Gestión de Riesgos

Metodología Gestión Riesgos

S17_s1

Dudas de la sesión anterior

OBJETIVO DE APRENDIZAJE

- Al finalizar la unidad el estudiante conoce la metodología MAGERIT, a través de la explicación de los conceptos y de ejemplos.

Riesgos de SI

Actividad en clase – Grupos

Analizar el video y responder:

1.Los sistemas de información deben protegerse ?

2.que riesgos o amenazas afectan los sistemas de información

https://www.youtube.com/watch?v=WRL-EYW3ncs&ab_channel=JaiverStickGutierrezCerquera

UTILIDAD

¿Qué riesgos enfrentan los sistemas de información?

¿Qué herramientas puede utilizar un auditor para gestionar los riesgos en sistemas de información ?

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

https://www.youtube.com/watch?v=06nKNXLc7pQ&ab_channel=NYCEMX

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

- **El CSAE1**
- ha elaborado y promueve Magerit2 como respuesta a la percepción de que la Administración Pública (y en general toda la sociedad) depende de forma creciente de los sistemas de información para alcanzar sus objetivos.
- **El uso de tecnologías de la información** y comunicaciones (TIC) supone unos beneficios evidentes para los ciudadanos.
- pero también da lugar a ciertos riesgos que deben gestionarse prudentemente con medidas de seguridad que sustenten la confianza de los usuarios de los servicios.

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

- **La gestión de los riesgos**
- es nuclear al gobierno de las organizaciones.
- **los riesgos que tienen su origen en el uso de tecnologías** de la información deben trasladarse a los órganos de gobierno y contextualizarse en la misión de la organización.

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

- Siguiendo la terminología de la normativa ISO 31000, Magerit responde a lo que se denomina "Proceso de Gestión de los Riesgos".
- **MAGERIT implementa el Proceso de Gestión de Riesgos** dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información.
-

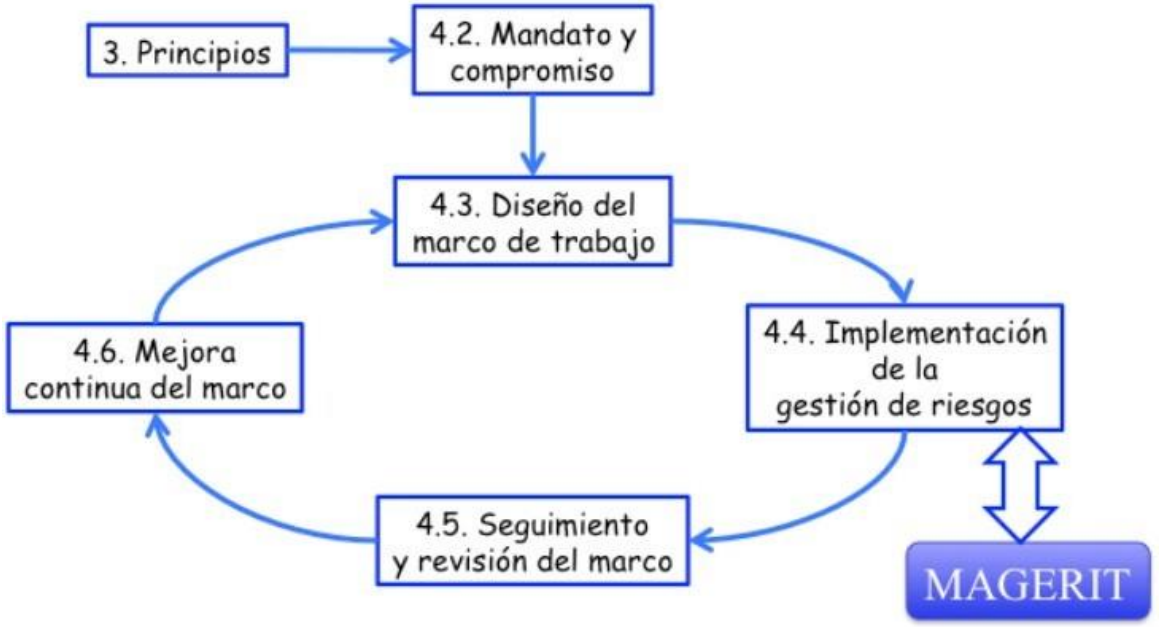


Ilustración 1. ISO 31000 - Marco de trabajo para la gestión de riesgos

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

- Las tareas de análisis y tratamiento de los riesgos no son un fin en sí mismas sino que se encajan en la actividad continua de gestión de la seguridad.
- El análisis de riesgos permite determinar cómo es, cuánto vale y cómo de protegido se encuentra el sistema.
- **En coordinación con los objetivos, estrategia y política de la Organización**, las actividades de tratamiento de los riesgos permiten elaborar un plan de seguridad .
- que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que acepta la Dirección.
- Al conjunto de estas actividades se le denomina Proceso de Gestión de Riesgos.

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

- Los sistemas de gestión de la seguridad de la información (SGSI) [ISO 27001] formalizan cuatro etapas cíclicas:

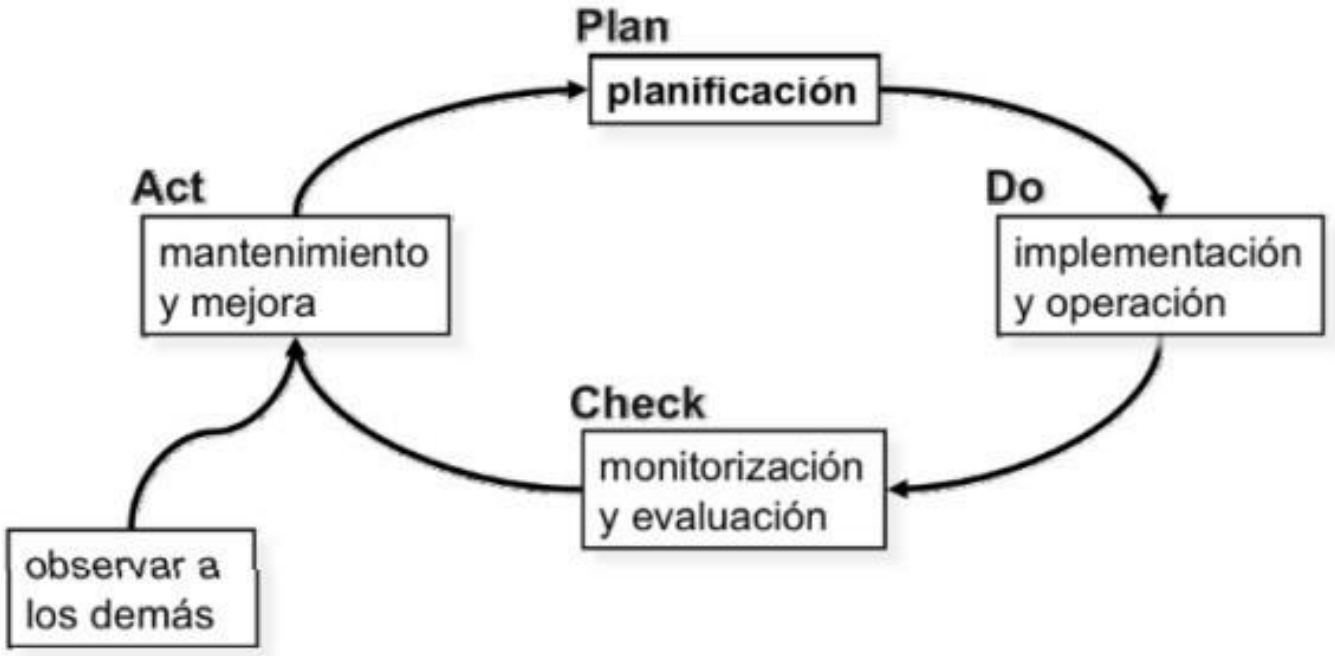


Ilustración 2. Ciclo PDCA

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

- **El análisis de riesgos** es una piedra angular de los procesos de evaluación, certificación, auditoría y acreditación que formalizan la confianza que merece un sistema de información

