



**UNAP**



**FACULTAD DE INGENIERÍA DE SISTEMAS E INFORMÁTICA**

**ESCUELA DE FORMACIÓN PROFESIONAL DE INGENIERÍA DE  
SISTEMAS E INFORMÁTICA**

**EXAMEN DE SUFICIENCIA PROFESIONAL**

**TÉCNICAS RECOMENDADAS PARA ANÁLISIS DE RIESGO**

PARA OPTAR EL TÍTULO PROFESIONAL DE  
**INGENIERO DE SISTEMAS E INFORMÁTICA**

Presentado por el Bachiller:

**EDINSON JASON RICARTE MORI MUÑOZ**

**IQUITOS, PERÚ  
2015**


**UNIVERSIDAD NACIONAL DE LA AMAZONIA PERUANA  
FACULTAD DE INGENIERIA DE SISTEMAS E INFORMATICA**
**ACTA DE EXAMEN ORAL DE SUFICIENCIA PROFESIONAL**

Siendo las 9:10 horas del día 26 de Setiembre del 2015, en la Instalación del Auditorio de esta Facultad, se ha constituido el jurado examinador integrado por los siguientes miembros:

Presidente : Eco. Wilson del Águila Panaífo.  
Primer Miembro : Ing. Luis Honorato Pita Astengo  
Segundo Miembro : Ing. Roberto Martín Tuesta Pereyra



Se procedió, al Acto Académico del Examen Oral de Suficiencia Profesional del Bachiller: **Edinson Jason Ricarte Mori Muñoz**, quien sustentó el tema "Técnicas Recomendadas para Análisis de Riesgo", para optar el Título Profesional de Ingeniero de Sistema e Informática, de acuerdo a lo establecido en el Reglamento de Grados y Títulos y sustentado en la Ley N° 30220.

Posteriormente, al Acto de sustentación del informe final del bachiller se procedió al cálculo de Calificación y Condición Final, obteniéndose el siguiente resultado:

	Calificaciones	
	En número	En letras
Promedio de la Calificación Final de las Asignaturas.	<u>14.75</u>	<u>CATORCE y 75/100</u>
Calificación de la Sustentación del Informe Final.	<u>09.73</u>	<u>NUEVE y 73/100</u>
<b>Calificación Final</b>	<u>12.24</u>	<u>DOCE y 24/100</u>

Se desprende que la Condición Final del Bachiller es (marcar el que corresponde):

- ( ) Aprobado con excelencia (18 a 20 puntos).  
 ( ) Aprobado por unanimidad (15 a 17.9 puntos).  
 (  ) Aprobado por mayoría (12 a 14.9 puntos).  
 ( ) Desaprobado (Menos de 12 puntos).

Siendo las 10:20 horas del mismo día, se da por concluido el acto académico, firmando en conformidad los miembros del Jurado Examinador.



Eco. Wilson del Águila Panaífo  
Presidente



Ing. Luis Honorato Pita Astengo  
Primer Miembro



Ing. Roberto Martín Tuesta Pereyra  
Segundo Miembro

## **DEDICATORIA**

**A mi padre y madre, por su apoyo incondicional y amor infinito.**

**A mí querida DORCAS, por estar siempre pendiente de mi seguridad y bienestar, por su apoyo incondicional y amor infinito.**

**A mi hijo LOAM GAEL por ser mi motor y motivo para salir adelante y llegar a cumplir mis metas.**

---

## RESUMEN

### Técnicas recomendadas para el Análisis de Riesgo

Este documento describe algunas técnicas utilizadas en análisis y gestión de riesgos. Se considera técnica a un conjunto de heurísticos y procedimientos que ayudan a alcanzar los objetivos propuestos.

Para cada una de las técnicas referenciadas:

- ✓ Se explica brevemente el objetivo que se persigue al utilizarlas
- ✓ Se describen los elementos básicos asociados,
- ✓ Se exponen los principios fundamentales de elaboración,
- ✓ Se presenta una notación textual y/o gráfica y
- ✓ Y se citan las fuentes bibliográficas que, sin ser exhaustivas, se han estimado de interés para que el lector profundice en cada materia.

(Revisar MAGERIT: Técnicas – Pág. 35 / Uso de tablas para la obtención sencilla de resultados (Pág. 35), Técnicas algorítmicas para la obtención de resultados elaborados (Pág. 36), Árboles de Ataque (Pág. 36), Técnicas Gráficas (Pág. 39))

Todas las técnicas de este ejemplar pueden utilizarse sin ayudas automatizadas; pero su aplicación repetitiva o compleja recomienda el empleo de herramientas tan amplia y frecuentemente como sea posible.

Es importante resaltar que la notación que se propone en la aplicación de la técnica en ningún caso se considerará obligatoria. Cada organización podrá utilizar la notación que desee, la que suele utilizar o la que ofrece sus herramientas de desarrollo, respetando las reglas y restricciones específicas de las distintas técnicas.

### Metodologías para el Análisis de Riesgo

En este capítulo se mencionan algunas metodologías existentes, los cuales nos indican los pasos a seguir para su correcta ejecución, ya que, como hemos visto, suelen ser muy complejos y tienen multitud de variables.

Estas metodologías son:

- CRAMM
- MAGERIT
- OCTAVE

---

## INDICE

<b>ACTA DE SUSTENTACIÓN .....</b>	<b>2</b>
<b>DEDICATORIA .....</b>	<b>3</b>
<b>RESUMEN .....</b>	<b>4</b>
<b>INDICE.....</b>	<b>5</b>
<b>INDICE DE FIGURAS.....</b>	<b>7</b>
<b>INDICE DE TABLAS.....</b>	<b>7</b>
<b>I. JUSTIFICACIÓN.....</b>	<b>8</b>
<b>II. OBJETIVOS.....</b>	<b>9</b>
2.1 OBJETIVO GENERAL.....	9
2.2 OBJETIVOS ESPECIFICOS.....	9
<b>III. DESARROLLO DEL TEMA .....</b>	<b>10</b>
<b>TÉCNICAS RECOMENDADAS PARA EL ANÁLISIS DE RIESGO .....</b>	<b>10</b>
3.1 DEFINICIÓN Y COMPONENTES DEL RIESGO .....	10
3.1.1 <i>Definiciones</i> .....	10
3.1.2 <i>Componentes del riesgo</i> .....	10
3.1.3 <i>Clases de riesgos</i> .....	10
3.2 AMENAZAS Y VULNERABILIDADES .....	11
3.2.1 <i>Amenazas</i> .....	11
3.2.2 <i>Vulnerabilidad</i> .....	12
3.3 MAPA DE RIESGOS.....	15
3.3.1 <i>Definición</i> .....	15
3.3.2 <i>Beneficio</i> .....	15
3.4 NIVELES DE ACEPTACIÓN DEL RIESGO.....	16
3.5 PLAN DE ACCIÓN .....	16
3.6 CONTROL Y MONITOREO DEL RIESGO .....	17
3.7 PLANIFICACIÓN DE LA GESTIÓN DE RIESGOS .....	17
3.7.1 <i>Entradas</i> .....	18
3.7.2 <i>Herramientas y técnicas</i> .....	18
3.7.3 <i>Salidas</i> .....	18
3.8 IDENTIFICACIÓN DE LOS RIESGOS .....	19
3.8.1 <i>Entradas</i> .....	20
3.8.2 <i>Herramientas y técnicas</i> .....	21
3.8.3 <i>Salidas</i> .....	21
3.9 ANÁLISIS CUALITATIVO DE LOS RIESGOS.....	22
3.9.1 <i>Entradas</i> .....	22
3.9.2 <i>Herramientas y técnicas</i> .....	23
3.9.3 <i>Salidas</i> .....	25
3.10 ANÁLISIS CUANTITATIVO DE LOS RIESGOS .....	25
3.10.1 <i>Entradas</i> .....	26
3.10.2 <i>Herramientas y técnicas</i> .....	27
3.10.3 <i>Salidas</i> .....	28
3.11 PLANIFICACIÓN DE LA RESPUESTA A RIESGOS.....	28
3.11.1 <i>Entradas</i> .....	29
3.11.2 <i>Herramientas y técnicas</i> .....	29
3.11.3 <i>Salidas</i> .....	31
3.12 SEGUIMIENTO Y CONTROL DE RIESGOS.....	32
3.12.1 <i>Entradas</i> .....	33

---

3.12.2 Herramientas y Técnicas .....	33
3.12.3 Salidas .....	34
3.13 METODOLOGÍAS PARA ANÁLISIS DE RIESGO.....	35
3.13.1 CRAMM .....	36
3.13.2 OCTAVE .....	37
3.13.3 MAGERIT .....	37
3.14 MAGERIT: TÉCNICAS .....	38
3.14.1 Técnicas Específicas .....	38
3.14.2 Técnicas Generales.....	42
<b>IV. CONCLUSIÓN .....</b>	<b>49</b>
<b>V. REFERENCIAS BIBLIOGRÁFICAS .....</b>	<b>51</b>

## INDICE DE FIGURAS

Figura N °1: Interacción de vulnerabilidades, amenazas y riesgos.....	14
Figura N °2: Ejemplo de contenido del Plan de Gestión de Riesgos.....	19
Figura N °3: Identificación de riesgos.....	19
Figura N °4: Análisis cualitativo de los riesgos.....	22
Figura N ° 5: Categorización de riesgos.....	25
Figura N ° 6: Análisis cuantitativo de los riesgos.....	26
Figura N ° 7: Diagrama de Árbol de decisiones.....	27
Figura N ° 8: Estrategias para Riesgos Negativos o Amenazas.....	30
Figura N ° 9: Estrategias para riesgos positivos u oportunidades.....	30
Figura N ° 10: Seguimiento y control de riesgos.....	32
Figura N ° 11: Gestión de Riesgo.....	35
Figura N ° 12: Técnica Gráfica: Por puntos y líneas.....	43
Figura N ° 13: Técnica Gráfica: Por barras.....	44
Figura N ° 14: Técnica Gráfica: Gráficos de radar.....	45
Figura N ° 15: Técnica Gráfica: Diagrama de torta.....	46

## INDICE DE TABLAS

Tabla N °1: Matriz de Probabilidad e Impacto.....	24
Tabla N ° 2: Matriz de Probabilidad e Impacto.....	24
Tabla N ° 3: Tabla sencilla de doble entrada.....	39

## I. JUSTIFICACIÓN

La meta principal del análisis del riesgo informático debería ser “proteger a la organización y su habilidad de manejar su misión” no solamente la protección de los elementos informáticos. Además, el proceso no solo debe de ser tratado como una función técnica generada por los expertos en tecnología que operan y administran los sistemas, sino como una función esencial de administración por parte de toda la organización.

Es importante recordar que el riesgo es el impacto negativo en el ejercicio de la vulnerabilidad, considerando la probabilidad y la importancia de ocurrencia. Por lo que podemos decir a grandes rasgos, que el análisis de riesgos es el proceso de identificación, evaluación y toma de decisiones para reducir el riesgo a un nivel aceptable por este motivo es de gran importancia el estudio de las amenazas y vulnerabilidades a las que estamos expuestos cotidianamente. Por esta razón es necesario conocer algunas técnicas que ayuden a realizar un análisis de riesgo.



## II. OBJETIVOS

### 2.1 OBJETIVO GENERAL

- a) Conocer y comprender los fundamentos teóricos e identificar las técnicas existentes que se utiliza para realizar el análisis de riesgos.

