Universidad de las Ciencias Informáticas
“Facultad 4”

Título: Gestión de Riesgos del proyecto Sistema de Gestión Penitenciaria (SIGEP).

Trabajo de Diploma para optar por el título de

Ingeniero Informático

Autor(es): Yusleimi González Cedeño

Tutor(es): Lic. Elizabeth Rodríguez Stiven

Ciudad de la Habana, junio 2008.

DECLARACIÓN DE AUTORÍA

Declaramos ser autores de la presente tesis y reconocemos a la Universidad de las Ciencias Informáticas los derechos patrimoniales de la misma, con carácter exclusivo.

Para que así conste firmo la presente a los ____ días del mes de _____ del año _____.

Yusleimi González Cedeño

_____
Firma del Autor

Elizabeth Rodríguez Stiven

_____
Firma del Tutor

DATOS DE CONTACTO

Tutora: Lic. Elizabeth Rodríguez Stiven.

- ✓ Licenciada en Ciencias de la Computación en la Universidad de la Habana en el año 2006.
- ✓ Profesora de la Universidad de las Ciencias Informáticas, en la Disciplina de Matemática desde el año 2006.
- ✓ Cuenta con 2 años de trabajo en la Educación Superior.
- ✓ Cursa la Maestría en Gestión de Proyectos Informáticos.

Correo electrónico: beth@uci.cu

AGRADECIMIENTOS

A la ***Revolución*** por permitirme la educación y formación profesional, por hacerme una persona digna de estos tiempos.

A la ***UCI*** por ser mi hogar, por darme la posibilidad de crecerme como persona, por educarme, por darme tantos amigos.

A mi tutora ***Elizabeth*** por asesorarme y ayuda incondicional.

A los ***profes*** por contribuir a mi formación profesional y revolucionaria.

A ***todos mis compañeros*** **de aula** que me hicieron sonreír y aportaron granitos de felicidad a mi estancia.

A ***todos*** los que me ayudaron de una u otra forma, gracias.

A *mi* ***Mamá*** **y Nelson** por su apoyo y sacrificio, por hacer de mí lo que soy hoy, por ese amor desmedido que me han dado.

A ***mi Papá*** por su apoyo y estar siempre a mi lado en todos los momentos de mi vida, por amarme tanto y ayudarme hacer lo que soy hoy.

A mi esposo **Yurien** por amarme, ser mi amigo, guía y compañía en estos cinco años y para toda la vida. Te amo.

A mis tíos(a) **Blanca, Fela, Andrea, Cuso y Ariel** por demostrarme que la vida continúa cuando todo suele empeorar, por quererme tanto y ayudarme en todas las esferas de mi vida.

A mis primas **Niurka y Solangel** por ser mis amigas, hermanas y madres. Por todos sus consejos y ayuda en todo los años de mi vida. Las quiero Mucho.

A mis suegros **Pancho y Migdalia** por su amor y ayuda en estos cinco años.

A mi abuelita **Luisa** por quererme tanto, porque sé que eres un ángel que me guías y que estas orgullosa de mi. No te defraudaré. Te amo.

A mi abuela **Isora** por quererme. Sé que estas orgullosa de mi.

A ***Yudaisy*****, Brisey** por la confianza, por ser mis amigas, por ayudarme y enseñarme tanto.

A ***Estercita y Adaima***, por ser mis amigas para siempre, por su apoyo, por estar siempre ahí para escucharme. Por compartir tantos momentos conmigo desde la infancia.

A **Alieski y Felicó** por su ayuda y consejos.

A **Carmita, Daynelis, Ivette y Ariel** por confiar en mí y ser mis amigos.

A **Cristo** por estar siempre a mi lado, porque sin él no sería nadie. Por su Fidelidad y amor incondicional.

DEDICATORIA

A mis padres y a mi abuela Luisa que aunque ya no está sé que hubiese disfrutado mucho de este triunfo en mi vida.

A toda aquella persona que en un futuro va a utilizar esta tesis para su desarrollo profesional.

RESUMEN

El presente trabajo tiene como objetivo establecer un modelo de gestión de riesgo para llevar a cabo el proceso de gestión de riesgo en el proyecto Sistema de Gestión Penitenciario (SIGEP) de manera que se minimice el impacto[1] de los riesgos que puedan afectar los objetivos finales del proyecto e ir educando al equipo de desarrolladores a comenzar la gestión del producto por la gestión de sus riesgos.

Más allá de suplir las necesidades del proyecto SIGEP este trabajo no se limitó a seleccionar y adaptar una metodología que beneficiará solo a SIGEP sino que extiende sus funcionalidades a todos los proyecto de la facultad 4, estableciendo una estructura taxonómica para la identificación y clasificación de los riesgos, una representación vectorial de los riesgo que facilita su posterior implementación, plantillas para la documentación del proceso y métrica que ayuda a evaluar el proyecto según sus riesgos.

Se identificaron y evaluaron los riesgos del proyecto SIGEP y se tomaron las medidas necesarias para que fueran mitigados según plantea la metodología Modelo de Gestión de Riesgos (MoGeRi). Otro de los aportes de esta investigación es proporcionar evidencia empírica de la gestión de riesgos en los proyectos de desarrollo de software, ante la escasez de casos existentes en la literatura.

PALABRAS CLAVE

Palabras claves: Gestión de Riesgos, Plan de Contingencia, Plan de Mitigación.

TABLA DE CONTENIDOS

Índice de Ilustraciones

Índice de tablas

INTRODUCCIÓN

Durante el desarrollo de un proyecto de software, factores como el entorno tecnológico, los recursos necesarios, las herramientas[2] utilizadas, los requerimientos del cliente y la estabilidad del personal, pueden sufrir cambios sustancialmente lo que conlleva a situaciones inesperadas que alteran el término del proyecto. Estas "sorpresas" que pueden ocasionar daños a los objetivos del proyecto, no son más que los riesgos.

A pesar de que se han producido amplios debates sobre la definición adecuada de riesgo de software, hay acuerdo común en que este siempre implica dos dimensiones:

Incertidumbre: El acontecimiento que caracteriza al riesgo puede, o no, ocurrir.

Pérdida: Si el riesgo se convierte en una realidad, esto tendrá consecuencias para el proyecto.

En el contexto de la gestión de proyectos, desde mediados de los años 80, las empresas reconocieron la necesidad de integrar los riesgos de carácter técnico con los de coste, planificación o calidad. A partir de allí se desarrollaron metodologías integradas de gestión de riesgos(1). De hecho, la mayor parte de los proyectos de ingeniería complejos dependen de una correcta identificación e incorporación de las tecnologías apropiadas para su desarrollo que deberán gestionar como parte del mismo. Estas tecnologías no siempre son suficientemente conocidas o maduras, por lo que su utilización no siempre genera los beneficios esperados(2).

La *gestión de riesgos:* es el proceso por el que los factores de riesgo se identifican sistemáticamente y se evalúan sus propiedades. Es una metodología sistemática y formal que se concentra en identificar y controlar áreas de eventos que tienen la capacidad de provocar un cambio no deseado. En el contexto de un proyecto, es el arte y ciencia de identificar, analizar y responder a los factores de riesgo a lo largo de la vida del proyecto y en el mejor cumplimiento de sus objetivos(1).

Cuando se pone mucho en un proyecto de software el sentido común nos aconseja realizar un análisis de los riesgos. Y sin embargo, la mayoría de los jefes de proyectos lo hacen de manera informal, si es que lo hacen. El tiempo invertido identificando, analizando y gestionando el riesgo merece la pena por muchas razones: menos trastornos durante el proyecto, una mayor habilidad de seguir y controlar y la confianza que da planificar los problemas antes de que ocurran. Para tratar de minimizar los efectos de un problema de seguridad se realiza lo que denominamos un ***Análisis de Riesgos:*** es un proceso por el cual se identifican las amenazas y vulnerabilidades de una organización. Con el fin de generar controles que minimicen los efectos de los riesgos(3).

Este análisis permite, el establecimiento de un nivel adecuado de seguridad tanto del software que se desea proteger como del que se desarrollará. También involucra un proceso de administración de riesgos, dado que es necesario evaluar periódicamente si los riesgos identificados se mantienen

vigentes. Tener conocimientos de los riesgos de un proyecto ya supone una ventaja, pues facilita un estado de alerta sobre los mismos, y permite disminuir sus consecuencias en caso de producirse.

En los proyectos de desarrollo de software la **Gestión de Riesgo** es crucial para obtener el éxito, pues aseguran la continuidad operacional de la organización, puedes manejar las amenazas y riesgos críticos y mantener una estrategia de protección y de reducción de riesgos. Esto evitaría que el proyecto pierda calidad[3] al producirse el incumplimiento de los cronogramas de trabajo, del horario de producción y planificación de las actividades, entre otras.

En los tiempos que trascurren, ha sido necesaria la informatización de distintos renglones de la economía y los servicios a escala global. La República Bolivariana de Venezuela no queda al margen de esto, por lo que decide informatizar algunos servicios de la sociedad entre ellos la Dirección General de Custodia y Rehabilitación del Recluso (DGCRR).

La DGCRR no cuenta con aplicaciones informáticas. Los expedientes de los privados de libertad se llevan mayormente en papel, salvo algunas iniciativas aisladas que utilizan hojas de cálculo para mantener alguna información(4).

El Sistema de Gestión Penitenciaria (SIGEP) permitirá a los establecimientos penitenciarios (Internados Judiciales, Centros Penitenciarios, Centros de Tratamiento Comunitario) y otras sedes (Coordinaciones Regionales y UTASP[1]), recopilar y controlar la información operativa que se genera en este tipo de centros. Esta solución controlará el tránsito de los privados de libertad por todos los componentes del sistema penitenciario, y en general manejará datos sobre la población penal y auditará los procesos legales para garantizar un cumplimiento justo de la sentencia. La solución incluye además la gestión de los servicios médicos y alimenticios y el tratamiento ofrecido en estos establecimientos penitenciarios, así como el apoyo para la toma de decisiones estratégicas de la DGCRR.

La informatización de la Dirección General de Custodia y Rehabilitación del Recluso (DGCRR) en la República de Venezuela fue una tarea encomendada por la 6ta Mixta Cuba-Venezuela y entonces surge el proyecto Sistema de Gestión Penitenciaria (SIGEP) tienen la misión de que este proyecto se realice y cumpla las expectativas un grupo de estudiantes e Ingenieros, profesores de la Universidad de las Ciencias informáticas (UCI) que radica en Cuba.

[1] Unidades técnicas de desarrollo al sistema penitenciario.

En las aplicaciones Web del Proyecto (SIGEP), como en todo proyecto de la vida laboral y social existen riesgos que obstaculizan la creación conceptual y el quehacer diario. Estos afectan a los futuros acontecimientos, implican toma de decisiones, cambios de opinión y de acciones.

Por la importancia que representa la Gestión de Riesgo (GR) durante el desarrollo del Software nos interesa resaltar la situación actual del proceso de GR en el proyecto SIGEP. Actualmente en el proyecto se conocen de cierta forma, un poco informalmente los riesgos que podrían afectar el proyecto, pero no se guían por una metodología formal de GR y mucho menos se procede a su análisis o gestión. Por lo que no se tiene medida del nivel de riesgo del proyecto y ocasiona incumplimientos en el término de los objetivos trazados y aumento del costo del mismo. Luego de realizar un profundo análisis de la información referente al Análisis y Gestión de Riesgos y la necesidad de ello en el proyecto, se plantea el siguiente **problema:**

¿Cómo desarrollar la Gestión de Riesgo en el Proyecto SIGEP aplicando un Modelo de Gestión de Riesgo?

El **objeto de investigación** del presente trabajo se centra en los modelos de Gestión de Riesgo y tiene como **campo de acción** el proceso de gestión de riesgo en el proyecto SIGEP.

Dada la necesidad existente, se desarrolla este trabajo que tiene como **objetivo general**:

Proponer una metodología para realizar la GR en el proceso de desarrollo de software del proyecto SIGEP. Aplicar la metodología a los riesgos del proyecto.

Se plantea la siguiente **Hipótesis**:

La aplicación de un Modelo de Gestión de Riesgo en la gestión de riesgo del proyecto SIGEP logrará mejorar la Gestión de Riesgo durante el desarrollo del Software.

Como ***objetivos específicos*** se definen:

1. Investigar sobre diferentes procesos de Gestión de Riesgos, definiciones y metodologías existentes en Cuba y en el mundo, que permita conocer su evolución, características fundamentales y tendencias actuales.
2. Determinar la metodología a usar en el proceso de Gestión de Riesgos del proyecto SIGEP.
3. Realizar un análisis de las características del modelo Gestión de Riesgo para adaptarlo a las características del proyecto SIGEP.
4. Aplicar el modelo escogido (con sus adaptaciones en la Gestión de Riesgo al proyecto SIGEP).
5. Evaluar la utilización del modelo de GR en el proyecto SIGEP.

Para cumplir estos objetivos es necesario establecer un conjunto de **Tareas:**

1. Revisar en la bibliografía de lo que existe en Cuba y en el mundo sobre la Gestión de Riesgos.

2. Realizar un estudio comparativo de las metodologías y tendencias actuales fundamentales de la Gestión de Riesgo.
3. Seleccionar la metodología para definir el proceso de Gestión de Riesgos en el proyecto SIGEP.
4. Determinar las distintas adaptaciones que se le debe hacer a la metodología para aplicarla al proyecto.
5. Realizar encuestas y entrevistas al equipo de desarrollo del proyecto para obtener información acerca de los riesgos.
6. Planificar la Gestión de Riesgo en el proyecto SIGEP.
7. Identificar Riesgos genéricos para PDSW que afecten a SIGEP y cualquier proyecto de la facultad.
8. Identificar riesgos específicos de SIGEP.
9. Analizar los riesgos encontrados.
10. Planificar respuestas a estos riesgos.
11. Seguir y controlar los riesgos identificados.

CAPÍTULO 1: FUNDAMENTOS TEÓRICOS DE LA GESTIÓN DE RIESGO

1. Introducción

En el presente capitulo se brindan los principales conceptos relacionados con el proceso de Gestión de Riesgo en proyectos de desarrollo Software.

El objetivo de la gestión del riesgo es lograr que la experiencia vivida de desastres y, de la respuesta a los mismos, nos permita tener una nueva visión que genere propuestas para reducir las condiciones actuales del riesgo conduciendo, al mismo tiempo, hasta el desarrollo sostenible.

1.1 Un poco de Historia sobre la Gestión de Riesgo

La gestión de riesgos pasa por tres generaciones de modelos de riesgos en proyectos informáticos:

Primera Generación G1 (Casuística)

Esta generación data de principios de los años 80 y está basada en listas casuísticas de riesgos especiales para proyectos, esto es, se identifican casos de riesgo y se extrapolan a otros proyectos. No hay una planificación específica. En esta generación se definen los Riesgos tecnológicos y las listas de comprobación de riesgos.

Segunda Generación G2 (Taxonómica)

Esta surge a principios de los años 90. Basada en modelos de procesos y eventos. Es la generación taxonómica de análisis de riesgos en los proyectos. Marcelo, Rodenes y Torralba, apuntan que los modelos de la G2 se han limitado a analizar los riesgos al inicio del proyecto y a planificar medidas y definen esta visión como “preventiva”, “teorizante” y de medidas “curativas”, improvisadas en mayor o menor medida, durante el avance del proyecto, para paliar[2] los riesgos según se presentan(5). Posteriormente califican a los modelos de la G2 como “meramente reactivos, con unas relaciones de causa-efecto basadas sólo en una confianza que parte de experiencias poco validadas”. Los marcos contenidos en esta generación son:

1. Modelo de Boehm.
2. Modelo de Hall.
3. Modelo del SEI.
4. Modelo SPR (Software Productivity Research) de Capers Jones.
5. Modelo SERIM (Software Engineering Risk Management) de Karolak: IEEE.
6. Modelo del PMI.
7. Modelo de McFarlan (adelantos de G3)

[2] Dícese aminorar, disminuir, mitigar, debilitar los riesgos.

Tercera Generación G3 (Causal)
Esta es la generación actualmente emergente. Está influida por otros modelos causales (proyectuales, ecológicos, etc.). Surge de forma simultánea en Europa y en EEUU, partiendo de la preocupación por proyectos de tanto riesgo como la adquisición o el desarrollo de software. Articula una causalidad más explicativa y por lo tanto más predictiva entre los elementos del modelo, sobre todo entre los factores de riesgo y sus medidas reductoras o salvaguardas. Esta generación, prepara el paso a la gestión de proyectos por los riesgos. Se apoya en modelos sistémicos, relacionales (redes de causas-efectos) y proactivos en el aseguramiento de los proyectos(5). Los marcos incluidos en esta generación son:

1. Eurométodo, del Consejo Superior de la Administración Electrónica de España.
2. MAGERIT: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información, del Consejo Superior de la Administración Electrónica de España.
3. ISPL (Information Services Procurement Library).
4. Proyectos de investigación europeos como RiskMan, DriveSPI, RiskDriver y los de autores como Moynihan, Barki y Schmidt.

1.2 Antecedentes de la Gestión de Riesgo

1.2.1 Gestión de Riesgo en el ámbito Internacional.

Aunque los diversos enfoques de GR aparecieron hace varias décadas, sigue siendo evidente la poca utilización de sus técnicas en los proyectos de desarrollo de software actuales. Por ejemplo, una demostración de lo anteriormente mencionado fue el estudio que se realizó durante el año 2001 con 268 organizaciones de todo el mundo y el resultado fue que: el 3% no utilizaba ningún marco de gestión del riesgo, el 18% utilizaba algún marco caótico para identificar sus riesgos, el 37% de los participantes habían utilizado algún marco informal, el 28% utilizaban procedimientos repetitivos y sólo un 14% utilizaba un enfoque formal para identificar riesgos.

Según este estudio, las razones más comunes para utilizar un marco informal son: la falta de procedimientos, las necesidades del proyecto mal definidas, la organización inexperta o inmadura y el compromiso del equipo. El riesgo en un proyecto de desarrollo de software incluye componentes técnicos y de conocimiento del riesgo. Diferentes estudios han mostrado que la mayoría de los proyectos fallan sobre todo en gestión, no tecnológicamente.

1.2.2 Gestión de Riesgo en el ámbito Nacional

Durante el año 2007 se le realizaron entrevistas a trabajadores de seis entidades diferentes del país, que se dedican de una forma u otra a la producción de Software; como son Desoft[3] en Ciudad de la

[3]Empresa cubana de Desarrollo de Software.

Habana, La Universidad Central de las Villas, la Universidad de las Ciencias Informáticas, el Instituto Superior Politécnico “José Antonio Echeverría” y en Desoft en Ciego de Ávila ; el resultado que se obtuvo fue que solamente en la Universidad de las Ciencias Informáticas en los proyectos productivos Tele banca y Control y Aseguramiento de la Calidad se utilizó algún marco informal de Gestión de Riesgos.

De cierta forma la Dirección de los proyectos de Software y el personal vinculado a los mismos, conocen los riesgos que podrían afectar su trabajo, pero es evidente que no son registrados, no son correctamente planteados y mucho menos se procede a su análisis o gestión. Se llegó a la conclusión que en la mayoría de las empresas cubanas que se dedican a la producción de software solamente se identifican los riesgos y de manera poco consciente.

1.3 Conceptos Básicos

1.3.1 Riesgo

Un riesgo es cualquier suceso que pueda afectar negativamente a la marcha del proyecto en el futuro, es la posibilidad de que existan consecuencias indeseables o inconvenientes, de un acontecimiento, cuya aparición no se puede determinar con prioridad. El riesgo se haya asociado de manera inexorable a cualquier actividad que se lleve a cabo y que imponga la decisión entre varias alternativas. El riesgo, -por tanto-, acompaña a todo cambio y está presente en cada decisión. El riesgo implica elección e incertidumbre.

1.3.2 Manejo de Riesgos

Manejo de riesgos consiste en la identificación de riesgos y la escritura de planes para minimizar el efecto de estos en el proyecto. Un riesgo se relaciona con la probabilidad de que ocurra alguna circunstancia adversa al proyecto.

1.3.3 Gestionar riesgos

Conjunto coherente y ordenado de estrategias, programas y proyectos, que se formulan para orientar las actividades de reducción de riesgos(6).

Se han considerado dos formas de clasificar estrategias para controlar los riesgos: reactivas y proactivas.

La estrategia *reactiva* es la que reacciona en el momento que ocurren los problemas, para a partir de ahí combatirlos. En el mejor de los casos, la estrategia *reactiva* supervisa el proyecto en previsión de posibles riesgos. Los recursos se ponen aparte, en caso de que pudieran convertirse en problemas reales, pero lo más frecuente es que el equipo de software no haga nada respecto a los riesgos hasta que algo esté mal. Después el equipo se agiliza para corregir el problema rápidamente. La gestión entra en crisis, encontrándose el proyecto en peligro real.

La otra estrategia considerada como la más inteligente para el control del riesgo es ser *proactivo*. La estrategia *proactiva* empieza mucho antes de que comiencen los trabajos técnicos. Se identifican los riesgos potenciales, se valoran su probabilidad y su impacto y se establece una prioridad según su importancia. Después el equipo de software establece un plan para controlar el riesgo. El primer objetivo es evitar el riesgo, aunque es poco común que todos puedan ser detectados. Entonces el equipo trabaja para desarrollar un plan de contingencia que le permita responder de una manera eficaz y controlada.

1.3.4 Riesgos del software.

Aunque ha habido amplios debates sobre la definición adecuada para riesgo de software, hay acuerdo común en que el riesgo siempre implica dos características(7):

Incertidumbre: El acontecimiento que caracteriza al riesgo puede o no ocurrir; por ejemplo, no hay riesgos de un 100 por ciento de probabilidad[4].

Pérdida: Si el riesgo se convierte en una realidad, ocurrirán consecuencias no deseadas o pérdidas.

Cuando se analizan los riesgos es importante examinar el nivel de incertidumbre y el grado de pérdidas asociado con cada riesgo. Para hacerlo, se consideran diferentes categorías de riesgos.

Los ***riesgos del proyecto*** amenazan al plan del proyecto. Es decir, si los riesgos del proyecto se hacen realidad, es probable que la planificación temporal del proyecto se retrase y que los costos aumenten. Los riesgos del proyecto identifican los problemas potenciales de presupuesto, planificación temporal, personal (asignación y organización), recursos, clientes y requisitos y su impacto en un proyecto de software.

Los ***riesgos técnicos*** amenazan la calidad y la planificación temporal del software que hay que producir. Si un riesgo técnico se convierte en realidad, la implementación puede llegar a ser difícil o imposible. Los riesgos técnicos identifican problemas potenciales de diseño, implementación, de interfaz, verificación y de mantenimiento. Además las ambigüedades de especificaciones, incertidumbre técnica, técnicas anticuadas y las "tecnologías de punta" son también factores de riesgo. Los riesgos técnicos ocurren porque el problema es más difícil de resolver de lo que pensábamos.

Los ***riesgos del negocio*** amenazan la viabilidad del software a construir. A menudo ponen en peligro el proyecto o el producto(8). Los candidatos para los principales riesgos del negocio son:

- Construir un producto o sistema excelente que no quiere nadie en realidad (riesgo de mercado).

[4] Un riesgo del 100 por 100 es una limitación del proyecto de software.

- Construir un producto que no encaja en la estrategia comercial general de la compañía (riesgo estratégico).
- Perder el apoyo de una gestión experta debido a cambios de enfoque o a cambios de personal (riesgo de dirección).
- Perder presupuesto o personal asignado (riesgos de presupuesto).

Es importante recalcar que no siempre funciona una categorización tan sencilla. Algunos riesgos son simplemente imposibles de predecir.

Los riesgos conocidos son todos aquellos que se pueden descubrir después de una cuidadosa evaluación del plan del proyecto del entorno técnico y comercial en el que se desarrolla el proyecto y otras fuentes de información fiables(8), ejemplo: fechas de entrega poco realistas, falta de especificación de requisitos o de ámbito del software, o un entorno pobre de desarrollo. Los riesgos predecibles se extrapolan de la experiencia en proyectos anteriores, ejemplo: cambio de personal, mala comunicación con el cliente, disminución del esfuerzo del personal a medida que atienden peticiones de mantenimiento, pueden ocurrir pero son extremadamente difíciles de identificar por adelantado.

1.3.5 Mitigación de riesgos

Planificación y ejecución de medidas de intervención dirigidas a reducir o disminuir el riesgo. La mitigación es el resultado de la aceptación de que no es posible controlar el riesgo totalmente; es decir, que en muchos casos no es posible impedir o evitar totalmente los daños y sus consecuencias y sólo es posible atenuarlas(6).

1.3.6 Plan de contingencia

Procedimientos operativos específicos y preestablecidos de coordinación, alerta, movilización y respuesta ante la manifestación o la inminencia de un fenómeno peligroso particular para el cual se tienen escenarios definidos(6).

1.3.7 Seguimiento de riesgos

La monitorización del riesgo consiste en controlar el progreso del proyecto en lo relativo a resolución de riesgos, tomando las acciones correctoras cuando sea necesario. Una técnica de monitorización puede ser el seguimiento de hitos.

- Determina regularmente cada riesgo identificado y decide si es probable o no que se presente.
- Determina si los efectos que provocaría el riesgo, han cambiado.
- Cada riesgo clave debe discutirse en las reuniones de avance del proyecto.

El seguimiento de riesgos hace posible la visibilidad del proceso de gestión de los mismos dentro del proyecto desde la perspectiva de los niveles de riesgo. El informe de los riesgos garantiza que el

equipo y los líderes estén al corriente del estado de los riesgos del proyecto y de los planes para administrarlos.

1.4 Gestión de Riesgo

Diferentes definiciones de la GR que pueden ayudar a tomar partido por una posición u otra:

La gestión de riesgos es el proceso por el que los factores de riesgo se identifican sistemáticamente y se evalúan sus propiedades. Es una metodología sistemática y formal que se concentra en identificar y controlar áreas de eventos que tienen la capacidad de provocar un cambio no deseado. La gestión de riesgos, en el contexto de un proyecto, es el arte y ciencia de identificar, analizar y responder a los factores de riesgo a lo largo de la vida del proyecto y en el mejor cumplimiento de sus objetivos.

- Constituye además un Proceso social complejo que conduce al planeamiento y aplicación de políticas, estrategias, instrumentos y medidas orientadas a impedir, reducir, prever y controlar los efectos adversos de fenómenos peligrosos sobre la población, los bienes y servicios(6).
- La Gestión del Riesgo es una técnica que maneja los recursos empleables en el proyecto para limitar la diferencia entre su Estado Final Deseado (EFD) y su Estado Final Conseguido (EFC). Si la diferencia supera un límite establecido, se materializa un riesgo de incumplimiento del objetivo. Para asegurar la pertinencia del resultado suelen requerirse decisiones de realización de nuevas acciones que permitan reducir esa diferencia. Si el EFC está muy alejado del EFD, el proyecto incumplirá el objetivo; hasta su misma consecución puede resultar imposible(5).
- La identificación, análisis y mitigación de riesgos en sistemas de información, a un nivel acorde al valor de los activos[4] protegidos(9).
- El proceso formal en el que los factores de riesgos son sistemáticamente identificados, evaluados y mitigados(10).

La Gestión de Riesgo presenta dos fases principales:

- Estimación de riesgos.
- Control de riesgos.

Ilustración 1: Componentes de la GR.