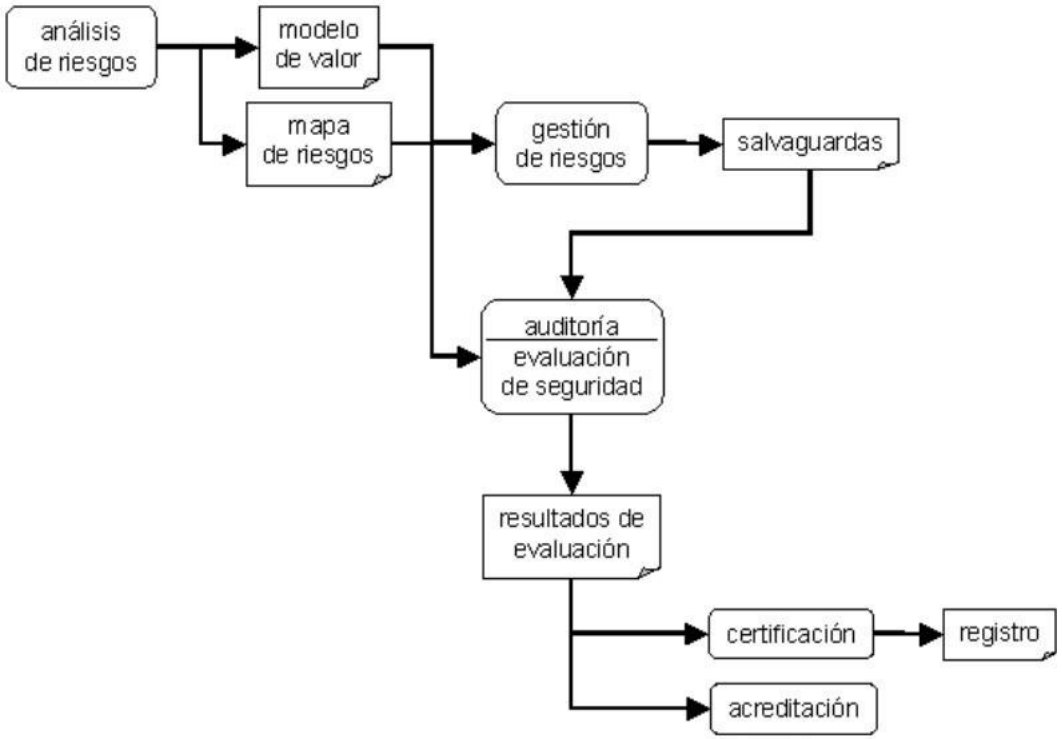


Ilustración 4. Contexto de certificación y acreditación de sistemas de información

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

- **Hay dos grandes tareas a realizar:**
- **I. análisis de riesgos**
- que permite determinar qué tiene la Organización y estimar lo que podría pasar.
- **II. tratamiento de los riesgos**
- que permite organizar la defensa concienzuda y prudente, defendiendo para que no pase nada malo y al tiempo estando preparados para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones.

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

- XXXX

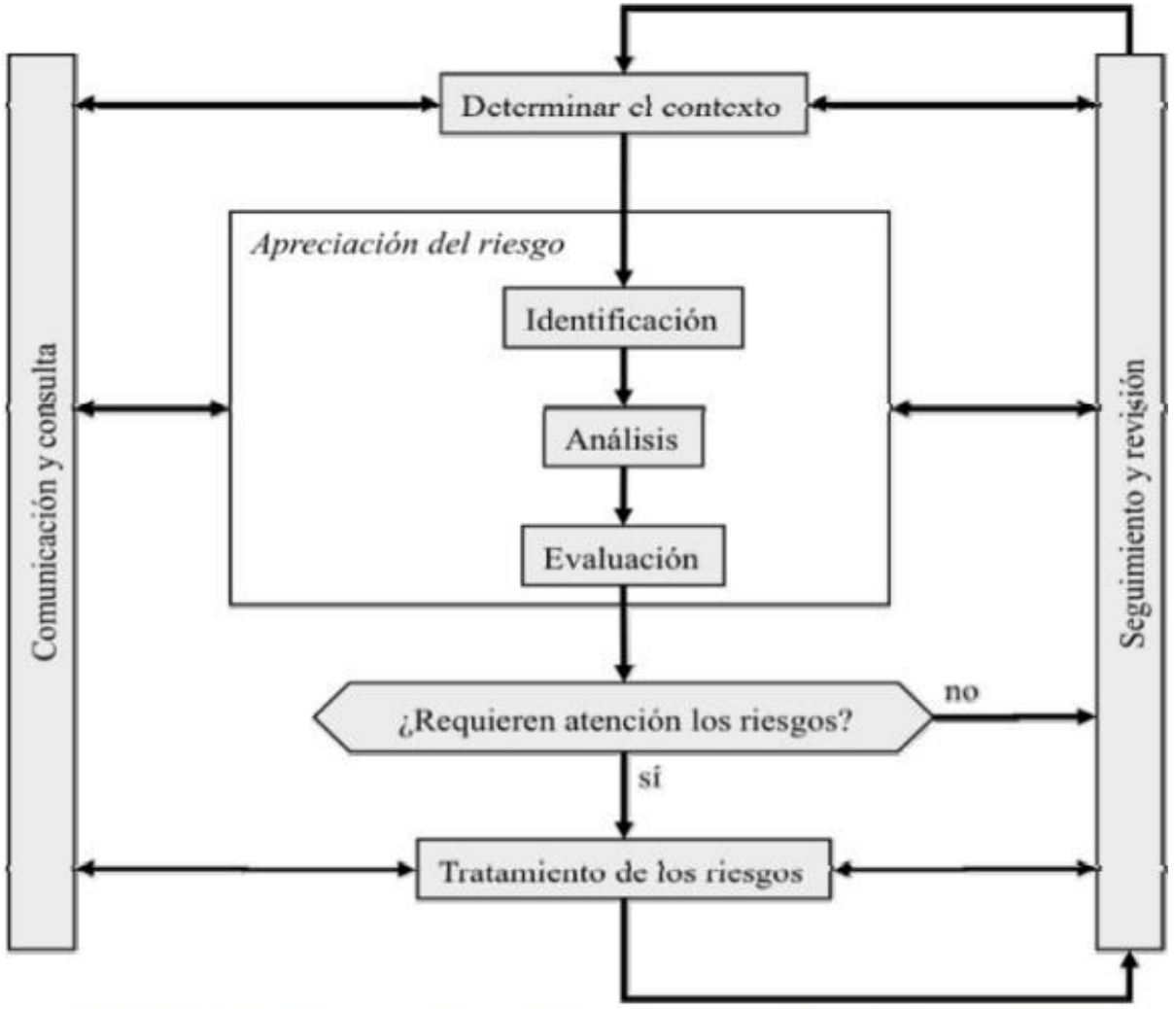


Ilustración 6. Proceso de gestión de riesgos (fuente: ISO 31000)

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

- **Método de análisis de riesgos**
- **1. determinar los activos relevantes para la Organización**, su interrelación y su valor, en el sentido de qué perjuicio (coste) supondría su degradación.
- **2. determinar a qué amenazas** están expuestos aquellos activos.
- **3. determinar qué salvaguardas** hay dispuestas y cuán eficaces son frente al riesgo.
- **4. estimar el impacto,** definido como el daño sobre el activo derivado de la materialización de la amenaza.
- **5. estimar el riesgo,** definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

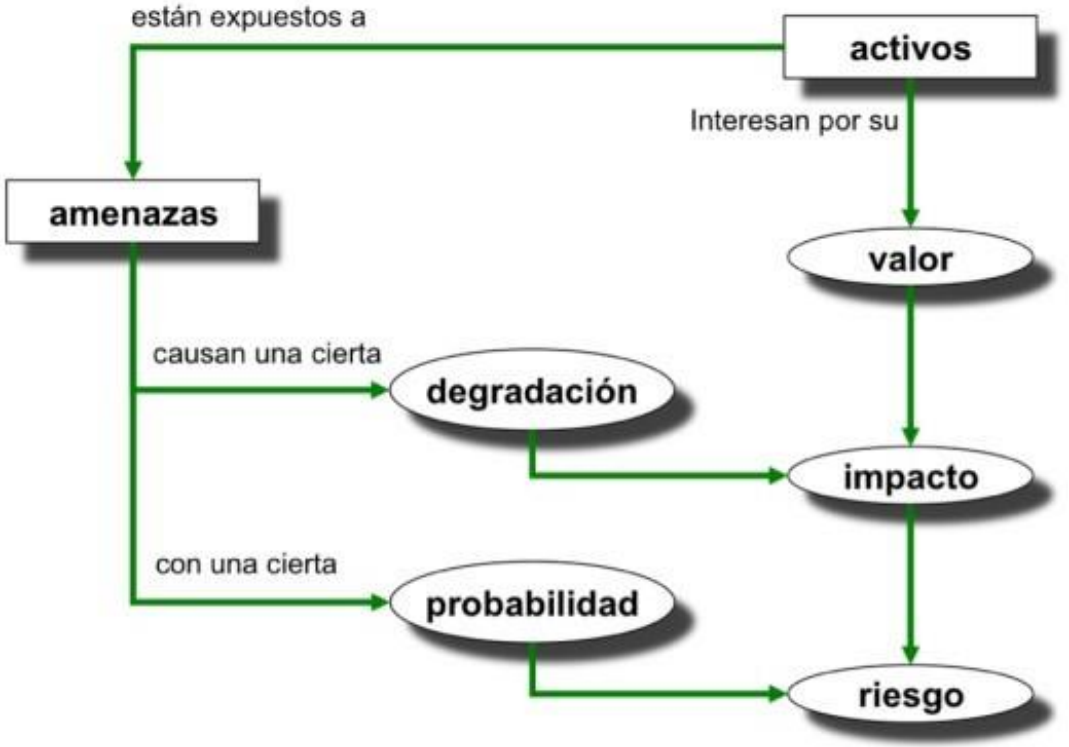


Ilustración 7. Elementos del análisis de riesgos potenciales

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

El análisis de riesgos considera los siguientes elementos:

activos, que son los elementos del sistema de información (o estrechamente relacionados con este) que soportan la misión de la Organización
amenazas, que son cosas que les pueden pasar a los activos causando un perjuicio a la Or-ganización

salvaguardas (o contra medidas), que son medidas de protección desplegadas para que aquellas amenazas no causen [tanto] daño.

