4
4.2. Índice de Figuras.....	5
4.3 Índice de Cuadros .....	6
<b>5. Justificación.....</b>	<b>7</b>
<b>6. Objetivos.....</b>	<b>8</b>
6.1. Objetivo General.....	8
6.3 Objetivos específicos.....	8
<b>7. Desarrollo del tema.....</b>	<b>9</b>
7.1. Teoría de la temática.....	9
7.1.1. Definición y componentes del riesgo.....	9
7.1.2. Amenazas y vulnerabilidades.....	9
7.1.3. Mapa de Riesgos.....	10
7.1.4. Niveles de Aceptación del Riesgo.....	10
7.1.5. Plan de acción.....	11
7.1.6. Control y Monitoreo del Riesgo.....	10
7.1.7. Gestión de Riesgos de los Proyectos.....	11
7.1.8. Procesos de la Gestión de Riesgos.....	11
7.1.8.1. Planificar la Gestión de Riesgos.....	11
7.1.8.2. Identificar los Riesgos.....	12
7.1.8.3. Realzar el Análisis Cualitativo de Riesgos.....	16
7.1.8.4. Realizar el Análisis Cuantitativo de Riesgos.....	18
7.1.8.5. Planificar la Respuesta a los Riesgos.....	19
7.1.8.6. Seguimiento y Control de Riesgos.....	21
7.2. Desarrollo de la metodología de Gestión de riesgos.....	23
7.3. Aplicación de la metodología- Caos de estudio.....	34
7.3.1. Descripción del Proyecto.....	34
7.3.2. Gestión de Riesgos.....	35
<b>8. Conclusiones.....</b>	<b>40</b>
<b>9. Referencia Bibliográfica.....</b>	<b>41</b>
<b>Anexos.....</b>	<b>42</b>
Anexo 1: Plantilla de Registro de Riesgo .....	39
Anexo 2: Plantilla de Registro de Lecciones Aprendidas.....	47
Anexo 3: Estructura de Descomposición de Trabajo ( Desarrollo del Sistema- Cámara de Comercio)....	49
Anexo 4: Cuestionario basado en la taxonomía.....	50
Anexo 5: Plan de Contingencia de Equipos de Cómputo y software para Iquitos Play.....	67
Anexo 6 - Planes de respuesta a los riesgos – Caso de estudio .....	71



### 3.2. Índice de Figuras

<b>FIGURA 1</b> Interacción entre vulnerabilidades, amenazas y riesgos .....	9
<b>FIGURA 2</b> Taxonomía de Riesgos de Desarrollo de Software .....	15
<b>FIGURA 3</b> Categorías relacionadas con la identificación de riesgos en proyectos de software.....	26
<b>FIGURA 4</b> : Distribución estadística de Riesgo Nro 2- @Risk .....	36
<b>FIGURA 5</b> : Distribución estadística de Riesgo Nro 3- @Risk .....	37
<b>FIGURA 6</b> : Distribución estadística de Riesgo Nro 6- @Risk .....	37
<b>FIGURA 7</b> : Distribución estadística de Riesgo Nro 8- @Risk .....	38
<b>FIGURA 8</b> : Simulación de Montecarlo- @Risk .....	39



### 3.3. Índice de Cuadros

<b>CUADRO 1</b> Valores de Probabilidad .....	23
<b>CUADRO 2</b> Valores de Impacto .....	24
<b>CUADRO 3</b> Impacto del Riesgo Negativo o Amenaza .....	24
<b>CUADRO 4</b> Impacto de la Oportunidad .....	25
<b>CUADRO 5</b> Matriz de Impacto .....	25



## 4. JUSTIFICION

Este proyecto pretende diseñar un proceso de gestión de riesgos que sea ágil, documentado y amigable que le permita a la organización cerrar las brechas que tiene respecto a los modelos de gestión de riesgos, permitiéndoles una disminución de tiempos y costos generados por problemas no previstos.

La puesta en marcha de un plan de gestión de riesgo, le permite a la institución contar con una serie de herramientas para valorar a que riesgos están expuestos, que probabilidad de ocurrencia tienen los mismos y como implementar un plan de respuesta al riesgo, considerando desde medidas preventivas hasta las acciones correctivas a implementar, posterior a la ocurrencia de los riesgos identificados.

El desarrollo de una metodología de gestión de riesgos permitirá que la empresa se prepare proactivamente a enfrentar las amenazas que afecten el resultado final de los proyectos. El propósito principal es proteger los intereses de los clientes (entregar a tiempo, cumplir con el presupuesto y dentro del alcance debidamente aprobado) y por supuesto evitar que la empresa deje de percibir ingresos por proyectos que se prolongan más de lo pactado o recursos que no pueden ser reasignados por permanecer más de lo calendarizado. Adicionalmente se espera poder anticiparse a posibles oportunidades que puedan impactar positivamente en el resultado de los proyectos, con planes debidamente trazados y objetivos bien estipulados.

Una organización como IquitosPlay, que tiene como su razón de ser prestar servicios, debe asegurar la satisfacción del cliente y una alta asertividad en los trabajos que obtiene, un componente esencial de la administración de proyectos que la organización ha detectado como una falencia en sus procesos es la gestión de riesgos, por lo que desarrollar un proyecto como éste, le permitirá fortalecer este punto, garantizando un mejor resultado interno y externo para la ejecución de los diversos proyectos que se realicen.



## 5. OBJETIVO

### 5.1. Objetivo General

Desarrollar una metodología de gestión de riesgos especializada en el desarrollo de proyectos de software, aplicar en la empresa IquitosPlay para enfrentar de manera proactiva los posibles eventos que afecten negativamente los proyectos de la compañía, así como para aprovechar las oportunidades que puedan presentarse y sean de beneficio para el resultado final de los mismos.

### 5.2. Objetivos Especificados

- Desarrollar los procedimientos necesarios para realizar una gestión profesional de riesgos en los proyectos, utilizando los procesos sugeridos por el PMBOK (PMI, 2004).
- Desarrollar las plantillas y los instructivos que serán utilizados en la aplicación de la metodología de gestión de riesgos en los proyectos de desarrollo de software para documentar los registros de la metodología planteada.
- Aplicar la metodología de gestión de riesgos a uno de los proyectos de IquitosPlay para documentar un caso de implementación de la metodología con el fin de utilizarlo como futura referencia para otras implementaciones.

## 6. DESARROLLO DEL TEMA

### 6.1. Teoría de la Temática

#### 7.1.1 Definición y Componentes del Riesgo

**Definición:** Según la definición del PMBOK (PMI, 2008), Es un evento o condición incierta que, de producirse, tiene un efecto positivo o negativo en uno o más de los objetivos del proyecto, tales como el alcance, el cronograma, el costo y la calidad. Incluye, por tanto, oportunidades y amenazas.

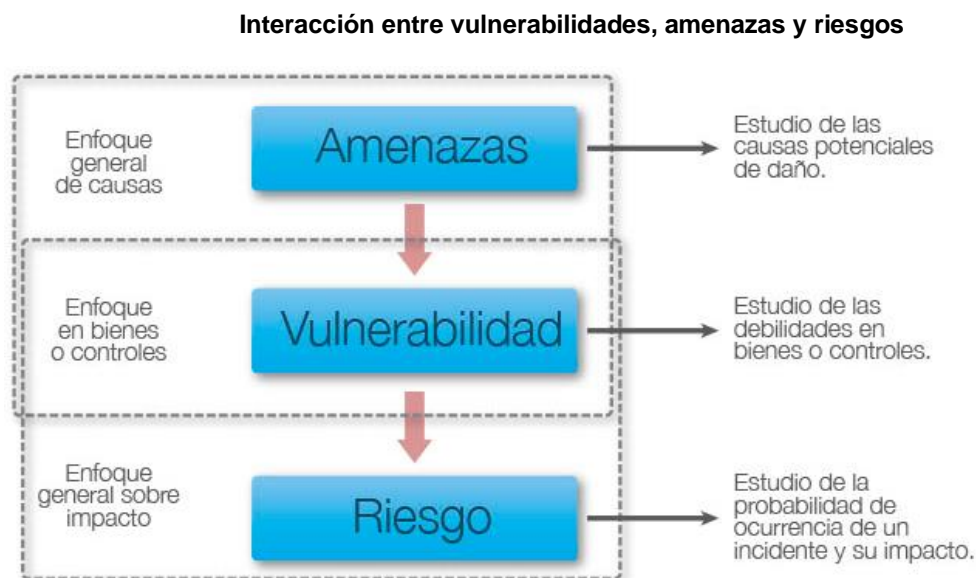
#### Componentes del Riesgo:

- **Un evento definible:** Acción o situación que se da o que sucede dentro de un grupo de acciones o situaciones posibles de suceder.
- **Probabilidad de ocurrencia:** Probabilidad de ocurrencia de cada riesgo
- **Consecuencia de la ocurrencia** (impacto)

#### 7.1.2 Amenazas y Vulnerabilidades.

**Amenazas:** Una Amenaza es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial). (La Guía del PMBOK®)

**Vulnerabilidad:** Es la capacidad, las condiciones y características que lo hace susceptible a amenazas, con el resultado de sufrir algún daño. En otras palabras, es la capacidad y posibilidad de un de responder o reaccionar a una amenaza o de recuperarse de un daño. (La Guía del PMBOK®)  
Las vulnerabilidades están en directa interrelación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no se puede ocasionar un daño.



**Figura 1** Interacción entre vulnerabilidades, amenazas y riesgos  
(Patricia Prandrini CISA y CRISC 2008)



### 7.1.3 Mapa de Riesgos

Según la guía para la valoración de riesgos en proyectos, el mapa de riesgos es un instrumento metodológico mediante el cual se identifica un conjunto ordenado y flexible de factores que pueden dar origen tanto a hechos que contribuyan al logro de un objetivo (aprovechar la oportunidad) o a calificar la presencia del riesgo (negativo) y se prevén sus posibles daños.

Igualmente, el mapa de riesgos es una herramienta gerencial que puede adaptarse a las necesidades y objetivos de quienes desean utilizarlo. Observando los distintos factores que lo integran y valorando la situación existente. En cada entidad es posible diseñar estrategias y acciones orientadas a evitar, controlar o minimizar la presencia de tales riesgos.

En el caso de los proyectos el Mapa de Riesgos se convierte en un instrumento de control y seguimiento que facilita la toma de decisiones para la consecución de los objetivos propios de los proyectos y los estratégicos institucionales.

### 7.1.4 Niveles de Aceptación del Riesgo.

El nivel de riesgo aceptado en los proyectos tiene una especial vinculación con los procesos de administración de costos, tiempo y calidad de los proyectos. Su definición se orienta hacia la disposición y capacidad de la institución en aceptar o retener las variaciones de los costos, cronogramas y requisitos de calidad de los proyectos, de manera que no se vean afectados los objetivos de los proyectos.

Los niveles de riesgos aceptables es un tipo de criterio de aceptación de riesgos que se emplea durante la etapa de evaluación de riesgos. Se debe definir antes de iniciar la valoración de riesgos, con el fin de contar con un elemento para la toma de decisión para la gestión del riesgo, para ello se toman en cuenta:

**-Parámetros de aceptabilidad del riesgo:** Se entiende como los criterios que permiten determinar si un nivel de riesgo específico se ubica dentro del nivel de riesgo aceptado por la institución.

**-Nivel de riesgo Aceptable:** Nivel de riesgo que el equipo de proyecto están dispuestos y en capacidad de aceptar para cumplir con los objetivos (relacionado a tiempo, costo, calidad, alcance), sin incurrir en costos ni efectos adversos excesivos en relación con sus beneficios esperados o ser incompatible con las expectativas de los interesados.

### 7.1.5 Plan de Acción

Un plan de acción es una presentación resumida de las tareas que deben realizarse por ciertas personas, en un plazo de tiempo específicos, utilizando un monto de recursos asignados con el fin de lograr un objetivo dado. De esta manera, un plan de acción se constituye como una especie de guía que brinda un marco o una estructura a la hora de llevar a cabo un **proyecto**.

En la gestión de riesgos es un documento que registra los eventos riesgosos que sucederán en un proyecto y reduce el impacto de dichos eventos si llegaran a suceder. Se desarrollan opciones y acciones introduciendo recursos y actividades en un plan de mitigación para mejorar las oportunidades del proyecto y también reducir las amenazas a los objetivos del proyecto.



### 7.1.6 Control y Monitoreo del Riesgo

Consiste en rastrear los riesgos identificados, monitorear los riesgos residuales, identificar nuevos riesgos, asegurar que los planes de respuesta a riesgos se ejecuten en el momento apropiado, y evaluar su efectividad a través del ciclo del proyecto.

Para cada riesgo o conjunto de riesgos para los cuales se ha definido una respuesta de contingencia, se debe haber especificado un correspondiente conjunto de condiciones o acciones llamados disparadores (triggers). Es la responsabilidad del propietario de acción asegurar que estas condiciones sean monitoreadas efectivamente y que las acciones correspondientes se lleven a cabo como se definieron, de una manera oportuna.

### 7.1.7 Gestión de Riesgos de los Proyectos

El PMBOK (PMI, 2008) define: Es el proceso sistémico de identificación, análisis y respuesta a los riesgos de los proyectos, este consiste entonces en aumentar la probabilidad e impacto de los eventos positivos y disminuir la probabilidad e impacto de los eventos adversos al proyecto, de tal forma que los objetivos de los proyectos se cumplan.

La Gestión de Riesgos del Proyecto trata de identificar y priorizar los riesgos antes de su ocurrencia, y proporcionar a los gestores de proyecto información orientada a la acción. Esta orientación requiere la consideración de eventos que pueden o no pueden ocurrir y por lo tanto los describe en términos de probabilidad de ocurrencia, además de otras dimensiones tales como el impacto en los objetivos.

Los beneficios que se obtienen al llevar a cabo una buena gestión de los riesgos son:

- ✓ Se reducen los costes del proyecto.
- ✓ Se mejora la satisfacción del cliente.
- ✓ Se incrementa la capacidad y probabilidades de éxito.
- ✓ Facilita el desarrollo del proyecto.
- ✓ Disminuye drásticamente las sorpresas en los proyectos.
- ✓ Ayuda a la empresa a conseguir los objetivos de negocio y proyecto evitando problemas que podrían causar pérdidas inesperadas y no planificadas.

### 7.1.8 Procesos de la Gestión de Riesgos

El PMBOK (PMI, 2008) divide la gestión de riesgos en 6 procesos: **Planificación de la Gestión de Riesgos**, **Identificación de Riesgos**, **Análisis Cualitativo de Riesgos**, **Análisis Cuantitativo de Riesgos**, **Planificación de la Respuesta a los Riesgos**, y **Seguimiento y Control de Riesgos**.

#### 7.1.8.1. Planificar la Gestión de Riesgos

Es el proceso de decidir cómo abordar y llevar a cabo las actividades de gestión de riesgos de un proyecto. Este proceso es indispensable que se complete en las fases tempranas de la planificación del proyecto, dado que es crucial para realizar con éxito los demás procesos de la Gestión de Riesgos.



El desarrollo del Plan de Gestión de Riesgos incluye:

- Definición de las herramientas y las fuentes de datos que serán utilizados para la gestión de riesgos en el proyecto (Factores ambientales de la empresa, Activos de los procesos de la organización, Registro de Interesados).
- Definición de los Roles y Responsabilidades: define al líder, soporte, los miembros del equipo de gestión de riesgo para cada tipo de actividad en el plan de gestión de riesgo y asigna personas a estos roles.
- Determinación de la Periodicidad de la gestión del riesgo: determina cuando y que tan a menudo se ejecutaran los procesos de gestión de riesgos durante el ciclo de vida del proyecto, y establecen las actividades de la gestión de riesgos que serán que serán incluidas en el cronograma de actividades.
- Categorización de Riesgos: Provee una estructura que asegura un proceso exhaustivo d identificación de riesgos. Proporcionan un medio para agrupar las causas potenciales de riesgo.
- Definición de la probabilidad e impacto de los riesgos: Se definen diferentes niveles de probabilidades de riesgos y de impactos para ser utilizados en el análisis cualitativo.
- Desarrollo de la matriz de probabilidad e impacto: Se desarrolla una matriz en la cual se priorizan los riesgos de acuerdo a la combinación impacto/probabilidad. Estas combinaciones son clasificadas usualmente como "alta", "media", "moderada", "baja" y normalmente son elegidos por la organización.
- Definición de los criterios de aceptación.
- Diseño de los formatos de informes: describe el contenido y formato de los registros de riesgo, así como cualquier otro reporte de riesgo que sea requerido.

#### 7.1.8.2. Identificar los Riesgos

Identificar los Riesgos es el proceso de determinar los riesgos que pueden afectar al proyecto y documentar sus características. El beneficio clave de este proceso es la documentación de los riesgos existentes y el conocimiento y la capacidad que confiere al equipo del proyecto para anticipar eventos. Identificar los riesgos es un proceso iterativo debido a que pueden evolucionar o se pueden descubrir nuevos riesgos conforme el proyecto avanza a lo largo de su ciclo de vida.

Existen varias herramientas y técnicas para identificar riesgos de un proyecto:

**Revisión de Documentación:** Consiste en una revisión estructurada de la documentación del proyecto, incluidos los planes, los supuestos, los archivos de proyectos anteriores, los acuerdos y otra información. La calidad de los planes, así como la consistencia entre dichos planes y los requisitos y supuestos del proyecto, pueden ser indicadores de riesgo en el proyecto.

#### Técnicas de Recopilación de Información

- ❖ **Tormenta de ideas:** El objetivo de la tormenta de ideas es obtener una lista completa de los riesgos del proyecto. Por lo general, el equipo del proyecto efectúa tormentas de ideas, a menudo con un grupo multidisciplinario de expertos que no forman parte del equipo. Bajo el liderazgo de un facilitador, se generan ideas acerca de los riesgos del proyecto, ya sea por medio de una sesión tradicional y abierta de tormenta de ideas, o en una sesión estructurada donde se utilizan técnicas de entrevista masiva. Como marco de referencia pueden utilizarse categorías de riesgo, como en una estructura de desglose de riesgos. Posteriormente se identifican y categorizan los riesgos según su tipo, y se refinan sus definiciones.



- ❖ **Técnica Delphi:** La técnica Delphi es una manera de lograr un consenso de expertos. Los expertos en riesgos del proyecto participan en esta técnica de forma anónima. Un facilitador utiliza un cuestionario para solicitar ideas acerca de los riesgos importantes del proyecto. Las respuestas son resumidas y posteriormente enviadas nuevamente a los expertos para recabar comentarios adicionales. En pocas rondas de este proceso se puede lograr el consenso. La técnica Delphi ayuda a reducir sesgos en los datos y evita que cualquier persona ejerza influencias indebidas en el resultado.
- ❖ **Entrevistas:** La realización de entrevistas a los participantes experimentados del proyecto, a los interesados y a los expertos en la materia ayuda a identificar los riesgos.

### **Análisis con Lista de Verificación**

Las listas de verificación para la identificación de riesgos se desarrollan sobre la base de la información histórica y del conocimiento acumulado a partir de proyectos anteriores similares y de otras fuentes de información. Si bien una lista de verificación puede ser rápida y sencilla, es imposible elaborar una lista exhaustiva, y se debe tener cuidado para asegurar que la lista de verificación no sea utilizada para evitar el esfuerzo de una adecuada identificación de riesgos. El equipo también debe explorar elementos que no aparecen en la lista de verificación. Además, la lista de verificación se debe depurar de vez en cuando para eliminar o archivar elementos relacionados. La lista de verificación debe revisarse durante el cierre del proyecto para incorporar nuevas lecciones aprendidas a fin de mejorarla para poder usarla en proyectos futuros.

### **Análisis de Supuestos**

Cada proyecto y su plan se conciben y desarrollan sobre la base de un conjunto de hipótesis, escenarios o supuestos. El análisis de supuestos explora la validez de los supuestos según se aplican al proyecto. Identifica los riesgos del proyecto relacionados con el carácter inexacto, inestable, inconsistente o incompleto de los supuestos.