Otra visión según Boehm:

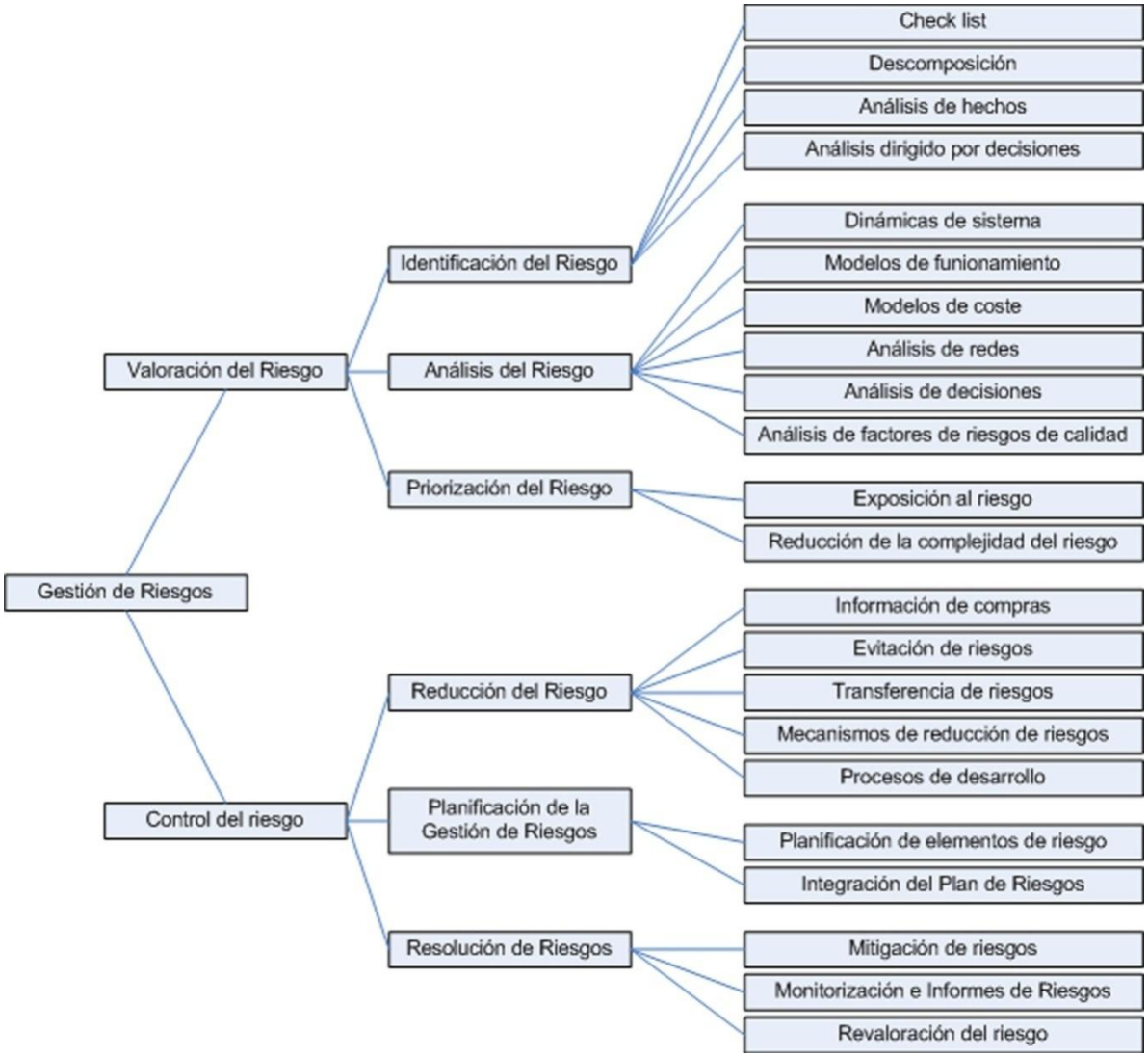

Ilustración 2: Componentes de la Gestión de Riesgos según Boehm.

1.4.1 Ventajas de Gestión de Riesgo:

Primero que nada, por aplicar el proceso de Gestión de Riesgo, los miembros del proyecto están obligados a responder acerca de los riesgos incurridos en el proyecto. La gestión de riesgo promueve la comunicación entre los integrantes del grupo de trabajo, como métricas, la información es rápidamente dada a los principales administradores, lo cual les permite tener una visión global sobre como avanza el proyecto.

Aplicar el proceso de Gestión de Riesgos lleva transparencia a la vida del proyecto: ayuda a no olvidar el problema que se ha encontrado. La experiencia es directamente tomada en cuenta, principalmente si un problema similar aparece en un proyecto similar.

El principal interés en la gestión de riesgo es aportar una importante e eficiente ayuda al administrador del proyecto para conducir el mismo.

1.4.2 Procesos de la Gestión de Riesgo

Proceso Identificación de Riesgos

La fase de identificación de riesgos consiste en descubrir factores de riesgo antes de que estos lleguen a ser problemas y deriven en daños o pérdidas. Es un intento sistemático para especificar las amenazas al plan del proyecto (estimaciones, planificación temporal, carga de recursos, etc.). Identificando los riesgos conocidos y predecibles, el gestor del proyecto da un paso adelante para evitarlos cuando sea posible y controlarlos cuando sea necesario(8).

Este es, probablemente, el paso más importante entre todos aquellos que componen las actividades de Gestión de Riesgos, ya que sin la correcta determinación de los mismos, no es posible desarrollar e implementar anticipadamente respuestas apropiadas a los problemas que puedan surgir en el proyecto. El resultado de la identificación de riesgos es una lista conteniendo los riesgos que se han identificados y su categoría correspondiente.

Existen dos tipos diferentes de riesgos: *genéricos* y *específicos* del producto.

Los riesgos *genéricos* son una amenaza potencial para todos los proyectos de software. Los *específicos* de producto sólo los pueden identificar los que tienen una clara visión de la tecnología, el personal y el entorno específico del proyecto en cuestión. Para identificar los riesgos específicos del producto se da una respuesta a la siguiente pregunta: ¿Qué características especiales de este producto pueden estar amenazadas por el plan del proyecto?

La clave del éxito está en adelantarse a los problemas y tener acciones contempladas para evitar que sucedan o disminuir su impacto y tanto los riesgos genéricos como los específicos del producto se deberían identificar sistemáticamente, porque: "Si no atacas activamente a los riesgos, ellos te atacarán activamente a ti"(11).

Proceso Análisis de Riesgo

El análisis de riesgos consiste en convertir los atributos del riesgo en información que sirva como base para tomar decisiones. Esto implica establecer valores para el impacto (la pérdida o efecto negativo en un proyecto en caso de que ocurra el riesgo); y la probabilidad (la probabilidad de que el riesgo ocurra)(12). Este análisis puede ser cuantitativo y otra cualitativo. La primera de ellas es con diferencia

la menos usada, ya que en muchos casos implica cálculos complejos o datos difíciles de estimar. Se centra en la cuantificación y priorización de los riesgos de forma objetiva. Se pueden resaltar sus principales funciones: determinar la probabilidad de realizar un objetivo específico del proyecto y cuantificar el riesgo del proyecto y determinar el tamaño de costo(13).

El segundo método de análisis de riesgos es el cualitativo, de uso muy difundido en la actualidad. Es mucho más sencillo e intuitivo que el anterior, consiste en evaluar cual es el impacto y la probabilidad de ocurrencia de un riesgo identificado. Tiende a priorizar los riesgos de acuerdo a su efecto potencial sobre los objetivos del proyecto. Requiere de métodos y herramientas de análisis cualitativo establecidas como por ejemplo matrices de probabilidad e impacto y evaluación de lo que se asumió en el proyecto.

Para realizar el análisis de riesgo se debe primeramente evaluar la probabilidad y las consecuencias del mismo. La probabilidad puede ser muy baja (<10%), baja (10-25%), moderada (25-50%), alta (50-75%) o muy alta (>75%) y las consecuencias ó impacto del riesgo pueden ser catastróficas, serias, tolerables o insignificantes.

Proceso de Planificación del Riesgo.

Tomando como entrada la lista priorizada de riesgos, la fase de planificación del riesgo consiste en decidir qué hacer y cuándo, para cada uno de los riesgos de la lista. La estrategia del riesgo para un riesgo específico puede ser diferente según el conocimiento actual de los riesgos del proyecto: transferir, mitigar, evitar o aceptar el riesgo(12). Como resumen se puede decir, que es el proceso que permite desarrollar opciones y determinar acciones para reducir las amenazas de los objetivos del proyecto. Incluye la identificación y la asignación de individuos para tomar la responsabilidad de cada respuesta a cada riesgo(13)

Proceso de Seguimiento del Riesgo

El seguimiento es el proceso de recogida de datos, de su análisis y posterior divulgación para los riesgos que están en observación o mitigación.(12)

Proceso de Control del Riesgo

La finalidad de esta fase es: corregir las desviaciones de los planes de mitigación. Además de controlar los riesgos de la lista actual del proyecto, el equipo debe estar atento a nuevos riesgos que puedan aparecer en su entorno a medida que el proyecto avanza(12)

Proceso de Comunicación

La finalidad de la fase de comunicación es: proporcionar información sobre las actividades de gestión del riesgo del proyecto, los riesgos actuales y los riesgos que puedan surgir. La comunicación es

esencial para el éxito de todas las otras funciones y es crítica para gestionar los riesgos. Para una gestión eficaz de los riesgos, una organización debe tener una comunicación abierta y ejercida de una manera continua. Ésta puede ser tanto formal como informal(12).

1.5 Factores de riesgo

Los factores de riesgo son elementos que determinan el riesgo. Es necesaria su medición y monitorización para determinar cuan cerca estamos del riesgo. Por cada riesgo se hace necesario identificar los factores que lo determinan. Un riesgo puede ser a su vez un factor de riesgo en otros riesgos.

En la siguiente Tabla, se muestran diferentes enfoques sobre los factores de riesgos consultados en la literatura para PDSW.

Factor	Propuesta
Boehm. Lista de riesgos según los accionista (BOEHM, B. 1991).	
Factor 1	Falta de personal calificado
Factor 2	Itinerario y presupuestos poco realistas
Factor 3	Desarrollo incorrecto de las funciones del software.
Factor 4	Desarrollo incorrecto de las interfaces del usuario
Factor 5	Adición de funciones o características innecesarias
Factor 6	Cambio constante en los requerimientos.
Factor 7	Fallas en los componentes subcontratados.
Factor 8	Pobre calidad de las tareas subcontratadas.
Factor 9	Fallas en tiempo real de respuesta.
Factor 10	Inhabilidad para implementar soluciones técnicas debido a la pobre capacidad de conocimiento en las ciencias de la computación.
Barki. Evaluación de riesgos en proyectos de desarrollo de software (BARKI 1993).	
Factor 1	Tecnológico.
Factor 2	Tamaño de la aplicación.
Factor 3	Falta de experiencia.
Factor 4	Complejidad de la aplicación.
Factor 5	Ambiente organizacional.
Jones. Factores de riesgos relevantes en el desarrollo de software (JONES 1998).	
Factor 1	Estimación y planeación inexacta del itinerario.
Factor 2	Reporte de estatus incorrectos y optimistas.
Factor 3	Presiones externas que dañan los proyectos.
Estéves y Pastor. Factores estratégicos y organizacionales (ESTEVES and PASTOR 2000).	
	Factores Estratégicos
Factor 1	Apoyo continuo de la alta dirección.
Factor 2	Gestión efectiva del cambio organizacional.
Factor 3	Buena gestión del ámbito del proyecto.
Factor 4	Composición adecuada del equipo del proyecto.
Factor 5	Rediseño adecuado de los procesos del negocio.
Factor 6	Papel adecuado del líder del proyecto.

Factor 8	Implicación y participación de los usuarios.
Factor 9	Confianza entre actores.
	Factores tácticos
Factor 1	Equipo y consultores dedicados.
Factor 2	Comunicación interna y externa.
Factor 3	Plan formalizado del proyecto.
Factor 4	Programa de formación adecuado.
Factor 5	Precisión de problemas inesperados.
Factor 6	Uso adecuado de consultores.
Factor 7	Responsables debidamente autorizados.
SEI. Taxonomía para riesgo de desarrollo de software (CARR *et al.* 1993).	
	Ingeniería del producto
Factor 1	Requerimientos.
Factor 2	Diseño.
Factor 3	Codificación y prueba unitaria.
Factor 4	Integración y prueba.
Factor 5	Especialidades de la ingeniería.
	Entorno de desarrollo
Factor 1	Proceso de desarrollo.
Factor 2	Sistema de desarrollo.
Factor 3	Proceso de Gestión.
Factor 4	Métodos de Gestión.
Factor 5	Entorno de trabajo.
	Restricciones del proyecto
Factor 1	Recursos.
Factor 2	Contrato.
Factor 3	Interfaces del proyecto.

Tabla 1: Resumen de factores de riesgo en proyectos de desarrollo de software.

1.6 Modelos utilizados para la Gestión de Riesgos

Aunque los enfoques de la gestión de riesgo surgieron hace más de una década, sigue viéndose la poca utilización de sus técnicas en los proyectos de desarrollo de software actuales. Existen diferentes marcos que nos ayudan a la hora de implementar las funciones básicas que deben llevarse a cabo para una efectiva Gestión de los Riesgos. A continuación le ofrecemos algunos de los modelos más conocidos por sus nombres o por las organizaciones que los avalan. Es sumamente importante destacar que cada método establece categorías para las funciones del riesgo en diferentes fases.

1.6.1 Modelo de Boehm

Para Boehm la GR pasa por dos fases fundamentales: Valoración del riesgo y Control del riesgo(14). Las actividades con que consta cada fase son las siguientes:

Valoración del riesgo:

- Identificar el riesgo
- Análisis de riesgo

- Priorización de riesgo

Control del riesgo:

- Reducción del Riesgo
- Planificación
- Gestión del riesgo
- Resolución del riesgo

Además Boehm incluye en su estudio una lista de diez riesgos (Top 10 Software RiskÍtems) muy generales y que pueden estar presentes en cualquier proyecto y también plantea una serie de técnicas a aplicar en la gestión del riesgo. **(Ver Anexo 2)**.

1.6.2 Modelo del SEI para la Gestión de Riesgos

El modelo Continuous Risk Management (SEI-CRM), desarrollado por el Software Engineering Institute (SEI) es unos de los métodos más conocidos y más completos, con más documentación detallada y cuya aplicación está más extendida en la industria; es un método en el ámbito de la ingeniería del software cuyos conceptos, procesos y herramientas permiten gestionar de manera continua los riesgos de un proyecto, proporcionando un entorno disciplinado para la toma preactiva de decisiones a lo largo de todas las fases del proyecto: análisis de los problemas en potencia (riesgos), determinación de los riesgos importantes para elaborar estrategias y planes para gestionarlos. Estos riesgos son controlados hasta que se resuelven o se convierten en problemas menores, y son tratados como tales. Además este método también incluye el concepto de gestionar estas actividades como un ciclo básico, es decir, identificar, analizar, planificar, seguir, controlar y comunicar los riesgos a lo largo de todo el ciclo de vida del proyecto.

El SEI expone tres dimensiones que representan la visión holística de Gestión de Riesgo(GR) de software: la dimensión temporal, la dimensión humana y la dimensión metodológica(15).

La dimensión temporal, se descompone en la visión Macro, que representa la perspectiva global del ciclo de vida de adquisición y la visión Micro, que representa la vista del gerente del proyecto.

La dimensión humana, se refiere a la dimensión intelectual de adquisición del software, la dimensión más crítica, pues el desarrollo del software es actividad intelectual. Esta dimensión aborda el aspecto individual, del equipo, la gestión y el stakeholder[5] (incluyendo los usuarios y los clientes).

La dimensión metodológica está dirigida a la adquisición y desarrollo de software.

[5] Stakeholder o Representante, aunque suele usarse el término en inglés.

1.6.3 Modelo de Hall

Este modelo define dos actividades principales: la evaluación y el control del riesgo. La GR en este modelo genera una estrategia para decidir qué hacer en cada momento y está basada en nueve teorías(16):

- Razona sobre la vulnerabilidad-probabilidad de riesgo usando las *Teorías de probabilidad*, de incertidumbre y la de portfolio.
- Razona sobre el impacto-consecuencia del riesgo, usando las *Teorías de la utilidad*, de juegos, del caos y/o la creatividad.
- Combina vulnerabilidad e impacto en el tiempo, usando la *Teoría de la decisión* y el Teorema de Bayes para elecciones dinámicas.

El Modelo 6-D, de las 6 disciplinas PPMMDD (Planear, Producir, Medir, Mejorar, Diseñar, Descubrir) soporta la mejora continua del proceso SEI (Humphrey) modelo de madurez de procesos en el desarrollo de software CMM (Capability Maturity Model) que es un método de definir y gestionar los procesos a realizar por una organización. Las disciplinas son las siguientes:

- Diseñar: transformar ideas en objetivos, creando y difundiendo la visión organizacional (CMM nivel 1)
- Planear: confrontar los recursos disponibles y los requerimientos derivados de los objetivos del proyecto (CMM nivel 2)
- Producir: implementar el plan para lograr el producto (CMM nivel 3)
- Medir: comparar los resultados esperados y los realiza (CMM nivel 4)
- Mejorar: aprender de experiencias como cambiar el plan (CMM nivel 5)
- Descubrir: concienciar sobre el futuro, razona sobre posibilidades con resultados inciertos buenos (oportunidades) o malos (riesgos).

Este modelo amplía el concepto del riesgo en sentido revolucionario de oportunidad (entendiendo oportunidad como consecuencias positivas) y soporta la mejora continua (modelo basado en la conciencia del pasado) y la reingeniería (modelo basado en la conciencia de futuro). Pero no se debe elegir entre ambos modelos pues sólo la coexistencia de la conciencia de pasado y futuro con el ciclo completo PPMMDD optimiza productos existentes y capitaliza nuevas oportunidades.

1.6.4 Modelo de McFarlan

Tras considerar las 5 consecuencias clásicas del riesgo (fracaso en beneficios, coste, plazo del proyecto, rendimiento y compatibilidad con otros sistemas), define tres factores de riesgo(17):

1. Experiencia en la tecnología aplicable (factor subjetivo interno): la familiarización del equipo con

el hardware, sistema operativo, gestores (DB, DC) y lenguajes comprendiendo también la absorción de experiencia externa, como puede ser la formación.

2. Estructuración del proyecto (factor subjetivo externo): Los objetivos iniciales del proyecto y sus resultados dependen de la claridad de los requerimientos trasladados por la organización *cliente* al equipo de desarrollo.
3. Tamaño del proyecto (factor objetivo, no reducible): Importa sobre todo la envergadura del proyecto (en coste años-hombre) relativo al tamaño de los que el equipo desarrolla normalmente.

Se definen además en el modelo, cuatro grupos de salvaguardas:

Integración interna (en el equipo): fortalecimiento del equipo técnico mediante mecanismos de comunicación y control, jefatura experimentada, trabajo conjunto anterior, reuniones, actas, revisiones técnicas, participación en objetivos y asistencia externa.

Integración externa (con los clientes-usuarios): implicación de los clientes o usuarios en el proyecto mediante la comunicación en varios niveles, autoformación, autoinstalación, participación en los cambios, decisión de fechas clave y proceso de aprobación.

Planificación formal: estimación previa de secuencias-recursos (hitos, normas, aprobación, auditoría) y definición clara de las reuniones de evaluación.

Control formal de resultados: control de la ejecución mediante mecanismos de estima del progreso y no conformidades, acciones correctoras a tiempo (informes, disciplinas de control de cambios, reuniones en los hitos, informes de desvíos al plan).

1.6.5 Metodología DriveSPI

La metodología de Gestión de Riesgo "*DriveSPI* "surge como resultado de aplicar metodologías de gestión de riesgos en varios proyectos piloto (distintos proyectos de desarrollo de software).

La metodología DriveSPI consta de los siguientes pasos:

- Establecer y mantener alcances y estrategias de gestión de riesgos.
- Identificar, documentar y clasificar riesgos.
- Definir métricas de riesgo.
- Desarrollar estrategias de mitigación.
- Monitorear y controlar riesgos.
- Mejorar prácticas de gestión de riesgos.

1.6.6 Eurométodo

El Eurométodo es un proyecto de la Comisión Europea, cuyos primeros planteamientos datan de 1989, y que culminó con el Eurométodo v.1.1 en 1996. Este marco metodológico ayuda a planificar y desarrollar contratos de proyectos y servicios referentes a sistemas de información.(16; 18; 19)

Las tres orientaciones principales actuales de Eurométodo son:

Apoya la relación contractual entre clientes y proveedores de Sistemas de Información, lo que origina un Dominio del contrato. Trata dos dominios básicos:

- El Dominio[5] Objetivo de la adaptación del Sistema de Información (SI) contiene los procesos de las unidades organizativas y/o áreas de actividad funcional de la Entidad.
- El Dominio del proyecto es otra organización, temporal, para realizar la adaptación del Sistema de Información del Dominio destinatario.

Proceso de contratación orientado a los productos entregables, claves en el proceso de producción de un SI ya que son la causa de que el proyecto exista y soportan las decisiones. Algunos, establecidos como objetivo del contrato. Son particularmente importantes: debe ser perfecto el mutuo entendimiento entre cliente y proveedor de sus fines, significado y contenido. Para el cliente, los productos importan más que las tareas para obtenerlos (el qué importa más que el cómo). Para el proveedor importan también los medios para elaborar los productos.

Eurométodo prepara y ordena rigurosamente con una Estrategia y con Planes de entregas sucesivos el esqueleto de las relaciones cliente/proveedor en todo el proceso de desarrollo del contrato (sobre todo en la fase de producción de la adaptación del SI).

1.6.7 Metodología desarrollada por PMI para la gestión de riesgos.

El Instituto de Administración de Proyectos (Project Management Institute PMI) es una organización mundialmente reconocida, su metodología de gestión de proyectos es muy específica y detallada, además ha sido utilizada y aplicada en las diferentes industrias, esta metodología es la más completa en cuanto a las funciones básicas que deben tenerse en cuenta para realizar una gestión de riesgos eficiente**.**

Esta metodología consta de cinco procesos. Es necesario considerar que cada uno de estos procesos ocurren generalmente al menos una vez en cada fase del proyecto. La siguiente figura presenta los procesos que se deben llevar a cabo para la gestión de riesgos según PMI.(20)

Ilustración 3: Procesos para la Gestión de Riesgo según PMI.

Entre los proyectos pueden existir algunos que tengan más o menos riesgos que otro. Es claro que los proyectos se desarrollan para que una organización alcance un objetivo que le proporcione ciertos beneficios. Pero desafortunadamente siempre van a surgir algunas indecisiones en torno al proyecto que pueden incidir de forma negativa en el logro del objetivo.

Muchos profesionales poseen un concepto erróneo del análisis y la gestión de riesgos y, en alguno de los casos, consideran esta actividad necesaria pero aburrida. Además piensan que solo se debe efectuar al comienzo de un proyecto y no es así. Los cambios continuos en el proyecto y en el entorno operativo obligan a los equipos a realizar valoraciones frecuentes del estado de los riesgos existentes y a actualizar de nuevo los planes para prevenir o actuar ante los problemas asociados a estos riesgos. Las actividades de gestión de riesgos deben integrarse en el ciclo de vida general del proyecto proporcionando la actualización de los planes y actividades del control de riesgo apropiadas.

No se trata, de enriquecer la gestión de riesgos dentro de un proyecto, sino, ante todo, combatir aquellos desarrolladores, que tristemente son la mayoría, que prescinden de esta etapa de la gestión de proyecto. Se habla en términos de educar a los equipos de trabajo a comenzar la gestión del

producto por la gestión de sus riesgos, se trata de hacerlos comprender la importancia de este proceso, de que se demuestren a ellos mismos como desarrolladores que el tiempo invertido en identificar, prevenir, combatir los riesgos, planificar los planes de contingencia, no es más que ganar en calidad y resultados de sus software.

1.6.8 Magerit.

Otro método que se utiliza es el **MAGERIT** "Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información de las Administraciones Públicas", es un método formal para investigar los riesgos que soportan los sistemas de información, y para recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos.

Este método ha sido elaborado por un equipo del Comité Técnico de Seguridad de los Sistemas de Información y Tratamiento Automatizado de Datos Personales, del Consejo Superior de Informática en España.

La versión 1.0 de MAGERIT se presenta en siete guías metodológicas:

Guía de Aproximación: Presenta los conceptos básicos de seguridad de los sistemas de información, con la finalidad de facilitar su comprensión por personal no especialista y ofrece una introducción al núcleo básico de MAGERIT, constituido por las Guías de Procedimientos y de Técnicas.

Guías de Procedimientos: Representa el núcleo del método, que se completa con la Guía de Técnicas. Ambas constituyen un conjunto autosuficiente, puesto que basta su contenido para comprender la terminología y para realizar el Análisis y Gestión de Riesgos de cualquier sistema de información.

Guías de Técnicas: Proporciona las claves para comprender y seleccionar las técnicas más adecuadas para los procedimientos de análisis y gestión de riesgos de seguridad de los sistemas de información.

Guía para Responsables del Dominio protegible: Explica la participación de los directivos "responsables de un dominio" en la realización del análisis y gestión de riesgos de aquellos sistemas de información relacionados con los activos cuya gestión y seguridad les están encomendados.

Guía para Desarrolladores de Aplicaciones: Está diseñada para ser utilizada por los desarrolladores de aplicaciones, y está íntimamente ligada con la Metodología de Planificación y Desarrollo de Sistemas de Información, Métrica v2.1.

Arquitectura de la información y especificaciones de la interfaz para el intercambio de datos: La interfaz para intercambio de datos posibilita que un usuario de MAGERIT establezca la comunicación con otras aplicaciones y sistemas facilitando la incorporación de sus productos a la herramienta MAGERIT y viceversa.

Referencia de Normas legales y técnicas: Lista de normas en materia de seguridad a fecha 31 de Diciembre de 1996.(21)

Magerit persigue los siguientes objetivos:(21)

1 Concienciar a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo.
2 Ofrecer un método sistemático para analizar tales riesgos.
3 Ayudar a descubrir y planificar las medidas oportunas para mantener los riesgos bajo control.
4 Apoyar la preparación a la Organización para procesos de evaluación, auditoria, certificación o acreditación, según corresponda en cada caso.

4.2.1 Modelo para GR en PDSW (MoGeRi)

Este fue un modelo concebido por la profesora Yeleny Zulueta en su tesis de maestría, para la GR en la producción de software de la UCI, donde se valoró todos los aspectos que caracterizan el desarrollo de software en la universidad. Además es un modelo con una estructura fácil de implementar y muy explicativa y abarcadora, durante los 6 procesos que conforman el modelo se le da un seguimiento secuencial y continuo a los riesgo durante todo la vida del proyecto y algo fundamental cumple con los estándares de calidad impuesto a nivel internacional en la GR. Una de los aspectos más importantes que tiene este modelo es que a diferencia de SEI y PMI que son modelos que incluyen entre su metodología un procesos para la comunicación de la información, el modelo GR en PDSW en la UCI incluye en la culminación de cada proceso la comunicación de la información y además tiene un proceso definido para eso, esto a pesar de parecer un poco recalcitrante es muy efectivo pues mantiene en todo momento al equipo de desarrollo informado del estado de los riesgos del proyecto.

El modelo propuesto consta de seis procesos que se muestran en la Ilustración 4:(13)

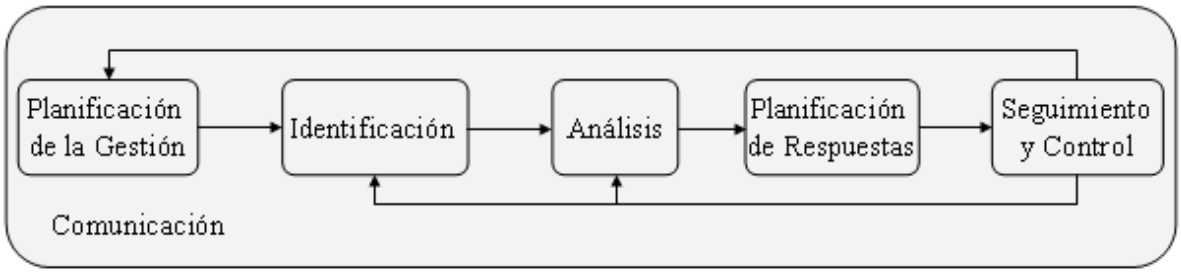

Ilustración 4: Submodelo de procesos[6] MoGeRi.