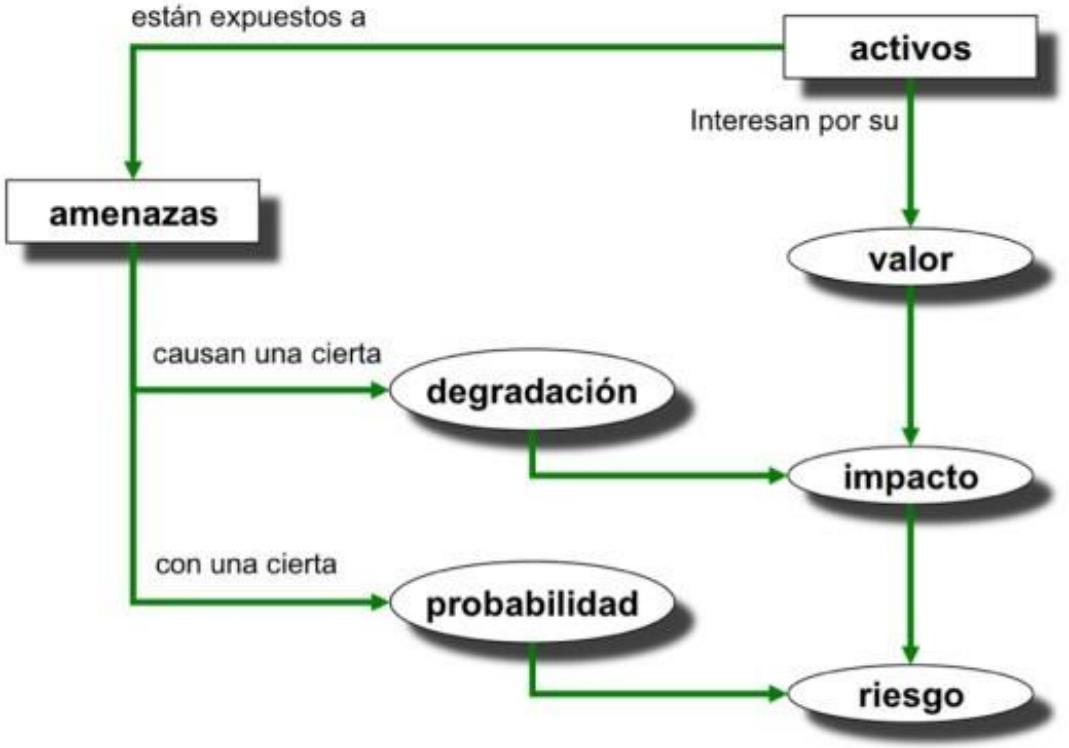


Ilustración 7. Elementos del análisis de riesgos potenciales

Con estos elementos se puede estimar:

el impacto: lo que podría pasar

el riesgo: lo que probablemente pase

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

El análisis de riesgos considera los siguientes elementos:

activos, que son los elementos del sistema de información (o estrechamente relacionados con este) que soportan la misión de la Organización

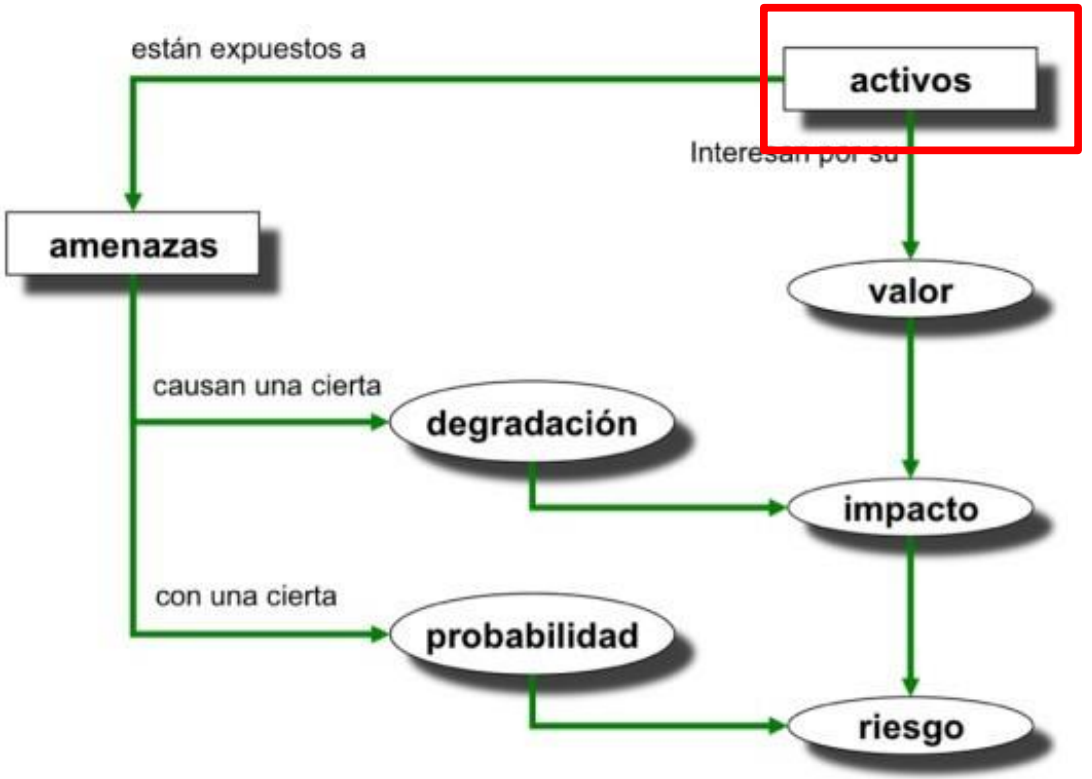


Ilustración 7. Elementos del análisis de riesgos potenciales

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

El análisis de riesgos considera los siguientes elementos:

Valoración:

La valoración se puede ver desde la perspectiva de la 'necesidad de proteger' pues cuanto más valioso es un activo, mayor nivel de protección requeriremos en la dimensión (o dimensiones) de seguridad que sean pertinentes.

El valor puede ser propio, o puede ser acumulado. Se dice que los activos inferiores en un es-quema de dependencias, acumulan el valor de los activos que se apoyan en ellos.

El valor nuclear suele estar en la información que el sistema maneja y los servicios que se prestan (activos denominados esenciales), quedando los demás activos subordinados a las necesidades de explotación y protección de lo esencial.

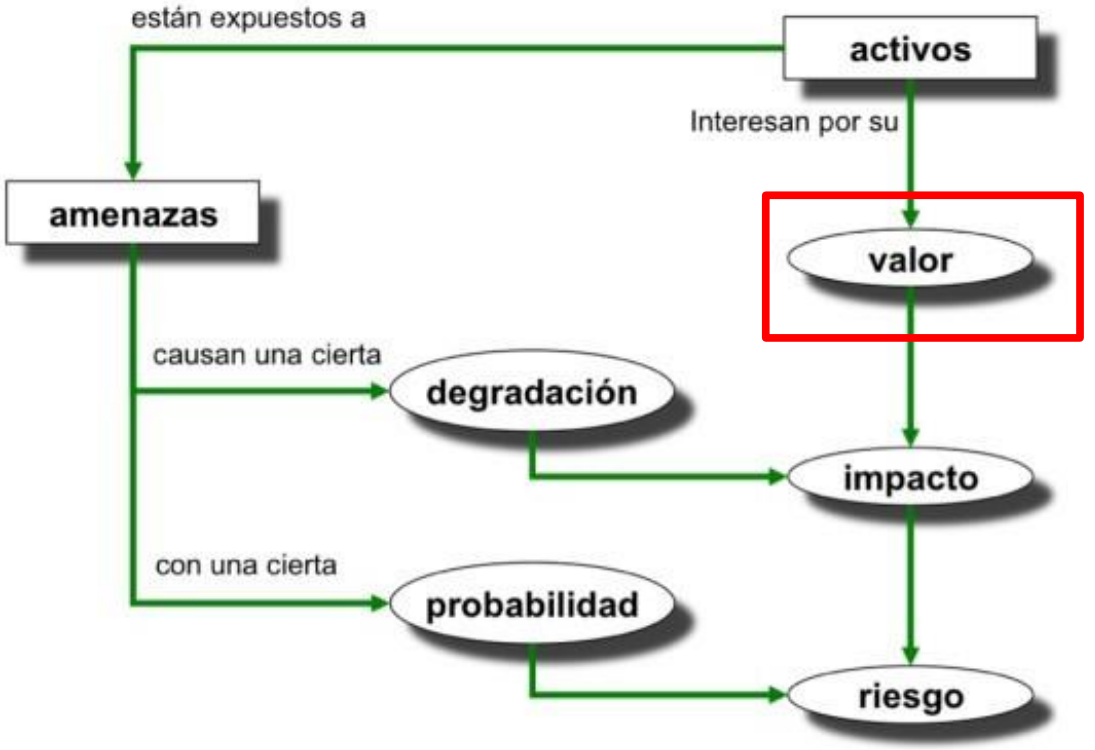


Ilustración 7. Elementos del análisis de riesgos potenciales

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

El análisis de riesgos considera los siguientes elementos:

Amenazas:

Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008] .