### 2.2 OBJETIVOS ESPECIFICOS

- a) Identificar las vulnerabilidades de la organización, a través del análisis de riesgos.
- b) Utilizar las innovaciones tecnológicas como arma, durante el proceso de análisis de riesgos.
- c) Tomar en cuenta las recomendaciones para el análisis de riesgos dentro de una organización.
- d) Evaluar las metodologías en análisis de riesgos y definir la más adecuada.
- e) Indagar hasta conseguir resultados, tras un debido análisis de riesgos.

---

### III. DESARROLLO DEL TEMA

## TÉCNICAS RECOMENDADAS PARA EL ANÁLISIS DE RIESGO

### 3.1 Definición y componentes del riesgo

#### 3.1.1 Definiciones

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

Es la posibilidad de ocurrencia de aquella situación (interna o externa), que puede afectar negativamente el logro del objetivo, o la gestión de un proceso.

El riesgo indica lo que le podría pasar a los activos si no se protegieran adecuadamente. Es importante saber qué características son de interés en cada activo, así como saber en qué medida estas características están en peligro, es decir, analizar el sistema.

Es la probabilidad o posibilidad de que pueda ocurrir un daño a partir de un peligro.

Se representa como la combinación de la frecuencia y la consecuencia de un incidente identificado.

#### 3.1.2 Componentes del riesgo

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

#### 3.1.3 Clases de riesgos

- **Riesgo estratégico:** Relacionados con la misión y el cumplimiento de los objetivos estratégicos, la clara definición de políticas.

- **Riesgos de imagen:** Están relacionados con la percepción y la confianza por parte de la ciudadanía hacia la institución.
- **Riesgos operativos:** Provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, de la estructura de la entidad.
- **Riesgos financieros:** Relacionados con el manejo de los recursos de la entidad.
- **Riesgos de cumplimiento:** Se asocian con el cumplimiento de los requisitos legales, contractuales, de ética pública, compromiso ante la comunidad.
- **Riesgos de tecnología:** Relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras.

## **3.2 Amenazas y vulnerabilidades**

### **3.2.1 Amenazas**

Es un peligro que está latente, que todavía no se desencadenó, pero que sirve como aviso para prevenir o para presentar la posibilidad de que sí lo haga. La amenaza es entendida como el anuncio de que algo malo o peligroso puede suceder. (Definición ABC).

Las amenazas son agentes capaces de explotar los fallos de seguridad, que denominamos puntos débiles y, como consecuencia de ello, causar pérdidas o daños a los activos de una empresa, afectando a sus negocios.

Los activos están constantemente sometidos a amenazas que pueden colocar en riesgo la integridad, confidencialidad y disponibilidad de la información. Estas amenazas siempre existirán y están relacionadas a causas que representan riesgos, las cuales pueden ser: causas naturales o no naturales causas internas o externas.

Las amenazas son constantes y pueden ocurrir en cualquier momento. Esta relación de frecuencia-tiempo, se basa en el concepto de riesgo, lo cual representa la probabilidad de que una amenaza se concrete por medio de una vulnerabilidad o punto débil.

- **Clasificación de las amenazas:**

- ✓ **Amenazas naturales:** condiciones de la naturaleza y la intemperie que podrán causar daños a los activos, tales como fuego, inundación, terremotos, entre otros.
- ✓ **Intencionales:** son amenazas deliberadas, fraudes, vandalismo, sabotajes, espionaje, invasiones y ataques, robos y hurtos de información, entre otras.
- ✓ **Involuntarias:** son amenazas resultantes de acciones inconscientes de usuarios, por virus electrónicos, muchas veces causadas por la falta de conocimiento en el uso de los activos, tales como errores y accidentes. Entre las principales amenazas, la ocurrencia de virus, la divulgación de contraseñas y la acción de *hackers* están entre los más frecuentes.

### 3.2.2 Vulnerabilidad

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

Uno de los primeros pasos para la implementación de la seguridad es rastrear y eliminar los puntos débiles de un ambiente de tecnología de la información. Al ser identificados los puntos débiles, será posible dimensionar los riesgos a los cuales el ambiente está expuesto y definir las medidas de seguridad apropiadas para su corrección.

Los puntos débiles dependen de la forma en que se organizó el ambiente en que se maneja la información. La existencia de puntos débiles está relacionada con la presencia de elementos que perjudican el uso adecuado de la información y del medio en que la misma se está utilizando.

#### ➤ Tipos

- ✓ **Vulnerabilidades físicas**  
Los puntos débiles de orden físico son aquellos presentes en los ambientes en los cuales la información se está almacenando o manejando.

Ejemplo Como ejemplos de este tipo de vulnerabilidad se distinguen: instalaciones inadecuadas del espacio de trabajo, ausencia de recursos para el combate a incendios; disposición desorganizada de cables de energía y de red, ausencia de identificación de personas y de locales, entre otros.

✓ **Vulnerabilidades naturales**

Los puntos débiles naturales son aquellos relacionados con las condiciones de la naturaleza que puedan colocar en riesgo la información. Muchas veces, la humedad, el polvo y la contaminación podrán causar daños a los activos. Por ello, los mismos deberán estar protegidos para poder garantizar sus funciones.

Entre las amenazas naturales más comunes podemos mencionar: Ambientes sin protección contra incendios, locales próximos a ríos propensos a inundaciones, infraestructura incapaz de resistir a las manifestaciones de la naturaleza como terremotos, maremotos, huracanes etc.

✓ **Vulnerabilidades de hardware**

Los posibles defectos en la fabricación o configuración de los equipos de la empresa que pudieran permitir el ataque o alteración de los mismos.

Existen muchos elementos que representan puntos débiles de hardware. Entre ellos podemos mencionar: la ausencia de actualizaciones conforme con las orientaciones de los fabricantes de los programas que se utilizan, y conservación inadecuada de los equipos.

✓ **Vulnerabilidades de software**

Los puntos débiles de aplicaciones permiten que ocurran accesos indebidos a sistemas informáticos incluso sin el conocimiento de un usuario o administrador de red. Los puntos débiles relacionados con el software podrán ser explotados por diversas amenazas ya conocidas: La configuración e instalación indebidas de los programas de computadora, Ejemplo: Lectores de e-mail que permiten la ejecución de códigos maliciosos, editores de texto que permiten la ejecución de virus de macro etc.

✓ **Vulnerabilidades de medios de almacenaje**

Los medios de almacenamiento son los soportes físicos o magnéticos que se utilizan para almacenar la información. Entre los tipos de

soporte o medios de almacenamiento de la información que están expuestos podemos citar: disquetes, cd, discos duros de los servidores y de las bases de datos, así como lo que está registrado en papel.

✓ **Vulnerabilidades de comunicación**

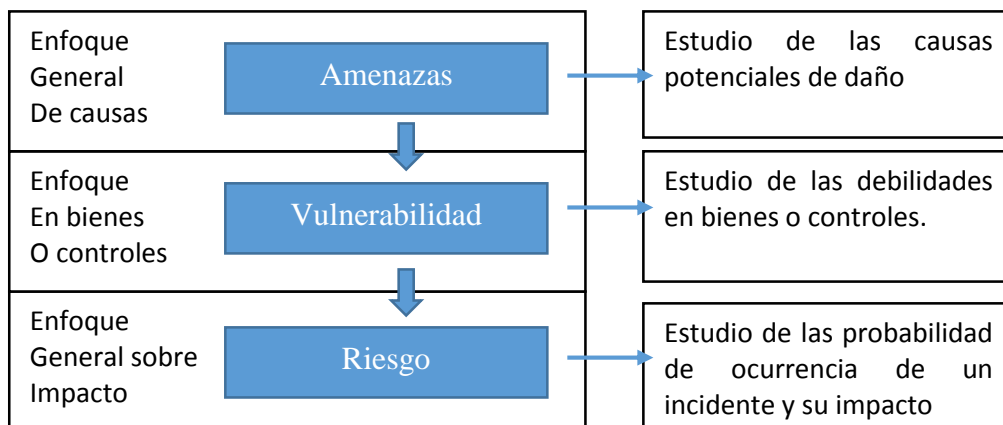
Este tipo de punto débil abarca todo el tránsito de la información. Donde sea que la información transite, ya sea vía cable, satélite, fibra óptica u ondas de radio, debe existir seguridad. El éxito en el tránsito de los datos es un aspecto crucial en la implementación de la seguridad de la información.

✓ **Vulnerabilidades humanas**

Esta categoría de vulnerabilidad está relacionada con los daños que las personas pueden causar a la información y al ambiente tecnológico que la soporta.

Los puntos débiles humanos también pueden ser intencionales o no. Muchas veces, los errores y accidentes que amenazan a la seguridad de la información ocurren en ambientes institucionales. La mayor vulnerabilidad es el desconocimiento de las medidas de seguridad adecuadas para ser adoptadas por cada elemento constituyente, principalmente los miembros internos de la empresa. Se Destacan dos puntos débiles humanos por su grado de frecuencia: la falta de capacitación específica para la ejecución de las actividades inherentes a las funciones de cada uno, la falta de conciencia de seguridad para las actividades de rutina, los errores, omisiones, insatisfacciones etc.

**Interacción entre vulnerabilidades, amenazas y riesgos**



**Figura N° 1: Interacción de Vulnerabilidades, amenazas y riesgos**

**Fuente: Metodología Magerit- Libro 1**

### **3.3 Mapa de riesgos**

#### **3.3.1 Definición**

Es una herramienta que permite organizar la información sobre los riesgos de las empresas y visualizar su magnitud, con el fin de establecer las estrategias adecuadas para su manejo.

Los mapas de riesgos pueden representarse con gráficos o datos. Los gráficos corresponden a la calificación de los riesgos con sus respectivas variables y a su evaluación de acuerdo con el método utilizado en cada empresa. Los datos pueden agruparse en tablas, con información referente a los riesgos; a su calificación, evaluación, controles y los demás datos que se requieran para contextualizar la situación de la empresa y sus procesos, con respecto a los riesgos que la pueden afectar y a las medidas de tratamiento implementadas.

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

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

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

#### **3.3.2 Beneficio**

Permite un mejor entendimiento en relación con la situación de los riesgos de la empresa en conjunto y de sus procesos o sus proyectos, al proporcionar información en forma global o discriminada.

En los casos en los cuales la gerencia no tiene conciencia de la necesidad de invertir en las medidas de control o financiamiento de los riesgos, o en el entrenamiento y sensibilización del personal, la información contenida en los mapas de riesgos puede servir de motivación para apoyar al desarrollo de los programas de administración de riesgos, orientar efectivamente las acciones al definir

prioridades para su manejo y al disponer de propuestas sobre las medidas de tratamiento.

Con el diseño e implementación de los mapas de riesgos se promueve el trabajo en equipo, lo cual incrementa el entendimiento de los participantes sobre los procesos analizados y crea un mayor nivel de responsabilidad y colaboración entre las dependencias, porque con ellos se logra entender las relaciones que tienen los procesos entre sí y sus implicaciones en la generación y administración de riesgos.

El mapa de riesgos permite también monitorear el desempeño de la organización en la administración de sus riesgos, con el establecimiento de comparativos anuales a partir de las evaluaciones de los diferentes riesgos y el análisis de la efectividad de las medidas de control implementadas.

### 3.4 Niveles de aceptación del riesgo

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

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

- a) **Parámetros de aceptabilidad del riesgo:** Se entiende como los criterios que permiten determinar si un riesgo específico se ubica dentro del nivel de riesgo aceptado por la institución.
  