4.2.2 Breve Resumen

La siguiente tabla muestra los diferentes métodos de gestión de riesgos mas considerablemente conocidos y de fácil acceso por sus nombres o por las organizaciones que los avalan: Euromethod,

Safe, SEI-CRM, Risklt y los métodos para la gestión de riesgos del IEEE y del PMI (Project Management Institute), también le agregamos el método MoGeRi de la UCI. Es sumamente importante destacar que cada método establece categorías para las funciones del riesgo en diferentes fases. Esta tabla describe las categorías de cada método.(12)

Categorías	Eurométodo	Safe	SEI	IEEE	Riskit	PMI	MoGeRi
Plan de Gestión		x				x	x
Identificación	X		x	x	x	x	x
Estimación	X		x	x	x	x	x
Evaluación	X	x	x	x	x	x	x
Planificación	X	x	x	x	x	x	x
Tratamiento	X	x	x	x	x	x	x
Seguimiento y control	X	x	x	x	x	x	x
Comunicación			x				x

Tabla 2: Métodos de Gestión de Riesgos y sus categorías.

1.7 Tratamientos de Riesgos en RUP.

El Proceso Unificado de Desarrollo de Software (RUP) es una metodología guiada por casos de uso, centrados en la arquitectura, iterativos e incrementales. RUP plantea que el primer paso hacia la división del proceso de desarrollo de software, consiste en separar las partes en cuatro fases atendiendo al momento en que se realizan: inicio, elaboración, construcción y transición. Cada una de las fases se divide en una o más iteraciones.

RUP propone crear una lista de riesgo en la fase de inicio. Al principio esto puede ser difícil por la falta de información pero conforme se va realizando el trabajo inicial se va apreciando cuáles serán los riesgos críticos aquellos que han de ser mitigados para poder ofrecer una planificación y un coste y para determinar un objetivo de calidad.

La Lista de Riesgos es desarrollada junto con los Casos de Negocio, los cuales formarán la base para la decisión de continuar o no con el proyecto. La Lista de Riesgos es mantenida a través de todo el ciclo de vida del proyecto.(22)

Para facilitar la administración de la lista de riesgos, se plantea seguir el siguiente esquema:

- **Descripción**: Comienza con una breve descripción y se van añadiendo detalles conforme se va aprendiendo.
- **Prioridad**: Se le asigna una prioridad al riesgo: crítico, significativo o rutinario
- **Impacto**: Qué partes del proyecto o del sistema se verán afectados por el riesgo.
- **Monitor**: Quién es responsable del seguimiento de un riesgo persistente.
- **Responsabilidad**: Qué individuo o unidad de la organización es responsable de eliminar el riesgo.
- **Contingencia**: Lo que ha de hacerse en caso de que el riesgo se materialice.

Al explicar los pasos a seguir en cada fase del proyecto, en RUP se perciben las siguientes actividades relacionadas con los riesgos:

1. **Inicio**: identificar los riesgos críticos, es decir, los que afectan la capacidad de construir el sistema y determinar si puede encontrarse una forma de mitigarlos, quizás en una etapa posterior. En esta fase se consideran solo los riesgos que afectan la viabilidad del sistema. Los no críticos son colocados en la lista de riesgos.
2. **Elaboración**: identifica los riesgos significativos, los que podrían perturbar los planes, costes y planificaciones de fases posteriores y los reduce a actividades que pueden ser medidas y presupuestadas
3. **Construcción**: materializar la monitorización de los riesgos críticos y significativos arrastrados desde las dos primeras fases y su mitigación.
4. **Transición**: no se definen tareas relacionadas con los riesgos.

1.8 GR en modelos de calidad.

ISO/IEC 12207

ISO/IEC 12207 es una norma técnica que establece un marco de referencia común para los procesos del ciclo de vida del software con una terminología bien definida. Contiene procesos, actividades y tareas para aplicar durante la adquisición de un sistema que contiene software, un producto software puro o un servicio software y durante el suministro, desarrollo, operación y mantenimiento de productos software.

Define los procesos de ingeniería de software como: “un conjunto de actividades que son realizadas por un conjunto de tareas que definen como las acciones transforman las entradas en salidas”.(22)

Los procesos que se emplean son: los procesos principales, los procesos de apoyo y los procesos organizativos del ciclo de vida.

Dentro de los procesos organizativos del ciclo de vida se incluye la Gestión de Riesgos(GR) que tiene en este caso el propósito de identificar, analizar, tratar y monitorear los riesgos continuamente(23). Para su exitosa implementación se deben realizar las siguientes actividades:

1. Determinar el alcance de la GR a ser ejecutado.
2. Definir e implementar estrategias apropiadas para la GR.
3. Identificar los riesgos en la planificación de proyectos.
4. Analizar los riesgos en términos de probabilidad y consecuencias y determinar la prioridad en el tratamiento de estos riesgos.
5. Definir, aplicar y evaluar las mediciones de riesgos para determinar los daños, el estado del riesgo y el progreso de las actividades de tratamiento.
6. Seguir el tratamiento apropiado para corregir o evitar el impacto del riesgo basados en su prioridad, probabilidad y consecuencia u otros principios de riesgo definido.

CMMI

El CMMI (Capability Maturity Model Integrated) se ha convertido en el nuevo estándar a nivel mundial para la medición de la calidad de los procesos de desarrollo de software(22). Este modelo de calidad del software clasifica las empresas en niveles de madurez y capacidad.

Nivel 1 Inicial: El proceso es informal.

Nivel 2 Gestionado: Se institucionalizan las particas de Gestión de Proyecto.

Nivel 3 Definido: Las prácticas técnicas se integran con las técnicas de gestión y se institucionalizan.

Nivel 4 Gestionado Cuantitativamente: el producto y el proceso se controlan cuantitativamente.

Nivel 5 Optimizado: Se institucionaliza la mejora del proceso.

En el nivel 2, en el Área de Proceso de Planificación de Proyectos se plantea que el plan debe incluir la *identificación y análisis de los posibles riesgos que pueda tener el proyecto*; pero la GR, como área de procesos, se contemplada en el nivel 3. Tiene como objetivo *identificar los problemas antes de que ocurran, y así planificar las actividades de administración de riesgos según lo que se necesite a través de los ciclos de vida del proyecto y atenuar impactos adversos en la obtención de los objetivos.*

Para llevar a cabo una exitosa GR, CMMI plantea las siguientes metas y tareas[7] Específicas.

Tareas Genéricas

1. Prepararse para la GR.
2. Identificar y analizar los riesgos.
3. Mitigar riesgos.
4. Análisis y resolución de toma de decisiones.

Tareas Específicas

1. Determinar las fuentes y categorías de los riesgos.
2. Definir los parámetros de los riesgos.
3. Establecer la estrategia de GR.
4. Identificar riesgos.
5. Evaluar, categorizar y priorizar los riesgos.
6. Desarrollar los planes de la mitigación del riesgo.
7. Implementación del plan de GR.

1.9 Conclusiones

La Gestión de Riesgos es un elemento fundamental dentro del proceso de desarrollo de software, ya que permite mantener controlados los posibles problemas que pueden aparecer durante el desarrollo del proyecto de software, dado que un riesgo es simplemente eso, un potencial problema. Si el riesgo se convierte en un problema, y en el proceso de software se contempla la Gestión de Riesgo, se tendrá ya determinado un plan de acción para atacar el inconveniente en cuestión no dejando que el mismo haga peligrar la finalización del proyecto. Caso contrario se deberá pensar en ese momento que se puede hacer para mitigar el problema.

Actuar frente a un riesgo de esta forma es actuar de una forma Reactiva, mientras que si aplicamos Gestión de Riesgo es actuar de una forma Proactiva. Esto se instrumenta mediante la aplicación de diferentes metodologías específicas como se ha visto en este capítulo que permite llevar adelante una acción proactiva sintetizándola de la siguiente forma:

- Identificar los riesgos desde un comienzo, y responsabilizar a una persona por cada uno.
- Clasificar, priorizar, para identificar sobre cuales riesgos prestar mayor atención.
- Definir un plan de acción para el caso que el riesgo se convierta en problema.
- Controlar los riesgos de mayor impacto y probabilidad de ocurrencia.
- Llevar documentación de cada riesgo y las acciones tomadas.

En este capítulo, se trataron profundamente los procesos que abarca la Gestión de Riesgo en la esfera de desarrollo de software, determinando los conceptos fundamentales de esta área del conocimiento, así como sus métodos utilizados. Se llegó a la conclusión que para los proyectos de desarrollo de software es una necesidad imperiosa realizar el proceso de Gestión de Riesgo, por tanto los mismos empezando deben trabajar sobre la base de educar a los equipos de desarrollo de software a comenzar la Gestión del Proyecto con la Gestión de los Riesgos, ya que el esfuerzo que les llevará comprender y aplicar la Gestión de Riesgo lo podrán entender después en la satisfacción de sus clientes, la calidad de sus productos y procesos.

CAPÍTULO 2: ANÁLISIS DE LOS ENFOQUES DE LA GR ESTUDIADOS. MODELO MoGeRi.

2.1 Introducción

En este capítulo se realiza un análisis de los enfoque de los modelos de GR estudiados en correspondencia con las necesidades y acciones en el proyecto SIGEP. Además se realizará un estudio detallado del modelo que se aplicará (MoGeRi) al proceso de Gestión de Riesgos en el proyecto SIGEP.

2.2 Análisis para la selección de la metodología

Después de razonar sobre la situación problémica presentada, el problema y teniendo en cuenta el estudio de los modelos existentes para la GR, se identifican algunos elementos importantes a tener en presente en la selección del modelo (MoGeRi):

Los modelos adscritos a la G1[6], se limitan solo a la identificación de los riesgos y la toma de medidas para enfrentar o mitigar el riesgo de forma general. La GR en el proyecto SIGEP, precisa mucho más, no basta con identificar los eventos que pueden afectar los procesos y productos y comportarse de manera reactiva.

Los modelos adscritos a esta generación (G3)[7], revolucionariamente proponen gestionar el proyecto por sus riesgos, sin embargo podría ser este un paso muy novedoso pero peligroso para el proyecto SIGEP por la poca experiencia que tiene el equipo de desarrollo en la gestión por lo que el trabajo en equipo no es lo suficientemente sólido.

Teniendo en cuenta que los modelos de la generación G2[8] más usados a nivel internacional por su reconocimiento, integralidad, actualidad y aplicación internacional son SEI y PMI ¿Por qué no apostar por ellos?

El modelo del Software Engineering Institute (SEI) presenta una completa pero compleja estructura para ser íntegramente implementado en el proyecto SIGEP debido a la poca experiencia del equipo de desarrolladores en la organización del proyecto según los riesgos.

La metodología del Project Management Institute (PMI) no fue concebida sobre la base de proyectos de software sino industriales. Sin embargo propone una estructura bien definida para la GR con datos de entrada, herramientas y técnicas y datos de salida bien definidos para sus procesos, aunque no trabaja como el SEI, las actividades de comunicación que tan necesarias son en SIGEP por el carácter

[6] Primera generación de Gestión de riesgo.

[7] Tercera generación de Gestión de riesgo.(Actualmente)

[8] Segunda generación de Gestión de riesgo.

docente de la producción. El PMI trabaja además de manera profunda la etapa de la planificación de la GR como parte de la planificación del proyecto.

¿Por qué no adoptar simplemente las acciones propuestas por RUP?

RUP no propone las actividades de GR formalmente en los flujos de trabajo y estas no completan todo un proceso sino que se centran más en la identificación de riesgo.

¿Por qué MoGeRi?

Este Modelo está situado en la frontera entre G2 y G3, tomando las mejores prácticas de ellos y permitiendo una fácil implementación del mismo para el equipo de desarrollo con poca experiencia en la GR (SIGEP). Fue creado para ser usado en el proceso productivo de la Universidad de la Ciencias Informáticas (UCI), por lo que se ajusta perfectamente a las necesidades del proyecto SIGEP. Una de sus fortalezas es que potencia la comunicación de experiencias verticalmente en ambos sentidos para un mejor funcionamiento y organización del equipo de desarrolladores, además MoGeRi crea la base para comenzar la gestión de riesgo desde la etapa conceptual del proyecto. Incluye la planificación de la gestión de Riesgo en la Planificación del Proyecto; siendo esta una fase que se suele violentar en nuestro proceso productivo, por lo que adoptándola como proceso inicial en la GR, apoya y refuerza la Planificación de los Proyectos.

2.3 Modelo para GR en PDSW. MoGeRi

Lo principal para el triunfo de un proyecto es la capacidad que tenga el equipo de proyecto para ocuparse con eficacia de los riesgos que forman parte de cada proceso de desarrollo del producto.

Muchos proyectos de desarrollo de software no realizan una buena gestión de riesgos o simplemente ni la hacen. No utilizan ninguna metodología y debido a esto están relacionados con una serie de riesgos que requieren de un plan de administración bien documentado y establecido; entonces es aquí donde vemos la verdadera importancia del proceso de gestión de riesgo, ya que este permite planificar y prevenir los riesgos que pueden surgir en un proyecto y lograr así una buena gestión de proyecto y que el cliente se sienta bien con el producto final.

Es importante decir que no existe ninguna metodología universal que garantice el éxito completamente de un proyecto de desarrollo de software, toda metodología debe ser adaptada al proyecto donde se va utilizar.

El *Modelo MoGeRi* consta de seis procesos. A continuación se explicarán detalladamente cada uno de ellos sus actividades y tareas. Estos procesos pueden involucrar el esfuerzo de uno o más individuos o grupos de individuos basado en las necesidades del proyecto y pueden ocurrir generalmente al menos una vez en cada fase del proyecto. **(Ver Anexo 1)**

2.3.1 Especificación de los participantes.(13)

Promotor: Es una figura singular encargada de perfilar la oportunidad de la GR. Debe ser una persona con visión de la GR dentro de un proyecto de software.

El promotor tiene su papel en la tarea P1A1T1.

Gestor de Riesgos: Es el encargado de guiar y dirigir los procesos en función de lograr una GR exitosa. Los gestores que obtienen resultados favorables mantienen un alto nivel de disciplina a la hora de adoptar decisiones; ello no significa que sean dogmáticos y burocráticos, sino que el gestor:

- Se asegura que se delimita debidamente el alcance de la situación.
- Identifica y valora los riesgos.
- Identifica opciones válidas para reducir el riesgo a un nivel aceptable.
- Recoge información apropiada y válida para valorar el riesgo y las opciones, además para supervisar el riesgo.
- Utiliza razonamientos bien fundados al realizar los intercambios.
- Se decide por una línea de acción concreta.

El Gestor de Riesgos se designa en P1A2T2.

Equipo de GR: Las responsabilidades de este equipo son:

- Llevar a cabo las tareas de GR.
- Recopilar, procesar y consolidar datos.
- Elaborar los informes previstos en el desarrollo de los procesos.

El Equipo de GR se determina en P1A2T3 y sus tareas se formalizan en P1A3T2.

Comité de Seguimiento y Control: Las responsabilidades de este comité son:

- Resolver las incidencias durante el desarrollo de la GR en el proyecto.
- Asegurar la disponibilidad de recursos humanos con los perfiles adecuados y su participación en las actividades donde es necesaria su colaboración (por ejemplo, la capacitación para la identificación de los riesgos).
- Cumplimentar los hitos de GR y su influencia en la línea de base del proyecto.
- Cumplir las tareas asignadas para el seguimiento y control de la GR en el proyecto.

El comité puede estar integrado por quienes desempeñan roles que en el proyecto, están también relacionadas con el seguimiento y el control de forma general, no necesariamente tiene que ser creado con el propósito exclusivo de seguir y controlar solo las actividades relacionadas con la GR si estas se desarrollan en el seno del proyecto.

2.3.2 Descripción de los procesos, actividades y tareas.

Proceso P1 Planificación de la Gestión de los Riesgos.

La planificación es el proceso de decidir cómo enfocar, planificar y ejecutar las actividades de GR para el proyecto. El objetivo principal de este proceso es establecer el marco general de referencia para la realización de la GR y por qué no, como apoyo para determinar la viabilidad del proyecto, si se realizan inscritas en la etapa de planificación del mismo. Además, la planificación permite motivar e involucrar a la Dirección o Gerencia del Proyecto, sobre la base de razonar la oportunidad de realizar la GR y además permite crear las condiciones humanas y materiales para su buen desarrollo.(13)

Actividad P1A1 Estudio de oportunidad.

Tarea P1A1T1 Determinar la oportunidad.

Actividad P1A2 Determinación del alcance del proyecto.

Tarea P1A2T1 Objetivos y restricciones generales.

Tarea P1A2T2 Determinar dominio y límites.

Tarea P1A2T3 Identificación del entorno.

Actividad P1A3 Planificación de la GR.

Tarea P1A3T1 Planificar el trabajo.

Tarea P1A3T2 Determinar los recursos necesarios

Actividad P1A4 Factibilidad de la GR.

Tarea P1A4T1 Estimar costos y beneficios de la GR.

Tarea P1A4T2 Decidir la realización de la GR.

Actividad P1A5 Comunicación de resultados.

Tarea P1A5T1 Comunicar resultados al equipo del proyecto.

Tarea P1A5T2 Documentar experiencias.

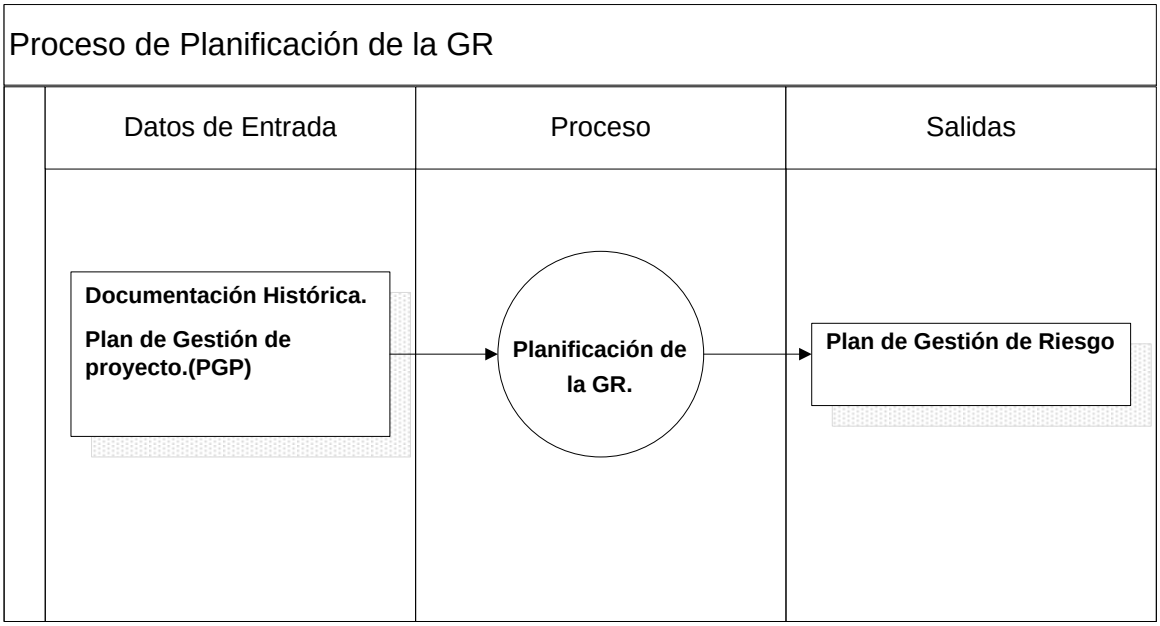

Ilustración 5: Entradas y Salidas del proceso Planificación de la GR.

Herramientas y Técnicas*:*

Reuniones*:* Realizar reuniones para analizar cómo se va a efectuar la planificación de las actividades relacionadas con la Gestión de Riesgos en los proyectos, para elaborar el plan de gestión de riesgo. En estas reuniones participa el Líder del proyecto y los directivos del equipo de desarrollo.

Entrevistas: Realizar entrevistas al equipo de desarrollo del proyecto para saber sus opiniones acerca de la GR.

Entrada:

Documentación histórica del proyecto: Documento Visión y Proyecto Técnico General.

Plan de Gestión del Proyecto (PGP).

Salidas:

Plan de Gestión de Riesgos: En este plan se van a planificar las actividades a ejecutar durante la Gestión de riesgo, así como definir las categorías a usar para clasificar los riesgos y definir los niveles de probabilidad e impacto que se van a utilizar en el proceso de análisis.

Proceso P2 Identificación de los Riesgos.

Consiste en determinar qué riesgos tienen probabilidad de afectar el proyecto y documentar las características de cada uno. No es un proceso que ocurra una sola vez sino que deberá ser ejecutado según una base regular sobre la duración del proyecto y/o según los resultados del Seguimiento y Control de los riesgos.(13)

El proceso consta de las siguientes actividades y tareas:

Actividad P2A1 Selección de herramientas y técnicas a aplicar.

Tarea P2A1T1 Capacitar acerca de herramientas y técnicas.

Tarea P2A1T2 Analizar información histórica.

Tarea P2A1T3 Seleccionar herramientas y técnicas.

Actividad P2A2 Identificación de riesgos.

Tarea P2A2T1 Identificar los riesgos.

Tarea P2A2T2 Caracterizar los riesgos.

Actividad P2A3 Comunicación de resultados.

Tarea P2A3T1 Comunicar resultados al equipo del proyecto.

Tarea P2A3T2 Documentar experiencias.

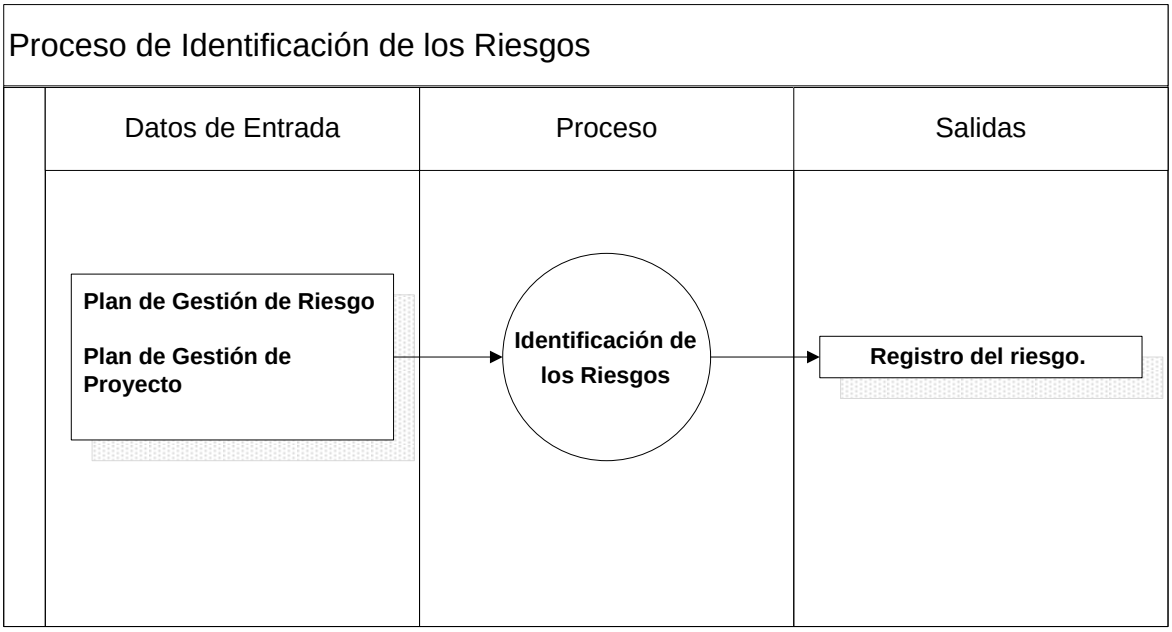

Ilustración 6: Entradas y Salidas del proceso Identificación de la GR.

Entradas:

Plan de Gestión de Riesgo: Este artefacto sirve como entrada al proceso de identificación de riesgos, pues en este plan quedaron definidas las responsabilidades y los roles que iban a llevar a cabo el proceso de gestión de riesgo, además de las categorías del riesgo y las actividades de gestión de riesgo necesarias a realizar en esta fase.

Plan de Gestión de Proyecto: El proceso de identificación de riesgo también requiere una comprensión del horario, costo, y los planes de gestión de la calidad encontrados en el plan de gestión de proyecto.

Herramientas y Técnicas:

Lluvia de ideas: Creada en el año 1941 por Alex Osborne. La lluvia de ideas (brainstorming) es la manera de aprovechar la energía y el conocimiento individual de un equipo de trabajo que puede generar un sin número de ideas originales y soluciones a problemas de un tema específico, en un corto periodo de tiempo y en un ambiente relajado. El objetivo principal de la lluvia de ideas es "generar alternativas" para la soluciones de los problemas propuestos.

Encuestas, entrevistas, cuestionarios: La utilización de cualquiera de los tres procedimientos es válida en aras de la identificación de riesgos por medio de la participación de interesados en el proyecto que pueden ayudar a identificar los riesgos que no fueron tenidos en cuenta en la etapa de planeación.

Listas de chequeo y apuntes: Las listas de chequeo para la identificación de riesgos se pueden desarrollar con base en registro histórico, la información y el conocimiento que han sido acumulados de proyectos anteriores y similares de otras fuentes de información. La ventaja de conformar una lista de chequeo es que la identificación de riesgo se hace de manera fácil y rápida, su desventaja es la difícil forma de configurar una lista lo suficientemente completa para que el usuario no quede limitado por las categorías de la lista.

Clasificación del riesgo: Los riesgos en los proyecto se pueden categorizar por fuentes, el riesgo, del área del proyecto afectado u otras categorías; de esta forma se pueden determinar las áreas del proyecto más expuestas a los efectos de riesgo.

Salidas:

Registro del riesgo: El registro de riesgo es un documento que contiene los resultados de varios procesos de administración de riesgos, una herramienta para documentar eventos de riesgo potenciales e información relacionada. Eventos de riesgo se refieren a eventos específicos e inciertos que pueden ocurrir en beneficio o perjuicio del proyecto.

Proceso P3 Análisis de los Riesgos

Es el proceso de examinar los riesgos en detalle para determinar su extensión, sus interrelaciones y su importancia a través del análisis cualitativo y/o cuantitativo de la probabilidad de ocurrencia y el impacto asociados.

Es importante analizar la probabilidad de cada riesgo y sus consecuencias en los objetivos del proyecto, como también en el grado total del proyecto y distinguir cuáles son los riesgos que requieren atención urgente.(13)

El proceso consta de las siguientes tareas.

Actividad P3A1 Análisis cualitativo de los riesgos.

Tarea P3A1T1 Estimar la probabilidad y el impacto del riesgo.
Tarea P3A1T2 Priorizar los riesgos.
Actividad P3A2 Análisis cuantitativo de los riesgos.
Tarea P3A2T1 Cuantificar la probabilidad de ocurrencia del riesgo.
Tarea P3A2T2 Cuantificar el impacto del riesgo.
Tarea P3A2T3 Priorizar los riesgos.
Actividad P3A3 Análisis de los atributos del Riesgo.
Tarea P3A3T1 Verificar exactitud de los datos, estimaciones y cálculos realizados.
Actividad P3A4 Comunicar resultados.
Tarea P3A4T1 Comunicar resultados al equipo del proyecto.
Tarea P3A4T2 Documentar experiencias.