Ilustración 7. Elementos del análisis de riesgos potenciales

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

El análisis de riesgos considera los siguientes elementos:

Impacto potencial:

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza.

Conociendo el valor de los activos (en varias dimensiones) **y la degradación que causan las amenazas**, es directo derivar el impacto que estas tendrían sobre el sistema.

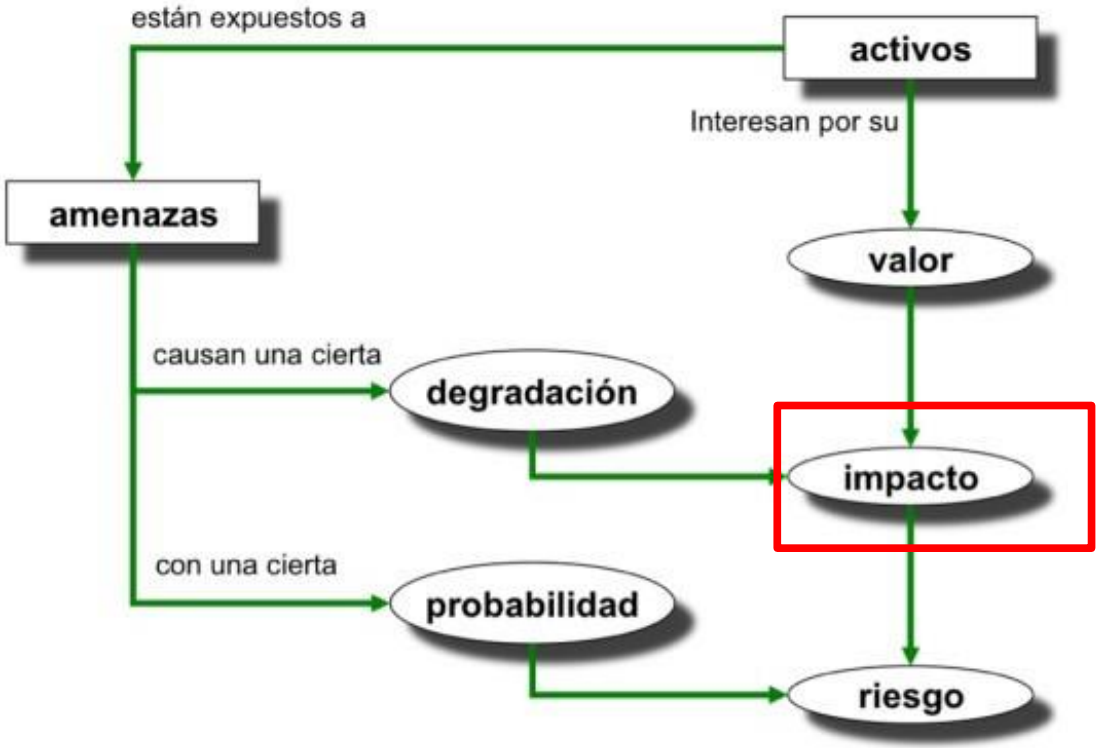


Ilustración 7. Elementos del análisis de riesgos potenciales

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

..