- b) **Nivel de riesgo aceptable:** Nivel de riesgo que el equipo de proyecto están dispuestos y en capacidad de aceptar para cumplir con los objetivos (relacionado a tiempo, costo, calidad, alcance), sin incurrir en costos ni efectos adversos excesivos en relación con sus beneficios esperados o ser incompatible con las expectativas de los interesados.

### 3.5 Plan de acción

Un plan de acción es una presentación resumida de las tareas que deben realizarse por ciertas personas, en un plazo de tiempo específico, utilizando un monto de recursos asignados con el fin de lograr un objetivo dado. De esta



manera, un plan de acción se constituye como una especie de guía que brinda un marco o una estructura a la hora de llevar a cabo un proyecto.

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

### **3.6 Control y monitoreo del riesgo**

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

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

### **3.7 Planificación de la gestión de riesgos**

La definición de cómo realizar las actividades de gestión de riesgos para un proyecto, se lleva a cabo mediante el proceso *Planificar la gestión de riesgos*.

Una planificación cuidadosa y explícita mejoran las posibilidades de éxito de los demás procesos de la gestión de riesgos del proyecto. Consiste en decidir cómo abordar y llevar a cabo todas las actividades de gestión de los riesgos de un proyecto. La planificación es importante para garantizar que el nivel, el tipo y la visibilidad de la gestión de riesgos estén de acuerdo con la importancia del proyecto para la organización. Durante este proceso, es interesante plantearse las siguientes cuestiones:

*¿Quiénes serán los responsables de identificar los riesgos?*

*¿En qué momento y cómo llevaremos a cabo la identificación de riesgos?*

*¿Qué escala utilizaremos para el proceso Realizar el Análisis Cualitativo de Riesgos?*

*¿Cómo priorizaremos los riesgos?*

*¿Es necesario Realizar el Análisis Cuantitativo de Riesgos? ¿Qué herramientas utilizaremos?*

*¿Qué estrategia adoptaremos para cada riesgo?*

*¿Cada cuánto tiempo realizaremos el control y seguimiento de riesgos?*

### 3.7.1 Entradas

- **Plan para la dirección del proyecto:** A la hora de planificar la gestión de riesgos, deben tenerse en cuenta todos los planes secundarios de gestión y las líneas base aprobados, de forma que el *Plan de gestión de riesgos* resulte consistente con ellos.
- **Acta de constitución:** Puede contener una descripción de riesgos de alto nivel.
- **Registro de interesados:** Proporciona una visión general de los roles de cada interesado para con el proyecto.

### 3.7.2 Herramientas y técnicas

- **Técnicas analíticas:** Se usan para entender y definir el contexto general de la gestión de riesgos.
- **Juicio de expertos:** Dependiendo del sector industrial del proyecto, cuando se manejan tecnologías no maduras, es posible que no existan fuentes de información objetivas. En este ambiente de incertidumbre total ó inespecífica, es casi obligado acudir al juicio de expertos para desarrollar algún tipo de estrategia de tratamiento del Riesgo. No se puede dejar de utilizar esta fuente de información incluso si existen fuentes objetivas de información, porque es necesario tener experiencia y criterio en el tratamiento de datos.
- **Reuniones:** Del equipo de Proyecto.

### 3.7.3 Salidas

- **Plan de Gestión de Riesgos:** Describe la forma en que se llevará a cabo la gestión de riesgos del Proyecto. Es un plan subsidiario del Plan para la Dirección del Proyecto



**Figura N° 2: Ejemplo de contenido del Plan de Gestión de Riesgos**  
**Fuente: PMBOK® 5TH EDICIÓN**

### 3.8 Identificación de los riesgos

Una vez establecido el Plan de Gestión de Riesgos del Proyecto se llevará a cabo el proceso *Identificar los riesgos*, que es el proceso por el cual se determinan los riesgos que pueden afectar el Proyecto y se documentan sus características.



**Figura N° 3: Identificación de Riesgos**  
**Fuente: PMBOK® 5TH EDICIÓN**

Entre las personas que participan en la identificación de riesgos se pueden incluir: el director del Proyecto, los miembros del equipo del Proyecto, el equipo

de gestión de riesgos (si está asignado), clientes, expertos en la materia externos al equipo del Proyecto, usuarios finales, otros directores del Proyecto, interesados y expertos en Gestión de Riesgos.

*Identificar los Riesgos* es un proceso **iterativo** que se actualiza en cada uno de los procesos de la Gestión de Riesgos, ya que se pueden descubrir nuevos riesgos o pueden evolucionar conforme el proyecto avanza a lo largo de su ciclo de vida. La frecuencia de iteración y quiénes participan en cada ciclo varía de una situación a otra.

### 3.8.1 Entradas

- **Plan de Gestión de Riesgos:** Las asignaciones de roles y responsabilidades, las reservas para contingencias y la categorización de los riesgos.
  
- **Planes y líneas de base:**
  - ✓ **El Plan de Gestión de Costos** proporciona procesos y controles que se pueden utilizar para ayudar a identificar los Riesgos a lo largo del Proyecto.
  - ✓ **El Plan de Gestión del Cronograma** proporciona conocimiento sobre los objetivos y expectativas relativos al tiempo y cronograma del Proyecto que pueden ser afectados por Riesgos.
  - ✓ **El Plan de Gestión de la Calidad** proporciona una línea base de medidas y métricas de calidad aplicables a la identificación de Riesgos.
  - ✓ **El Plan de Gestión de los Recursos Humanos** proporciona una guía sobre el modo en que se deben definir, adquirir, dirigir y finalmente liberar los recursos humanos del Proyecto, así como los roles y responsabilidades dentro del Proyecto.
  - ✓ *La línea Base del Alcance* recoge los supuestos del Proyecto.
  
- **Estimaciones de costo y duración de las actividades**
  
- **Registro de interesados:** Cualquier información sobre ellos será útil a la hora de pedir que contribuyan identificando los Riesgos del Proyecto. Hay que asegurar que los actores interesados clave, especialmente el cliente, son entrevistados o incluso que participen durante el proceso de identificación de Riesgos.
  
- **Documentos del Proyecto:** Registro de supuestos, informes de desempeño, informes sobre el valor ganado, diagramas de red, líneas base, etc.

- **Documentación de adquisiciones:** Cuando el Proyecto requiere una adquisición externa, los documentos de ésta son entrada para este proceso

### 3.8.2 Herramientas y técnicas

- **Revisiones de la Documentación:** Se puede realizar una revisión de toda la documentación del Proyecto, incluidos planes, asunciones y archivos de Proyectos anteriores y otra información. La calidad de los planes, así como la consistencia entre esos planes con requisitos y asunciones, pueden ser indicadores de Riesgos.
- **Técnicas de recopilación de información:** Brainstorming (tormenta de ideas), técnica Delphi, entrevistas o análisis casual.
- **Análisis con listas de verificación:** Las listas de verificación para identificación de Riesgos pueden ser desarrolladas basándose en información histórica y en el conocimiento que ha sido acumulado de Proyectos anteriores similares y de otras fuentes de información.
- **Análisis de supuestos:** Diferentes grupo de hipótesis, escenarios y supuestos para cada riesgo identificado.
- **Técnicas de diagramación:** Pueden ser, Diagramas de causa y efecto (Ishikawa), Diagrama de flujo o sistemas o Diagrama de influencias.
- **Análisis SWOT o FODA:** Debilidades, Amenazas, Fortalezas y Oportunidades.
- **Juicio de expertos:** Sin olvidar a las personas de la organización con experiencia en Proyectos similares realizados anteriormente.

### 3.8.3 Salidas

- **Registro de Riesgos:** Contiene al final los resultados de los demás procesos de gestión de riesgos a medida que se llevan a cabo, dando como resultado un incremento en el nivel y tipo de información contenida en el registro de riesgos conforme transcurre el tiempo. La preparación del registro de riesgos comienza en el proceso Identificar los Riesgos con la siguiente información, y luego queda a disposición para otros procesos de dirección de proyectos y de Gestión de los Riesgos del Proyecto:

- ✓ *Lista de riesgos identificados.*
- ✓ *Lista de respuestas potenciales.*

### 3.9 Análisis cualitativo de los riesgos

El Análisis cualitativo de Riesgos incluye los métodos para priorizar los riesgos identificados para realizar otras acciones, como Análisis cuantitativo de Riesgos o planificación de la respuesta a los riesgos. Las organizaciones pueden mejorar el rendimiento del Proyecto de manera efectiva centrándose en los Riesgos de alta prioridad.

La definición de niveles de probabilidad e impacto puede reducir la influencia de parcialidades. Realizar el *Análisis Cualitativo de Riesgos* es por lo general un medio rápido y económico de establecer prioridades para la planificación de la respuesta a los riesgos y sienta las bases para realizar el análisis cuantitativo de riesgos, si se requiere.



**Figura N° 4: Análisis cualitativo de los riesgos**

**Fuente: PMBOK® 5TH EDICIÓN**

#### 3.9.1 Entradas

- **Plan de Gestión de Riesgos:** Algunos elementos del Plan de Gestión de Riesgos pueden ser clave para el Análisis cualitativo de Riesgos. Por ejemplo, los roles y responsabilidades de la Gestión de Riesgos, las asignaciones presupuestarias y actividades del cronograma dedicadas a la Gestión de Riesgos, las categorías de riesgo, las definiciones de probabilidad e impacto, la matriz de probabilidad por impacto y la revisión

de las tolerancias al riesgo por parte de los interesados, además de los factores ambientales de la empresa. Estos elementos normalmente se adaptan al proyecto durante el proceso planificación de la gestión de riesgos, pero también pueden desarrollarse durante el proceso *Análisis Cualitativo de Riesgos*.

- **Línea Base del alcance del Proyecto:** Los Proyectos de tipo común o recurrente tienden a tener más Riesgos bien comprendidos. Los Proyectos que usan tecnología punta o primera en su clase, así como los Proyectos altamente complejos, tienden a tener mayor incertidumbre. Todo esto puede ser evaluado examinando el enunciado del alcance del Proyecto.
- **Registro de Riesgos:** Del registro de Riesgos, la lista de Riesgos identificados es un elemento clave para el Análisis Cualitativo de Riesgos.
- **Activos de los Procesos de la Organización:** Por ejemplo, la información procedente de proyectos anteriores similares y las bases de datos de riesgos disponibles.

### 3.9.1 Herramientas y técnicas

- **Evaluación de probabilidad e impacto de los Riesgos:** La evaluación de la probabilidad de los riesgos estudia la probabilidad de ocurrencia de cada riesgo específico. La evaluación del impacto de los riesgos investiga el efecto potencial de los mismos sobre un objetivo del proyecto, tal como el cronograma, el costo, la calidad o el desempeño, incluidos tanto los efectos negativos en el caso de las amenazas, como positivos, en el caso de las oportunidades.
- **Matriz de probabilidad e impacto:** Tabla de doble entrada que combina la probabilidad de que ocurra un evento, con el impacto que éste puede causar en el Proyecto. De esta manera, conseguimos establecer una priorización de los riesgos.

La escala para categorizar y priorizar los riesgos será fijada en el Plan de Gestión de Riesgos y es subjetiva, es decir, establecida por la Organización el responsable de Realizar el análisis Cualitativo de Riesgos.