### **Técnicas de Diagramación**

Las técnicas de diagramación de riesgos pueden incluir:

- **Diagramas de causa y efecto.** Estos diagramas también se conocen como diagramas de Ishikawa o diagramas de espina de pescado y son útiles para identificar las causas de los riesgos.
- **Diagramas de flujo de procesos o de sistemas.** Estos diagramas muestran cómo se relacionan entre sí los diferentes elementos de un sistema, y el mecanismo de causalidad.
- **Diagramas de influencias.** Son representaciones gráficas de situaciones que muestran las influencias causales, la cronología de eventos y otras relaciones entre las variables y los resultados.

### **Análisis FODA**

Esta técnica examina el proyecto desde cada uno de los aspectos FODA (fortalezas, oportunidades, debilidades y amenazas) para aumentar el espectro de riesgos identificados, incluidos los riesgos generados internamente. La técnica comienza con la identificación de las fortalezas y debilidades de la organización, centrándose ya sea en el proyecto, en la organización o en el negocio en general. El análisis FODA identifica luego cualquier oportunidad para el proyecto con origen en las fortalezas de la organización y cualquier amenaza con origen en las debilidades de la organización. El análisis también examina el grado en el que las fortalezas de la organización contrarrestan las amenazas, e identifica las oportunidades que pueden servir para superar las debilidades.



### Identificación de Riesgos Basado en Taxonomía

Este método de identificación de riesgos ha sido desarrollado por el Instituto de Ingeniería de Software (SEI por sus siglas en inglés). El método está basado en la taxonomía de riesgos para proyectos de desarrollo de software, la cual sirve como marco de trabajo para organizar y estudiar la amplitud de los problemas y asuntos inherentes a estos proyectos, y por lo tanto provee una estructura para dar organización y facilitar la comprensión de los riesgos.

El proceso de identificación de riesgos consiste en un cuestionario basado en la taxonomía. La taxonomía organiza los riesgos de desarrollo de software en 3 niveles – clases, elementos y atributos. El cuestionario basado en taxonomía (TBQ basado por sus siglas en inglés) consiste en elaborar preguntas debajo de cada atributo designado para obtener el rango de riesgos y problemas potenciales que afectan un producto de software. La aplicación de este proceso está designada de manera que el cuestionario puede ser aplicado de manera práctica y eficiente, con el propósito de descubrir e identificar los riesgos del proyecto.

El método de identificación de riesgos de SEI mapea las características del desarrollo de software y por lo tanto los riesgos del desarrollo de software. Está basado en las siguientes asunciones:

- Los riesgos de desarrollo de software son generalmente conocidos por el equipo técnico del proyecto pero son muy mal comunicados.
- Un método de identificación de riesgos que sea estructurado y repetible es necesario para una consistente gestión del riesgo.
- El proceso de identificación de riesgos debe crear y sostener un ambiente en el cual los puntos de vista controversiales y provisionales son tomados en cuenta.
- No se podrá emitir ningún juicio en general sobre el éxito o fracaso de un proyecto basado únicamente en el número o la naturaleza de los riesgos no descubiertos.

El TBQ es un método semi-estructurado. Las preguntas y su secuencia son utilizadas como una guía pero no como una limitación. Las preguntas se han desarrollado de manera que permita el desarrollo de una discusión de manera natural. En efecto, el método TBQ puede ser considerado como una tormenta de ideas estructurada.

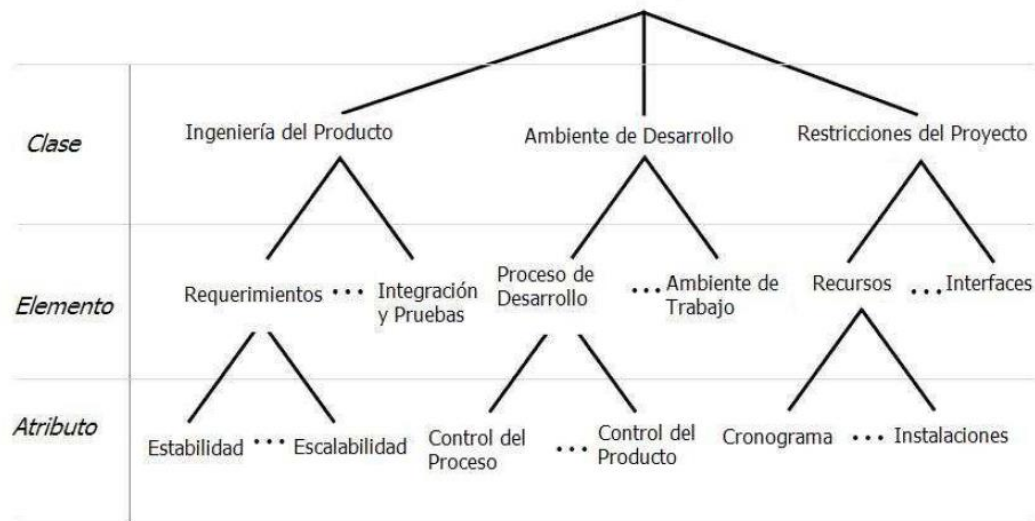
En el centro del método de identificación se encuentra la taxonomía de desarrollo de software. Como se mencionó anteriormente la taxonomía provee un marco de trabajo para organizar y estudiar la amplitud o rango de problemas potenciales que se pueden presentar en proyectos de desarrollo de software.

La Taxonomía está organizada en 3 clases principales:

- **Ingeniería del Producto:** Los aspectos técnicos del trabajo a realizar.
- **Ambiente de Desarrollo:** Los métodos, procedimientos y herramientas a utilizar para producir el producto.
- **Restricciones del Producto:** Factores contractuales, organizacionales y operacionales dentro de los cuales el software es desarrollado pero los cuales están generalmente fuera del control directo de la gerencia del proyecto.

Cada una de éstas clases se subdividen en elementos y las mismas se subdividen en atributos.

## Estructura de Riesgos en Proyectos de Desarrollo de Software



**Figura 2:** Taxonomía de Riesgos de Desarrollo de Software  
(Marvin J. Carr, 1993)

El cuestionario consiste en preguntas a nivel de los atributos junto con preguntas de seguimiento o de recomendaciones. Dado que el TBQ es exhaustivo, contiene preguntas que podrían no ser relevantes para todas las etapas del ciclo de vida del desarrollo de software, para ciertos dominios de software específicos o para ciertas organizaciones. Típicamente el cuestionario se adapta al proyecto particular a la etapa en el ciclo de vida por el cual se está desarrollando, eliminando las preguntas que no son relevantes. Por ejemplo, un proyecto sin subcontratos podría eliminar las preguntas relacionadas a los mismos.

**Como resultado del proceso de identificar los Riesgos tenemos el “Registro del Riesgo” con información inicial de:**

- **Lista de riesgos identificados.** Los riesgos identificados se describen con un nivel de detalle razonable. Se puede utilizar una estructura para describir los riesgos mediante enunciados de riesgo, como por ejemplo: Se puede producir un EVENTO que causaría un IMPACTO, o Si existe CAUSA, puede dar lugar a este EVENTO que produciría tal EFECTO. Además de la lista de riesgos identificados, las causas raíz de esos riesgos pueden aparecer de manera más evidente. Se trata de condiciones o eventos fundamentales que pueden dar lugar a uno o más riesgos identificados. Se deben registrar y utilizar para favorecer la identificación futura de riesgos, tanto para el proyecto en cuestión como para otros proyectos.



### 7.1.8.3. Realizar el Análisis Cualitativo de Riesgos

Realizar el Análisis Cualitativo de Riesgos es el proceso de priorizar riesgos para análisis o acción posterior, evaluando y combinando la probabilidad de ocurrencia e impacto de dichos riesgos. El beneficio clave de este proceso es que permite reducir el nivel de incertidumbre y concentrarse en los riesgos de alta prioridad.

Realizar el Análisis Cualitativo de Riesgos evalúa la prioridad de los riesgos identificados a través de la probabilidad relativa de ocurrencia, del impacto correspondiente sobre los objetivos del proyecto si los riesgos llegaran a presentarse, así como de otros factores, tales como el plazo de respuesta y la tolerancia al riesgo por parte de la organización, asociados con las restricciones del proyecto en términos de costo, cronograma, alcance y calidad.

Realizar el Análisis Cualitativo de Riesgos es por lo general un medio rápido y económico de establecer prioridades para Planificar la Respuesta a los Riesgos y sienta las bases para Realizar el Análisis Cuantitativo de Riesgos.

Para realizar el Análisis Cualitativo de Riesgos se utilizan Técnicas y Herramientas:

#### Evaluación de Probabilidad e Impacto de los Riesgos

La evaluación de la probabilidad de los riesgos estudia la probabilidad de ocurrencia de cada riesgo específico. La evaluación del impacto de los riesgos estudia el efecto potencial de los mismos sobre un objetivo del proyecto, tal como el cronograma, el costo, la calidad o el desempeño, incluidos tanto los efectos negativos en el caso de las amenazas, como los positivos, en el caso de las oportunidades.

Para cada uno de los riesgos identificados, se evalúan la probabilidad y el impacto. Los riesgos se pueden evaluar a través de entrevistas o reuniones con participantes seleccionados por estar familiarizados con las categorías de riesgo.

Durante estas entrevistas o reuniones, se evalúan el nivel de probabilidad de cada riesgo y su impacto sobre cada objetivo del proyecto. Las probabilidades e impactos de los riesgos se califican de acuerdo con las definiciones proporcionadas en el plan de gestión de los riesgos. Los riesgos con una baja calificación en cuanto a probabilidad e impacto se incluirán en el registro de riesgos como parte de una lista de observación para su futuro monitoreo.

#### Matriz de Probabilidad e Impacto

La matriz de probabilidad e impacto permite una evaluación de la importancia de los riesgos de su prioridad de atención, visualiza los riesgos en combinaciones de probabilidad e impacto, clasificándolos con una prioridad baja, moderada o alta.

Cada riesgo se califica de acuerdo con su probabilidad de ocurrencia y con el impacto sobre un objetivo, en caso de que se materialice. La organización debe determinar qué combinaciones de probabilidad e impacto dan lugar a una clasificación de riesgo alto, riesgo moderado y riesgo bajo. En una matriz en blanco y negro, estas condiciones se representan mediante diferentes tonalidades de gris:

- El área gris oscuro (con las cifras más altas) representa un riesgo alto.
- El área gris intermedio (con las cifras más bajas) representa un riesgo bajo.
- El área gris claro (con las cifras intermedias) representa el riesgo moderado.



La calificación de los riesgos ayuda a definir las respuestas a los mismos. Por ejemplo, los riesgos que tienen un impacto negativo sobre los objetivos, conocidos como amenazas cuando se materializan, y que se encuentran en la zona de riesgo alto (gris oscuro) de la matriz, pueden requerir prioridad en la acción y estrategias de respuesta agresivas. Las amenazas que se encuentran en la zona de riesgo bajo (gris intermedio) pueden no requerir una acción de gestión proactiva, más allá de ser incluidas en el registro de riesgos como parte de la lista de observación o de ser agregadas a una reserva para contingencias. Lo mismo ocurre para las oportunidades, debe darse prioridad a las oportunidades que se encuentran en la zona de riesgo alto (gris oscuro), ya que se pueden obtener más fácilmente y proporcionar mayores beneficios. Las oportunidades en la zona de riesgo bajo (gris intermedio) deben monitorearse.

### **Categorización de Riesgos**

Los riesgos del proyecto se pueden categorizar por fuentes de riesgo (p.ej., utilizando desglose de riesgos), por área del proyecto afectada (p.ej., utilizando la EDT/WBS) o por otras categorías útiles (p.ej., fase del proyecto) a fin de determinar qué áreas del proyecto están más expuestas a los efectos de la incertidumbre. Los riesgos también se pueden categorizar por causas raíces comunes. Esta técnica ayuda a determinar los paquetes de trabajo, las actividades, las fases del proyecto o incluso los roles del proyecto que pueden conducir al desarrollo de respuestas eficaces frente al riesgo.

### **Evaluación de la Urgencia de los Riesgos**

Los riesgos que requieren respuestas a corto plazo pueden ser considerados de atención más urgente. Entre los indicadores de prioridad se pueden incluir la probabilidad de detectar el riesgo, el tiempo para dar una respuesta a los riesgos, los síntomas y las señales de advertencia, y la calificación del riesgo. En algunos análisis cualitativos, la evaluación de la urgencia de un riesgo se combina con la calificación del riesgo obtenida a través de la matriz de probabilidad e impacto para obtener una calificación final de la severidad del riesgo.

### **Como resultado de este proceso de Realizar el Análisis Cualitativo de Riesgos se obtiene:**

Actualizaciones de los documentos:

- Actualizaciones al registro de riesgos. A medida que se dispone de nueva información a través de la evaluación cualitativa de riesgos, se va actualizando el registro de riesgos. Las actualizaciones al registro de riesgos pueden incluir evaluaciones de probabilidad e impacto para cada riesgo, clasificación y calificación de riesgos, información de la urgencia o categorización de los riesgos, así como una lista de observación para los riesgos de baja probabilidad o que requieren análisis adicional.
- Actualizaciones al registro de supuestos. A medida que se dispone de nueva información a través de la evaluación cualitativa de riesgos, los supuestos pueden cambiar. Es preciso revisar el registro de supuestos para dar cabida a esta nueva información. Los supuestos se pueden incorporar en el enunciado del alcance del proyecto o en un registro de supuestos independiente.



#### 7.1.8.4. Realizar el Análisis Cuantitativo de Riesgos

Realizar el Análisis Cuantitativo de Riesgos es el proceso de analizar numéricamente el efecto de los riesgos identificados sobre los objetivos generales del proyecto. El beneficio clave de este proceso es que genera información cuantitativa sobre los riesgos para apoyar la toma de decisiones a fin de reducir la incertidumbre del proyecto.

El proceso Realizar el Análisis Cuantitativo de Riesgos se aplica a los riesgos priorizados mediante el proceso Realizar el Análisis Cualitativo de Riesgos por tener un posible impacto significativo sobre las demandas concurrentes del proyecto.

En algunos casos puede que no sea posible llevar a cabo el proceso Realizar el Análisis Cuantitativo de Riesgos debido a la falta de datos suficientes para desarrollar los modelos adecuados. El proceso Realizar el Análisis Cuantitativo de Riesgos debe repetirse, según las necesidades, como parte del proceso Controlar los Riesgos, para determinar si se ha reducido satisfactoriamente el riesgo global del proyecto. Las tendencias pueden indicar la necesidad de una mayor o menor atención a las actividades adecuadas en materia de gestión de riesgos.

Para realizar el Análisis Cuantitativo de Riesgos se utilizan Técnicas y Herramientas:

##### Técnicas de Recopilación y Representación de Datos

- ❖ **Entrevistas:** Las técnicas de entrevistas se basan en la experiencia y en datos históricos para cuantificar la probabilidad y el impacto de los riesgos sobre los objetivos del proyecto. La información necesaria depende del tipo de distribuciones de probabilidad que se vayan a utilizar. Por ejemplo, para algunas distribuciones comúnmente usadas, la información se podría recopilar agrupándola en escenarios optimistas (bajo), pesimistas (alto) y más probables.
- ❖ **Distribuciones de probabilidad:** Las distribuciones continuas de probabilidad, utilizadas ampliamente en el modelado y simulación, representan la incertidumbre en valores tales como las duraciones de las actividades del cronograma y los costos de los componentes del proyecto. Las distribuciones discretas pueden emplearse para representar eventos inciertos, como el resultado de una prueba o un posible escenario en un árbol de decisiones.

##### Técnicas de Análisis Cuantitativo de Riesgos y de Modelado

- ❖ **Análisis de sensibilidad:** El análisis de sensibilidad ayuda a determinar qué riesgos tienen el mayor impacto potencial en el proyecto. Ayuda a comprender la correlación que existe entre las variaciones en los objetivos del proyecto y las variaciones en las diferentes incertidumbres. Por otra parte, evalúa el grado en que la incertidumbre de cada elemento del proyecto afecta al objetivo que se está estudiando cuando todos los demás elementos inciertos son mantenidos en sus valores de línea base. Una representación típica del análisis de sensibilidad es el diagrama con forma de tornado el cual resulta útil para comparar la importancia y el impacto relativos de las variables que tienen un alto grado de incertidumbre con respecto a las que son más estables. El diagrama con forma de tornado también resulta útil a la hora de analizar escenarios de asunción de riesgos basados en riesgos específicos cuyo análisis cuantitativo pone de relieve posibles beneficios superiores a los impactos negativos correspondientes. Un diagrama con forma de tornado es un tipo especial de diagrama de barras que se utiliza en el análisis de sensibilidad para comparar la importancia relativa de las variables. En un diagrama con forma de tornado el eje Y representa cada tipo de incertidumbre en sus valores base, mientras que el eje X representa la dispersión o correlación de la incertidumbre con la salida que se está estudiando.
- ❖ **Análisis del valor monetario esperado:** El análisis del valor monetario esperado (EMV) es un concepto estadístico que calcula el resultado promedio cuando el futuro incluye escenarios que pueden ocurrir o no (es decir, análisis bajo incertidumbre). El EMV de las oportunidades se expresa por lo general con valores positivos, mientras que el de las amenazas se expresa con valores negativos. El EMV requiere un supuesto de neutralidad del riesgo, ni de aversión al riesgo



ni de tracción por éste. El EMV para un proyecto se calcula multiplicando el valor de cada posible resultado por su probabilidad de ocurrencia y sumando luego los resultados.

- ❖ **Modelado y simulación:** Una simulación de proyecto utiliza un modelo que traduce las incertidumbres detalladas especificadas para el proyecto en su impacto potencial sobre los objetivos del mismo. Las simulaciones se realizan habitualmente mediante la técnica Monte Carlo. En una simulación, el modelo del proyecto se calcula muchas veces (mediante iteración) utilizando valores de entrada (p.ej., estimaciones de costos o duraciones de las actividades) seleccionados al azar para cada iteración a partir de las distribuciones de probabilidad para estas variables. A partir de las iteraciones se calcula un histograma (p.ej., costo total o fecha de finalización). Para un análisis de riesgos de costos, una simulación emplea estimaciones de costos. Para un análisis de los riesgos relativos al cronograma, se emplean el diagrama de red del cronograma y las estimaciones de la duración.

Mediante este proceso de Análisis Cuantitativo de Riesgos se obtienen:

- ✓ Cuantificar los posibles resultados del proyecto y sus probabilidades.
- ✓ Evaluar la probabilidad de lograr los objetivos específicos del proyecto.
- ✓ Identificar los riesgos que requieran la mayor atención mediante cuantificación de su contribución relativa al riesgo general del proyecto.
- ✓ Identificar los objetivos de costo, cronograma o alcance, realistas y viables, dados los riesgos del proyecto.

#### 7.1.8.5. Planificar la Respuesta a los Riesgos

Planificar la Respuesta a los Riesgos es el proceso de desarrollar opciones y acciones para mejorar las oportunidades y reducir las amenazas a los objetivos del proyecto. El beneficio clave de este proceso es que aborda los riesgos en función de su prioridad, introduciendo recursos y actividades en el presupuesto, el cronograma y el plan para la dirección del proyecto, según las necesidades.

Existen varias estrategias de respuesta a los riesgos. Para cada riesgo, se debe seleccionar la estrategia o la combinación de estrategias con mayor probabilidad de eficacia:

#### Estrategias para Riesgos Negativos o Amenazas

Las tres estrategias que normalmente abordan las amenazas o los riesgos que pueden tener impactos negativos sobre los objetivos del proyecto en caso de materializarse, son: evitar, transferir y mitigar. La cuarta estrategia, aceptar, puede utilizarse para riesgos negativos o amenazas así como para riesgos positivos u oportunidades. Cada una de estas estrategias de respuesta a los riesgos tiene una influencia variada y única sobre la condición del riesgo. Estas estrategias deben seleccionarse en función de la probabilidad y el impacto del riesgo sobre los objetivos generales del proyecto. Las estrategias de evitar y mitigar habitualmente son eficaces para riesgos críticos de alto impacto, mientras que las de transferir y aceptar normalmente son buenas estrategias para amenazas menos críticas y con bajo impacto global. A continuación se describen con mayor detalle las cuatro estrategias para abordar los riesgos negativos o amenazas:

- **Evitar:** Evitar el riesgo es una estrategia de respuesta a los riesgos según la cual el equipo del proyecto actúa para eliminar la amenaza o para proteger al proyecto de su impacto. Por lo general implica cambiar el plan para la dirección del proyecto, a fin de eliminar por completo la amenaza. El director del proyecto también puede aislar los objetivos del proyecto del impacto del riesgo o cambiar el objetivo que se encuentra amenazado. Ejemplos de lo anterior son la ampliación del cronograma, el cambio de estrategia o la reducción del alcance. La estrategia de evasión más drástica consiste en anular por completo el proyecto. Algunos riesgos que surgen en etapas tempranas del proyecto se pueden evitar aclarando los requisitos, obteniendo información, mejorando la comunicación o adquiriendo experiencia.