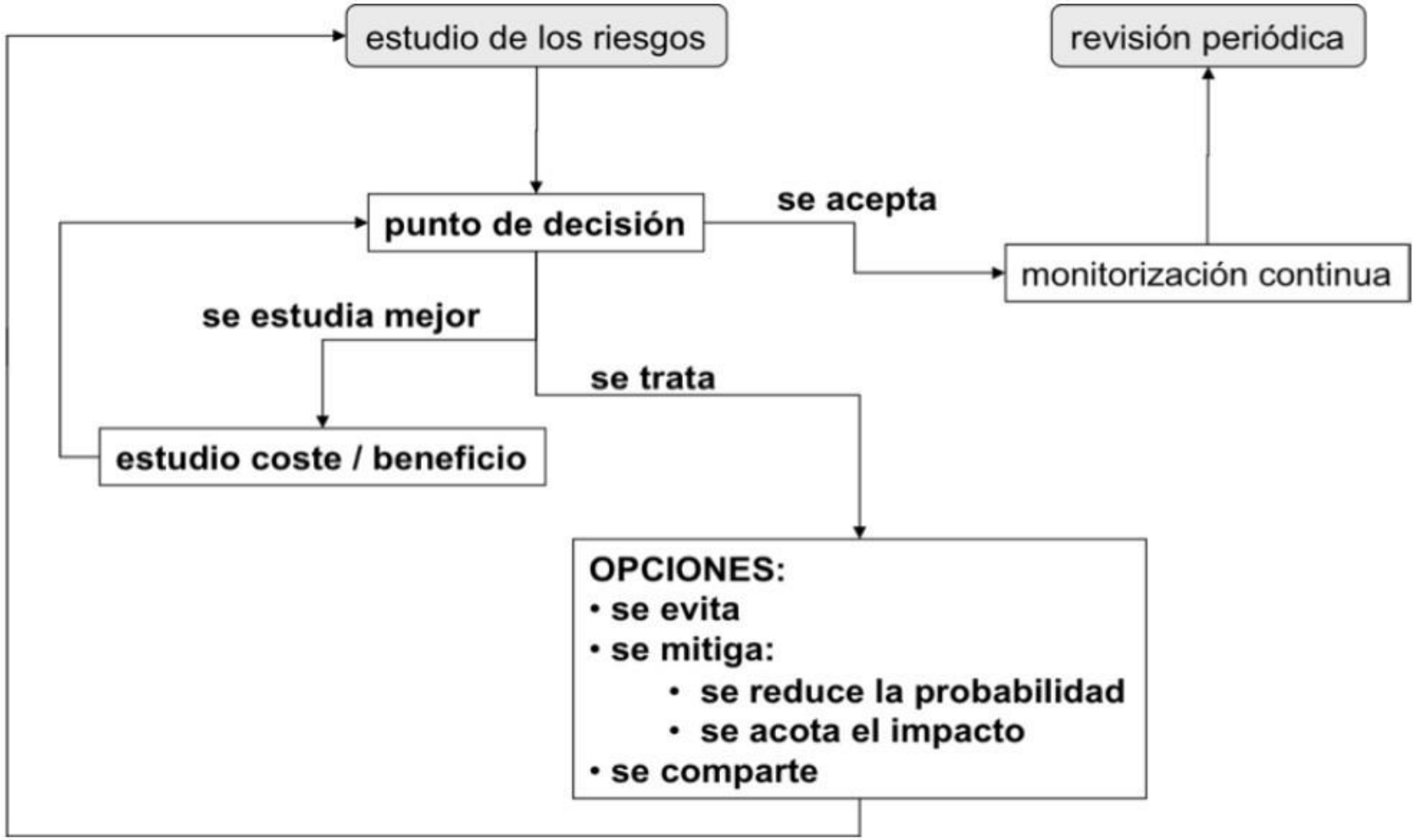


Ilustración 11. Decisiones de tratamiento de los riesgos

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

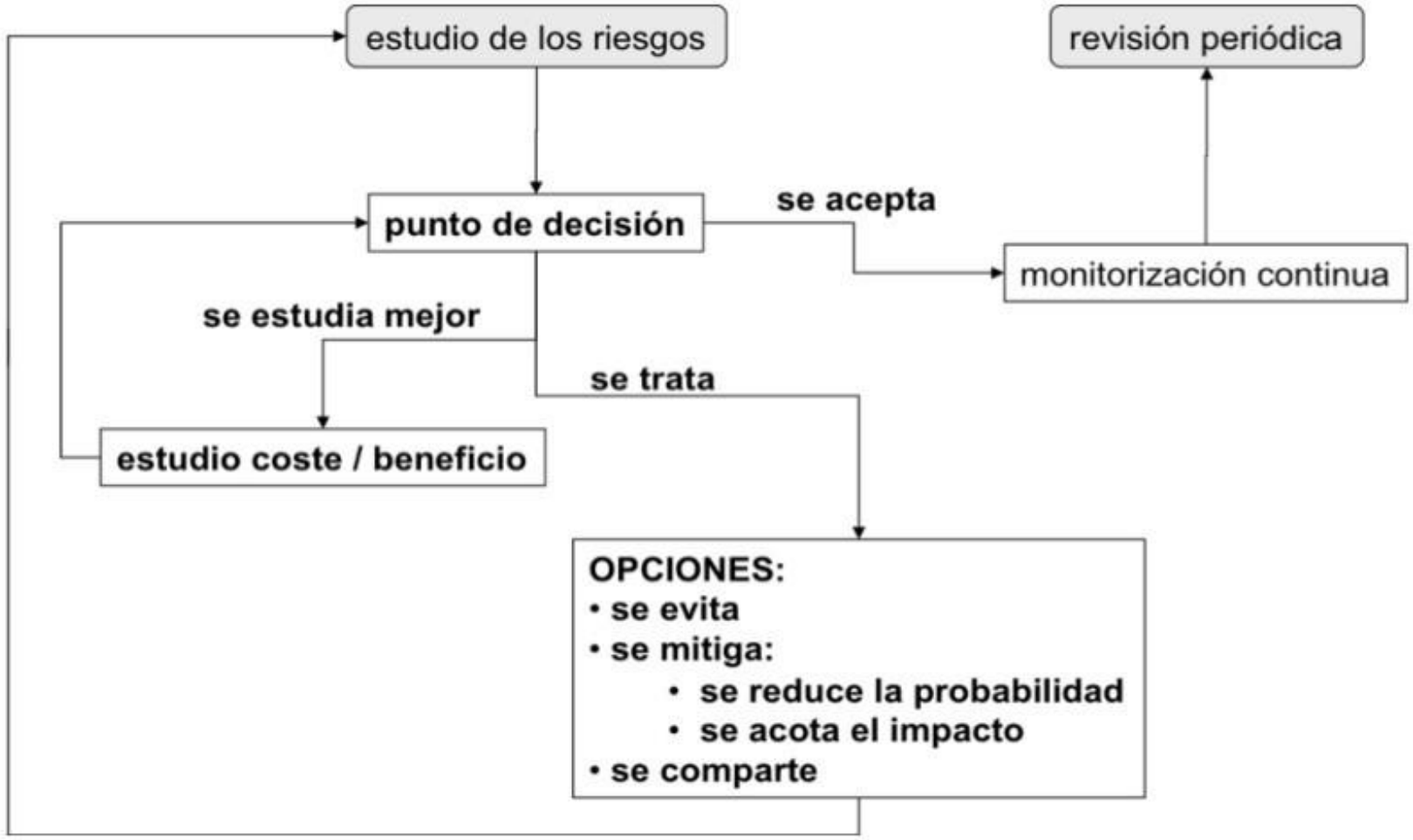


Ilustración 11. Decisiones de tratamiento de los riesgos

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

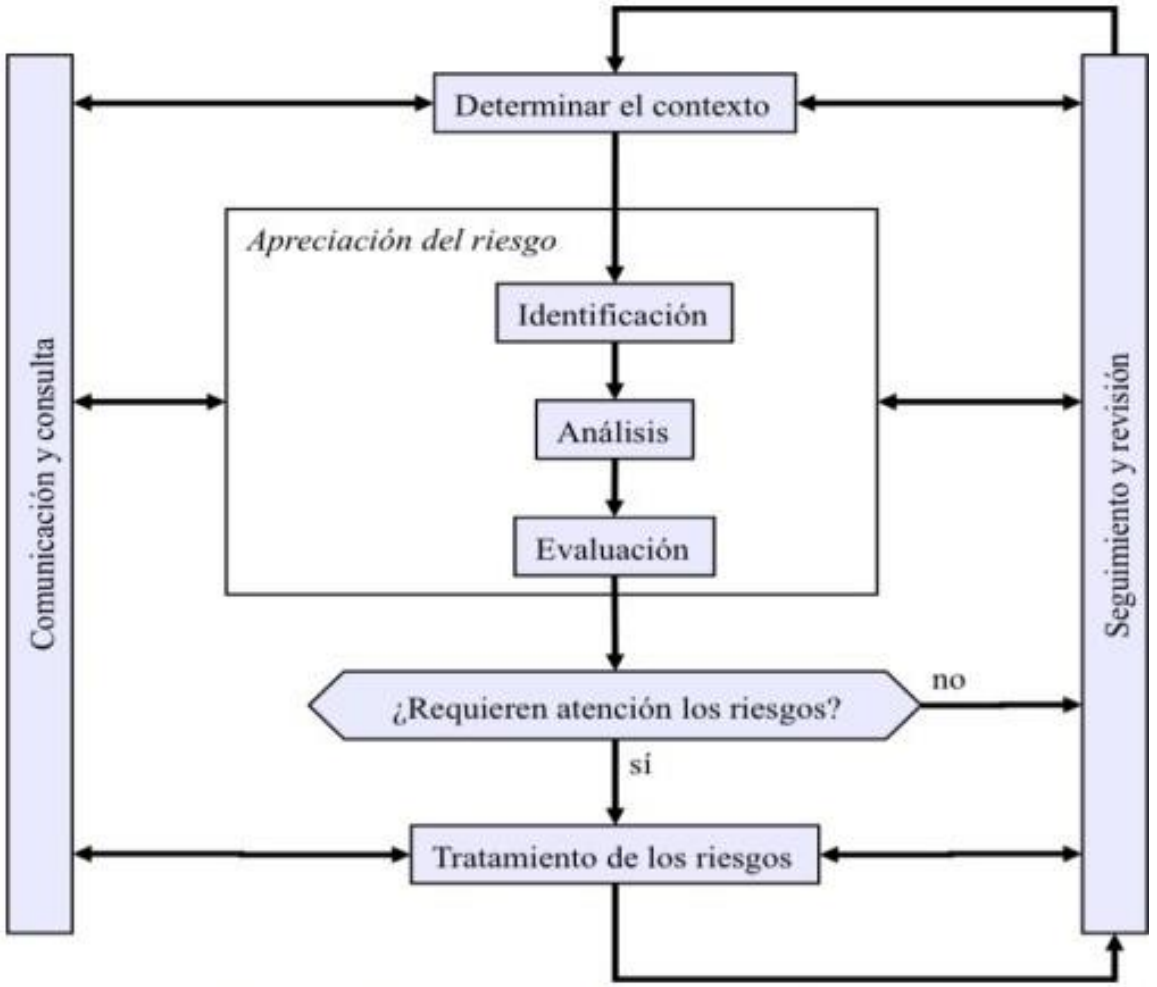
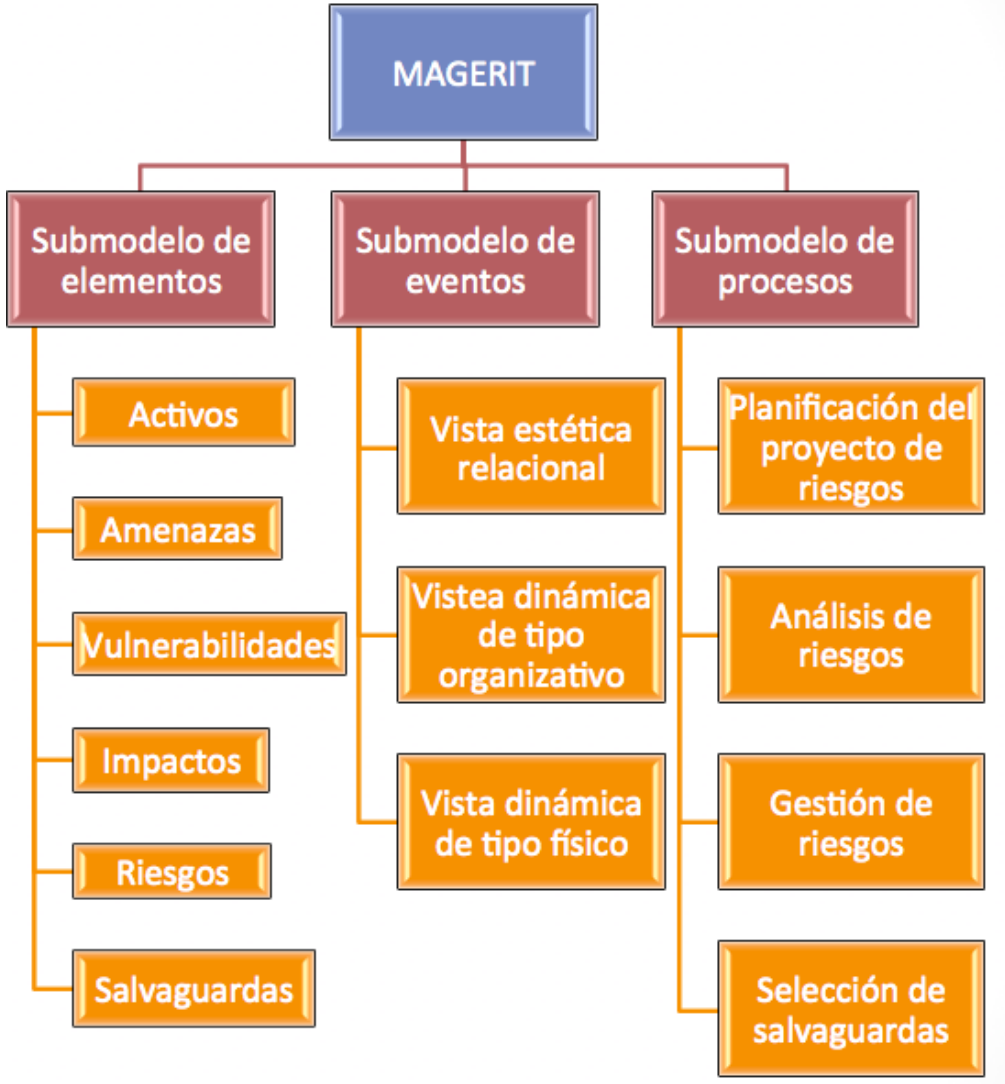