Por ejemplo:

PROBABILIDAD		IMPACTO	
Nada probable	0,10	Muy bajo	0,05
Poco probable	0,30	Bajo	0,10
Medianamente probable	0,50	Moderado	0,20
Bastante probable	0,70	Alto	0,40
Muy probable	0,90	Muy alto	0,80

**Tabla N° 1: Tabla de probabilidad e Impacto**  
**Fuente: PMBOK® 5TH EDICIÓN**

Probabilidad	Amenazas					Oportunidades				
0.90	0.05	0.09	0.18	0.36	0.72	0.72	0.36	0.18	0.09	0.05
0.70	0.04	0.07	0.14	0.28	0.56	0.56	0.28	0.14	0.07	0.04
0.50	0.03	0.05	0.10	0.20	0.40	0.40	0.20	0.10	0.05	0.03
0.30	0.02	0.03	0.06	0.12	0.24	0.24	0.12	0.06	0.03	0.02
0.10	0.01	0.01	0.02	0.04	0.08	0.08	0.04	0.02	0.01	0.01
Escala relativa	0.05	0.10	0.20	0.40	0.80	0.80	0.40	0.20	0.10	0.05
	Impacto en, al menos, un objetivo del proyecto (C, T y/o Alcance)									

Cada riesgo es calificado de acuerdo con su probabilidad de ocurrencia y el impacto sobre un objetivo en caso de que ocurra. Los umbrales de la organización para riesgos bajos, moderados o altos se muestran en la matriz y determinan si el riesgo es calificado como alto, moderado o bajo para ese objetivo.

**Tabla N° 2: Matriz de Probabilidad e Impacto**  
**Fuente: PMBOK® 5TH EDICIÓN**

- **Evaluación de la calidad de los datos sobre Riesgos:** El análisis cualitativo requiere datos exactos, lo que implica examinar el grado de entendimiento del riesgo y la exactitud, calidad, fiabilidad e integridad de los datos relacionados con el riesgo.
- **Categorización de Riesgos:** Risk Breakdown Structure (RBS) La agrupación de los riesgos en función de sus causas más comunes, puede llevar al desarrollo de respuestas efectivas a los riesgos.





**Figura N° 5: Categorización de Riesgos**

**Fuente: PMBOK® 5TH EDICIÓN**

- **Evaluación de la Urgencia de los Riesgos:** Estudio de aquellos riesgos que requieren respuesta a corto plazo.
- **Juicio de expertos**

### 3.9.3 Salidas

- **Actualizaciones a los documentos del Proyecto:**
  - ✓ Clasificación relativa o lista de prioridades de los riesgos del Proyecto.
  - ✓ Riesgos agrupados por categorías.
  - ✓ Causas de riesgos o áreas del Proyecto que requieren particular atención.
  - ✓ Lista de riesgos que requieren respuesta a corto plazo.
  - ✓ Lista de riesgos que requieren análisis y respuesta adicionales.
  - ✓ Lista de supervisión para riesgos de baja prioridad.
  - ✓ Tendencias en los resultados del análisis cualitativo de riesgos.

### 3.10 Análisis cuantitativo de los riesgos

El Análisis Cuantitativo de Riesgos se realiza primero sobre los Riesgos definidos como prioritarios en el proceso de *Realizar el Análisis Cualitativo de Riesgos*. El proceso *Realizar el Análisis Cuantitativo de Riesgos* analiza el efecto de esos Riesgos y les asigna una cuantificación numérica que permite tomar decisiones en caso de incertidumbre.

Puede utilizarse para asignar a esos riesgos una calificación numérica individual o para evaluar el efecto acumulativo de todos los riesgos que afectan el Proyecto. También presenta un enfoque cuantitativo para tomar decisiones en caso de incertidumbre.

A pesar de que es una entrada al proceso planificación de la respuesta a los Riesgos, el Análisis Cuantitativo de Riesgos debe repetirse también después de la planificación de la respuesta a los Riesgos, para determinar si el Riesgo general del Proyecto ha sido reducido satisfactoriamente. También, como parte del proceso *Seguimiento y Control de Riesgos*, con el fin de establecer la tendencia de mitigación del Riesgo, lo que puede indicar la necesidad de más o menos acciones de Gestión de Riesgos.



**Figura N° 6: Análisis cuantitativo de los riesgos**  
**Fuente: PMBOK® 5TH EDICIÓN**

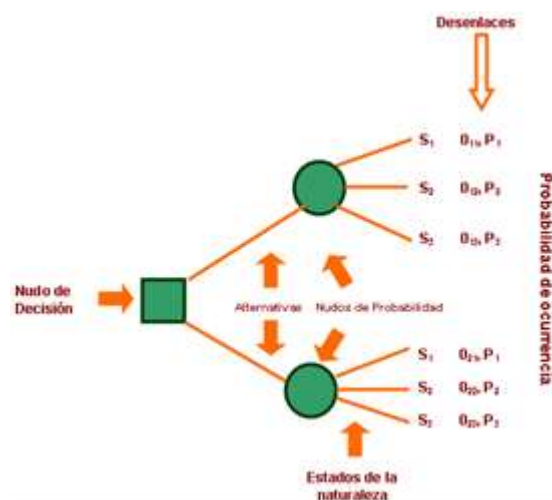
### 3.10.1 Entradas

- **Registro de Riesgos:** Algunos elementos clave del registro de Riesgos para el Análisis Cuantitativo de Riesgos incluyen la lista de Riesgos identificados, la lista de prioridades o clasificaciones relativas de los Riesgos del Proyecto y los Riesgos agrupados por categorías.
- **Plan de Gestión de Riesgos:** Algunos elementos del Plan de Gestión de Riesgos son clave para el Análisis Cuantitativo de Riesgos, por ejemplo los roles y responsabilidades de la Gestión de Riesgos, asignaciones presupuestarias y actividades del cronograma destinados a la Gestión de Riesgos, categorías de Riesgo, la RBS y las tolerancias al Riesgo por parte de los interesados en el Proyecto.
- **Planes de Gestión de Costos y del Cronograma:** El plan de Gestión de Costos del Proyecto establece el formato y los criterios para planificar, estructurar, estimar, preparar el presupuesto y controlar los costes del Proyecto, incluidas las asignaciones a la Gestión de Riesgos. El plan de Gestión del cronograma del Proyecto establece el formato y los criterios

para desarrollar y controlar el cronograma del Proyecto, incluidas las acciones de Gestión de Riesgos.

### 3.10.2 Herramientas y técnicas

- **Técnicas de recopilación y representación de datos:** Entrevistas y reuniones. Distribuciones de probabilidad. Juicio de expertos.
- **Técnicas de análisis cuantitativo de riesgos y de modelado:** Las más comunes son:
  - ✓ **Análisis de sensibilidad.** Ayuda a determinar qué riesgos tienen un mayor impacto potencial en el proyecto. Este método evalúa el grado en que la incertidumbre de cada elemento del proyecto afecta el objetivo que está siendo examinado, cuando todos los demás elementos inciertos se mantienen en sus valores de línea base.
  - ✓ **Análisis del valor monetario esperado (EMV).** Concepto estadístico que calcula el resultado promedio cuando el futuro incluye escenarios que pueden o no ocurrir (es decir, análisis bajo incertidumbre). El valor monetario esperado de las oportunidades se expresará por lo general con valores positivos, mientras que el de los riesgos será negativo. Se calcula multiplicando el valor de cada posible resultado por su probabilidad de ocurrencia, y sumando luego los resultados. Este tipo de análisis se utiliza comúnmente en el análisis mediante árbol de decisiones.



**Figura N° 7: Diagrama de Árbol de Decisiones**  
**Fuente: PMBOK® 5TH EDICIÓN**

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

➤ **Juicio de expertos**

### 3.10.3 Salidas

➤ **Actualizaciones a los documentos del Proyecto:**

- ✓ *Análisis probabilístico del Proyecto.*
- ✓ *Probabilidad de alcanzar los objetivos de costo y tiempo.*
- ✓ *Lista priorizada de riesgos cuantificados.*
- ✓ *Tendencias en los resultados del análisis cuantitativo de riesgos.*

### 3.11 Planificación de la respuesta a riesgos

Este proceso desarrolla las opciones y acciones para mejorar las oportunidades y reducir las amenazas a los objetivos del Proyecto. Se realiza después de los procesos de *Realizar el Análisis Cualitativo de Riesgos* y *Realizar el Análisis Cuantitativo de Riesgos* (en el caso de que éste se aplique).

Incluye la identificación y asignación de una persona (el “propietario de la respuesta a los riesgos”) para que asuma la responsabilidad de cada respuesta a los riesgos acordada y financiada. El proceso *Planificar la Respuesta a los Riesgos* aborda los riesgos en función de su prioridad, introduciendo recursos y actividades en el presupuesto, el cronograma y el plan para la dirección del Proyecto, según se requiera.

Las respuestas a los Riesgos planificadas deben ser congruentes con la importancia del Riesgo, tener un coste efectivo en relación al desafío, ser aplicadas a su debido tiempo, ser realistas dentro del contexto del Proyecto, estar acordadas por todas las partes implicadas, y a cargo de una persona responsable. A menudo, es necesario seleccionar la mejor respuesta a los

Riesgos entre varias opciones. La sección planificación de la respuesta a los Riesgos presenta los enfoques comúnmente usados para planificar las respuestas a los Riesgos. Los Riesgos incluyen las amenazas y las oportunidades que pueden afectar al éxito del Proyecto, y se discuten las respuestas para cada una de ellas.

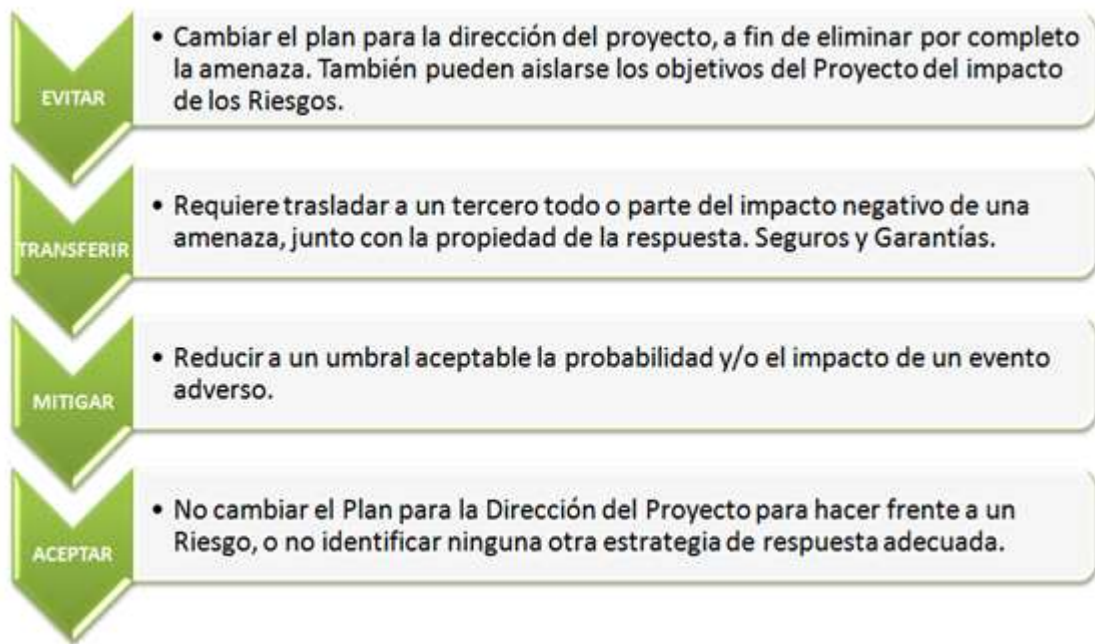
### 3.11.1 Entradas

- **Registros de Riesgos:** El registro de Riesgos se desarrolla por primera vez en el proceso de *Identificar los Riesgos*, y se actualiza durante los procesos de Análisis cualitativo de Riesgos y Análisis Cuantitativo de Riesgos. Es posible que el proceso de planificación de la respuesta a los Riesgos tenga que remitirse a los Riesgos identificados, las causas de los Riesgos, las listas de posibles respuestas, los propietarios de los Riesgos, los síntomas y las señales de advertencia para desarrollar las respuestas a los Riesgos.
- **Plan de Gestión de Riesgos:** Entre los componentes importantes del plan de Gestión de Riesgos se incluyen los roles y responsabilidades, las definiciones del análisis de Riesgos, los umbrales de Riesgo para los Riesgos bajo, moderado y alto, el tiempo y el presupuesto necesarios para la Gestión de los Riesgos del Proyecto. Algunos componentes del plan de Gestión de Riesgos que son entradas importantes a la planificación de la respuesta a los Riesgos pueden incluir umbrales de Riesgo para los Riesgos bajo, moderado y alto para ayudar a entender los Riesgos para los cuales se necesitan respuestas, la asignación de personal y la preparación del cronograma y el presupuesto para la planificación de la respuesta a los Riesgos.