- **Transferir:** Transferir el riesgo es una estrategia de respuesta a los riesgos según la cual el equipo del proyecto traslada el impacto de una amenaza a un tercero, junto con la responsabilidad de la respuesta. La transferencia de un riesgo simplemente confiere a una tercera parte la responsabilidad de su gestión; no lo elimina. La transferencia no implica que se deje de ser el propietario del riesgo por el hecho de transferirlo a un proyecto posterior o a otra persona sin su conocimiento o consentimiento. Transferir el riesgo casi siempre implica el pago de una prima de riesgo a la parte que asume el riesgo. La transferencia de la responsabilidad de un riesgo es más eficaz cuando se trata de la exposición a riesgos financieros. Las herramientas de transferencia pueden ser bastante diversas e incluyen, entre otras, el uso de seguros, garantías de cumplimiento, fianzas, certificados de garantía, etc. Para transferir a un tercero la responsabilidad de riesgos específicos se pueden utilizar contratos o acuerdos.
- **Mitigar:** Mitigar el riesgo es una estrategia de respuesta a los riesgos según la cual el equipo del proyecto actúa para reducir la probabilidad de ocurrencia o impacto de un riesgo. Implica reducir a un umbral aceptable la probabilidad y/o el impacto de un riesgo adverso. Adoptar acciones tempranas para reducir la probabilidad de ocurrencia de un riesgo y/o su impacto sobre el proyecto, a menudo es más eficaz que tratar de reparar el daño después de ocurrido el riesgo. Ejemplos de acciones de mitigación son adoptar procesos menos complejos, realizar más pruebas o seleccionar un proveedor más estable.
- **Aceptar:** Aceptar el riesgo es una estrategia de respuesta a los riesgos según la cual el equipo del proyecto decide reconocer el riesgo y no tomar ninguna medida a menos que el riesgo se materialice. Esta estrategia se adopta cuando no es posible ni rentable abordar un riesgo específico de otra manera. Esta estrategia indica que el equipo del proyecto ha decidido no cambiar el plan para la dirección del proyecto para hacer frente a un riesgo, o no ha podido identificar ninguna otra estrategia de respuesta adecuada. Esta estrategia puede ser pasiva o activa. La aceptación pasiva no requiere ninguna acción, excepto documentar la estrategia dejando que el equipo del proyecto aborde los riesgos conforme se presentan, y revisar periódicamente la amenaza para asegurarse de que no cambie de manera significativa. La estrategia de aceptación activa más común consiste en establecer una reserva para contingencias, que incluya la cantidad de tiempo, dinero o recursos necesarios para manejar los riesgos.

### Estrategias para Riesgos Positivos u Oportunidades

Tres de las cuatro respuestas se sugieren para tratar riesgos con impactos potencialmente positivos sobre los objetivos del proyecto. La cuarta estrategia, aceptar, puede utilizarse para riesgos negativos o amenazas así como para riesgos positivos u oportunidades. Las estrategias descritas a continuación, son explotar, compartir, mejorar o aceptar.

- **Explotar:** La estrategia de explotar se puede seleccionar para los riesgos con impactos positivos, cuando la organización desea asegurarse de que la oportunidad se haga realidad. Esta estrategia busca eliminar la incertidumbre asociada con un riesgo a la alza en particular, asegurando que la oportunidad definitivamente se concrete. Algunos ejemplos de respuestas de explotación directa incluyen la asignación al proyecto de los recursos más talentosos de una organización para reducir el tiempo hasta la conclusión, o el uso de nuevas tecnologías o mejoras tecnológicas para reducir el costo y la duración requeridos para alcanzar los objetivos del proyecto.
- **Mejorar:** La estrategia de mejorar se utiliza para aumentar la probabilidad y/o los impactos positivos de una oportunidad. La identificación y maximización de las fuerzas impulsoras clave de estos riesgos de impacto positivo pueden incrementar su probabilidad de ocurrencia. Entre los ejemplos de mejorar las oportunidades se cuenta la adición de más recursos a una actividad para terminar más pronto.
- **Compartir:** Compartir un riesgo positivo implica asignar toda o parte de la propiedad de la oportunidad a un tercero mejor capacitado para capturar la oportunidad en beneficio del proyecto. Entre los ejemplos de acciones de compartir se cuentan la formación de asociaciones de riesgo conjunto, equipos, empresas con finalidades especiales o uniones temporales de empresas, que se pueden establecer con el propósito expreso de aprovechar la oportunidad, de modo que todas las partes se beneficien a partir de sus acciones.
- **Aceptar:** Aceptar una oportunidad es estar dispuesto a aprovechar la oportunidad si se presenta, pero sin buscarla de manera activa.



## Estrategias de Respuesta a Contingencias

Algunas estrategias de respuesta se diseñan para ser usadas únicamente si se producen determinados eventos. Para algunos riesgos, resulta apropiado para el equipo del proyecto elaborar un plan de respuesta que sólo se ejecutará bajo determinadas condiciones predefinidas, cuando se prevé que habrá suficientes señales de advertencia para implementar el plan. Se deben definir y rastrear los eventos que disparan la respuesta para contingencias, tales como no cumplir con hitos intermedios u obtener una prioridad más alta con un proveedor. Las respuestas a los riesgos identificadas mediante esta técnica se denominan a menudo planes de contingencia o planes de reserva, e incluyen los eventos desencadenantes identificados que ponen en marcha los planes.

En el proceso Planificar la Respuesta a los Riesgos se actualizan diversos documentos del proyecto, según las necesidades. Por ejemplo, cuando se seleccionan y se acuerdan respuestas adecuadas a los riesgos, éstas se incluyen en el registro de riesgos. El registro de riesgos debe escribirse con un nivel de detalle que se corresponda con la clasificación de prioridad y la respuesta planificada. A menudo, los riesgos altos y moderados se tratan en detalle. Los riesgos considerados de baja prioridad se incluyen en una lista de observación para su monitoreo periódico.

Las actualizaciones al registro de riesgos incluyen:

- ✓ Los propietarios del riesgo y sus responsabilidades asignadas.
- ✓ Las estrategias de respuesta acordadas.
- ✓ Las acciones específicas para implementar la estrategia de respuesta seleccionada.
- ✓ El presupuesto y las actividades del cronograma necesarios para implementar las respuestas seleccionadas.
- ✓ Los planes de contingencia y disparadores que requieren su ejecución.

### 7.1.8.6. Seguimiento y control de riesgos

Es el proceso de implementar los planes de respuesta a los riesgos, dar seguimiento a los riesgos identificados, monitorear los riesgos residuales, identificar nuevos riesgos y evaluar la efectividad del proceso de gestión de los riesgos a través del proyecto. El beneficio clave de este proceso es que mejora la eficiencia del enfoque de la gestión de riesgos a lo largo del ciclo de vida del proyecto para optimizar de manera continua las respuestas a los riesgos.

Las respuestas a los riesgos planificadas que se incluyen en el registro de riesgos se ejecutan durante el ciclo de vida del proyecto, pero el trabajo del proyecto debe monitorearse continuamente para detectar riesgos nuevos, riesgos que cambian o que se tornan obsoletos.

Para el proceso de Seguimiento y control de riesgos se utilizan técnicas y herramientas:

#### Revaluación de los Riesgos

Controlar los Riesgos a menudo da lugar a la identificación de nuevos riesgos, la revaluación de los riesgos actuales y el cierre de riesgos obsoletos. Deben programarse periódicamente revaluaciones de los riesgos del proyecto. La cantidad y el nivel de detalle de las repeticiones que corresponda hacer dependerán de la manera en que el proyecto avanza con relación a sus objetivos.

#### Auditorías de los Riesgos

Las auditorías de riesgos examinan y documentan la eficacia de las respuestas a los riesgos identificados y sus causas, así como la eficacia del proceso de gestión de riesgos. El director del proyecto es el responsable de asegurar que las auditorías de riesgos se realicen con una frecuencia adecuada, tal y como se definiera en el plan de gestión de los riesgos del proyecto. Las auditorías de riesgos se pueden incluir en las reuniones de rutina de revisión del proyecto, o bien, pueden celebrarse reuniones específicas de auditoría de riesgos si el equipo así lo decide. El formato de la auditoría y sus objetivos deben definirse claramente antes de efectuar la auditoría.



### **Análisis de Variación y de Tendencias**

Numerosos procesos de control utilizan el análisis de variación para comparar los resultados planificados con los resultados reales. Con el propósito de controlar los riesgos, deben revisarse las tendencias en la ejecución del proyecto utilizando la información relativa al desempeño. El análisis del valor ganado y otros métodos de análisis de variación y de tendencias del proyecto pueden utilizarse para monitorear el desempeño global del proyecto. Los resultados de estos análisis pueden pronosticar la desviación potencial del proyecto en su conclusión con respecto a los objetivos de costo y cronograma. La desviación con respecto al plan de línea base puede indicar el impacto potencial de amenazas u oportunidades.

### **Medición del Desempeño Técnico**

La medición del desempeño técnico compara los logros técnicos durante la ejecución del proyecto con el cronograma de logros técnicos. Requiere la definición de medidas objetivas y cuantificables del desempeño técnico que se puedan utilizar para comparar los resultados reales con los planificados. Dichas mediciones del desempeño técnico pueden incluir pesos, tiempos de transacción, número de piezas defectuosas entregadas, capacidad de almacenamiento, etc. Una desviación, como por ejemplo ofrecer una mayor o menor funcionalidad con respecto a la planificada para un hito, puede ayudar a predecir el grado de éxito que se obtendrá en el cumplimiento del alcance del proyecto.

### **Análisis de Reservas**

A lo largo de la ejecución del proyecto se pueden materializar algunos riesgos, con impactos positivos o negativos sobre las reservas para contingencias del presupuesto o del cronograma. El análisis de reservas compara la cantidad de reservas para contingencias restantes con la cantidad de riesgo remanente en un momento dado del proyecto, con objeto de determinar si la reserva restante es suficiente.

### **Reuniones**

La gestión de los riesgos del proyecto debe ser un punto del orden del día en las reuniones periódicas sobre el estado del proyecto. El tiempo requerido para tratar este asunto variará en función de los riesgos que se hayan identificado, de su prioridad y de la dificultad de respuesta. La gestión de riesgos se torna más sencilla conforme se practica con mayor frecuencia. Los debates frecuentes sobre los riesgos aumentan las posibilidades de que las personas identifiquen los riesgos y las oportunidades.



## 7.2 DESARROLLO DE LA METODOLOGIA DE GESTION DE RIESGOS

Con base en la literatura estudiada y a las necesidades actuales de IQUITOSPLAY, se planteó una metodología de gestión de riesgos.

La metodología desarrollada propone lo siguiente:

### Procedimientos de Gestión de Riesgos.

A continuación se muestra el procedimiento de Gestión de Riesgos. Los siguientes pasos deberán ser ejecutados para administrar los riesgos del proyecto cada paso en este procedimiento define las entradas y salidas de la información:

#### 7.2.1. Desarrollar el Plan de Gestión de Riesgos.

El propósito de este plan es documentar los procedimientos a utilizar para la identificación y el manejo de eventos inciertos que causen variaciones en el resultado del proyecto.

- **Entradas**
  - ✓ Acta de Constitución del Proyecto / Documento de Requisitos.
  - ✓ EDT
  
- **Salidas:**
  - ✓ Plan de Gestión de Riesgos

##### 7.2.1.1.1. Definir los parámetros de riesgos:

Define valores comunes para ser utilizados en el proceso de gestión de riesgo. Las buenas prácticas en el análisis cualitativo de riesgos indican que se debe utilizar un conjunto definido de valores tanto para la probabilidad como para el impacto. Estos valores conducirán a una clasificación de riesgos que será utilizada para categorizar y agrupar los riesgos, y para proveer una guía a los Project managers sobre donde se debe enfocar el esfuerzo.

Utilizando valores fijos en lugar de permitir valores variados escogidos por cada equipo de trabajo, se establecerá una base común para la evaluación cualitativa y la interpretación entre diferentes proyectos. Sin esta base, no existirá una manera de comparar efectivamente los riesgos de un proyecto a otro, o determinar como la organización mejora su manejo del riesgo a través del tiempo

**7.2.1.2. Probabilidad de riesgo:** Se define como la posibilidad de que un evento suceda.

La siguiente tabla muestra la definición de la probabilidad de los riesgos. Durante el análisis de riesgos, la probabilidad de que un evento dado ocurra es evaluada y su valor es asignado basado en los valores que se muestran en el siguiente cuadro.

Categoría de la Probabilidad	Probabilidad	Descripción
Muy Alta	0.90	Se espera que el evento del riesgo ocurra
Alta	0.70	Es mayor la posibilidad de que ocurra
Probable	0.50	Puede o no puede ocurrir
Baja	0.30	La probabilidad de que ocurra es menor
Muy Baja	0.10	No se espera que ocurra

Cuadro 1. Valores de Probabilidad.



**7.2.1.3. Impacto del Riesgo:** Es el efecto en los objetivos del riesgo si el evento ocurre.

Los siguientes cuadros muestran las definiciones del impacto sobre cada una de las áreas potencialmente impactadas en el proyecto (costo, cronograma, alcance y calidad). Existe un cuadro que define cualitativamente el impacto tanto para los riesgos negativos (amenazas) como para los positivos (oportunidades). Durante el análisis de riesgo el impacto potencial se lleva a cabo para cada riesgo y su impacto es categorizado apropiadamente según los cuadros que se muestran a continuación.

<b>Valores de Impacto</b>	
Muy Bajo	0.10
Bajo	0.20
Moderado	0.40
Alto	0.60
Muy Alto	0.80

**Cuadro 2.** Valores de Impacto.

Objetivo del proyecto	Muy Bajo 0.10	Bajo 0.20	Moderado 0.40	Alto 0.60	Muy Alto 0.80
Costo	Impacto insignificante	< 10% Impacto en Costo	10-20% Impacto en costo	20-40% Impacto en costo	> 40% Impacto en costo
Cronograma	Impacto insignificante	< 5% Impacto en Cronograma	5-10% Impacto en Cronograma	10-20% Impacto en Cronograma	> 20% Impacto en Cronograma
Alcance	Apenas perceptible	Áreas menores impactadas	Áreas mayores impactadas	Cambios inaceptables por el patrocinador	Producto efectivamente inútil
Calidad	Apenas perceptible	Únicamente afectadas aplicaciones muy demandantes	Reducción en calidad debe ser aprobado por Patrocinador	Reducción en Calidad inaceptable por el patrocinador	Producto efectivamente Inútil.

**Cuadro 3.** Impacto del Riesgo Negativo o Amenaza



Objetivo del proyecto	Muy Bajo 0.10	Bajo 0.20	Moderado 0.40	Alto 0.60	Muy Alto 0.80
Costo	Mejora insignificante	< 10% Reducción en costo	10-20% Reducción en costo	20-40% Reducción en costo	> 40% Reducción en costo
Cronograma	Mejora insignificante	< 5% Reducción En Cronograma	5-10% Reducción en Cronograma	10-20% Reducción en Cronograma	> 20% Reducción en Cronograma
Alcance	Apenas perceptible	Áreas menores optimizadas	Áreas mayores optimizadas	El alcance será impactado en más de un 50%	Producto redefinido positivamente en términos de Alcance.
Calidad	Apenas perceptible	Áreas menores optimizadas	Áreas mayores optimizadas	La calidad será mejorada en más de un 50%	Producto redefinido positivamente en términos de Calidad.

**Cuadro 4.** Impacto de la Oportunidad

#### 7.2.1.4. Matriz de Impacto

Consiste en una matriz cuyos valores son asignados combinando la probabilidad cualitativa por el impacto. El color de la matriz indica cual será el rango de valores que será alto (rojo), moderado (amarillo) y bajo (verde).

Matriz de Impacto					
0.90	0.09	0.18	0.36	0.54	0.72
0.70	0.07	0.14	0.28	0.42	0.56
0.50	0.05	0.1	0.20	0.30	0.40
0.30	0.03	0.05	0.12	0.18	0.24
0.10	0.01	0.02	0.04	0.06	0.08
	0.10	0.20	0.40	0.60	0.80

**Cuadro 5.** Matriz de Impacto

#### 7.2.1.5. Roles y Responsabilidades:

**Project Manager:** Es el responsable de aprobar el Plan de gestión de Riesgos (este documento), lidera y participa en el proceso de gestión de riesgos en todas sus etapas (identificación, análisis, planificación de la respuesta, seguimiento y control) y es el responsable de ejecutar el plan de respuesta a los riesgos cuando llega el momento. Es el responsable de la última decisión de las acciones a tomar en coordinación con los patrocinadores del proyecto.

**Project Team:** Los miembros del proyecto (analistas, desarrolladores, testers, etc.) participan en el proceso de identificación y en las tareas de monitoreo y mitigación en las reuniones de equipo.

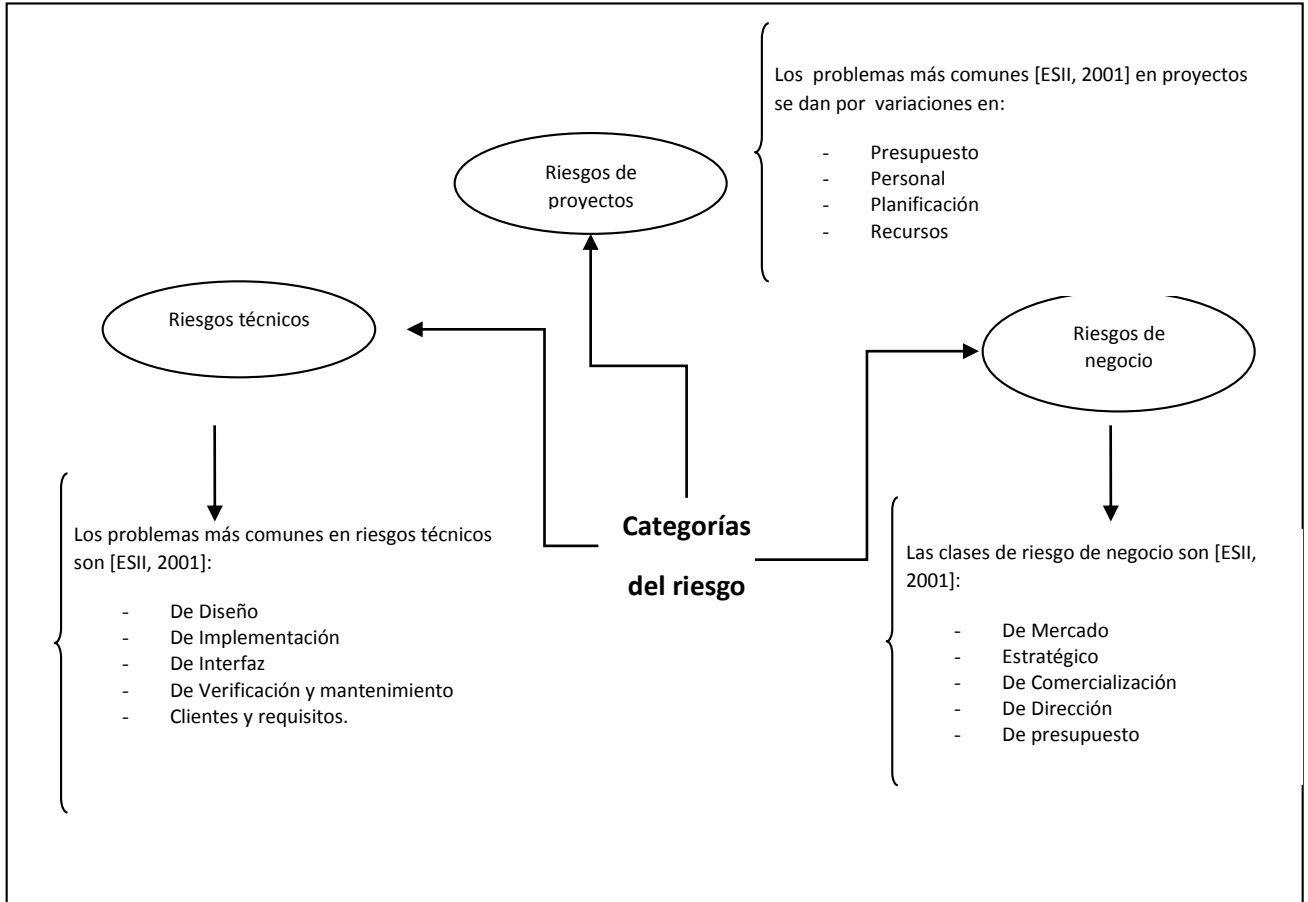
**Patrocinadores:** Participan en la identificación de riesgos y en las actividades del plan de respuesta a los riesgos de ser necesario.