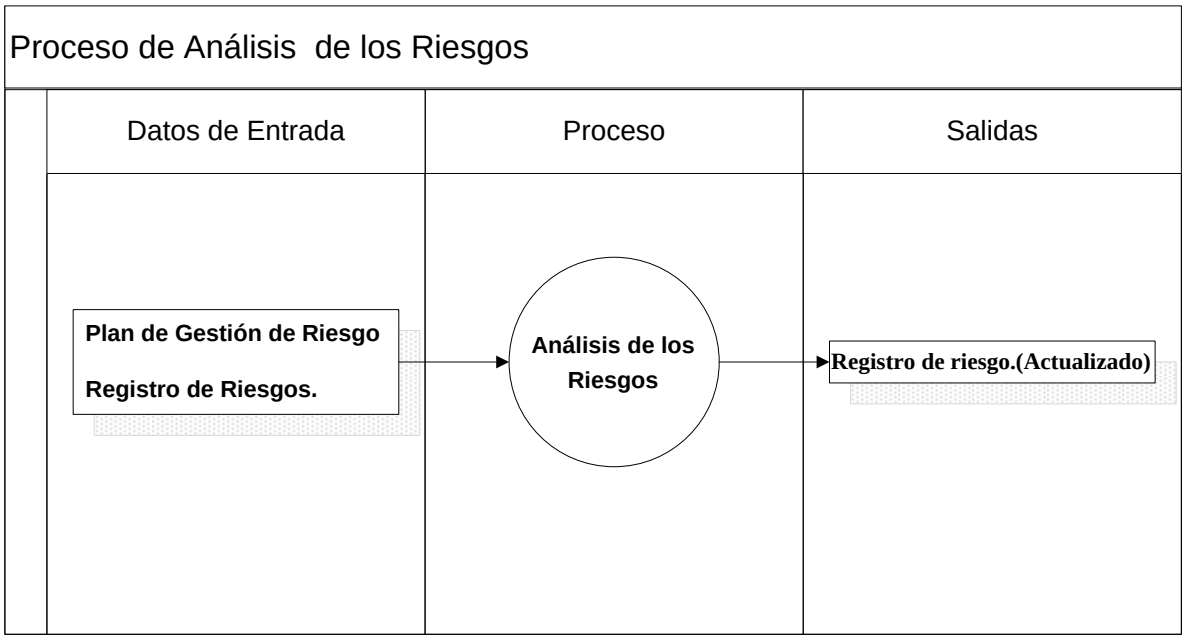

Ilustración 7: Entradas y Salidas del proceso Análisis de la GR

Entradas:

Plan de Gestión de Riesgos: En este plan quedan definidos los valores (escala) de dos elementos de suma importancia para realizar una eficiente gestión de riesgos; la probabilidad y el impacto, además queda definida la matriz de probabilidad e impacto del riesgo, dando paso a otro elemento muy importante la exposición al riesgo. Es válido destacar que si esta información no queda definida en el proceso de planificación de la gestión de riesgos, puede ser desarrollada entonces sin ningún problema en la fase del análisis cualitativo del riesgo.

Registro de Riesgos: es importante porque aquí se pueden ver los riesgos que fueron identificados y analizarlos.

Herramientas y Técnicas:

Definición de la Probabilidad e Impacto del riesgo: La probabilidad y el Impacto se determinan para cada riesgo identificado. La probabilidad del riesgo investiga la probabilidad con que ocurrirá cada riesgo específico. El impacto del riesgo investiga el efecto potencial sobre un objetivo del proyecto tal como tiempo, costo, alcance, o calidad, incluyendo los efectos negativos para las amenazas y los efectos positivos para las oportunidades. A veces, los riesgos con grados obviamente bajos de probabilidad e impacto no serán clasificados, sino serán incluidos en una lista para la supervisión futura.

Matriz de la probabilidad e impacto de los riesgos: Esta matriz especifica combinaciones de la probabilidad y el impacto que conducen a clasificar los riesgos como Críticos, Graves, Apreciables o Asumibles. Generalmente, estas reglas del grado de riesgo son especificadas por la organización antes del proyecto, e incluidas en los activos del proceso de la planificación.

Métodos para cuantificar la probabilidad como son: Árbol de decisión, Método de estado Natural y Análisis de sensibilidad.

Métodos para cuantificar el impacto como son: Sumas estadísticas, Simulación, Árboles de decisión y Opinión Experta.

Reuniones de Análisis: estas reuniones son muy importantes para priorizar los riesgos.

Salidas:

Registro de Riesgo (Actualizado): Se definen la probabilidad y el impacto para cada riesgo, se priorizan los riesgos según su efecto (Probabilidad x impacto) y se especifican los riesgos que requieren respuestas a corto plazo.

Proceso P4 Planificación de las Respuestas a los Riesgos.

El principal objetivo de la Planificación de las Respuestas a los Riesgos es desarrollar un plan detallado para controlar los riesgos más importantes identificados durante el análisis de riesgos e integrarlo en los procesos de gestión estándar del proyecto para garantizar su realización.

Las actividades de planificación convierten la lista de riesgos con prioridades en planes de acción. Esto implica desarrollar acciones para cada uno de los riesgos principales, establecer prioridades para las acciones de un riesgo, y crear un plan integrado de GR o sea, implementar las tareas en la programación del proyecto.(13)

El proceso consta de las siguientes actividades y tareas:

Actividad P4A1 Valoración de la estrategia para enfrentar el riesgo.

Tarea P4A1T1 Identificar estrategias viables frente al riesgo.

Tarea P4A1T2 Seleccionar estrategia para enfrentar el riesgo.

Actividad P4A2 Planificación de las Respuestas.

Tarea P4A2T1 Identificar respuestas según estrategia.

Tarea P4A2T2 Planificar respuesta.

Tarea P4A2T3 Valorar factibilidad de la respuesta.

Actividad P4A3 Comunicar resultados.

Tarea P4A3T1 Comunicar resultados al equipo del proyecto.

Tarea P4A3T2 Documentar experiencias.

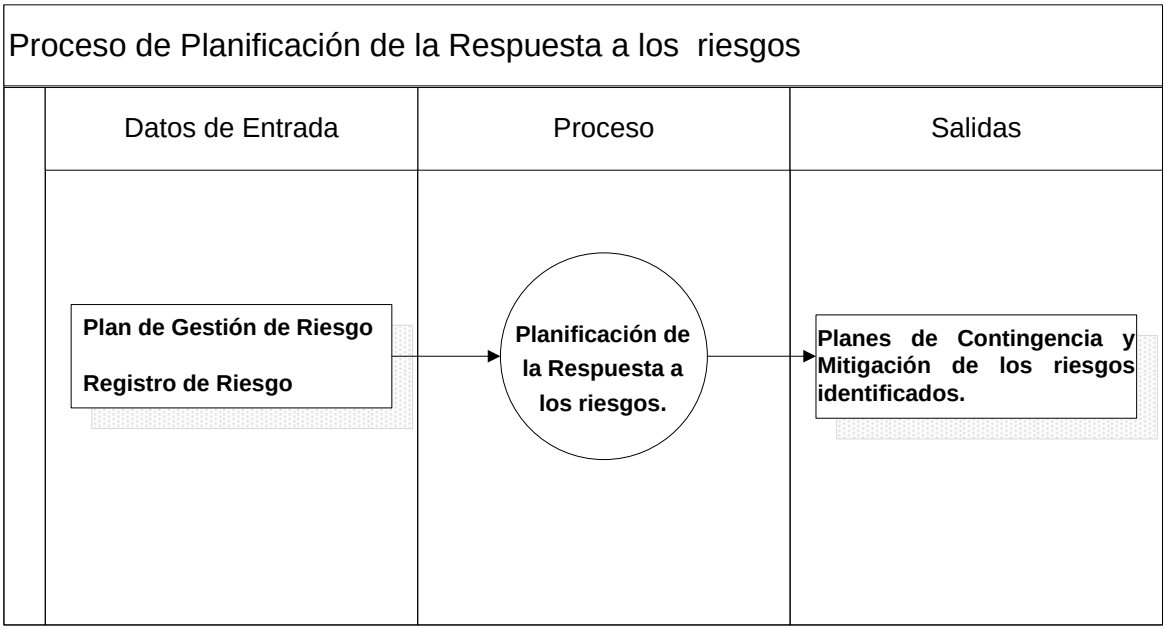

Ilustración 8: Entradas y Salidas del proceso Planificación de la respuesta a los Riesgos.

Entradas:

Plan de Gestión de Riesgo: Este plan incluye componentes importantes, por ejemplo se puede saber quién es el responsable de llevar a cabo el proceso de Planificación de la Respuesta al Riesgo en el proyecto, además de incluir las definiciones de los valores de la probabilidad y el impacto, de estos dos elementos se obtiene uno muy importante que es la exposición al riesgo, este último elemento permite poderle dar una prioridad al riesgo y por esa prioridad es que se van a elaborar las respuestas de los riesgos.

Registro de Riesgo: Podemos ver los riesgos mas críticos y empezar a darle respuestas a estos. (Actualizar el registro)

Herramientas y Técnicas:

Estrategias de Contingencia: Algunas respuestas se diseñan para que se usen solamente si ocurren ciertos acontecimientos. Para algunos riesgos, es apropiado que el equipo de proyecto haga un Plan de Contingencia que sea ejecutado solamente bajo ciertas condiciones predefinidas.

Estrategia para las amenazas y las oportunidades:

Aceptación: Esta estrategia se adopta cuando raramente es posible eliminar todo el riesgo de un proyecto.

Además indica que el equipo del proyecto ha decidido no cambiar el plan de gestión de proyecto para resolver el problema y simplemente acepta seguir trabajando con el riesgo o no puede identificar cualquier otra estrategia conveniente para darle respuesta.

Estrategias para los riesgos o las amenazas: Existen tres estrategias para los riesgos que pueden tener impactos negativos en los objetivos del proyecto, estas son: transferir, mitigar o evitar el riesgo:

Evitar. Evitar el riesgo implica elaborar medidas para eliminar la amenaza planteada por un riesgo adverso, para aislar los objetivos del proyecto del impacto del mismo o para relajar el objetivo que está en peligro.

Transferir: A veces un riesgo puede transferirse para que pueda ser administrado por otra entidad fuera del proyecto. La transferencia del riesgo no significa que el riesgo se haya eliminado, sino que generará riesgos que seguirán necesitando una gestión proactiva pero que reducen el grado de riesgo a un nivel aceptable.

Mitigar: La mitigación de riesgos implica acciones y actividades que se realizan con anticipación para evitar que se produzcan riesgos o para reducir el impacto y las consecuencias del mismo a un nivel aceptable.

Salidas:

Planes de Contingencia y Mitigación de los riesgos identificados: Consiste en elaborar medidas y estrategias de gestión de riesgos orientadas a minimizarlos o eliminarlos.

Proceso P5 Seguimiento y Control de los Riesgos.

El Seguimiento y control de los riesgos es esencial para la implementación de un PGR eficaz. Permite asegurar que las tareas que implementan medidas preventivas o planes de contingencia, se realizan en el tiempo previsto dentro de las restricciones de recursos del proyecto.

Las respuestas a los riesgos planificadas son incluidas en el PGP y ejecutadas durante el ciclo de vida del proyecto, pero el trabajo del Equipo de GR enmarcado en el proyecto, debe ser continuamente monitoreado con vistas a controlar el desenvolvimiento de los riesgos, tanto los nuevos, como las modificaciones en los ya identificados.

El Seguimiento y control de los riesgos involucra, ejecutar el PGR de manera que se dé respuesta a los eventos de riesgo sobre la vida del proyecto. Cuando ocurren los cambios, el ciclo básico de identificar, cuantificar y responder, es repetido. Es importante entender que hasta el análisis más completo y exhaustivo no puede identificar todos los riesgos y probabilidades de manera correcta; para esto se requiere control e iteración.(13)

El proceso consta de las siguientes actividades y tareas:

Actividad P5A1 Seguimiento de los riesgos

Tarea P5A1T1 Aplicar métricas para valoración de la calidad de procesos, técnicas y herramientas y resultados.

Tarea P5A1T2 Monitorear del estado de los riesgos.

Actividad P5A2 Control de los riesgos.

Tarea P5A2T1 Verificar cumplimiento de las respuestas a los riesgos.

Tarea P5A2T2 Verificar cumplimiento de los hitos de GR.

Tarea P5A2T3 Tomar decisiones sobre las pautas de GR.

Actividad P5A3 Comunicación de resultados.

Tarea P5A3T1 Comunicar resultados al proyecto.

Tarea P5A3T2 Documentar experiencias.

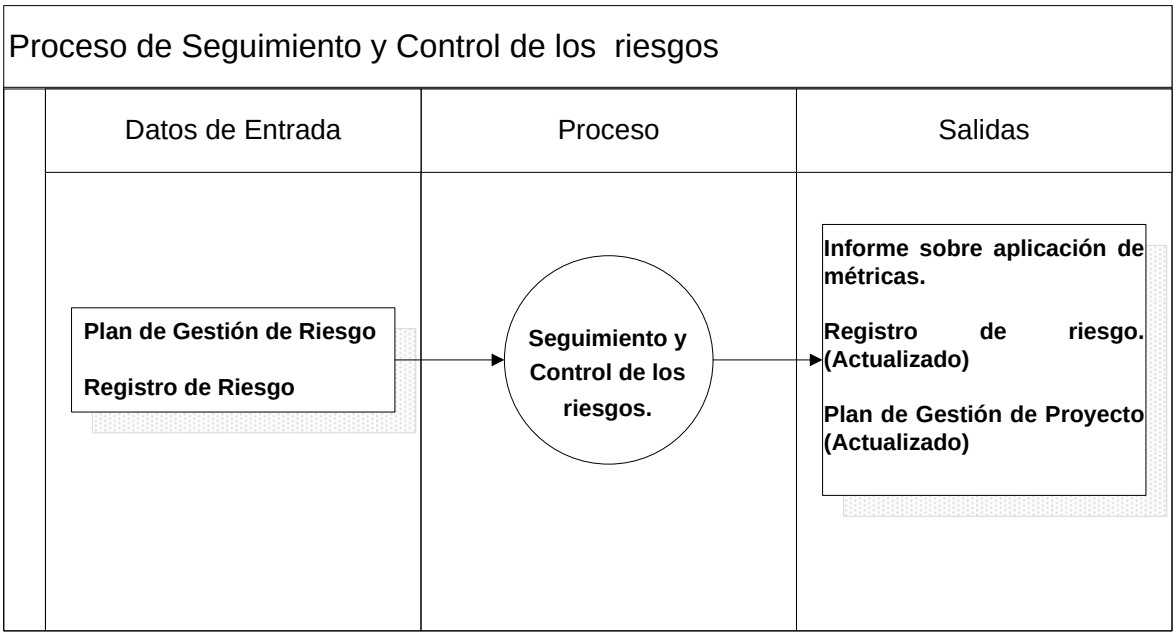

Ilustración 9: Entradas y Salidas del proceso Seguimiento y Control de la GR.

Entradas:

Plan de Gestión de Riesgos y Registro de los Riesgos: En esta fase es donde se le da seguimiento

a estos dos artefactos.

Herramientas y Técnicas:

Reanálisis del riesgo: La supervisión y el control del riesgo requiere a menudo la identificación de nuevos riesgos y la nueva valoración de estos, estas nuevas valoraciones de los riesgos en proyectos deben programarse regularmente.

Intervención del riesgo: Las intervenciones del riesgo examinan y documentan la eficacia de las respuestas del riesgo haciendo frente a riesgos ya identificados y a sus causas.

Reuniones del chequeo: La gestión de riesgo del proyecto puede ser un asunto del orden del día en las reuniones periódicas del proyecto, esta gestión de riesgos se convierte en cuanto más a menudo se practica más fácil, y las discusiones frecuentes sobre riesgos particularmente amenazas, se hacen cada vez más exactas.

Salidas:

Un registro actualizado del riesgo: Resultados de las nuevas valoraciones del riesgo, de las intervenciones, y de las revisiones periódicas del mismo. Estos resultados pueden incluir actualizaciones a la probabilidad, al impacto, a la prioridad, a los planes de la respuesta y a otros elementos del registro del riesgo.

Plan de gestión del proyecto (actualizaciones): Si las peticiones aprobadas del cambio tienen un efecto en los procesos de la gestión de riesgos, los documentos correspondientes del plan de gestión de proyecto serán revisados y reeditados para reflejar los cambios aprobados.

Proceso P6 Comunicación de la Información sobre los Riesgos.

Es importante tener presente que en muchas ocasiones los integrantes de un equipo conocen los riesgos, pero no los comunican en la forma adecuada. Por lo general, es fácil informar de los riesgos hacia abajo en la cadena de mando (desde la dirección hasta los miembros), pero es difícil hacerlo en sentido contrario. En todos los niveles, las personas pretenden conocer los riesgos de los niveles inferiores, pero muchas veces no los comunican abiertamente a quienes están a un nivel más alto. El flujo de información restringido relacionado con los riesgos es un factor que puede aumentar la aparición de riesgos porque las decisiones acerca de estos riesgos deben tomarse con menos información. En la jerarquía del proyecto, los responsables deben ser los primeros en mostrarse abiertos y comunicativos en lo relacionado con los riesgos y asegurarse de que todo el mundo comprende perfectamente los procesos, actividades y tareas que se emprenden.(13)

Este proceso debe formalizar las lecciones aprendidas y los elementos y herramientas relevantes del proyecto y plasmar esta información en un formato reutilizable para el equipo, el resto de los proyectos y hasta para la institución. Su papel en las actividades de GR es además estratégico y organizativo.

Esta fase se conoce también como *aprovechamiento* o *aprendizaje* de los riesgos para destacar los conocimientos que se obtienen en términos de experiencia adquirida, así como la propia mejora del proceso de GR. La **Comunicación de la información sobre los riesgos** debe constituirse como un proceso continuado durante la GR y puede ponerse en práctica en cualquier momento. Se centra en la consecución de tres objetivos claves de forma general:(13)

1. Proporcionar calidad a las actividades de GR para que el equipo pueda obtener información.
2. Hacer acopio de las lecciones aprendidas, especialmente las relativas a la identificación de riesgos y a las estrategias de mitigación, para que otros equipos puedan hacer uso de ellas. Esta información permitirá aumentar la base de conocimientos de los riesgos.
3. Mejorar el proceso de GR gracias a la información proporcionada por el equipo.

Para la consecución de estos objetivos en cada uno de los procesos ya descritos se implementa una actividad y tareas para que la comunicación no quede restringida a algún proceso de la GR. Y es que el equipo necesita ser informado y saberse informado.

Este proceso no es solo un canal para que fluyan datos en el proyecto, la Comunicación debe ganar dimensiones y convertirse en la vía para estipular la información de manera formal y reutilizable: el mismo proyecto y otros, podrán utilizarla como información histórica y aprender de ella.(13)

2.4 Conclusiones

MoGeRi surge luego de identificar las características y tendencias de la GR, analizar los principales marcos de GR y su evolución, comprender necesidades y las peculiaridades del proceso productivo.

Este modelo Recoge las prácticas adecuadas según las necesidades de SIGEP, fomentando la comunicación del equipo de desarrollo dentro del proyecto. Promueve la reutilización y registro de datos, no solo de los riesgos sino de la información histórica del proyecto, apoya y complementa la planificación, seguimiento y control, y de forma general, la Gestión de Proyectos. Facilita la gestión de los recursos en el proyecto, pues el impacto de los riesgos afecta directamente los recursos.

En resumen este modelo, define procesos que permiten planificar las actividades sobre los riesgos, identificarlos, analizarlos, planificar las respuestas ante ellos, seguir y controlar los riesgos en el contexto del proyecto, así como comunicar la información generada al respecto. Precisamente son estas acciones formales las que posibilitan gestionar los riesgos en el proyecto SIGEP y en cualquier PDSW de la Facultad 4.

CAPÍTULO 3: APLICACIÓN DE MOGERI EN EL PROYECTO SIGEP

2.1 Introducción

En este capítulo se explica cómo se aplicó el modelo MoGeRi en el proyecto Sistema de Gestión Penitenciaria (SIGEP) para resolver la situación problémica planteada en la Introducción. Se describe como se realizaron los procesos y los resultados logrados en el proyecto.

2.2 Proceso de Gestión de Riesgo en SIGEP.

El proceso de Gestión de Riesgo, es un proceso relativamente joven en la Ingeniería de Software y si bien hay un entendimiento normal de que es lo que hace, hay poco conocimiento relativo de los términos que se usan y cómo debe hacerse correctamente. Según International Organization for Standardization (ISO) para que un proyecto realice una buena gestión de riesgo debe comenzar por establecer una metodología de GR, esta ayuda a la organización del proceso y a la obtención de resultados que apoyan a la Gestión del proyecto como minimizar el impacto de los riesgos (el incremento de los costos, la cancelación del proyecto, la insatisfacción del cliente, entre otras) en el proceso de desarrollo de Software. Este proceso debe iniciarse en la primera etapa de un proyecto y se desarrolla a lo largo de todo su ciclo de vida.

En el proyecto SIGEP no está definida la metodología a seguir, la GR es llevada de manera empírica y reactiva, se identifican los riesgo conocidos en el inicio del proyecto y durante el ciclo de vida del proyecto se trabaja de manera reactiva, es por ello que aunque no catastróficos, si han ocurrido hechos (riesgos) que repercuten directamente en factores como el presupuesto del proyecto, satisfacción del cliente y retrasos del equipo de desarrolladores.

2.3 ¿Qué se mejora con la Propuesta diseñada?

Realizar el proceso de Gestión de Riesgos utilizando el modelo MoGeRi, le brinda al proyecto seguridad además de permitir que se cumplan todos los planes establecidos y que se logre un proceso de desarrollo con calidad y organización, que favorezca el cumplimiento en tiempo de los objetivos del proyecto.

Permite conocer en cada momento el estado del riesgo, lo que prepara al equipo de desarrollo para la toma de decisiones. La propuesta está diseñada para suplir no solo las necesidades del proyecto sino que tiene también el objetivo de ser usada en los proyectos de la facultad.

2.4 Descripción de los procesos, actividades y tareas en SIGEP.

A continuación se describe como se realizaron cada uno de los procesos de la GR propuestos por MoGeRi en el proyecto SIGEP.

2.4.1 Proceso P1: Planificación de la GR en el proyecto SIGEP.

La planificación tiene como objetivo: describir como serán afrontadas y planificadas las actividades de la GR en el proyecto. Este proceso se implementa en la fase Estructural y Conceptual del proyecto para que sirva de apoyo a determinar la viabilidad de este; y que el equipo de desarrollo se vaya adaptando a comenzar la Gestión del proyecto por sus riesgos.

Como resultado se defino una plantilla titulada *Planificación de la Gestión de Riesgo*; en la cual se especifica el alcance de la gestión de riesgo en el proyecto(es decir; una explicación detallada de los *objetivos de la GR*, los *roles involucrados*, *actividades de revisión* y *reporte de los riesgos*, *herramientas y técnicas* a utilizar en cada uno de los procesos) y el *Plan o cronograma de la GR* que contendrá toda la información de cómo serán estructurados y realizados todos los procesos por los que pasa la Gestión de Riesgo según la metodología (MoGeRi). **(Anexo 3 y Anexo 3A).**

A continuación se muestra algunos aspectos que recoge la plantilla *Planificación de la Gestión de Riesgo* que son de vital importancia para la GR del proyecto SIGEP.

Organización del personal

Roles:

Gestor de Riesgo: Jefe del Proyecto

Equipo de GR: Diseñadores de cada modulo, arquitectos y el Gestor de riesgo.

Comité seguimiento y control: Equipo de Calidad del proyecto.

Niveles de Probabilidad e Impacto que se usarán

Probabilidad Impacto:

Para definir la probabilidad existen varias escalas nosotros utilizamos la escala Ordinal y Cardinal Lineal:

- Escala Ordinal: muy baja, baja, moderada, alta, muy alta
- Escala Cardinal:
  - Lineales (.10/ .30/ .50/ .70/ .90/).
  - No lineales (.05/ .10/ .25/ .70/ .95).

Ilustración 10: Nivel de Probabilidad.

Definición de la escala de probabilidad e impacto (Proyecto SIGEP)

Probabilidad		**Impacto**	
Escala	**Definición**	**Escala**	**Definición**
0.1	**Muy Baja**	**0.1**	**Insignificante**
0.3	**Baja**	**0.3**	**Insignificante**
0.5	**Moderada**	**0.5**	**Tolerable**
0.7	**Alta**	**0.7**	**Serio**
0.9	**Muy Alta**	**0.9**	**Catastrófico**

Tabla 3: Escala de probabilidad e impacto (Proyecto SIGEP).

Clasificación de los riesgos según criterios

Taxonomía de los riesgos SIGEP:

Esta taxonomía es la que nos va ayudar a organizar los riesgos por criterios, para la identificación y clasificación de los mismos y así proporcionar información de los riesgos a proyectos futuros, ante la escasez de casos existentes en la literatura.

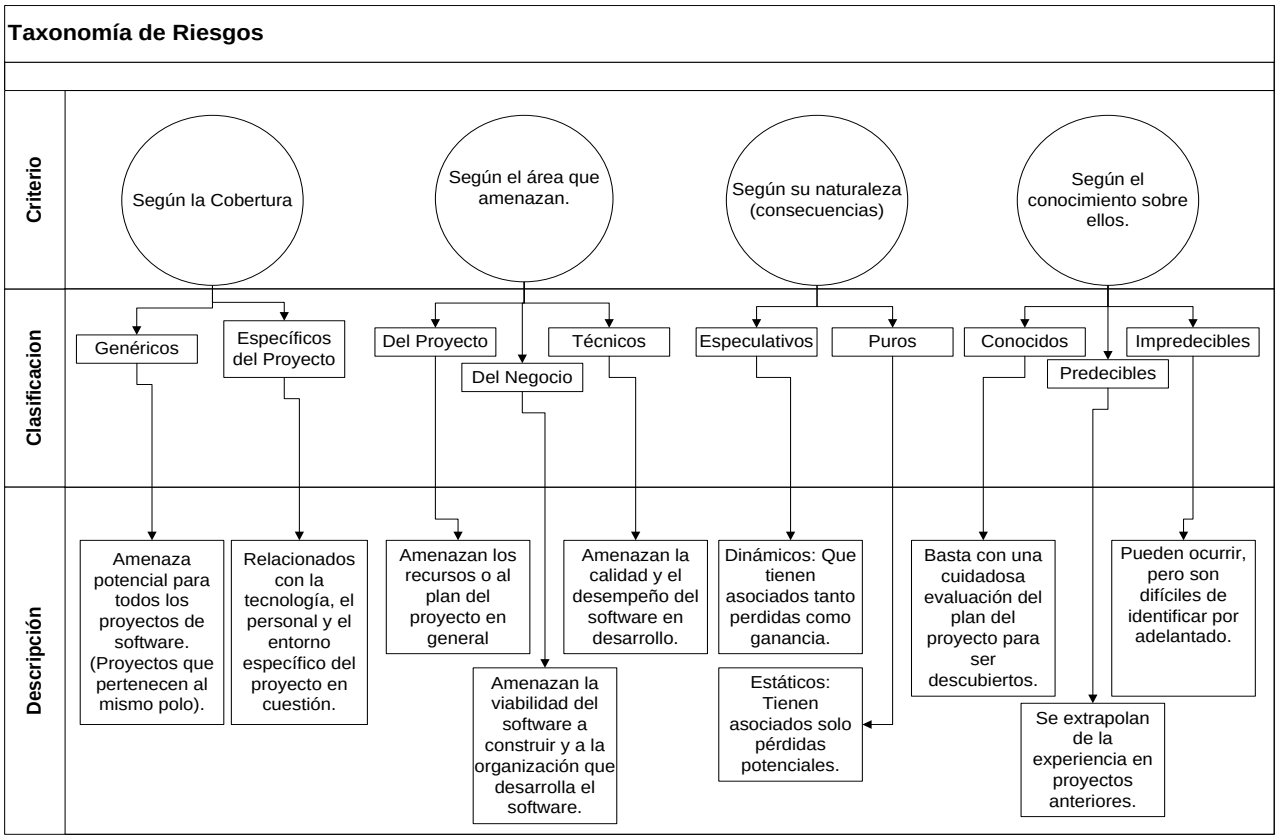

Ilustración 11: Taxonomía de los riesgos proyecto SIGEP.

Tareas para la Gestión de Riesgos:

Los riesgos serán identificados mediante listas de chequeo, serán analizados en la matriz de probabilidad e impacto para luego poder priorizarlos según su efecto.

La estrategia que vamos a utilizar para dar respuesta a los riesgos consiste en desarrollar una lista de los riesgos más importantes para el proyecto, es decir una cantidad restringida de riesgos por lo general 15 o menos. Se les dará seguimiento al estado de cada riesgo significativo así como las actividades de mitigación.