### 3.11.2 Herramientas y técnicas

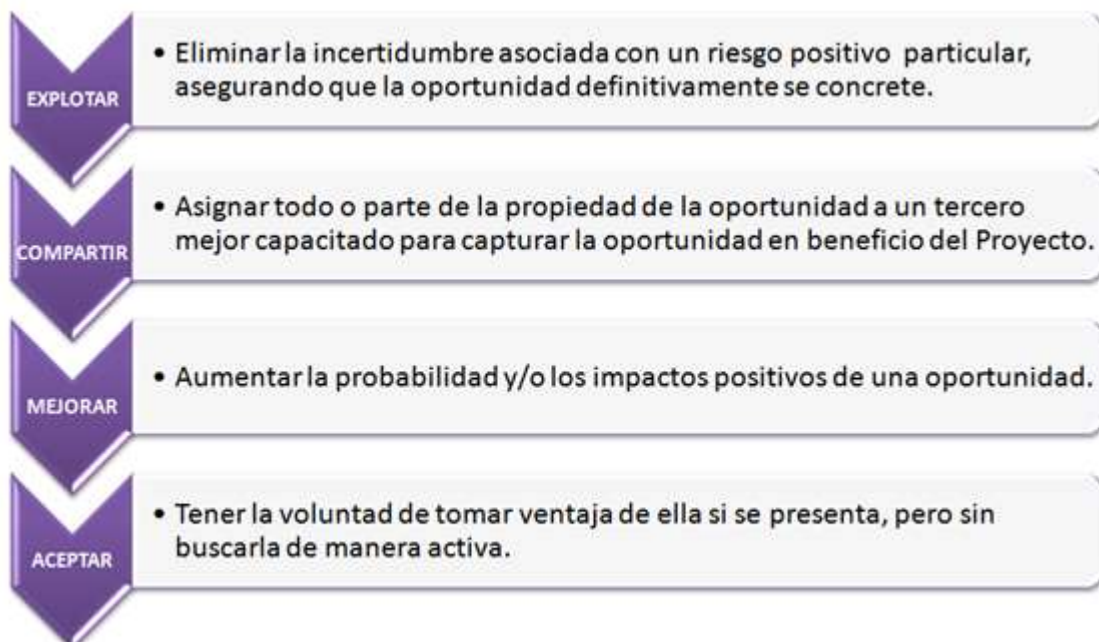
Existen varias estrategias de respuesta a los riesgos. Para cada riesgo, se debe seleccionar la estrategia o la combinación de estrategias con mayor probabilidad de eficacia. Las herramientas de análisis de riesgos, tales como el análisis mediante árbol de decisiones, pueden utilizarse para seleccionar las respuestas más apropiadas.

✓ **Estrategias para Riesgos Negativos o Amenazas:**



**Figura N° 8: Estrategias para Riesgos Negativos o Amenazas**  
**Fuente: PMBOK® 5TH EDICIÓN**

✓ **Estrategias para Riesgos Positivos u Oportunidades:**



**Figura N° 9: Estrategias para Riesgos Positivos u Oportunidades**  
**Fuente: PMBOK® 5TH EDICIÓN**

- ✓ **Estrategias de respuesta para Contingencias:** Algunas estrategias se diseñan para ser usadas únicamente si se presentan determinados eventos. Para algunos riesgos, resulta apropiado para el equipo del proyecto elaborar un plan de respuesta que sólo se ejecutará bajo determinadas condiciones predefinidas, si se cree que habrá suficientes señales de advertencia para implementar el plan.
  
- ✓ **Juicio de expertos.**

### 3.11.3 Salidas

- **Actualizaciones a los Documentos del Proyecto:** los componentes del registro de riesgos pueden incluir:
  - ✓ *Los riesgos identificados, sus descripciones, el o las áreas del proyecto afectadas, sus causas y cómo pueden tener un efecto sobre los objetivos del proyecto.*
  - ✓ *Los propietarios del riesgo y sus responsabilidades asignadas.*
  - ✓ *Las salidas del proceso Realizar el Análisis Cualitativo de Riesgos, incluyendo las listas priorizadas de los riesgos del proyecto.*
  - ✓ *Las estrategias de respuesta acordadas.*
  - ✓ *Las acciones específicas para implementar la estrategia de respuesta seleccionada.*
  - ✓ *Los disparadores, los síntomas y las señales de advertencia relativos a la ocurrencia de riesgos.*
  - ✓ *El presupuesto y las actividades del cronograma necesarios para implementar las respuestas seleccionadas.*
  - ✓ *Los planes de contingencia y disparadores que requieren su ejecución.*
  - ✓ *Los planes de reserva para usarse como una reacción a un riesgo que ha ocurrido y para el que la respuesta inicial no ha sido la adecuada.*
  - ✓ *Los riesgos residuales que se espera que permanezcan después de la ejecución de las respuestas planificadas, así como los riesgos que han sido aceptados deliberadamente.*
  - ✓ *Los riesgos secundarios que surgen como resultado directo de la implementación de una respuesta a los riesgos.*
  - ✓ *Las reservas para contingencias que se calculan tomando como base el análisis cuantitativo de riesgos del proyecto y los umbrales de riesgo de la organización.*
  
- **Actualizaciones al Plan para la Dirección del Proyecto:** El plan de Dirección del Proyecto se actualiza a medida que se añaden actividades de respuesta a los Riesgos.

### 3.12 Seguimiento y control de riesgos

Las respuestas a los Riesgos planificadas que están incluidas en el *Plan para la Dirección del Proyecto* se ejecutan durante el ciclo de vida del Proyecto, pero el trabajo del Proyecto debe ser supervisado continuamente para detectar riesgos nuevos o que cambien. El seguimiento y control de riesgos es el proceso de identificar, analizar y planificar nuevos riesgos, realizar el seguimiento de los riesgos identificados y los que se encuentran en la lista de supervisión, volver a analizar los riesgos existentes, realizar el seguimiento de las condiciones que disparan los planes para contingencias, realizar el seguimiento de los riesgos residuales y revisar la ejecución de las respuestas a los riesgos mientras se evalúa su efectividad. Este proceso, así como los demás procesos de Gestión de riesgos, es un proceso continuo que se realiza durante la vida del Proyecto.

Durante el control de riesgos podemos tener que elegir estrategias alternativas, ejecutar un plan para contingencias o de reserva, adoptar acciones correctivas y modificar el *Plan para la Dirección del Proyecto*. El propietario de la respuesta a los riesgos debe informar periódicamente al director del Proyecto acerca de la efectividad del plan, de cualquier efecto no anticipado y cualquier corrección sobre la marcha que sea necesaria para gestionar el riesgo correctamente. El proceso de seguimiento y control de riesgos también incluye la actualización de los activos de los procesos de la organización, incluidas las bases de datos de las lecciones aprendidas del Proyecto y las plantillas de gestión de riesgos para beneficio de Proyectos futuros.



**Figura N° 10: Seguimiento y control de riesgos**  
**Fuente: PMBOK® 5TH EDICIÓN**



### 3.12.1 Entradas

- **Registro de Riesgos:** El registro de riesgos tiene entradas clave que incluyen los riesgos identificados y los propietarios de los riesgos, las respuestas a los riesgos acordadas, las acciones de implementación específicas, los síntomas y las señales de advertencia de riesgos, riesgos residuales y secundarios, lista de supervisión de riesgos de baja prioridad, y las reservas para contingencias de tiempo y coste.
- **Plan para la Dirección del Proyecto:** Este plan contiene el *plan de gestión de riesgos*, con entradas clave para la gestión de los riesgos del Proyecto, que incluyen la asignación de personas, incluidos los propietarios de los riesgos y otros recursos.
- **Datos sobre el Desempeño del Trabajo**
- **Informes de Desempeño:** Los informes de rendimiento proporcionan información sobre el rendimiento del trabajo del Proyecto, tal como un análisis que puede influir en los procesos de gestión de riesgos.