También reciben escalaciones de riesgos y sus respectivas respuestas.

**Interesados:** Asisten monitoreando la efectividad de las acciones tomadas frente los riesgos y participan en la escalación de riesgos de ser necesario.

### 7.2.1.6. Categorización de Riesgos

El modelo establece tres categorías del riesgo como un mecanismo para clasificar y organizar los riesgos pensando en la futura fase de identificación.



**Figura 3 1.** Categorías relacionadas con la identificación de riesgos en proyectos de software.

A continuación se da una breve descripción de cada una de las categorías:

- **Riesgos de proyecto:** Relacionados al plan de proyecto. Para el modelo se consideran dos específicamente:
  - a) **Riesgos en calendario:** eventos que generan retrasos en la terminación de actividades y también, pueden generar retraso en la terminación del proyecto.
  - b) **Riesgos en costos:** Son los riesgos asociados con la capacidad del proyecto de mantener el costo del ciclo de vida planeado.
- **Riesgos técnicos:** son aquellos aspectos o eventos asociados con la definición del alcance del proyecto que podrían afectar el nivel actual de funcionalidad del sistema con respecto a la misión requerida y el análisis de requerimientos documentado.
- **Riesgos de negocio:** Riesgos que afectan la viabilidad de negocio del software desarrollado.



Para la fase de Identificación de los riesgos, se utilizará la técnica de identificación basada en taxonomía de riesgos para desarrollos de software elaborada por SEI (Instituto de Ingeniería de Software):

## A. INGENIERÍA DE PRODUCTO

### 1. Requisitos

- a) Estabilidad
- b) Completitud
- c) Claridad
- d) Validez
- e) Factibilidad
- f) Precedente
- g) Escala

### 2. Diseño

- a) Funcionalidad
- b) Dificultad
- c) Interfaces
- d) Rendimiento
- e) Capacidad de probarse
- f) Las limitaciones de hardware
- g) Software no desarrollado

### 3. Código y Prueba Unitaria

- a) Factibilidad
- b) Pruebas
- c) Codificación/ Implementación

### 4. Integración y Prueba

- a) Entorno
- b) Producto
- c) Sistema

### 5. Ingeniería Especialidades

- a) Mantenibilidad
- b) Confiabilidad
- c) Seguridad
- d) Garantía
- e) Factores Humanos
- f) Especificaciones

## B. ENTORNO DE DESARROLLO

### 1. Proceso de Desarrollo

- a) Formalidad
- b) Adecuación
- c) Control del Proceso
- d) Familiaridad
- e) Control de Productos

### 2. Sistema de Desarrollo

- a) Capacidad
- b) Idoneidad
- c) Usabilidad

d) Familiaridad

e) Confiabilidad

f) Apoyo al sistema

g) Entregas

### 3. Proceso de Gestión

- a) Planificación
- b) Organización del proyecto
- c) Gestión de la Experiencia
- d) Interfaces Programa

### 4. Métodos de Gestión

- a) Monitoreo
- b) Administración de Personal
- c) Seguro de calidad
- d) Gestión de la Configuración

### 5. Entorno de Trabajo

- a) Actitud de Calidad
- b) Cooperación
- c) Comunicación
- d) Moral

## C. RESTRICCIONES DEL PROGRAMA

### 1. Recursos

- a) Cronograma
- b) Personal
- c) Presupuesto
- d) Instalaciones

### 2. Contrato

- a) Tipo de contrato
- b) Restricciones
- c) Dependencias

### 3. Interfaces Programa

- a) Cliente
- b) Contratistas Asociados
- c) Subcontratistas
- d) Contratista Principal
- e) Gestión de la empresa
- f) Proveedor



### 7.2.2. Identificar Riesgos.

Descripción de la estrategia y los métodos a utilizar para la identificación de los riesgos en el proyecto

- **Entradas:**
  - ✓ Plan de Gestión de Riesgos.
- **Salidas:**
  - ✓ Lista de Riesgos identificados.

#### 7.2.2.1. Antecedentes y Marco de trabajo

Durante la identificación de riesgos se desarrolla una búsqueda de causas y eventos potenciales de riesgos y oportunidades para el proyecto. Una lista predefinida de categorías de riesgos provee una estructura que ayuda a asegurar a que un proceso sistemático se llevará a cabo para identificar los riesgos. Se utilizará como base la taxonomía de riesgos para desarrollos de software elaborada por SEI.

Como parte de la identificación de riesgos se propone utilizar esta técnica por las siguientes razones:

- Provee un marco de trabajo inicial basado en una taxonomía de riesgos para desarrollos de Software la cual corresponde perfectamente a la línea de negocio en la cual IquitosPlay se desenvuelve.
- El método de identificación es semi-estructurado, es decir, que orienta y focaliza la búsqueda de riesgos en el ámbito de desarrollo de proyectos de software, pero no se cierra únicamente a la estructura ni a las preguntas presentadas en el cuestionario, sino que la herramienta genera una discusión cuyo fin es dirigir los esfuerzos de identificación sin cerrar la posibilidad a analizar o evaluar temas que no estén explícitamente incluidos en la taxonomía o en el cuestionario.
- Su aplicación es de corta duración y ha producido resultados muy importantes según estudios realizados por el SEI (Instituto de Ingeniería de Software).

Una vez identificado y categorizado, el evento del riesgo debe ser ingresado en el registro de riesgos.

#### 7.2.2.2. Fuentes

La identificación de riesgos se realiza a través de todo el ciclo de vida del proyecto, sin embargo la mayoría de los riesgos deberían ser identificados de manera temprana de manera tal que se pueda realizar un plan de respuesta apropiado y un monitoreo y control adecuado. Se considerarán las siguientes técnicas y herramientas para la identificación de riesgos:

- Análisis de entregables.
- Análisis del WBS y el cronograma.
- Análisis de las solicitudes de cambio al alcance.
- Análisis de las asunciones del proyecto.
- Cuestionario Basado en Taxonomía de Riesgos del SEI.
- Lecciones aprendidas y documentación de proyectos anteriores.

#### 7.2.2.3. Documentación:

Todos los riesgos identificados deben ser documentados e ingresados en el registro de riesgos. Durante la identificación de riesgos, la siguiente información se requiere documentar como mínimo:

- Categoría del riesgo.
- Evento.
- Resultado del evento (positivo o negativo).
- Levantado por
- Fecha del levantamiento.
- Origen del riesgo organizar



El disparador del riesgo es un evento que debería ocurrir antes de que el resultado del evento se pueda observar. Cuando un disparador se ejecuta, el riesgo deja de ser riesgo y se convierte en un hecho, un problema materializado que necesita una resolución o bien una oportunidad que necesita ser abordada.

### 7.2.3. Análisis Cualitativo de Riesgos

El Análisis de riesgos consiste primordialmente en determinar a cuales eventos de riesgos se le garantizará una respuesta proactiva en el plan.

- **Entradas:**
  - ✓ Plan de Gestión de Riesgos.
  - ✓ Lista de Riesgos Identificados.
- **Salidas:**
  - ✓ Lista Priorizada de riesgos.

El análisis constará de dos partes:

- **Análisis Cualitativo:** consiste en evaluar el impacto y la posibilidad de que el evento del riesgo impacte los objetivos del proyecto. Las etiquetas de impacto y probabilidad se definen en la herramienta para analizar y priorizar riesgos, según las necesidades y el conocimiento adquirido de la compañía.
- **Priorización:** consiste en priorizar los riesgos identificados para enfocar los recursos y esfuerzos de este plan en los riesgos y/u oportunidades de mayor probabilidad y mayor impacto en los objetivos del proyecto.

El análisis será determinado considerando los costos del proyecto (nivel de esfuerzo, duración de las tareas, costo de hora laboral, materiales directos, equipos y herramientas) y el cronograma del proyecto (escasez de recursos, expansión de la duración, atrasos).

La probabilidad y los impactos estimados serán basados en la información derivada de:

- Valores estimados
- Juicio de expertos
- Datos Históricos
- Métricas financieras

En la definición de los parámetros del riesgos se ha establecido una base para el análisis cualitativo .La escala de las probabilidades y las definiciones del impacto del riesgo se ha sido definido. Una vez que el impacto y la probabilidad han sido debidamente seleccionadas, procede determinar su calificación. La matriz de probabilidad e impacto también se definió. La matriz muestra la combinación del impacto y la probabilidad y su asociada prioridad (mostrado en rojo, amarillo y verde según las prioridades definidas). Se debe utilizar la función de ordenamiento de Excel para ordenar las líneas de mayor a menor, para poder obtener las de mayor calificación arriba (en color rojo) y las de menor calificación abajo (en color verde).

La prioridad de Riesgos es utilizada durante la planeación de respuesta a los riesgos y durante la fase de monitoreo y control Es importante comprender que la prioridad de cada riesgo permite al equipo del proyecto entender la importancia relativa de cada riesgo.



**Documentación:** El análisis de riesgos será documentado en el registro de riesgos. Se requiere como mínimo la siguiente información:

- Impacto del Riesgo
- Probabilidad del Riesgo
- Calificación del Riesgo (Calculado por la hoja de cálculo una vez que se ingresa el impacto y la probabilidad)
- Prioridad del Riesgo (Calculado por la hoja de cálculo una vez que se ingresa el impacto y la probabilidad)
- Impacto Cualitativo (Un comentario descriptivo sobre el impacto potencial del riesgo).

#### 7.2.4. Análisis Cuantitativo de los Riesgos.

Realizar el Análisis Cuantitativo de Riesgos es el proceso de analizar numéricamente el efecto de los riesgos identificados sobre los objetivos generales del proyecto. El beneficio clave de este proceso es que genera información cuantitativa sobre los riesgos.

- **Entradas:**
  - ✓ EDT
  - ✓ Lista de Riesgos Identificados.
- **Salidas:**
  - ✓ Valores cuantitativos del impacto de los riesgos

Este proceso utiliza la información obtenida en el análisis cualitativo, pues se aplica a los riesgos priorizados en dicho procesos.

**Modelado y Simulación:** Mediante la simulación y Modelado se obtiene el impacto potencial de los riesgos sobre los objetivos. Se realizara mediante la técnica Monte Carlo.

**Técnica monte Carlo:** El modelado y Simulación se realiza mediante iteración, utilizando valores de entrada, como estimaciones de costo o duraciones de actividades. Esta técnica permite focalizar la gestión en aquellos riesgos que realmente nos interesa tratar, permitiéndonos ahorrar tiempo.

En la técnica de Montecarlo se utiliza la herramienta @Risk , mediante la herramienta se da variabilidad a los datos que se estudian, por ejemplo: inicialmente para la codificación del software se tiene 20 días, dar variabilidad se refiere a tratar ahora mediante intervalos de tiempo [10días-30 días] para ello se utiliza distribución estadística (Distribución triangular)

#### 7.2.5. Plan de Respuesta de Riesgos.

El plan de respuesta tiene como propósito responder tanto a las amenazas como a las oportunidades para cada riesgo seleccionado en el proceso de priorización, como mínimo, para los riesgos cuya calificación sea Alta.

- **Entradas:**
  - ✓ Plan de Gestión de Riesgos.
  - ✓ Lista priorizada de Riesgos.
  - ✓ Valores cuantitativos del impacto de los riesgos
- **Salidas:**
  - ✓ Plan de Respuesta de Riesgos.



## Estrategias

Existen varias estrategias para responder a los eventos probables que pueden afectar el resultado de un proyecto. A continuación se listan las estrategias que serán utilizadas:

- **Eliminar:** Evitar el riesgo implica hacer los cambios necesarios en el plan de gestión de un proyecto, de manera que la amenaza sea eliminada, aislando el objetivo del impacto de ese riesgo o eliminando el impacto que ese evento pueda producir cuando ocurra.
- **Transferir:** La transferencia de los riesgos implica mover el impacto negativo de una amenaza (y la posesión u “ownership” de la respuesta a un tercero. La transferencia no elimina la amenaza, simplemente transfiere la responsabilidad a un tercero de manejarla.
- **Mitigar:** La acción de mitigar un riesgo negativo o amenaza consiste en reducir la probabilidad y/o el impacto a un nivel más aceptable. Tomando una acción proactiva hacia el riesgo es mucho más efectiva que tratar de reparar el daño una vez que el riesgo se ha convertido en un hecho. Desarrollar planes de contingencia son ejemplos de mitigación de riesgo.
- **Compartir:** Compartir consiste en asignar la propiedad de una oportunidad a un tercero mejor capacitado para explotarla en beneficio del proyecto. Implica una activa participación por parte de la gerencia de los riesgos que podrían afectar los objetivos del proyecto, producto de esta estrategia. Ejemplo de esto son Alianzas, Consorcios y Asociaciones temporales.
- **Explotar:** Una vez que se ha identificado un evento posible que podría traer un resultado positivo si llegara a realizarse, se trata de eliminar toda incertidumbre de manera que sea un hecho y poder así sacar provecho de esta oportunidad.
- **Mejorar:** Consiste en aumentar la probabilidad y/o el impacto de una oportunidad. Se deben identificar cuáles son los eventos o circunstancias causales de esta oportunidad y trabajar sobre ellas, para aumentar la probabilidad de que sucedan, así como el impacto sobre los objetivos del proyecto.
- **Aceptar:** La aceptación es usualmente tomada como una estrategia para gestionar riesgos (sean estos oportunidades o amenazas) ya que es difícil tener un plan de respuesta para cada riesgo identificado para no afectar la rentabilidad del proyecto. La aceptación de los riesgos debe ser tomada únicamente para los riesgos de baja prioridad. Puede ser pasiva, donde ninguna acción es tomada, o activa donde se puede hacer una reserva de presupuesto o en el cronograma para los riesgos conocidos o desconocidos.

## Presupuesto

Cada uno de los Planes de respuesta (excepto aceptar se menciona más adelante) tiene un costo asociado, el cual debe ser indicado y actualizado en el registro de riesgos y en el Plan Gestión del Proyecto.

Para los riesgos aceptados (usualmente los que tienen menor calificación en la matriz de Probabilidad e Impacto) se definirán provisiones de contingencia para cubrir esos eventos, así como para posibles riesgos aún no identificados. Para definir estos montos se utilizarán los siguientes métodos:

- Uso de provisiones estándar (monto fijo).
- Porcentajes basados en la experiencia.

## Documentación

El resultado del proceso de la planificación de la respuesta a los riesgos debe ser documentado en los registros de riesgo. La siguiente información debe ser ingresada en los registros:

- Estrategia de respuesta (Eliminar, mitigar, aceptar, mejorar, compartir, explotar, transferir)
- Propietario del Riesgo
- Descripción del plan. Se deben describir cuáles serán las acciones a tomar y de qué manera serán abordadas. Pueden ser indicadas en el registro de riesgos y/o anexadas en el Apéndice de este documento según corresponda. Asimismo estas acciones deben ser incluidas en el Plan de Gestión del proyecto, por lo que el alcance (WBS) y el cronograma deben ser actualizados.



### 7.2.6. Seguimiento y Control.

Las estrategias definidas para este proyecto deben ser ejecutadas según se requiera durante el ciclo de vida del proyecto, y adicionalmente se debe monitorear el surgimiento de nuevos riesgos o el cambio de los riesgos ya existentes. Durante la etapa de monitoreo y control, las siguientes tareas son realizadas:

- Identificar, analizar y planificar para los nuevos riesgos y oportunidades.
- Llevar control de los riesgos identificados y monitorear las condiciones de los disparadores definidos.
- Revisar la información de desempeño del proyecto (progreso, reportes de estado, problemas, acciones correctivas)
- Analizar nuevamente si ha variado el riesgo, la probabilidad, el impacto o la respuesta apropiada para dicho evento.
- Revisar la ejecución de las respuestas a los riesgos y analizar su efectividad
- Asegurar que las políticas y procedimientos de gestión de riesgos están siendo correctamente utilizados por los miembros del equipo del proyecto.
  
- **Entradas:**
  - ✓ Plan de Gestión de Riesgos.
  - ✓ Plan de Respuesta de Riesgos.
  - ✓ Registro de Riesgos
  
- **Salidas:**
  - ✓ Plan de Gestión de Riesgos actualizado.
  - ✓ Registro de Riesgos actualizado.
  - ✓ Comunicaciones.

#### Periodicidad

Se debe definir la periodicidad del proceso de monitoreo y control durante el ciclo de vida del proyecto según las necesidades del proyecto y la organización.

#### Documentación

El proceso de monitoreo y control debe ser documentado en los registros de riesgo. Como mínimo, la siguiente información debe ser ingresada en los registros:

- Estado – Los estados válidos son:
  - Identificado: Riesgo documentado, pero no ha sido aún analizado.
  - Análisis Completado: Analizado, pero no tiene aún un plan de respuesta asociado.
  - Planificación Completada: Plan de respuesta completado para este riesgo.
  - Disparado: El disparador ha ocurrido y la amenaza u oportunidad está siendo analizada.
  - Resuelto: El evento del riesgo ha sido abordado por el plan de respuesta.
  - Retirado: El riesgo identificado no requiere mayor seguimiento (i.e. el disparador ha ocurrido y el evento no se dio).
- Fecha del evento (Si el disparador del riesgo se ha dado)
- Notas
- Impacto Real/Tiempo: Valor agregado manualmente para ser utilizado posteriormente para analizar cuales eventos impactaron más el cronograma.
- Impacto Real/Costo: Valor agregado manualmente para ser utilizado posteriormente para analizar cuales eventos impactaron más el costo.



### 7.2.7. Cierre de Gestión de Riesgos.

Esta fase consiste en documentar las lecciones aprendidas del proceso de gestión de riesgos como parte del cierre del proyecto en el repositorio común de lecciones aprendidas del proyecto. Éstas incluyen una evaluación de la efectividad de los planes de respuesta, el desempeño del equipo de trabajo durante la etapa de seguimiento y control de riesgos, información estadística de la ocurrencia de los eventos para aumentar la exactitud de los valores probabilísticos, entre otros.

- **Entradas:**
  - ✓ Plan de Gestión de Riesgos
  - ✓ Registro de Riesgos
- **Salidas:**
  - ✓ Repositorio de Lecciones Aprendidas



## 7.3 APLICACIÓN DE LA METODOLOGIA- CASO DE ESTUDIO

### 7.3.1. Descripción del Proyecto.

Para el caso de estudio se aplicara al Proyecto "SIS- CAMARA DE COMERCIO", la empresa IquitosPlay desarrolla el Sistema Informático para la Cámara de Comercio de Iquitos. El proyecto tiene una duración de 3 meses, contando con un total de 3 programadores.

Los módulos con lo que cuenta el Sistema informático son:

1. Módulo de Personal
2. Modulo Directorio de Asociados
3. Modulo Administración y Catálogo de Servicios
4. Modulo Caja
5. Modulo Reportes
6. Modulo Control Documentario.

