
# UNIVERSIDAD CATÓLICA DEL NORTE

**FACULTAD DE CIENCIAS DE INGENIERÍA Y CONSTRUCCIÓN**

**Departamento de Gestión de la Construcción**

## METODOLOGÍA DE ADMINISTRACIÓN DE RIESGOS EN PROYECTOS TIC - MINEROS

Tesis para optar al grado de Magíster en Gestión Integral de Proyectos

**JUAN FRANCISCO ZALDÍVAR ARIAS**

Profesor Tutor: Boris Heredia Rojas, Magíster en Ciencias de la Ingeniería.

**Antofagasta, Chile**

**2012**

## AGRADECIMIENTOS

Mis mas sinceros agradecimientos en primera instancia a Jorge y Patricio quienes me incentivaron a dar termino a un camino que estaba postergado. También quiero agradecer a Paulina y John, quienes ayudaron con el desarrollo de este trabajo.

No hubiese sido posible comenzar, ni terminar este trabajo sin el apoyo de “La Bruja” Florencia y mi hija Kony; quienes siempre me ayudaron para asistir a clases y poder estudiar. Sin este apoyo este trabajo nunca hubiese sido terminado.

Se retribuye a profesores guías por su constancia e interés.

## INDICE GENERAL

# INDICE DE TABLAS

# INDICE DE FIGURAS

## GLOSARIO

**Acción potencial de mejora:** Recomendaciones para reducir riesgos.

**Activos:** Bienes que posee una organización o negocio. Estos pueden ser de naturaleza tangible o intangible.

**Alcance del riesgo:** Descripción cualitativa de los sucesos, su tamaño, tipo, número y dependencias.

**Amenaza:** Un evento con el potencial para causar acceso no autorizado, modificación, revelación o destrucción de un activo organizacional. En caso de un área informática, se puede interpretar al activo como información, aplicaciones, sistemas o recursos informáticos.

**Análisis "FODA":** Análisis de fortalezas, oportunidades, debilidades y amenazas (FODA). Técnica que analiza la exactitud de las asunciones e identifica los riesgos del proyecto causados por el carácter impreciso, incoherente o incompleto de las asunciones.

**Análisis de causa raíz:** Una técnica analítica utilizada para determinar el motivo subyacente básico que causa una variación, un defecto o un riesgo. Más de una variación, defecto o riesgo pueden deberse a una causa.

**Análisis de riesgos:** El proceso de identificar activos y amenazas, priorizando la vulnerabilidad de la amenaza e identificar apropiadamente los controles respectivos.

**Análisis de sensibilidad:** Una técnica de análisis cuantitativo de riesgos y de modelado utilizada para ayudar a determinar qué riesgos tienen el mayor impacto posible sobre el proyecto. Este método evalúa el grado en que la incertidumbre de cada elemento del proyecto afecta al objetivo que está siendo examinado cuando todos los demás elementos inciertos son mantenidos en sus valores de referencia. La representación habitual de los resultados es un diagrama con forma de tornado.

**Análisis de valor monetario esperado:** Una técnica estadística que calcula el resultado promedio cuando el futuro incluye escenarios que pueden ocurrir o

no. Esta técnica se usa comúnmente dentro del análisis del árbol de decisiones. Se recomienda el uso de modelos y la simulación para el análisis de costes y riesgos del cronograma, porque es más efectivo y está menos sujeto a errores de aplicación que el análisis del valor monetario esperado.

**Análisis de árbol de decisiones:** El árbol de decisiones es un diagrama que describe una decisión que se está considerando y las consecuencias de seleccionar una u otra de las alternativas disponibles. Se usa cuando algunos escenarios futuros o resultados de acciones son inciertos. Incorpora las probabilidades y los costes o recompensas de cada camino lógico de eventos y decisiones futuras, y usa el análisis del valor monetario esperado para ayudar a la organización a identificar los valores relativos de las acciones alternativas. Véase también análisis del valor monetario esperado.

**"Checklist":** Término en inglés que respecta a una lista de quehaceres, los cuales se van descartando a medida que se realizan.

**Control:** Medidas protectoras implementadas para asegurar que los activos se encuentran dispuestos a alcanzar los requerimientos del negocio.

**Control de riesgos:** Una política, procedimiento, recurso, sistema o acción que actúa para limitar la inseguridad en el logro de la planificación de la unidad de negocios y objetivos estratégicosy/o para asegurar el cumplimiento con la ley.

**Cuantificación del riesgo:** Importancia y probabilidad.

***"Customizar"*:** Modificar una herramienta u objeto para adaptarlo a las preferencias de su usuario o propietario

**Identificación de riesgos:** El proceso de determinar qué riesgos podrían afectar el proyecto y documentar sus características.

**Interesados:** Referirse a "StakeHolders".

**Lluvia de ideas:** Herramienta de trabajo en grupo, en que todos los miembros aportan sus ideas, pero nadie tiene derecho a rebatirlas. Todas las ideas son bienvenidas.

**Metodología:** Un sistema de prácticas, técnicas, procedimientos y normas utilizado por quienes trabajan en una disciplina.

**"Mind Maps":** Mapas mentales, utilizados para mantener ideas relacionadas, similar a lluvia de ideas.

**Mitigación:** Acciones para contener

**Naturaleza del riesgo:** Ej. Estratégicos, operacionales, financieros, de gestión del conocimiento y de conformidad.

**PMI:** Referirse a "Project Management Iniciative".

**Política y estrategia a desarrollar:** Identificación del responsable de la función de desarrollo de la política y la estrategia.

**"Project Management Iniciative":** Iniciativa sobre la administración de proyectos. El Instituto de Administración de Proyectos provee guías y pautas para llevar a cabo proyectos de manera efectiva y eficiente.

**"Prompt List":** Lista de sistema utilizada para listar ideas o enunciados similares a una lluvia de ideas.

**RCA:** Referirse a Análisis de Causa Raíz.

**Registro de riesgos:** El documento que contiene los resultados del análisis cualitativo de riesgos, análisis cuantitativo de riesgos y planificación de la respuesta a los riesgos. El registro de riesgos detalla todos los riesgos identificados, incluso la descripción, categoría, causa, probabilidad de ocurrencia, impactos en los objetivos, respuestas propuestas, responsables y condición actual. El registro de riesgos es un componente del plan de gestión del proyecto.

**Riesgo:** La probabilidad en que una amenaza en particular explote una vulnerabilidad en especifica.

**Riesgo residual:** Riesgo que permanece después de haber implementado las respuestas a los riesgos.

**Riesgo secundario:** Un riesgo que surge como resultado directo de la implantación de una respuesta a los riesgos.

**"Root Cause Analysis":** Referirse a Análisis de Causa Raíz.

**"StakeHolders":** Personas y organizaciones como clientes, patrocinadores, organización ejecutante y el público, involucrados activamente con el proyecto, o cuyos intereses pueden verse afectados de manera positiva o negativa por la ejecución o conclusión del proyecto. También pueden influir sobre el proyecto y sus productos entregables. También conocido como: Interesados o Involucrados.

**"Step Back":** Paso atrás, tomar un momento para reflexionar.

**Tratamiento del riesgo y mecanismos de control:** Medios primarios por los que se gestiona el riesgo actualmente. Niveles de confianza en el control existente. Identificación de protocolos de supervisión y revisión.

**Técnica Delphi:** La técnica Delphi es una forma de llegar a un consenso de expertos en forma anónima.

**Tecnologías de la información:** Tecnología dedicada a satisfacer las necesidades de información estratégica, mediante aplicaciones y herramientas computacionales, aplicables a una organización

**Tecnologías de la información y comunicación:** Concierne a las Tecnologías de la Información, y la manera en que se comunica a los interesados, mediante canales tecnológicos.

**TI:** Referirse a Tecnologías de la Información.

**TIC:** Referirse a Tecnologías de la Información y Comunicación.

**Tolerancia del riesgo** / **apetito:** Potencial de pérdida e impacto financiero del riesgo. Valor en riesgo. Probabilidad y tamaño de las pérdidas/ganancias potenciales. Objetivos del control de riesgo y nivel deseado de rendimiento.

**Valoración de riesgos:** el proceso general de análisis y de evaluación de riesgos

**Vulnerabilidad**: Una debilidad en un sistema, aplicación, infraestructura, control o diseño defectuoso que puede ser explotado para violar la integridad de algún sistema TI.

**WBS:** Referirse a "Work Breakdown Structure".

**"Work Breakdown Structure":** Estructura de desglose de Trabajo. Método que se utiliza para organizar el trabajo a realizar en modo de paquetes y tareas, hasta llegar al nivel más bajo de actividades.

# RESUMEN

Este documento describe el trabajo realizado tanto, en Investigación, modelado de propuestas, y en aplicación de conocimiento, teoría y práctica que el alumno autor tiene sobre el tema del presente documento de memoria, que es la Metodología de Administración de Riesgos en Proyectos TIC – Mineros.

La problemática que abarca el presente documento es la incertidumbre a la que están sujetas las administraciones de proyectos, especialmente aquellos sobre las Tecnologías de la Información en la industria minera. Esto es debido a que los riesgos pueden representar pérdidas millonarios en proyectos de gran envergadura, o la cancelación del proyecto en sí. Hoy el mercado de riesgo está desarrollando nuevos alcances para la administración y gobierno, es por eso que se ha desarrollado una investigación sobre las metodologías existentes para la administración de riesgos en un marco de proyectos.

Para abordar esta problemática se realizó una investigación profunda de documentación actual y de prestigio – registrada en los primeros dos capítulos de este texto. La cual se transformó en la creación de una metodología que permite analizar los riesgos de proyectos informáticos – mineros obteniendo como resultado un proceso costo-eficiente que se encuentra con los objetivos y resultados básicos de toda administración de proyecto. Esta metodología se detalla en el capítulo tres para seguir con un caso de estudio en el capítulo posterior.

Por último, se entregan las conclusiones del trabajo realizado, en donde se mira en retrospectiva la investigación realizada, el método realizado y el caso de estudio abarcado para informar sobre los aportes contribuidos a la formación profesional del alumno.

# CAPÍTULO I

# Introducción

## 1.1 Descripción

Todo negocio se encuentra sujeto a un ambiente dinámico e inestable, en donde surgen incertidumbres que se necesitan mitigar. El problema radica en que existen distintos factores de riesgos, todos ellos con demasiados escenarios posibles, lo que ha impedido la automatización en su reducción o administración.

*La Administración del riesgo es la aplicación sistemática de políticas de administración, procedimientos y prácticas dirigidas a las actividades de analizar, evaluar, controlar, mitigar y comunicar los conflictos de riesgo.*[1]

Es cierto que existen riesgos genéricos, de modo que se conocen las estrategias para abordarlos. Por ejemplo, el riesgo de la competencia, de los proveedores, los compradores, las condiciones cambiantes, los productos sustitutos y la rivalidad en el ranking de posiciones de la industria.2 Pero el presente proyecto de tesis se ha enfocado en los riesgos desde el punto de vista informático, específicamente en los riesgos inherentes de área de proyectos mineros.

En el contexto con la administración de proyectos mineros, cada vez se hace más necesario el uso de herramientas que apoyen el control de los riesgos informáticos. Es por ello que se pretende identificar los factores de incertidumbre y clasificarlos a través de una metodología clara y entendible, y así obtener las acciones a seguir en el proceso de evaluación, buscando la mitigación del impacto de los riesgos como resultado del modelo análisis de riesgos propuesto.

[1] Saner, M. (2005). *Information Brief On International Risk Management Standards.*

[2] Porter, Michael E. (2008). *The Five Competitive Forces That Shape Strategy*; Hardvard Business Review.

## 1.2 Justificación

Este proyecto de tesis nace por la necesidad de consolidar una metodología que abarque las mejores prácticas utilizadas para la administración de riesgos en los proyectos informáticos mineros.

Las metodologías planteadas por PMI, CISSP, ISO27002 y COBIT a las que generalmente se recurren, por lo general no especifican una metodología y si lo hacen, ésta se basa en información de estadísticas de éxitos y fracasos de proyectos, que en una búsqueda a fuentes formales de información en Chile, como ACTI y ENTI, no se lograron encontrar datos estadísticos que permitan conocer cuáles son los riesgos de los proyectos TI-Mineros, y que además proporcionen la información necesaria para la utilización de los modelos cuantitativos planteados por las normas internacionales

Un ejemplo es CISSP define una metodología de evaluación de riesgos basada en la probabilidad de ocurrencia, expresada en una variable llamada ARO (annualized rate of occurrence), y que define la cantidad de veces que se espera experimentar un desastre cada año, además define un factor de exposición (Exposure factor) para cada activo, que expresa la cantidad de daño que un riesgo afecta a un activo expresada en un porcentaje. Por lo tanto luego de obtener el factor de exposición de un activo y multiplicándolo por el valor del activo, se puede obtener una expectativa de pérdida monetaria expresada en la variable SLE (Single Loss Expectancy). (Michael Stewart, 2011)

Por otra parte la Academia Mundial de Ciencia de la Ingeniería y Tecnología, WASET por sus siglas en ingles, plantea un modelo de evaluación de riesgos basado en un confuso proceso de análisis jerárquico, que define una matriz de probabilidad de ocurrencia, obtenida mediante estructuras jerárquicas de riesgos y extensos cálculos matemáticos de comparaciones por pares. (Iranmanesh, Nazari Shirkouhi, & Skandari, 2008)

Con estos datos se logra evidenciar que estos cálculos son basados en historia corporativa, definiendo expectativas basadas en proyectos pasados y que debido a que no se cuentan con tales datos, así como también a las diferencias en el ambiente organizativo, aspectos legales, diferencia en las condiciones medioambientales propias de cada país, etc. El uso de estadísticas internacionales puede llevar a una mala percepción de los riegos y su posible impacto.

Pero, por otra parte y como pieza fundamental de la justificación de este proyecto de tesis, se debe tener en cuenta la importancia que durante mucho tiempo se le ha estado dando al proceso de análisis de riesgos en los proyectos, ya sean TI o de cualquier índole, referente al éxito de los mismos y como la evaluación de riesgo contribuye a esto.

Bakker, Boonstra, Wortmann (2010), plantean cómo se puede aprender de los factores de riesgos emergentes luego de realizar una evaluación de riesgos, y que éstos sirvan de ayuda para análisis futuros en los nuevos proyectos (ver Figura 1.1).

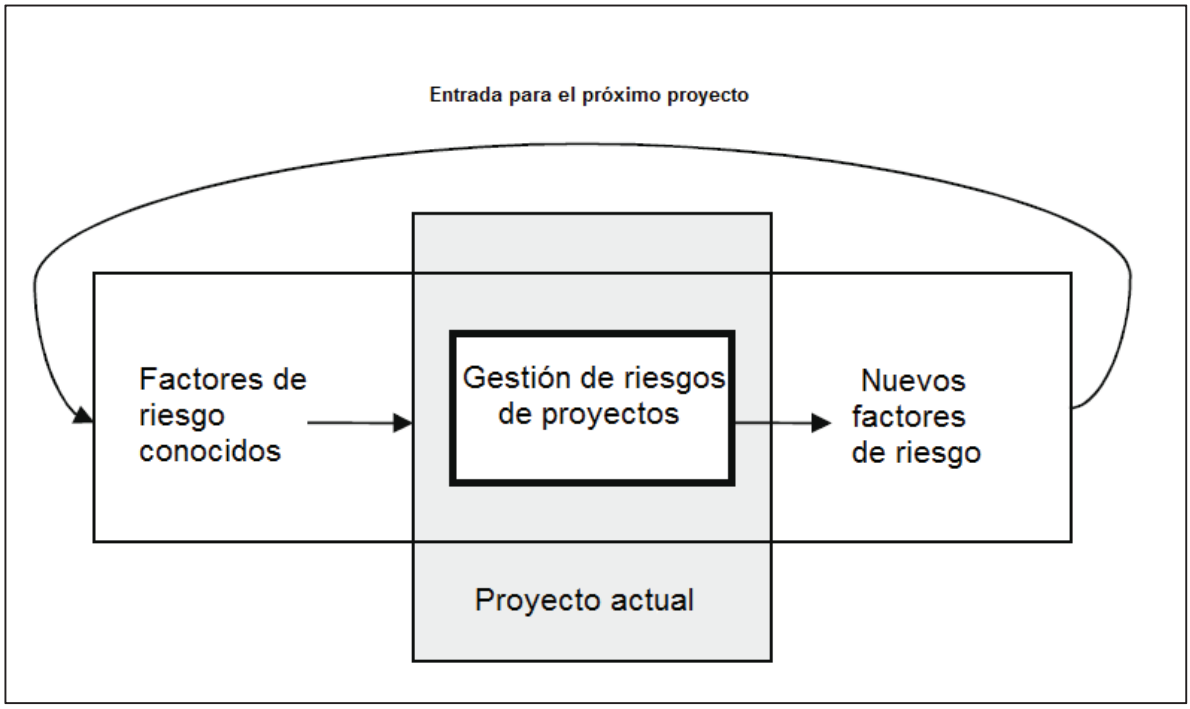


**Figura 1. 1:** Enfoque de evaluación de riesgos (Bakker et al., 2010)

Entonces, ya que para llegar a un modelo cuantitativo principalmente se tiene una problemática de datos, es mucho más sencillo partir por un modelo cualitativo que sirva para crear historia corporativa, estadísticas, es decir, información que pueda servir para estimaciones en proyectos futuros, para así poder llegar a un modelo cuantitativo de evaluación de riesgos TI-Mineros.
Por otra parte, como se ve en la figura 1.2, la inversión de presupuesto en TI en la industria minera, alcanza un 0,6 % de su facturación. Este porcentaje es el menor en comparación con otros rubros, pero se debe considerar que, en la

industria minera chilena la facturación alcanza un valor de 18 millones de dólares por día, con un mínimo de 6 millones de dólares.

Por lo tanto la inversión en la industria minera es mayor que en otros rubros, y dado esto se puede considerar que existe una oportunidad para la realización de estudios basados en proyectos TI-Mineros.

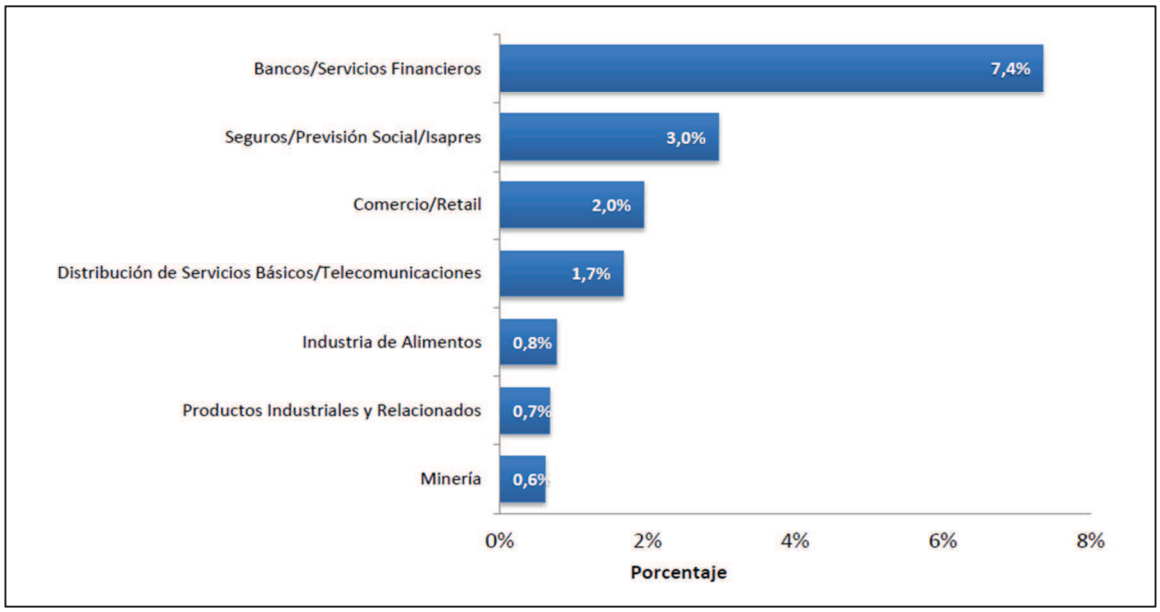


**Figura 1. 2:** Presupuesto de TI como porcentaje de facturación (CETIUC, 2011)

Además, el gasto en TI por parte de las empresas mineras, se puede complementar con el número promedio de usuarios TI que ocupan en sus actividades, y que alcanza la cantidad mayor por sobre otros rubros (ver figura 1.3).

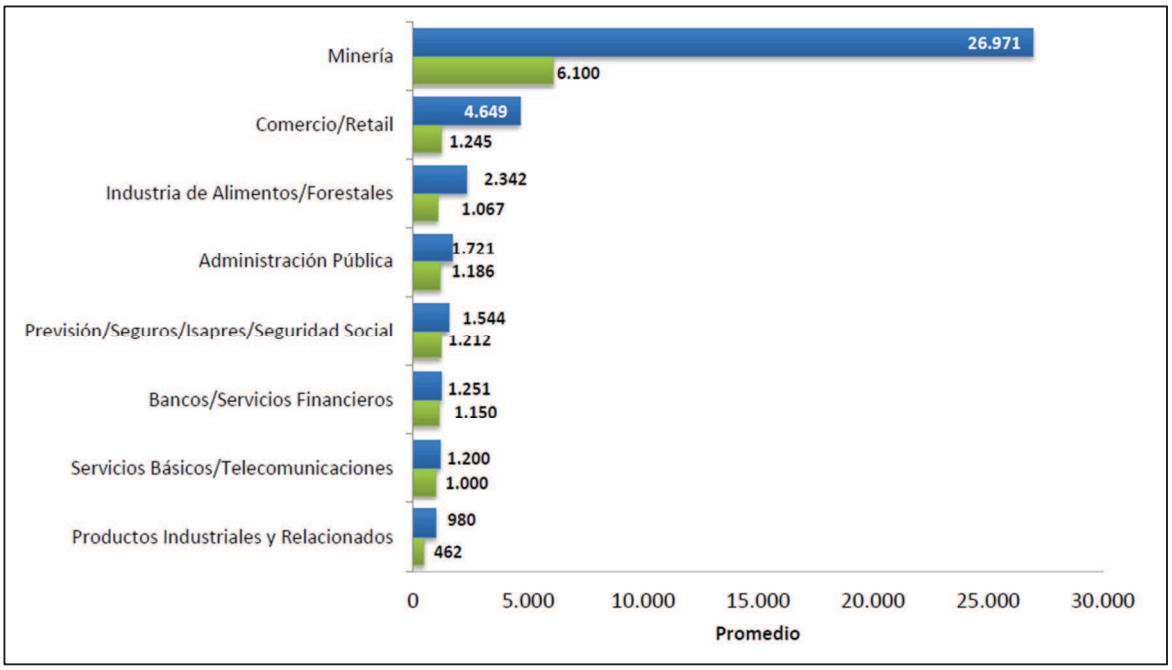


**Figura 1. 3:** Promedio de empleados y usuarios TI (CETIUC, 2011)

Y por último, es conocido el aporte que entregan los modelos estandarizados a las organizaciones, permitiendo alcanzar un nivel de madurez mayor y posicionando la marca de la compañía entre las mejores, si estos procesos están bien definidos, es por esto que la definición de esta metodología proveerá de una base sólida que permita alcanzar un nivel de madurez mayor.

Para aquello, Farah (2011) planteó un modelo de madurez para la gestión de riesgos en las tecnologías de información (ver Tabla I.1) que es aplicable hoy en Chile y que ayudará en la definición del nivel actual de una organización y el nivel que ha alcanzado luego de aplicar esta metodología de evaluación de riesgos TI-Mineros.

| Nivel | Madurez | Atributo |
|---|---|---|
| **1** | Ad hoc | Ad hoc informal. El proceso de gestión de riesgos de TI es desorganizado y en ocasiones incluso caótico. Los sistemas y procesos no están definidos. El éxito de la gestión de riesgos depende del esfuerzo individual. Existen problemas de programación y costos. |
| **2** | Abreviado | Se han establecido algunos procesos y sistemas de gestión de riesgos TI para realizar un seguimiento de los costos, cronograma y desempeño. Las disciplinas subyacentes, sin embargo, no se conocen bien o no son seguidas consistentemente. El éxito de la gestión de riesgos TI es muy impredecible y existen problemas de costo, horario, y rendimiento. |
| **3** | Organizado | Los sistemas y procesos de gestión de riesgos TI están documentados, estandarizados e integrados en un proceso de extremo a extremo para la empresa. El éxito de la gestión de riesgos TI es más predecible. |
| **4** | Gestionado | Las medidas detalladas de la eficacia de la gestión de riesgos TI es recopilada es utilizada por la administración. El proceso se entiende y se controlada. El éxito de la gestión de riesgos TI es más uniforme. El costo y la programación se ajustan a lo previsto. |
| **5** | Adaptativo | La mejora continua del proceso de gestión de riesgos de TI está habilitada por la retroalimentación del proceso y experimentar ideas y tecnologías innovadoras. El costo y la programación están mejorando continuamente. |

**Tabla I. 1:** Modelo de madurez para la gestión de riesgos en tecnologías de información (Farah, 2011)

Por lo tanto, basado en la oportunidad que se tiene, tanto en la ausencia de un modelo de este tipo, como en la significativa relevancia que tiene un método de evaluación de riesgos en la industria minera, con este proyecto de tesis se pretende generar un modelo que:

1. Tomando como base los estándares internacionales permita atender el proceso de evaluación de riesgos en una base cualitativa para así poder recopilar información de éxitos y fracasos de proyectos que permitan en una futura investigación llegar a un modelo cuantitativo de evaluación de riegos, y

2. Referente a la nueva metodología de evaluación de riesgos, dado que el tiempo que demora cubrir un ciclo de análisis de riesgos crea un desfase crucial para la mitigación y contención necesaria, se pretende saciar esta brecha disminuyendo el tiempo de análisis y automatizándolo acorde a los factores que inciden en el riesgo venidero.

