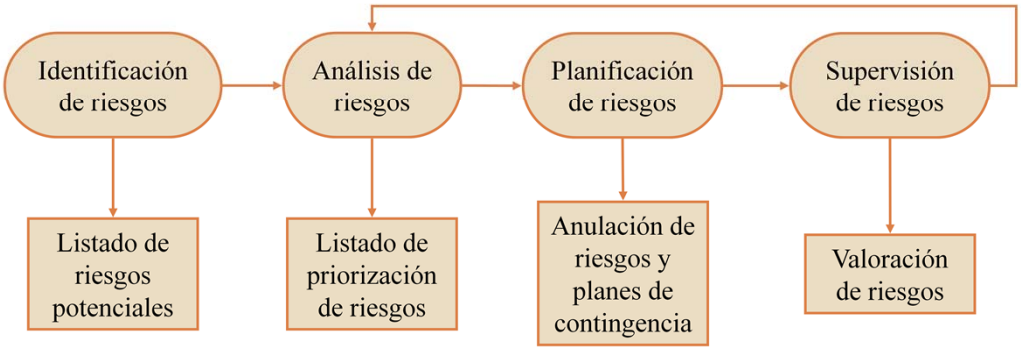
Modelo en Espiral

- Administración del riesgo:



Modelo en Espiral: análisis de riesgos

DEFINICIONES:

- **Activos,** son los elementos del sistema de información que soportan la misión de la Organización
- **Amenazas,** que son cosas que les pueden pasar a los activos causando un perjuicio a la Organización
- **Salvaguardas** (o contramedidas), que son medidas de protección desplegadas para que aquellas amenazas no causen [tanto] daño

Auditoría de Sistemas y Calidad del Software

Metodología de Magerit

Activos: Datos, Servicios, Software, Hardware, BD, Redes de comunicaciones, Instalaciones (CPD), Personas, .

Modelo en Espiral: análisis de riesgos

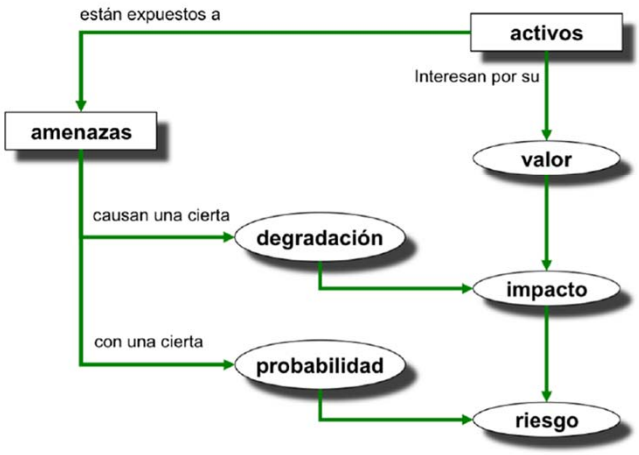
DEFINICIONES:

- **Riesgo:** estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.
- **Análisis de riesgos:** proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.
- **Proceso de gestión/administración de riesgos:** proceso destinado a modificar el riesgo.

Análisis del Riesgo: cap. 3, libro I de MAGERIT

Proceso de gestión de riesgos (cap 4, libro II) de MAGERIT

Modelo en Espiral: análisis de riesgos



MAGERIT *Elementos del análisis de riesgos potenciales*

Pag. 22, Magerit 3.0

Modelo en Espiral: análisis de riesgos

- ACTIVOS: La información y/o los servicios:
  - **Los soportes de información** que son dispositivos de almacenamiento de datos.
  - **El equipamiento auxiliar** que complementa el material informático.
  - **Las redes de comunicaciones** que permiten intercambiar datos.
  - **Las instalaciones** que acogen equipos informáticos y de comunicaciones.
  - **Las personas** que explotan u operan todos los elementos anteriormente citados.

Modelo en Espiral: análisis de riesgos

- Dimensiones de la información:
  - su **confidencialidad**: ¿qué daño causaría que lo conociera quien no debe? Esta valoración es típica de datos.
  - su **integridad**: ¿qué perjuicio causaría que estuviera dañado o corrupto? Esta valoración es típica de los datos, que pueden estar manipulados, ser total o parcialmente falsos o, incluso, faltar datos.
  - su **disponibilidad**: ¿qué perjuicio causaría no tenerlo o no poder utilizarlo? Esta valoración es típica de los servicios