Actividades de Revisión y Reporte de los Riesgos:

- El parte del estado del proyecto según los riesgos se analiza cada 1 o 2 meses depende de la duración de la etapa en que se encuentra el mismo, preferentemente durante la revisión del avance del proyecto de software. Para elaborar este parte se utilizan dos métricas una llamada "*Impacto del Riesgo"* la cual tiene como objetivo evaluar el nivel del proyecto según sus riesgos y utiliza como referencia el impacto de los riesgos identificados, se calcula de la siguiente manera**:**

Catastrófico 1

núm. Riesgo = ∑Impacto

Critico 2

∑Impacto <= núm. Riesgo *2

Marginal 3

∑Impacto <= núm. riesgo *3

Despreciable 4

∑Impacto <= núm. riesgo *4

La segunda métrica la creamos basándonos en las necesidades del proyecto, puesto que ya teníamos un método para medir el impacto del riesgo; entonces por qué no medir también la exposición y surge esta métrica Exposición al Riesgo (Relación Impacto-Probabilidad de Riesgo) y su objetivo es estimar el nivel de exposición que tiene un proyecto frente a los riesgos, es decir, estimar cuán riesgoso puede ser mi proyecto, tiene como entrada la matriz de probabilidad e impacto. **(Ver Anexo 8)**

- Los participantes de estas reuniones de actualización son el Equipo de riesgos, el equipo de Seguimiento y Control y el Gestor de riesgo, los cuales pueden identificar nuevos riesgos que aparecerán durante las fases del proyecto.
- La métrica de *Medición de la Identificación de los Riesgos* es una medida de la información acerca de los riesgos generado por el proyecto con el fin de beneficiar a los proyectos de la facultad. Esta métrica se aplica al final de cada etapa y se usan como atributos medibles la matriz de ubicación taxonómica y la matriz de registro del riesgo que son las estructuras que recogen información pertinente al riesgo. Es una medida para guardar los riesgos más comunes en cada una de las etapas del desarrollo del software así como las consecuencias que traen consigo cada uno de ellos (el incremento de los costos, la cancelación del proyecto, la insatisfacción del cliente, entre otras), de manera tal que al cabo de cierto tiempo guardando estos registros históricos al comenzar un nuevo proyecto se tengan identificados los posibles riesgos y prevenirlos, valorando además su repercusión en cuanto al alcance (cuánto se afecta) y la duración (por cuánto tiempo se manifiesta).
- Después del primer ciclo de reuniones (identificación y análisis), los miembros del proyecto pueden hacer la actualización sin expertos en Gestión de Riesgo. Solamente las personas claves en el proyecto son necesarias.
- La actualización On-line de la documentación de la GR estará guardada en el repositorio central del proyecto.

- El Fin de cada etapa será un Hito para la GR, donde se analizará el nivel del proyecto según los riesgos y las acciones realizadas por la GR.
- El proceso de seguimiento se realizará continuamente por el equipo de GR y se supervisará al final de cada semana por el equipo revisor (seguimiento y control).

Herramientas y Técnicas:

Herramientas para almacenar el Riesgo:

- Matriz de registro del riesgo.
- Matriz de ubicación taxonómica.

Herramientas para evaluar el Riesgo:

- Definición de la Probabilidad e Impacto del riesgo.
- Matriz de la probabilidad e impacto de los riesgos.

Herramientas para seguir el Riesgo:

- Reanálisis del riesgo.
- Intervención del riesgo.
- Reuniones del chequeo.

Plan de Gestión de Riesgos

Atributos

- Roles y Responsabilidades: Define que miembros del proyecto van a trabajar en la actividad especificada y el responsable.
- Sincronización: Define las actividades que se llevaran a cabo en cada proceso de la GR y cuando y cuantas veces será realizado.
- Seguimiento: Define cómo los procesos de la gestión de riesgo serán revisados.
- Intervalos de revisión: Determina momento en que se activa el proceso de monitoreo.

2.4.2 Proceso P2: Identificación de los riesgos en el proyecto SIGEP.

Según el Modelo de Gestión de Riesgo (MoGeRi) la Identificación de los riesgos consiste en determinar que riesgos pueden afectar el proyecto y documentar las características de estos. Este proceso no se hace una sola vez sino que se hace regularmente durante el ciclo de vida del proyecto monitoreado por el proceso Seguimiento y Control de los riesgos.

El objetivo de este proceso inicialmente es elaborar una lista de los riesgos con los que el equipo de desarrollo del proyecto deberá afrontarse y durante el curso del proyecto se ejecutará como parte del proceso de Seguimiento y control para identificar nuevos riesgos ocasionados producto a cambios realizados en el proyecto. En la figura que se muestra a continuación, se describe como ocurrirá el proceso de identificación en el proyecto.

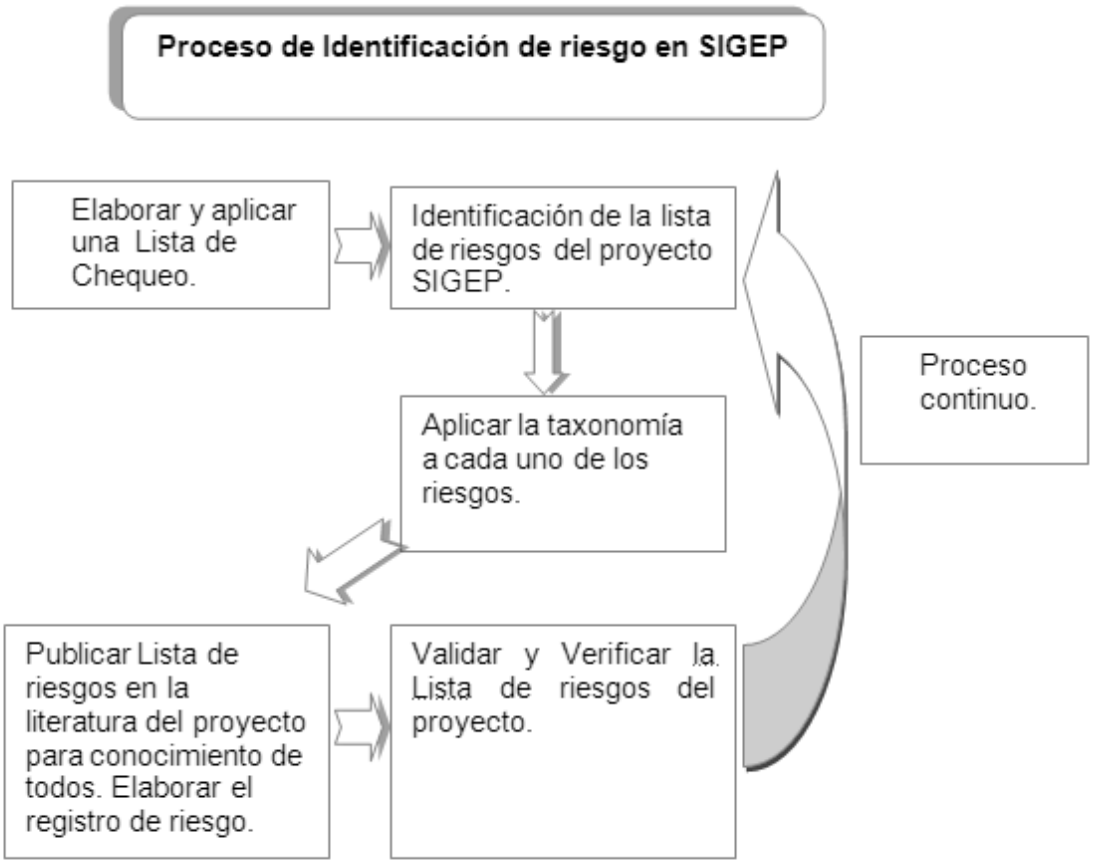

Ilustración 12: Proceso de Identificación de riesgos proyecto SIGEP.

A continuación se definen los riesgos del proyecto Sistema de Gestión Penitenciaria (SIGEP), y se documenta cada una de sus características. Es importante que se entienda que aunque se haga un análisis exhaustivo de los riesgos no siempre se van a identificar todos los riesgos y sus probabilidades de manera definitiva. Es por ello que esta tarea requiere sistematicidad en el control de los riesgos, y previendo que aparezcan nuevos riesgos, por lo que nos encontramos frente a un proceso iterativo e incremental.

Herramienta o técnica a utilizar.

Un método para identificar riesgos es crear una lista de chequeo que involucre elementos de riesgo. Esta lista es un cuestionario que recolecta información de una investigación, por tanto no debe tener preguntas inconsistentes sino que cada una de ellas debe estar relacionada con algún aspecto del problema planteado en la investigación. La siguiente Ilustración muestra los pasos realizados en el proyecto SIGEP para construir la lista de chequeo.

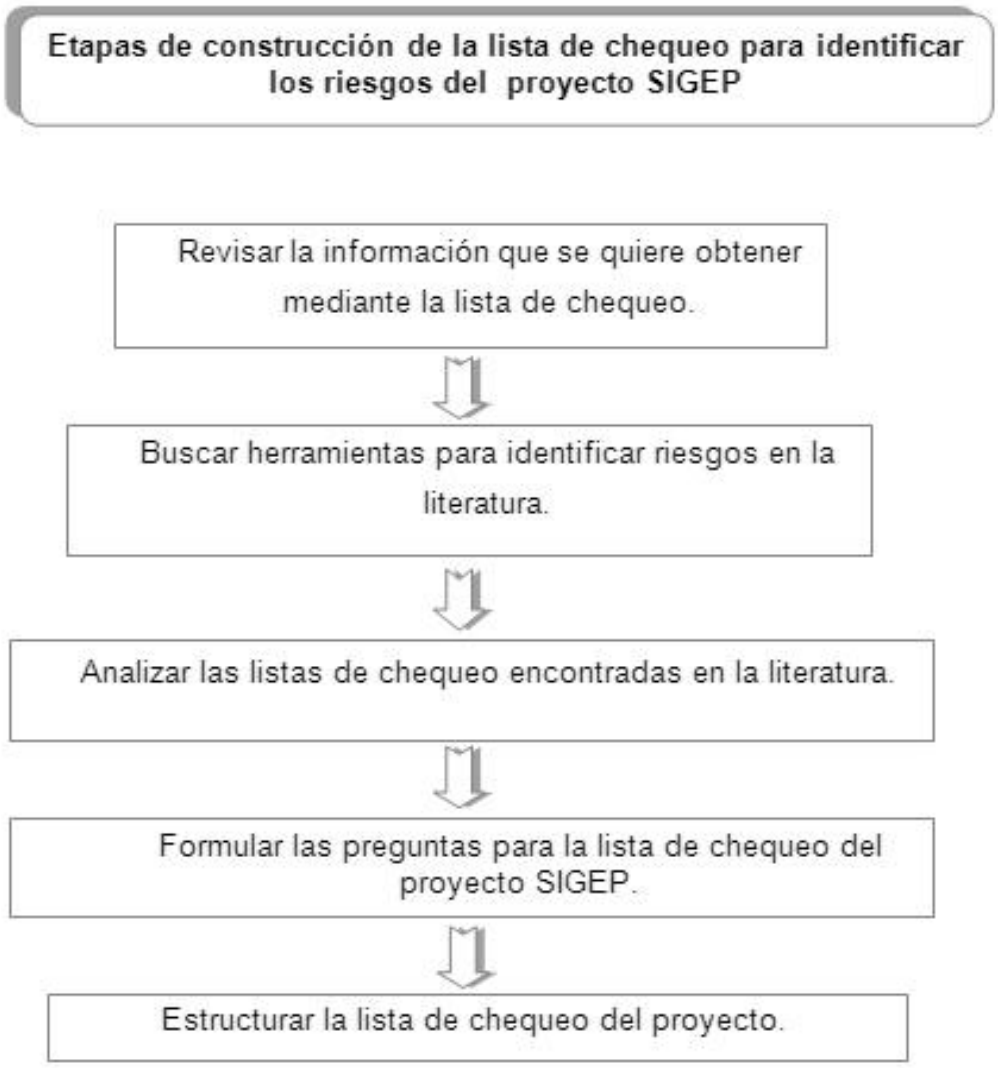

Ilustración 13: Etapas de construcción de la lista de chequeo de identificación de riesgos del SIGEP.

1. Revisar la información que se quiere obtener mediante la lista de chequeo. El objetivo de esta lista de chequeo es identificar los riesgos del proyecto, tecnológicos y del negocio.
2. Buscar herramientas para identificar riesgos en la literatura. Analizar las listas de chequeo encontradas en la literatura.

   Se realizó una búsqueda sobre el diseño de listas de chequeo en listas ya elaboradas por otros autores, relacionadas con identificación de riesgos en proyectos de desarrollo de software. Para tener conocimientos a la hora de elaborar la del proyecto.
3. Formular las preguntas para la lista de chequeo del proyecto SIGEP.

Se elaboraron las preguntas para le identificación de los riesgos guiándonos por las listas de chequeo encontradas en la literatura.

4. Estructurar la lista de chequeo del proyecto.

   Las preguntas se organizaron de acuerdo a un orden lógico. Es decir las preguntas de un mismo tema se unieron formando grupos de preguntas comunes.

Finalmente se obtuvo una lista de 106 preguntas con respuestas de Sí ó No. En el **Anexo 4** se muestra la lista de chequeo del proyecto SIGEP para la identificación de los riesgos.

Riesgos percibidos.

Después de haber descrito la técnica a utilizar para realizar el proceso de identificación, sigue realizar un análisis general para identificar los riesgos más predominantes en el proyecto, clasificarlos y elaborar la matriz final de riesgos del proyecto SIGEP, la matriz taxonómica; conjuntamente con el registro de Riesgo el cual se actualiza después en la fase da análisis.

La Lista inicial se obtiene así:

- Aplicar el cuestionario a todo el personal del proyecto.
- Analizar cada una de las repuestas.
- Contar la cantidad de entrevistados.
- Se analizó la cantidad de personas que respondieron y se valoraron aquellas respuestas que podían constituir riesgos para el proyecto.

El cuestionario fue aplicado a 41 alumnos del equipo de desarrollo del proyecto SIGEP que representan el 58% del total, se le aplicó también al líder del proyecto y a tres profesores que trabajan directamente en el.

La lista de chequeo del proyecto SIGEP quedó dividido en 7 grupos, conformados por preguntas relacionadas con los temas de: Personal, Entorno de Desarrollo, Organización, Tecnología, Negocio, Cliente, Proceso; las respuestas a estas preguntas pueden ser negativas (No) ó positivas (Si), pero no quiere decir que todas las respuestas positivas representen un riesgo para el proyecto, esto depende del tipo de pregunta, es decir tanto las preguntas que tengan respuestas negativas como positivas pueden representar riesgos para el proyecto o no.

Las preguntas del 1-15, conforman el grupo asociado con el personal del proyecto; las mismas hacen referencia a atributos como: experiencia, conocimiento, responsabilidad, cumplimiento, entre otros.

Las preguntas del 16-26; conforman el grupo asociado con el Entorno de Desarrollo del proyecto; y hacen referencia a atributos como: disponibilidad y uso de las herramientas.

Las preguntas del 27-38; conforman el grupo asociado con la Organización del proyecto; las mismas hacen referencia a atributos como: revisiones técnicas, planificación, estimación, entre otros.

Las preguntas del 39-75, conforman el grupo asociado con los aspectos tecnológicos del proyecto; estas hacen referencia a atributos como: dificultad en la utilización de las nuevas tecnologías del proyecto y del lenguaje de programación.

Las preguntas del 76-85, conforman el grupo asociado con los aspectos de Negocio del proyecto; estas hacen referencia a atributos como: Costos, viabilidad del producto, limitaciones.

Las preguntas del 86-93, conforman el grupo asociado con los aspectos del Cliente del proyecto; estas hacen referencia a atributos como: Disponibilidad del cliente en algunas tareas del proyecto y participación.

Las preguntas del 94-106, conforman el grupo asociado con los aspectos del Proceso del proyecto; estas hacen referencia a atributos como: formación de trabajadores y revisiones al desarrollo del proyecto.

Una vez aplicada esta técnica se alcanzaron los siguientes resultados: se identificaron 34 riesgos generales es decir que pueden ocurrir en cualquier proyecto de Software en la facultad y 19 riesgos específicos del proyecto SIGEP.

Como resultado de este proceso se decidió crear dos plantillas la primera de ellas es el *Archivo de riesgos* la cual está compuesta por la Matriz de registros riesgo, la Matriz de ubicación taxonómica de los riesgos y la Matriz de severidad del riesgo que se llena en el proceso de Análisis. **(Anexo 5 y Anexo 5A)**. La segunda plantilla es el registro de riesgos.

El registro de riesgo tiene una estructura vectorial con todas sus propiedades lo que facilita la implementación computacional, su búsqueda y análisis, está compuesto por**:(Anexo 6 y Anexo 6A)**

- Id: identificador único del riesgo.
- Causa: descripción textual de la causa que origina el riesgo. (El nombre de cada evento de riesgo).
- Descripción: descripción textual del suceso incierto que causa preocupación.
- Consecuencia: descripción textual de las consecuencias que trae la ocurrencia del evento.
- Categoría: identificador de la categoría.(Una de las definidas por el modelo o la entidad)
- Etapa: etapa del proyecto donde se manifiesta el riesgo (Conceptual /Estructural / Ejecución / Cierre / Soporte).
- Probabilidad: valor numérico indicando la probabilidad de ocurrencia.
- Impacto: valor de impacto para cada objetivo de proyecto, de acuerdo a lo definido en la planificación.
- Efecto: (Probabilidad) X (Impacto). Grado de peligrosidad o prioridad del riesgo.
- Estrategia de mitigación: estrategia utilizada para mitigar el riesgo.

- Estado: uno de estos valores: identificado, analizado, activo, cerrado, reabierto.

2.4.3 Proceso P3: Análisis Cualitativo de los Riesgos en el Proyecto SIGEP

Esta fase tiene como objetivo priorizar los riesgos identificados y tomar las acciones necesarias. Lo cual conlleva a evaluar el impacto y la probabilidad de los riesgos, es simple, intuitivo y rápido. Cuando asignamos prioridades a los riesgos es con el propósito de tratar en primer lugar los riesgos que mas afecten al proyecto.

El análisis de los riesgos en el proyecto SIGEP se organizó así: evaluación de la probabilidad y el impacto de los riesgos encontrados, cálculo de la exposición al riesgo, priorización de los mismos y elaboración del registro de riesgos del proyecto.

No se procederá a cuantificar los riesgos puesto que anteriormente nunca se había hecho una GR en el proyecto, por tanto no se tiene ningún tipo de documentación histórica y esta es muy importante para este tipo de análisis.

Después de haber estudiado varias literaturas encontramos que existen varias técnicas para el análisis cualitativo de los riesgos como:

- Matriz probabilidad / impacto
- Seguimiento de los 10 ítems de riesgo superior
- Juicio de expertos

El MoGeRi que es la metodología por la cual se está rigiendo el proceso de Gestión de Riesgo del proyecto SIGEP, recomienda la evaluación de los riesgos en la matriz de Probabilidad e Impacto. Esta presenta la probabilidad relativa de la ocurrencia de un riesgo Vs el impacto relativo de ocurrir el riesgo; es decir se toman las decisiones reunidas por el equipo en dos de los más universales componentes del riesgo, la probabilidad de que el riesgo ocurra y el impacto que es la pérdida o el efecto negativo en caso de que el riesgo ocurra y luego se multiplican estos dos valores dando origen a una métrica denominada exposición al riesgo.

Definición de la matriz de Probabilidad e Impacto: Este paso se divide en dos; definición de la escala a utilizar en la matriz y evaluación de los riesgos en la matriz. La escala a utilizar en la matriz ya se especificó en el proceso de planificación. **(Ver tabla 4)**

A continuación se muestran los riesgos evaluados en la matriz de probabilidad e impacto.

Probabilidad	**Amenazas**				
0.9	**0.09**	**0.27**	**0.45**	**0.63**	**0.81**

0.7	**0.07**	**0.21**	**0.35**	**0.49**	**0.63**
0.5	**0.05**	**0.15**	**0.25**	**0.35**	**0.45**
0.3	**0.03**	**0.09**	**0.15**	**0.21**	**0.27**
0.1	**0.01**	**0.03**	**0.05**	**0.07**	**0.09**
Impacto	**0.1**	**0.3**	**0.5**	**0.7**	**0.9**

Tabla 4: Matriz de probabilidad e impacto proyecto SIGEP.

El área más sombreada representa los riesgos más Críticos, el área moderadamente sombreada representa los riesgos Grave y el área menos sombreada representa los menos importantes pueden ser Apreciables o Asumibles. Aquellos riesgos que se encuentran en la región más sombreada y moderadamente sombreada son riesgos que tienen un impacto alto en los objetivos del proyecto y una probabilidad de ocurrencia alta y moderada, por tanto requieren que se le dé una prioridad mayor sobre los riesgos que se encuentran en la región menos sombreada, planteando estrategias agresivas de mitigación.

El cálculo de la probabilidad y el impacto es sumamente subjetivo (una suposición) lo que trae consigo que hay que evaluar la probabilidad con un grado de seguridad. Cuando hablamos del término probabilidad nos referimos a un resultado estadístico preciso: por ejemplo “una medida de la frecuencia o posibilidad relativa de ocurrencia de un evento, cuyo valor oscila entre cero (imposibilidad) y uno (certeza), el cual surge, bien sea de una distribución teórica o a partir de observaciones”(24) .El cálculo de la probabilidad se torna confuso; ello es particularmente cierto para aquellos proyectos donde no hay mayores datos de las probabilidades de riesgos de proyectos anteriores o éstos no fueron relevantes. En el caso de nuestro proyecto, evaluaremos la probabilidad y el impacto mediante la observación debido a que el proceso de GR en este proyecto es nuevo y no se tiene ningún registro de riesgos que ocurrieron o no ocurrieron, además de que en la universidad la GR esta en un nivel primitivo. Por tanto con la ausencia de estas evidencias se hace difícil la evaluación de la probabilidad y el impacto, y hay que hacerla entonces con una perfecta observación y con la ayuda del equipo del proyecto basándonos en criterios de expertos.

Evaluación de los riesgos en la matriz de severidad de riesgos.

Para esta etapa se utiliza la matriz de riesgos elaborada en la fase de Identificación, con el propósito de obtener y clasificar los riesgos que mas impactan al proyecto.

Para realizar este análisis se toma cada uno de los riesgos de la matriz de riesgos, y se valora su probabilidad e impacto. Seguidamente se multiplican estos dos factores para calcular así el valor de exposición del riesgo, lo cual permitirá conocer si el riesgo es crítico, grave, apreciable y asumible. Finalmente se ordena la matriz de riesgo por el nivel de clasificación:

1. Es **crítico** en el sentido de que requiere atención urgente.
2. Es **grave** en el sentido de que requiere atención.
3. Es **apreciable** en el sentido de que pueda ser objeto de estudio para su tratamiento.
4. Es **asumible** en el sentido de que no se van a tomar acciones para impedirlo.

Esta información nos sirve de base a la hora de asignar prioridades al riesgo.

Podemos decir que el análisis cualitativo de los riesgos proporciona al equipo una lista de prioridades de riesgos muy útil y ventajosa para planificar las actividades de respuesta a estos riesgos. La investigación detallada y minuciosa de los riesgos, las consecuencias y la unidad de medición utilizada para la asignación de prioridades (probabilidad, impacto y exposición), son factores muy importantes para lograr con eficiencia la Gestión de Riesgo. Esta lista es un punto de partida muy importante del proceso de Gestión de Riesgos y debe actualizarse a lo largo de todo el ciclo de vida del proyecto.

2.4.4 Proceso P4: Planificación de Respuesta al Riesgo en el proyecto SIGEP

Es en este proceso donde se trazan medidas, planes y estrategias para mitigar el riesgo o simplemente controlarlo y se apoya básicamente en la información que se obtuvo al realizar el análisis de los riesgos en la fase anterior. Su objetivo es desarrollar un plan para controlar los riesgos más importantes identificados durante el análisis de riesgos. En esta fase se decidió que hacer para cada uno de los riesgos de la lista tomando solo los riesgos Críticos y se plantean las medidas para cada uno de ellos.

Una de las técnicas para planificar la respuesta a los riesgos consiste en desarrollar una lista de los riesgos más importantes para el proyecto. Lo fundamental es seleccionar una cantidad restringida de los riesgos que deben gestionarse con mayor prioridad nosotros proponemos 15 o menos. Aunque a veces se quieran gestionar más de esta cantidad de riesgos resulta más eficaz centrarse en un número reducido de riesgos y luego dedicarse a gestionar aquellos que causen menos daños para el proyecto; pero eso si ya cuando el primer grupo de riesgos que implican mayor peligro estén controlados. Después de escoger los riesgos se deberá elaborar una estrategia para su gestión.

Para reducir la exposición al riesgo utilizamos los siguientes enfoques:

Mitigación: Implica las acciones que se van a realizar con anterioridad para evitar que se produzca el riesgo o para reducir su impacto y consecuencias a un buen nivel.

Contingencia: Implica las acciones que se van a realizar después de que un riesgo se produce es decir si no se pudo mitigar para minimizar sus daños.

Aceptar: En algunos riesgos ya no es posible intervenir con medidas preventivas porque ya este pasó. En este caso el plan deberá incluir los motivos que han empujado al equipo a aceptar el riesgo sin desarrollar ningún plan de mitigación ó contingencia.

Como artefacto de salida en este proceso se generó una plantilla llamada *Plantilla de respuesta al riesgo* la cual está compuesta por la Matriz De Los Riesgos Más Significativos y el Plan De Mitigación. **(Anexo 7)**.

A continuación se nombran los 15 riesgos escogidos por nosotros para su gestión, dentro de estos hay siete riesgos que corresponden a la fase despliegue que actualmente nuestro proyecto se encuentra enmarcado en ella (9-15) las respuestas a todos estos riesgos se encuentran en el Plan de Mitigación: **(Anexo 7A)**.

1. Superficial captura de requisitos.
2. Cambio de los requisitos del software.
3. Mayoría de diseñadores y programadores en 5to año.
4. Inexperiencia de los nuevos incorporados al proyecto.
5. Posible egreso de la UCI de los programadores y diseñadores más experimentados.
6. Desarrollar más casos de uso que los acordados.
7. No satisfactorio nivel de definición de procesos operativos.
8. Los sistemas externos no ofrecen las interfaces necesarias para establecer la comunicación con estos.
9. Falta de infraestructura para el despliegue.
10. Mal estado de la infraestructura física.
11. Ausencia de personal técnico para administrar el sistema.
12. Uso inadecuado de las aplicaciones informáticas.
13. Inseguridad en el interior de los establecimientos penitenciarios.
14. Mantenimiento de la tecnología instalada.
15. Fallo en la conectividad.

2.4.5 Proceso P5: Seguimiento y Control del Riesgo en el proyecto SIGEP.

Esta fase tiene como objetivo principal corregir las desviaciones de los planes de mitigación y contingencia, además de seguir los riesgos identificados y los de la lista de supervisión. Por tanto se debe estar alerta ante la aparición de nuevos riesgos que puedan aparecer a medida que el proyecto avanza. También incluye la supervisión de probabilidades e impacto y exposición.

La figura describe el proceso de seguimiento y control propuesto para el proyecto SIGEP.

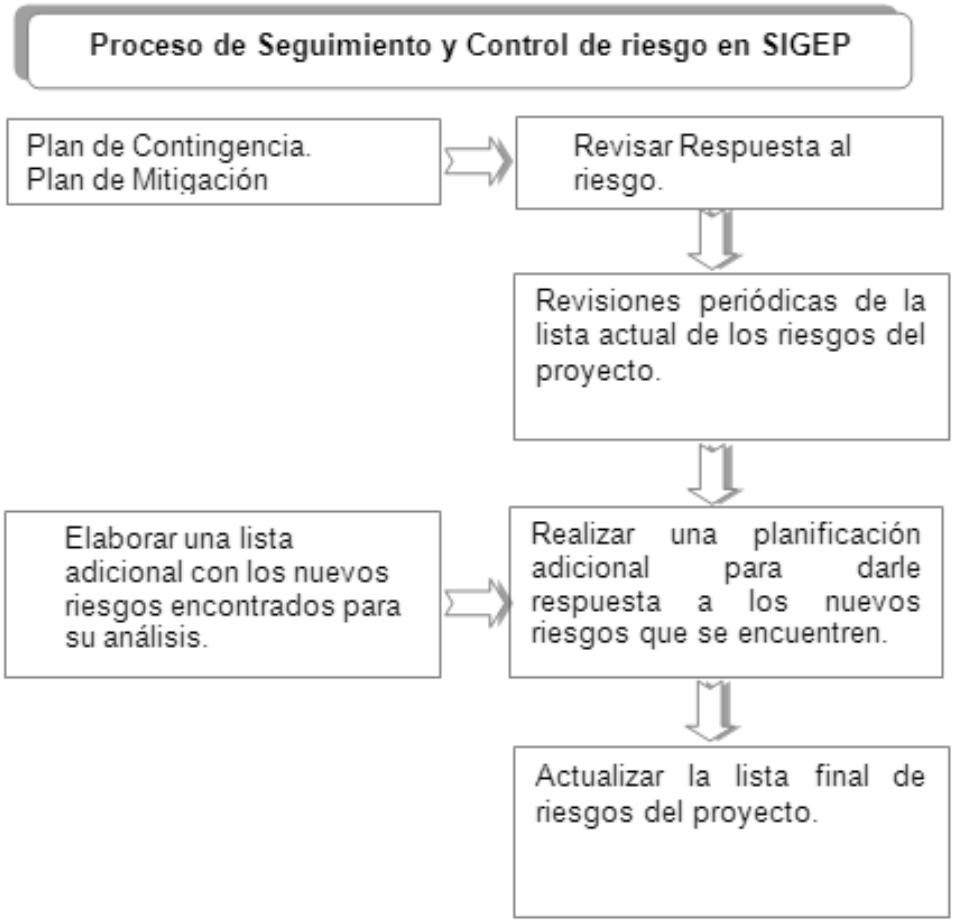

Ilustración 14: Proceso de Seguimiento y Control proyecto SIGEP.