## 1.3 Objetivos

Se pretende llevar a cabo una investigación que proporcione el planteamiento de una metodología sistemática concerniente a IT Projects Risk Management (ITPRM) for Mining, en donde se abarquen las etapas necesarias para concretar acciones en la mitigación de riesgos informáticos presentes en la mayoría de los proyectos mineros chilenos, a través de mecanismos cualitativos para evaluar el nivel de tolerancia de los riesgos, severidades e impactos. Este proceso formal que se implementará tiene como fin priorizar los riesgos y las respectivas contramedidas.

Todo lo anterior basado en fundamentos sobre la administración de riesgos, las mejores prácticas en la administración de proyectos, y una customización de las metodologías mineras en la evaluación de riesgos.

Para cumplir la presente meta global, se deben facilitar los siguientes objetivos específicos:

## 1.4 Objetivos específicos

**1.4.1** Estudio teórico que proporcione iniciativas fundamentadas en la administración de riesgos, con el fin de conseguir posibles parámetros cualitativos para establecer niveles de severidad, impacto y riesgo residual, para la problemática planteada previamente. Es decir, un marco de referencia acerca de los principios de la administración de riesgos sujetos a plataformas proyectos informáticos-mineros.

**1.4.2** Plantear una metodología sistemática aplicable a organizaciones que contemplen proyectos informáticos en una industria minera con necesidad de innovar en las herramientas de administración de riesgos. Ésta se describirá mediante etapas evolutivas del estado de avance del riesgo en el proyecto, otorgando entregables y actividades que se

complementen con las mejores prácticas en la administración de riesgos, y en la administración integral de proyectos.

**1.4.3** Llevar a la práctica el sistema desarrollado sobre un caso de estudio, en donde se entregará un alineamiento para diferenciar amenazas, vulnerabilidades y causas que afectan un proyecto TIC en la industria minera. Se demostrará un escenario en donde se estudiarán los riesgos y se procesarán mediante el método presentado, en donde los entregables de esta etapa comprometa priorizar, evaluar y otorgar actividades de mitigación en pos de una mejora en el control de riesgos.

## 1.5 Resultados esperados

Al finalizar este trabajo de memoria, se espera la creación de una metodología basada en estándares internacionales para la administración del riesgo y adaptada a las necesidades de la industria en los proyectos TI-mineros, que aporte un sistema que simplifique el análisis de los riesgos y sea aplicable en nuestro país. Así de éste modo llegar con mayor facilidad a un curso de acción sobre los posibles riesgos que se puedan presentar.

A pesar de ser de naturaleza teórica, el modelo contribuye al dominio de la gestión de riesgos aplicado específicamente a la administración de riesgos TI-Mineros, abriendo la posibilidad de realizar más investigaciones para su futura verificación. Es por ello que se pretende publicar para:

- Próximos estudiantes de la materia que utilicen el modelo para mejorarlo.
- Profesionales lo utilicen para perfeccionar su ámbito laboral.
- Organizaciones lo utilicen para optimizar sus prácticas en la administración del riesgo en proyectos TI-mineros.

Por otra parte cómo estudiante de Magíster en Gestión Integral de Proyectos, se busca la aplicación de la administración del riesgo sujeto a lo aprendido, y así poder emplear y mostrar la utilidad de los estudios en combinación con otras mejores prácticas certificadas.

## 1.6 Estructura de la tesis

Para el logro de los objetivos se ha desarrollado una investigación que conecta las distintas aristas de la administración del riesgo, en donde el método de cómo se enfrentara este trabajo de tesis se puede resumir en la figura 1.4 mostrada a continuación:


**Figura 1. 4:** Metodología aplicada de memoria (Elaboración propia)

Como se puede observar, las tres etapas principales están directamente relacionadas a los tres objetivos específicos del proyecto de tesis, los cuales se desarrollarán secuencialmente.

Para un mejor entendimiento de la estructura del proyecto de tesis, la figura 1.5 refleja el proceso de investigación y propuesta.

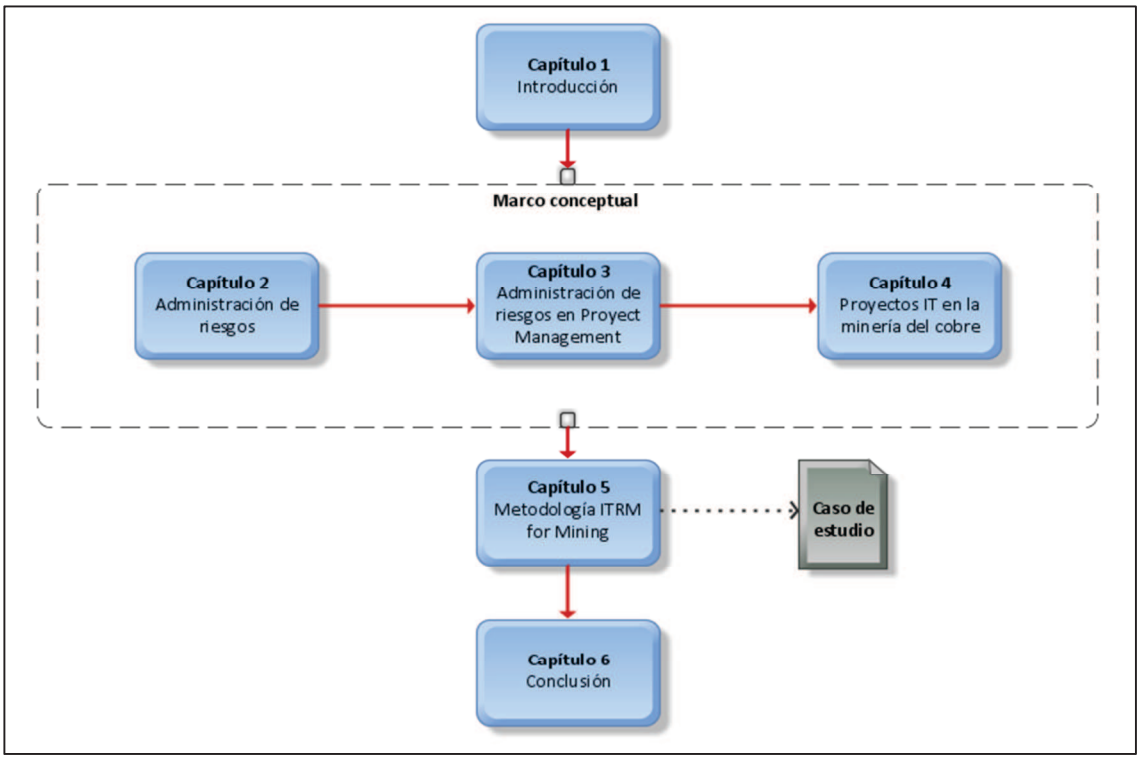


**Figura 1. 5**: Estructura de la tesis (Elaboración propia).

En un inicio se realizará la investigación que abarcará la base teórica a partir de un estudio exhausto de literatura, que se encuentra elaborada por entidades y autores de renombre mundial, esta investigación se basa en la administración de riesgos empleada por las organizaciones para tratar los riesgos relacionados con sus actividades, y que tiene como finalidad ser una herramienta para el continuo cumplimiento de sus objetivos.

Luego, se establecerá una metodología que permita priorizar los riesgos asociados a proyectos minero-informáticos y que está basada en estándares internacionales y adaptados a las necesidades del rubro minero. De este modo se puede obtener el nivel de tolerancia y su mitigación asociada desde un modelo cualitativo hacia uno cuantitativo. Finalmente se probará la metodología generada en un caso de estudio con un escenario posible, en donde se espera obtener resultados satisfactorios.

Cabe destacar que esta memoria está basada en una investigación planificada, por lo que los resultados que se obtendrán se podrán estimar, pero no serán reales. Es por esto, que el escenario que se conseguirá se contrastará con las acciones tomadas realmente en el momento de su ejecución, pues dicho escenario será basado en experiencias profesionales del autor. Lo que se

espera mostrar es que hay acciones que no se consideraron gatillar dada la falta de tiempo de análisis de los riesgos, y que en cambio la metodología sí lo contemplará.

# CAPÍTULO II

## Marco teórico de la administración del riesgo

El marco teórico dotará las bases referenciales para la creación de la metodología de Administración de Riesgos Proyectos TIC - Mineros. Lo cual abarcó gran parte del tiempo invertido por parte del alumno en el desarrollo de esta investigación. Por lo mismo, se da énfasis en reconocer que el estudio contemplará abstractos relevantes para la metodología a implementar en próximos capítulos, que va por encima del material reconocido y cimentado por otros autores, los cuales serán citados apropiadamente.

### 2.1 Conceptos de riesgos

Se aclararán brevemente algunos conceptos relacionados a los riesgos de una organización. De este modo se definirán los términos que se utilizarán a través de toda la investigación y la metodología. La fuente de información para esta sección se rescato desde la publicación de los Estándares de Gerencia de Riesgos de la Federación Europea de Asociaciones de Administración de Riesgos[3].

#### 2.1.1 Riesgo

El riesgo se puede definir como la combinación de la probabilidad de un suceso y sus consecuencias. En todos los tipos de empresa existe un potencial de sucesos y consecuencias que constituyen oportunidades para conseguir beneficios (lado positivo) o amenazas para el éxito (lado negativo). Se reconoce cada vez más que la administración de riesgos trata tanto los aspectos positivos como los negativos de los riesgos. Por lo tanto, los presentes estándares consideran el riesgo desde ambas perspectivas. En el campo de la seguridad, se suele admitir que las consecuencias son sólo negativas, por lo que la administración de riesgos de seguridad se centra en la prevención y en la mitigación del daño.

[3] FERMA. (2003). *Estándares de gerencia de riesgos.* FERMA.

### 2.1.2 Administración de riesgos

La administración de riesgos es una parte esencial de la gestión estratégica de cualquier empresa. Es el proceso por el que las empresas tratan los riesgos relacionados con sus actividades, con el fin de obtener un beneficio sostenido en cada una de ellas y en el conjunto de todas las actividades.

Una administración de riesgos eficaz se centra en la identificación y tratamiento de estos riesgos, su objetivo es añadir el máximo valor sostenible a todas las actividades de la empresa, introduce una visión común del lado positivo y del lado negativo potenciales de aquellos factores que pueden afectar a la empresa, aumenta la probabilidad de éxito y reduce tanto la probabilidad de fallo como la incertidumbre acerca de la consecución de los objetivos generales de la empresa.

La administración de riesgos debe:

1. ser un proceso continuo y en constante desarrollo que se lleve a cabo en toda la estrategia de la empresa y en la aplicación de esa estrategia.

2. Tratar metódicamente todos los riesgos que rodeen a las actividades pasadas, presentes y, sobre todo, futuras de la empresa

3. Estar integrada en la cultura de la empresa con una política eficaz y un programa dirigidos por la alta dirección.

4. Convertir la estrategia en objetivos tácticos y operacionales, asignando responsabilidades en toda la empresa, siendo cada gestor y cada empleado responsable de la administración de riesgos como parte de la descripción de su trabajo.

Respaldando la responsabilidad, la medida y la recompensa del rendimiento, promoviendo así la eficiencia operacional a todos los niveles.

### 2.1.3 Factores externos e internos

Los riesgos a los que se enfrentan una empresa y sus operaciones pueden resultar de factores tanto internos como externos a la empresa (ver figura 2.1). La figura que sigue recoge ejemplos de riesgos clave en estas áreas y muestra que algunos riesgos específicos pueden verse afectados por factores internos y externos y, por ello, abarcan las dos áreas. Se pueden clasificar en diferentes categorías de riesgo tales como: de azar, financieros, operacionales, estratégicos, entre otros.

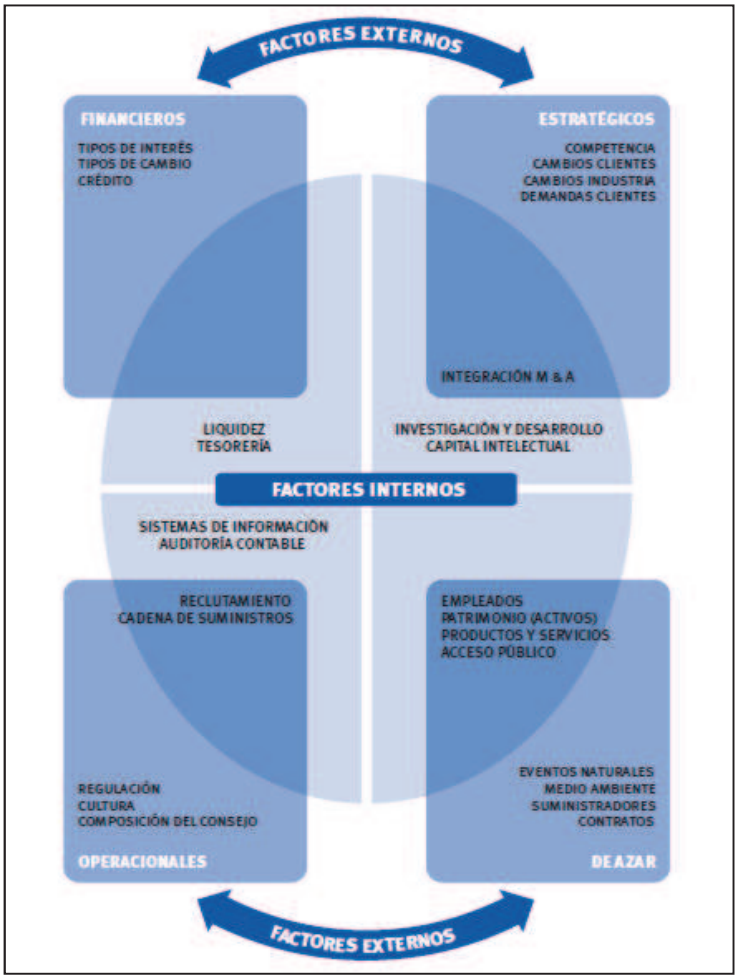


**Figura 2. 1**: Ejemplo de factores internos y externos de riesgos. (FERMA, 2003)

### 2.1.4 Proceso de administración de riesgos

La administración de riesgos protege y añade valor a la empresa y sus interesados mediante el apoyo a los objetivos de la empresa a través de:

- Proveer una estructura que permite que las actividades futuras se desarrollen de forma consistente y controlada.

- Mejorar la toma de decisiones, la planificación y el establecimiento de prioridades mediante una visión integrada y estructurada del negocio, su volatilidad y las oportunidades y amenazas del proyecto.

- Contribuir a una asignación más eficiente del capital y los recursos dentro de la organización.

- Reducir la volatilidad en las áreas no esenciales del negocio.

- Proteger y mejorar los activos y la imagen de la compañía.

- Desarrollar y apoyar a los empleados y la base de los conocimientos de la organización.

- Optimizar la eficiencia operacional.

### 2.1.5 Identificación de riesgos

La identificación de riesgos se propone identificar la exposición de una empresa a la incertidumbre. Ello requiere un conocimiento detallado de dicha empresa, del mercado en el que opera, del entorno legal, social, político y cultural que le rodea, así como el desarrollo de una visión común coherente de su estrategia y de sus objetivos operacionales, incluyendo los factores críticos para su éxito y las amenazas y oportunidades relacionadas con la consecución de estos objetivos.

Hay que enfocar la identificación de riesgos de forma metódica para asegurarse de que se han identificado todas las actividades importantes de la organización y que se han definido todos los riesgos que implican dichas actividades. La volatilidad relacionada con estas actividades debe ser identificada y categorizada.

Las actividades y decisiones empresariales pueden clasificarse en distintas categorías, que incluirían las estratégicas, operacionales, financieras, administración del conocimiento y conformidad.

### 2.1.6 Descripción de riesgos

El objetivo de la descripción de riesgos es mostrar los riesgos identificados de una forma estructurada, por ejemplo, utilizando una tabla. El uso de una estructura bien diseñada es necesario para asegurar un proceso exhaustivo de identificación, descripción y valoración de riesgos. Al tener en cuenta la consecuencia y probabilidad de cada uno de los riesgos que constan en la tabla, debería ser posible dar prioridad a los riesgos clave que tienen que ser analizados con más detalle.

La identificación de los riesgos asociados a las actividades empresariales y la toma de decisiones se pueden calificar como estratégica, táctica u operacional. Es importante incorporar la administración de riesgos en la fase de concepción de los proyectos así como a lo largo de la vida de un proyecto específico.

### 2.1.7 Estimación de riesgos

La estimación de riesgos puede ser cuantitativa, semi-cuantitativa o cualitativa en términos de probabilidad de ocurrencia y de sus posibles consecuencias. Por ejemplo, las consecuencias en términos de amenazas (riesgos negativos) y oportunidades (riesgos positivos) pueden dividirse en altas, medias o bajas.

La probabilidad puede clasificarse como alta, media o baja pero requiere diferentes definiciones respecto a las amenazas y las oportunidades. Algunas empresas opinarán que se adecuarán mejor a sus necesidades medidas de consecuencia y probabilidad diferentes. Por ejemplo, muchas empresas opinan que clasificar las consecuencias y probabilidades como altas, medias o bajas, se adapta bastante bien a sus necesidades y se pueden presentar en una matriz 3x3.

### 2.1.8 Evaluación de riesgos

Cuando el proceso de análisis de riesgos se ha llevado a cabo, es necesario comparar los riesgos estimados con los criterios de riesgo establecidos por la empresa. Los criterios de riesgo pueden incluir costos y beneficios asociados, requisitos legales, factores socioeconómicos y medioambientales, preocupaciones de los interesados, entre otro. Por tanto, se usa la evaluación de riesgos para tomar decisiones acerca de la importancia de los riesgos para la empresa y sobre si se debe aceptar o tratar un riesgo específico.

### 2.1.9 Tratamiento de riesgos

El tratamiento de riesgos es el proceso que consiste en seleccionar y aplicar medidas para modificar el riesgo. El tratamiento de riesgos incluye, como principal elemento, el control o mitigación del riesgo, pero también se extiende más allá, por ejemplo, a la elusión de riesgos, a la transferencia de riesgos, a la financiación de riesgos. Cualquier sistema de tratamiento de riesgos debe proporcionar como mínimo un funcionamiento efectivo y eficiente de la organización, controles internos efectivos y conformidad con las leyes y reglamentos.

### 2.1.10 La estructura y la administración de riesgos

La política de administración de riesgos de una empresa debe definir su enfoque y apetito del riesgo, así como su enfoque de la administración de riesgos. La política también debe establecer las responsabilidades de la administración de riesgos en toda la empresa.

Además, debe referirse a cualquier requerimiento legal para los principios de la política, por ejemplo, en el campo de la salud y la seguridad. Vinculado al proceso de administración de riesgos, debe existir un conjunto integrado de herramientas y técnicas para usar en las diferentes fases del proceso empresarial.

El consejo de administración tiene la responsabilidad de determinar la dirección estratégica de la empresa y de crear el entorno y las estructuras necesarias para que la administración de riesgos opere de forma eficaz. Esta tarea se puede realizar a través de una dirección ejecutiva, una comisión no ejecutiva,

un comité de auditoría o cualquier otra función que se ajuste al modo de operar de la organización y que sea capaz de actuar como promotor de la administración de riesgos.

El papel de las unidades de negocio incluye lo siguiente:

- Las unidades de negocios tienen la responsabilidad primaria de gestionar los riesgos en el día a día.

- La dirección de las unidades de negocios es responsable de promover la conciencia del riesgo en sus operaciones; deben introducir objetivos de administración de riesgos en su actividad.

- La administración de riesgos debe ser un tema habitual en las reuniones de la dirección para considerar las exposiciones y fijar nuevas prioridades en el trabajo a la luz de un análisis de riesgos efectivo.

- La dirección de las unidades de negocios debe asegurar que la administración de riesgos está incorporada en la fase conceptual de los proyectos, así como a lo largo de la vida de los mismos.

El papel de la función de administración de riesgos incluye lo siguiente:

- Establecer la política y la estrategia de administración de riesgos.

- Primer defensor de la administración de riesgos en los niveles estratégico y operacional.

- Crear una cultura consciente de riesgos dentro de la empresa, incluyendo la formación apropiada.

- Establecer la política y estructuras de riesgos internas para las unidades de negocios.

- Diseñar y revisar los procesos de administración de riesgos.

- Coordinar las diversas actividades funcionales que informan de los temas de administración de riesgos dentro de la empresa.

- Desarrollar procesos de respuesta al riesgo, incluyendo planes de contingencia y de continuidad del negocio.

- Preparar los informes de riesgos para el consejo de administración y los interesados.

El papel de la auditoría interna puede variar de una empresa a otra. En la práctica, este papel puede incluir todas o alguna de las siguientes tareas:

- Enfocar el trabajo de la auditoría interna sobre los riesgos importantes, identificados por la dirección, y revisar los procesos de administración de riesgos en toda la empresa.

- Producir confianza en la administración de riesgos.

- Proporcionar un apoyo activo y participar en el proceso de administración de riesgos.

- Facilitar la identificación y valoración de riesgos y formar al personal de operaciones en la administración de riesgos y el control interno.

- Coordinar los informes de riesgos al consejo de administración, al comité de auditoría, entre otros.

### 2.1.11 Supervisión y revisión del proceso

Una administración de riesgos efectiva requiere una estructura de informe y revisión para asegurar que los riesgos están identificados y evaluados eficazmente, que se llevan a cabo los controles oportunos y que las reacciones son las apropiadas.

Se deben efectuar con regularidad auditorías de la política y de conformidad con los estándares, así como revisiones del rendimiento de los estándares para

identificar las oportunidades de mejora, cabe recordar que las empresas son dinámicas y que operan en entornos dinámicos.

Es imprescindible identificar los cambios en la empresa y en el entorno en el que opera, y efectuar las modificaciones apropiadas en los sistemas. El proceso de supervisión debe asegurar que existen los controles apropiados de las actividades de la empresa y que se entienden y se siguen los procedimientos establecidos.

## 2.2 Administración de riesgos

Aquí se analizarán las etapas asociadas a la administración de los riesgos genéricamente. Precisamente, este informe presenta algunos de los aspectos más interesantes de las principales normas internacionales - aspectos que son de interés para la administración de riesgos basado en la investigación del prestigioso Institute Of Governance[4].

La administración de riesgos es un enfoque sistemático para establecer el mejor curso de acción en condiciones de incertidumbre mediante la identificación, la comprensión, la evaluación, priorización, y comunicación acerca de las amenazas potenciales, si afectan a la opinión pública social, financiera o económica, el bienestar, la salud y la seguridad o el medio ambiente.

La administración de los riesgos implica la asignación de los limitados recursos que pueden hacer el mayor bien para el mayor número de personas. Incluye los siguientes pasos:

- La identificación de la cuestión en riesgo.
- La evaluación del nivel y la severidad del riesgo.
- El desarrollo de las opciones, la decisión, la aplicación de la decisión, y
- La evaluación y revisión de la decisión.

En cada paso del proceso, las comunicaciones y las actividades de consulta, las consideraciones legales y en curso las actividades operacionales también deben tenerse en cuenta en el riesgo estrategias de administración efectiva.

[4] Saner, M. (2005). *Information Brief On International Risk Management Standars.*

A continuación se muestra en la figura 2.2 el proceso de toma de decisiones en la administración de riesgos.


**Figura 2. 2:** Proceso de toma de decisiones en la administración de riesgos. (Institute On Governance, 2005)

Existen cinco actividades clave dentro de un marco de Gestión de Riesgos que aplican dentro del proceso de toma de decisiones.

- Establecer metas y enfoque: la identificación de contexto, dando prioridad a los objetivos, y establecer el alcance y la enfoque de todo el ejercicio. Las decisiones tomadas dentro de esta actividad se basan en un juicio sobre los intereses – ¿los intereses de quién valen? – Y entidades – ¿Cuáles entidades tienen un valor? Esto es a veces se llama "Selección de punto final" - ¿Cuál riesgo estamos considerando?

- Describir: llegar a una comprensión objetiva de la probabilidad y la magnitud de un impacto, en términos cualitativos ó en términos cuantitativos. Como tal, es en gran medida una técnica o la actividad científica.

- Prescribir: la evaluación de la calidad de las previsiones contempladas en el paso descriptivo, el equilibrio de los efectos positivos y negativos, las decisiones sobre la forma de mitigar y otra gestionar el riesgo y la aplicación de las medidas. Como tal, es la evidencia y juicio en que se basó la actividad que requiere la consideración de la gran imagen. Representa la clave la toma de decisiones paso en el marco de gestión de riesgos, que no implica que las decisiones de otra naturaleza no se toman en otro lugar.

- Comunicar: la comunicación entre los actores clave en el proceso, así como con los beneficiarios y otras partes interesadas. La comunicación puede ser entendida en sentido amplio como para incluir la información pública, consulta, participación o asociación.

- Monitorear y aprender: una actividad que describe el seguimiento de los efectos de las decisiones y actividades que causan cambios en las condiciones ambientales y la aparición de nuevas pruebas. Las decisiones sobre la necesidad de volver a las evaluaciones y la aplicación de las lecciones aprendidas son parte de esta actividad orientada a los resultados. Estas actividades son componentes de medición del desempeño y la gestión basada en los resultados.

Hasta el momento, se ha estudiado la administración de riesgo en forma genérica dentro de una organización, lo cual debe estar sustentada por normas y estándares internacionales que otorguen fuerza a este proceso.

La terminología de la Organización Internacional de Normalización (*International Standards Organization,* 2002) describe la administración de riesgos como responsabilidad de la empresa a nivel global, mientras que el análisis de riesgo es considerado una tarea científica interna de la empresa.