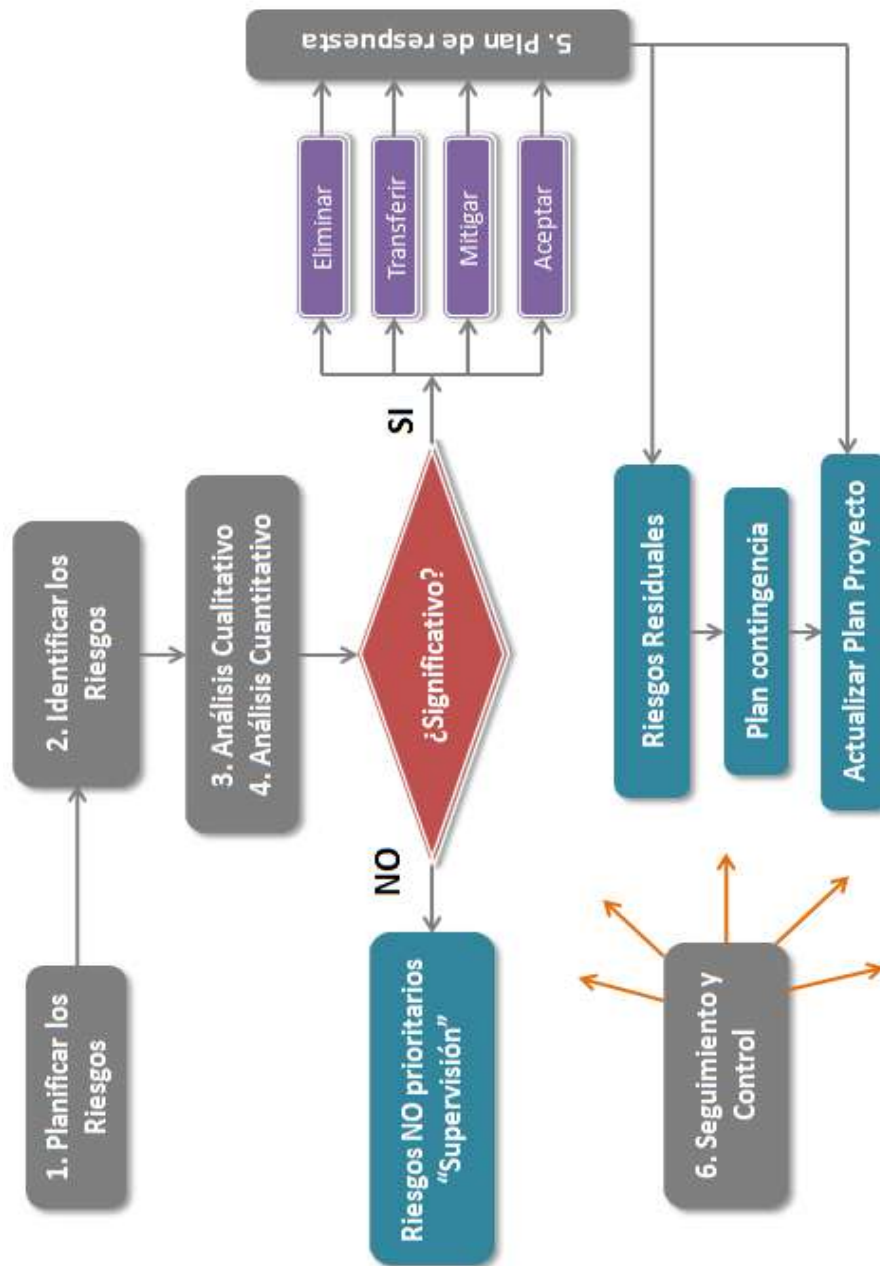
### 3.12.2 Herramientas y Técnicas

- **Reevaluación de Riesgos:** Este proceso, a menudo requiere la identificación de nuevos riesgos y la reevaluación de los riesgos ya identificados. Las reevaluaciones de los riesgos del Proyecto deben ser programadas con regularidad. La gestión de los riesgos del Proyecto debe ser un punto habitual del orden del día de las reuniones del equipo del Proyecto.
- **Auditorías de Riesgos:** Las auditorías de los riesgos examinan y documentan la efectividad de las respuestas a los riesgos para tratar los riesgos identificados y sus causas, así como la efectividad del proceso de gestión de riesgos.
- **Medición del Desempeño Técnico:** La medición del rendimiento técnico compara los logros técnicos de la ejecución con el cronograma de logros técnicos establecido en el Plan para la Dirección del Proyecto. El análisis de la desviación puede ayudar al éxito en lograr el alcance del Proyecto.
- **Análisis de Reserva:** El análisis de reservas compara la cantidad de reservas para contingencias que resta con la cantidad de riesgo residual a efectos de determinar si son suficientes.

- **Análisis de Variación y Tendencia:** Usando datos de rendimiento debe ser revisadas las tendencias de la ejecución del Proyecto. Para realizar el seguimiento del rendimiento general del Proyecto puede usarse el análisis del valor ganado. Los resultados de estos análisis pueden predecir la desviación respecto de la línea base Proyecto y proyectar sus objetivos a su compleción. La desviación puede deberse a impactos de eventos de riesgo.
  
- **Reuniones:** La gestión de los riesgos del Proyecto puede ser un punto del orden del día en las reuniones periódicas sobre el estado del Proyecto. Dependiendo de los Riesgos que hayan sido identificados, su prioridad y dificultad de respuesta ese punto puede llevar mucho tiempo. Cuanto más se practica la gestión de riesgos, más fácil resulta llevarla a cabo y que se haga con mayor exactitud.

### 3.12.3 Salidas

- **Información sobre el Desempeño del Trabajo:** La información de desempeño, como salida del proceso *Controlar los Riesgos*, proporciona un mecanismo para comunicar y apoyar la toma de decisiones del Proyecto.
  
- **Solicitudes de Cambio:** Para dar respuesta a los riesgos, a veces es necesario implementar planes para contingencias y/o soluciones alternativas, lo que lleva a cambiar el plan de Gestión del Proyecto.



**Figura N° 11: Gestión de Riesgo**  
**Fuente: PMBOK® 5TH EDICIÓN**

### 3.13 Metodologías para Análisis de Riesgo

Existen multitud de metodologías que nos pueden facilitar la realización de un análisis de riesgos.

Estas metodologías nos indican los pasos a seguir para su correcta ejecución, ya que, como hemos visto, suelen ser muy complejos y tienen multitud de variables.

Utilizar una herramienta para llevar a cabo el análisis de riesgos facilita su elaboración y permite realizar las labores de manera más sistemática. Esto facilita que la información resultante sea reutilizable y comparable con resultados de sucesivos análisis.

Algunas de estas metodologías son:

- ✓ CRAMM: “CCTA Risk Assessment and Management Methodology” fue originalmente desarrollado para uso del gobierno de UK pero ahora es propiedad de Siemens;
- ✓ MAGERIT “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información” está disponible tanto en español como en inglés.
- ✓ OCTAVE: “Operationally Critical Threat, Asset, and Vulnerability Evaluation” Metodología de Análisis y Gestión de Riesgos desarrollada por el CERT; las Metodologías anteriores se puede decir o aclarar que en si buscan lo mismo, analizar los riesgos informáticos en una compañía u organización.

### **3.13.1 CRAMM**

CRAMM es la metodología de análisis de riesgos desarrollado por la Agencia Central de Comunicación y Telecomunicación del gobierno británico. El significado del acrónimo proviene de **CCTA Risk Analysis and Management Method**. Su versión inicial data de 1987 y la versión vigente es la 5.2. Al igual que MAGERIT, tiene un alto calado en administración pública británica, pero también en empresas e instituciones de gran tamaño. Dispone de un amplio reconocimiento.

La metodología de CRAMM incluye las siguientes 3 etapas:

- La primera de las etapas recoge la definición global de los objetivos de seguridad entre los que se encuentra la definición del alcance, la identificación y evaluación de los activos físicos y software implicados, la determinación del valor de los datos en cuanto a impacto en el negocio y la identificación.
- En la segunda etapa de la metodología se hace el análisis de riesgos, identificando las amenazas que afecta al sistema, así como las

vulnerabilidades que explotan dichas amenazas y por último el cálculo de los riesgos de materialización de las mismas.

- En la tercera etapa se identifican y seleccionan las medidas de seguridad aplicadas en la entidad obteniendo los riesgos residuales, CRAMM proporciona una librería unas 3000 medidas de seguridad.

### **3.13.2 OCTAVE**

**OCTAVE** Sus siglas significan: Evaluación de la vulnerabilidad ante Amenazas desde el punto de vista operativo crítico, activo OCTAVE clasifica a los componentes de la empresa en activos y los ordena de acuerdo a su importancia en amenazas y vulnerabilidad, OCTAVE fue desarrollada pensando en las empresas, y ser flexible y adaptable a cualquier entorno.

Desarrollar una perspectiva de seguridad dentro de una organización, teniendo en cuenta perspectivas de todos los niveles para asegurarse que las soluciones puedan implementarse con facilidad. Se basan en los criterios del estándar con un enfoque en la práctica y evaluación de la seguridad basada en la información de riesgo.

La metodología **OCTAVE** está compuesta en tres fases:

- **Visión de organización:** Donde se definen los siguientes elementos: activos, vulnerabilidades de organización, amenazas, exigencias de seguridad y normas existentes.
- **Visión tecnológica:** se clasifican en dos componentes o elementos: componentes claves y vulnerabilidades técnicas.
- **Planificación de las medidas y reducción de los riesgos:** se clasifican en los siguientes elementos: evaluación de los riesgos, estrategia de protección, ponderación de los riesgos y plano de reducción de los riesgos.

### **3.13.3 MAGERIT**

Para lograr un buen nivel de seguridad se utilizará una metodología que es necesaria para realizar un plan de seguridad, la cual nos ayuda a realizar el análisis y gestión de riesgos, hablamos de la metodología MAGERIT (Metodología de Análisis y Gestión de Riesgos de IT).

La Metodología MAGERIT fue desarrollada por el Consejo Superior de Administración Electrónica (CSAE), y publicada por el Ministerio de

Administraciones Pública (MAP) encargado de la preparación, elaboración, desarrollo y aplicación de la política informática del Gobierno Español.

La primera versión se publicó en 1997, la segunda en el 2005 y la versión vigente en la actualidad es la versión 3.0, publicada en 2012. Se trata de una metodología abierta, de uso muy extendido en el ámbito español, y de uso obligatorio por parte de la Administración Pública Española.

Dispone de una herramienta de soporte, PILAR (Proceso Informático-Lógico para el Análisis y la gestión de Riesgos), de uso gratuito para la Administración Pública española y comercial para organizaciones privadas.

### **3.14 MAGERIT: Técnicas**

#### **3.14.1 Técnicas Específicas**

Técnicas que no se utilizan en otros contextos de trabajo. Se han considerado de especial interés:

➤ **Uso de tablas para la obtención sencilla de resultados.**

Dícese análisis de la distinción y separación de las partes de un todo hasta llegar a conocer sus principios o elementos. En el análisis de riesgos hay que trabajar con múltiples elementos que hay que combinar en un sistema para ordenarlo por importancia sin que los detalles, muchos, perjudiquen la visión de conjunto.

La experiencia ha demostrado la utilidad de métodos simples de análisis llevados a cabo por medio de tablas que, sin ser muy precisas, sí aciertan en la identificación de la importancia relativa de los diferentes activos sometidos a amenazas.

Sea la escala siguiente útil para calificar el valor de los activos, la magnitud del impacto y la magnitud del riesgo:

- ✓ **MB:** muy bajo
- ✓ **B:** bajo
- ✓ **M:** medio
- ✓ **A:** alto
- ✓ **MA:** muy alto

Se puede calcular el impacto en base a tablas sencillas de doble entrada:

<i>Impacto</i>		<i>degradación</i>		
		1%	10%	100%
<i>valor</i>	MA	M	A	MA
	A	B	M	A
	M	MB	B	M
	B	MB	MB	B
	MB	MB	MB	MB

**Tabla N° 3: Tabla sencilla de doble entrada**  
**Fuente: Magerit- Libro III**

Aquellos activos que reciban una calificación de impacto muy alto (MA) deberían ser objeto de atención inmediata.

➤ **Técnicas algorítmicas para la obtención de resultados elaborados**

Dícese análisis de la distinción y separación de las partes de un todo hasta llegar a conocer sus principios o elementos. En ciencias químicas, dícese análisis cualitativo del que tiene por objeto descubrir y aislar los elementos o ingredientes de un cuerpo compuesto. A diferencia del análisis cuantitativo que es el que se emplea para determinar la cantidad de cada elemento o ingrediente.

En las siguientes secciones se presentan dos enfoques algorítmicos. Primero, un modelo cualitativo que busca una valoración relativa del riesgo que corren los activos (¿qué es lo más frente a qué es lo menos?). Segundo, un modelo cuantitativo que ambiciona responder a la pregunta de cuánto más y cuánto menos. A continuación se presenta un modelo escalonado, típico del análisis de impacto sobre la disponibilidad de los sistemas de información. Por último se incluye un modelo para estimar la eficacia de un paquete de salvaguardas.

- ✓ **Modelo Cualitativo:** En un análisis de riesgos cualitativo se busca saber qué es lo que hay, sin cuantificarlo con precisión más allá de relativizar los elementos del modelo.
- ✓ **Modelo Cuantitativo:** En un análisis de riesgos cuantitativo se busca saber qué y cuánto hay, cuantificando todos los aspectos posibles
- ✓ **Modelo Escalonado:** Ciertas dimensiones de degradación de un activo se modelan más adecuadamente como escalones de valor.