**Modulo Personal.** Indispensable para registrar al personal encargado de la gestión del sistema, así como la información de la institución. Permitiendo tener un control estricto sobre los datos de la Institución con los que trabajara el sistema.

Este módulo servirá específicamente para controlar los accesos al sistema según rol y/o perfil del trabajador, siendo de utilidad para la bitácora del sistema ante cualquier modificación de información sensible de la institución.

**Modulo Directorio de Asociados.** Responsable de la Administración del directorio de Asociados. Este módulo será responsable de registro y el seguimiento de pagos de los asociados de la Institución.

**Modulo Administración y Catálogo de Servicios.** Contendría la gestión de los servicios que brinda la Institución, así como un catálogo de los mismos para brindar información a sus clientes como las tarifas o precios que cobra. Además permitirá el registro de los servicios brindados a sus clientes, para luego ser derivados al módulo Caja.

**Modulo caja.** Indispensable para el registro de los pagos de diferentes servicios brindados y para el registro y control de pagos de los asociados. Permitirá conocer en cualquier momento el saldo de caja en efectivo al día.

Además se permitirá el registro y control de los egresos incluyendo al responsable, así como la información de los documentos sustentatorios.

Se define entonces que las funciones de este Módulo son:

- Control de pagos de Servicios
- Control de Pagos de Asociados
- Control de Caja Chica.

**Módulo de Reportes.** En este módulo contendrá todos los tipos de reportes que le Cliente defina, Sera diseñado a solicitud y e coordinación del cliente.

**Modulo Control Documentario.** Que permitirá el control de Emisión de los documentos hacia y desde la Institución.

**7.3.2. Gestión de Riesgos.**

❖ **Mediante la Aplicación de la Metodología se obtuvo los siguientes Riesgos:**

Nro. Ref.	Riesgo	Categoría	Tax.
1	Cambia la alta gerencia del cliente y reduce su interés en el proyecto, originando problemas de comunicación (retroalimentación)	Riesgo del Negocio	-
2	Miembros clave del proyecto renuncian, originando un retraso significativo.	Riesgo del Proyecto	[71]
3	Cambio excesivo de requerimientos originando retraso y mayor costo.	Riesgo del Proyecto	[1]
4	Se subestimó el tamaño, originando mayores costos.	Riesgo del Proyecto	-
5	Los ciclos de revisión/decisión del cliente para los planes, prototipos, y las especificaciones son más lentas de lo esperado.	Riesgo del Proyecto	[166]
6	El usuario final encuentra en última instancia el producto insatisfactorio, requiriendo el reajuste y la reanudación.	Riesgo del Proyecto	-
7	Agregan al nuevo personal del desarrollo tarde en el proyecto, y los gastos indirectos adicionales del entrenamiento y de las comunicaciones reducen eficacia a miembros existentes.	Riesgo del Proyecto	[71]
8	El uso de otra herramienta resulta retraso en tiempo en cuanto a la aplicación de la misma.	Riesgo del Proyecto	[12}
9	Planteamiento de Nuevos Requerimientos	Riesgo del Proyecto	[1]
10	Cambio excesivo de requerimientos origina mala funcionalidad.	Riesgos Técnicos	[1]
11	Los componentes de software elegidos no trabajan adecuadamente.	Riesgos Técnicos	-
12	Existen requisitos/ funcionalidades que se conoce que debe estar en la especificación, pero no lo están	Riesgos Técnicos	[4]
13	Si se presentan problemas de performance podrían darse problemas de aceptación de producto final.	Riesgos del Proyecto	-
14	Si se presentan atrasos en el cronograma y se compromete el tiempo para las pruebas podrían existir problemas de calidad no detectados	Riesgos Técnicos	[35]
15	Si no se puede contar con el personal de desarrollo en el momento que indica el cronograma podrían existir atrasos en el mismo.	Riesgo del Proyecto	[71]
16	Si los datos provistos para el ambiente de pruebas no son significativos, entonces la etapa de pruebas podría dar resultados no realistas y por lo tanto problemas de aceptación futuros.	Riesgo del Proyecto	[46]



❖ **A continuación se muestra el resultado del análisis y priorización de los riesgos.**

Nro. Ref.	Probabilidad	Impacto	Calificación
1	0.30	0.20	0.06
2	0.30	0.60	0.18
3	0.50	0.40	0.2
4	0.30	0.60	0.18
5	0.50	0.20	0.1
6	0.10	0.80	0.08
7	0.30	0.40	0.12
8	0.70	0.40	0.28
9	0.50	0.40	0.2
10	0.30	0.40	0.12
11	0.10	0.80	0.08
12	0.70	0.40	0.28
13	0.50	0.40	0.20
14	0.30	0.40	0.12
15	0.10	0.40	0.04
16	0.50	0.40	0.2

❖ **Se encontró el siguiente resultado en el análisis cuantitativo:**

Se priorizaron los riesgos: 2, 3, 6,8

**Riesgo Nro 2:**

Distribución estadística

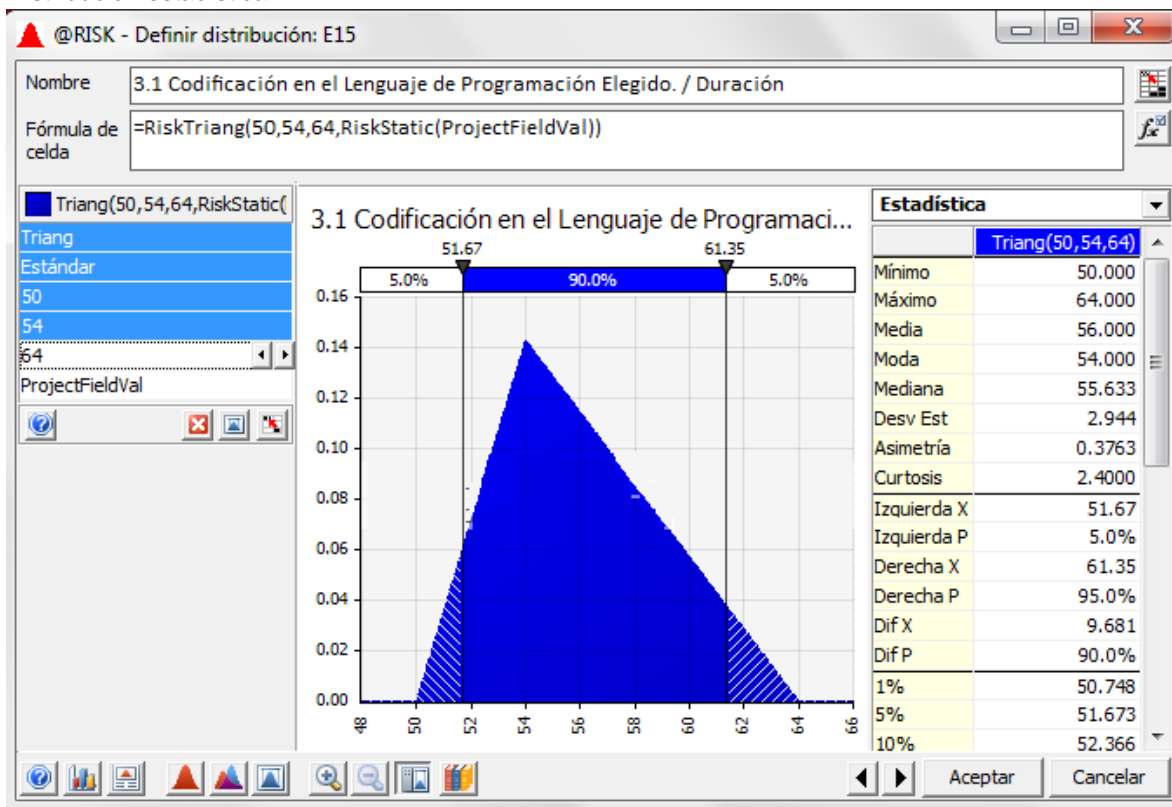


Figura 4 : Distribución estadística de Riesgo Nro 2- @Risk

### Riesgo Nro. 3:

Distribución estadística

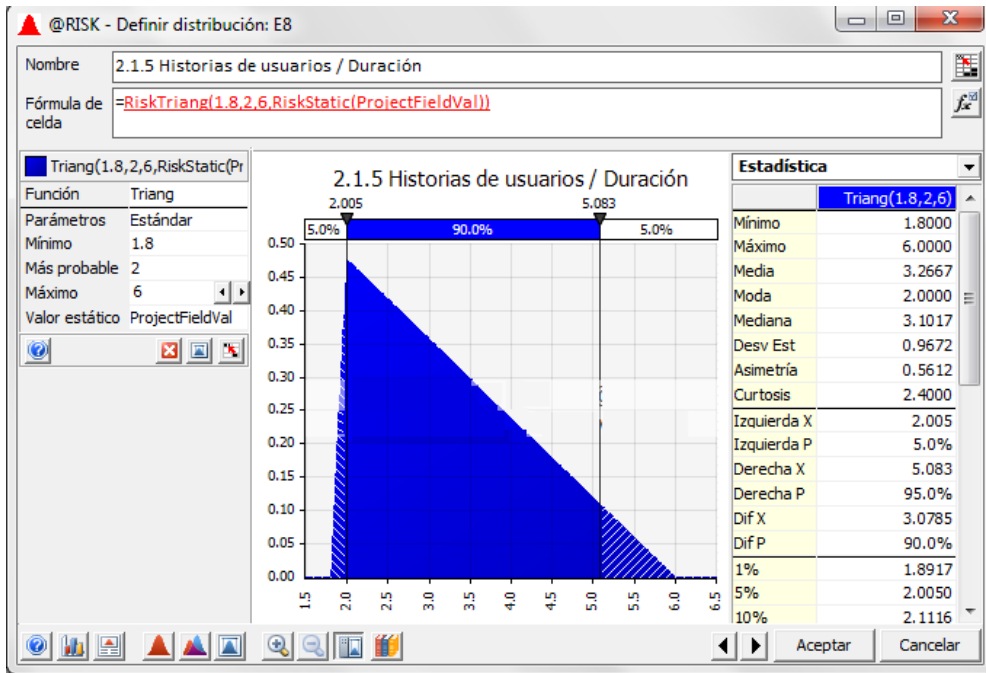


Figura 5 : Distribución estadística de Riesgo Nro 3- @Risk

### Riesgo Nro 6:

Distribución estadística

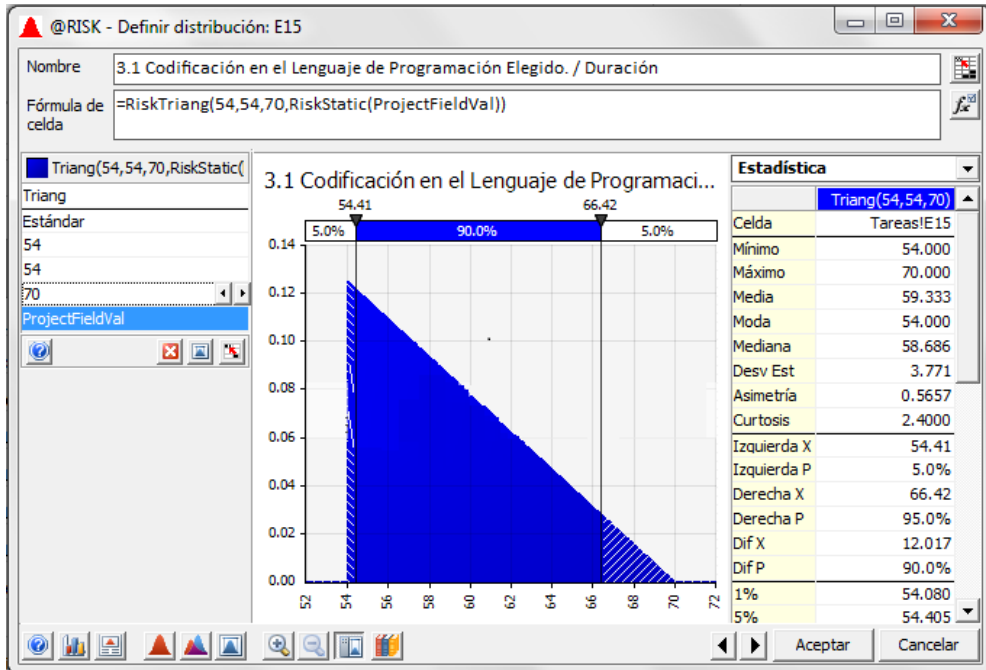


Figura 6 : Distribución estadística de Riesgo Nro 6- @Risk

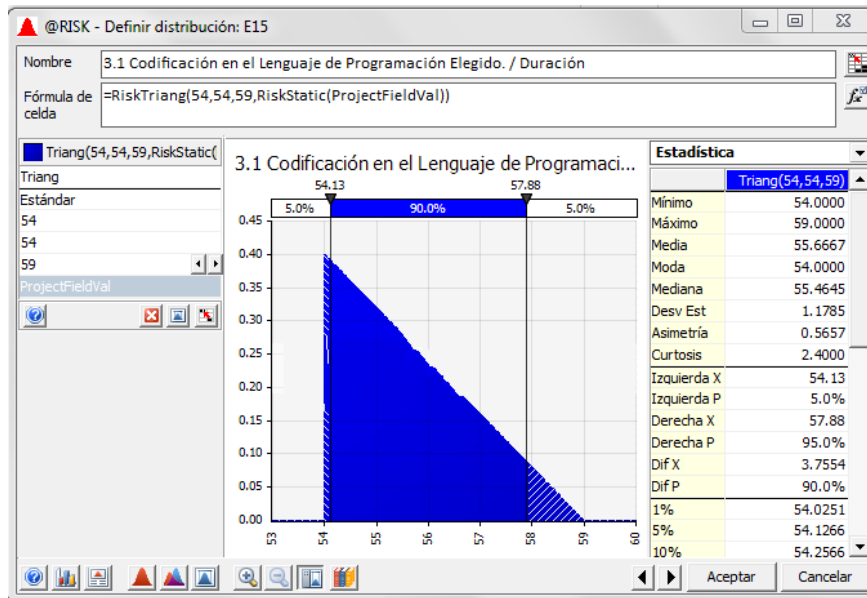
**Riesgo Nro 8:**

Figura 7: Distribución estadística de Riesgo Nro 8- @Risk

- Como vemos en las distribuciones estadísticas las actividades afectadas son la Codificación y Desarrollo de Historia de Usuarios, Siendo el Riesgo Nro 6 el que mayor abarca en la Distribución y para el Desarrollo de Historia de Usuarios solo es el Riesgo Nro.3. Por lo tanto la simulación de Mote Carlo se hará con el riesgo 6 y 3.

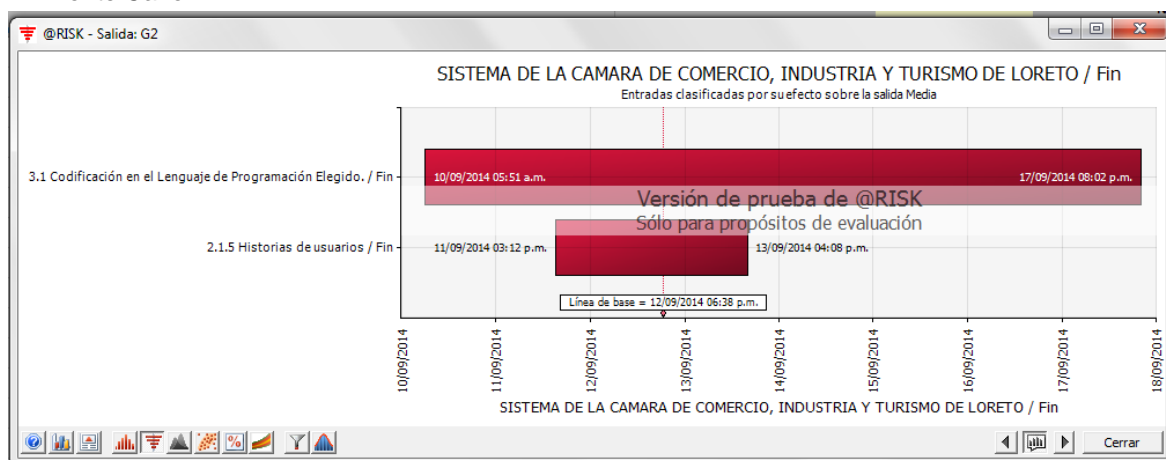
**Monte Carlo:**

Figura 8: Simulación de Montecarlo- @Risk

- El resultado nos muestra que el riesgo 6 es el que tiene mayor impacto sobre el cronograma del proyecto, pues nos muestra como termino del proyecto para el 17/09/2014, teniendo como atraso de 8 días.

❖ **Se desarrollaron planes de respuesta para los riesgos arriba mencionados:**

Nro. Ref.	Estrategia	Descripción
1	Aceptar	Se utilizara las reservas de tiempo para nuevas reuniones.
2	Mitigar	Se contratara personal calificado para el puesto del miembro que renunció.
3	Mitigar- Aceptar	-Realizar Entrevistas para obtener Requerimientos estables - Si los Nuevos Requerimientos aparecen, se desarrolla el planteamiento de nuevos requerimientos para medir el impacto en el proyecto, producto y realizar negociaciones con el cliente.
4	Mitigar	Se detallará la toma de requerimientos y se revisará el estimado del tiempo previsto inicialmente en el cronograma versus la estimación resultante del análisis. En caso de haber una discrepancia se negociará con el cliente. Nota: Debido a que se identificó este riesgo de manera proactiva, ya se han iniciado las conversaciones de antemano y se ha tomado en cuenta ésta posibilidad como una enmienda al contrato. Se han agregado las tareas en el cronograma para llevar a cabo dicho plan.
5	Mitigar	Involucrar activamente al cliente en cada una de las etapas del proyecto y sensibilizarlo acerca de la importancia de su participación.
6	Mitigar	Se programa reuniones con el cliente, para mostrar avances del software. (Se incluye actividades al cronograma del proyecto)
7	Mitigar	Realizar un plan de formación interno para maximizar y evaluar el personal de desarrollo.
8	Eliminar	Incluir en el cronograma del proyecto una capacitación/ investigación acerca de la nueva herramienta.
9	Aceptar	Gestionar por parte del equipo de diseño, el planteamiento de nuevos requerimientos para medir el impacto en el proyecto y el producto y realizar negociaciones con el cliente.
10	Mitigar- Aceptar	-Realizar Entrevistas para obtener Requerimientos estables - Si los Nuevos Requerimientos aparecen, se desarrolla el planteamiento de nuevos requerimientos para medir el impacto en el proyecto, producto y realizar negociaciones con el cliente.
11	Mitigar	Realizar pruebas Unitarias y Pruebas de Integración durante el ciclo de desarrollo.
12	Explotar	Se realizara flujos de comunicación y respuestas de los componentes, para mejorar funcionalidades o encontrar posibles nuevos requisitos
13	Mitigar	Se programa reuniones con el cliente, para mostrar avances del software. (Se incluye actividades al cronograma del proyecto)
14	Mitigar	Se incluyen actividades de pruebas de calidad
15	Mitigar	Se debe aplicar sanción y descuentos a los trabajadores que no cumplan con lo planificado. Se contrata personal.
16	Transferir	Se aclarará este riesgo con el cliente. La empresa IquitosPlay no se puede hacer responsable del comportamiento de la aplicación cuando ésta entre en producción si no cuenta con un ambiente de pruebas y datos significativos para realizar las pruebas del sistema. Se agregaron tareas en el cronograma para llevar a cabo este proceso (reuniones, negociación para tomar una decisión).