La evaluación de riesgos corresponde al paso que se toman las decisiones claves sobre los riesgos, y el asesoramiento de riesgos es la combinación del análisis y la evaluación, de esto modo se obtiene como producto el tratamiento de los riesgos, en donde se administran los riesgos estimados aceptables en la organización. Este último paso utiliza como sinónimo el control de riesgo.

En cambio, el Consejo Internacional de Gobierno de Riesgos (*International Risk Governance Counsil*, 2004) define la administración de riesgos como el gobierno de riesgos. Incluye la totalidad de los actores, las normas, convenciones, procesos y mecanismos relacionados con la cantidad de información relevante de riesgo, analiza y comunica las decisiones de administración tomadas.

Abarcando las variadas decisiones relevantes de riesgos y acciones de los protagonistas públicos y privados, este proceso toma relevancia dado que no hay un actor que decida por sí solo. Sino que se considera una actividad grupal de todos los interesados en el riesgo en cuestión, es decir, no existe una autoridad única para tomar una decisión de gestión del riesgo, sino dada la naturaleza del riesgo requiere de la colaboración y la coordinación entre diversas partes interesadas. Sin embargo, la administración de riesgos no sólo incluye un proceso de múltiples facetas, de múltiples factores de riesgo, sino también llama a la consideración de los factores contextuales, tales como las normas institucionales.

Por ejemplo, el marco regulatorio y legal que determina la relación, los roles y responsabilidades de los actores y los mecanismos de coordinación, tales como los mercados, los incentivos o normas autoimpuestas, junto a la cultura y política como las diferentes percepciones de riesgo. A continuación se muestra en la figura 2.3 el marco de gobierno de riesgos.

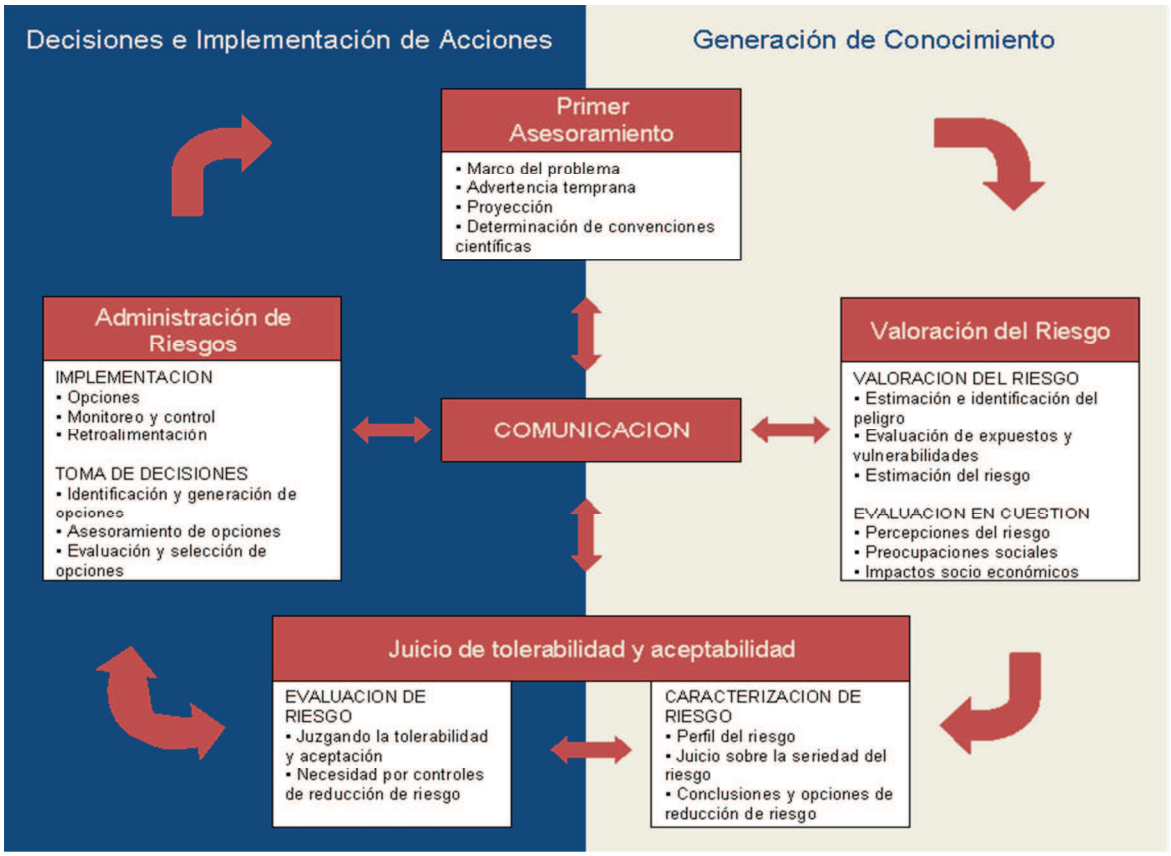


**Figura 2. 3:** Marco del gobierno d riesgos. (Institute On Governance, 2005)

En este marco se aprecian dos grandes clasificaciones de actividades, la toma de decisiones e implementación de acciones y la generación de conocimiento. Cada uno definida por el área de gestión en la administración de riesgos y otra es el plano técnico respectivamente.

## 2.3 Análisis de riesgos en seguridad informática

En el presente capítulo se estudia el análisis de riesgos desde el punto de vista informático, basada en la investigación de la propuesta de Peltier, 2001. Quien plantea que los análisis de riesgos se justifican para la toma de decisiones que se deben realizar cuando están en juego inversiones, recursos, capitales, o simplemente al comenzar una tarea, un proyecto o algún tipo de desarrollo.

Las personas que deben efectuar el análisis deben ser los expertos internos sobre la actividad a realizar. Por ejemplo, si se está tomando a cabo el análisis de riesgos de un proyecto para crear un nuevo proceso en un área de una empresa, las personas que deben ejecutar el análisis de riesgos son precisamente quienes conocen el proceso a implementar, dado que ellos realmente conocen los pro y los contra de la nueva actividad, y los efectos que tendrán sobre las actividades acostumbradas. Aunque el análisis en sí lo realicen los expertos, quienes estudian sus resultados son las personas que toman las decisiones.

El análisis de riesgos idealmente debe durar unos días, no semanas ni meses. Pues es una actividad concisa, pero sí reiterativa. Dado que el análisis pretende revisar tareas, proyectos e ideas a realizar, a modo de verificar su vialidad y si es prudente proceder. El éxito de un análisis de riesgos se mide al ver el mínimo límite de costos de una actividad, en donde se identificaron e implementaron los controles necesario versus sus costos.

Ahora, el análisis de riesgos es parte del programa de aseguramiento de calidad de una organización. En donde la administración de riesgos requiere la identificación de la información como un activo empresarial. La clasificación de la información debe estar bien definida, y se debe aplicar una metodología para determinar el nivel de valor de la información. Para los cuales se tienen controles que varían acorde a su disponibilidad, integridad o confidencialidad.

- Integridad: la información es como fue intencionada, sin modificaciones inapropiadas ni corrupción.

- Confidencialidad: la información es protegida de accesos no autorizados o revelación accidental.

- Disponibilidad: Usuarios autorizados tienen accesos a sistemas y aplicaciones cuando es requerido para realizar una actividad.

El objetivo de la administración de riesgos se plasma en la figura 2.4, en donde se observa un foco central que representa el activo que se está analizando. La primera parte consiste en asistir al riesgo y determinar sus necesidades, lo cual implica realizar el respectivo análisis de riesgos

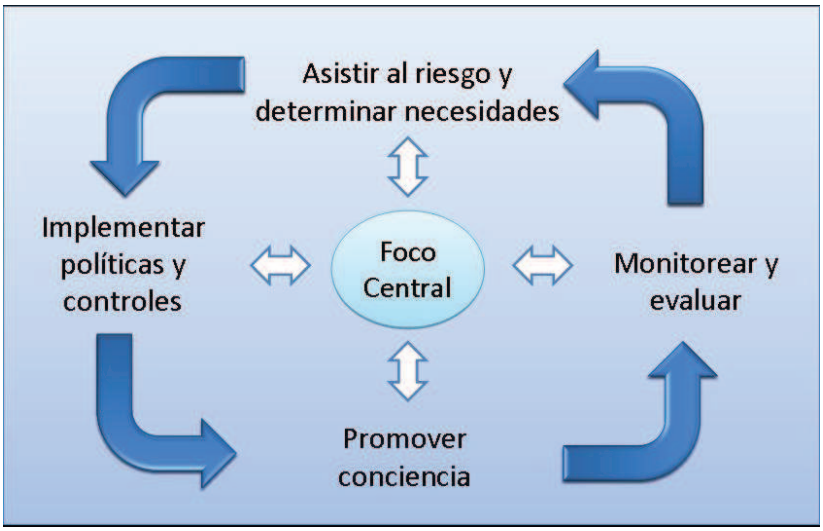


**Figura 2. 4:** Ciclo de la administración de riesgos. (Peltier, 2001)

La metodología estándar de administración de riesgos propuesta identifica el activo a ser revisado, ya sea físico y tangible ó lógico e intangible, este último se refiere a la propiedad intelectual o conocimiento de la empresa. Luego busca las amenazas, riesgos o problemas concernientes al activo para priorizarlos, y así determinar las vulnerabilidades del mismo.

Una herramienta que se utiliza para la estimación de las ocurrencias de una amenaza es precisar la probabilidad de que suceda y multiplicarla por el valor monetario que se adjudica la pérdida que pueda producir un impacto al activo en cuestión, de este modo concretizar una escala numérica para prevalecer las mitigaciones nacientes.

Una vez realizado esto, se efectúan medidas correctivas o controles para atenuar o aceptar los riesgos determinados. Con esto se pueden crear relaciones entre las políticas y estándares con los riesgos que representan, con el fin de mantenerlos y administrarlos adecuadamente.

Luego se debe promover la conciencia sobre los riegos identificados con la empresa o compañía, y educar al personal continuamente sobre las políticas y controles creados, esto tiene como fin el comenzar a trabajar en una cultura empresarial que considere importante los riesgos que amenazan su trabajo periódicamente.

La última fase corresponde a la de monitoreo y evaluación de los riesgos. Aquí se deben realizar actividades como controlar los factores que afectan los riesgos, indicar la efectividad en la seguridad, enviar los resultados a líneas gerenciales para que dirijan esfuerzos en caso de requerirlo, y estar al tanto de nuevas herramientas o técnicas que puedan facilitar el monitoreo o la mitigación del riesgo.

| | Análisis de Riesgo Cuantitativo | Análisis de Riesgo Cualitativo |
|---|---|---|
| Ventajas | Los resultados son basados sustancialmente en objetivos de procesos y métricas independientes.<br><br>Un gran esfuerzo está puesto en la determinación de valor de activos y mitigación de riesgos.<br><br>El esfuerzo en asesoramiento de costo/beneficio es esencial.<br><br>Los resultados pueden ser expresados en lenguaje específico de administración (valores monetarios, porcentajes y probabilidades). | Los cálculos son simples (no existen).<br><br>No es necesario determinar el valor monetario de los activos.<br><br>No es necesario cuantificar la frecuencia de las amenazas.<br><br>Es más sencillo involucrar a personas que no estén dedicadas ni a la seguridad ni a personal técnico.<br><br>Provee flexibilidad en los reportes y procesos. |
| Desventajas | Los cálculos pueden ser complejos.<br><br>Históricamente, sólo trabaja bien con una herramienta automatizada y asociada con una base de conocimiento.<br><br>Requiere un gran trabajo preliminar.<br><br>Generalmente no es presentada a un nivel personal.<br><br>Los participantes no pueden ser fácilmente entrenados a través del proceso.<br><br>Es difícil cambiar de dirección. | Es subjetivo por naturaleza.<br><br>Los resultados caen únicamente en la calidad del equipo de administración de riesgos.<br><br>Para desarrollar valor monetario por activos objetivos se requiere un esfuerzo limitado.<br><br>No existen bases para el análisis de riesgos mitigador en costos/beneficios. |

**Figura 2. 5:** Ventajas y desventajas de los análisis de riesgos cuantitativos y cualitativos. (Peltier, 2001)

Para que este modelo tome fuerza, se deben considerar los distintos tipos de análisis de riesgos, estos se pueden clasificar en dos grandes grupos, los análisis de riesgos cuantitativos y los cualitativos.

El primero intenta asignar objetivos de valores numéricos independientes a cada componente del análisis de riesgo y al nivel de potencial perdida. Cuando

todos los elementos (valor de activo, frecuencia de amenaza, efectividad de los controles, costo de los controles, incerteza y probabilidad) con cuantificados, el proceso se considera completamente cuantitativo.

El análisis de riesgo cualitativo no intenta asignar valores numéricos a los componentes, sino que trabaja más con los escenarios o en las preguntas "Qué pasaría si…", dada su naturaleza subjetiva. En la figura 2.5 se muestran las ventajas y desventajas de ambos análisis de riesgos. En realidad ambos análisis se consideran válidos para trabajar con riesgos de empresas o proyectos, pero dada que las tecnologías de información y la seguridad de la información está basada en activos intangibles, se considera dar mayor énfasis en el análisis de riesgo cualitativo. A continuación se explican con mayor detalle.

### 2.3.1 Análisis de riesgos cualitativos

En análisis de riesgos cualitativo provee un examen sistemática de la santa trinidad Activos – Amenazas – Vulnerabilidades. También otorga una revisión de contramedidas y controles propuestos para determinar la mejor implementación costo/beneficio.

Al establecer un equipo de administración de riesgos de calidad, este análisis queda sujeto a la experiencia de los expertos internos de la organización. El proceso completo es subjetivo por naturaleza, por lo que el equipo mismo debe ser constituido por personal con el conocimiento de trabajo y experiencia necesaria.

El análisis de riesgo cualitativo es una técnica que puede ser utilizada para determinar el nivel de protección requerida para aplicaciones, sistemas, instalaciones o activos empresariales informáticos. La metodología cualitativa intenta priorizar los elementos de los distintos riesgos en términos subjetivos, a continuación se explican los pasos teóricos para llevarlo a cabo.

- 1° Paso – Desarrollar el enunciado de alcance.

En el primer paso se describe lo que será analizado, ya sea un datacenter o un sistema o una red o una restructuración como ejemplo. También se debe identificar quién será el patrocinador o dueño de lo que será analizado. De igual modo se deben definir los límites sobre lo analizado, lo cual en la seguridad de la información se generaliza lo que estará en cuestión bajo los impactos de

amenazas de integridad, confidencialidad y disponibilidad de la información relacionada al objetivo.

- 2° Paso – Reunir un equipo competente.

Es necesario que el personal seleccionado para conformar el equipo de análisis sea altamente calificado y competente. Para que el equipo sea efectivo, debe estar compuesto por personas expertas en diferentes áreas especializadas. Por ejemplo, dueños funcionales de la empresa; usuarios de sistemas; analistas de sistemas; programadores de sistemas; administradores de bases de datos; personal de auditoría; personal de seguridad física; personal de redes de comunicaciones; asesores legales; gerentes de operaciones; e personal de seguridad de la información.

- 3° Paso – Identificar las amenazas.

Los miembros del equipo de trabajo determinan cuáles amenazas pueden causar daño al activo bajo revisión. Esto se puede hacer de muchas maneras, pero la que se utiliza usualmente es realizar una lista de todas las amenazas posibles, y que los expertos decidan si aplican o no a la situación. Inclusive se puede categorizar las amenazas en caso que resulten muchas, y por lo mismo la parte negativa de este ejercicio es que consume mucho tiempo del proceso de análisis de riesgos cualitativo.

- 4° Paso – Priorizar las amenazas.

Una vez identificadas las amenazas se trabaja en otorgar una frecuencia de ocurrencia para cada una, pero dado su origen subjetivo la frecuencia debe ser Baja, Media o Alta. Numéricamente, también pueden ser valores como 1, 2 o 3. Para esto, cada miembro del equipo debe asignar una frecuencia a cada amenaza, y para obtener un resultado simplemente se pueden promediar las frecuencias de cada integrante del equipo, o se puede revisar una a una para consensuar un resultado.

- 5° Paso – Priorizar los impactos.

Este paso pretende determinar la pérdida que se produce si una amenaza llega a ocurrir. Al igual que en el paso 4, cada integrante debe asignar una pérdida por cada amenaza, pero ésta escala tiene 5 peldaños (Baja, Baja-Media, Media, Media-Alta, Alta). En números se evalúa del 1 al 5. De igual modo, para obtener un resultado final se pueden promediar los resultados, o analizar amenaza por amenaza cuál sería su pérdida en el activo en cuestión. Como el equipo tiene distintas experiencias, se considera oportuno realizar una revisión de pérdida en conjunto, a modo que todos entiendan la relación de pérdida de negocio/activo.

- 6° Paso – Calcular el total de impacto por amenaza.

Ahora se debe crear un factor de riesgo, el cual se calcula acorde los valores entregados en los pasos anteriores. El factor de riesgo tiene una escala desde el 2 hasta el 10, considerando que el valor 6 debe tener como requerimiento un mínimo de Medio en las etapas anteriores. Al igual que antes, cada integrante debe otorgar un valor para luego promediarlo o consensuarlo como grupo de trabajo. Como resultado se obtendrá la priorización de cada amenaza que puede ocurrir al activo analizado. Esto se puede plasmar en un archivo como se muestra en la tabla II.1 siguiente.

| Amenaza | Prioridad | Pérdida | Factor Riesgo |
|---|---|---|---|
| Fuego | 3 | 5 | 8 |
| Daño de tuberías | 2 | 5 | 7 |
| Robo | 2 | 3 | 5 |
| Terremoto | 3 | 5 | 8 |

**Tabla II. 1:** Hoja de trabajo completada con los controles identificados. (Peltier, 2001)

- 7° Paso – Identificar controles.

En el paso 7 el equipo analiza las vulnerabilidades identificadas y busca por controles técnicos, administrativos y físicos para ofrecer un nivel costo efectivo aceptable como protección del activo sujeto a revisión. Como resultado se espera contar con controles que consideren:

- Evitar: Controles proactivos que intenten minimizar el riesgo.

- Asegurar: Controles a través de herramientas y estrategias empleadas para asegurar la efectividad de los controles existentes.

- Detectar: Controles en forma de técnicas y programas usados para asegurar la detección, intervención y respuesta temprana ante una amenaza.

- Recuperar: Controles para planificar y responder servicios para rápidamente devolver un ambiente seguro e investigar ante ocurrencias de amenazas.

- 8° Paso – Análisis costo/beneficio.

En este punto se deben considerar todos los controles encontrados y verificar que son costo efectivos, dado que cada control cambiará el modo en que hoy se trabaja en la empresa u organización, ya sea asignando más personas o sistemas para implementar dichos controles. En caso que los controles encontrados no sean aceptables, se debe volver al paso 6 y volver a estudiar. Lo ideal es hallar controles que ataquen más de una amenaza.

- 9° Paso – Especificar los controles en orden prioritario.

Considerando que los recursos para implementación de controles son limitados, se deben priorizar antes de presentar a la administración que los utilizará. Por lo mismo, el equipo de análisis de riesgos cualitativo debe comprender el negocio y los controles encontrados para presentarlos en orden de implementación. Es importante considerar que los controles deben encontrarse con los objetivos de la empresa, por ningún motivo contradecirlos. También es importante destacar que los administrativos pueden elegir aceptar el riesgo ante el control sugerido.

- 10° Paso – Reportar análisis de riesgo.

Como parte de la metodología, el último paso consiste en entregar el análisis en un reporte, el cual debe estar compuesto por: Introducción; Resumen ejecutivo; Identificación de amenazas; Determinación del factor de riesgo; Identificación

de los controles; Análisis costo/beneficio; Controles recomendados; y Apéndices del trabajo realizado.

Otra manera de abordar el análisis de riesgo cualitativo es asignando un sistema de evaluación para habilitar los riesgos como activos financieros, permitiendo al equipo de análisis de riesgo considerar segundos impactos en los activos en cuestión. Este método comienza luego que se ha conformado el equipo de análisis de riesgos cualitativos, y considera tablas que ayudan a retratar los costos asociados al compromiso de los activos que se están evaluando. Sus etapas son las siguientes:

1° Etapa – Tasación de los activos.

La primera etapa consiste en determinar cuál sería el impacto en la empresa si uno de sus activos de ve comprometido. Para esto se elabora una escala de impactos al negocio, la cual se muestra como ejemplo en la tabla II.2 y nace por medio de numerosas entrevistas con personal clave del negocio.

Una vez lista la escala, se asigna uno de sus valores de pérdida a cada activo que puede afectar el negocio y para consensuar los valores de los impactos se puede promediar o discernir como equipo (ver tablas II.3 y II.4). Estos valores de pérdida/control se reportan a la administración o dueño del análisis de riesgos cualitativos para que él autorice seguir con la segunda etapa.

| Pérdida Financiera | Valores |
|---|---|
| X < $2,000 | 1 |
| $2,000 < X < $15,000 | 2 |
| $15,000 < X < $40,000 | 3 |
| $40,000 < X < $100,000 | 4 |
| $100,000 < X < $300,000 | 5 |
| $300,000 < X < $1,000,000 | 6 |
| $1,000,000 < X < $3,000,000 | 7 |
| $3,000,000 < X < $10,000,000 | 8 |
| $10,000,000 < X < $30,000,000 | 9 |
| $30,000,000 < X | 10 |

**Tabla II. 2:** Escala de pérdida financiera (Peltier, 2001)

| Valores de pérdida de activo versus impacto | Pérdida Financiera | Interrupción a Usuarios | Impactos Legales | Confidencialidad | Vergüenza Empresarial |
|---|---|---|---|---|---|
| Desclasificación | | | | | |
| Modificación | | | | | |
| No Disponibilidad | | | | | |
| Destrucción | | | | | |

**Tabla II. 3:** Valores de pérdida de activo versus impacto. (Peltier, 2001)

| Vergüenza Empresarial | Valores |
|---|---|
| Dentro del proyecto | 1 |
| Otras áreas de la organización | 2 |
| A toda la empresa | 3 |
| Prensa local | 5 |
| Cobertura nacional | 7 |
| Acciones e inversiones | 10 |

**Tabla II. 4:** Valores de pérdida ante el impacto de Vergüenza Empresarial. (Peltier, 2001)

2° Etapa – Evaluación de riesgos.

En esta etapa se identifican las amenazas que pueden impactar a los activos evaluados, y al mismo tiempo se detectan las vulnerabilidades de los activos que facilitan la ocurrencia de dichas amenazas. Para comenzar, se crea una lista de todas las posibles amenazas que puedan ocurrir, siguiendo con sus probabilidades de ocurrencia y su impacto sobre el activo. Esta actividad es similar al método anterior, pero los valores otorgados corresponden a impactos al negocio. Estos valores se rescatan desde la etapa anterior, como ejemplo se muestran los valores en la tabla II.5.

| Vulnerabilidades de las Amenazas | | Impacto | | |
|---|---|---|---|---|
| | | Bajo | Medio | Alto |
| Probabilidad | Alto | 3 | 6 | 9 |
| | Medio | 2 | 5 | 8 |
| | Bajo | 1 | 4 | 7 |

**Tabla II. 5:** Vulnerabilidades de las amenazas identificadas. (Peltier, 2001)

En el caso que una amenaza no aplique a la situación el valor correspondiente es “N/A”. También es recomendado hacer esta evaluación considerando las amenazas sin controles (ya sean existentes o no), y otra con los controles que se determinen.

3° Etapa – Administración de riesgos.

Las dos etapas anteriores conducen a la identificación de controles que pueden ser implementados para minimizar la vulnerabilidad de las amenazas a un nivel de administración aceptable. La parte más importante de cualquier proceso de administración de riesgos son las recomendaciones de los controles que pueden ayudar a mitigar el nivel de la amenaza o vulnerabilidad del activo en cuestión. Esto se facilita a través de la tabla II.6, en donde se muestra este análisis como resultado final para exponer al patrocinador o dueño del proyecto.

Por último, una herramienta que facilita la identificación de los riesgos es la Matriz de Análisis de Riesgos que indica los controles adecuados por cada riesgo. Ésta matriz se muestra en la figura 2.6.

| Activo Bajo Análisis | Puntajes | | | | | |
|---|---|---|---|---|---|---|
| | Desclasificación | Modificación | No Disponibilidad | Destrucción | Valores de las Vulnerabilidades | |
| | | | | | Sin Control | Con Control |
| Amenazas: | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

**Tabla II. 6:** Análisis de Riesgos Cualitativo. (Peltier, 2001)

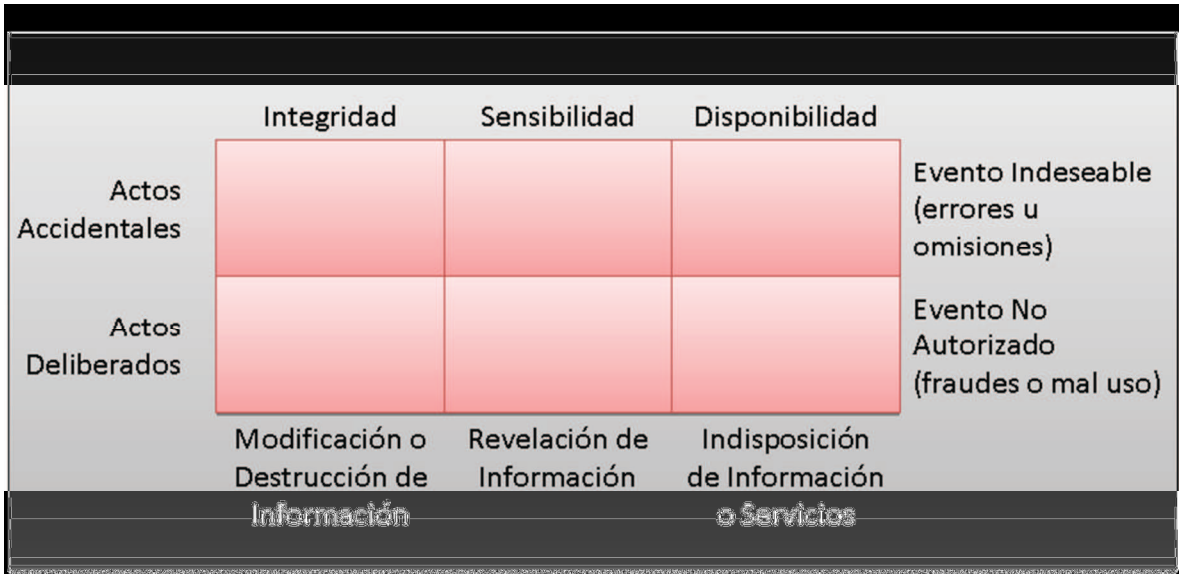


**Figura 2. 6:** Matriz de análisis de riesgos. (Peltier, 2001)

Esta matriz es utilizada para ser completada con los riesgos identificados y posteriormente con los controles respectivos, tal como se muestra en las figuras 2.7 y 2.8.