- ✓ **Sobre la Eficacia de los Salvaguardas:** Todos los modelos requieren una evaluación de la eficacia de las salvaguardas que se despliegan para proteger a un activo de una amenaza. Se describe a continuación un modelo común para evaluar la eficacia de un conjunto de salvaguardas aplicadas sobre un activo

➤ **Árboles de ataque:**

Los árboles de ataque son una técnica para modelar las diferentes formas de alcanzar un objetivo. Aunque han existido durante años con diferentes nombres, se hicieron famosos a partir de los trabajos de B. Schneier que propuso su sistematización en el área de los sistemas de información.

El objetivo del atacante se usa como raíz del árbol. A partir de este objetivo, de forma iterativa e incremental se van detallando como ramas del árbol las diferentes formas de alcanzar aquel objetivo, convirtiéndose las ramas en objetivos intermedios que a su vez pueden refinarse. Los posibles ataques a un sistema se acaban modelando como un bosque de árboles de ataque.

- ✓ **Nodos con Atributos:**

Identificadas las diferentes maneras de alcanzar un objetivo, los nodos del árbol se pueden enriquecer con información de detalle, que puede ser de muy diferentes tipos; por ejemplo:

- ❖ Conocimientos que se requieren del atacante: cualquiera, alguna experiencia, un ingeniero, un *hacker* profesional, etc.
- ❖ Inversión del atacante: cantidad de dinero y tiempo que tendría que desembolsar para realizar la acción.
- ❖ Riesgo para el atacante: si es capturado, ¿qué consecuencias afrontaría?

Si la información del árbol con estos atributos se procesa automáticamente, podemos obtener escenarios simplificados de ataque:

- ❖ Usuarios inexpertos pero con bastante dinero.



- ❖ Atacantes profesionales pero sin capacidad de inversión (o sin necesidad de realizar una inversión adicional para perpetrar este ataque).
- ❖ Atacantes que quedarían impunes, etc.

Para alcanzar estos escenarios especializados basta eliminar del árbol las ramas que no satisfagan una condición cualitativa o cuantitativa.

Sobre un árbol con atributos es posible determinar el ataque más probable, simplemente extrayendo aquel ataque que requiere menos medios y menos conocimiento por parte del atacante. También es posible determinar cuál será la línea de acción de un posible perfil de atacante (que se determina en base al tipo de servicio o información que estamos protegiendo): aquel que con menos coste satisfaga los conocimientos mínimos para realizar el ataque.

#### ✓ **Riesgo Residual**

Cuando se han desplegado salvaguardas, su efecto puede reflejarse sobre el árbol de ataque:

- ❖ Incrementando el conocimiento que el atacante necesitaría para alcanzar su objetivo pese a las salvaguardas desplegadas: idealmente debería ser imposible por mucho que supiera.
- ❖ Incrementando el desembolso que el atacante tendría que realizar para alcanzar su objetivo a la vista de las salvaguardas desplegadas: idealmente el coste debería ser superior al beneficio para el atacante.

Un sistema ideal de salvaguardas eliminaría todas las ramas del árbol. Un sistema real suele llevar los atributos a niveles elevados de conocimiento e inversión que reducen la posibilidad de que el ataque se materialice a un nivel residual aceptado por la Dirección

#### ✓ **Construcción del Árbol**

La construcción del árbol es laboriosa. Marcar el objetivo final requiere un conocimiento de dónde está el valor en la Organización y cuál puede ser el objetivo del atacante respecto del mismo. El enriquecimiento en forma de ramas debería ser exhaustivo; pero está limitado por la imaginación del analista; si el atacante es más listo tiene una oportunidad para utilizar una vía imprevista. La experiencia

permite ir enriqueciendo el árbol con nuevos ataques realmente perpetrados o simplemente detectados en el perímetro con un buen sistema de monitorización.

Puede encontrarse ayuda a la construcción del árbol en:

- ❖ La experiencia propia o ajena en sistemas similares
- ❖ Grupos de reflexión (*brain storming meetings*) en los que de forma informal se van exponiendo cosas que posiblemente pensarían los atacantes; estas sesiones suelen generar mucho material en bruto que hay que organizar y estructurar para ser utilizado como herramienta de análisis.
- ❖ Herramientas que sugieran ataques en base a la naturaleza de los activos presentes en el sistema.

Si se dispone de un modelo de valor como el desarrollado en las actividades de la metodología Magerit, es posible utilizar éste para determinar la naturaleza de los activos y las dependencias entre ellos, de forma que podemos elaborar el árbol de ataques en base al conocimiento de los activos inferiores que constituyen la vía de ataque para alcanzar los activos superiores en los que suele residir el valor para la Organización.

### 3.14.2 Técnicas Generales

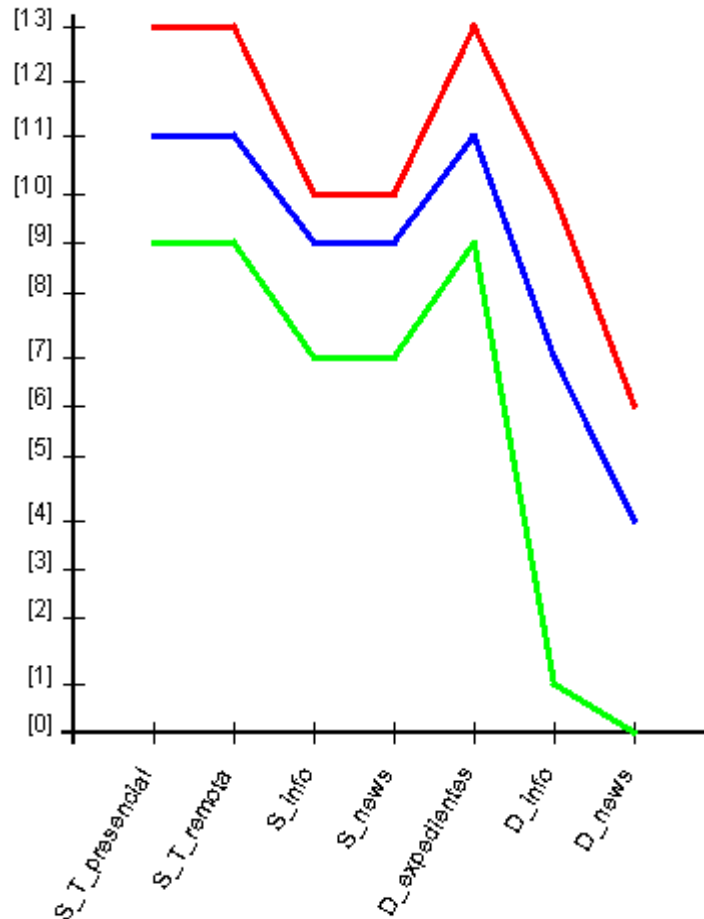
En este capítulo nos referiremos a técnicas generales que, entre otros casos, son de utilizad en el desarrollo de un proyecto de análisis y gestión de riesgos. No obstante su generalidad, cuando procede se ha indicado cómo se aplican en el contexto del análisis y gestión de riesgos. Las indicaciones dadas en este libro complementan a las presentadas a lo largo de la metodología.

#### ➤ Técnicas Graficas

Esta sección se centra en cómo algunas representaciones gráficas de los elementos de un proyecto AGR pueden apoyar a dicho proyecto, tanto como soporte a presentaciones, como en la toma de decisiones.

✓ **Por Puntos y Líneas**

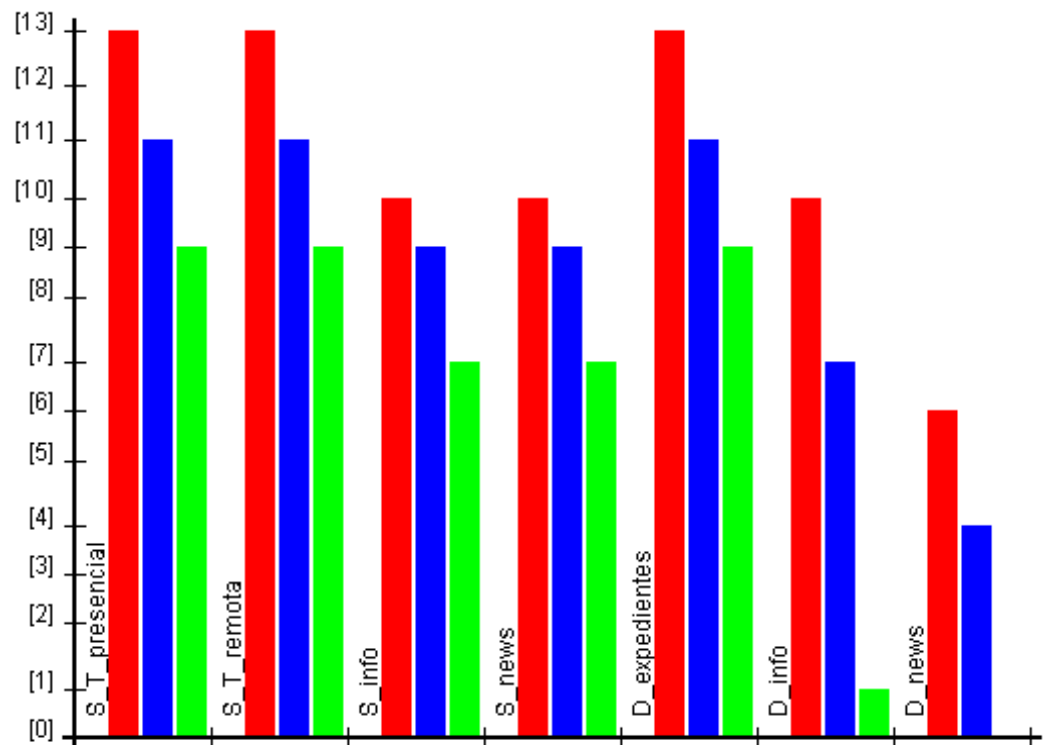
Es la forma más clásica de presentación de resultados. Se limita a usar los ejes cartesianos usando las abscisas para recoger los datos y las ordenadas para mostrar su valor.



**Figura N° 12: Técnica Gráfica: Por Puntos y Líneas**  
**Fuente: Magerit- Libro III**

✓ **Por Barras**

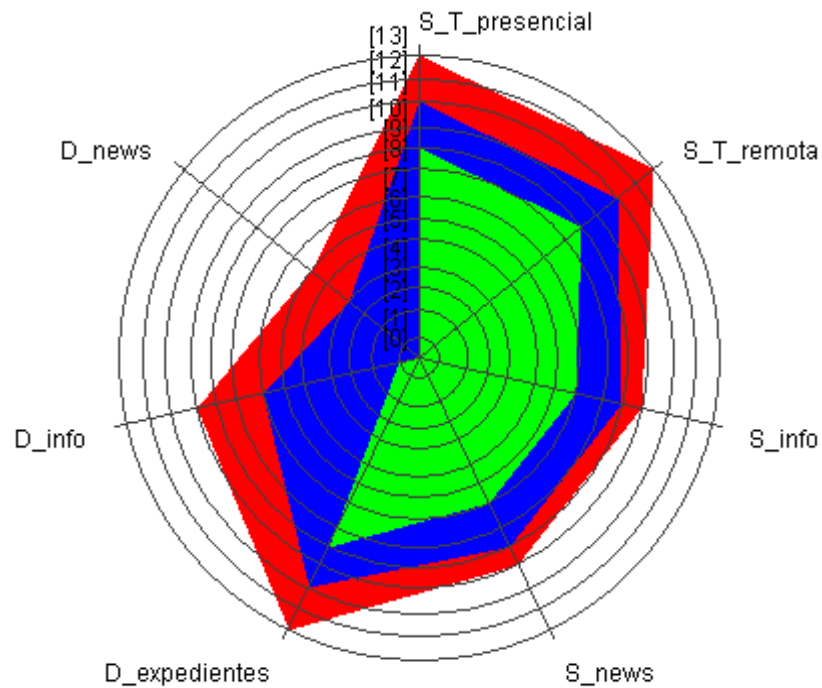
Los diagramas de barras disponen los elementos en unas coordenadas cartesianas convencionales: los elementos a considerar en un eje y los valores en el otro eje. Son muy similares a las presentaciones por puntos y líneas, aunque permiten menos resultados (dado que las barras ocupan más espacio que los puntos).