## 7. CONCLUSIONES

- Se logró desarrollar una metodología de gestión de riesgos especializada en el desarrollo de proyectos de software, mediante las especificaciones de los procedimientos para realizar la gestión de riesgos, proporcionando plantillas e instructivos que se utilizan en la aplicación de la metodología.
- Se comprobó que el cuestionario de identificación de Riesgos basado en Taxonomía de Software brinda un punto de partida significativo para la identificación de riesgos, debido a que cubre una gran cantidad de aspectos que se sabe de antemano que afectarán el resultado de los proyectos de este tipo.
- Generar un análisis de riesgo es beneficioso para un proyecto, sin embargo este pierde toda validez si únicamente es analizado en documentos y no se lleva a la práctica. Debe existir un estricto plan de monitoreo que verifique el estado de los compromisos o acciones iniciales y las condiciones de los disparadores identificados.
- Para el éxito de la gestión de riesgos es imprescindible que estos sean identificados de forma temprana, siendo clave que esto ocurra antes de comprometer con el cliente del producto el alcance, fecha de entrega y presupuesto del proyecto. Una vez identificados, sus planes de respuesta deben ser contemplados en la planificación en la forma de cambios de alcance en las actividades, modificación de la forma de realizar el trabajo, inclusión de holguras y reservas de presupuesto, así como decisiones de incorporación de personal con mayor experticia o subcontrataciones con terceros.
- La aplicación de la metodología de gestión de riesgos en la empresa permitirá que ésta se prepare proactivamente contra las amenazas que afecten el resultado y la rentabilidad de sus proyectos.
- El Proyecto permitió identificar que en IquitosPlay se requiere fortalecer la cultura de gestión de riesgos, esto involucra desde el estudio y aprobación del proyecto hasta el cierre. Con ese proyecto se avanza en esa dirección ya que le permite a IquitosPlay tener una documentación completa de dicho proceso. Se evidenció que el manejo de riesgos en forma documentada y estandarizada bajo los lineamientos del PMI (Project Management Institute), le brinda a IquitosPlay un valor agregado y aumenta el nivel de compromiso de sus colaboradores en la ejecución de las labores ya que el manejo empírico y sin documentación que se realizaba anteriormente causaba un desgaste de los trabajadores y mayor gasto económico para IquitosPlay.



## 8. REFERENCIA BIBLIOGRÁFICA

- **[Fundamentos Para la Dirección de Proyectos (Guía del PMBOK)]**  
Guía de los fundamentos para la dirección de proyectos- Quinta edición.  
©2013 Project Management Institute, 595 páginas.
- **[URL01]**  
Gestión de Riesgos en Ingeniería de Software.  
URL disponible: [http://dis.um.es/~barzana/Informatica/IAGP/IAGP\\_riesgos.html](http://dis.um.es/~barzana/Informatica/IAGP/IAGP_riesgos.html)
- **[URL02]**  
Riesgos, PMBOK Gestión  
URL disponible: [http://pmbok1.blogspot.com/p/blog-page\\_2251.html](http://pmbok1.blogspot.com/p/blog-page_2251.html)
- **[URL03]**  
Gestión de los Riesgos del Proyecto  
URL disponible: <http://whatisprojectmanagement.wordpress.com/2013/01/24/gestion-de-los-riesgos-del-proyecto/>
- **[URL04]**  
Gestión de Riesgos  
URL disponible: [http://pmbokmetodologiaibmp.blogspot.com/2012/10/normal-0-21-false-false-false-es-x-none\\_15.html](http://pmbokmetodologiaibmp.blogspot.com/2012/10/normal-0-21-false-false-false-es-x-none_15.html)
- **[URL05]**  
Gestión de Riesgos en Proyectos Software.pdf  
URL disponible:  
[http://www.google.com.pe/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CBkQFjAA&url=http%3A%2F%2Focw.unican.es%2Fensenanzas-tecnicas%2Fingenieria-del-software-ii%2Fmateriales%2Ftema7-gestionRiesgos.pdf&ei=uJLrU-vLJoPKsQTquYCoAQ&usq=AFQjCNHWX\\_Zgqak1EbCiq6jPmpGP8yx7-w&bvm=bv.72938740.d.b2U](http://www.google.com.pe/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=0CBkQFjAA&url=http%3A%2F%2Focw.unican.es%2Fensenanzas-tecnicas%2Fingenieria-del-software-ii%2Fmateriales%2Ftema7-gestionRiesgos.pdf&ei=uJLrU-vLJoPKsQTquYCoAQ&usq=AFQjCNHWX_Zgqak1EbCiq6jPmpGP8yx7-w&bvm=bv.72938740.d.b2U)
- **[URL06]**  
Una taxonomía para la identificación de riesgos en los proyectos de desarrollo de software de la Universidad de las Ciencias Informáticas .pdf  
URL disponible: <http://publicaciones.uci.cu/index.php/SC/article/view/785/511>







**Instructivo**

Columna	Instrucciones
Nro. De Ref.	Numeración del riesgo, permite hacer referencia al riesgo por su número.
Descripción del problema	Describe las causas inmediatas (directas) que dan origen a la incertidumbre asociada con el riesgo.
Riesgo	Se expresa en términos del objetivo de proyecto que podría verse afectado, que son: Alcance, Cronograma, Costo y Calidad. Por ejemplo: Retraso en el cronograma, Costos mayores a los esperados, Alcance no aceptado por el cliente, fallos de calidad inaceptables, entre otros.
Causas Raíz	Se documenta con base en la investigación detallada del problema, identificando la causa que dio origen. Para identificar causas raíz se utiliza el cuestionario basado en la taxonomía.
Fecha de Identificación	La Fecha (en formato dd/mm/aaaa) en que fue identificado el riesgo por primera vez en el proceso de Gestión de Riesgos. Los riesgos deben identificarse en las etapas de inicio y planeación, que debe ser antes que estos ocurran durante la ejecución.
Tipo de Riesgo	Se marca con una X si el riesgo tiene un efecto adverso sobre el objetivo de proyecto (amenaza) o si tiene un efecto positivo (oportunidad).
Categoría de Riesgo	Categorías en las que se clasificaran los riesgos, , estos pueden ser: Técnicos, de Proyectos, de Negocio.
Objetivo de proyecto afectado	Se marca con una X el objetivo de proyecto afectado entre las siguientes opciones: Alcance, Tiempo, Costo y Calidad. El efecto puede ser adverso si el riesgo es de tipo amenaza (según columna "Tipo") o puede ser positivo si se trata de un riesgo de tipo "Oportunidad".
Tipo de Impacto	Se marca con una X si el evento de riesgo tiene impacto "Directo" o "Indirecto" sobre el objetivo de proyecto afectado. Impacto directo se refiere a cuando el efecto es inmediato y directamente vinculado con el evento, mientras que los efectos indirectos pueden manifestarse tardíamente o en otras áreas del proyecto.
Probabilidad	Probabilidad de ocurrencia del Riesgo.
Valoración de Impacto	Se valora el impacto del riesgo para cada uno de los siguientes objetivos de proyecto: Alcance, Tiempo, Costo y Calidad. Para cada uno se asigna un valor e una escala del 0 al 1, 0 siendo mínimo impacto y 1 máximo impacto.



Probabilidad por Impacto	Utilizando matrices de probabilidad e impacto se determina la valoración probabilidad e impacto para cada objetivo de proyecto, es decir Alcance, Tiempo, Costo y Calidad. La Matriz de probabilidad e impacto no está incluida en otra plantilla. Una alternativa frente a la matriz de probabilidad e impacto es realizar la multiplicación de la probabilidad por el impacto en cada objetivo. En esta plantilla, la formula está registrada de esta forma.
Valoración Global del Riesgo	Se calcula a partir de las valoraciones de Probabilidad por Impacto de cada objetivo de Proyecto, aplicando una ponderación que se basa en que objetivo es más importante para cada proyecto.
Prioridad	El nivel de prioridad puede asignarse a partir de la valoración global, utilizando umbrales para asignarles prioridad Alta, Media y Baja. Por ejemplo, riesgos con más de 0,4 de valoración podrían tener prioridad alta.
Dueño (Owner)	Persona o grupo gerencial que es responsable de asegurar que la probabilidad de ocurrencia e impactos sean minimizados, si se trata de amenazas, o maximizados, si se trata de oportunidad.
Responsable	Persona o grupo gerencia que por lo general puede ser el mismo dueño (owner), sin embargo, el dueño puede delegar esta tarea en otro responsable. Por ejemplo si un ejecutivo (Vicepresidente) es el dueño de un riesgo, este puede delegar la responsabilidad en uno de sus grupos gerenciales.
Estrategia de Respuesta adaptada	Indicar la estrategia del Plan de respuesta, según las siguientes opciones: - Para las amenazas: Evitar, Mitigar, Transferir o Aceptar. - Para las oportunidades: Explotar, Mejorar, Compartir o Aceptar.
Plan de Respuesta adaptado	Se deben describir cuáles serán las acciones a tomar y de qué manera serán abordadas
Riesgo Residual (Secundario)	En los casos que se toman acciones de mitigación o transferencia de un riesgo u oportunidad, pueden surgir riesgos secundarios de esta forma de hacer el trabajo. Estos riesgos también deben ser evaluados o valorados y agregados al listado de riesgo en sus propios renglones. Utilice columna para hacer referencia (usando número de referencia) a estos riesgos en el mismo listado.
¿Riesgo Activado?	Se marca con una X si el riesgo anticipado en la etapa de inicio y planeación ha ocurrido durante el proyecto. Esto aplica sólo para los riesgos no mitigados, durante la fase de planeación.
Fecha de Activación	La Fecha (en formato dd/mm/aaaa) en que un riesgo previamente identificado desencadenó en un evento. Si se aplicó una adecuada gestión de riesgos del proyecto, la fecha de activación debería ser mucho después que la fecha de identificación.



**Instructivo**

Columna	Instrucciones
Nro. De Referencia	Numeración de la lección aprendida.
Nombre del Proyecto	Nombre descriptivo del proyecto en el que se identificó la lección aprendida.
Área / Categoría	Categorías en las que se clasificaran las lecciones aprendidas, por ejemplo, en un proyecto de Desarrollo de Software éstas pueden ser Técnicas, Funcionales, Comunicación, Gestión de los implicados, entre otros; o por ejemplo podrían usarse las áreas de conocimiento de la Gestión de Proyecto, por ejemplo alcance, tiempo, calidad, comunicaciones, entre otros.
Fecha	Día, mes y año en que se presentó la situación descrita.
Amenaza / Oportunidad	Se indica si la lección aprendida está relacionado con un efecto adverso (amenaza) que debe evitarse en el futuro o está asociado con un efecto positivo en el proyecto (oportunidad) sobre el cual deben tomarse acciones para mantenerlo.
Título	Alusivo a la situación presentada.
Descripción de la Situación	Describe los antecedentes y circunstancias que ocasionaron el asunto sujeto de la lección aprendida, siendo importante el identificar las causas raíz que ocasionaron la situación.
Descripción del Impacto en los objetivos del proyecto	Efecto que la situación planteada tuvo sobre los objetivos del proyecto, por ejemplo: Retraso en la fecha de entrega del proyecto, incremento de los costos, reducción de niveles de calidad, insatisfacción del cliente, entre otros. También puede reflejar impactos positivos, por ejemplo, se terminó la actividad antes de la fecha planificada, se ejecutó una actividad a una fracción del costo, entre otros. Es importante expresar el impacto en términos que se puedan medir.
Acciones Correctivas y Preventivas Implementadas	Enumerar las acciones correctivas implementadas para reducir o mejorar los efectos de la situación (dependiendo si son amenazas u oportunidades) y acciones preventivas para reducir o incrementar la probabilidad que se vuelvan a presentar en el futuro.
Lección Aprendida / Recomendaciones	Resume las acciones y estrategias a adoptar en el futuro para evitar que se presente nuevamente la amenaza o para aprovechar la oportunidad (si es una lección de impacto positivo). Se construye a partir de las experiencias de las acciones tomadas para corregir la situación.



### **Anexo 3 - Estructura de Descomposición del trabajo EDT**

**(Desarrollo del Sistema- Cámara de Comercio, Industria y Turismo de Loreto)**

	Nombre de tarea	Duració	Comier	Fin
1	▲ SISTEMA DE LA CAMARA DE COMERCIO, INDUSTRIA Y TURISMO DE LORETO	80 días	21/05/14	09/09/14
2	▲ 1. Planificación de Proyecto.	5 días	21/05/14	27/05/14
3	▲ 1.1. Determinación de Requerimientos	4 días	21/05/14	26/05/14
4	2.1.1. Definición del caso de estudio	1 día	21/05/14	21/05/14
5	2.1.2. Estudio de la organización	1 día	21/05/14	21/05/14
6	2.1.3. Análisis de procedimientos	1 día	22/05/14	22/05/14
7	2.1.5 Historias de usuarios	2 días	23/05/14	26/05/14
8	1.2. Descripción del Sistema Propuesto	1 día	27/05/14	27/05/14
9	▲ 2. Diseño	9 días	28/05/14	09/06/14
10	2.1. Diseño de Salidas/Interfaz	5 días	28/05/14	03/06/14
11	2.2. Definición de la Base de Datos	2 días	04/06/14	05/06/14
12	2.3. Tarjetas CRC	2 días	06/06/14	09/06/14
13	▲ 3. Programacion	55 días	10/06/14	25/08/14
14	3.1 Codificación en el Lenguaje de Programación Elegido.	2.7 mss	10/06/14	22/08/14
15	3.2 Compilación y Depuración del Programa	2.7 mss	10/06/14	22/08/14
16	3.3. Liberación del Programa	1 día	25/08/14	25/08/14
17	▲ 4. Prueba	4 días	26/08/14	29/08/14
18	4.1. Pruebas Unitarias	2 días	26/08/14	27/08/14
19	4.2 Pruebas de Aceptacion	2 días	28/08/14	29/08/14
20	▲ 5. Implantación	7 días	01/09/14	09/09/14
21	5.1. Prueba del Sistema	2 días	01/09/14	02/09/14
22	5.2 Documentacion del Sistema	5 días	03/09/14	09/09/14



## **Anexo 4 - Cuestionario basado en la taxonomía**

### **A. Ingeniería de Producto**

#### **1. Requisitos**

##### **a) Estabilidad**

**[¿Son requisitos cambiantes, incluso a medida que se desarrolla el producto?]**

[1] ¿Los requisitos son estables?

(No) (1.a) ¿Cuál es el efecto en el sistema?

- Calidad
- Funcionalidad
- Integración
- Diseño
- Pruebas

[2] ¿Están cambiando las interfaces externas?

##### **b) Completitud**

**[¿Son requisitos incompletos o pocos específicos?]**

[3] ¿Hay requisitos que faltan definir en las especificaciones?

[4] ¿Existen requisitos que usted conoce que debe estar en la especificación, pero no lo están?

(Sí) (4.a) ¿Serás capaz de conseguir estos requisitos?

[5] ¿El cliente tiene requisitos no escritos / expectativas?

(Sí) (5.a) ¿Hay una manera de capturar estos requisitos?

[6] ¿Están las interfaces externas definidas por completo?

##### **c) Claridad**

**[¿Son requisitos poco claros o con necesidad de interpretación?]**

[7] ¿Es capaz de comprender los requisitos según lo escrito?

(No) (7.a) ¿Las ambigüedades se resuelvan de manera satisfactoria?

(Sí) (7.b) ¿No hay ambigüedades o problemas de interpretación?

##### **d) Validez**

**[¿Los requisitos conducen al producto que el cliente tiene en mente?]**

[8] ¿Hay algún requisito que no puede especificar lo que el cliente realmente quiere?

(Sí) (8.a) ¿Cómo estás resolviendo esto?

[9] ¿Usted y el cliente entiende lo mismo por los requisitos?

(Sí) (9.a) ¿Existe un proceso mediante el cual se determina esto?

[10] ¿Cómo validar los requisitos?

- Prototipos
- Análisis
- Simulaciones



**e) Factibilidad**  
**[Son requisitos factibles desde un punto de vista analítico?]**

- [11] ¿Hay algún requisito que son técnicamente difíciles de implementar?  
(Sí) (11.a) ¿Qué son?  
(Sí) (11.b) ¿Por qué son difíciles de implementar?  
(No) (11.c) ¿Se realizan estudios de viabilidad de estos requisitos?  
(Sí) (11.C.1) ¿Qué tan seguro está usted de las hipótesis formuladas en el estudio?

**f) Precedente**  
**[¿Los requisitos especifican algo nunca hecho antes, o que su empresa no ha hecho antes?]**

- [12] ¿Hay algún requisito que requiere nueva tecnología/ herramienta/técnica?  
• Tecnologías  
• Métodos  
• Idiomas  
• Hardware  
(No) (12.a) ¿Alguno de ellos algo nuevo para usted?  
(Sí) (12.b) ¿El programa tiene los conocimientos suficientes en estas áreas?  
(No) (12.B.1) ¿Existe un plan para la adquisición de conocimiento en estas áreas?

**g) Escala**  
**[¿Los requisitos especifican un producto más grande, más complejo, o que requieren una organización más grande que en la experiencia de la compañía?]**

- [13] ¿Es el tamaño del sistema y la complejidad es un problema?  
(No) (13.a) ¿Has hecho algo de este tamaño y complejidad antes?  
  
[14] ¿El tamaño requiere de una organización más grande de lo habitual para su empresa?

**2. Diseño**

**a) Funcionalidad**  
**[¿Existen problemas potenciales en el cumplimiento de los requisitos de funcionalidad?]**

- [15] ¿Existen algoritmos específicos que pueden no satisfacer los requisitos?  
(No) (15.a) ¿Alguno de los algoritmos o diseños marginal con respecto a la reunión requisitos?  
  
[16] ¿Cómo se determina la viabilidad de los algoritmos y los diseños?  
• Prototipos  
• Modelado  
• Análisis  
• Simulación

**b) Dificultad**  
**[¿El diseño y / o implementación será difícil de lograr?]**

- [17] ¿Algún diseño dependen de suposiciones poco realistas u optimistas?  
  
[18] ¿Hay algún requisito o funciones que son difíciles de diseñar?  
(No) (18.a) ¿Tiene soluciones para todas las necesidades?  
(Sí) (18.b) ¿Cuáles son los requisitos?



-¿Por qué son difíciles?

**c) Interfaces (espacio- comunicaciones)**

**[¿Están las interfaces internas (hardware y software) bien definidas y controladas?]**

[19] ¿Son las interfaces internas bien definidas?

- Software-software
- Software-al hardware

[20] ¿Existe un proceso para definir las interfaces internas?

(Sí) (20.a) ¿Existe un proceso de control de cambios para las interfaces internas?

[21] ¿Es el hardware que se desarrollan en paralelo con el software?

(Sí) (21.a) ¿Están cambiando las especificaciones de hardware?

(Sí) (21.b) ¿Se han definido todas las interfaces con software?

**d) Rendimiento**

**[¿Hay tiempo de respuesta estricta o requisitos de rendimiento?]**

[22] ¿Hay algún problema con el rendimiento?

- Rendimiento
- Asincrónicos Programación eventos en tiempo real
- Respuesta en tiempo real
- Líneas de tiempo de recuperación
- Tiempo de respuesta
- Base de datos de respuesta, contención, tratamiento o acceso.

[23] ¿Se ha hecho un análisis del rendimiento?

(Sí) (23.a) ¿Cuál es su nivel de confianza en el análisis del rendimiento?

(Sí) (23.b) ¿Tiene usted un modelo a seguir el rendimiento a través del diseño e implementación?

**e) Capacidad de Probarse**

**[¿El producto es difícil o imposible probar?]**

[24] ¿El software va a ser fácil de probar?

[25] ¿El diseño incluye características para ayudar a las pruebas?

[26] ¿No se involucran en el análisis de los requisitos a los probadores?

**f) Las limitaciones de hardware**

**[¿Existen fuertes restricciones en el hardware de destino?]**

[27] ¿Limita el hardware de su capacidad para cumplir con los requisitos?

- Arquitectura
- Capacidad de la memoria
- Rendimiento
- Respuesta en tiempo real
- Tiempo de respuesta
- Líneas de tiempo de recuperación
- El rendimiento de base de datos
- Funcionalidad
- Confiabilidad
- Disponibilidad



**g) Software no desarrollado**

**[¿Hay problemas con el software utilizado en el programa pero no desarrollado por el programa?]**

**Si re-usada o existe software rediseñado**

[28] ¿Está reutilizando software no desarrollado en el programa?

(Sí) (28.a) ¿Prevé usted algún problema?