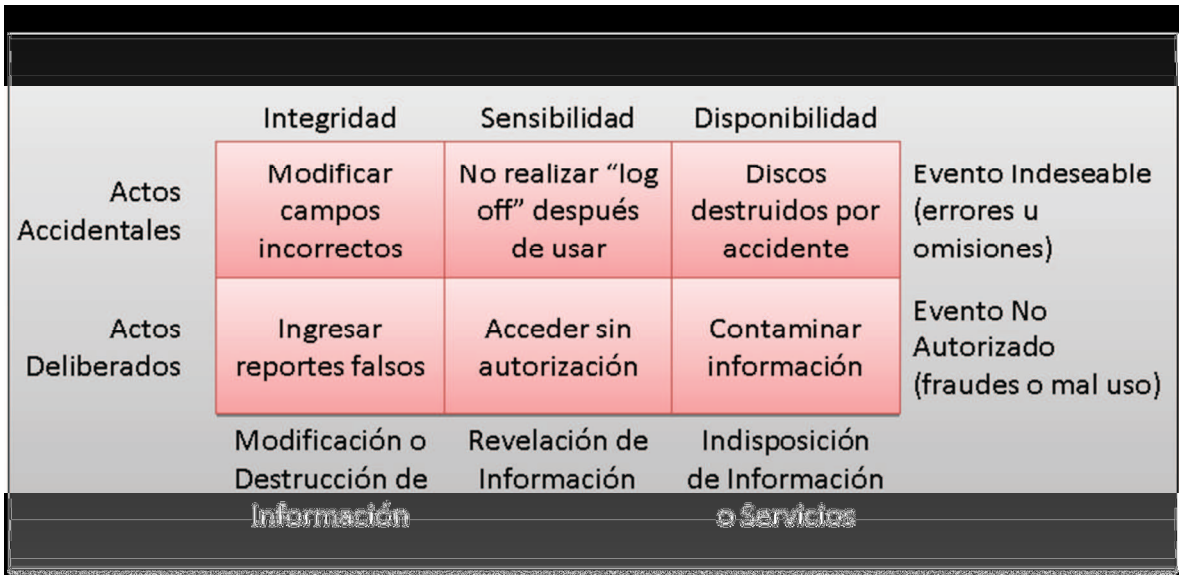


**Figura 2. 7:** Matriz de análisis de riesgos completada con riesgos. (Peltier, 2001)

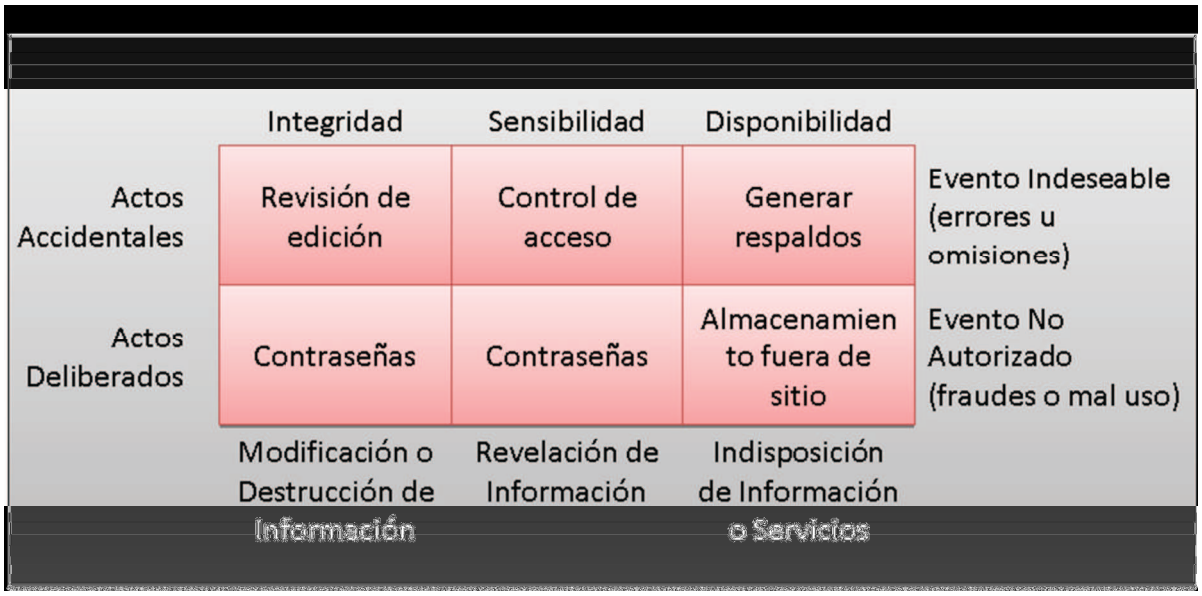


**Figura 2. 8:** Matriz de análisis de riesgos completada con controles. (Peltier, 2001)

En conclusión, el análisis de riesgo cualitativo es un proceso que permite a las empresas evaluar expuestos tangibles o intangibles de los activos de la organización. Provee un método lógico y consistente para revisar las amenazas y sus impactos en los activos bajo revisión. Los dos métodos mostrados son los cimientos para la administración de riesgos en IT, pero no son suficientes para un análisis de riesgos.

Es cierto que el resultado del análisis está sujeto al equipo que realiza su evaluación, pero la mayoría de los expertos no tienen conocimientos en la valoración de activos informáticos. Es por esto que se sugiere fuertemente que los dueños de los activos en cuestión sean o se involucren cuando se asignan los valores de impacto al negocio cuando dichos activos se ven comprometidos.

# CAPÍTULO III

# Marco teórico de la administración de riesgos en el Project Management

## 3.1 Project Management.

Se estudiará el cómo se manejan los riesgos en la administración de proyectos, desde el punto de vista mostrado en la guía del PMBOK[5]. En donde se buscará la correlación de lo estudiado previamente junto a las herramientas facilitadas por el PMI®.

En esta documentación se encuentran las mejoras practicas en la administración de proyectos, presentada por módulos que están compuestos por procesos que se interrelacionan a lo largo del ciclo de vida de un proyecto. A continuación se estudiaran los procesos dentro del modulo de administración de riesgos.

Los procesos de la administración de riesgos en proyectos están definidos por seis procesos que intentan amplificar la probabilidad e impacto de eventos positivos, mientras disminuyen la de eventos negativos en el proyecto que se está trabajando. Estos se definen textualmente como:

> *"Planificación de la Administración de Riesgos: decidir cómo enfocar, planificar y ejecutar las actividades de administración de riesgos para un proyecto.*
>
> *Identificación de Riesgos: determinar qué riesgos pueden afectar al proyecto y documentar sus características.*
>
> *Análisis Cualitativo de Riesgos: priorizar los riesgos para realizar otros análisis o acciones posteriores, evaluando y combinando su probabilidad de ocurrencia y su impacto.*

[5] Project Management Institute (2008). *A Guide to the Project Management Body of Knowledge*. [s.n]

*Análisis Cuantitativo de Riesgos: analizar numéricamente el efecto de los riesgos identificados en los objetivos generales del proyecto.*

*Planificación de la Respuesta a los Riesgos: desarrollar opciones y acciones para mejorar las oportunidades y reducir las amenazas a los objetivos del proyecto.*

*Seguimiento y Control de Riesgos: realizar el seguimiento de los riesgos identificados, supervisar los riesgos residuales, identificar nuevos riesgos, ejecutar planes de respuesta a los riesgos y evaluar su efectividad a lo largo del ciclo de vida del proyecto. ”* (Project Management Institute, 2008)

## 3.2 Planificación de la administración de riesgos

Como en cualquier proyecto, una buena planificación es la base para que las etapas posteriores resulten exitosas. En este primer proceso de administración de riesgos se decide como afrontar con éxito las actividades en la gestión de riesgo, obteniendo como resultado un plan de administración de riesgos acorde a los riesgos existentes y su implicancia en el proyecto. De este modo de otorgar los recursos y tiempos necesarios para las evaluaciones requeridas.

En la figura 3.1 se pueden observar las entradas al proceso, que proporcionarán la información suficiente para generar el plan de administración de riesgos. Lo cual se llevará a cabo por medio de reuniones y análisis con los interesados del proyecto, con quienes se definirán las acciones y tiempos a asignar al proyecto.

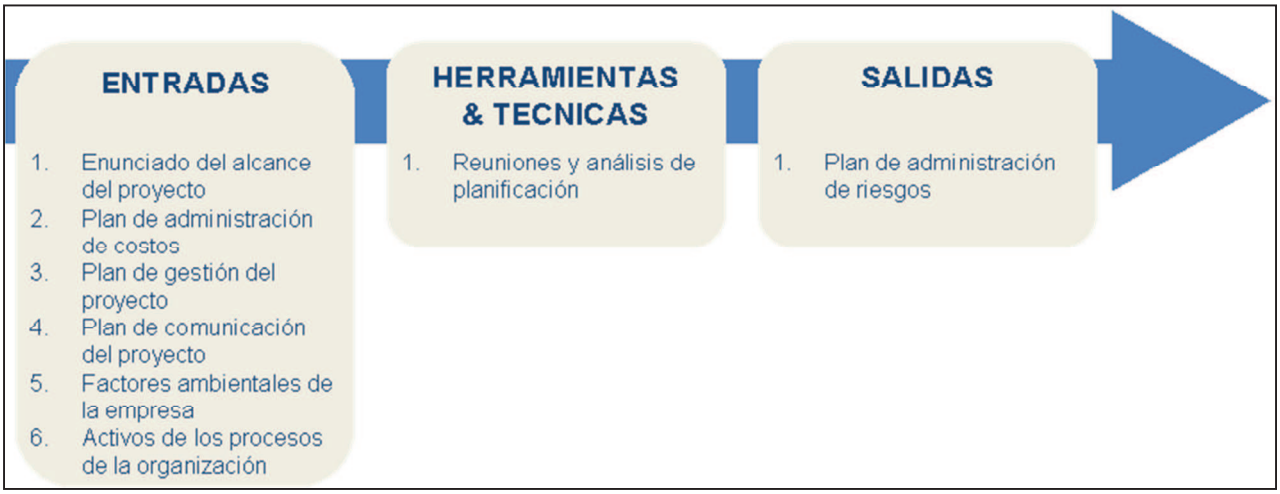


**Figura 3. 1:** Entradas, herramientas & técnicas, salidas del proceso de planificación de la administración de riesgos. (PMI, 2008)

En la salida de la figura se puede observar que el único entregable será el plan de administración de riesgo, en donde se indicarán las metodologías a utilizar, los roles, responsabilidades, preparación de presupuesto, tiempos, categorías de riesgos, las tolerancias aceptables por los interesados, los formatos de reportes, seguimiento y por último se establecerán las probabilidades e impactos asociados a los riesgos por identificar en el próximo proceso.

Para ejecutar lo último, la PMI sugiere elaborar una matriz de impacto a base de los objetivos del proyecto, en donde se clasifican los impactos por categorías de pérdidas. Esta matriz será utilizada más adelante al momento de evaluar riesgos según sus impactos, facilitando las escalas propuestas en esta fase. De igual modo se puede elaborar una matriz de oportunidades acorde a los impactos que se identificarán más adelante.

## 3.3 Identificación de riesgos

En este proceso se identifican los riesgos que pueden impactar los objetivos del proyecto para luego ser documentados. Las personas que identifican los riesgos deben incluir a todos los involucrados en el proyecto, dado que conviene contar con la mayor experiencia posible para obtener un resultado robusto. Este proceso es iterativo a lo largo del proyecto, dado que pueden surgir nuevos riesgos en nuevas etapas por abordar en la vida del proyecto. Por

lo mismo, es importante contar con una documentación de riesgos accesible para compararla en distintas etapas, de modo identificar variantes en los factores de riesgo, procurando involucrar a todas las personas que inicialmente participaron. De este modo asegurar su participación y compromiso a lo largo del proyecto.

En la figura 3.2 se muestran las entradas del proyecto, que contendrán toda la información necesaria para el proceso, la cual será encausada para obtener un registro completo de los riesgos a identificar. Esto se puede facilitar por medio de una lluvia de ideas, entrevistas, técnica Delphi y RCA. El resultado esperado es un registro de los riesgos en donde se indiquen un listado de aquellos identificados, una lista de posibles respuestas por cada uno, sus causales y la categorización.


**Figura 3. 2:** Entradas, herramientas & técnicas, salidas del proceso de identificación de riesgos. (PMI, 2008)

## 3.4 Análisis cualitativo de riesgos

El tercer proceso pretende priorizar los riesgos identificados para que el proyecto pueda trabajar en aquellos sean de mayor relevancia, siempre y cuando los riesgos restantes sean aceptablemente tolerados. El análisis

cualitativo otorga la prioridad según su probabilidad de ocurrencia, según su impacto en los objetivos y en otras propiedades del proyecto.

En la figura 3.3 se pueden observar las entradas requeridas en el proceso, las cuales serán sometidas a un análisis de probabilidad de ocurrencia e impactos. Esto se puede plasmar en una matriz complementaria a la trabajada en el proceso anterior, así poder visualizar fácilmente los impactos y oportunidades con una alta probabilidad de suceder. Además, se realiza un análisis de calidad de los datos sobre los riesgos, para mantener un nivel de efectividad costo eficiente para el proyecto, y así aportar valor a los planes de respuesta de riesgos. Adicionalmente, se trabaja en la categorización de los riesgos y en la evaluación de urgencia de cada riesgo. Todo lo anterior con la constante experiencia de las personas involucradas del proyecto en el análisis de riesgos.

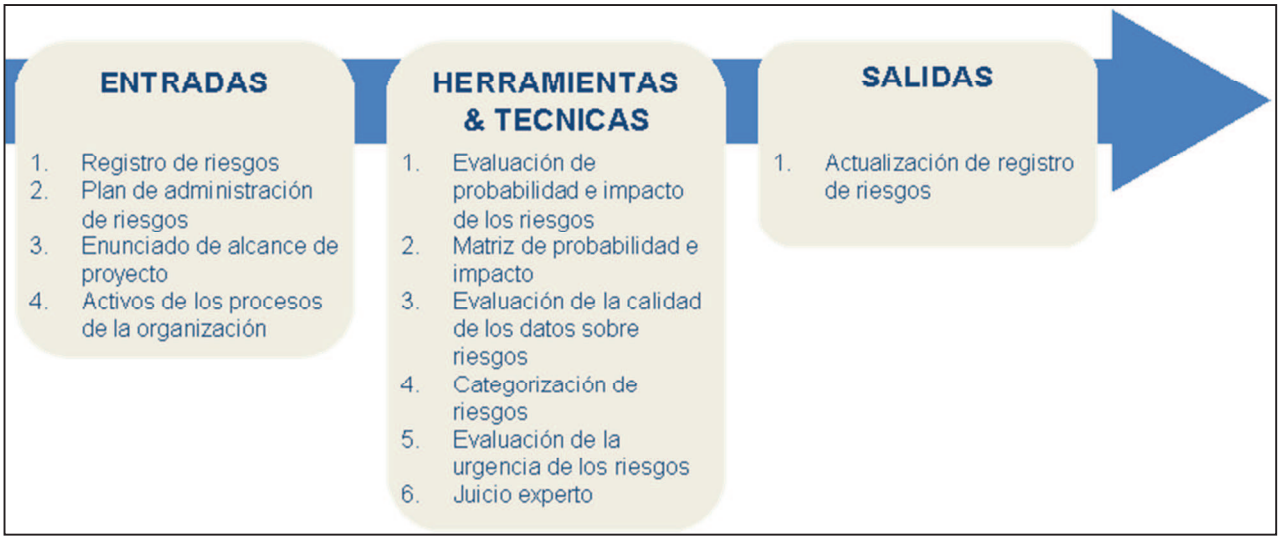


**Figura 3. 3**: Entradas, herramientas salidas & técnicas, del proceso de análisis cualitativo de riesgos. (PMI, 2008)

Como resultado se espera poder actualizar el registro de riesgos con mayor detalle sobre los mismos, elaborar una lista de prioridades de riesgos categorizados, lista de los riesgos que requieren respuesta a corto plazo, lista de riesgos que necesitan mayor investigación, una lista de riesgos con baja prioridad, y por último mantener en registro las tendencias a las cuáles se dirigen los riesgos del proyecto.

## 3.5 Análisis cuantitativo de riesgos

Este proceso tiene como meta cuantificar los impactos sobre los objetivos del proyecto, utilizando los eventos que derivan a los riesgos que registraron una alta ocurrencia en el proceso anterior. También presenta una forma cuantitativa de tomar decisiones sobre los riesgos asociados al proyecto. Pero esta fase puede no aplicar para ciertos proyectos, dada su alta demanda de recursos del proyecto. Por lo mismo, en el plan de administración de riesgos se debe dar un espacio para evaluar si este proceso será aplicado o no.

En la figura 3.4 se muestran las entradas solicitadas para el proyecto. Las herramientas y técnicas a utilizar incluyen la recopilación y representación de datos, ya sea por medio de entrevistas para cuantificar las probabilidades e impactos de los riesgos, o sea por distribuciones de probabilidades para representar incertidumbres de los valores de tiempos o costos del proyecto.


**Figura 3. 4:** Entradas, herramientas & técnicas, salidas del proceso de análisis cuantitativo de riesgos. (PMI, 2008)

En cuanto a las técnicas de análisis y modelado, se incluye un análisis de sensibilidad, análisis del valor monetario esperado, un análisis de árbol de decisiones, y modelado y simulación de datos, para obtener los valores de los impactos de manera más concreta en comparación al proceso anterior. Todo lo anterior bajo la supervisión del juicio experto que compone el equipo de trabajo en la administración de riesgos.

Como resultado esperado se actualizará el registro de riesgos con información financiera que facilitará la toma de decisiones sobre los riesgos y sus

tolerancias ante los interesados del proyecto. Esta actualización incluye un análisis probabilístico del proyecto, las estadísticas ante el logro de los objetivos monetarios y tiempos, una lista priorizada por los riesgos cuantificados, y la tendencia de los riesgos a lo largo del proyecto.

### 3.6 Planificación de la respuesta a los riesgos

En esta parte de los procesos, la planificación de las respuestas de los riesgos determina las acciones a seguir y las opciones que se tienen para tomar oportunidades y reducir las amenazas del proyecto. En este punto se asignan las responsabilidades a una o más personas sobre las acciones acordadas y financiadas que se establezcan para cada respuesta de los riesgos existentes, para que las lleven a cabo acorde a su prioridad asignada en el proyecto. Quién selecciona las respuestas a seguir son los interesados del proyecto en conjunto, dado que los recursos en todo proyecto es limitado se debe trabajar con aquellas que pueden impactar al proyecto significativamente.

En la figura 3.5 se muestran las entradas del proceso, el registro de riesgos actualizado y el plan de administración de riesgos preparado. Con ello se establecen las estrategias a seguir con las amenazas u oportunidades identificadas, ya sea para evitarlas, transferirlas, mitigarlas o aceptarlas, o bien para explotar, compartir, mejorar o aceptarlas respectivamente. De este modo prepara las respuestas a los riesgos e incorporarlas al registro de riesgos vigente, y así poder generar las salidas solicitadas. Estas últimas hacen referencia al plan de administración de proyecto (tiempos, costos, calidad, adquisiciones, recursos humanos, WBS y planes), acuerdos contractuales relacionados a los riesgos (supuestos y documentación técnica), y a la actualización de documentos del proyecto, con el fin de incorporar las amenazas u oportunidades que pueden afectar el éxito del proyecto.

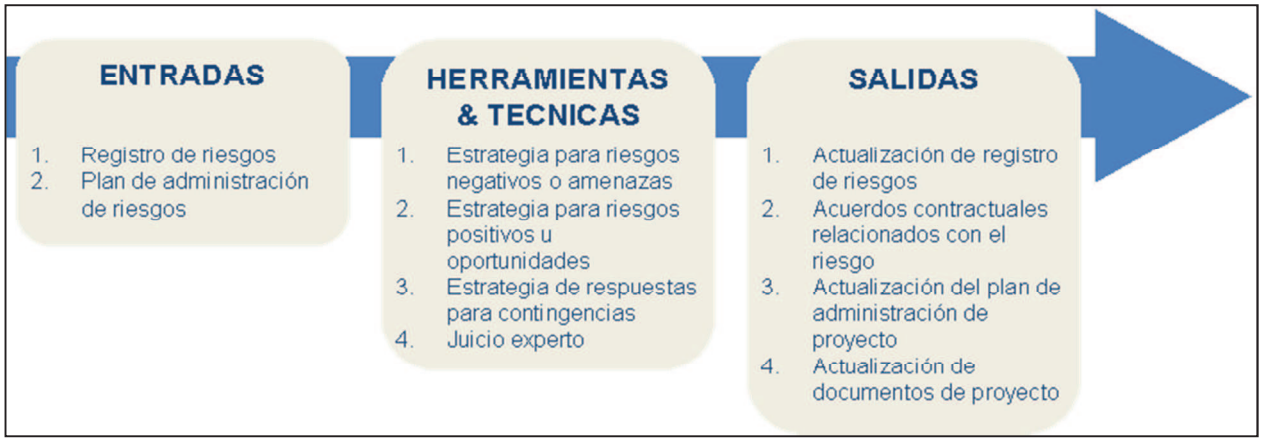


**Figura 3. 5:** Entradas, herramientas & técnicas, salidas del proceso de planificación de la respuesta a los riesgos. (PMI, 2008)

## 3.7 Seguimiento y control de riesgos

Este último proceso presta atención a los riesgos nuevos que puedan aparecer a lo largo del ciclo de vida del proyecto constantemente, pero al mismo tiempo mantiene la supervisión sobre los riesgos ya identificados, especialmente aquellos que quedan en la lista de revisión de riesgos con baja prioridad (riesgos residuales). En esta etapa también se validan los supuestos del proyecto, si las evaluaciones de riesgos permanecen vigentes, si se siguen las políticas y procedimientos establecidos del proyecto y si las reservas de contingencia se pueden modificar para alinear los riesgos del proyecto.

En la figura 3.6 se muestran las entradas, las herramientas y técnicas y las salidas del proceso. Entre las herramientas se realizan las reevaluaciones de los riesgos del proyecto, las auditorías a los mismos, el respectivo análisis de variaciones y tendencias, las mediciones de rendimiento técnico, y el análisis de reserva mencionado previamente. Una vez hecho esto, se realizan reuniones sobre el estado de la situación actual del proyecto para estudiar los cambios que se requieren hacer o no para alinearse lo más posible con los objetivos del proyecto. Como salida se obtienen las actualizaciones del registro de los riesgos, de los activos de los procesos de la organización, del plan de administración de proyecto y los documentos respectivos. Finalmente se realizan los cambios solicitados.

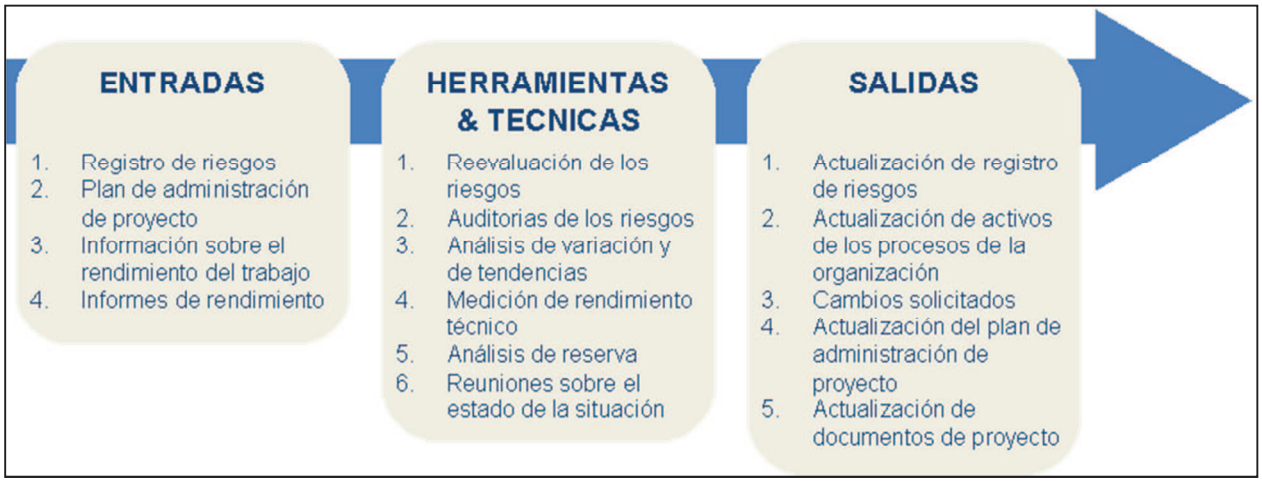


**Figura 3. 6:** Entradas, herramientas & técnicas, salidas del proceso de seguimiento y control de riesgos. (PMI, 2008)

# CAPÍTULO IV

## Proyectos IT en la minería del cobre

Se instruirá sobre la administración de proyectos informáticos en la industria de la minería del cobre, en donde se presentarán el modo en que se desarrollan exitosamente incluyendo la mitigación de riesgos, basado en la experiencia laboral del alumno y las herramientas adquiridas a través de la trayectoria de certificaciones. La administración de riesgo en proyectos o cambios en la industria del cobre es la estrategia para toda la empresa para la prevención eficaz de riesgos, un método estructurado y consistente que alinea a la estrategia, los procesos, personas, tecnología y conocimientos, con el propósito de evaluar y administrar las incertidumbres que enfrenta la empresa para crear valor para los accionistas. La administración de riesgos es una manera de administrar y tratar el impacto de cambios, tanto internos como externos. Involucra:

- Identificación del riesgo asociado con el cambio.
- Análisis y evaluación del riesgo
- Selección e implementación de una estrategia/control apropiado para manejar el riesgo.
- El monitoreo y la revisión de la estrategia/control.