**Figura N° 13: Técnica Gráfica: Por Barras**  
**Fuente: Magerit- Libro III**

✓ **Gráficos de Radar**

Estos gráficos representan las distintas variables o factores del fenómeno en estudio sobre semiejes o radios que parten de un centro. Estos radios, tantos como factores, se gradúan para representar sus niveles y posibles umbrales en escala normal o logarítmica, según convenga.



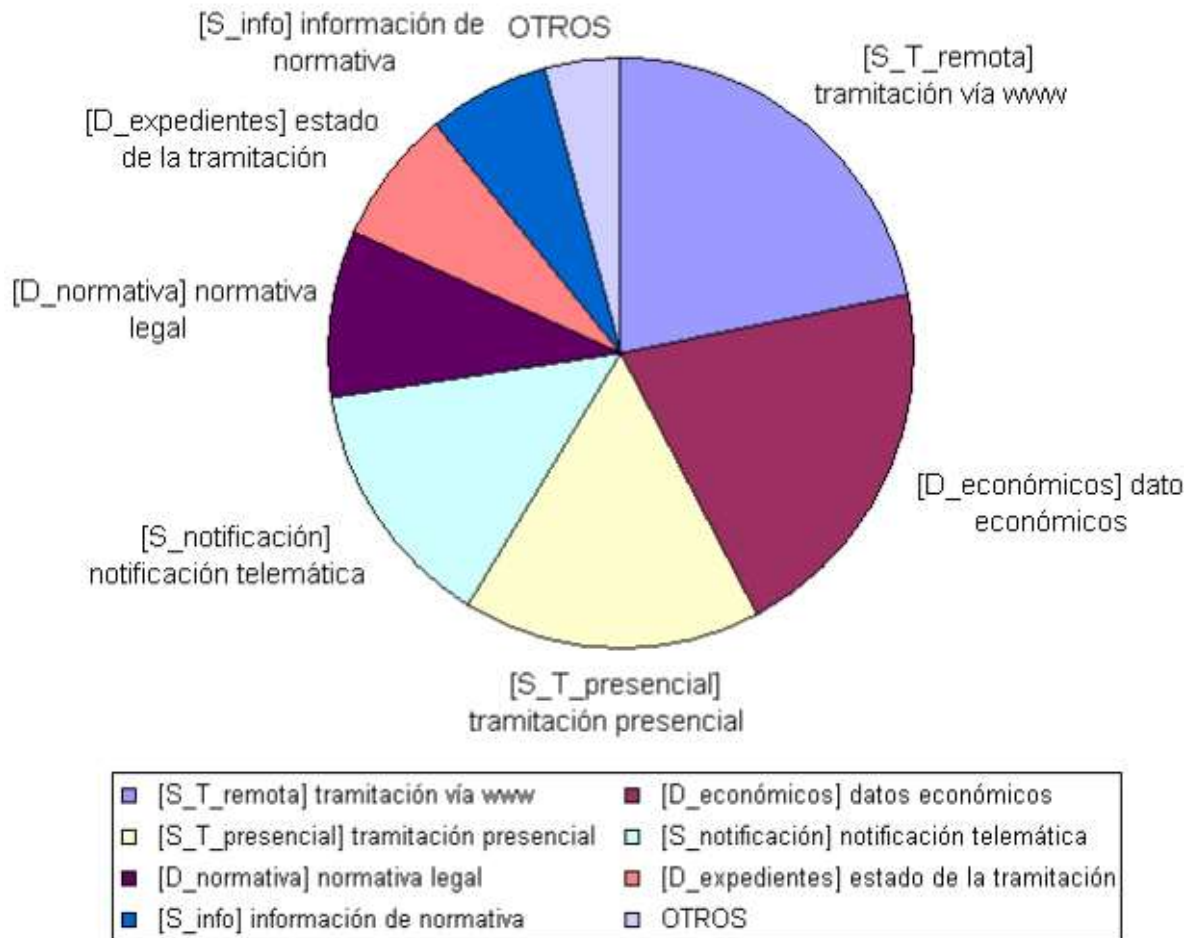
**Figura N° 14: Técnica Gráfica: Gráficos de Radar**  
**Fuente: Magerit- Libro III**

✓ **Diagramas de Pareto**

Una gráfica de Pareto es utilizada para separar gráficamente los aspectos más significativos de un problema que el equipo sepa dónde dirigir sus esfuerzos para mejorar.

✓ **Diagrama de Tarta**

Estos diagramas presentan los datos como fracciones de un círculo, distribuidos los 360° de éste en proporción al valor que es representado en cada sección. La proporción suele ser lineal; rara vez logarítmica.



**Figura N° 15: Técnica Gráfica: Diagrama de Tarta**  
**Fuente: Magerit- Libro III**

### ➤ Sesiones de Trabajo

Las sesiones de trabajo tienen diversos objetivos. Dependiendo del tipo de sesión que se realice, los objetivos pueden ser: obtener información, comunicar resultados, reducir el tiempo de desarrollo, activar la participación de usuarios y directivos o aumentar la calidad de los resultados. Las sesiones de trabajo pueden ser de varios tipos en función de las personas que participen en ellas, el objetivo que se persiga y el modo de llevarlas a cabo.

### ✓ Entrevistas

En proyectos de análisis y gestión de riesgos suelen practicarse entrevistas semi-estructuradas en las que, existiendo un guión preestablecido de preguntas, el entrevistado tiene margen para ex-

tenderse en puntos no previstos o, más frecuentemente, responderlas en un orden diferente al previsto. En cualquier caso el guión se emplea para no olvidar nada.

✓ **Reuniones**

Las reuniones tienen como objetivo obtener información que se encuentra repartida entre varias personas, tomar decisiones estratégicas, tácticas u operativas, transmitir ideas sobre un determinado tema, analizar nuevas necesidades de información, así como comunicar los resultados obtenidos como consecuencia de un estudio.

✓ **Presentaciones**

El objetivo de las presentaciones es la comunicación de avances, conclusiones y resultados por parte del equipo de trabajo al auditorio que corresponda. Se llevan a cabo con el fin de informar sobre el estado de un proyecto en su totalidad o de alguno de los procesos, o exponer uno o varios productos finales de un proceso para su aprobación.

➤ **Valoración Delphi**

Puede ser utilizada con éxito en multitud de campos y sectores. Delphi es especialmente adecuada para Magerit por las razones siguientes:

- ✓ Es una técnica netamente cualitativa que relativamente permite tratar con alta precisión problemas técnicamente complejos.
- ✓ Está planteada como una reflexión organizada de expertos sobre un tema concreto, reflexión que permite recoger las ideas y opiniones más cualificadas en el ámbito de la seguridad (valoración de activos e identificación de amenazas e impactos).
- ✓ Se desarrolla a partir de un cierto \_escenario inicial de modo que permita una adecuada recapitulación e identificación de los problemas que ya existen actualmente.
- ✓ Desarrolla una prospectiva mucho más rica que la mera identificación de la opinión mayoritaria, por medio de un proceso de convergencia de opiniones que se consigue mediante rondas sucesivas de entrevistas.

- ✓ Garantiza satisfactoriamente la limpieza de la investigación, impidiendo el predominio de unos expertos sobre otros por razones ajenas a la calidad de sus opiniones.

La técnica Delphi es un instrumento de uso múltiple que se utiliza con muy variados objetivos:

- ✓ Identificar problemas.
- ✓ Desarrollar estrategias para la solución de problemas, fijando un rango de alternativas posibles.
- ✓ Identificar factores de resistencia en el proceso de cambio.
- ✓ Establecer previsiones de futuro sobre la evolución de las tendencias que se observan en un determinado campo o sector.
- ✓ Contrastar opiniones en un tema abarcando un amplio campo de disciplinas o sectores.



#### IV. **CONCLUSIÓN**

1. Se definió los fundamentos teóricos, tales como concepto de riesgo, amenazas, vulnerabilidades, entre otros; que permiten tener un amplio conocimiento de cómo realizar un análisis de riesgo; así mismo las técnicas existentes que permiten realizar un adecuado análisis de riesgo.
2. Una vez que se realiza el análisis de riesgos, la organización tiene en sus manos una poderosa herramienta para el tratamiento de sus vulnerabilidades y un diagnóstico general sobre el estado de la seguridad de su entorno como un todo. A partir de este momento es posible establecer políticas para la corrección de los problemas ya detectados, y la gestión de seguridad de ellos a lo largo del tiempo, para garantizar que las vulnerabilidades encontradas anteriormente no sean más sustentadas o mantenidas, gestionando de esa manera la posibilidad de nuevas vulnerabilidades que puedan surgir a lo largo del tiempo.
3. Cuando se sabe que las innovaciones tecnológicas son cada vez más frecuentes, aparecen una serie de nuevas oportunidades para que individuos maliciosos se aprovechen de ellas y realicen acciones indebidas en los entornos humanos, tecnológicos, físicos y de procesos.
4. Una vez que se tienen las recomendaciones, se inician las acciones de distribución de ellas para corregir el entorno y reducir los riesgos a que está sometida la infraestructura humana, tecnológica, de procesos y física que respalda a uno o más procesos de negocio de una organización. De esa manera es posible implementar en los activos analizados, y también en los activos de mismas características que los analizados, las medidas de corrección y tratamiento de las vulnerabilidades.
5. Se optó por MAGERIT porque proporciona una metodología sistemática de análisis de riesgos y tratamiento oportuno de estos por medio de salvaguardas, preparando a la compañía para procesos de auditoría, evaluación, certificación y acreditación. La utilización de esta metodología requiere de un proceso empezando por la planificación (donde se establecen los objetivos y recursos necesarios para ejecutar el trabajo), después por el análisis de riesgos (donde se identifican los activos, la relación entre estos y los riesgos asociados a los activos) y finalmente la gestión de riesgos (donde se establecen las salvaguardas, la calidad y eficacia de estas en la mitigación de riesgos).

6. Una vez que los resultados son rastreados y puntuados con relación a su valor crítico y relevancia, uno de los productos finales del análisis de riesgos, la matriz de valor crítico, indica a través de datos cualitativos y cuantitativos la situación de seguridad en que se encuentran los activos analizados, al listar las vulnerabilidades, amenazas potenciales y respectivas recomendaciones de seguridad para corrección de las vulnerabilidades.

## V. REFERENCIAS BIBLIOGRÁFICAS

### Libros Digitales:

- [Guía PMBOK, 2008]  
Fundamentos Para la Dirección de Proyectos, Quinta Edición, 2008, 595 Pág.
- [MAGERIT – versión 3.0]  
Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información  
-  
Libro I, II, III.

### Páginas Web:

- <https://whatisprojectmanagement.wordpress.com/category/gestion-de-los-riesgos/>  
**WHAT IS PROJECT MANAGEMENT?**  
**Project Manager's Essential Guide, by Gladys Gbenedji.**