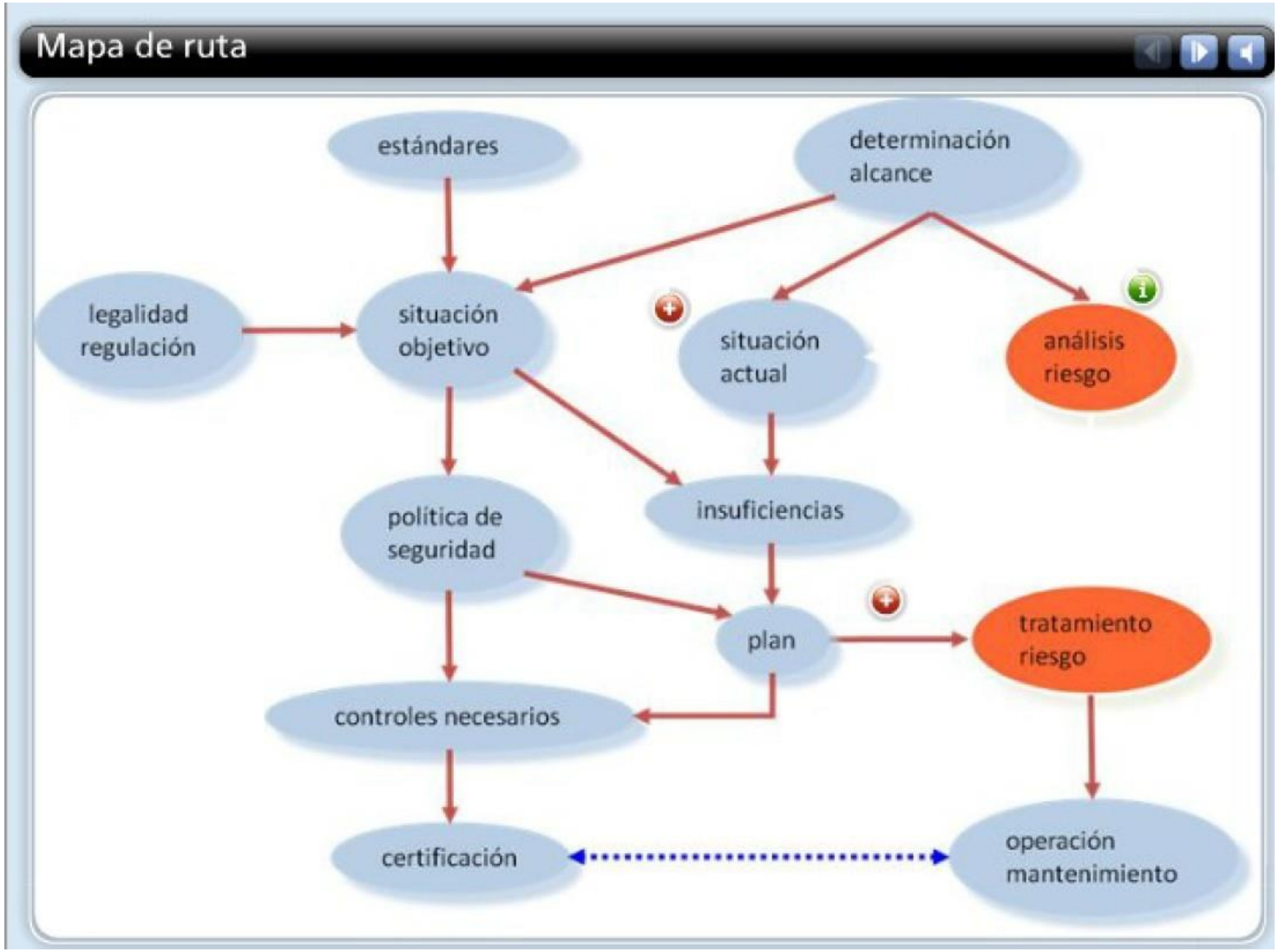
Ilustración 15. Proceso de gestión de riesgos

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

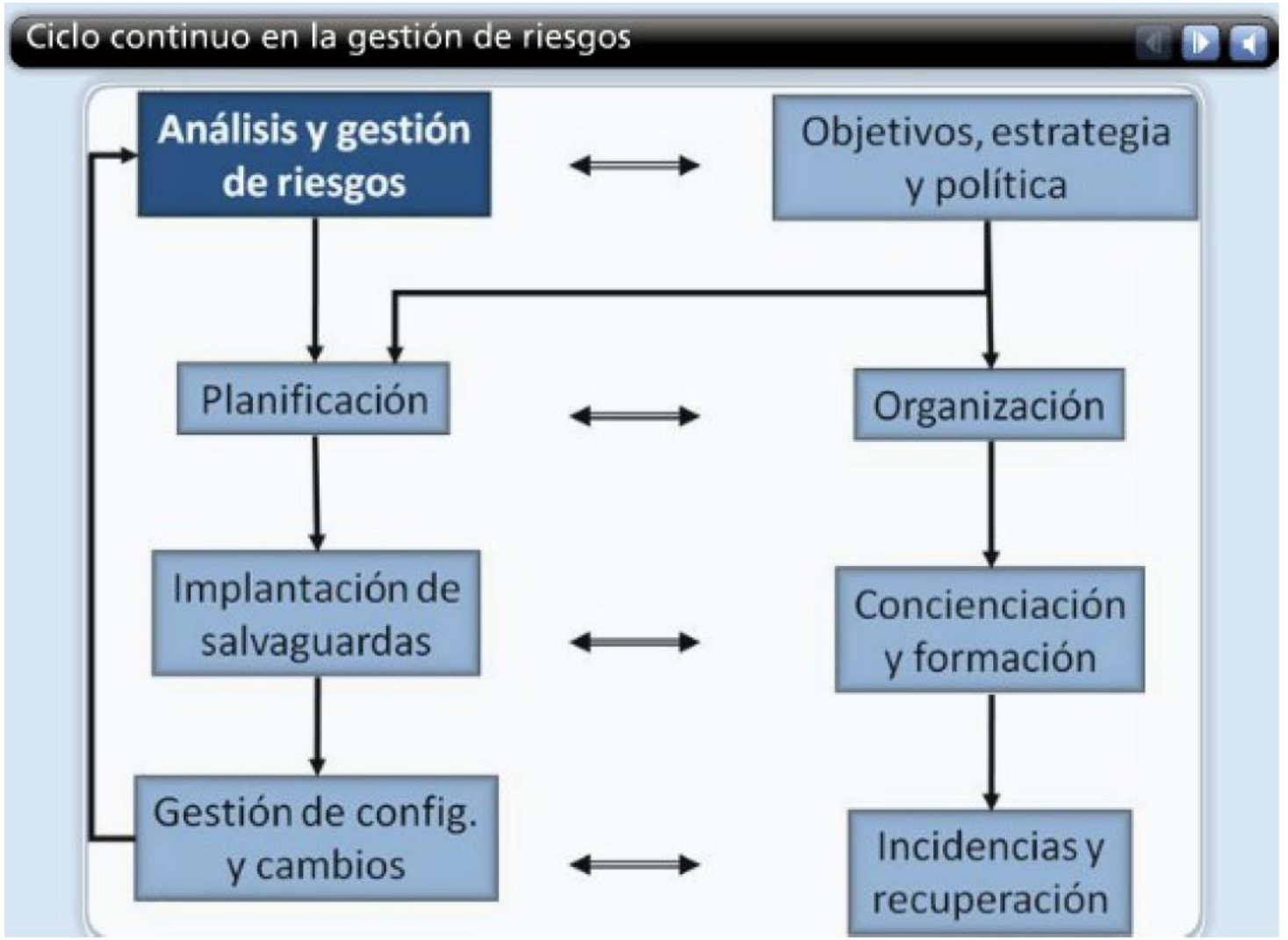


Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

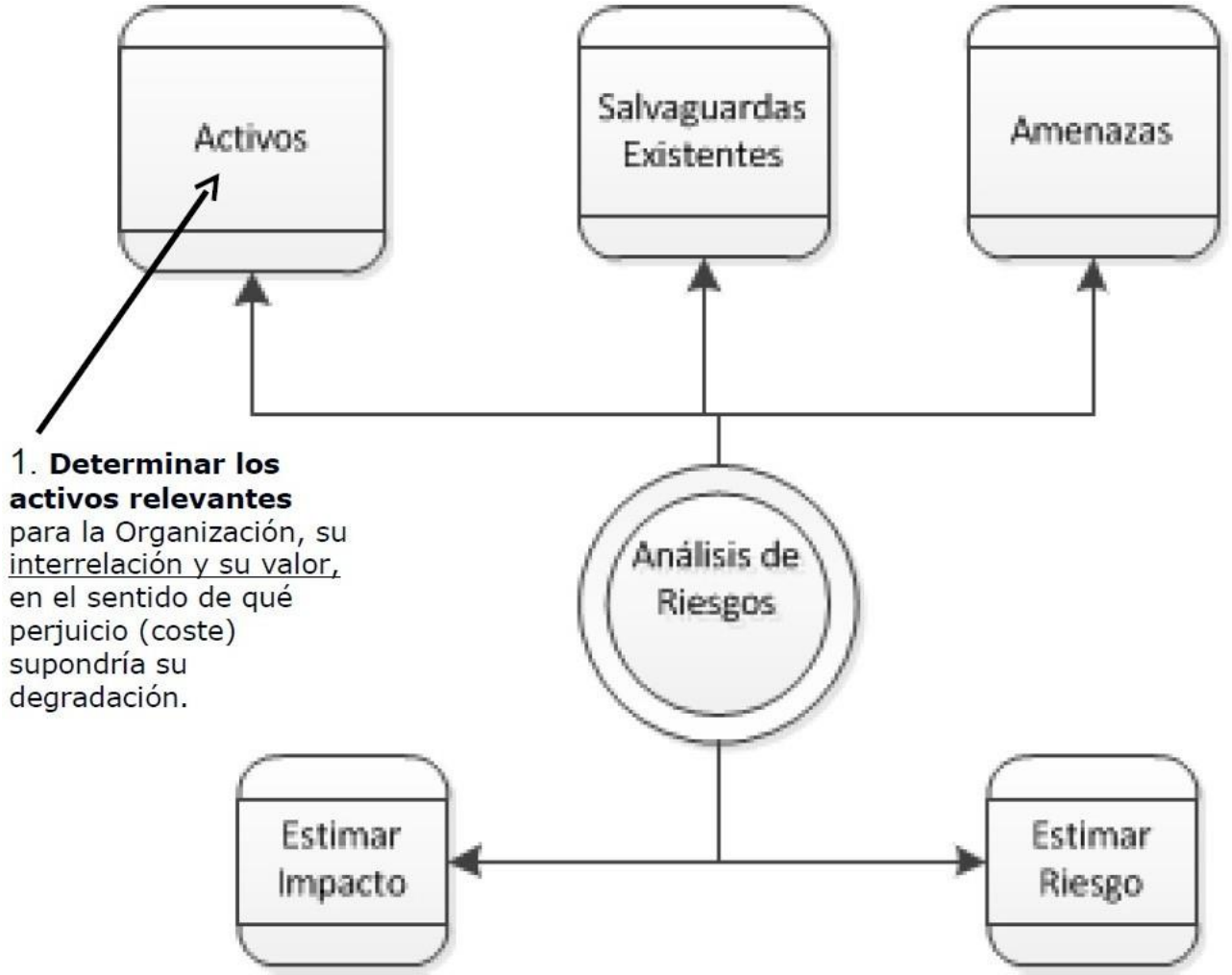
Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información