Una clasificación de estándares y pautas de administración de riesgo forman la base fundamental de la estrategia y política de la misma. Para una empresa minera, el éxito radica en la necesidad de que la administración de riesgos esté integrada con las actividades cotidianas de administrar y manejar cambios (ver figura 4.1).

El riesgo se define como exposición a las consecuencias de la incertidumbre, y tiene 2 dimensiones, la probabilidad que ocurra algo y las consecuencias si fuera a ocurrir. Se evalúan todos los riesgos usando las mismas herramientas de administración de riesgos, con referencia a los mismos estándares y pautas de la administración de riesgos, asegurando de esa manera que todos hablan el

mismo idioma cuando se conversa y evalúan los riesgos para toda la empresa minera.

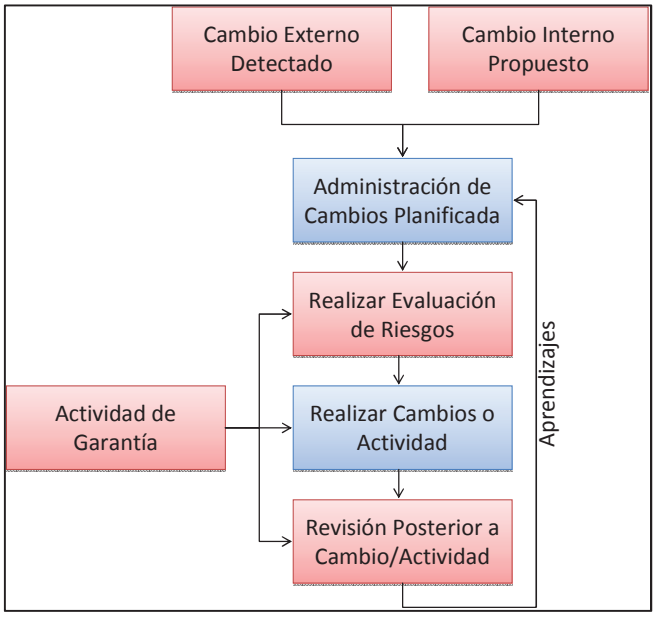


**Figura 4. 1:** Estándar minera en la administración de riesgos.(Elaboración propia)

En esta industria, la necesidad de evaluar riesgos se ve determinada por las consecuencias críticas que se podrían gatillar si no se tiene un control de ellos, estas consecuencias implican tanto al personal como a las operaciones que mantienen el negocio. Los cubos de riesgos (Ver figura 4.2) muestran cómo los tipos de riesgos operacionales, que la mayoría de las personas asocia con la administración de riesgos, frecuentemente son transformaciones de, y respuesta a, los riesgos externos impuestos en el ambiente de la empresa.

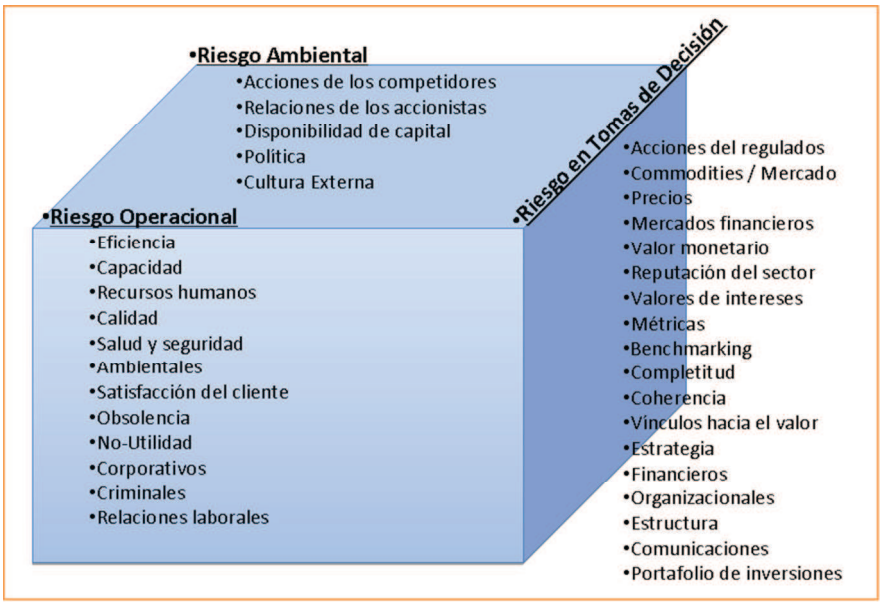


**Figura 4. 2:** Acercamiento holístico al riesgo (Elaboración propia).

El modelo del sistema, el cual está detrás del proceso "Qué Pasaría Si…", indica una variedad de riesgos que se podrían aplicar a cualquier problema, ordenados en input, procesos y output (ver figura 4.3). Trabajando consistentemente en estas áreas puede ser de utilidad para asegurar una evaluación completa de riesgos.

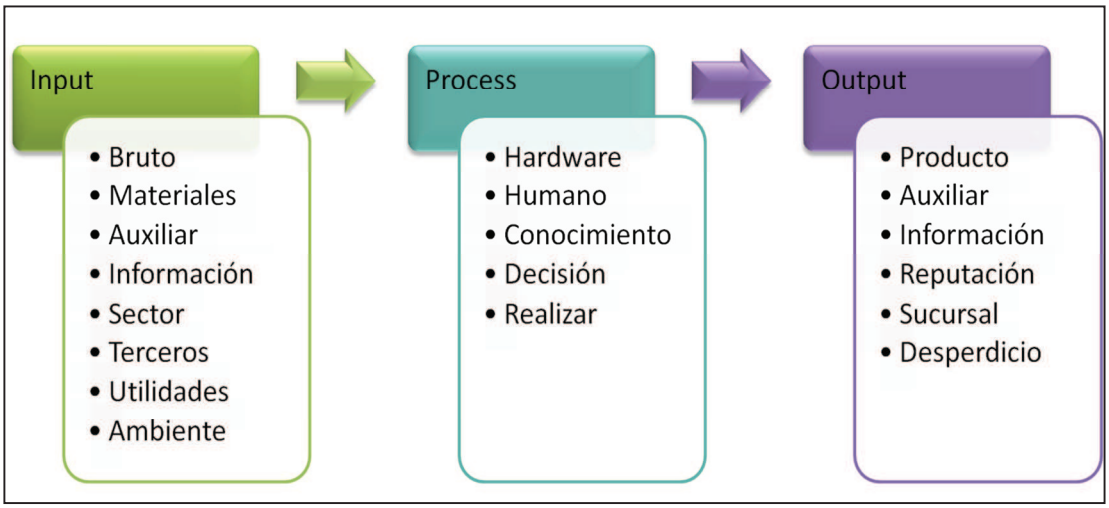


**Figura 4. 3:** Modelo Entrada / Proceso / Salida "Acercamiento sistemático al riesgo"

Cuando un cambio es planificado, detectado o iniciado, debería ser llevado a cabo un asesoramiento de los riesgos u oportunidades asociadas con el proceso de cambio mismo, o los logros de los objetivos del negocio minero o estratégico. El asesoramiento de riesgos está enfocado en determinar aquellos cambios, eventos inciertos y situaciones que podrían prevenir o retrasarnos en el logro del plan de negocios y los objetivos estratégicos.

## 4.1 Método simple de evaluación de riesgos

Es realizado por una persona que ha identificado el problema y puede ser accionado y tratado de inmediato debido a que la severidad de las consecuencias potenciales a la minera es mínima. Involucra la persona que identificó el cambio, pensando en las implicaciones del cambio antes de realmente implicarlo o aceptarlo. Si las implicaciones del cambio son inaceptables, se debe tomar acciones apropiadas de control de riesgos. Hay dos métodos para realizar una evaluación simple, se refieren a estos como: Los tres “Qué” y Step Back.

Los tres “Qué”: Antes de actuar, la persona que propone un cambio o que ha detectado que un cambio está a punto de ocurrir debe considerar lo que podría fallar, lo que podría causar qué falla y qué podría prevenir qué falla.

Step Back: Consiste en la persona que identifica el cambio, haciendo una pausa para pensar en los riesgos. Pensando qué daños, deterioro o pérdida podrían ocurrir. Pensando en qué podría pasar para que ocurra ese daño, deterioro o pérdida. Decidiendo qué hay que hacer para manejar esas causas para prevenir que ocurra el daño, deterioro o pérdida. Tomando esas acciones ellos mismos o notificando a otros sobre qué hay que hacer y por qué. Realizando un cierre asegurando que se tomen las acciones y que sean eficaces antes de que haya una exposición al riesgo.

## 4.2 Clasificación de riesgos

La clasificación de riesgos mostrada en la Figura 4.4 es un método para calcular el riesgo residual que queda con los controles existentes. La severidad es el nivel de pérdida, daño o perjuicio que podría ocurrir, que podría tener un impacto sobre la empresa minera, su marca registrada y sus interesados. Ó puede ser una visión positiva, el nivel de oportunidad esperado no aprovechado que se podría perder.

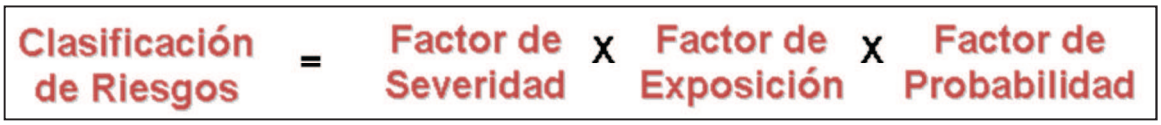


**Figura 4. 4:** Definición de clasificación de riesgos

La exposición es el tamaño más probable del periodo disponible durante el cual la minera y sus interesados estarán expuestos a las consecuencias de ese nivel de severidad. La probabilidad es la oportunidad más probable que ocurran consecuencias tan severas durante el periodo de exposición. En las tablas IV.1, IV.2 y IV.3 se muestran estos factores para la industria minera.

| Exposición | Descripción | Factor |
|---|---|---|
| Constante | En cualquier momento | 16 |
| Frecuente | Una vez al mes | 4 |
| Ocasión | Una vez al año | 2 |
| inusual | Una o dos veces cada 20 años | 1 |

**Tabla IV. 1:** Exposición (Elaboración propia).

| Probabilidad | Descripción | Factor |
|---|---|---|
| Probable | Ocurre con facilidad | 3 |
| Posible | Podría ocurrir | 2 |
| Improbable | No podría ocurrir | 1 |

**Tabla IV. 2:** Probabilidades (Elaboración propia)

| Prioridad | Índice de Riesgo | Acción Sugerida | Programación Sugerida | Tolerancia Continua Autorizada |
|---|---|---|---|---|
| 1 | X > 100 | Cesación hasta reducir el riesgo residual a 50 o menos | Inmediato | Presidente y Junta Directiva |
| 3 | 60 < X < 100 | Planificar Tratamiento de acuerdo a las necesidades del negocio. | Mediano Plazo | Informes Directos del Presidente |
| 4 | 30 < X < 60 | Planificar de acuerdo a demás Prioridades | Cuando hay Tiempo | Gerente |
| 5 | X < 30 | Decisión propia | - | - |

Tabla IV. 3: Pautas de Prioridad (Elaboración propia)

## 4.3 Eligiendo un método de evaluación

La evaluación de riesgos no es un proceso único para toda situación. Por ejemplo, un proceso largo y completo de evaluación no es lo que se requiere para un cambio que es bien entendido y tiene poco impacto. La elección del método dependerá de si el cambio es creciente (operacional) o radical (estratégico).

El método de evaluación de riesgos por perfil debe estar reservado para cambios complejos de gran envergadura donde la severidad potencial de las consecuencias identificadas es alta.

Se debe definir una tabla de severidades que contemple las diferentes dimensiones en donde puede ser afectada la organización. Por ejemplo, algunas dimensiones que pueden ser usadas en esta tabla pueden ser:

- Basándose en la norma ISO 27001, en seguridad de la información, las dimensiones son: Integridad, confidencialidad y disponibilidad.

- COBIT en base a sus criterios de información, plantea las siguientes dimensiones: Efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

- La industria hace hincapié en las dimensiones; HSE, financieros, reputación, etc.

Luego de definir la tabla de severidades, es importante determinar que se hará dependiendo del impacto que pueda causar algún riesgo, la tabla IV.5 muestra una posible clasificación para este punto.

| Nivel de Severidad | Método | Realizado Por |
|---|---|---|
| a | "Perfil" seguido por análisis específico al riesgo | Facilitador capacitado, después un especialista en el tipo de riesgo |
| b | "Perfil" seguido por análisis específico al riesgo | Facilitador capacitado, después un especialista en el tipo de riesgo |
| c | "Perfil" seguido por análisis específico al riesgo | Facilitador capacitado, después un especialista en el tipo de riesgo |
| d | "Perfil" | Facilitador capacitado |
| e | "Perfil" | Facilitador capacitado |
| f | Simple | Todos los empleados |
| g | Simple | Todos los empleados |

**Tabla IV. 4**: Selector de método de evaluación de riesgos (Elaboración propia)

## 4.4 Evaluación de riesgos por perfil

Es utilizado en todas las instancias con consecuencias con nivel de severidad “e” o superior. Requiere una reunión facilitadora (un taller de asesoramiento de riesgo) o una revisión por un grupo de personas involucradas como reunión. También requiere la participación de los dueños del cambio, los interesados y se debe seguir un esquema organizado sistemático. El objetivo de esto es detallar los riesgos y sus causas, potenciales consecuencias, controles y el cálculo de la clasificación del riesgo para obtener las acciones a seguir.

## 4.5 Rol del facilitador antes de realizar los talleres

### 4.5.1 Reunir información de antecedentes

Investigar el riesgo particular o conjunto de riesgos. Se podría querer revisar: el plan de negocios y los objetivos estratégicos; el registro de riesgos y cualquier problema de riesgos relevante documentado en él; informes recientes de auditorías internas, externas u otras; Mapas de procesos y diagramas organizacionales; registros de autoevaluaciones anteriores de controles, si son relevantes; datos de accidentes incidentes incluyendo a investigaciones / análisis; documentos legales relevantes; experiencias previas con este tipo de riesgo; datos gubernamentales e industriales; estándares y pautas de administración de riesgos relevantes.

### 4.5.2 Considerar quién debe participar en el equipo

Decidir quiénes son los interesados principales, ¿Quiénes deben estar en el equipo? Apuntar a 5 a 8 miembros del equipo para eficacia máxima e interrupción mínima. Sin embargo, este consciente que es posible una cantidad de 4 a 20 personas, dependiendo de los interesados involucrados. Los requerimientos claves para los miembros del equipo son: del lugar de trabajo que se está evaluando (para crear un sentido de dominio); una buena representación de los interesados involucrados; los miembros del equipo deben tener la experiencia relevante, ganada sobre un periodo de tiempo razonable; el equipo debe incluir la persona que estará usando los resultados, la cual podría o no ser la de más antigüedad / posición para acordar las acciones que resulten del taller; por último, es necesario incluir especialistas en la materia (puede incluir personal externo a la minera).

### 4.5.3 Resumir la información relevante para los miembros del equipo

Resumir la información de antecedentes para los miembros del equipo de taller. Necesitarán una buena visión general del riesgo, con detalles suficientes en aquellas áreas donde el facilitador cree se justifique. Asegurar que lo que prepare sea “digerible” para los demás miembros del equipo. Pensar en qué tan complejo es el problema / riesgo / cambio, y calcular cuánto tiempo necesitará para realizar el taller. Puede ser de 2 a 3 horas, hasta una sesión de medio día.

### 4.5.4 Invitar al equipo

Conseguir que los interesados invitados mantengan un registro diario de taller. Tratar de hacer el taller en la mañana cuando todo el mundo se siente despejado. Distribuir la información de antecedentes antes de la reunión para que tengan la oportunidad de leerla y entenderla. Avisar a los participantes en el taller qué es lo que pueden esperar, es decir, aproximadamente 4 horas en un esfuerzo a evaluar los riesgos particulares, sin distracciones, ni celulares, entre otros.

### 4.5.5 Realizar entrevistas

Entrevistar a los interesados principalmente aquellos que no pueden asistir al taller, donde sea necesario. Tenga como objetivo contar con todas las personas

que necesite en el taller. El proceso de entrevistas es un respaldo en caso de que sea la única manera de conseguir la corroboración de un interesado principal. Cuando el tiempo lo permita, la información reunida de las entrevistas debe ser integrada con la demás información de antecedentes que envíe a los miembros como lectura previa a la reunión.

### 4.5.6 Organizar un registrador que asista a la reunión

Un registrador es vital para asegurar que las discusiones de los resultados queden registradas correctamente. La facilitación de una evaluación de riesgos es un rol exigente. Frecuentemente esto significa que es mejor que otra persona se encargue de la tarea de registrar la evaluación. Las características de un buen registrador son: alguien con un buen entendimiento del contexto de la discusión y de la terminología que ocupará el equipo; alguien con habilidades suficientes en computación para mantenerse al tanto con la conversación, Deben ser capaces de escuchar, digitar y entender.

### 4.5.7 Organizar un lugar / instalaciones para la reunión

Debe ser de tamaño suficiente para que alberge alrededor de 10 personas. Es ideal que tenga un diseño circular para que nadie domine la mesa. Si el taller toma el tiempo que normalmente incluye almuerzo o colaciones, organizar un servicio para que nadie tenga que salir del taller. Reservar la sala para 4 horas como mínimo, o más si el problema es complejo, Organizar un servicio de mensajería para que los miembros del equipo puedan trabajar sin interrupciones.

## 4.6 Evaluación y asesoramiento de riesgos holísticos

Esta actividad contiene una serie de tareas y herramientas para ejecutar:

- Una presentación que introduce los conceptos y procesos de la administración de riesgos, además del sistema de clasificación de riesgos.

- Mapa de entendimiento por parte del facilitador (mind maps).

- Hojas de clasificación de riesgos.

- Planilla del registro de riesgos

- Otros: formularios de asistencias, tarjetas para nombres y reglas básicas del taller.

Para abrir la reunión, como facilitador necesita introducir al equipo en contexto antes de empezar la evaluación de riesgos. Se debe explicar las reglas básicas del taller y las herramientas disponibles que están incluidas en el taller. Podrían usar también algunos de los temas fundamentales de la administración de riesgos para hacerles recordar los conceptos claves de evaluación de riesgos.

También se entrega un objetivo de visión general para el taller, los resultados esperados y determinar los controles apropiados para ellos. Empiece guiando al equipo por la información que se reunió. El rol de facilitador no es liderar, sino que guiar. Esto se hace con cuidado o el quipo le dejará a usted hacer todas las preguntas. Ellos deben hacer las preguntas y es trabajo del facilitador asegurar que se siga un sistema y que no se olviden de nada.

**FORMULARIO DE INFORME DE AUTOEVALUACION DE CONTROLES**

AREA / TEMA _____
PROYECTO _____
FACILITADOR _____
FECHA _____

| Identificación | | | Estrategia de Control | | | | Evaluación | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| N° Problema | Causas | Impactos | Gerente Responsable | Controles Existentes | Efecto del Control (%) | Más acciones | Severidad | Exposición | Probabilidad | Índice | Exposición Bruta (US$M) |
| 1 | | | | | | | | | | | |
| 2 | | | | | | | | | | | |
| 3 | | | | | | | | | | | |
| 4 | | | | | | | | | | | |
| 5 | | | | | | | | | | | |
| 6 | | | | | | | | | | | |
| 7 | | | | | | | | | | | |
| 8 | | | | | | | | | | | |
| 9 | | | | | | | | | | | |
| 10 | | | | | | | | | | | |
| 11 | | | | | | | | | | | |
| 12 | | | | | | | | | | | |
| 13 | | | | | | | | | | | |
| 14 | | | | | | | | | | | |
| 15 | | | | | | | | | | | |
| 16 | | | | | | | | | | | |
| 17 | | | | | | | | | | | |
| 18 | | | | | | | | | | | |
| 19 | | | | | | | | | | | |
| 20 | | | | | | | | | | | |

**Figura 4. 5:** Resultado de la evaluación de riesgos (Elaboración propia)

Use un proceso estructurado siguiendo un mapa de entendimiento o lista de impulso (“Prompt List”) para asegurar que se trata de todos los aspectos. Puntos a seguir en este proceso incluyen el asunto o problema en cuestión, su causa e impacto posible, los controles existentes y faltantes, evaluar si es adecuado los resultados hasta ahora y priorizar las acciones a seguir.

Se debe alentar el pensamiento lateral por parte de los participantes, para pensar por fuera del cuadro para asegurar que identifiquen tantos riesgos como sean posibles. También es importante resumir con frecuencia y avance cuando se haya conversado adecuadamente un tema. Verificar que la persona que escribe el informe entiende el resumen. Se muestra un documento que refleja los resultados de la evaluación en la figura 4.5. Realizar todas las clasificaciones de riesgos al final del taller o cuando la atención decaiga.

## 4.7 Estrategia de control de riesgos

Para los riesgos identificados en el taller como de alta severidad hay varias tácticas que se pueden considerar dado el nivel de incertidumbre resultado y la habilitada para ejercer un control sobre el riesgo (actitud). La matriz de la figura 4.6 muestra como los elementos se combinan para representar una estrategia de control de riesgos apta para las circunstancias.


**Figura 4. 6:** de tácticas de riesgos (Peltier, 2001)

El nivel de incertidumbre muestra cuatro tipos:

- Tipo 1 – un resultado suficientemente claro, el riesgo residual es irrelevante porque el cambio es beneficioso o inevitable y el impacto es predecible.

- Tipo 2 – resultados alternativos, típicamente una situación que ha sido enfrentada antes, donde ustedes tiene la idea bastante buena de la elección disponible en base del precedente.

- Tipo 3 – rango de resultados, donde los resultados reales podrían mentir en cualquier parte del rango, pero no hay resultado naturalmente discretos, por lo tanto hay ambigüedad.

- Tipo 4 – ambigüedad total, la situación esta sujeta a una tremenda incertidumbre y es impredecible.

Habilidad de ejercer un control sobre el riesgo:

- Formación de riesgos – donde tiene el poder a forzar el riesgo y puede actuar para controlarlo.

- Adaptación de riesgos – donde no controla el riesgo directamente, pero tiene la habilidad de adaptar sus acciones y estrategias para acomodar la situación.

- Posición de reservas – donde no puede formar el riesgo de ninguna manera, y no se puede controlar. Por lo tanto, se debe ir a la posición más beneficiosa y privilegiada donde queremos asegurar que se tendrá un derecho a futuro.

Tácticas legítimas:

- Actuar “sin remordimientos” – en este caso siempre hay una recompensa, sin importar el resultado. Esta táctica es para inversiones

de tiempo, esfuerzo y capital que obviamente son beneficiosos y donde no se puede perder. Se deben usar aún en tiempos de incertidumbre.

- Realizar "grandes apuestas" – Estos son compromisos grandes de capital, inversiones grandes o cambios dramáticos en la forma o propósito organizacional. Los riesgos acá son grandes con gran potencial positivo y negativo. Esta táctica será aceptable solamente donde hay bajos niveles de incertidumbre.

- Adoptar Opciones – Aquí se debe tomar acción para asegurar el mayor beneficio para los resultados del mejor caso mientras actúen para minimizar las pérdidas de los resultados en el peor caso.

- No hacer nada – No hacer nada en este momento, esperar que haya más certeza o que tenga un mayor control sobre el riesgo.

## 4.8 Tendencias en la administración de riesgos

Dentro de toda la documentación investigada para el presente trabajo de memoria, se encontraron nuevas tendencias en la administración de riesgos, que pueden aportar valor a la metodología que se pretende plantear por medio de enfoques que aún están en desarrollo. A continuación se desarrollan.

### a. Planificación para una década impredecible[6]

El rápido desarrollo de la gestión de riesgos, y su turno para convertirse en una herramienta estratégica que soporta el negocio, no podría haber llegado en un momento más oportuno. La creciente complejidad del negocio global, y multiplicando los riesgos que acechan en toda actividad empresarial, significa que es más necesario que nunca una función que pueda ayudar a identificar los posibles problemas y oportunidades.

Apesta a orgullo decir que se puede predecir el futuro, pero esto no significa que no se obtendrán beneficios considerando lo que los próximos años puedan deparar. Así como la estrategia corporativa se basa en la planificación de varios

[6] World Economic Forum. (2009). *Global Risks 2009 A global Risk Network Report.* WEF.

años en el futuro, la gestión del riesgo también debe tener en cuenta los potenciales problemas que se podrían tener en la planificación de los procesos.