- Documentación
- Rendimiento
- Funcionalidad
- Entrega oportuna
- Personalización

**Si se está utilizando el software COTS**

[29] ¿Hay algún problema con el uso de COTS (off-the-shelf comercial) de software?

- Documentación insuficiente para determinar las interfaces, el tamaño o el rendimiento
- Bajo rendimiento
- Requiere una gran parte de la memoria de almacenamiento o base de datos
- Dificultad para interactuar con el software de aplicación
- No se ha probado a fondo
- No es libre de errores
- No mantenimiento adecuado
- Respuesta lenta vendedor

[30] ¿Prevé usted algún problema con la integración de las actualizaciones de software COTS o revisiones?

Nota: Un tipo de software no desarrollado que es suministrado por fuentes comerciales

**3. Código y Prueba Unitaria**

**a) Factibilidad**

**[¿La implementación del diseño es difícil o imposible?]**

[31] ¿Alguna de las partes de la aplicación del producto no está completamente definido por el diseño, especificaciones?

[32] ¿Son los algoritmos y diseños seleccionados fácil de implementar?

**b) Pruebas**

**[¿Son el nivel y la hora especificada para las pruebas unitarias adecuadas?]**

[33] ¿Comienzan las pruebas de unidad antes de comprobar el código en relación con el diseño?

[34] ¿Se ha especificado la unidad de pruebas suficientes?

[35] ¿Hay tiempo suficiente para realizar todas las pruebas de unidad que usted piensa se debe hacer?

[36] ¿Se hará compromisos con respecto a si hay problemas de horario de pruebas unitarias?



**c) Codificación / Implementación**

**[¿Hay algún problema con la codificación y la aplicación?]**

- [37] ¿Son las especificaciones de diseño con detalles suficientes para escribir el código?
- [38] ¿El diseño cambia mientras que la codificación se está haciendo?
- [39] ¿Existen restricciones del sistema que hacen que el código sea difícil de escribir?
- Momento
  - Memoria
  - Almacenamiento externo
- [40] ¿Es el lenguaje de programación adecuado para producir el software en este proyecto?
- [41] ¿Existen múltiples lenguajes de programación que se utilizan en el programa?  
(Sí) (41.a) ¿Existe compatibilidad de interfaz entre el código producido por el diferentes compiladores?
- [42] ¿Es el equipo de desarrollo lo mismo que el equipo de destino?  
(No) (42.a) ¿Existen diferencias compilador entre los dos?

**Si se está utilizando hardware de desarrollo**

- [43] ¿Son las especificaciones de hardware adecuada para codificar el software?
- [44] ¿Las especificaciones de hardware cambian mientras se está escribiendo el código?

**4. Integración y Prueba**

**a) Medio ambiente / Entorno**

**[¿El entorno de integración y prueba es adecuada?]**

- [45] ¿Habrá hardware suficiente para hacer la integración y las pruebas adecuadas?
- [46] ¿Hay algún problema con el desarrollo de escenarios realistas y datos de ensayos para demostrar algún requisito?
- El tráfico de datos especificado
  - Respuesta en tiempo real
  - Tratamiento de eventos asíncronos
  - Interacción multiusuario
- [47] ¿Es capaz de verificar el rendimiento en sus instalaciones?
- [48] ¿instrumentación de hardware y software facilita las pruebas?  
(Sí) (48.a) ¿Es suficiente para todas las pruebas?

**b) Producto**

**[¿Es la definición de la interfaz adecuada, instalaciones inadecuadas, falta de tiempo?]**

- [49] ¿El hardware de destino estén disponibles cuando sea necesario?
- [50] ¿Se han acordado los criterios de aceptación para para todas las necesidades?  
(Sí) (50.a) ¿Existe un acuerdo formal?
- [51] ¿Son las interfaces externas definidos, documentados?



[52] ¿Hay algún requisito que serán difíciles de probar?

[53] ¿Se ha especificado que integración del producto es suficiente?

[54] ¿Se ha asignado un tiempo adecuado para la integración de productos y la prueba?

**Si COTS**

[55] ¿Datos del proveedor serán aceptados en la verificación de los requisitos asignados a COTS productos?

(Sí) (55 a) ¿Es claro en el contrato?

**c) Sistema**

**[¿La integración de sistemas descoordinados, definición de interfaz pobre, o instalaciones inadecuadas?]**

[56] ¿Se ha especificado suficiente integración de sistemas?

[57] ¿Se ha asignado un tiempo adecuado para la integración de sistemas y la prueba?

[58] ¿Son todos los miembros del proyecto parte del equipo de la integración?

[59] ¿El producto puede integrar en un sistema existente?

(Sí) (59.a) ¿Hay un período de corte y cambio paralelo con el sistema existente?

(No) (59.a.1) ¿Cómo va a garantizar que el producto funcionará correctamente cuando se integrado?

[60] ¿La integración del sistema se producirá en el sitio del cliente?

**5. Ingeniería Especialidades**

**a) Mantenibilidad**

**[Será la implementación de difícil comprensión o mantener?]**

[61] ¿La arquitectura, el diseño o código crean las dificultades de mantenimiento?

[62] ¿Son la gente de mantenimiento involucrados temprano en el diseño?

[63] ¿Es la documentación del producto adecuado para el mantenimiento por una organización externa?

**b) Confiabilidad**

**[¿Los requisitos difíciles de cumplir fiabilidad o disponibilidad?]**

[64] ¿Son requisitos de confiabilidad asignado al software?

[65] ¿Son los requisitos de disponibilidad asignados al software?

(Sí) (65.a) ¿Son los plazos de recuperación de cualquier problema?

**c) Seguridad**

**[¿Son los requisitos de seguridad no factibles y no demostrables?]**

[66] ¿Son los requisitos de seguridad asignados al software?

(Sí) (66.a) ¿Ve usted alguna dificultad para cumplir los requisitos de seguridad?

[67] ¿Será difícil para verificar la satisfacción de los requisitos de seguridad?



**d) Seguridad**

**[¿Son los requisitos de seguridad más estrictos que el estado actual de la práctica o programa experimentar?]**

[68] ¿Existen requisitos de seguridad sin precedentes (nuevo) o de tecnología avanzada?

[69] ¿Es un sistema de Orange Book?

**Nota:** Orange Book - Un estándar de seguridad establecido por el Gobierno de Estados Unidos

[70] ¿Ha implementado este nivel de seguridad antes?

**e) Factores Humanos**

**[¿El sistema será difícil de utilizar debido a la mala definición de interfaz humana?]**

[71] ¿Ves alguna dificultad en el cumplimiento de los requisitos relativos a factores humanos?

(No) (71.a) ¿Cómo garantizarán que se encontrará con la interfaz humana requerida?

**Si la creación de prototipos**

(Sí) (71.a.1) ¿Es un prototipo de usar y tirar?

(No) (71.a.1a) ¿Está usted haciendo desarrollo evolutivo?

(Sí) (71.a.1a.1) ¿Tiene experiencia en este tipo de desarrollo?

(Sí) (71.a.1a.2) ¿Puedan entregarse las versiones provisionales?

(Sí) (71.a.1a.3) ¿Esta el control de cambios complicarte?

**f) Especificaciones**

**[¿Es la documentación adecuada para diseñar, implementar y probar el sistema?]**

[72] ¿Es la especificación de requisitos de software adecuado para diseñar el sistema?

[73] ¿Son las especificaciones de hardware adecuada para diseñar e implementar el software?

[74] ¿Están los requisitos de interfaz externas bien definidas?

[75] ¿Son las especificaciones de prueba suficientes para probar completamente el sistema?

**Antes o en la fase de implementación**

[76] Son las especificaciones de diseño adecuado para implementar el sistema?

- Las interfaces internas

**B. Entorno de desarrollo**

**1. . Proceso de Desarrollo**

**a) Formalidad**

**[¿Será la implementación difícil comprensión o mantener?]**

[77] ¿Hay más de un modelo de desarrollo que se utiliza?

- Espiral
- Cascada
- Incremental

(Sí) (77.a) ¿La coordinación entre ellos es un problema?



[78] ¿Hay, planes controlados formales para todas las actividades de desarrollo?

- El análisis de requerimientos
- Diseño
- Código
- Integración y pruebas
- Instalación
- Seguro de calidad
- Gestión de la configuración

(Sí) (78.a) ¿Los planes especifican el proceso bien?

(Sí) (78.b) ¿Son los desarrolladores familiarizados con los planes?

**b) Idoneidad**

**[¿El proceso adecuado para el modelo de desarrollo, por ejemplo, espiral, prototipos?]**

[79] ¿Es el proceso de desarrollo adecuado de este producto?

[80] ¿El proceso de desarrollo tiene el apoyo de un conjunto compatible de procedimientos, métodos y herramientas?

**c) Control del Proceso**

**[¿Se hace respetar el proceso de desarrollo de software, supervisa y controla utilizando métricas? ¿Son sitios de desarrollo distribuidas coordinadas?]**

[81] ¿Todo el mundo sigue el proceso de desarrollo?

(Sí) (81.a) ¿Cómo se asegura esto?

[82] ¿Se puede medir si el proceso de desarrollo está cumpliendo con su productividad y objetivos de calidad?

**Si se distribuyen los sitios de desarrollo**

[83] ¿Existe una coordinación adecuada entre los sitios de desarrollo distribuidos?

**d) Familiaridad**

**[¿Los miembros del proyecto tienen experiencia en el uso del proceso? ¿El proceso es comprendido por todos miembros del personal?]**

[84] ¿La gente está cómoda con el proceso de desarrollo?

**e) Control de Productos**

**[¿Existen mecanismos para controlar los cambios en el producto?]**

[85] ¿Existe un mecanismo de trazabilidad de requisitos que rastrea los requisitos de la fuente especificación a través de casos de prueba?

[86] ¿Es el mecanismo de trazabilidad utilizado en la evaluación del impacto del cambio requerimiento análisis?

[87] ¿Existe un proceso formal de control de cambios?

(Sí) (87.a) ¿Cubre todos los cambios de requisitos en línea diseño, código, y documentación?

[88] ¿Son los cambios a cualquier nivel asignados hasta el nivel del sistema y abajo a través de la prueba nivel?

[89] ¿Existe un análisis adecuado cuando se añaden nuevos requisitos para el sistema?

[90] ¿Tiene una manera de seguir interfaces?



[91] ¿Son los planes de pruebas y procedimientos actualizados como parte del proceso de cambio?

## 2. Sistema de Desarrollo

### a) Capacidad

**[¿Hay suficiente potencia de la estación de trabajo de procesamiento, la memoria o la capacidad de almacenamiento?]**

[92] ¿Hay suficientes estaciones de trabajo y la capacidad de transformación para todo el personal?

[93] ¿Hay capacidad suficiente para las fases superpuestas, como la codificación, integración y pruebas?

### b) Idoneidad

**[¿Apoya el sistema de desarrollo de todas las fases, actividades y funciones?]**

[94] ¿Apoya el sistema de desarrollo de todos los aspectos del programa?

- El análisis de requerimientos
- Análisis de los resultados
- Diseño
- Codificación
- Prueba
- Documentación
- Gestión de la configuración
- Seguimiento de Gestión
- Requisitos de trazabilidad

### c) Usabilidad

**[¿Qué tan fácil es el sistema de desarrollo a utilizar?]**

[95] ¿La gente encuentra el sistema de desarrollo fácil de usar?

[96] ¿Existe una buena documentación del sistema de desarrollo?

### d) Familiaridad

**[¿Hay poca experiencia de la empresa o previa experiencia de los miembros del proyecto con el sistema de desarrollo?]**

[97] ¿La gente utilizaba estas herramientas y métodos antes?

### e) Confiabilidad

**[¿El sistema sufre de los errores de software, el tiempo de inactividad, insuficiente integrada de respaldo?]**

[98] ¿El sistema se considera confiable?

- Compilador
- Las herramientas de desarrollo
- Hardware

### f) Apoyo al sistema

**[¿Hay expertos a tiempo o el soporte del proveedor para el sistema?]**



[99] ¿Son las personas capacitadas en el uso de las herramientas de desarrollo?

[100] ¿Tiene acceso a expertos en el uso del sistema?

[101] ¿Responden proveedores a los problemas con rapidez?

**g) Entregas**

**[¿No se ha planificado la definición la aceptación para la entrega del sistema de desarrollo para el cliente?**

[102] ¿Entrega usted el sistema de desarrollo para el cliente?

(Sí) (102.a) ¿Se han asignado suficientes presupuesto, cronograma y recursos para este entregable?

**3. Proceso de Gestión**

**a) Planificación**

**[¿Es la planificación oportuna, conduce técnicas incluidas, planes de contingencia hace?]**

[103] ¿El programa está gestionado de acuerdo con el plan?

(Sí) (103.a) ¿Hace que la gente habitualmente se retira en su lucha contra los incendios?

[104] ¿Se hace volver a la planificación cuando se producen interrupciones?

[105] ¿La gente de todos los niveles están incluidos en la planificación su propio trabajo?

[106] ¿Hay planes de contingencia para los riesgos conocidos?

(Sí) (106.a) ¿Cómo se determina cuándo activar las contingencias?

[107] ¿En cuestiones de largo plazo están abordando de manera adecuada?

**b) Organización del proyecto**

**[¿Son los roles y relaciones de reporte claras?]**

[108] ¿Es la organización eficaz de los programas?

[109] ¿La gente entiende sus roles y los roles de los demás en el programa?

[110] ¿La gente sabe quién tiene la autoridad- para qué?

**c) Gestión de la Experiencia**

**[¿Los gerentes con experiencia en desarrollo de software, gestión de software, la aplicación dominio, el proceso de desarrollo, o en programas de gran tamaño?]**

[111] ¿Los directivos tienen experiencia?

- Gestión de Software
- El desarrollo de software
- Con este proceso de desarrollo
- En el dominio de la aplicación
- El tamaño o la complejidad del programa

**d) Interfaces Programa**

**[¿Hay mala interacción con los clientes, otros contratistas, directivos y / o compañeros?]**

[112] ¿La gerencia comunica los problemas de arriba y abajo de la línea?



[113] ¿En los conflictos con el cliente se resuelve manera oportuna?

[114] ¿Existe la gestión de los miembros del programa adecuados en las reuniones con el cliente?

- Los líderes técnicos
- Desarrolladores
- Analistas

[115] ¿Funciona la administración para asegurar que todas las facciones de los clientes están representados en decisiones con respecto a la funcionalidad y operación?

[116] ¿Es una buena política para presentar un panorama optimista para el cliente o la alta gerencia?

#### 4. Métodos de Gestión

##### a) Monitoreo

**[¿Están definidos los parámetros de gestión y el avance del desarrollo rastreado?]**

[117] ¿Existen informes periódicos de estado estructurados?

(Sí) (117.a) ¿Las personas tienen una respuesta a sus informes sobre la situación?

[118] ¿Tiene la información adecuada son reportados a los niveles de organización adecuados?

[119] ¿El seguimiento del progreso va contra el plan?

(Sí) (119.a) ¿La gerencia tiene una idea clara de lo que está pasando?

##### b) Administración de Personal

**[¿Está el personal de proyectos entrenados y usados apropiadamente?]**

[120] ¿La gente se entrenó en las habilidades requeridas para este programa?

(Sí) (120.a) ¿Es esto parte del plan del programa?

[121] ¿La gente se asignó al programa que no coincide con el perfil de experiencia para su área de trabajo?

[122] ¿Es fácil para los miembros del programa obtener una acción de gestión?

[123] ¿Los miembros del programa sabe el estado de todos los niveles sobre frente al plan?

[124] ¿Siente que la gente es importante para mantener el plan?

[125] ¿Consulta de gestión con la gente antes de tomar decisiones que afectan a su trabajo?

[126] ¿Existe la gestión de los miembros del programa adecuados en las reuniones con el cliente?

- Los líderes técnicos
- Desarrolladores
- Analistas

##### c) Seguro de calidad

**[¿Existen procedimientos y recursos adecuados para asegurar la calidad de los productos?]**

[127] ¿Es la función de garantía de la calidad del software personal adecuado para este programa?

[128] ¿Se han definido los mecanismos para garantizar la calidad?



- (Sí) (128.a) ¿Todas las áreas y fases tienen procedimientos de calidad?  
(Sí) (128.b) ¿La gente está acostumbrada a trabajar con estos procedimientos?

**d) Gestión de la Configuración**  
**[¿Son los procedimientos de cambio o control de versiones, incluyendo lugar de instalación (s), adecuados?]**

- [129] ¿Tiene un sistema de gestión de la configuración adecuada?  
[130] ¿Es la función de gestión de la configuración el personal adecuado?  
[131] ¿Es necesaria la coordinación con un sistema instalado?  
(Sí) (131.a) ¿Existe una adecuada gestión de la configuración del sistema instalado?  
(Sí) (131.b) ¿El sistema de gestión de la configuración sincronizar su trabajo con cambios en el sitio?  
[132] ¿Va a instalar en varios sitios?  
(Sí) (132.a) ¿Proporciona el sistema de gestión de la configuración para múltiples sitios?

**5. Medio Ambiente de Trabajo**

**a) Actitud de Calidad**  
**[¿Hay una falta de orientación hacia la calidad del trabajo?]**

- [133] ¿En todos los niveles del personal está orientado hacia los procedimientos de calidad?  
[134] ¿El horario se interpone en el camino de la calidad?

**b) Cooperación**  
**[¿Hay una falta de espíritu de equipo? ¿Tiene solución de conflictos que requiere la intervención de gestión?]**

- [135] ¿La gente trabaja de forma cooperativa a través de fronteras funcionales?  
[136] ¿La gente funciona de manera efectiva para lograr metas comunes?  
[137] ¿es la intervención de gestión a veces necesaria para que la gente a trabajar juntos?

**c) Comunicación**  
**[¿Hay poca conciencia de la misión o metas, la falta de comunicación de la información técnica entre compañeros y directivos?]**

- [138] ¿Hay una buena comunicación entre los miembros del programa?  
• Gerentes  
• Los líderes técnicos  
• Desarrolladores  
• Testers  
• Gestión de la configuración  
• Seguro de calidad  
[139] ¿Los gerentes son receptivos a la comunicación del personal del programa?  
(Sí) (139.a) ¿Se siente libre de pedir a sus directivos en busca de ayuda?  
(Sí) (139.b) ¿Los miembros del programa que puedan aumentar los riesgos sin tener una solución en la mano?  
[140] ¿Los miembros del programa puede obtener la oportuna notificación de eventos que puedan afectar a su trabajo?



(Sí) (140.a) ¿Es este formal o informal?

**d) Moral**

**[¿Hay un ambiente no productivo, no creativa? ¿Las personas sienten que no hay un reconocimiento o recompensa por un trabajo superior?]**

[141] ¿Cómo es la moral en el programa?

(No) (141.a) ¿Cuál es el principal factor que contribuye a la baja moral?

[142] ¿Hay algún problema de mantenimiento de las personas que usted necesita?

**C. RESTRICCIONES DEL PROGRAMA**

**1. Recursos**

**a) Cronograma**

**[¿Es el cronograma inadecuado o inestable?]**

[143] ¿El programa se ha mantenido estable?

[144] ¿El cronograma realista?

(Sí) (144.a) ¿El método de cálculo basado en datos históricos?

(Sí) (144.b) ¿El método funcionó bien en el pasado?

[145] ¿Hay algo que no fue planeado horario adecuado?

- Análisis y estudios
- Capacitación
- Los cursos de mantenimiento y capacitación
- Bienes de equipo
- Sistema de desarrollo Entregable

[146] ¿Hay dependencias externas que puedan afectar a la programación?

**b) Personal**

**[¿El personal inexperto, carente de conocimiento del dominio, a falta de habilidades, o faltos?]**

[147] ¿Hay algún área en la que las habilidades técnicas requeridas faltan?