La implementación de esta fase comienza poniendo en el repositorio central del proyecto el plan de Mitigación para que cada miembro del equipo de desarrollo sepa qué hacer ante la presencia de los riesgos identificados. El gestor de riesgo tiene la responsabilidad de subir esta información al repositorio y cuando el equipo conozca cada una de los riesgos y las medidas orientadas a minimizarlos o eliminarlos; se debe esperar al menos tres meses para poder comprobar si estas medidas fueron satisfactorias es decir si se logró un resultado positivo. También se debe comprobar si se identificaron nuevos riesgos y si es así encargarse de que se realizaran cada uno de los procesos descritos.

Es en esta fase donde se aplican las métricas del Impacto del Riesgo y la relación Impacto-Probabilidad del Riesgo, justo para saber el nivel que tiene un proyecto según sus riesgos además de medir el nivel de probabilidad que tiene un proyecto de ser riesgoso. Cuando se aplicaron estas dos métricas al inicio ambas coincidieron en que el proyecto tenía un nivel crítico de riesgos, por tanto

tuvimos que tomar medidas de mitigación y no dejar de observar los riesgos para que no ocurrieran resultados catastróficos y el desarrollo de software siguiera su curso satisfactoriamente. (Ver Ilustración 15)

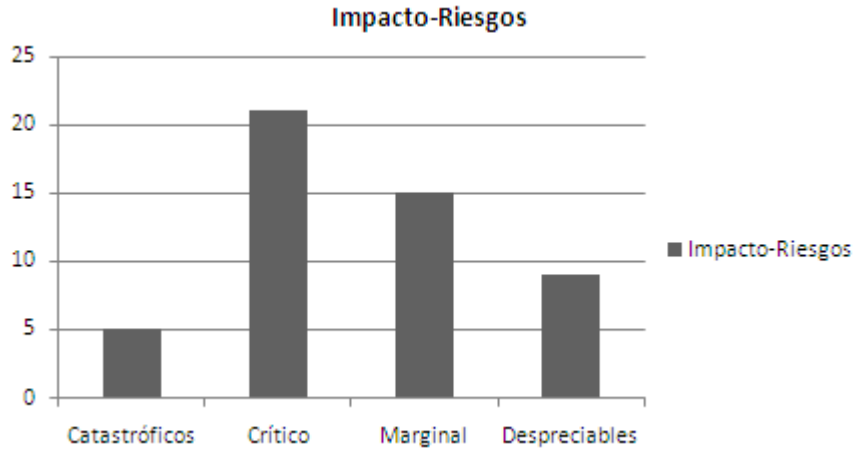

Ilustración 15: Gráfico relación Impacto-Riesgo.

Gracias a las estrategias de mitigación y de darle un buen seguimiento a los riesgos, después de dos meses se aplicó nuevamente las métricas a los 15 riesgos seleccionados en el proceso de Planificación y respuesta y sus resultados fueron que el proyecto se encuentra en un nivel Marginal de acuerdo con estos riesgos es decir que los resultados de la gestión han sido buenos. (Ver Ilustración 15A)

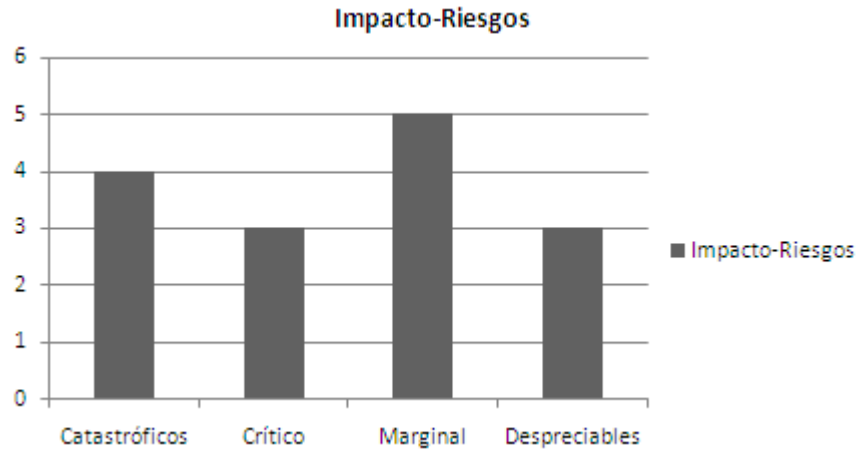

Ilustración 15A: Gráfico relación Impacto-Riesgo.

También aplicamos la Métrica de identificación y tuvimos resultados satisfactorios; ya que en nuestra GR se guardan los riesgos más comunes y se definieron plantillas para el control y almacenamiento de los mismos como (Matriz del registro de riesgo y Matriz de Ubicación Taxonómica).

2.4.6 Proceso P6: Comunicación de la Información sobre los Riesgos.

La metodología para la Gestión de Riesgo MoGeRi plantea que la comunicación debe constituirse como un proceso continuado durante la GR y puede ponerse en práctica en cualquier momento.

Para esto en cada uno de sus procesos en nuestro proyecto se propuso una actividad y tareas para que la comunicación no quedara restringida a algún proceso de la GR. Es muy importante aclarar que este proceso no solo va hacer un canal para que fluyan los datos sino que debe ir más a fondo y convertirse en la vía para estipular la información de manera formal y reutilizable; para que el mismo proyecto y otros puedan utilizarla como información histórica y aprender de ella.

Para la Planificación de la gestión de riesgo en el proyecto SIGEP nosotros implementamos la Comunicación realizando reuniones de análisis donde se les informó a los integrantes del equipo de desarrollo sus responsabilidades y se discutieron los informes (Plan de Gestión de Riesgo) y las decisiones tomadas en este proceso. Así nos aseguramos de que todo el personal comprendiera perfectamente los procesos, actividades y tareas que se fueran a realizar.

En el proceso de identificación el propósito es mantener informado al equipo del proyecto acerca de los riesgos; esto lo logramos con el *Registro de Riesgos* que es muy importante como información histórica ya que desde el inicio; los integrantes del proyecto pueden saber cómo marcha el trabajo, este registro se puede ver en el repositorio central del proyecto y también se informa en las reuniones.

Es muy importante aclarar que la comunicación en el proyecto se realiza de forma vertical es decir no solo se informan los riesgos desde la dirección hasta los miembros; sino que cualquier miembro del proyecto que se encuentre en el camino de desarrollo del software algún factor de riesgo este se lo informa a la dirección. Quiero aclarar que esto se logró gracias a que los responsables del proyecto siempre se mantienen abiertos y comunicativos; precisamente este es uno de los objetivos que se quería lograr con la fase de comunicación.

Durante el proceso de análisis se utilizó como artefacto de comunicación la *Matriz de Severidad de riesgo* y el *Registro de Riesgo* y en ellos se puede ver el nivel de probabilidad de ocurrencia que tiene el riesgo y su impacto, además de la etapa del proyecto que puede ocurrir. Mientras que en el proceso de planificar la respuesta al riesgo se creó un plan de mitigación y un plan de contingencia para cada riesgo y estos se publicaron en el repositorio central del proyecto, conjuntamente se informa en reuniones para que cada integrante del equipo de desarrollo conozca las acciones que debe tomar para evitar el riesgo o combatirlo.

2.4.7 Resultados Alcanzados con la aplicación y adaptación del modelo. (Conclusiones)

La implantación del modelo MoGeRi en el proyecto hasta el momento ha contribuido satisfactoriamente en los resultados del mismo. Desde la GR se logró concientizar al equipo de trabajo de la importancia

de controlar los riesgos y obtener de estos más que perdidas oportunidades. Con el uso de una metodología se logró organizar el trabajo, obtener documentación del proceso que sirven de apoyo a la toma de decisiones en próximos proyectos, aspecto este importantísimo en la GR debido a su carácter probabilístico, y mantener a todo el equipo de desarrollo preparado para enfrentar los problemas que puedan ocasionar pérdidas en el proyecto.

Al comenzar este trabajo nos encontramos que en SIGEP no había un control de los riesgos por lo que en una fase inicial de la implantación del modelo se lograron identificar 53 riesgos, de los cuales 34 fueron genéricos, es decir, que pueden ocurrir en SIGEP y en cualquier proyecto de desarrollo de software de la facultad y 19 riesgos específicos de SIGEP. Luego de realizar el análisis pertinente en una primera iteración del proceso se clasificaron según su exposición 35 riesgo críticos, 15 graves, y 3 asumibles lo que situaba al proyecto en un estado crítico según sus riesgos, esto nos decía que las perdidas eran sustanciales para el mismo. Con el transcurso de la ejecución del proceso y la vinculación consiente del equipo de desarrollo a la GR finalmente comenzamos a obtener resultados satisfactorios y por consiguiente la motivación de los desarrolladores. Manteniendo un adecuado control y seguimiento del estado de los riesgo identificados y los que surgieron debido a los cambios ocurridos, en este momento hemos logrado que el nivel del proyecto se encuentre en un estado marginal según sus riesgo, lo que dice que el trabajo en equipo ha logrado minimizar grandemente el impacto de los riesgos sobre el proyecto.

Además de mantener el proyecto en un estado marginal respecto a los riesgos, con este trabajo se logró establecer una metodología de trabajo para llevar la GR en SIGEP, la cual fue adaptada a las necesidades del mismo generando artefactos de salidas en los procesos vitales para un seguimiento adecuado de estos, se aplicaron métricas que permitieran conocer que tanto podíamos perder si los riesgos se convertían en problemas reales y generar la documentación necesaria para poder realizar un análisis menos subjetivo en próximos iteraciones de SIGEP y próximos proyectos.

CONCLUSIONES

Con la realización del presente trabajo se obtuvo un conocimiento basto de las tendencias actuales de la GR, lo que permitió evaluar las distintas metodologías existentes y determinar una para realizar la GR en SIGEP con la calidad requerida que incluye los 6 procesos estándares a llevar a cabo en el proceso.

Este modelo no fue aplicado estrictamente como sugiere la metodología, sino, que se adaptó para que supliera todas las necesidades de un proyecto que se está iniciando en las prácticas de la GR como SIGEP. Se definieron 4 plantillas (Planificación de la Gestión de Riesgo, Archivo de riesgos la cual está compuesta por la Matriz de registros riesgo, la Matriz de ubicación taxonómica de los riesgos y la Matriz de severidad del riesgo, Registro de riesgos que contiene toda la historia del riesgo durante el desarrollo del sistema y Plantilla de respuesta al riesgo la cual está compuesta por la Matriz De Los Riesgos más Significativos y el Plan De Mitigación), se especificó una taxonomía para clasificar los riesgo según 4 criterios (Según la cobertura, el área que amenazan, su naturaleza y el conocimiento sobre ellos). También se aplicaron 3 métricas, dos para conocer cuan riesgoso es nuestro proyecto, una de ellas definida por nosotros y la tercera es para medir el nivel de información que puede brindar el proyecto para tomar futuras decisiones.

Se comprendió la necesidad de educar a los equipos de desarrollo de software en comenzar la Gestión del Proyecto con la Gestión de sus Riesgos y de incluir en la etapa de planificación del proyecto la PGR. Muy importante también, es que se cuenta ya con los resultados que brinda utilizar una metodología para la GR, lo que contribuye a que otros proyecto se preocupen por comenzar a realizar este proceso.

RECOMENDACIONES

Al concluir con los objetivos propuestos en la investigación se recomienda al proyecto SIGEP:

- Dar seguimiento al proceso de GR con toda la documentación generada para el proyecto SIGEP hasta el fin del mismo.
- Utilizar la documentación de este proceso para realizar en un futuro el análisis cuantitativo de los riesgos en próximas iteraciones de SIGEP y otros proyectos de la facultad.
- Incorporar técnicas de recolección de información en tiempo real, con el propósito de obtener los datos cuantitativos necesarios.
- Implementar un sistema de gestión de información acerca de los riesgos.
- Aplicar este modelo con los artefactos generados en este trabajo en otros proyectos de la facultad.

REFERENCIAS BIBLIOGRÁFICAS

1. NUCHERA, A. H. *Una introducción a la gestión de riesgos tecnológicos* [Consultado el: Febrero 20 de 2007]. (Tribuna Debate). Disponible en: http://www.madrimasd.org/revista/revista23/tribuna/tribuna1.asp.
2. APARICIO, F. *Análisis y Gestión de Riesgos.* 2005, 36 p. Disponible en: http://www.fistconference.org/data/presentaciones/AnalisisyGestiondeRiesgos.pdf.
3. FARIAS-ELINOS, M. *La seguridad Inicia con el Análisis de Riesgo.* 2003, Disponible en: http://seguridad.internet2.ulsa.mx/congresos/2003/esime/ariesgo.pdf.
4. ORIZONDO, A. C. A. Proyecto Técnico de Asesoría Especializada, Colaboración Médica Odontológica, Comunicación Institucional y Solución Tecnológica para apoyar la modernización del Sistema Penitenciario de la República Bolivariana de Venezuela. 28 de Agosto 2006, nº p. 95. [Consultado el: 17/12/2007].
5. COCHO, J. M. *Estudio exploratorio sobre los métodos de gestión de proyectos de alto riesgo.* 2003,
6. *Conceptos y Definiciones de Relevancia en la Gestión del Riesgo* [Consultado el: Diciembre 8 de 2007]. Disponible en: http://www.snet.gob.sv/Documentos/conceptos.htm.
7. PRESSMAN, R. S. *Ingeniería del Software. Un enfoque práctico.* 2005. vol. Parte 1,
8. MENÉNDEZ, R. *Gestión de Riesgos en Ingeniería del Software.* 2004.
9. CIAO. *Practices for Securing Critical Information Assets Critical Infrastructure Assurance Office.* 2000.
10. SEI. *Risk Management* [Consultado el: Enero 20 de 2008]. Disponible en: http://www.sei.cmu.edu/news-atsei/columns/the_cots_spot/2000/march/cots-mar00.htm.
11. BASTERRA, R. V. D. *Administrando la Inseguridad.* 2006.
12. J.ESTEVEZ, J. A. P. *Implementación y Mejora del Método de Gestión Riesgos del SEI en un proyecto universitario de desarrollo de software.* 2005, Disponible en: http://www.ewh.ieee.org/reg/9/etrans/vol3issue1March2005/3TLA1_13Esteves.pdf.
13. VELIZ, Y. Z. *Modelo de Gestión de Riesgos en Proyectos de Desarrollo de Software.* TESIS EN OPCIÓN AL TÍTULO ACADÉMICO DE MASTER EN GESTIÓN DE PROYECTOS INFORMÁTICOS, Universidad de las Ciencias Informáticas, 2007.
14. BOEHM, B. *Software Risk Management. IEE Computer, 1989:*

-Software Risk Management: principles and practices. IEEE, 1998.

-A Spiral Model of Software Development and Enhancement. IEEE Computer, 1988.

15. HIGUERA R.P, Y. Y. H. Software Risk Management. Pittsburgh, Pennsylvania, Carnegie Mellon University. Software Engineering Institute. 1996.
16. MARCELO, J.; M. RODENES, et al. Estudio exploratorio sobre los métodos de gestión de proyectos de alto riesgo. Primer Congreso REFERENCIAS 81 SOporte del COnocimiento con la Tecnología, SOCOTE, Valencia. España. 2003, nº
17. ALLER, N. Mejora y ampliación de la aplicación de gestión de riesgos bajo el framework JRisk para empresa dedicada a realizar proyectos de software. Escuela Universitaria de Ingeniería Técnica en Informática. Oviedo. 2005, nº
18. EUROMÉTDO. *El proyecto Eurométodo. Ejercicio de validación de EM v0,* 1996.
19. MAP. *El proyecto Eurométodo. Ejercicio de validación de EM v0,* 1996,
20. PMI. *Project Management Body of Knowledge. PMI Communications.* 2004,
21. IAGP. *Gestión de riesgos en ingeniería del software. Consultado en marzo 15,2008* 2005/06., Disponible en: http://www.um.es/docencia/barzana/IAGP/Iagp5.html.
22. ALFONSO ROMERO B., D. L. D., SIMEÓN YARINGAÑO Y., SILVANA FLORES CH. *Gestión de riesgos con CMMI, RUP e ISO en Ingeniería de Software Minero.* 2007, vol. Vol. 10, Nº 19, 55-61 (2007), Disponible en: http://sisbib.unmsm.edu.pe/BibVirtualData/publicaciones/geologia/vol10_n19/a05.pdf.
23. INDECOPI. *Norma Técnica peruana NTP-ISO/IEC 12207.* 2006.
24. DR DAVID HILLSON, D. D. T. H. *Calculando probabilidades de riesgos: Métodos alternativos.* 2004, Disponible en: http://www.pmi-bcn.org/articulos/DH%20-%20Calculando%20 Probabilidades %20 de%20Riesgos.pdf.

BIBLIOGRAFÍA

ARIAS, O. Y. A. "Proyecto Técnico de Asesoría Especializada, Colaboración Médica Odontológica, Comunicación Institucional y Solución Tecnológica para apoyar la modernización del Sistema Penitenciario de la República Bolivariana de Venezuela", 2006.

Albert's, C. and A. Dorofee, Advanced Risk Analysis for High-Performing Organizations. 2006, SEI.

Bohem, BW. (1986). A spiral model of software development and enhancement.ACM Sigsoft Software Engineering Notes.

Boehm, B., Software Risk Management: principles and practices. 1991: IEEE.

Barki, H.A., Toward an assessment of sw development risk. Journal of Management Information System Risk, 1993. Vol 10.

Cocho, J.M., M.R. Adam, and J.M. Torralba. Estudio exploratorio sobre los métodos de gestión de proyectos de alto riesgo. Primer Congreso Soporte del Conocimiento con la Tecnología, SOCOTE. 2003. Valencia. España.

Estevez, J; Pastor, J. (2000).Towards the Unification of Critical Success Factors for ERP Implementations, 10th Annual Bit Conference, Manchester, UK.

Graves, Roger. (2000).PM Qualitative Risk Assessment-Network October.

Hoffman T. (1998). Risk management still a wild frontier and Computerworld, p. 10.

Jones, C. (1998).Minimizing the risk of software development. Cutter IT Journal.

Jiang, J., G. Klein, and R. Discenza, Information Systems Success as impacted by risks and development strategies. IEEE transactions on Engineering Management, 2001. 48: p. 46-55.

Kontio, J. (1997).Empirical Evaluation of a risk management Method.SEI conference on risk management, USA.80

MAP. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Método. (V 1.1).

PÚBLICAS, M. D. A., Catálogo general de publicaciones oficiales, 2006.

MENÉNDEZ, R. "Gestión de riesgos en ingeniería del software", 2004.

PRESSMAN, R. S. "Ingeniería del Software. Un Enfoque Práctico". 1998.

Schmidt, R., Identifying software project risks, an international Delphi study. Journal of Management Information Systems, 2001. 17: p. 5-36.

ANEXOS

Anexo 1: Distribución de los procesos de riesgos en las fases de desarrollo de un proyecto de software.

Área	Procesos	Conceptual	Estructural	Ejecución	Cierre	Soporte
Riesgos	Planificación de la Gestión de Riesgos	x	x			
	Identificación de Riesgos	x	x	x	x	x
	Análisis cualitativo de Riesgos	x	x	x	x	x
	Análisis Cuantitativo de Riesgos		x	x	x	x
	Planificación de la Respuesta a los Riesgos	x	x	x	x	x
	Seguimiento y Control de los Riesgos		x	x	x	x

Anexo 2.Boehm incluye una lista de "Top 10 Software Risk Ítems" junto con una serie de técnicas de gestión del riesgo.

Las técnicas definidas por Boehm son:

A) Contratar las personas clave proactivamente

B) Construir equipos proactivamente (desarrollar valores compartidos)

C) Estimar los plazos y presupuestos 'reactivamente' (con fondo para riesgos)

D) Diseñar 'forfait' proactivamente: usar el presupuesto/plazo fijo para priorizar los requerimientos; diseñar con arquitectura que permita retrasar lo no obligatorio; modular la funcionalidad entregada para adecuarla al presupuesto/plazo disponible.

E) Desarrollar incrementalmente las funcionalidades (requerimientos prioritarios...)

F) Desarrollar por prototipos (o sea, subconjuntos para 'comprar' información)

G) Reducir requerimientos usando las priorizaciones desarrolladas para D, E), F).

H) Analizar la misión: análisis organizacional, coste-beneficio, ingeniería del usuario.

I) Encapsular la información para reducir requisitos volátiles y reutilizar software.

J) Comprobar los referentes y auditar por expertos externos antes de decidir.

K) Ingenierizar rendimientos con técnicas para simular, modelar, prototipar, afinar.

L) Analizar las capacidades de las tecnologías informáticas para resolver FCE.

Matriz elemento de riesgos y técnicas de gestión de riesgo.

Elemento de riesgo	Técnica de gestión del riesgo											
	A	B	C	D	E	F	G	H	I	J	K	L
Insuficiencias de personal (Recursos)	X	X										
Planificaciones y presupuestos poco realistas (Recursos)			X	X	X		X					
Desarrollo de las funciones y propiedades erróneas (Requerimientos)						X		X				
Desarrollo erróneo del interfaz de usuario (Requerimientos)						X		X				
Especificaciones excesivas (Requerimientos)				X		X	X	X				
Continua corriente de cambios en los requisitos (Requerimientos)					X				X			
Deficiencias en componentes proporcionados externamente (Subcontratas)										X	X	
Deficiencias en tareas desarrolladas externamente (Subcontratas)		X		X						X		
Deficiencias en rendimiento del sistema al funcional realmente (Diseño)											X	
Exprimir las capacidades de las tecnologías informáticas (Diseño)								X		X	X	X

Anexo 3.Plantilla Planificación de la GR.

albet
INGENIERÍA Y SISTEMAS

Proyecto para la Humanización Penitenciaria

Sistema de Gestión Penitenciaria

PLANIFICACION DE LA GR.

VERSION <X.X>

Revisión Histórica

Fecha	Versión	Descripción	Autor
<dd/mmm/yy>	<x.x>	<detalles>	<nombre>

Reglas de Seguridad

El que recibe el documento asume la custodia y control, comprometiéndose a no reproducir, divulgar, difundir o de cualquier manera hacer de conocimientos público su contenido, excepto para cumplir el propósito para el cual se ha generado.

Estas reglas son aplicables a las __ páginas de este documento.

Tabla de Contenido

[Breve descripción de las tareas de gestión durante el proyecto. Se debe describir lo siguiente:

- *La estrategia a utilizar para identificar el riesgo y cómo serán analizados y priorizados.*
- *Estrategias para la mitigación, evasión, y/o prevención para los riesgos más importantes (máximo 10 riesgos)*
- *Como se van a dar seguimiento al estado de cada riesgo significativo y las actividades de mitigación*
- *Actividades de revisión y reporte de los riesgos. LA revisión de los riesgos debe formar parte de cada revisión de iteración y de aceptación de fases*

2.7 Herramientas y Técnicas

[Lista de las herramientas y/o técnicas que serán utilizadas para almacenar los riesgos, evaluar el riesgo, seguir el riesgo, o generar reportes del control de los riesgos]

3. Plan de Gestión de Riesgos (PGR):

Proceso	Roles y responsabilidades	Sincronización	Seguimiento	Intervalos de Revisión
Identificación del Riesgo				
Análisis del riesgo				
Planificación de la respuesta a los riesgos				

Atributos del plan:

- Roles y Responsabilidades: Define que miembros del proyecto van a trabajar en la actividad especificada y el responsable.
- Sincronización: Define las actividades que se llevaran a cabo en cada proceso de la GR y cuando y cuantas veces será realizado.
- Seguimiento: Define cómo los procesos de la gestión de riesgo serán revisados.
- Intervalos de revisión: Determina momento en que se activa el proceso de monitoreo.

Anexo 3A.Plan de GR Proyecto SIGEP

Proceso	Roles y responsabilidades	Sincronización	Seguimiento	Intervalos de Revisión
Identificación del Riesgo	Equipo de desarrollo del proyecto SIGEP. Equipo de GR. **Gestor de Riesgo:** Jefe de Proyecto	**Actividades** -Selección de herramientas y técnicas a aplicar para la identificación. -Reuniones con el personal del proyecto. -Realizar el cuestionario para identificar los riesgos. - Elaborar la Matriz de riesgo. -Elaborar el registro de los riesgos. -Caracterizar los riesgos (Matriz Taxonómica). -Comunicar Resultados al proyecto.	-Controlar los riesgos identificados -Identificar nuevos riesgos.	-Cada 1 o 2 meses depende la duración de la etapa en que se encuentre el proyecto. -Durante las reuniones normales del proyecto.
Análisis del riesgo	Equipo de GR.	**Actividades** -Establecer valores para el impacto de los riesgos. -Determinar la probabilidad de ocurrencia de los riesgos.	-Priorizar los nuevos riesgos encontrados - Dar parte del estado del proyecto según sus riesgos.	-Cada 1 o 2 meses depende la duración de la etapa en que se encuentre el proyecto. -Durante las reuniones normales del proyecto.

		-Evaluar los riesgos en la matriz de probabilidad e impacto. -Priorizar los riesgos. -Comunicar Resultados al proyecto.		
Planificación de la respuesta a los riesgos	Equipo de GR. Equipo del proyecto. **Gestor de Riesgo:** Jefe de Proyecto	-Elaboración de un plan de mitigación de riesgos. -Elaboración de un plan de Contingencias. -Comunicar Resultados al proyecto.	-Revisar continuamente los planes de mitigación y contingencia -Verificar si las medidas tomadas han sido satisfactorias.	-Cada 1 o 2 meses depende la duración de la etapa en que se encuentre el proyecto. -Durante las reuniones normales del proyecto.

Anexo 4. Lista de chequeo para la identificación de los riesgos del proyecto SIGEP.

Identificar riesgos Asociados con el Personal:

1. ¿Ha existido incompatibilidad con los horarios en el equipo?
2. ¿Ha existido falta de conocimiento y experiencias en el personal del proyecto?
3. ¿Han existido cambios en el personal del proyecto?
4. ¿Ha existido falta de motivación en el proyecto?
5. ¿Algún miembro del equipo ha pedido la baja ó ha desertado del proyecto?
6. ¿El personal del proyecto cumple con el horario de trabajo?
7. ¿Han existido disputas entre personal de trabajo?
8. ¿Ha existido la necesidad de más programadores en el proyecto?
9. ¿El personal del proyecto anteriormente a este había trabajado en equipo?
10. ¿Tienen experiencias los miembros del equipo en los roles que desempeñan?
11. ¿Tienen los miembros del equipo otras cargas además del trabajo en el proyecto?
12. ¿Ha participado todo el personal del proyecto en las etapas de las BET para adelantar el mismo?
13. ¿Ha existido dificultad en el uso de algunas herramientas por parte del equipo?
14. ¿No han logrado los miembros del equipo trabajar bien juntos?
15. ¿No se ha realizado correctamente el seguimiento de los riesgos en el proyecto?