Técnicas tales como la planificación de escenarios, permiten a los ejecutivos considerar futuros posibles y entender las interdependencias entre las distintas categorías de riesgo de una forma creíble, y puede ser una herramienta valiosa para ayudar a ver cómo su estrategia puede verse afectada por una gama de posibles resultados.

Problemas recientes en los mercados de crédito y vivienda, y las predicciones pesimistas de algunos comentaristas que el ciclo económico puede haber llegado, hacen hincapié en la necesidad de comprender el alcance y la naturaleza de los riesgos que enfrenta la compañía. Se citan riesgos económicos, como las crisis del precio del petróleo, el colapso de los precios de los activos, y la recesión mundial, entre los más graves a enfrentar, también se cree que estos riesgos son bastante probables que se materialicen.

Existe un creciente reconocimiento de que las empresas deben hacer más para abordar los riesgos a largo plazo, tales como el cambio climático y el cambio demográfico, pero los niveles de preparación en estas áreas son actualmente bastante bajos. El enfoque a corto plazo de muchas empresas, especialmente las públicas, como consecuencia de las presiones para reunir objetivos trimestralmente, puede contribuir a esta falta de planificación.

### b. Riesgo inteligente[7]

Se cree que la Inteligencia de Riesgos tiene mucho que ofrecer a los líderes en sus esfuerzos para administrar el riesgo, consiste en ampliar las habilidades para anticipar y reaccionar con anterioridad a los cambios del mercado, los cuales traen tanto oportunidades como amenazas nuevas a las empresas. Los enfoques tradicionales de administración de riesgos priorizan medidas de mitigación basadas en la probabilidad de eventos de riesgo. Esa es una razón por la que muchas empresas fueron sorprendidas por la reciente crisis financiera. Las probabilidades de obtener una situación tan mala parecían tan bajas que pocas empresas sentían que era necesario planificar para esa eventualidad. La inteligencia de riesgo invita a no ser parte de ese grupo, y preparar una estrategia de riesgo como un objetivo del día a día en una organización.

---

[7] Deloitte. (2009). *Risk Intelligence in a downturn Balancing risk and reward in volatile times.* Deloitte.

De acuerdo con el marco empresarial de Riesgo Inteligente, la gestión eficaz del riesgo depende de tres componentes clave:

- Riesgo de gobierno, incluida la toma de decisiones estratégicas y supervisión de riesgos, encabezada por el consejo de administración.

- Infraestructura y gestión del riesgo, incluyendo el diseño, implementación y mantener un programa eficaz de los riesgos, liderado por la dirección ejecutiva.

- La propiedad de riesgo, incluyendo la identificación, medición, seguimiento y presentación de informes sobre riesgos específicos, dirigidos por las unidades de negocio y sus funciones.

Las actividades de todos estos niveles se integran en un programa sistemático a través de toda la empresa, e incorporan un marco estratégico sobre los riesgos en todos los aspectos de la administración empresarial, y que da a los líderes una visión clara de los retos y oportunidades que el riesgo puede crear.

Nueve principios fundamentales de un programa de Inteligencia de Riesgo:

1. En una empresa de riesgo inteligente, se utiliza constantemente en toda la organización. una definición común de riesgo, que aborda tanto la preservación del valor, como la creación de valor,

2. En una empresa de riesgo inteligente, se utiliza, en toda la organización, un Framework basado en normas internacionales para gestionar los riesgos.

3. En una empresa de riesgo inteligente, están claramente definidos y delimitados dentro de la organización, los roles claves, las responsabilidades y autoridades en relación a la administración de los riesgos.

4. En una empresa de riesgo inteligente, una infraestructura de gestión de riesgos común es utilizada para apoyar las unidades de negocio y funciones en el desempeño de sus responsabilidades sobre riesgos.

5. En una empresa de riesgo inteligente, los órganos de gobierno (por ejemplo, las juntas, comités de auditoría, entre otros) tienen una transparencia adecuada y la visibilidad en las prácticas de la administración de riesgos de otras organizaciones para cumplir con sus responsabilidades.

6. En una empresa de riesgo inteligente, la dirección ejecutiva está a cargo de la responsabilidad de diseñar, implementar y mantener un programa eficaz de los riesgos.

7. En una empresa de riesgo inteligente, las unidades de negocio (departamentos, agencias, áreas) son responsable de la ejecución de sus negocios y la administración de los riesgos que toman en el marco de riesgo establecido por la dirección ejecutiva.

8. En una empresa de riesgo inteligente, ciertas funciones (por ejemplo, Finanzas, Legal, Fiscal, IT, RRHH) tienen un impacto generalizado en el negocio y brindan apoyo a las unidades de negocio, ya que hacen referencia al programa de riesgo de la organización.

9. En una empresa de riesgo inteligente, ciertas funciones (por ejemplo, la auditoría interna, gestión de riesgos, cumplimiento) ofrecen garantías objetivas, así como supervisar e informar sobre la eficacia del programa de riesgo de una organización a los órganos rectores y ejecutivos de administración.

### c. Riesgo inteligente empresarial[8]

Las empresas que se consideran inteligentes en riesgos tienen en común muchas características, tales como prácticas de administración de riesgos que abarca todo el negocio. Tienen estrategias de administración de riesgos que se ocupan de todo el espectro de los riesgos, incluidos los específicos de la industria, el cumplimiento, la competencia, seguridad del medio ambiente, privacidad, continuidad del negocio, estratégico, presentación de informes, y de funcionamiento. Sus procesos de evaluación de riesgos aumentan el convencional énfasis en la probabilidad mediante la colocación de un peso

[8] Deloitte. (2006). *The Risk Intelligent Enterprise ERM Done Right.* Deloitte.

significativo en vulnerabilidad. Sus enfoques de administración de riesgos que no sólo consideran eventos individuales, sino también tener en cuenta los escenarios de riesgo y la interacción de múltiples riesgos.

Las prácticas de gestión de riesgos que se infunden en la cultura empresarial, de modo que la estrategia y la toma de decisiones evolucionan a partir de un proceso de riesgo, en lugar de tener las consideraciones de riesgo impuesto después de los hechos. La filosofía de administración de riesgos se centra no solo en la evasión de riesgos, sino que también en la toma de riesgos como un medio para la creación de valor. Los pasos fundamentales para formar a ser parte de este tipo de empresas son los siguientes:

- Establecer un marco general de política, y el proceso para la evaluación y gestión del riesgo.

- Identificar los principales riesgos y vulnerabilidades y los planes para dirigirlos exitosamente. Evaluar el valor y determinar los riesgos podrían impactarlo.

- Establecer el apetito de riesgo. Determinar la cantidad de riesgo que han asumido. Decidir si puede asumir más o se deben tomar menos.

- Decidir quién tiene la responsabilidad y autoridad para tomar riesgo en nombre de la empresa.

- Determinar su capacidad para administrar el riesgo en una forma integrada y sostenible.

## d. Inteligencia en riesgos, de la teoría a la práctica[9]

### i. Los beneficios que conlleva una inteligencia de riesgos exitosa

- Foco en la administración proactiva y mejorada.

[9] Deloitte. (2007). *Risk Intelligence: From theory to practice.* Deloitte.

- Minimiza la gestión de crisis y gestión de riesgos reactiva.

- Permite la administración para evaluar y tomar decisiones sobre una base bien informada.

- Define la filosofía de la asunción de riesgos de la organización y promueve el apetito por el riesgo.

- Cultura de conocimiento de riesgos y la mayor rendición de cuentas.

  - Compromete la administración superior y al Consejo y aclara la propiedad (la rendición de cuentas) de los riesgos.

  - Hace la administración de riesgo un trabajo de todos y otorga mayor fuerza e independencia a los empleados.

- Gestión de costos efectiva y asignación de recursos.

  - Permite una mejor estimación de las necesidades de capital y más eficiente despliegue de capital.

  - Proporciona la capacidad de gestionar mejor los fondos limitados y asignar recursos a las áreas prioritarias.

- Establece una visión integrada del riesgo en toda la organización.

  - Pone énfasis en las concentraciones de riesgo y considera riesgos que pueden haber sido revisados previamente.

  - Permite tomar decisiones informadas de la hora de responder a la evolución de regulación y entorno externo.

  - Identifica los riesgos que pueden impedir el logro de los objetivos de su negocio.

- Mejora de la capacidad para responder a las expectativas de las partes interesadas.

    - Las agencias de calificación crediticia están incorporando la inteligencia en riesgos empresariales en sus criterios de evaluación.

## ii. Construyendo un marco sustentable para la inteligencia de riesgos empresarial

La falta de recursos con experiencia puede ser el único gran factor que limita la capacidad de las organizaciones para sostener su Inteligencia de Riesgos Empresarial. El asesoramiento en la creación de un marco, a una mayor probabilidad de supervivencia incluye:

- Desarrollar una visión clara para la aplicación del marco, articulando un objetivo final de destino y las medidas de éxito.

- Diseñar un plan de trabajo adaptado a las prioridades y el correcto ritmo de aplicación para su organización.

- Adoptar un enfoque basado en componentes para el marco, la elección de elementos de una secuencia lógica de aumentar la adaptación y el uso.

- Asegúrese de educar, comunicar y sensibilizar la definición de administración de riesgos y su asociada política.

## iii. Barreras de integración para la inteligencia de riesgos empresarial

- La falta de comprensión de los requisitos debido a la complejidad del proceso o a una educación insuficiente.

- Falta de herramientas de apoyo y estructura.

- La Inteligencia de Riesgos no se está incorporando en las métricas de rendimiento ni a la medición adecuada.

- La imposibilidad de demostrar de manera adecuada cómo la Inteligencia de Riesgos agrega valor a la organización.

- La falta de visibilidad sobre cómo la Inteligencia de Riesgos contribuye a la toma de decisiones.

- La Inteligencia de Riesgos es visto como un programa más, sin relevancia estratégica.

## 4.9 Apología del marco teórico

Por medio de toda la documentación estudiada, y los temas propuestos en el Marco Teórico del presente documento, se ha construido un conocimiento base para la creación de una metodología.

Hemos revisado conceptos teóricos de riesgos y de la administración de riesgos – tanto genéricamente, como aplicado a proyectos y específicamente a Gerencias de Tecnologías de la Información. Pero los resultados encontrados son muy similares, dado que las herramientas pueden ser aplicables a distintos ámbitos y rubros.

Incluso al estudiar las tendencias de la administración de riesgo, nos hemos encontrado con un enfoque con grandes expectativas. Lo que se traduce a incorporar la administración de riesgos dentro de la estrategia corporativa de las organizaciones, lo cual amplía los límites de la administración de riesgo, pero no los resuelve, al contrario, lo complica aún más.

Con certeza se puede decir que se ha encontrado un común denominador en la administración de riesgos, las herramientas utilizadas. Por lo que se propone llevarlas al próximo paso, al incorporarlas dentro de una metodología sistemática que simplifique y agilice el proceso de administrar el riesgo.

Esta metodología se profundiza en el siguiente capítulo.

# CAPÍTULO V

## Metodología sistemática

La metodología propuesta, comprende toda la investigación del capítulo anterior, agregando conexiones entre las metodologías presentadas, las cuales aportan integridad y completitud al ciclo de vida de la administración de riesgos.

La propuesta de este modelo proviene de una composición de todas las materias alcanzadas en el marco teórico, manteniendo un énfasis especial en la administración de proyectos que presenta el PMI integrando la administración basada en actividades. Pero el resultado directo de este modelo proviene del estudio realizado por el alumno autor, quién ha estado expuesto a situaciones en las que ha adquirido un gran conocimiento sobre las repercusiones de una administración de riesgos efectiva, así como también aquellas que resultan contraproducentes.

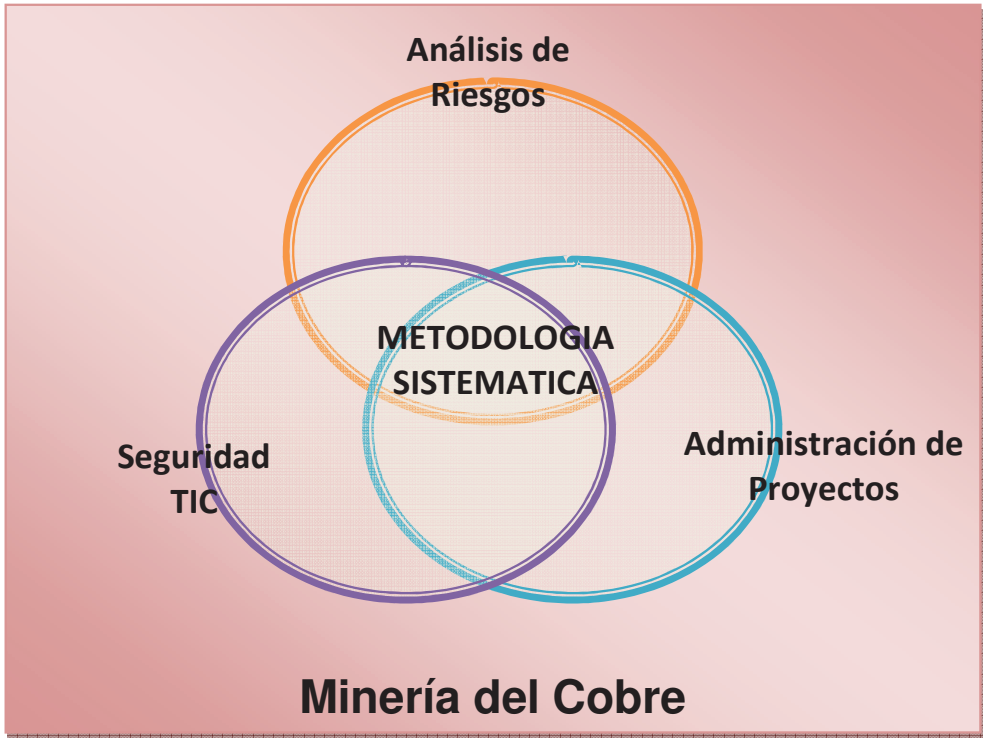


**Figura 5. 1:** Modelo de la Metodología Sistemática para la Administración de Riesgos (Elaboración propia)

Como se puede observar en la figura 5.1, la metodología rescata tres grandes áreas de estudio. Principalmente se utilizarán los conceptos de administración de riesgos abarcados en donde se emplearán las herramientas entregadas para un análisis de riesgo íntegro y robusto. También se utilizará la seguridad en las tecnologías de la información, dado que el enfoque de esta investigación va dirigido a los proyectos del ámbito informático.

Y la guía de las mejoras prácticas de la administración de riesgo, dentro del marco de la administración de proyectos, se facilita a través de los procesos obtenidos del PMBOK. Todo lo anterior bajo el contexto de la industria minera del cobre, la cual se nutre a partir de la experiencia del alumno autor.

## 5.1 Introducción

Dentro de un proyecto de cualquier índole, los riesgos representan barreras que la administración debe superar para satisfacer los objetivos del proyecto. Estas barreras otorgan resistencia al progreso del proyecto impidiendo su avance, especialmente si son de gran envergadura y que pueden detener o cancelar el proyecto en acción. Como se muestra en la figura 5.2, la administración del riesgo otorga confianza al desarrollo del proyecto al estar preparado para acontecimientos que representan resistencia al avance de las actividades. Esta confianza se genera por medio de tareas mitigadoras y preventivas de riesgos, a modo de obtener un control sobre los acontecimientos que pueden impactar el proyecto. Lo cual permite progresar al proyecto sin detenciones innecesarias para su crecimiento.

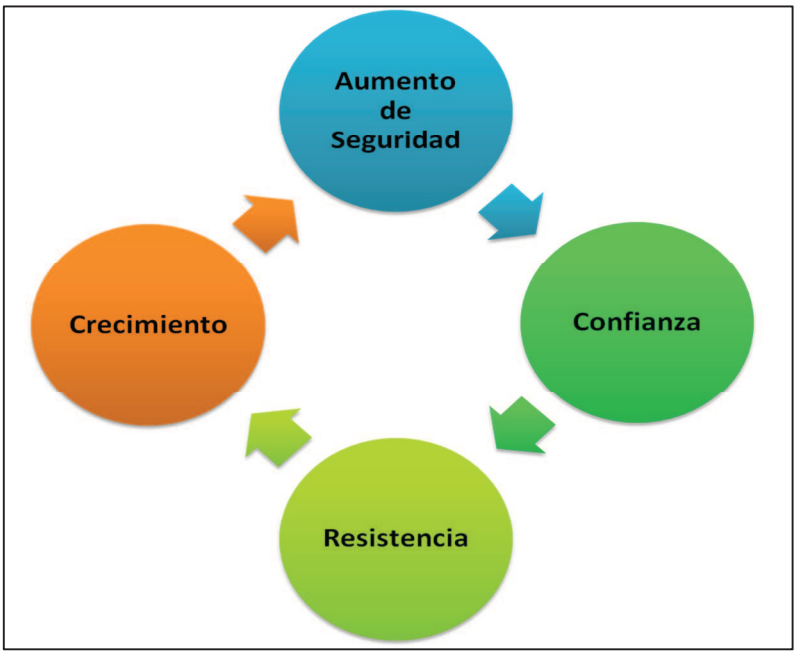


**Figura 5. 2:** Esquema Buena Administración de Riesgos
(Elaboración propia)

Dado que la administración de riesgo debe mantenerse continúa durante el desarrollo de un proyecto, el aumento de seguridad también debe ser constante. En caso contrario, el proyecto puede sufrir repercusiones ya sea al inicio, en la implementación y al cierre del proyecto a causa de riesgos que cambiaron de características en el tiempo. Esto es válido considerando que el ambiente minero está sujeto a fuertes cambios mundiales, tanto económicos, industriales, como de suministros.

La metodología que se está planteando, proporciona una herramienta sistemática que habilita el análisis de los riesgos que rodean un proyecto para que la toma de decisiones sea más informada y efectiva, dejando poco espacio para errores por falta de entendimiento. Esta metodología será utilizada a lo largo de toda la administración de riesgo, la cual al mismo tiempo prevalece a lo largo del ciclo de vida de un proyecto (Ver figura 5.3).


**Figura 5. 3:** Presencia de la administración de riesgos en la vida de un proyecto (Elaboración propia).

Considerando que la administración de riesgos consiste en cuatro grandes etapas, como las indicadas en la figura 5.4, se puede entender que la base de una buena administración de riesgo es una planificación sólida. Esta debe abarcar la estrategia con la se trabajará para tratar los riegos a lo largo de un proyecto, definiendo los activos que se estarán supervisando para que no sufran cambios indeseados, los tiempos en los que se reevaluarán, el equipo capacitado y multidisciplinario que estará a cargo de ellos y el alcance de los riesgos en la administración en el proyecto.

Ahora entra un actor al modelo propuesto, la persona que estará a cargo de realizar los trabajos y actividades relacionadas a la administración de cambios, el encargado de riesgos. Esta persona, asignada en la etapa de planificación, tendrá como responsabilidad asegurar que todos los interesados expresen sus aportes, mediante entrevistas y reuniones personales, en donde se discuta desde la identificación de los riesgos hasta su evaluación final. Seguidamente se trabaja en la identificación de los riesgos que amenazan el proyecto, utilizando como herramienta la lluvia de ideas entre todos los interesados del proyecto.

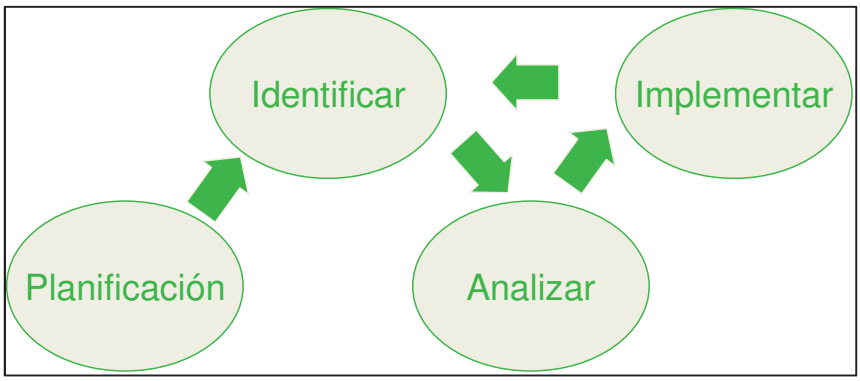


**Figura 5. 4:** Modelo de administración de riesgos (Elaboración propia).

Lo importante de esta fase no es sólo la identificación del riesgo, sino que el activo al que amenaza, dado que se trabajará sobre él en la metodología sistemática. En este momento, se comienza el ciclo continuo en la administración del riesgo, ya que las etapas se reiteran con el fin de mitigar o prevenir el riesgo residual del proyecto.

Posteriormente viene la epata de análisis e implementación, las cuales tiene como fin entregar una evaluación de los riesgos, vulnerabilidades, amenazas y el plan de respuesta a ejecutar. La implementación considera la realización de los controles acordados, ya sean mitigadores o preventivos. No se dará relevancia a la clasificación de los controles del plan de respuesta, dado que el enfoque buscado difiere de lo teórico acercándose a lo práctico de los controles.

A continuación se explica la metodología sistemática planteada, y posteriormente se hará un caso de estudio implementando esta metodología de análisis de riesgos.

## 5.2 Metodología sistemática de análisis de riesgos de proyectos

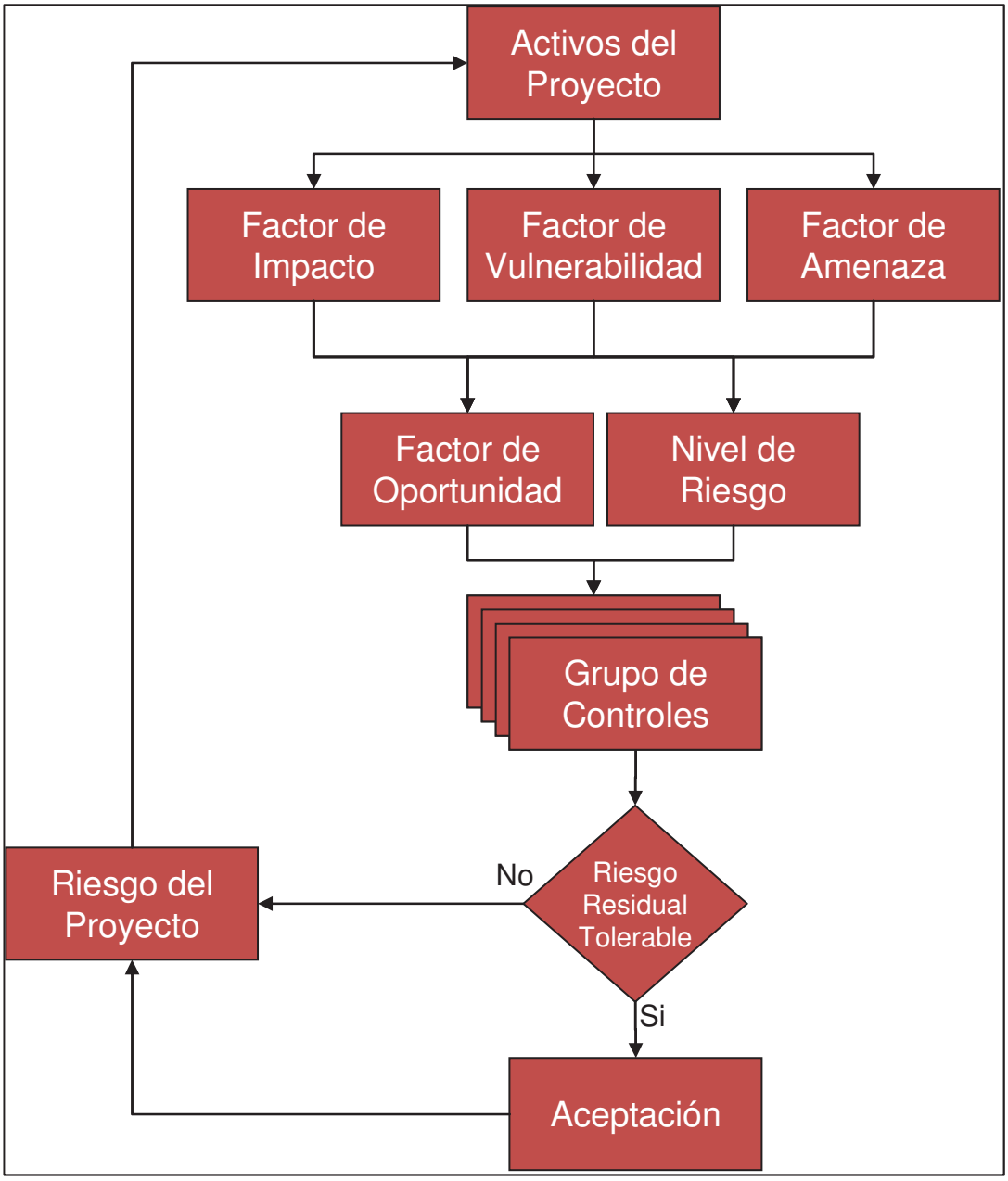


**Figura 5. 5:** Metodología sistemática de análisis de riesgos de proyecto (Elaboración propia)

Esta metodología está enfocada en la medición del impacto en la planificación de un proyecto, generado por los distintos riesgos que afectan a sus activos y que inhiben la capacidad de trabajo continuo del proyecto.

### 5.2.1 Descripción de la metodología

Para evaluar los riesgos en un proyecto TI-Minero se necesita una metodología ágil y concreta que dé a conocer los riesgos a los que está expuesto un proyecto dentro de la organización, y cómo la aplicación de controles pueden mitigar el impacto del riesgo, siempre y cuando estos controles no sobrepasen la barrera costo/beneficio para la organización, y por supuesto que la tolerancia al riesgo de la organización este sobre los valores resultantes. A continuación se detallan los pasos en el proceso de análisis de riesgos planteado en el proyecto de memoria.