- La ingeniería de software y los requisitos de procedimiento de análisis
- Experiencia Algoritmo
- Diseño y métodos de diseño
- Lenguajes de programación
- Los métodos de integración y pruebas
- Confiabilidad
- Mantenibilidad
- Disponibilidad
- Factores Humanos
- Gestión de la configuración
- Seguro de calidad
- Entorno de Target
- Nivel de seguridad
- Sistema operativo
- Base de datos
- Dominio de aplicación
- Análisis de los resultados



- Las aplicaciones de tiempo crítico

- [148] ¿Tiene el personal adecuado al programa?
- [149] ¿Es estable la dotación de personal?
- [150] ¿Tiene acceso a las personas adecuadas cuando los necesitas?
- [151] ¿Los miembros del programa han implementado sistemas de este tipo?
- [152] ¿es el programa dependiente de pocas personas clave?
- [153] ¿Hay algún problema que falta ser aclarado a la gente?

**c) Presupuesto**

**[¿Es la financiación insuficiente o inestable?]**

- [154] ¿Es el presupuesto estable?
- [155] ¿Es el presupuesto sobre la base de una estimación realista?  
(Sí) (155.a) ¿El método de cálculo basado en datos históricos?  
(Sí) (155.b) ¿El método funcionó bien en el pasado?
- [156] ¿tienen características o funciones que han sido eliminadas como parte de un esfuerzo de diseño a costo?
- [157] ¿Hay algo que no se asignó presupuesto adecuado?
- Análisis y estudios
  - Capacitación
  - Cursos de Mantenimiento
  - Bienes de equipo
  - Sistema de desarrollo Entregable
- [158] ¿Los acompañan los cambios de requisitos en el presupuesto?  
(Sí) (158.a) ¿Es esto una parte estándar del proceso de control de cambios?

**d) Comodidades**

**[Son las instalaciones adecuadas para la construcción y entrega del producto?]**

- [159] ¿Son las instalaciones para el desarrollo adecuado?
- [160] ¿El entorno de integración adecuada?

**2. Contrato**

**a) Tipo de contrato**

**[¿El contrato tipo es una fuente de riesgo para el programa?]**

- [161] ¿Qué tipo de contrato tiene usted? (Costo gasto premio, precio fijo,....)  
(161a) ¿Presenta esto algún problema?
- [162] ¿El contrato oneroso en cualquier aspecto del programa?
- Declaración de trabajo (Declaración de Trabajo)
  - Especificaciones
  - DID (Descripciones de datos del artículo)
  - Las partes del contrato
  - La implicación del cliente excesiva
- [163] ¿La documentación requerida es costoso?



- Cantidad excesiva
- Ciclo de aprobación largo

**b) Restricciones**

**[¿El contrato causar alguna restricción?]**

[164] ¿Hay problemas con los derechos de datos?

- El software COTS
- Software de Desarrollo
- Las partidas no de desarrollo

**c) Dependencias**

**[¿El programa tiene alguna dependencia en los productos o servicios fuera?]**

[165] ¿Hay dependencias de los productos o servicios que puedan afectar el producto externo, presupuesto o calendario?

- Contratistas Asociados
- Primer contratista
- Subcontratistas
- Los vendedores o proveedores
- Equipo suministrado al cliente o software

**3. Interfaces Programa**

**a) Cliente**

**[¿Existen problemas de los clientes, tales como: largo ciclo de documentos de homologación, la mala la comunicación y el dominio insuficiente experiencia?]**

[166] ¿es el ciclo de aprobación de los clientes a tiempo?

- Documentación
- Revisiones del programa
- Revisiones formales

[167] ¿Alguna vez se avanza antes de recibir la aprobación del cliente?

[168] ¿El cliente entiende los aspectos técnicos del sistema?

[169] ¿El cliente entiende software?

[170] ¿Interfiere el cliente a los procesos o las personas?

[171] ¿Funciona la gestión con el cliente para llegar a decisiones mutuamente aceptables de manera oportuna?

- Requisitos de la comprensión
- Criterios de prueba
- Ajustes Calendario
- Interfaces

[172] ¿Qué tan efectivas son sus mecanismos para llegar a acuerdos con el cliente?

- Grupos de trabajo (pactadas?)
- Las reuniones de intercambio técnico (pactadas?)

[173] ¿Son todas las facciones de los clientes implicados en alcanzar acuerdos?

(Sí) (173.a) ¿Es un proceso formalmente definido?

[174] ¿La administración presentan un cuadro realista u optimista para el cliente?



**Si hay contratistas asociados**

**b) Contratistas Asociados**

**[¿Hay problemas con los contratistas asociados, como inadecuadamente definidos o inestable interfaces, la falta de comunicación, falta de cooperación?]**

[175] ¿En las interfaces externas cambiando sin notificación adecuada, coordinación o procedimientos formales de cambio?

[176] ¿Hay un plan de transición adecuado?

(Sí) (176.a) ¿Tiene el apoyo de todos los contratistas y personal de la obra?

[177] ¿Hay algún problema con la obtención de horarios o datos de la interfaz de socio contratistas?

(No) (177.a) ¿Son exactas?

**Si hay subcontratistas**

**c) Subcontratistas**

**[¿El programa depende de subcontratistas para las áreas críticas?]**

[178] ¿Hay ambigüedades en las definiciones de tareas subcontratadas?

[179] ¿Es el reporte subcontratista y procedimiento de control diferente del programa de requisitos de presentación de informes?

[180] ¿Es la administración subcontratista y gestión técnica realizado por un independiente organización?

[181] ¿Está muy dependiente de la experiencia subcontratista en cualquier área?

[182] ¿Es el conocimiento subcontratista de ser trasladado a la empresa?

[183] ¿Hay algún problema con la obtención de horarios o datos de la interfaz de los subcontratistas?

**Si el programa es un subcontrato**

**d) Contratista Principal**

**[¿El programa enfrenta dificultades con su primer contratista?]**

[184] ¿En sus definiciones de tareas es ambigua?

[185] ¿Se realiza la interfaz con dos organizaciones principales separados para la administración y técnico gestión?

[186] ¿Está altamente dependiente del Primer nivel de experiencia en todas las áreas?

[187] ¿Hay algún problema con la obtención de horarios o datos de la interfaz del primer nivel?

**e) Gestión de la empresa**

**[¿Hay una falta de apoyo o micro gestión de la alta dirección?]**



[188] ¿La administración del programa comunica sus problemas a la administración superior?  
(Sí) (188.a) ¿Le parece que sea eficaz?

[189] ¿La gerencia corporativa da apoyo oportuno en la solución de sus problemas?

[190] ¿La gerencia corporativa tienden a micro-gestión?

[191] ¿La administración presentan un cuadro realista u optimista a la alta gerencia?

**f) Los Proveedores**

**[¿Son los Proveedores responden a las necesidades del programa/proyecto?]**

[192] ¿Está confiando en los proveedores para la entrega de los componentes críticos?

- Los compiladores
- Hardware
- COTS

**g) Política**

**[¿La política es debida un problema para el programa?]**

[193] ¿La política que afectan al programa?

- Empresa
- Cliente
- Contratistas Asociados
- Subcontratistas

[194] ¿La política en que afectan a las decisiones técnicas?



## **Anexo 5 - Plan de Contingencia de Equipos de Cómputo y software para Iquitos Play.**

Actualmente la Empresa IquitosPlay no cuenta con un plan de contingencia informático. Haciendo que los riesgos referidos a los equipos de cómputos y software que utilizan afecten el desarrollo de los proyectos de la empresa; por tal motivo se ha decidido incluir el presente plan de contingencia.

### **Plan de Contingencia para los Equipos de Cómputo y Software**

#### **Definición de eventos susceptibles de contingencia**

El Plan de Contingencia abarca todos los aspectos que forman parte de los equipos informáticos de IquitosPlay, en tal sentido, resulta de vital importancia considerar todos los elementos susceptibles de provocar eventos que conlleven a activar la contingencia. Los principales elementos, que serán considerados para su evaluación:

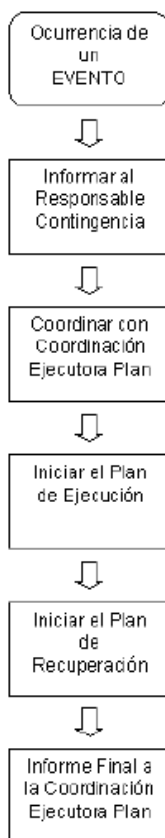
#### Hardware

- ✓ Estaciones de trabajo( laptops y PC´s)
- ✓ Equipos multimedia

#### Software

- ✓ Software de Base de Datos
- ✓ Aplicativos utilizados por IquitosPlay.
- ✓ Software Base (Sistemas operativos y Ofimática).

Proceso de la Aplicación del plan de contingencia.





## Desarrollo de las actividades

### Contingencias relacionadas a los sistemas de información

#### Objetivo:

Los planes de contingencia de los eventos relacionados a los Sistemas de Información tienen por objetivo que ante cualquier evento que atente contra la normal operación tanto en hardware, software como en cualquier elemento interno o externo relacionado a los mismos, se dispongan de alternativas de solución frente al problema a fin de asegurar la operación del servicio y/o minimizar el tiempo de interrupción.

#### ❖ Evento: Infección de Equipos por virus.

### 1. PLAN DE PREVENCIÓN

**a. Descripción del evento:** Virus informático es un programa de software que se propaga de un equipo a otro y que interfiere el funcionamiento del equipo. Además, Un virus informático puede dañar o eliminar los datos de un equipo.

Este evento incluye los siguientes elementos mínimos identificados, los mismos que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, los cuales se muestran a continuación:

#### Hardware

- Estaciones de Trabajo

#### Software

- Software Base
- Aplicativos utilizados por el IquitosPlay

### Condiciones de Prevención de Riesgo

- ✓ Establecimiento de políticas de seguridad para prevenir el uso de aplicaciones no autorizadas en las estaciones de trabajo.
- ✓ Restringir el acceso a Internet a las estaciones de trabajo que por su uso no lo requieran.
- ✓ Eliminación de disketteras, quemadores de CD, etc. en estaciones de trabajo que no lo requieran.
- ✓ Deshabilitar los puertos de comunicación USB en las estaciones de trabajo que no los requieran habilitados, para prevenir la conexión de unidades de almacenamiento externo.
- ✓ Aplicar filtros para restricción de correo entrante, y revisión de archivos adjuntos en los correos y así prevenir la infección de los terminales de trabajo por virus.
- ✓ Contar con antivirus instalados en cada estación de trabajo, el mismo que debe estar actualizado permanentemente.
- ✓ Contar con equipos de respaldo ante posibles fallas de las estaciones, para su reemplazo provisional hasta su desinfección y habilitación.

### 2. PLAN DE EJECUCIÓN

#### Eventos que activan la Contingencia

- Mensajes de error durante la ejecución de programas.
- Lentitud en el acceso a las aplicaciones.
- Falla general en el equipo (sistema operativo, aplicaciones).



### Descripción de las Actividades después de activar la contingencia

- Desconectar la estación infectada de la red de IquitosPlay.
- Verificar si el equipo se encuentra infectado, utilizando un detector de virus actualizado.
- Rastrear de ser necesario el origen de la infección (archivo infectado, correo electrónico, etc.)
- Eliminar el agente causante de la infección.
- Remover el virus del sistema.
- Probar el sistema.
- En caso no solucionarse el problema :
  - Formatear el equipo
  - Personalizar la estación para el usuario
- Conectar la estación a la red de IquitosPlay .
- Efectuar las pruebas necesarias con el usuario.
- Solicitar conformidad del servicio.

#### ❖ Evento: Perdida de Sistemas

### 1. PLAN DE PREVENCIÓN

Este evento incluye los siguientes elementos mínimos identificados por IquitosPlay, que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia, como se muestran a continuación:

#### Software

- Software base
- Software base de datos
- Aplicativos utilizados por el Hardware

#### Información

- Respaldo de base de datos
- Respaldo de las aplicaciones utilizadas por IquitosPlay
- Respaldo De Software Base

### Condiciones de Prevención de Riesgo

Tomar las siguientes acciones preventivas que debe implementar asegurar el servicio de las aplicaciones:

- ✓ Contar con equipos de respaldo ante posibles fallas de los equipos.
- ✓ Contar con mantenimiento preventivo para dichos equipos.
- ✓ Contar con los backups de información necesarios para restablecer las aplicaciones Anexo A04  Copias de Respaldo.
- ✓ Contar con backups de las aplicaciones y de las bases de datos Anexo



## 2. PLAN DE EJECUCIÓN

Eventos que activan la Contingencia

- Falla de Acceso a Aplicaciones.
- Mensaje Pérdida de Conexión a La BD.

Descripción de Las Actividades Después de Activar La Contingencia

Remitirse a los Procedimientos de recuperación de sistemas:

El encargado de Informática, luego de verificar la corrección del problema de acceso a los servidores, coordinará con los demás miembros para la reanudación de los trabajos operativos con las aplicaciones de IquitosPlay.

### ❖ Evento: Falla del Sistema Operativo.

Falla en el control de computadoras, en el interfaz hombre-máquina, recursos hardware y software. Este evento incluye los siguientes elementos mínimos identificados, que por su naturaleza pueden ser considerados como parte afectada o causa de la contingencia:

#### Software

- Aplicativos utilizados por IquitosPlay

#### Hardware

- Pc's

#### Información

- Respaldo de Base de Datos
- Respaldo de las Aplicaciones utilizadas por IquitosPlay

## 1. PLAN DE PREVENCIÓN

### Condiciones de Prevención de Riesgo

Se debe asegurar de cubrir los siguientes aspectos:

Contar con los backups diarios de datos de las aplicaciones en producción en la institución  
Contar con servicios de soporte vigentes para los principales causantes del evento:

- El IMARPE debe asegurarse de mantener acuerdos con sus Proveedores de Servicio.
- Estaciones de trabajo deberán contar con antivirus actualizados.

## 2. PLAN DE EJECUCIÓN

### Eventos que activan la Contingencia

Detención de las funciones de trabajo en estaciones de trabajo.

- Identificación de falla en el monitor de estaciones de trabajo.

### Descripción de Las Actividades Después de Activar La Contingencia

- ✓ Proceder a la revisión de los Equipos de trabajo para determinar la causa de la falla.
- ✓ Verificar si el equipo se encuentra infectado, utilizando un detector de virus actualizado.
- ✓ Rastrear de ser necesario el origen de la infección (archivo infectado, correo electrónico, etc.)
- ✓ Remover el virus del sistema.
- ✓ Probar el sistema.

En caso no solucionarse el problema:

- Formatear el equipo
- Personalizar el equipo para el usuario
- ✓ Efectuar las pruebas necesarias con el usuario.
- ✓ Solicitar conformidad del servicio.

**Anexo 6 - Planes de respuesta a los riesgos – Caso de estudio.**

Nro. Ref. Riesgo	Estrategia	Actividades
1	Aceptar	Se realiza reunión diaria durante 2 días seguidos con el nuevo cliente de alta gerencia, debido a que él es el encargado de proporcionar los requisitos. Durante las reuniones, el encargado del proyecto dará a conocer los requisitos ya planteados por la anterior gerencia, así mismo el avance del proyecto.
2	Mitigar	<ol style="list-style-type: none"><li>1. Se verifica si hay personal de IquitosPlay que se encuentre disponible para incorporar al proyecto.</li><li>2. Durante 01 día, se dará a conocer los alcances del proyecto al nuevo miembro del proyecto.</li></ol> <b>En caso de no haber personal disponible</b> <ol style="list-style-type: none"><li>3. Se sigo el procedimiento de contrato de la empresa.</li></ol>
3	Mitigar-Aceptar	<ol style="list-style-type: none"><li>1. Realizar Entrevistas para obtener Requerimientos estables <b>Si los Nuevos Requerimientos aparecen</b></li><li>2. Se verifica el contrato del proyecto, para ver las consideraciones de los nuevos requisitos.</li><li>3. Se desarrolla el planteamiento de nuevos requerimientos para medir el impacto en el proyecto, producto y realizar negociaciones con el cliente.</li></ol>
4	Mitigar	<ol style="list-style-type: none"><li>1. Se detallará la toma de requerimientos</li><li>2. Se revisará el estimado del tiempo previsto inicialmente en el cronograma versus la estimación resultante del análisis.</li><li>3. En caso de haber una discrepancia se negociará con el cliente.</li></ol> <p>Nota: Debido a que se identificó este riesgo de manera proactiva, ya se han iniciado las conversaciones de antemano y se ha tomado en cuenta ésta posibilidad como una enmienda al contrato. Se han agregado las tareas en el cronograma para llevar a cabo dicho plan.</p>
5	Mitigar	En el cronograma se incluye 01 día, al inicio del desarrollo del proyecto, para sensibilizar al cliente, se explica el alcance del proyecto, y la vital importancia de la participación del cliente durante el desarrollo del proyecto.
6	Mitigar	Considerando que se está utilizando la metodología XP, se incluye en el cronograma reuniones semanales con los clientes, de esta manera el cliente estará más informado del avanza del proyecto, y mayor retroalimentación.
7	Mitigar	Desarrollar un plan de formación y capacitación de personal, el plan tendrá un máximo de 1 semana. En el plan se debe dar a conocer las herramientas que se utilizan, la metodología, la programación ,etc.
8	Eliminar	Se incluye al cronograma 01 semana para capacitación e investigación acerca de la nueva herramienta a utilizar.
9	Aceptar	<ol style="list-style-type: none"><li>1. Gestionar por parte del equipo de diseño, el planteamiento de nuevos requerimientos para medir el impacto en el proyecto.</li><li>2. Se verifica el contrato del proyecto, para ver las consideraciones de los nuevos requisitos.</li><li>3. Se realiza las negociaciones con el cliente.</li></ol>



10	Mitigar-Aceptar	<ol style="list-style-type: none"><li>1. Realizar Entrevistas para obtener Requerimientos estables <b>Si los Nuevos Requerimientos aparecen</b></li><li>2. Se verifica el contrato del proyecto, para ver las consideraciones de los nuevos requisitos.</li><li>3. Se desarrolla el planteamiento de nuevos requerimientos para medir el impacto en el proyecto, producto y realizar negociaciones con el cliente.</li></ol>
11	Mitigar	<p>En el cronograma se incluye las pruebas unitarias y las pruebas de integración.</p> <ul style="list-style-type: none"><li>➤ Para las pruebas unitarias se utiliza <b>NUnit</b>: Versión del framework para la plataforma.NET.</li><li>➤ En la prueba de integración, los módulos individuales de software son combinados y testeados como un grupo. Son las pruebas posteriores a las pruebas unitarias y preceden el testeado de sistema.</li></ul>
12	Explotar	<p>Cuando se termina la captura de requisitos se realiza la técnica de flujos de comunicación y respuesta de componentes para mejorar funcionalidades o encontrar posibles nuevos requisitos, de encontrar nuevos requisitos se procede a plantear dichos requisitos al cliente.</p>
13	Mitigar	<p>Considerando que se está utilizando la metodología XP, se incluye en el cronograma reuniones semanales con los clientes, de esta manera el cliente estará más informado del avanza del proyecto, y mayor retroalimentación</p>
14	Mitigar	<p>Se incluyen pruebas:</p> <ol style="list-style-type: none"><li>1. <b>Función:</b> Pruebas fijando su atención en la validación de las funciones, métodos, servicios, caso de uso.</li><li>2. <b>Seguridad:</b> Asegurar que los datos o el sistema solamente es accedido por los actores deseados.</li><li>3. <b>Volumen:</b> Enfocada en verificando las habilidades de los programas para manejar grandes cantidades de datos, tanto como entrada, salida o residente en la BD.</li></ol>
15	Mitigar	<p>Se debe aplicar sanción y descuentos a los trabajadores que no cumplan con lo planificado.</p> <ol style="list-style-type: none"><li>1. Se verifica si hay personal de IquitosPlay que se encuentre disponible para incorporar al proyecto.</li><li>2. Durante 01 día, se dará a conocer los alcances del proyecto al nuevo miembro del proyecto.</li></ol> <p><b>En caso de no haber personal disponible</b> Se siga el procedimiento de contrato de la empresa.</p>
16	Transferir	<p>Se aclarará este riesgo con el cliente. La empresa IquitosPlay no se puede hacer responsable del comportamiento de la aplicación cuando ésta entre en producción si no cuenta con un ambiente de pruebas y datos significativos para realizar las pruebas del sistema. Se agregaron tareas en el cronograma para llevar a cabo este proceso (reuniones, negociación para tomar una decisión).</p>