Modelo en Espiral: análisis de riesgos

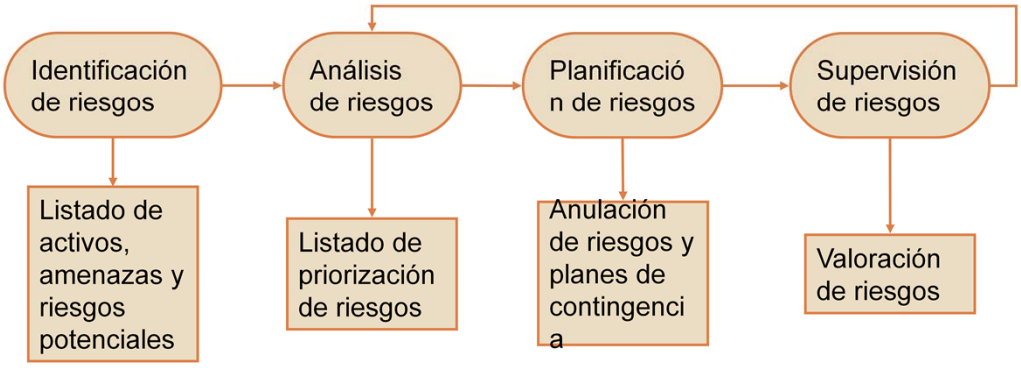
- Dimensiones de los servicios:
  - la **autenticidad:** ¿qué perjuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
  - la **trazabilidad** del uso del servicio: ¿qué daño causaría no saber a quién se le presta tal servicio? Es decir, ¿quién hace qué y cuándo?
  - la **trazabilidad** del acceso a los datos: ¿qué daño causaría no saber quién accede a qué datos y qué hace con ellos?

Modelo en Espiral: análisis de riesgos

- Amenaza: Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008]
- Tipos:
  - De origen natural
  - Del entorno (de origen industrial)
  - Defectos en las aplicaciones
  - Causadas por las personas de forma accidental
  - Causadas por las personas de forma deliberada

Modelo en Espiral: análisis de riesgos

- Administración del riesgo:



Modelo en Espiral: análisis de riesgos

- Administración del riesgo:
  - Identificar los riesgos.
    - Determinar los activos relevantes para la organización
    - Determinar a que amenazas están expuestos dichos activos
    - Definir el riesgo como la probabilidad de un activo esté expuesto a una amenaza.
    - Clasificación en taxonomías. ***Sommerville 2005, Technical Reports SEI***
      - Del proyecto afectan a la calendarización o recursos.
      - Del producto afectan a la calidad o desempeño del software
      - Del negocio afectan a la organización responsable del desarrollo
  - Análisis de riesgos
    - Para cada riesgo, evaluamos la probabilidad de que ocurra (baja, moderada, alta...) y sus consecuencias (impacto o degradación) (Catastrófico, serio, tolerable...)
  - Planificación del riesgo
    - Estrategias para la administración de riesgos: Estrategias de prevención, Estrategias de minimización, planes de contingencia y transferencia
  - Gestión de riesgos
    - Supervisión del proyecto en base a indicadores asociados a cada riesgo, para la detección temprana del mismo, minimizando sus daños, con tareas previstas en caso de aparición

Ingeniería del Software

Pressman 97 5ª ed.

Sommerville 7, 95

Sommerville 9, 595

Practica de Riesgos- CV Espiral

- Administración del riesgo:
  - Identificar los riesgos.
    - Del **proyecto** afectan a la calendarización o recursos.
    - Del **producto** afectan a la calidad o desempeño del software
    - Del **negocio** afectan a la organización responsable del desarrollo
  - Clasificación en taxonomías. ***Sommerville 2005, Technical Reports SEI***
    - ***Tecnología, Personal, Organizacionales, Herramientas, Requerimientos, Estimación***

Practica de Riesgos- CV Espiral

- Administración del riesgo:
  - Identificar los riesgos.
  - Análisis de riesgos
    - Para cada riesgo, evaluamos:
      - la probabilidad de que ocurra:
        - Baja
        - Moderada
        - Alta
      - sus consecuencias:
        - Catastrófico
        - Serio
        - Tolerable
        - Insignificante

Practica de Riesgos- CV Espiral

- Administración del riesgo:
  - Identificar los riesgos.
  - Análisis de riesgos
  - Planificación del riesgo
    - Estrategias para la administración de riesgos:
      - Estrategias de prevención: Reducción de la probabilidad de aparición
      - Estrategias de minimización: Reducción del impacto
      - Planes de contingencia: Estrategia a seguir una vez que se ha dado la situación de riesgo analizada
      - Transferencia: Transferir el riesgo a través de la asunción de un coste

Practica de Riesgos- CV Espiral

- Administración del riesgo:
  - Identificar los riesgos.
  - Análisis de riesgos
  - Planificación del riesgo
  - Gestión de riesgos
    - Supervisión del proyecto para la detección temprana de los riesgos, minimizando sus daños, con tareas previstas en caso de aparición
    - Búsqueda de indicios que presupongan la aparición de un riesgo
    - Análisis continuo de la probabilidad de aparición y efecto sobre el proyecto