Para entender la metodología planteada se debe definir previamente lo siguiente:

**a) Metodología**

- **Parámetros**
  - Dimensiones
  - Factor de impacto
  - Factor de vulnerabilidad
  - Factor de Amenaza
  - Período de evaluación
  - Activos

- **Diccionario**
  - Vulnerabilidades
  - Amenazas
  - Controles

**b) Modelo BPMN de los procesos de análisis de riesgos**

#### A. Metodología

#### 1. Parámetros

Antes de realizar el análisis de riesgos se necesitan definir todos los parámetros que serán utilizados en el análisis, éstos son la referencia clave para concretar la base del análisis de riesgos, como se muestra en la figura 5.6.

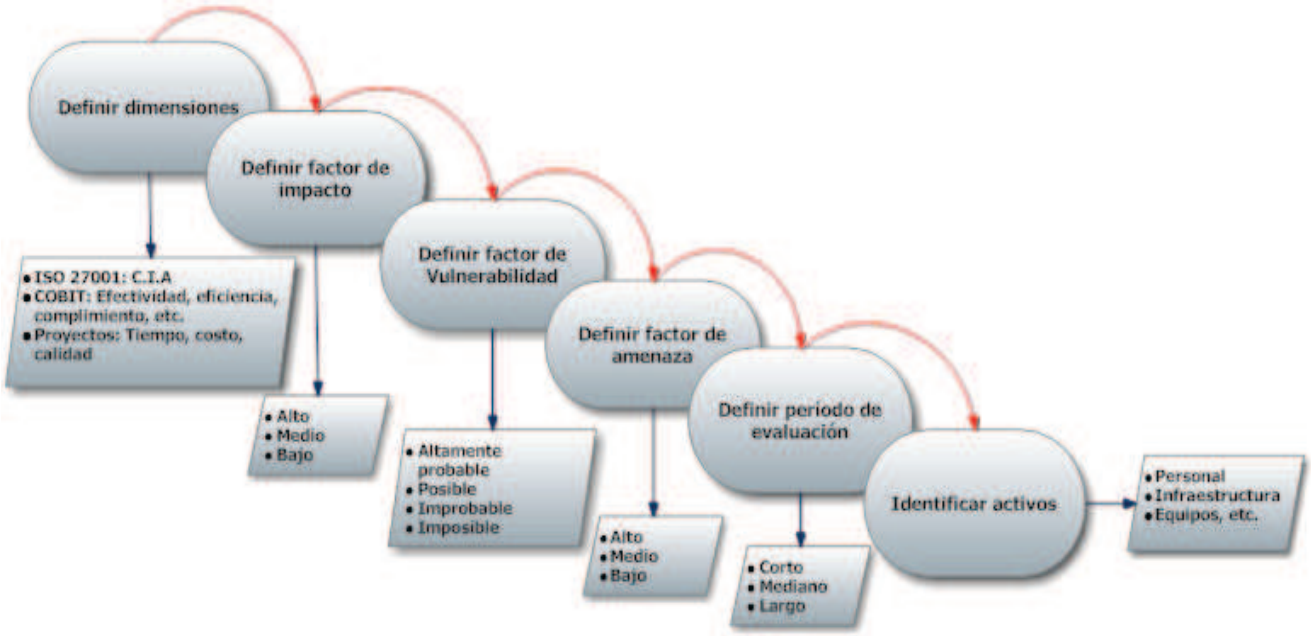


**Figura 5. 6:** Metodología de evaluación (Elaboración propia).

A continuación se detallan cada uno de los parámetros mencionados anteriormente:

## 1.1 Dimensiones

Los ejes de impacto toman un rol importante a la hora de realizar un análisis de riesgos, estos definen el valor de impacto de los riesgos en una clasificación definida.

Como se mencionó anteriormente (Punto 4.3) Basándose en la norma ISO 27001, en seguridad de la información, los ejes de impacto son: Integridad, confidencialidad y disponibilidad.

COBIT en base a sus criterios de información, plantea los siguientes ejes: Efectividad, eficiencia, confidencialidad, integridad, disponibilidad, cumplimiento y confiabilidad.

La industria hace hincapié en los ejes de HSE, financieros, reputación, etc.

Y por último, y en relación al caso de estudio, los proyectos agregan tres ejes importantes, que son: Tiempo, Costo y Calidad.

Distintos ejes para realizar una evaluación de riesgos, que dependerán de la organización cuál de ellos elegir, pero un gran paso en este ámbito sería mantener constantes los ejes definidos, y así crear una estandarización para la gestión de riesgos.

### 1.2 Factor de impacto

Este factor determina que tan importante es el activo dentro de la organización y cuál sería el impacto potencial si es que el activo fuera afectado.

### 1.3 Factor de vulnerabilidad

Vulnerabilidad se define como la debilidad de un sistema que puede ser *explotado para violar su integridad y/o funcionamiento, este factor determina la* probabilidad de ocurrencia en el tiempo de que una debilidad en el proyecto permita a una amenaza materializarse.

### 1.4 Factor de amenaza

Una amenaza es todo evento con el potencial para causar daño a un activo organizacional, este factor define la probabilidad que la amenaza se materialice explotando una vulnerabilidad.

### 1.5 Período de evaluación

El periodo de evaluación influye fuertemente en el análisis de riesgos, ya que un impacto no tiene la misma criticidad para distintos periodos de evaluación, en esta parte del proceso, se debe definir qué es corto, mediano o largo plaza para el proyecto.

### 1.6 Activos

Es preciso identificar todos los activos implicados en el desarrollo del proyecto, para cada activo se deben identificar las posibles amenazas, sus vulnerabilidades, factores de riesgo y controles correspondientes. Algunos activos pueden ser: Personas, infraestructura, sitios, etc.

## 2. Diccionario

El diccionario es una base de datos, información estructurada o no estructura, que cuenta con las vulnerabilidades, amenazas y controles que se van a usar en el análisis de riesgos del proyecto (Ver figura 5.7). Esta base de datos se define antes de iniciar el análisis, y puede alimentarse de nuevos datos mientras el análisis esté en ejecución.

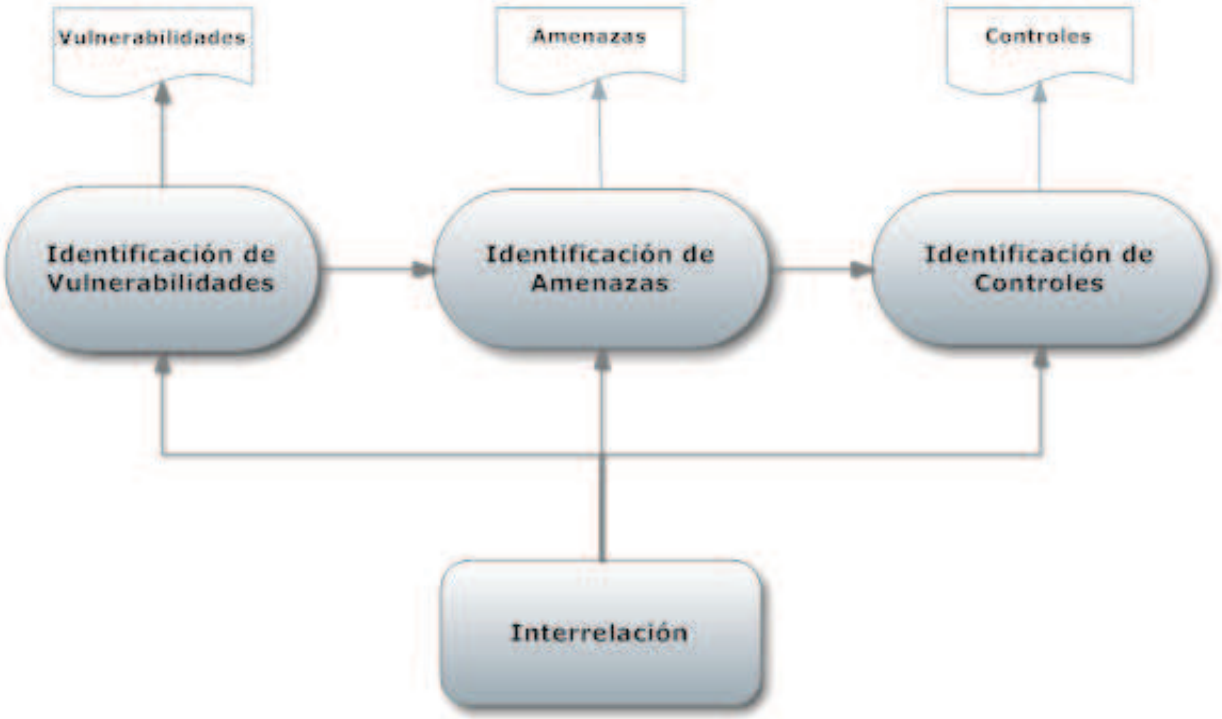


**Figura 5. 7:** Diccionario de datos (Elaboración propia)

La interrelación que existe entre estos tres procesos, se refiere a que la identificación de vulnerabilidades determina qué tipo de amenazas pueden materializarse, como también la cantidad de estas, por consiguiente, dado que las amenazas al encontrar una vulnerabilidad pueden crear un riesgo, se necesitan controles que puedan mitigar el impacto de estos riesgos. A continuación en la figura 5.8 se muestra cómo la norma ISO 27001 en su catálogo de Vulnerabilidades, Amenazas y controles, muestra la relación entre estas.

| | Vulnerabilidade | Amenaza (T no.) | Salvaguarda (S no.) | Control 27001 Anexo A |
|---|---|---|---|---|
| **Personal** | | | | |
| 2.4 | Excesiva autoridad/control | 5.4-5.5<br>5.8<br>5.10<br>5.15<br>5.22<br>5.24<br>5.27<br>5.29-5.31<br>5.34<br>5.42<br>6.12-6.13<br>6.16<br>7.1-7.3<br>7.22 | 2.5<br>2.7<br>2.8<br>2.30<br>2.32<br>2.38<br>2.63 | A.6.1.1<br>A.6.1.3<br>A.6.1.3<br>A.6.2.1<br>A.8.1.1<br>A.8.1.3<br>A.10.1.3<br>A.10.9.1<br>A.10.8.5<br>A.11.2.1<br>A.11.2.2<br>A.11.2.4 |
| 2.5 | Falta de conciencia de seguridad | 3.5<br>3.10<br>4.6-4.7<br>5.9 | 2.23<br>2.41<br>3.2<br>3.5 | A.5.1.1<br>A.7.1.2<br>A.7.1.3<br>A.5.1.2 |

**Figura 5. 8:** Ejemplo Catálogo VAC ISO 27001 (Elaboración propia).

## 2.1 Identificación de vulnerabilidades

Se deben identificar todas las vulnerabilidades del proyecto y crear una lista ordenada por ID de la forma V.1, V.2, etc., estas serán agregadas al diccionario para luego realizar el análisis de riesgos en cualquier proyecto, cabe destacar que esta lista es dinámica, ya que a medida que avanza el análisis, nuevas vulnerabilidades pueden ser agregadas a la base de datos. Un ejemplo de vulnerabilidad es, “Monitoreo insuficiente de medidas de seguridad para el medioambiente e infraestructura”.

## 2.2 Identificación de amenazas

Todas aquellas posibles amenazas que puedan causar un riesgo en el proyecto, deben ser identificadas en una lista ordenada por ID de la forma A.1, A.2, etc., esta lista de amenazas puede ser modificada en cualquier momento de la ejecución del análisis de riesgos, agregando datos nuevos a la lista. Un ejemplo de amenaza puede ser, “Subidas de voltaje / fluctuaciones”.

## 2.3 Controles

Preventivos o mitigadores, los controles son parte de los activos de los procesos de la organización, es decir, son controles ya absorbidos y de uso como respuesta a las evaluaciones de riesgos (Preventivos, para reducir la probabilidad de ocurrencia), así como también en eventos de riesgos (Mitigadores, para limitar el impacto).

PMBOK plantea un plan de respuesta al riesgo para evitar, transferir, mitigar o aceptar el riesgo, como una estrategia de respuesta. La metodología planteada se alinea con el PMBOK en base a que los controles tienen la característica de ser preventivos (Evitar y/o transferir el riesgo), o mitigadores (Mitigar el riesgo).

Por ejemplo, un control puede ser la contratación de un seguro para los daños que pudieran ocurrir de un determinado riesgo, en este caso el control pasa a ser una estrategia de respuesta, como parte del plan de respuesta a los riesgos.

Establecido el alineamiento entre estos tópicos, es importante destacar que el objetivo principal de los controles es reducir los niveles de riesgo y así puedan ser aceptables o tolerables para la organización. Estos controles actúan como barreras protectoras, tal como se muestra en la figura 5.9.

Generalmente los controles no se realizan aisladamente, sino que se llevan a cabo por grupos, dependiendo de los riesgos que se quieren mitigar. Esto facilita la evaluación de los distintos grupos de controles por implementar, y la elección del grupo de controles adecuado.

Por ejemplo, si se desea mitigar el riesgo de una tarea peligrosa, el grupo de controles que aplicarían sería la capacitación del personal que efectuará la tarea; la creación de procedimientos previos que apliquen, durante y al fin de la actividad; la adquisición de elementos de protección personal necesaria para

resguardar la seguridad del personal involucrado; y por último la ejecución de una evaluación ambiental de las condiciones óptimas para realizar la labor.

Con esto, se vuelve a realizar el análisis de riesgo considerando la efectividad de estos controles, para que en esta oportunidad las vulnerabilidades aparezcan con un factor menor, de igual modo con las amenazas. Este análisis se realiza las veces que sean necesarias para obtener el nivel de riesgo deseado. La gran ventaja de este análisis, es que permite la implementación de los controles necesarios, permitiendo ofrecer a los interesados del proyecto una cobertura precisa ante sus necesidades.

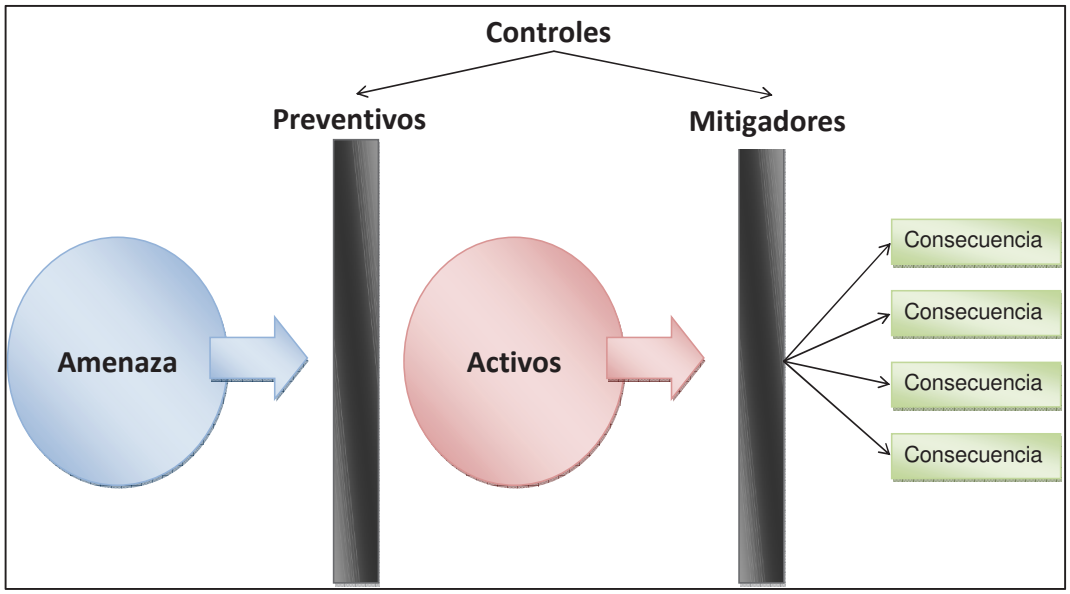


**Figura 5. 9:** Evaluación de controles (Elaboración propia).

## B. Modelo BPMN del proceso de análisis de riesgos

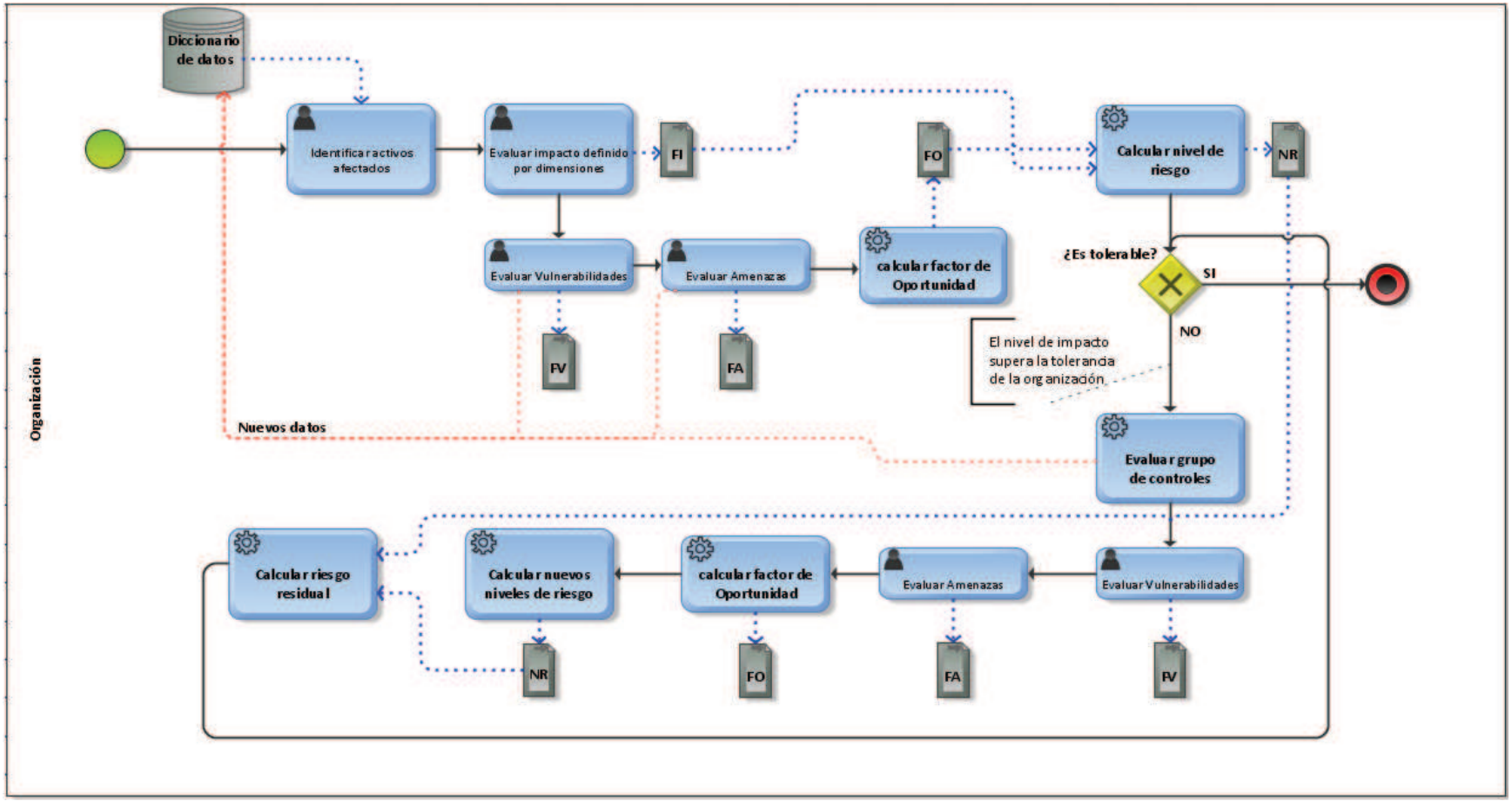


**Figura 5. 10:** Modelo BPMN Proceso Análisis de Riesgos (Elaboración propia)

## 5.3 Planilla de la metodología sistemática para el análisis de riesgos

IDENTIFICADOR ____ FACILITADOR _____ FECHA _____
PROYECTO_____RIESGO _____

| Activo | IMPACTO | | | | VULNERAB. | | AMENAZA | | Factor Oportunidad | Nivel de Riesgo | CONTROLES | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Disponibilidad | Integridad | Confiabilidad | Factor Impacto (FI) | Vulnerabilidad | Factor Vulnerabilidad (FV) | Amenaza | Factor Amenaza (FA) | | | Grupos Mitigadores | | Vulnerabilidad | FV | Amenaza | FA | Factor Oportunidad | Nivel de Riesgo |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |
| | | | | | | | | | | | | | | | | | | |

**Figura 5. 11:** Planilla de la metodología sistemática para el análisis de riesgos (Elaboración propia)

## 5.4 Caso de estudio

### 5.4.1 Introducción

Debido a las continuas amenazas que están expuestas las organizaciones, los métodos de evaluación de riesgos juegan un papel importante en el aseguramiento del trabajo continuo, no en su totalidad para prevenir, pero sí en estar preparados para actuar en el momento oportuno, así como también saber donde enfocar los recursos necesarios, esto permite tener una visión general de cuáles son los riesgos que la organización puede mitigar, y cuáles estarán dentro de sus niveles de aceptación.

En relación a los proyectos TI-Mineros pasa exactamente lo mismo, éstos se ven expuestos a amenazas que pueden causar desde un aplazamiento en la entrega hasta la cancelación del proyecto.

Tomando como referencia todos métodos expuestos, se pasa a detallar el caso de estudio que expondrá la utilización de la evaluación de los riesgos, amenazas y vulnerabilidades presentes en una organización.

### 5.4.2 Descripción del caso de estudio

El caso de estudio se ha centrado en una de las principales empresas mineras de la zona norte del país, cuya principal actividad es la extracción de cobre.

De su organigrama se extrae que, el departamento de informática -que es donde se ha centrado este estudio- reporta directamente al departamento de finanzas y este a su vez a la presidencia de la compañía.

Los proyectos TIC permiten optimizar los procesos de producción que son claves para la compañía, implementando, por ejemplo, sistemas de comunicación, sistemas de apoyo al control de las operaciones, etc., los cuales son indispensables en el proceso productivo de la compañía, pero se debe tener en cuenta que si llegasen a fallar, el proceso productivo de extracción de material, así como también el proceso de movimiento de tierra se deben detener por completo, esto se hace para proteger la seguridad de las personas que pasa a ser la primera prioridad en toda la organización. Todas estas consideraciones se enmarcan en el cumplimiento de las normas que dicta el SERNAGEOMIN.

Hoy en la administración de riesgos de la gerencia de tecnología y sistemas de información no existe una metodología sistemática para realizar las

evaluaciones del impacto de los servicios de TI, ya sean estos por modificación en la plataforma o la incorporación de nuevas componentes, es por ello que se diseñó el siguiente proceso.

#### 5.4.2.1 Descripción del proyecto

A raíz de la implementación de diversos proyectos, se han identificado requerimientos que tienen relación con la instalación de nuevos circuitos eléctricos o el consumo de energía para circuitos eléctricos en torno a las instalaciones existentes y, como consecuencia de estos, se requiere intervenir tableros de distribución así como también agregar cargas adicionales.

Los objetivos de este proyecto son:

Realizar levantamiento de sistema de distribución eléctrico con y sin respaldo UPS de la sala de servidores y con ello tener información actualizada sobre el estado de estos, capacidades y posibilidades de crecimiento futuro. La duración estimada para este proyecto es de 3 meses.

### 5.4.3 Aplicación del método de análisis de riesgos

A continuación se detalla el proceso de análisis de riesgos basado en la metodología planteada.

#### A. Identificación de activos

Como primer paso en la metodología, se necesitan identificar los activos que se verán afectados en el proyecto y que requieren de una evaluación de riesgos (Ver figura 5.12).

En este proyecto, se identificaron los siguientes activos.

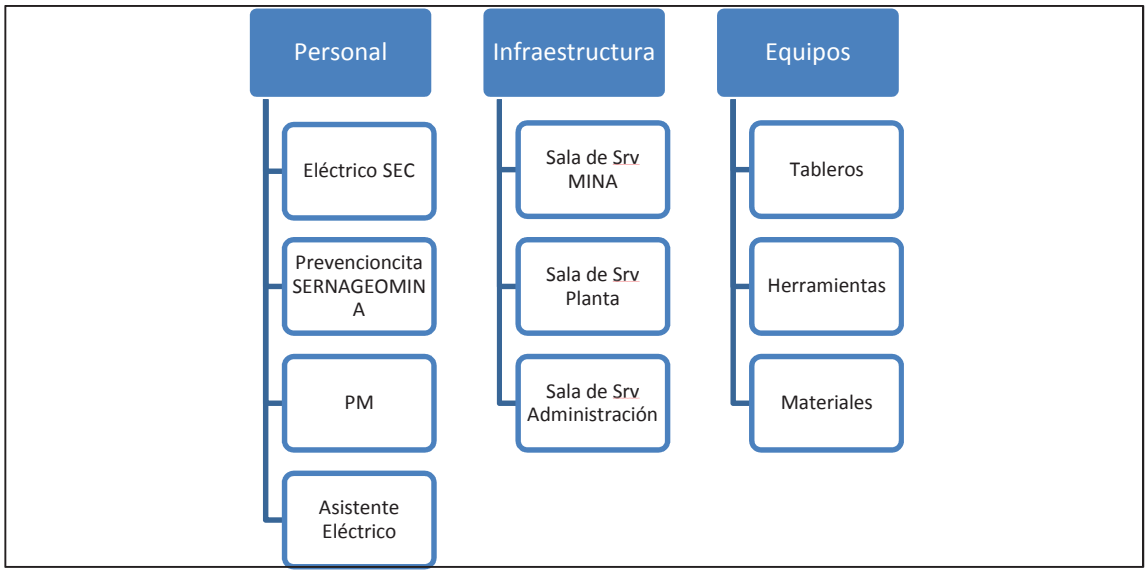


**Figura 5. 12:** Activos identificados en el proyecto (Elaboración propia).

Una vez identificados los activos, es necesario evaluar su factor de impacto basado en las dimensiones mencionadas anteriormente.