Identificar riesgos asociados al Entorno de Desarrollo:

16. ¿Existen herramientas de análisis y diseño disponibles?
17. ¿Hay disponibles herramientas de pruebas apropiadas para el producto que se va a realizar?
18. ¿Se tiene disponibles herramientas para la gestión de configuración de software?
19. ¿Se hace uso del entorno de bases de datos o información almacenada?
20. ¿Existen expertos que respondan a las dudas que surjan con las herramientas?
21. ¿Se han empleado herramientas de software para apoyar la planificación y seguimiento de las actividades?
22. ¿Tenemos disponible una herramienta de gestión de proyectos de software?
23. ¿Hay disponibles compiladores o generadores de código apropiados para el producto a construir?
24. ¿Hace uso el entorno de bases de datos o información almacenada?
25. ¿Están todas las herramientas de software integradas entre sí?
26. ¿Se ha formado a los miembros del equipo del proyecto en todas las herramientas?

Identificar riesgos organizacionales:

27. ¿Se llevan a cabo periódicamente revisiones técnicas formales de las especificaciones de requisitos, diseño y código?

28. ¿Se llevan a cabo periódicamente revisiones técnicas de los procesos de pruebas y de los casos de prueba?
29. ¿Se documentan todos los resultados de las revisiones técnicas incluyendo los errores encontrados y recursos empleados?
30. ¿Hay algún mecanismo de control de cambio de los requisitos del cliente que impacten en el software?
31. ¿El cliente siempre está dispuesto a participar en las revisiones?
32. ¿Se han incumplido en la planificación del flujo de trabajo de proyecto por otras actividades como marchas, actos, etc.?
33. ¿Se han distribuido siempre adecuadamente las tareas entre los miembros del equipo?
34. ¿Han existido cambios en las condiciones de los laboratorios?
35. ¿Han existido cambios en la fecha de entrega porque el producto no ha estado terminado?
36. ¿Se han definido y empleado reglas especificas para la documentación del código?
37. ¿Se ha establecidos métricas de Calidad en el proyecto?
38. ¿Ha sido correcta la repartición del trabajo?

Identificar riesgos Tecnológicos del Proyecto SIGEP

39. Ha existido un eficiente acceso a la Base de Datos.
40. Es suficiente la capacidad de almacenamiento del servidor.
41. Se han utilizado nuevas tecnologías desconocidas por los estudiantes del proyecto.
42. Ha existido un aprendizaje ineficaz de las nuevas tecnologías de los integrantes del proyecto.
43. La base de Datos que usa el proyecto es adecuada.
44. La interfaz grafica del proyecto funciona adecuadamente.
45. Han surgido limitaciones en el lenguaje de programación utilizado.
46. Se ha tenido necesidad de tener mayores recursos de hardware (Disco duros, memorias).
47. Ha existido falta de espacio en los laboratorios asignados al proyecto.
48. Se ha contado con pocos equipos y estos con tecnología atrasada.
49. Han ocurrido problemas entre la BD y la Aplicación.
50. Se han asignado las PC necesarias para el proyecto.
51. Han existido problemas con la BD y el Sub Versión.
52. Se ha tenido problema con la electricidad.
53. Problemas con el servidor.
54. Problemas con el rendimiento y la velocidad de respuestas en las aplicaciones Web del proyecto.
55. Demandan los requisitos una interfaz de usuario especial.
56. Demandan los requisitos del producto el empleo de nuevos métodos de análisis, diseño o pruebas.

57. No está seguro el cliente que las funcionalidades pedidas sea factibles.
58. ¿Se emplean técnicas de especificación de aplicaciones para ayudar en la comunicación entre el cliente y el desarrollador?
59. ¿Se emplean métodos específicos para el análisis del software?
60. ¿Emplea un método específico para el diseño de datos y arquitectónico?
61. ¿Está escrito su código en más de un 90 por ciento en lenguaje de alto nivel?
62. ¿Se han definido y empleado reglas específicas para la documentación del código?
63. ¿Emplea métodos específicos para el diseño de casos de prueba?
64. ¿Se emplean herramientas de software para apoyar la planificación y el seguimiento de las actividades?
65. ¿Se emplean herramientas de software de gestión de configuración para controlar y seguir los cambios a lo largo de todo el proceso del software?
66. ¿Se emplean herramientas de software para apoyar los procesos de análisis y diseño del software?
67. ¿Se emplean herramientas para crear prototipos software?
68. ¿Se emplean herramientas de software para dar soporte a los procesos de prueba?
69. ¿Se emplean herramientas de software para soportar la producción y gestión de la documentación?
70. ¿Se han establecido métricas de calidad para todos los proyectos de software?
71. ¿Se han establecido métricas de productividad para todos los proyectos de software?
72. ¿El software interactúa con hardware nuevo o no probado?
73. ¿Interactúa el software a construir con productos software suministrados por el vendedor que no se hayan probado?
74. ¿Demandan los requisitos del producto la creación de componentes de programación distintos de; los que su organización haya desarrollado hasta ahora?
75. ¿Demandan los requisitos el empleo de nuevos métodos de análisis, diseño o pruebas?

Identificar riesgos asociados con el impacto en el negocio

76. ¿Efecto de este producto en los ingresos de la compañía?
77. ¿Viabilidad de este producto para los gestores expertos?
78. ¿Es razonable la fecha límite de entrega?
79. ¿Número de clientes que usarán este producto y la consistencia de sus necesidades relativas al producto?
80. ¿Número de otros productos/sistemas con los que este producto debe tener interoperabilidad?
81. ¿Sofisticación del usuario final?

82. ¿Cantidad y calidad de la documentación del producto que debe ser elaborada y entregada al cliente?
83. ¿Limitaciones gubernamentales en la construcción del producto?
84. ¿Costos asociados por un retraso en la entrega?
85. ¿Costos asociados con un producto defectuoso?

Identificar riesgos asociados con el cliente

86. ¿Ha trabajado con el cliente anteriormente?
87. ¿Tiene el cliente una idea formal de lo que se requiere? ¿Se ha molestado en escribirlo?
88. ¿Aceptará el cliente gastar su tiempo en reuniones formales de requisitos para identificar el ámbito del proyecto?
89. ¿Está dispuesto el cliente a establecer una comunicación fluida con el desarrollador?
90. ¿Está dispuesto el cliente a participar en las revisiones?
91. ¿Es sofisticado técnicamente el área del producto?
92. ¿Está dispuesto el cliente a dejar a su personal hacer el trabajo? Es decir, ¿resistirá la tentación de mirar por encima del hombro durante el trabajo técnico?
93. ¿Entiende el cliente el proceso del software?

Identificar riesgos asociados con aspectos del proceso

94. ¿Ha desarrollado su organización una descripción escrita del proceso del software a emplear en este proyecto?
95. ¿Están de acuerdo los miembros del personal con el proceso del software tal y como está documentado y están dispuestos a usarlo?
96. ¿Se emplea este proceso del software para otros proyectos?
97. ¿Ha desarrollado o adquirido su organización cursos de formación de ingeniería del software para jefes de proyecto y personal técnico?
98. ¿Se ha proporcionado una copia de los estándares de ingeniería del software publicados a cada desarrollador y gestor de software?
99. ¿Se han desarrollado diseños de documentos y ejemplos para todas las entregas definidas como parte del proceso del software?
100. ¿Se llevan a cabo regularmente revisiones técnicas formales de las especificaciones de requisitos, diseño y código?
101. ¿Se llevan a cabo regularmente: revisiones técnicas de los procedimientos de prueba y de los casos de prueba?
102. ¿Se documentan todos los resultados de las revisiones técnicas, incluyendo los errores encontrados y recursos empleados?

103. ¿Existe algún mecanismo para asegurarse de que el trabajo realizado en un proyecto se ajusta a los estándares de ingeniería del software?

104. ¿Se emplea una gestión de configuración para mantener la consistencia entre los requisitos del sistema/software, diseño, código y casos de prueba?

105. ¿Hay algún mecanismo de control de cambios de los requisitos del cliente que impacten en el software?

106. ¿Hay alguna declaración de trabajo documentada, una especificación de requisitos software y un plan de desarrollo del software para cada subcontratación?

Anexo 5. Plantilla Archivo de Riesgos.

albet
INGENIERÍA Y SISTEMAS

Proyecto para la Humanización Penitenciaria

Sistema de Gestión Penitenciaria

ARCHIVO DE RIESGOS

VERSION <X.X>

Revisión Histórica

Fecha	Versión	Descripción	Autor
<dd/mmm/yy>	<x.x>	<detalles>	<nombre>

Reglas de Seguridad

El que recibe el documento asume la custodia y control, comprometiéndose a no reproducir, divulgar, difundir o de cualquier manera hacer de conocimientos público su contenido, excepto para cumplir el propósito para el cual se ha generado.

Estas reglas son aplicables a las __ páginas de este documento.

Tabla de Contenido

1. Introducción

[Información necesaria para entender el documento]

1.1 Alcance

[Proyecto SIGEP y proyectos facultad 4]

1.2 Referencias

[Lista de documentos a los que se hace referencia en el Plan]

1.3 Glosario

[En caso de usarse en la plantilla términos básicos de difícil comprensión o siglas no evidentes]

2. Matriz de Riesgos

ID	Riesgos	Descripción
<1>	*Nombre del Riesgo*	*Breve descripción del riesgo*

3. Matriz taxonómica de Riesgos

CRITERIO	Según La Cobertura		Según el área que amenazan			Según el conocimiento sobre ellos		Según su naturaleza (Consecuencias)		
CLASIFICACIÓN	Genéricos	Específicos del Proyecto	Del Proyecto	Del Negocio	Técnicos	Especulativos	Puros	Conocidos	Predecibles	Impredecibles
ID										

4. **Riesgos Evaluados en la Matriz de Probabilidad e Impacto**

ID	Riesgos	Probabilidad	Impacto	Efecto
<1>	*Nombre del Riesgo*	*Probabilidad de ocurrencia.*	*Impacto del riesgo.*	*Probabilidad x Impacto.*

Anexo 5A. Matriz de los riesgos del proyecto SIGEP, Matriz taxonómica de los riesgos y riesgos evaluados en la matriz de severidad del riesgo.

Aquí se muestra una representación de 15 riesgos en los artefactos mencionados anteriormente.

Matriz de los riesgos del proyecto SIGEP.

ID	Riesgos	Descripción
36	Superficial captura de requisitos.	Sería la principal causa de fracaso del proyecto. Es importante realizar un detallado modelo de negocio, el cual sería imposible sin el contacto directo con los futuros usuarios del sistema y sin comprender cómo funcionan los establecimientos penitenciarios y sus necesidades informativas.
37	Cambio de los requisitos del software	Puede conllevar a la reestructuración del proyecto o a la adquisición de nuevas tecnologías.
38	Falta de infraestructura para el despliegue.	Es posible que el software posea funciones inhabilitadas, o que por no tenerlas previstas presente errores de ejecución.
39	Mayoría de diseñadores y programadores en 5to año.	Rendimiento de programadores afectado y esto conlleva a atraso en el proyecto.
40	Inexperiencia de los nuevos incorporados al proyecto.	El desarrollo de esta etapa no pueda sustentarse en el corto plazo con los compañeros incorporados.
42	Posible egreso de la UCI de los programadores y diseñadores más experimentados.	Puede influir negativamente tanto en la finalización de la programación, como en la puesta a punto de la solución de software durante el piloto y el período de soporte.
43	Desarrollar más casos de uso que los acordados.	Más tiempo de desarrollo, o un sobreesfuerzo del equipo de desarrollo.
45	No uniformidad en cuanto a forma y contenido de la información que actualmente se maneja.	Actualmente la información que maneja cada establecimiento penitenciario con relación a los privados de libertad, es diversa, no recoge los mismos datos y no obedece un flujo informativo uniforme; y el nuevo modelo de funcionamiento necesita ser organizado previo a la carga inicial de los datos al sistema, a modo de garantizar que pueda ser almacenada la información histórica en el sistema informático.
46	No satisfactorio nivel de definición de procesos operativos	En las áreas en las que no se cuente con una adecuada descripción de los procesos, el producto informático no contemplará un nivel de detalle de los mismos, pudiendo quedar actividades sin informatizar y otras a un nivel elemental o detalladas a partir de la experiencia del equipo de desarrollo en

		otros sistemas similares.
47	Mal estado de la infraestructura física.	De manera general existe un deterioro en la infraestructura civil de los establecimientos penitenciarios. Además no existen los locales apropiados con las condiciones mínimas requeridas para la instalación de la tecnología (servidor de datos y aplicaciones, equipos telemáticos).

ID	Riesgos	Descripción
48	Ausencia de personal técnico para administrar el sistema.	Las actividades administrativas para mantener disponible la tecnología instalada requieren de la participación de un personal técnico con conocimientos sobre administración de bases de datos Oracle, administración de aplicaciones Web sobre J2EE y de administración de redes locales. Este personal no existe actualmente en la institución y se requiere de su presencia oportuna, a fin de que reciba la preparación necesaria para garantizar el uso y explotación del sistema en cada uno de los establecimientos penitenciarios.
49	Uso inadecuado de las aplicaciones informáticas.	Independientemente de las políticas de seguridad propias del sistema, estas no son efectivas si no existe organización en el manejo administrativo de la documentación y la gobernabilidad en los establecimientos penitenciarios, que garantice un uso correcto del sistema informático por las personas encargadas de operarlo.
50	Inseguridad en el interior de los establecimientos penitenciarios.	La ejecución de muchas actividades podrá verse afectada por la ocurrencia de cualquier contingencia en los establecimientos penitenciarios e incluso por información que se maneje sobre la posibilidad de su ocurrencia. Esta situación también interfiere con la operación cotidiana del SIGEP, poniendo en peligro la integridad de la data y los equipos.
51	Mantenimiento de la tecnología instalada.	El óptimo funcionamiento de la tecnología instalada en los establecimientos penitenciarios, se garantiza a través de una política de mantenimiento (sea preventivo o correctivo) que deberá ejecutar un personal técnico debidamente capacitado.
52	Fallo en la conectividad.	Algunas tareas administrativas remotas no podrán ejecutarse si la conectividad no es buena, como tampoco podrían realizarse consultas a la base de datos central.
53	Los sistemas externos no ofrecen las interfaces necesarias para establecer la comunicación con estos.	Para desarrollar las interfaces de comunicación con sistemas externos es necesario establecer un protocolo entre ambas partes y desarrollar cada una, los componentes necesarios para ofrecer los servicios que se requieren por la otra parte.

Matriz Taxonómica de los riesgos.

CRITERIO	Según La Cobertura		Según el área que amenazan			Según el conocimiento sobre ellos		Según su naturaleza (Consecuencias)		
CLASIFICACIÓN	Genéricos	Específicos del Proyecto	Del Proyecto	Del Negocio	Técnicos	Especulativos	Puros	Conocidos	Predecibles	Impredecibles
ID		36	36				36	36		
		37	37			37	37			37
		38	38				38	38		
		39	39			39	39	39		
		40	40				40	40		
		42	42				42	42		

CRITERIO	Según La Cobertura		Según el área que amenazan			Según el conocimiento sobre ellos		Según su naturaleza (Consecuencias)		
CLASIFICACIÓN	Genéricos	Específicos del Proyecto	Del Proyecto	Del Negocio	Técnicos	Especulativos	Puros	Conocidos	Predecibles	Impredecibles
ID		43			43	43	43			43
		45			45		45	45		
		46	46				46	46		
		47			47		47	47		
		48	48		48		48	48		
		49	49				49	49		

CRITERIO	Según La Cobertura		Según el área que amenazan			Según el conocimiento sobre ellos		Según su naturaleza (Consecuencias)		
CLASIFICACIÓN	Genéricos	Específicos del Proyecto	Del Proyecto	Del Negocio	Técnicos	Especulativos	Puros	Conocidos	Predecibles	Impredecibles
ID		50	50		50		50	50		
		51			51		51	51		
		52			52		52	52		
		53	53				53	53		

Matriz de severidad del riesgo.

ID	Riesgos	Probabilidad	Impacto	Efecto
36	Superficial captura de requisitos.	0.7	0.9	Crítico
37	Cambio de los requisitos del software.	0.7	0.5	Crítico
38	Falta de infraestructura para el despliegue.	0.7	0.7	Crítico
39	Mayoría de diseñadores y programadores en 5to año.	0.9	0.7	Crítico
40	Inexperiencia de los nuevos incorporados al proyecto.	0.9	0.7	Crítico
42	Posible egreso de la UCI de los programadores y diseñadores más experimentados.	0.7	0.7	Crítico
43	Desarrollar más casos de uso que los acordados.	0.7	0.7	Crítico
45	No uniformidad en cuanto a forma y contenido de la información que actualmente se maneja.	0.9	0.7	Crítico
46	No satisfactorio nivel de definición de procesos operativos	0.9	0.9	Crítico
47	Mal estado de la infraestructura física.	0.9	0.9	Crítico
48	Ausencia de personal técnico para administrar el sistema.	0.9	0.7	Crítico
49	Uso inadecuado de las aplicaciones informáticas.	0.7	0.7	Crítico
50	Inseguridad en el interior de los establecimientos penitenciarios.	0.9	0.9	Crítico
51	Mantenimiento de la tecnología instalada.	0.7	0.9	Crítico
52	Fallo en la conectividad.	0.7	0.7	Crítico
53	Los sistemas externos no ofrecen las interfaces necesarias para establecer la comunicación con estos.	0.7	0.7	Crítico

Anexo 6: Plantilla del registro de riesgos.

Proyecto para la Humanización Penitenciaria

Sistema de Gestión Penitenciaria

REGISTRO DE RIESGOS

VERSION <X.X>

Revisión Histórica

Fecha	Versión	Descripción	Autor
<dd/mmm/yy>	<x.x>	<detalles>	<nombre>

Reglas de Seguridad

El que recibe el documento asume la custodia y control, comprometiéndose a no reproducir, divulgar, difundir o de cualquier manera hacer de conocimientos público su contenido, excepto para cumplir el propósito para el cual se ha generado.

Estas reglas son aplicables a las __ páginas de este documento.

Tabla de Contenido

1. Introducción

[Información necesaria para entender el documento]

1.1 Alcance

[Proyecto SIGEP y proyectos facultad 4]

1.2 Referencias

[Lista de documentos a los que se hace referencia en el Plan]

1.3 Glosario

[En caso de usarse en la plantilla términos básicos de difícil comprensión o siglas no evidentes]

2. Registro de Riesgo SIGEP.

Id	Categoría	Probabilidad	Impacto	Efecto
Identificador	*Identificador de la categoría.(Una de las definidas por el modelo)*	*Probabilidad de ocurrencia*	*Impacto*	*Probabilidad x Impacto*
Causa	*Descripción textual de la causa que origina el riesgo. (El nombre de cada evento de riesgo).*			
Descripción	*Descripción textual del suceso incierto que causa preocupación.*			
Consecuencia	*Descripción textual de las consecuencias que trae la ocurrencia del evento.*			
Etapa	*Etapa del proyecto donde se manifiesta el riesgo (Conceptual /Estructural / Ejecución / Cierre / Soporte).*			
Estrategia de Mitigación	*Estrategia utilizada para mitigar el riesgo.*			
Estado	*Uno de estos valores: identificado, analizado, activo, cerrado, reabierto.*			

Anexo 6A: Representación de los 15 riesgos analizados en el Registro de Riesgos.

Id	Categoría	Probabilidad	Impacto	Efecto
36	Proyecto	0.7	0.9	Crítico
Causa	Superficial captura de requisitos.			
Descripción	El sistema penitenciario está sufriendo una sustancial modificación. Si no se tienen contactos con las personas que dirigen el sistema penitenciario, con quienes dirigen los penales y con los futuros usuarios del sistema la captura			

	de requisitos será superficial.
Consecuencia	Sería la principal causa de fracaso del proyecto. Es importante realizar un detallado modelo de negocio, el cual sería imposible sin el contacto directo con los futuros usuarios del sistema y sin comprender cómo funcionan los establecimientos penitenciarios y sus necesidades informativas.
Etapa	Ejecución
Estrategia de Mitigación	Entrevistas con funcionarios de la Dirección General de Custodia y Rehabilitación del Recluso. Realizar visitas a centros penitenciarios, observar el funcionamiento de los mismos y entrevistarse con los principales involucrados en la gestión del penal y futuros usuarios del sistema. Tener una contraparte venezolana que revise el artefacto Visión, el Modelo de Casos de Uso, el prototipo de Interfaz de usuario, de manera
Estado	Cerrado

Id	**Categoría**	**Probabilidad**	**Impacto**	**Efecto**
37	Proyecto	0.7	0.5	Crítico
Causa	Cambio de los requisitos del software.			
Descripción	Los requisitos por naturaleza pueden ser cambiantes y no es posible capturar el 100% de ellos estrictamente en las primeras etapas del desarrollo del proyecto.			
Consecuencia	Puede conllevar a la reestructuración del proyecto o a la adquisición de nuevas tecnologías.			
Etapa	Ejecución			
Estrategia de Mitigación	Es un riesgo que no se puede evitar, pero se puede minimizar haciendo un esfuerzo en el diseño, para en el caso de tener que cambiar algo se pueda hacer de la manera más eficiente sin tener que reestructurar todo el proyecto.			
Estado	Cerrado			

Id	**Categoría**	**Probabilidad**	**Impacto**	**Efecto**
38	Proyecto	0.7	0.5	Crítico
Causa	Falta de infraestructura para el despliegue.			
Descripción	El software pudiera estar elaborado sobre suposiciones de una tecnología de			

	base instalada y tales condiciones no existan a la hora de instalar la aplicación. Por ejemplo, puede que la infraestructura de red no esté y no puedan ejecutarse funcionalidades programadas. Este tipo de problema puede presentarse debido a la actual inexistencia de infraestructura informática en las prisiones venezolanas y por las distancias a las que algunas se encuentran de centros urbanos que dificultarían una comunicación a través de una red de transmisión de datos.
Consecuencia	Es posible que el software posea funciones inhabilitadas, o que por no tenerlas previstas presente errores de ejecución.
Etapa	Cierre
Estrategia de Mitigación	El diseño deberá considerar un abanico de posibilidades en cuanto a la infraestructura de hardware y el ambiente en que funcionará el software. Deberá tenerse en cuenta este aspecto durante la captura de requisitos.
Estado	Activo

Id	**Categoría**	**Probabilidad**	**Impacto**	**Efecto**
39	Proyecto	0.9	0.7	Crítico
Causa	Mayoría de diseñadores y programadores en 5to año.			
Descripción	Los 34 estudiantes de 5to año que pertenecen al proyecto representan el 38% de sus miembros y concentran los roles fundamentales de la implementación (diseñadores y programadores). La productividad está sustentada fundamentalmente en esta fuerza de trabajo por ser los más experimentados y preparados. El rendimiento de estos compañeros puede verse afectado por actividades docentes propias de este año: Prueba de nivel: los compañeros que participaron en Venezuela en la puesta a punto del piloto durante los meses noviembre-enero, tienen pendiente este examen, el cual debe efectuarse en la semana del 17-21 de marzo. Tesis: los estudiantes en su mayoría han desarrollado su trabajo práctico, pero tienen pendiente la realización del documento de tesis, labor que consumirá tiempo.			
Consecuencia	Rendimiento de programadores afectado y esto conlleva a atraso en el proyecto.			
Etapa	Ejecución, Cierre			
Estrategia de Mitigación	• Los profesores del proyecto están impartiendo preparación a los estudiantes que tienen pendiente la prueba de nivel. • Se elaboró una propuesta para modificar el contenido del documento de tesis de modo que se ajuste a un formato más reducido, sin dejar de incluir el problema, los objetivos y la solución propuesta. El conjunto de documentos conformarían una memoria colectiva del			

	proyecto. La propuesta fundamentada fue presentada en la primera quincena de enero a la facultad. Aun no se ha recibido una respuesta oficial de aprobación o rechazo de la misma. Esta variante de tesis ofrecería mayor disponibilidad de tiempo a los desarrolladores más experimentados.
Estado	Cerrado

Id	**Categoría**	**Probabilidad**	**Impacto**	**Efecto**
40	Proyecto	0.9	0.7	Crítico
Causa	Inexperiencia de los nuevos incorporados al proyecto.			
Descripción	Se incorporan 24 miembros al proyecto como programadores y aseguradores de calidad, en su mayoría estudiantes de 3er año que tiene una carga docente elevada. Recibieron una preparación previa pero no tienen experiencia en el trabajo en proyecto, ni han creado las habilidades que se requieren para ser totalmente productivos en un primer momento. Esto determina que el desarrollo de esta etapa no pueda sustentarse en el corto plazo con los compañeros incorporados.			
Consecuencia	El desarrollo de esta etapa no pueda sustentarse en el corto plazo con los compañeros incorporados traería atraso y deficiencias en el trabajo.			
Etapa	Ejecución, Cierre			
Estrategia de Mitigación	Fueron distribuidos entre los equipos de desarrollo de modo que trabajen de conjunto con los programadores de experiencia. Se les irán asignado tareas que gradualmente aumentarán su nivel de complejidad.			
Estado	Activo			

Id	**Categoría**	**Probabilidad**	**Impacto**	**Efecto**
42	Proyecto	0.7	0.7	Crítico
Causa	Posible egreso de la UCI de los programadores y diseñadores más experimentados.			
Descripción	Como el fin del proyecto está previsto para julio, el egreso de los estudiantes de 5to año puede influir negativamente tanto en la finalización de la programación, como en la puesta a punto de la solución de software durante el piloto y el período de soporte.			
Consecuencia	Puede influir negativamente tanto en la finalización de la programación, como en la puesta a punto de la solución de software durante el piloto y el período de soporte.			
Etapa	Ejecución, Cierre			

Estrategia de Mitigación	Proponer a la dirección de la Facultad 4 y de la UCI, mantener en la universidad una vez graduados, a aquellos miembros del equipo de desarrollo cuyo trabajo sea significativo para el éxito del proyecto.
Estado	Cerrado

Id	**Categoría**	**Probabilidad**	**Impacto**	**Efecto**
43	Técnico	0.7	0.7	Crítico
Causa	Desarrollar más casos de uso que los acordados.			
Descripción	Durante la recién concluida captura de requisitos fueron identificados 200 casos de uso. Este número pudiera variar ligeramente durante el análisis, pero puede tomarse como referencia. Si a esta cantidad de casos de uso, se le suman los 223 ya desarrollados en la etapa I, el total sería de 423. Lo pactado en contrato fueron 351, incluyendo los del portal web. El total actual sobrepasaría lo acordado en 71 casos de uso.			
Consecuencia	Más tiempo de desarrollo, o un sobreesfuerzo del equipo de desarrollo.			
Etapa	Ejecución			
Estrategia de Mitigación	Negociar con la parte venezolana aplazar el desarrollo de los módulos menos significativos para el negocio para una próxima Mixta (Ejemplo: biblioteca, plan de presentaciones).			
Estado	Cerrado			

Id	**Categoría**	**Probabilidad**	**Impacto**	**Efecto**
46	Técnico	0.9	0.7	Crítico
Causa	No satisfactorio nivel de definición de procesos operativos.			
Descripción	La Dirección General de Custodia y Rehabilitación del Recluso, institución para la cual se pretende desarrollar el SIGEP, se encuentra inmersa en un profundo proceso de transformación organizacional. En este proceso surgen nuevas áreas de trabajo, se modifican los cargos y en general se encaminan esfuerzos para crear un nuevo modelo de funcionamiento, para una institución que hasta el momento no ha alcanzado los niveles de eficacia deseados en el cumplimiento de su misión con su modelo actual. En las áreas en las que no se cuente con una adecuada descripción de los procesos, el producto informático no contemplará un nivel de detalle de los mismos, pudiendo quedar actividades sin informatizar y otras a un nivel elemental o detalladas a partir de la experiencia del equipo de desarrollo en			

	otros sistemas similares.
Consecuencia	El tiempo que debe emplearse en las tareas de adecuación de la descripción de los procesos, puede impactar en el cronograma de ejecución de la solución de software, puesto que un levantamiento de requisitos objetivo, dependería de este resultado.
Etapa	Estructural
Estrategia de Mitigación	Se recomienda avanzar en la definición detallada de estos procesos a través, por ejemplo, de reuniones grupales en las que participen los especialistas funcionales de cada área, el componente de recursos humanos que diseñó la transformación, representantes del componente tecnológico, el grupo de asesores cubanos en materias penitenciarias, una especialista en procesos y un experto en temas legales, con el objetivo de readecuar la descripción de los procesos y el flujo de información a partir del resultado del trabajo de esos encuentros. Además, para mitigar este importante riesgo, el desarrollo del software se concibe por etapas, para incluir progresivamente en cada una de ellas, las áreas funcionales y procesos que poseen un mayor nivel de definición, dejando los menos definidos para las etapas finales, de modo que se pueda avanzar en la concepción de estos previos a su automatización.
Estado	Cerrado

Id	**Categoría**	**Probabilidad**	**Impacto**	**Efecto**
47	Técnico	0.9	0.9	Crítico
Causa	Mal estado de la infraestructura física			
Descripción	De manera general existe un deterioro en la infraestructura civil de los establecimientos penitenciarios. Además no existen los locales apropiados con las condiciones mínimas requeridas para la instalación de la tecnología (servidor de datos y aplicaciones, equipos telemáticos).			
Consecuencia	Cabe destacar que el despliegue de la solución de software está supeditado a la realización de estas adecuaciones.			
Etapa	Cierre			
Estrategia de Mitigación	Se hace necesario realizar un recorrido por cada una de las entidades del sistema penitenciario donde será instalado el SIGEP, con el objetivo de diagnosticar las condiciones de infraestructura existentes y establecer las adecuaciones necesarias tanto de la obra civil, como las que garanticen seguridad, clima y suministro de energía eléctrica demandadas por la tecnología a instalarse. El recorrido requiere del apoyo de la Dirección General de Custodia y Rehabilitación del Recluso, con su participación directa en las actividades del diagnóstico de condiciones físicas, a modo de garantizar las coordinaciones necesarias para la realización de la visita, para la selección de los locales de instalación de la tecnología y la posterior			

	ejecución de las adecuaciones en la infraestructura.
Estado	Activo

Id	**Categoría**	**Probabilidad**	**Impacto**	**Efecto**
48	Técnico	0.9	0.9	Crítico
Causa	Ausencia de personal técnico para administrar el sistema.			
Descripción	El sistema concibe la instalación de un servidor de base de datos y de aplicaciones para cada uno de los establecimientos penitenciarios, así como una infraestructura de red que requiere ser gestionada. Las actividades administrativas para mantener disponible la tecnología instalada requieren de la participación de un personal técnico con conocimientos sobre administración de bases de datos Oracle, administración de aplicaciones Web sobre J2EE y de administración de redes locales.			
Consecuencia	No se puede instalar los sistemas en las prisiones y no se puede mantener el sistema porque no se tiene el personal adecuado.			
Etapa	Soporte			
Estrategia de Mitigación	Seleccionar el personal requerido para esta tarea y una vez que estén definidos empezar con la capacitación de ellos para que reciban la preparación necesaria para garantizar el uso y explotación del sistema en cada uno de los establecimientos penitenciarios.			
Estado	Analizado			

Id	**Categoría**	**Probabilidad**	**Impacto**	**Efecto**
49	Proyecto	0.7	0.7	Crítico
Causa	Uso inadecuado de las aplicaciones informáticas.			
Descripción	Existe necesidad de que la información que entre al sistema informático sea veraz, aprobada por el nivel correspondiente, auditada e introducida por las personas autorizadas. Independientemente de las políticas de seguridad propias del sistema, estas no son efectivas si no existe organización en el manejo administrativo de la documentación y la gobernabilidad en los establecimientos penitenciarios, que garantice un uso correcto del sistema informático por las personas encargadas de operarlo.			