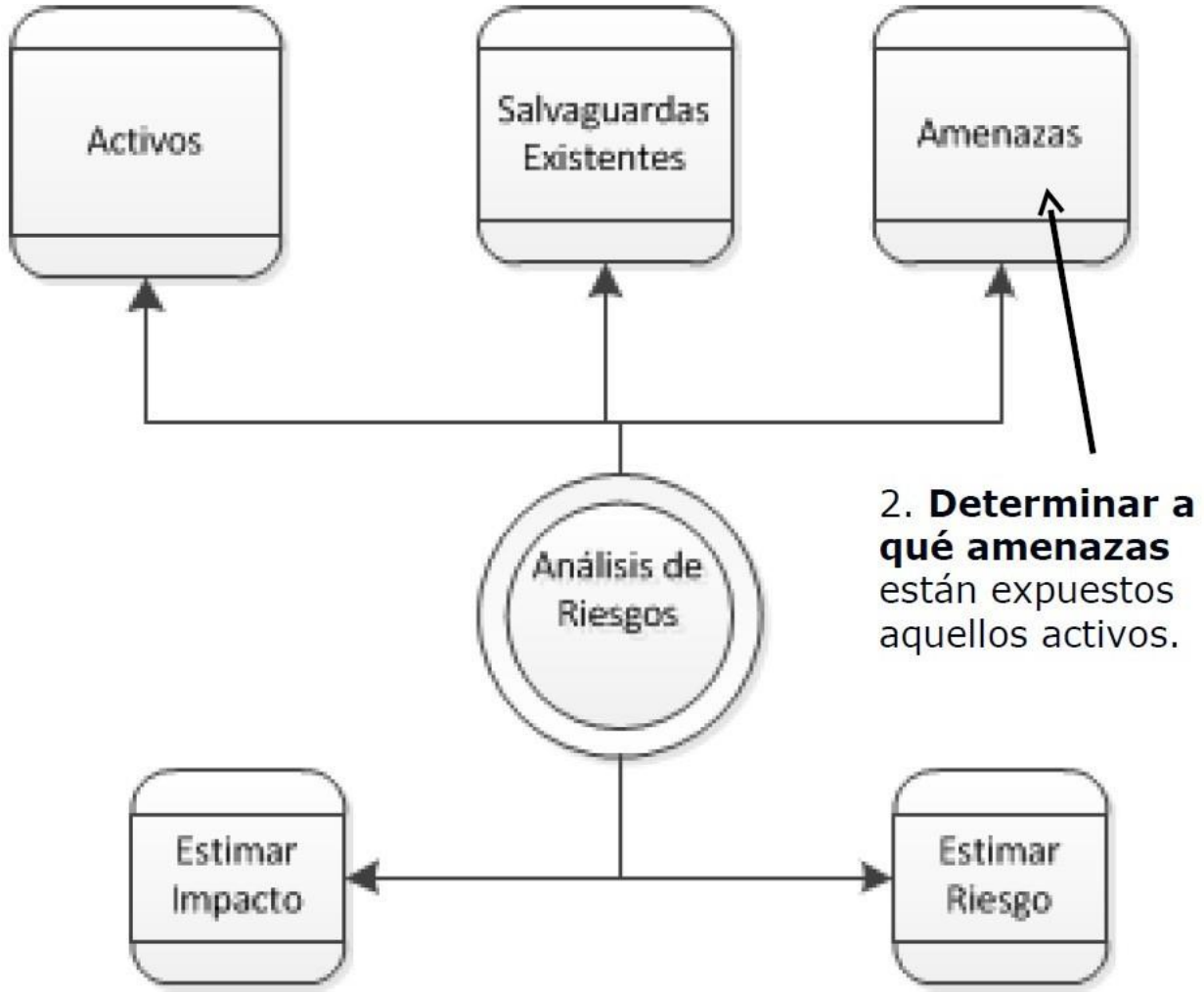
Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

- 

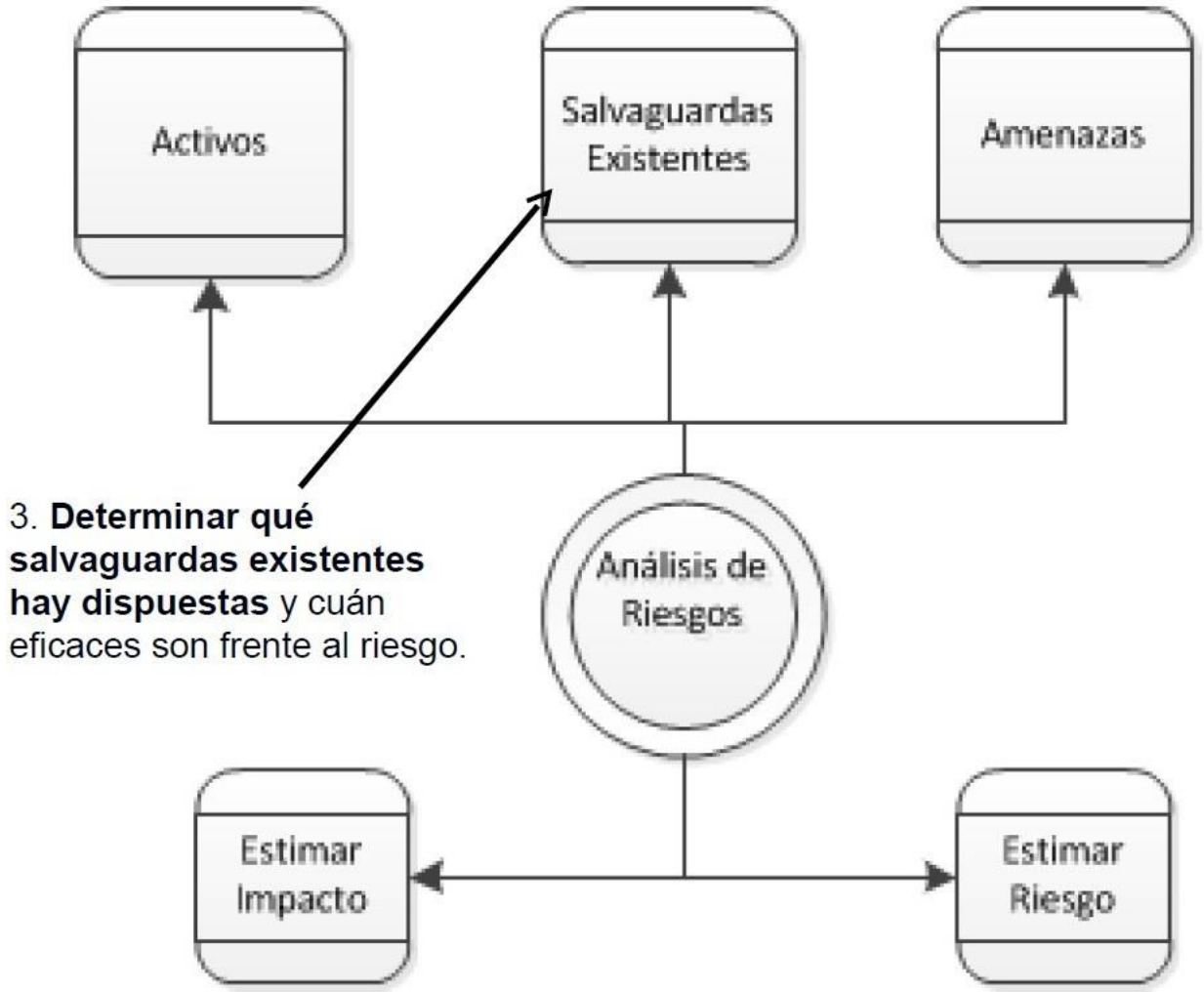
Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información



Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

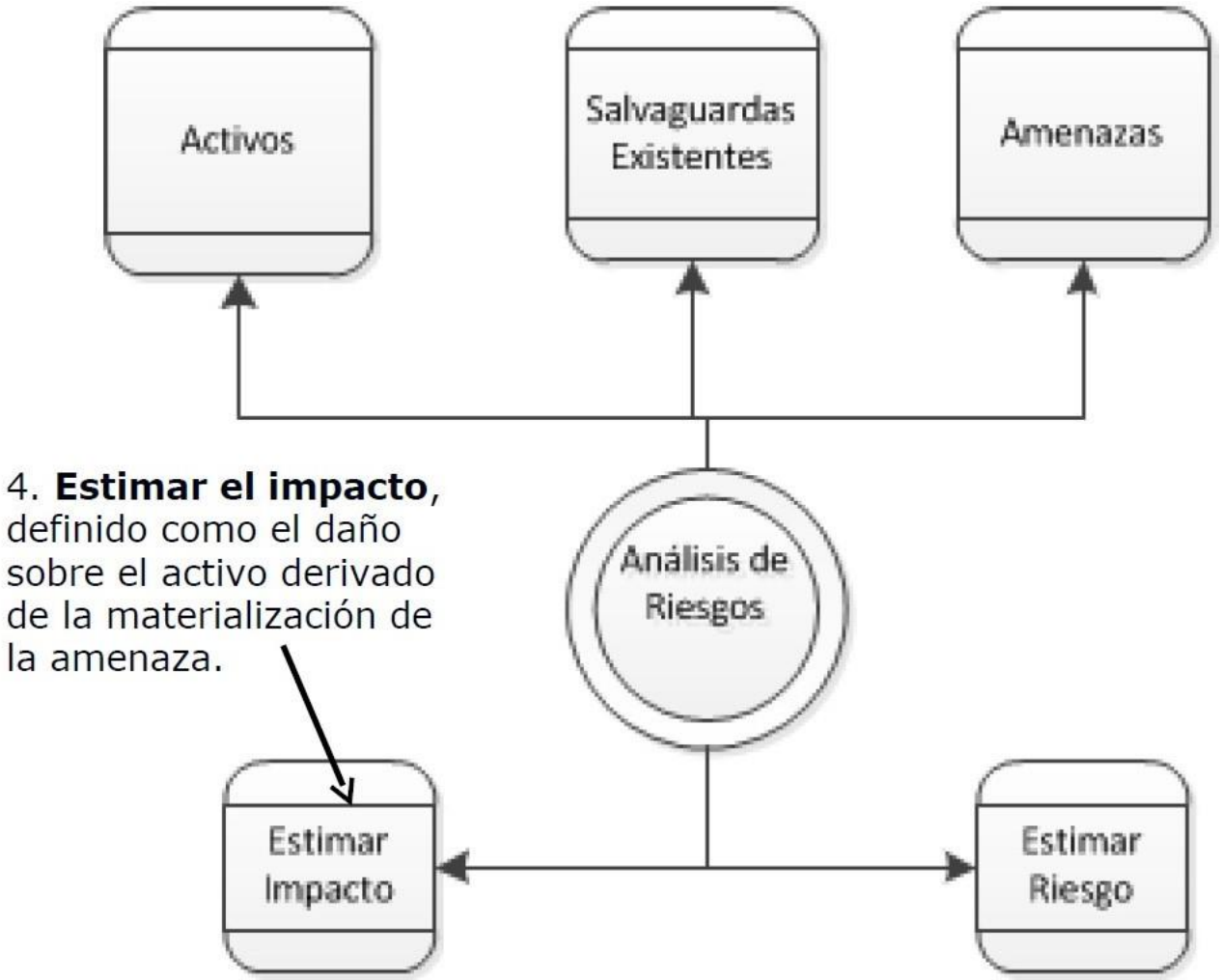


Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

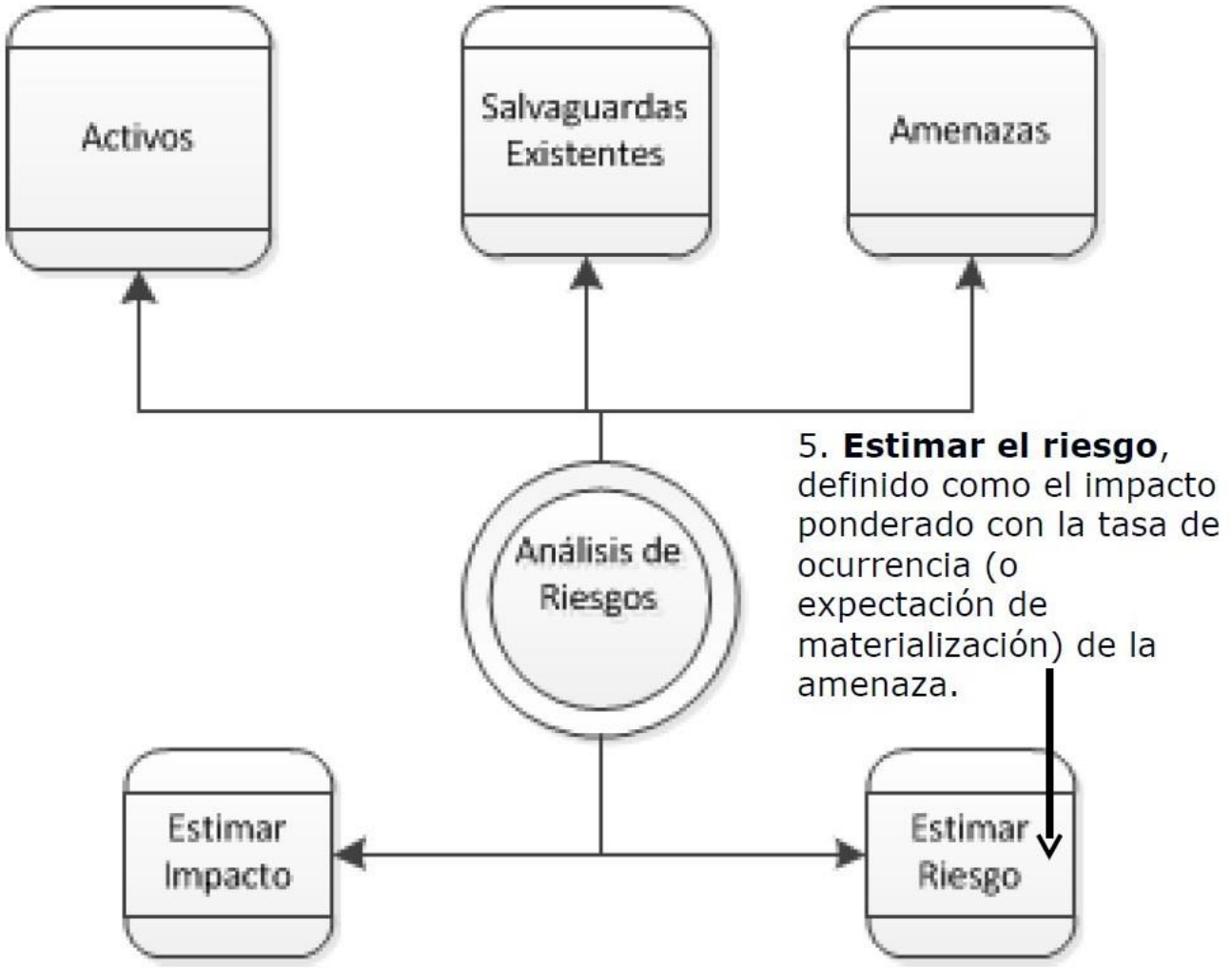


3. **Determinar qué salvaguardas existentes hay dispuestas** y cuán eficaces son frente al riesgo.

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información



Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información



Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

-

4.4. Indicadores de control del proceso de gestión de riesgos

√	actividad	tarea
	Se han definido los roles y responsabilidades respecto de la gestión de riesgos	4.2.1
	Se ha establecido el contexto de gestión de riesgos	4.2.2
	Se han establecido los criterios de valoración de riesgos y toma de decisiones de tratamiento	4.2.3
	Se han interpretado los riesgos residuales en términos de impacto en el negocio o misión de la Organización	4.2.4
	Se han identificado y valorado opciones de tratamiento de los riesgos residuales (propuesta de programas de seguridad)	4.2.5
	Los órganos de gobierno han adoptado una propuesta de tratamiento — evitar el riesgo — prevenir: mitigar la probabilidad de que ocurra — mitigar el impacto si ocurriera — compartir el riesgo con un tercero — asumir el riesgo	4.2.5
	Se han previsto recursos para acometer el plan de seguridad	4.2.5

Conclusiones

- Los procesos de auditoria deben tener en cuenta la evaluación de los riesgos de los sistemas de información
- Se debe utilizar un enfoque o metodología que tengas buenas practicas de la industria como MAGERIT.

Pongamos en Práctica lo aprendido

Universidad Tecnológica del Perú

Universidad
Tecnológica
del Perú