Para este proyecto las dimensiones establecidas son:

- Tiempo
- Costo
- Legal
- HSE

## B. Evaluar factor de impacto

En primer lugar, el factor de impacto se pondera de la siguiente manera, mostrado en la tabla V.1:

| FACTOR IMPACTO (FI) | |
|---|---|
| Alto | 3 |
| Medio | 2 |
| Bajo | 1 |

**Tabla V. 1:** Ponderación del factor de impacto (Elaboración propia).

A modo de ejemplo se muestra la evaluación del factor de impacto de los activos clasificados en personal. Y posteriormente se realizarán las siguientes evaluaciones con el activo “Eléctrico SEC”.

Como bien se mencionó anteriormente, el factor de impacto dirá cuanto le afecta al proyecto, en las distintas dimensiones, la usencia del activo.

El factor de impacto se calcula mediante la suma de todos los valores asignados en las distintas dimensiones (Ver figura 5.13)

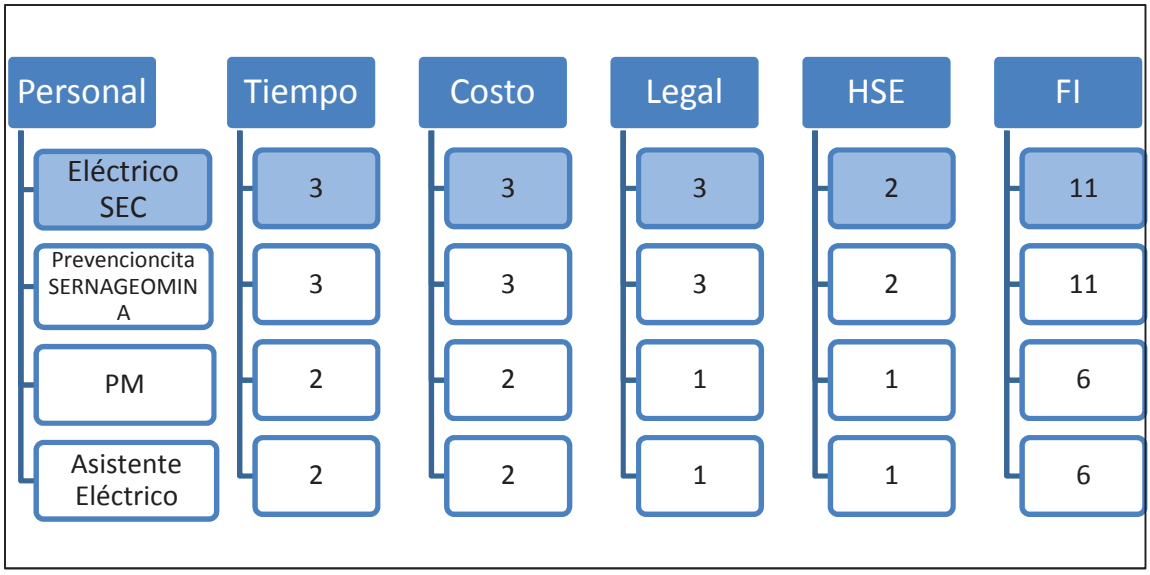


**Figura 5. 13:** Evaluación del factor de impacto (Elaboración propia).

## C. Evaluar factor de vulnerabilidad

Una vez determinado el valor de impacto, es necesario identificar las vulnerabilidades propias del activo seleccionado. Para luego determinar su factor de vulnerabilidad, que permitirá evidenciar que tan probable es que el activo sea afectado por alguna amenaza.

El factor de vulnerabilidad se pondera de la siguiente manera, mostrado en la tabla V.2:

| FACTOR VULNERABILIDAD (FV) | |
|---|---|
| Altamente Probable | 4 |
| Posible | 3 |
| Improbable | 2 |
| Imposible | 1 |

**Tabla V. 2:** Ponderación del factor de vulnerabilidad (Elaboración propia).

Las vulnerabilidades identificadas, con su respectivo factor de vulnerabilidad se muestran a continuación en la figura 5.14.

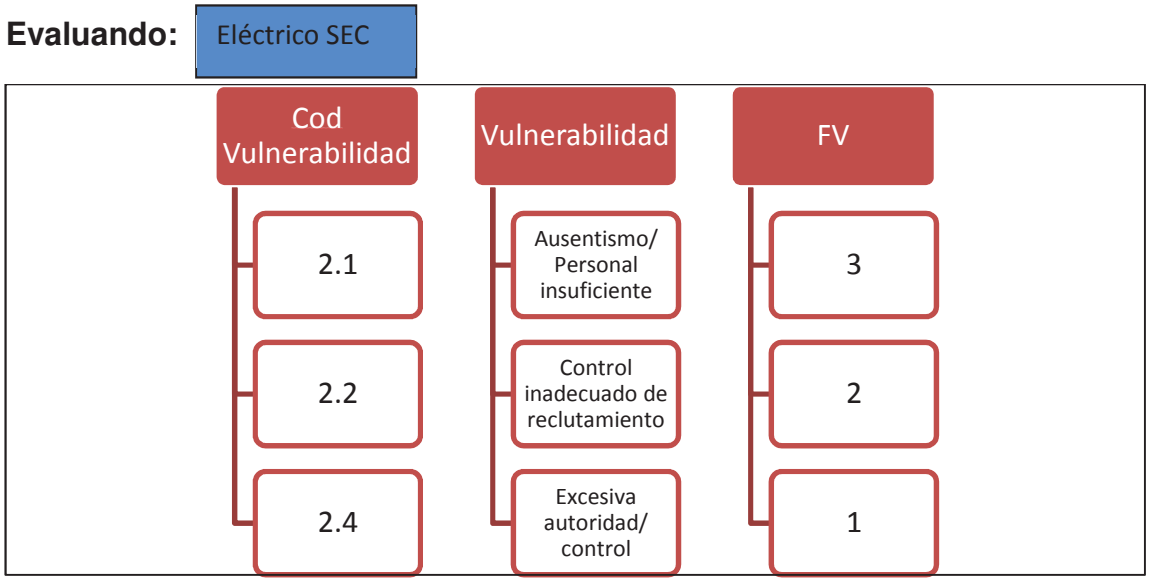


**Figura 5. 14:** Evaluación del factor de vulnerabilidad (Elaboración propia)

Al igual que en la evaluación del factor de impacto, a modo de ejemplo, se seleccionará una vulnerabilidad para continuar con la evaluación.

## D. Evaluar factor de amenaza

La evaluación de riesgos continúa con la evaluación del factor de amenaza, este factor se pondera de la siguiente manera, mostrado en la tabla V.3:

| FACTOR AMENAZA (FA) | |
|---|---|
| Alto | 3 |
| Medio | 2 |
| Bajo | 1 |

**Tabla V. 3:** Ponderación del factor de vulnerabilidad (Elaboración propia)

Una vez identificadas las vulnerabilidades, se deben identificar las amenazas que las podrían afectar y gatillar un riesgo.
Las amenazas identificadas, con su respectivo factor de amenaza se muestran a continuación en la figura 5.15.

**Evaluando:** Eléctrico SEC

Ausentismo/Personal insuficiente

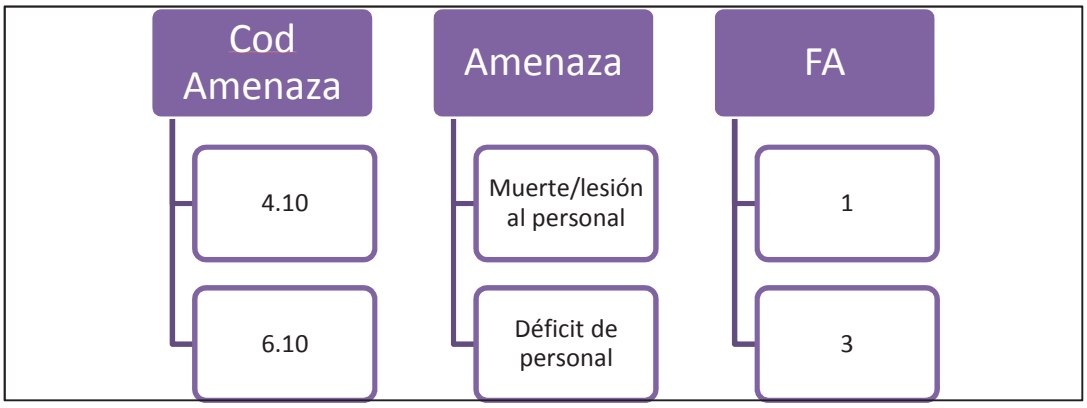


**Figura 5. 15:** Evaluación del factor de vulnerabilidad (Elaboración propia)

## E. Calcular el nivel de riesgo

Una vez determinados, el factor de impacto, factor de vulnerabilidad y factor de amenaza, es necesario calcular el nivel de riesgo.

El nivel de riesgo se calcula según las siguientes fórmulas mostradas en la figura 5.16:

$$NR = FI * \mathrm{FO}$$
$$FO = FV * \mathrm{FA}$$

**Figura 5. 16:** Fórmulas para el cálculo del nivel de riesgo (Elaboración propia)

Por lo tanto, para el caso descrito, y evaluando las dos amenazas identificadas anteriormente, los valores son los siguientes (Ver figura 5.17).

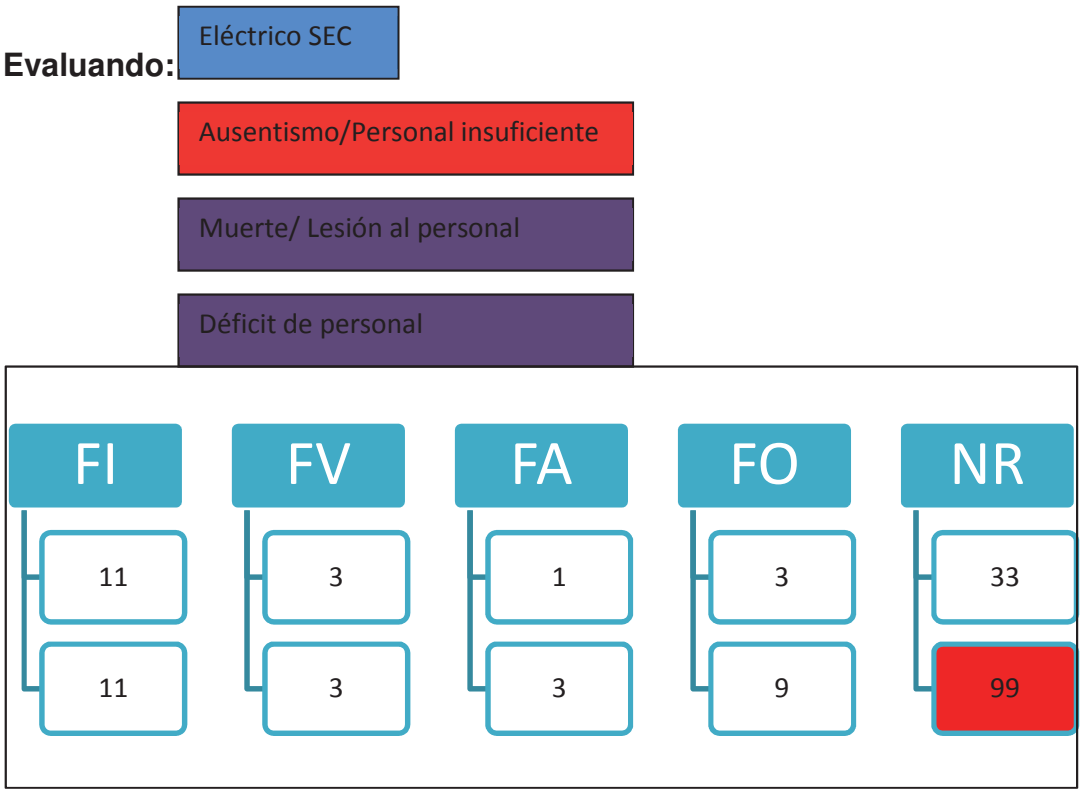


**Figura 5. 17:** Evaluación del factor de vulnerabilidad (Elaboración propia).

Como se puede ver, la amenaza “Déficit de personal” tiene el nivel de riesgo más alto, ahora ¿Cómo sabemos qué nivel de riesgo puede tolerar la organización? Este nivel de tolerancia se debe definir previo al análisis de riesgo a nivel de Governance, para este caso el nivel de tolerancia aceptable se definió como el 50% del nivel de riesgo máximo.

Como el nivel de riesgo máximo que puede obtener algún componente de la evaluación es 144, el Nivel de riesgo aceptable será 72.

En este caso, la amenaza “Déficit de personal” obtuvo un nivel de riesgo igual a 99, por lo tanto está sobre el nivel de tolerancia de la organización y se debe implementar un plan de respuesta al riesgo de “Ausencia del eléctrico SEC por déficit de personal”.

## F. Evaluar el plan de respuesta al riesgo

Para hacer frente a un riesgo, la metodología plantea un plan de respuesta basado en grupos de controles dispuestos a mitigar el riesgo, para esto se deben seleccionar los controles pertinentes y aplicables al riesgo y volver a evaluar los factores de vulnerabilidad y amenaza. Por lo tanto se obtendrá un nuevo nivel de riesgo, que puede ser mayor, en caso de que un control genere un nuevo riesgo, menor, si es que el grupo de controles ayudó en la mitigación del nivel de riesgo, o igual, en caso que el grupo de controles no funcionara.

A continuación en la figura 5.18 se muestran dos grupos de controles aplicables para mitigar el impacto del riesgo presentado.

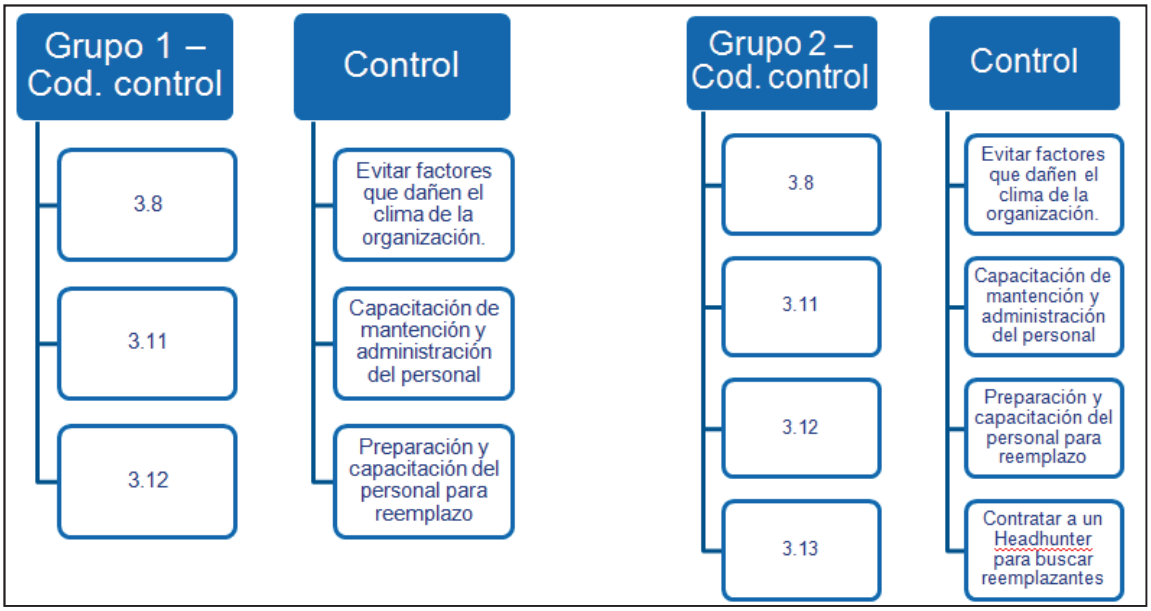


**Figura 5. 18:** Grupo de controles aplicables (Elaboración propia).

Estos controles están orientados a disminuir el impacto del riesgo y su manera de evaluar su eficacia es materia de un estudio posterior, es por esto que la metodología planteada es un modelo vivo, no exento de modificaciones en un futuro.

A continuación y como parte final del caso de estudio en la figura 5.19 se muestra la matriz de evaluación, con todos sus valores de riesgo, al igual que el plan de respuesta aplicado.

### 5.4.4 Resultado de análisis

| Evaluación | | | | | | | | | | | | Plan de Respuesta | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| (B) | Tiempo | Costo | Legal | HSE | FI | V | FV | A | FA | FO | NR | Grupo Control | | V | FV | A | FA | FO | NR |
| Eléctrico SEC | 3 | 3 | 3 | 2 | 11 | V2.1 | 3 | A4.10 | 1 | 3 | 33 | | | | | | | | |
| | | | | | | | | A6.10 | 3 | 9 | 99 | G1 | C3.8, C3.11, C3.12 | V2.2 | 2 | A6.2 | 2 | 4 | 44 |
| | | | | | | | | | | | | | | | | A6.16 | 2 | 4 | 44 |
| | | | | | | | | | | | | | | V2.15 | 2 | A5.16 | 2 | 4 | 44 |
| | | | | | | | | | | | | | | | | A6.2 | 2 | 4 | 44 |
| | | | | | | | | | | | | G2 | C3.8, C3.11, C3.12, C3.13 | V2.2 | 2 | A6.2 | 2 | 4 | 44 |
| | | | | | | | | | | | | | | | | A6.16 | 1 | 2 | 22 |
| | | | | | | | | | | | | | | V2.15 | 2 | A5.16 | 2 | 4 | 44 |
| | | | | | | | | | | | | | | | | A6.2 | 2 | 4 | 44 |
| | | | | | | | | | | | | | | | | A7.1 | 1 | 2 | 22 |
| | | | | | | | | | | | | | | V2.17 | 3 | A6.10 | 2 | 6 | 66 |
| | | | | | | V2.2 | 2 | A6.2 | 2 | 4 | 44 | | | | | | | | |
| | | | | | | | | A6.16 | 1 | 2 | 22 | | | | | | | | |
| | | | | | | | | A6.21 | 2 | 4 | 44 | | | | | | | | |
| | | | | | | V2.4 | 1 | A6.16 | 1 | 1 | 11 | | | | | | | | |
| | | | | | | | | A7.1 | 1 | 1 | 11 | | | | | | | | |
| | | | | | | V2.9 | 2 | A4.10 | 1 | 2 | 22 | | | | | | | | |

**Figura 5. 19:** Aplicación del modelo de análisis de riesgos (Elaboración propia)

### 5.4.5 Conclusiones

Una vez terminada la evaluación de riesgos del proyecto se puede concluir lo siguiente:

Todo proyecto nunca está exento de riesgos, ya sea en el grupo de procesos de iniciación, planificación, ejecución, y mucho menos en los grupos de seguimiento y control y finalmente el cierre, sin importar el tipo, dificultad o duración, un proyecto puede ser amenazado constantemente por riesgos que inhabilitan su capacidad de operación continua y cumplimiento de objetivos.

El análisis de riesgos expuesto plantea, en base a un análisis cualitativo llegar a una forma cuantitativa de evaluación de riesgos, se hace de esta forma porque, en una búsqueda a fuentes formales de información en Chile no se encontraron medidas cuantitativas que se puedan aplicar a una evaluación de riesgos.

Los valores de medición existentes corresponden a valores extranjeros, que si se llevan a la realidad chilena podrían no ser aplicables, por factores como política, estándares, factores medioambientales, etc., estos valores se crean con historia, o sea, una documentación detallada a través del tiempo, de mediciones, valores y acciones tomadas en eventos de riesgos pasados, y hoy en Chile no se cuenta con este tipo de documentación.

Por otra parte, dentro de la metodología de trabajo, se puede definir que los métodos de evaluación de riesgos permiten visualizar y estar preparados ante cualquier amenaza que pudiera materializarse sin importar la etapa de un proyecto TI-Minero, como por ejemplo, los cambios de alcance que se pudieran identificar debido a un evento fortuito.

Pero los métodos de evaluación de riesgos partiendo desde la iniciación hasta los controles de monitoreo, que fueron presentados y probados en esta memoria, no se limitan a un área específica sin poder extrapolar sus métodos de evaluación, si no por el contrario, pueden adaptarse fácilmente a cualquier otra área operativa, incluso a otras funciones, de la compañía.

La forma de adaptar el modelo a otras áreas es sencilla, esta adaptación se hace mediante la modificación del modelo de tabulación en las tablas de Periodo de evaluación y Activos, se debe definir nuevamente el tiempo para corto, mediano y largo plazo, además se deben identificar los nuevos activos a evaluar.

El factor de exposición, vulnerabilidad y amenaza no tendrán el mismo valor para proyectos de otras áreas que se ven afectadas por otros riesgos, –a pesar de que muchos de ellos son riesgos que existen en común para cualquier proyecto, sea cual sea su área específica– pero la tabulación no sufre modificación, solo el valor del factor.

Por otra parte el diccionario de datos crece con cada evaluación, por lo tanto frente a un cambio de área, muchos de los riesgos relevantes ya estarán identificados, en conclusión, el proceso de evaluación sigue siendo el mismo, y completamente adaptable a cualquier área de la compañía.

# Capítulo VI

# Conclusiones

Este documento tiene como base una exhaustiva investigación sobre diferentes temáticas relativas a la administración de riesgos. Esta sirvió de base para contextualizar la metodología sistemática creada. Se da a relucir este punto, debido a que los conocimientos adquiridos por el alumno autor son primordiales para la línea profesional que se pretende seguir. Por otro lado, es un tema relativamente nuevo, por lo menos dentro de Chile, en donde la mezcla entre las Tecnologías de la Información con la administración de proyectos, proporciona ventajas junto a nuevos horizontes profesionales a optar.

Profesionalmente, la metodología presentada converge sobre varias herramientas y técnicas en la administración de riesgos. Es por esto que se concluye un método congruente y robusto para Proyectos IT enfocados en la Minería del Cobre. De hecho, el método de igual forma puede servir para la administración de riesgo general, especialmente para gerencias de Information Management. La metodología mostrada será utilizada en proyectos que el alumno lleve a cabo en su vida laboral, esperando obtener óptimos resultados en relación al esfuerzo dedicado.

En el ámbito personal, alumno aprendió a realizar una investigación ordenada y de un modo que permitió explayar distintos puntos de vista sobre el mismo tema. Por un lado, la mayor dificultad del trabajo, fue la ejecución de la investigación, dado que los tiempos presupuestados fueron superados por los reales. De esto se aprende que, como en cualquier proyecto, una excelente planificación es la clave para abordar una tarea con éxito. Se pudieron aplicar los conocimientos adquiridos en el Magíster cursado, y plasmarlos en un método elaborado por el alumno.

Los próximos pasos en este tema son la generación e incorporación de la data de vulnerabilidades, amenazas y controles para extrapolar la metodología a las distintas unidades de negocio, y por otra parte, la automatización de esta herramienta, para permitir su facilidad de uso y entendimiento.

Esta metodología deja mucho espacio para crecer, abarcando la automatización en una aplicación informática, o puede ser *customizada* para otros campos laborales. En realidad, la investigación también puede ser profundizada más a fondo, incurriendo en la administración del riesgo como parte de la estrategia de

una organización. Lo importante es recordar que esta metodología fue rescatada de otras herramientas por otros autores, por lo que tiene fundamentos sólidos y por lo mismo, su transformación también los tendrá.

# BIBLIOGRAFÍA


Bakker, K., Boonstra, A., & Wortmann, H. (2009). *Does risk management contribute to IT project success? A meta-analysis of empirical evidence.* ELSEVIER.

CETIUC. (2011). *Reporte semestral de presupuesto TI junio de 2011.* Chile: CETIUC.

Deloitte. (2009). *Global Economic Outlook.* Deloitte.

Deloitte. (2008). *Recognise and manage risk.* Deloitte.

Deloitte. (2009). *Risk Intelligence in a downturn Balancing risk and reward in volatile times.* Deloitte.

Deloitte. (2007). *Risk Intelligence: From theory to practice.* Deloitte.

Deloitte. (2008). *The Risk Intelligent Board.* Deloiite.

Deloitte. (2006). *The Risk Intelligent Enterprise ERM Done Right.* Deloitte.

Deloitte. (2008). *The Risk Intelligent IT Internal Auditor IT IA Takes Flight.* Deloitte.

Deloitte. (2009). *The Risk Intelligent technology company Managing risk to capture value.* Deloitte.

Deloitte. (2009). *Tracking the trends 2009 The top 10 global mining issues.* Deloitte.

Ernst & Young. (2009). *Is risk management broken.* Ernst & Young.

Farah, B. (2011). *A maturity Model for the Management of Information Technology Risk.* USA: Eastern Michigan University.

FERMA. (2003). *Estándares de gerencia de riesgos.* FERMA.

Institute On Governance. (2005). *Information Brief on International Risk Management Standards.* Institute On Governance.

Iranmanesh, H., Nazari Shirkouhi, S., & Skandari, M. R. (2008). *Risk Evaluation of Information Technology Projects Based on Fuzzy Analytic Hierarchal Process.* Waset.

Michael Stewart, J. (2011). *Certified Information Systems Security Professional.* SYBEX.

Peltier, T. (2001). *Information Security Risk Analysis.* Auerbach Publications.

PMI. (2008). *Guía de los fundamentos para la dirección de proyectos* (Cuarta edición ed.). PMI.

Saner, M. (2005). *Information Brief On International Risk Management Standars.*

The Economist. (2008). *Risk 2008 Planning for an unpredictable decade.* The Economist.

World Economic Forum. (2009). *Global Risks 2009 A global Risk Network Report.* WEF.