Consecuencia	El software no cumple su objetivo ya que el personal que esta a cargo de el puede introducir información no clasificada. Es decir se pierde la integridad del software y el valor para el cual fue hecho.
Etapa	Cierre
Estrategia de Mitigación	Se recomienda la incorporación de personal confiable para el manejo del sistema informático y garantizar el respeto por las políticas de acceso que propone el sistema. Se recomienda también la formulación de un reglamento que contenga todas disposiciones necesarias para lograr uniformidad y disciplina en el uso del sistema. Contemplar la automatización en el sistema de validaciones de uso y coherencia, que activen notificaciones a los niveles táctico y estratégico.
Estado	Analizado

Id	**Categoría**	**Probabilidad**	**Impacto**	**Efecto**
50	Técnico, Proyecto	0.9	0.9	Crítico
Causa	Inseguridad en el interior de los establecimientos penitenciarios.			
Descripción	El clima de violencia y de inseguridad existente en los establecimientos penitenciarios condiciona el trabajo de los especialistas técnicos, encargados de la instalación de la tecnología informática y del entrenamiento en sitio previsto para el personal que operará el sistema. La ejecución de estas actividades podrá verse afectada por la ocurrencia de cualquier contingencia en los establecimientos penitenciarios e incluso por información que se maneje sobre la posibilidad de su ocurrencia.			
Consecuencia	Interfiere con la operación cotidiana del SIGEP, poniendo en peligro la integridad de la data y los equipos.			
Etapa	Cierre y Soporte			
Estrategia de Mitigación	Se recomienda aprovechar las adecuaciones de la infraestructura física para contar con un espacio de resguardo de los equipos en caso que se presente una situación que amenace su integridad. Se recomienda además proteger los equipos a través de la adquisición de un seguro que cubra robo, vandalismo, desastres, etc., pues esto no se contempla dentro del alcance del presente proyecto.			
Estado	Activo			

Id	**Categoría**	**Probabilidad**	**Impacto**	**Efecto**
51	Técnico, Proyecto	0.9	0.9	Crítico

Causa	Mantenimiento de la tecnología instalada.
Descripción	El óptimo funcionamiento de la tecnología instalada en los establecimientos penitenciarios, se garantiza a través de una política de mantenimiento (sea preventivo o correctivo) que deberá ejecutar un personal técnico debidamente capacitado.
Consecuencia	Si el sistema sufre algún desperfecto y no se encuentra el soporte técnico cerca hay que esperar por el y esto trae atraso en el trabajo; además este soporte esta planificado solo por un año y después de esto cada establecimiento debe garantizar la buena funcionalidad del sistema. Para que el trabajo sea fructífero.
Etapa	Soporte
Estrategia de Mitigación	Si bien dentro del alcance de la solución de software está previsto el soporte técnico por período de un año, a partir del momento de la instalación en cada establecimiento, la Dirección General deberá garantizar un equipo técnico, que debidamente entrenado, pueda atender el mantenimiento y la actualización, tanto de las aplicaciones informáticas, como del equipamiento instalado. Este equipo técnico debe estar conformado por ingenieros especializados en las áreas de la informática y la telemática, y familiarizados además con la tecnología de software y hardware usadas en la solución.
Estado	Analizado

Id	**Categoría**	**Probabilidad**	**Impacto**	**Efecto**
52	Técnico	0.7	0.7	Crítico
Causa	Fallo en la conectividad.			
Descripción	Por la ubicación distante de la mayoría de los establecimientos penitenciarios y la necesidad de mantener actualizada la información del centro de datos, es imprescindible garantizar con este punto, una conexión disponible y de calidad, desde los establecimientos penitenciarios.			
Consecuencia	Algunas tareas administrativas remotas no podrán ejecutarse si la conectividad no es buena, como tampoco podrían realizarse consultas a la base de datos central.			
Etapa	Cierre, Soporte			
Estrategia de Mitigación	Para minimizar este riesgo, el sistema funcionará de manera autónoma con una base de datos local en cada establecimiento penitenciario y sólo utilizaría el canal de comunicación con el exterior para las actividades de réplica de la base de datos y consulta de datos globales. De igual modo la			

	comunicación se debe establecer por un canal seguro.
Estado	Analizado

Id	**Categoría**	**Probabilidad**	**Impacto**	**Efecto**
53	Proyecto	0.7	0.7	Crítico
Causa	Los sistemas externos no ofrecen las interfaces necesarias para establecer la comunicación con estos.			
Descripción	Para desarrollar las interfaces de comunicación con sistemas externos es necesario establecer un protocolo entre ambas partes y desarrollar cada una, los componentes necesarios para ofrecer los servicios que se requieren por la otra parte. El SIGEP, previo acuerdo con las partes interesadas, ofrecerá las interfaces que se demanden y a su vez usará las interfaces que los sistemas externos provean para estos fines.			
Consecuencia	Sino se acuerda un protocolo común para estas interfaces el sistema no podrá usarlas ya que en ningún caso, el desarrollo del SIGEP concibe crear las interfaces de terceros sistemas, sino usar las interfaces ya existentes o acordadas con estos sistemas y proveer las necesarias. Esto afecta la funcionalidad del sistema.			
Etapa	Cierre			
Estrategia de Mitigación	Para que esto se lleve a cabo con éxito, es necesario que estén desarrollados los servicios para la comunicación o que se hagan las coordinaciones pertinentes con los desarrolladores de los sistemas externos con el objetivo de acordar un protocolo común y se construyan estas interfaces.			
Estado	Analizado			

Anexo 7: Plantilla plan de Mitigación.

Proyecto para la Humanización Penitenciaria

Sistema de Gestión Penitenciaria

PLAN DE MITIGACIÓN DE RIESGOS

VERSION <X.X>

Revisión Histórica

Fecha	Versión	Descripción	Autor
<dd/mmm/yy>	<x.x>	<detalles>	<nombre>

Reglas de Seguridad

El que recibe el documento asume la custodia y control, comprometiéndose a no reproducir, divulgar, difundir o de cualquier manera hacer de conocimientos público su contenido, excepto para cumplir el propósito para el cual se ha generado.

Estas reglas son aplicables a las __ páginas de este documento.

Tabla de Contenido

1. Introducción

[Información necesaria para entender el documento]

1.1 Alcance

[Proyecto SIGEP y proyectos facultad 4]

1.2 Referencias

[Lista de documentos a los que se hace referencia en el Plan]

1.3 Glosario

[En caso de usarse en la plantilla términos básicos de difícil comprensión o siglas no evidentes]

2. Riesgos

[Poner los riesgos a los cuales se les va a hacer el plan de Mitigación.]

ID	Riesgos	Descripción	Probabilidad	Impacto	Efecto

2.1 Gestión de Riesgo

ID	Riesgo	Probabilidad	Impacto	Mitigación del riesgo	Monitoreo del riesgo	Administración del riesgo

Atributos:

Mitigación

¿Cómo se puede evitar el riesgo?

Monitoreo

¿Qué factores podemos vigilar que nos permitan ser capaces de determinar si el riesgo es más o menos probable?

Administración

¿Con qué planes de contingencia contamos si el riesgo se vuelve realidad?

Anexo 7A. Plan de Mitigación.

ID	Riesgo	Probabilidad	Impacto	Mitigación del riesgo	Monitoreo del riesgo	Administración del riesgo
36	Superficial captura de requisitos.	0.7	0.9	Entrevistas con funcionarios de la Dirección General de Custodia y Rehabilitación del Recluso. Realizar visitas a centros penitenciarios, observar el funcionamiento de los mismos y entrevistarse con los principales involucrados en la gestión del penal y futuros usuarios del sistema. Tener una contraparte venezolana que revise el artefacto Visión, el Modelo de Casos de Uso, el prototipo de Interfaz de usuario, de manera que se puedan corregir a tiempo errores e inconsistencias en los requisitos.	Velar que la parte venezolana revise los artefactos.	Reunirse con los analistas y la contraparte venezolana para saber cuales fueron los principales errores e inconsistencias y plantear una solución.
37	Cambio de los requisitos del software.	0.7	0.5	Es un riesgo que no se puede evitar, pero se puede minimizar haciendo un esfuerzo en el diseño, para en el caso de tener que cambiar algo se pueda hacer de la manera más eficiente sin tener que reestructurar todo el proyecto.	Velar el Diseño.	Reunirse con los miembros del proyecto y explicarles la situación bien detallada. Reestructurar las partes afectadas del proyecto.

38	Falta de infraestructura para el despliegue.	0.7	0.7	El diseño deberá considerar un abanico de posibilidades en cuanto a la infraestructura de hardware y el ambiente en que funcionará el software. Deberá tenerse en cuenta este aspecto durante la captura de requisitos.	Velar por las condiciones que deben existir a la hora de instalar la aplicación.	Los interesados tienen que asumir la responsabilidad y tratar de optimar esos detalles lo más rápido que se pueda para implantar el software.

ID	Riesgo	Probabilidad	Impacto	Mitigación del riesgo	Monitoreo del riesgo	Administración del riesgo
39	Mayoría de diseñadores y programadores en 5to año.	0.9	0.7	Los profesores del proyecto están impartiendo preparación a los estudiantes que tienen pendiente la prueba de nivel. Se elaboró una propuesta para modificar el contenido del documento de tesis de modo que se ajuste a un formato más reducido, sin dejar de incluir el problema, los objetivos y la solución propuesta. El conjunto de documentos conformarían una memoria colectiva del proyecto. La propuesta fundamentada fue presentada en la primera quincena de enero a la facultad. Aun no se ha recibido una respuesta oficial de aprobación o rechazo de la misma. Esta variante de tesis ofrecería mayor disponibilidad de tiempo a los desarrolladores más experimentados.	Velar por el rendimiento de estos estudiantes.	Se debe planificar un horario especial para la recuperación de los estudiantes de quinto año del tiempo perdido. Distribuir las tareas entre los estudiantes que se encuentran mas liberados; es decir los que tienen las tesis adelantadas y prueba de nivel aprobada. Utilizar estudiantes de cuarto año en esa labor y poner al de quinto año a asesorarlo.

ID	Riesgo	Probabilidad	Impacto	Mitigación del riesgo	Monitoreo del riesgo	Administración del riesgo
40	Inexperiencia de los nuevos incorporados al proyecto.	0.9	0.7	Fueron distribuidos entre los equipos de desarrollo de modo que trabajen de conjunto con los programadores de experiencia. Se les irán asignado tareas que gradualmente aumentarán su nivel de complejidad.	Velar por la productividad.	Hacer un esfuerzo por parte de cada integrante del grupo de trabajo y dedicar un tiempo de dos horas al día al estudio de las nuevas tecnologías usadas en el proyecto, teniendo un tiempo límite de aprendizaje de la misma; esto sería suficiente para minimizar el problema. Poner un estudiante que tenga los suficientes conocimientos a asesorar a los nuevos incorporados.
42	Posible egreso de la UCI de los programadores y diseñadores más experimentados.	0.7	0.7	Proponer a la dirección de la Facultad 4 y de la UCI, mantener en la universidad una vez graduados, a aquellos miembros del equipo de desarrollo cuyo trabajo sea significativo para el éxito del proyecto.	Velar cuan cerca está ese posible egreso.	Que los estudiantes más experimentados le den preparación a otros de tercer año para así garantizar la continuidad del proyecto.

43	Desarrollar más casos de uso que los acordados.	0.7	0.7	Negociar con la parte venezolana aplazar el desarrollo de los módulos menos significativos para el negocio para una próxima Mixta (Ejemplo: biblioteca, plan de presentaciones).		
46	No satisfactorio nivel de definición de procesos operativos.	0.9	0.9	Se recomienda avanzar en la definición detallada de estos procesos a través, por ejemplo, de reuniones grupales en las que participen los especialistas funcionales de cada área, el componente de recursos humanos que diseñó la transformación, representantes del componente tecnológico, el grupo de asesores cubanos en materias penitenciarias, una especialista en procesos y un experto en temas legales, con el objetivo de readecuar la descripción de los procesos y el flujo de información a partir del resultado del trabajo de esos encuentros. Además, para mitigar este importante riesgo, el desarrollo del software se concibe por etapas, para incluir progresivamente en cada una de ellas, las áreas funcionales y procesos que poseen un mayor nivel de definición, dejando los menos definidos para las etapas finales, de modo que se pueda avanzar en la concepción de estos previos a su automatización.	Velar porque la Dirección General de Custodia y Rehabilitación del Recluso establezca las definiciones necesarias para el funcionamiento operativo de algunas áreas claves dentro de la institución (por ejemplo: Control Penal, Acompañamiento post-penitenciario, Gestión de Riesgos, etc.), Que cada área tenga una adecuada descripción de los procesos.	En las áreas en las que no se cuente con una adecuada descripción de los procesos las actividades a informatizar serán detalladas a partir de la experiencia del equipo de desarrollo en otros sistemas similares. (Y esto puede causar que existan actividades sin automatizar y otras a un nivel elemental).

ID	Riesgo	Probabilidad	Impacto	Mitigación del riesgo	Monitoreo del riesgo	Administración del riesgo
47	Mal estado de la infraestructura física.	0.9	0.9	Se hace necesario realizar un recorrido por cada una de las entidades del sistema penitenciario donde será instalado el SIGEP, con el objetivo de diagnosticar las condiciones de infraestructura existentes y establecer las adecuaciones necesarias tanto de la obra civil, como las que garanticen seguridad, clima y suministro de energía eléctrica demandadas por la tecnología a instalarse. El recorrido requiere del apoyo de la Dirección General de Custodia y Rehabilitación del Recluso, con su participación directa en las actividades del diagnóstico de condiciones físicas, a modo de garantizar las coordinaciones necesarias para la realización de la visita, para la selección de los locales de instalación de la tecnología y la posterior ejecución de las adecuaciones en la infraestructura.	Velar porque después que se haga el recorrido por cada establecimiento existan los locales apropiados con las condiciones mínimas requeridas para la instalación de la tecnología (servidor de datos y aplicaciones, equipos telemáticos).	Los interesados tienen que asumir la responsabilidad y tratar de optimar esos detalles lo más rápido que se pueda para implantar el software. Instalar el software solo en los establecimientos que esté creada la infraestructura.

ID	Riesgo	Probabilidad	Impacto	Mitigación del riesgo	Monitoreo del riesgo	Administración del riesgo
48	Ausencia de personal técnico para administrar el sistema.	0.9	0.7	Seleccionar el personal requerido para esta tarea y una vez que estén definidos empezar con la capacitación de ellos para que reciban la preparación necesaria para garantizar el uso y explotación del sistema en cada uno de los establecimientos penitenciarios.	Velar porque el personal seleccionado reciba la capacitación necesaria para garantizar la explotación del sistema.	Poner el software solo en los establecimientos donde este el personal técnico adecuado. Y los interesados tienen que asumir la responsabilidad de buscar el personal que falta para garantizar el uso y explotación del sistema en cada uno de los establecimientos penitenciarios.

49	Uso inadecuado de las aplicaciones informáticas.	0.7	0.7	Se recomienda la incorporación de personal confiable para el manejo del sistema informático y garantizar el respeto por las políticas de acceso que propone el sistema. Se recomienda también la formulación de un reglamento que contenga todas disposiciones necesarias para lograr uniformidad y disciplina en el uso del sistema. Contemplar la automatización en el sistema de validaciones de uso y coherencia, que activen notificaciones a los niveles táctico y estratégico.	Velar para que la información que entre al sistema informático sea veraz, aprobada por el nivel correspondiente, auditada e introducida por las personas autorizadas.	Analizar y tomar medidas con la persona que tuvo un uso inadecuado de la tecnología. Se le hará ver su error y si no fue muy grave se le da otra oportunidad y si reincidiera se ve la posibilidad de la expulsión del establecimiento.
50	Inseguridad en el interior de los establecimientos penitenciarios.	0.9	0.9	Se recomienda aprovechar las adecuaciones de la infraestructura física para contar con un espacio de resguardo de los equipos en caso que se presente una situación que amenace su integridad. Se recomienda además proteger los equipos a través de la adquisición de un seguro que cubra robo, vandalismo, desastres, etc., pues esto no se contempla dentro del alcance del presente proyecto.	El clima de violencia y de inseguridad que existente en los establecimientos. Ocurrencia de cualquier contingencia en los establecimientos penitenciarios.	En caso de ocurrir cualquier vandalismo, robo o desastre debe emitirse hacia el seguro. La persona encargada del establecimiento es la responsable del hecho divido que no tomo las medidas a tiempo.

ID	Riesgo	Probabilidad	Impacto	Mitigación del riesgo	Monitoreo del riesgo	Administración del riesgo
51	Mantenimiento de la tecnología instalada.	0.7	0.9	Si bien dentro del alcance de la solución de software está previsto el soporte técnico por período de un año, a partir del momento de la instalación en cada establecimiento, la Dirección General deberá garantizar un equipo técnico, que debidamente entrenado, pueda atender el mantenimiento y la actualización, tanto de las aplicaciones informáticas, como del equipamiento instalado. Este equipo técnico debe estar conformado por ingenieros especializados en las áreas de la informática y la telemática, y familiarizados además con la tecnología de software y hardware usadas en la solución.	Velar porque se cumplan las políticas de mantenimientos.	La empresa es la encargada de solucionar el problema. En caso de que no tenga el personal adecuado para este mantenimiento deberá pagarle a una persona externa que tenga los conocimientos necesarios.

52	Fallo en la conectividad.	0.7	0.7	Para minimizar este riesgo, el sistema funcionará de manera autónoma con una base de datos local en cada establecimiento penitenciario y sólo utilizaría el canal de comunicación con el exterior para las actividades de réplica de la base de datos y consulta de datos globales. De igual modo la comunicación se debe establecer por un canal seguro.	Velar por una conexión disponible y de calidad.	En caso de algún fallo de conectividad se debe informar al responsable de soporte técnico. Esperar que este avise que está lista la conectividad para usarse otra vez.
53	Los sistemas externos no ofrecen las interfaces necesarias para establecer la comunicación con estos.	0.7	0.7	Para que esto se lleve a cabo con éxito, es necesario que estén desarrollados los servicios para la comunicación o que se hagan las coordinaciones pertinentes con los desarrolladores de los sistemas externos con el objetivo de acordar un protocolo común y se construyan estas interfaces. En ningún caso, el desarrollo del SIGEP concibe crear las interfaces de terceros sistemas, sino usar las interfaces ya existentes o acordadas con estos sistemas y proveer las necesarias.	Velar para que los sistemas externos provean las interfaces para estos fines.	En caso de que un sistema externo no ofrezca las interfaces necesarias los interesados deben asumir la responsabilidad ante este hecho. Analizar por que no estaba hecha la interfaz y tomar las medidas pertinentes con el responsable del hecho.

Anexo 8. Métrica: Exposición al Riesgo (Relación Impacto - Probabilidad De Riesgo).

Objetivo: Estimar el nivel de exposición que tiene un proyecto frente a los riesgos, es decir, estimar cuán riesgoso puede ser mi proyecto.

Valor de la métrica: un valor numérico que indique el nivel de exposición frente al riesgo del proyecto.

Interrogante que resuelve: ¿Cuán expuestos estamos a sufrir pérdidas significativas si nuestros riesgos se convierten en problemas?

Datos de entrada: Matriz de Exposición al riesgo o de probabilidad e impacto.

Esta es la matriz que expresa la exposición del riesgo, se obtiene multiplicando la escala de impacto por la escala de probabilidad asociada a un riesgo y luego se clasifica en crítico, grave y asumible. Mientras más cercano a 1 este más crítico será.

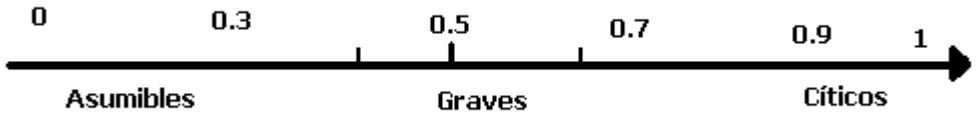

Ilustración 16 Relación impacto-probabilidad

Escala de Probabilidad	**Amenazas**				
				CRÍTICOS	
		GRAVE			
	ASUMIBLE				
Escala de Impacto					

Tabla 5 Exposición al riesgo

Cálculo:

Para realizar el cálculo es necesario definir una escala asociado a la exposición del riesgo obtenida de la matriz, a continuación se muestra la escala.

CRRIP	**ESCALA**
CRÍTICO	1
GRAVE	2

ASUMIBLE	3

Tabla 6 Escala de exposición

CRRIP: Clasificación de riesgo según relación Impacto-Probabilidad.

NPR: Nivel del proyecto según sus riesgos.

EER: Escala de exposición del Riesgo según CRRIP.

NTR: Número Total de Riesgos.

CATASTRÓFICO

$Si \quad \sum EER = NTR$ El proyecto tiene un nivel **CATASTRÓFICO**

CRÍTICO

$Si \quad NTR < \sum EER \leq 2NTR$ El proyecto tiene un nivel **CRÍTICO**

DESPRECIABLE

$Si \quad 2NTR < \sum EER \leq 3NTR$ El proyecto tiene un nivel **DESPRECIABLE**

El nivel de riesgo de un proyecto expresa cuan expuesto está el proyecto al impacto del riesgo según su probabilidad de ocurrencia. Esto nos ayuda a determinar la viabilidad del proyecto, las posibles afectaciones al presupuesto, tiempo planificado, etc. Este nivel se clasificará en:

1. Catastrófico: Implica que el 100% de los riesgos analizados son críticos según la Matriz de exposición al riesgo, lo cual deja claro que el proyecto puede no ser viable.
2. Crítico: Implica que más del 50% de los riegos analizados son críticos o graves según la Matriz de exposición al riesgo, por lo que el proyecto puede tener grandes afectaciones durante su desarrollo.
3. Despreciable: Implica que más del 50% de los riesgos analizados son asumibles según la Matriz de exposición al riesgo y que el proyecto no sufrirá perdidas significativas.

ACRÓNIMOS

CMM: Capability Maturity Model, Modelo de Capacidad y Madurez.

CMMI: Modelo de Madurez de Capacidades Integrado.

DriveSPI: Risk-Driven Software Process Improvement, Mejora del Proceso de Software basado en Directivas de Riesgo.

DESOFT: Empresa cubana de DEsarrollo de SOFTware.

IEC: International Electrotechnical Commission, Comisión Internacional de Electrónica.

IEEE: Institute of Electrical and Electronics Engineers, Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización.

ISO: International Standards Organization, Organización Internacional de Estándares.

ISPL: Information Services Procurement Library, Librería de Adquisición de Sistemas de Información.

MAGERIT: Metodología de Análisis y Gestión de Riesgos de los sistemas de Información[8] de las Administraciones Públicas.

MAP: Ministerio de Administraciones Públicas, España.

PDSW: Proyecto de Desarrollo de Software.

PGP: Plan de Gestión del Proyecto.

PGR: Plan de Gestión de Riesgos.

PMBoK: Project Management Body of Knowledge, Cuerpo Del Conocimiento de Gestión de Proyectos[9].

PMI: Project Management Institute, Instituto de Gestión de Proyectos.

PSP: Personal Software Process, Proceso de Software Personal.

RUP: Rational Unified Process, Proceso Unificado de Desarrollo.

SEI: Software Engineering Institute, Instituto de Ingeniería de Software[10].

UCI: Universidad de las Ciencias Informáticas.

SIGEP: Sistema de Gestión Penitenciaria.

UTASP: Unidades técnicas de desarrollo al sistema penitenciario.

GLOSARIO

[1]**Impacto:** Alcance de lo que sucedería si el riesgo se materializara (la dimensión efecto). Pérdida que ocasiona el riesgo.

[2] **Herramientas:** Utensilios o provisiones necesarias para poder emprender un proyecto de software. Soportan los procesos de desarrollo de software modernos.

[3] **Calidad:** Conjunto de propiedades y características de un producto o servicio que le confieren su aptitud para satisfacer unas necesidades explícitas o implícitas.

[4] **Activos:** Recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.

[5] **Dominio:** Unidades en las que se centra la GR.

[6] **Submodelo de Procesos:** Descripción funcional (esquema explicativo) de la GR.

[7] **Tarea:** Concepto utilizado en el submodelo de procesos, que conlleva las acciones a realizar, los productos y documentos a obtener, y las técnicas utilizables en su realización.

[8] **Información:** Conocimientos sobre objetos, como por ejemplo hechos, *eventos*, cosas, *procesos* o ideas, inclusive conceptos, que dentro de un contexto determinado poseen un significado concreto. Mensajes que se utilizan para representar un hecho o un concepto dentro de un proceso de comunicación a fin de incrementar los conocimientos.

[9] **Gestión de proyecto:** La Gestión de Proyectos tiene como finalidad principal la planificación, el seguimiento y control de las actividades y de los recursos humanos y materiales que intervienen en el desarrollo de un Sistema de Información o en la vida de un proyecto.

[10] **Ingeniería de Software:** Tratamiento sistemático de todas las fases del ciclo de vida del software.