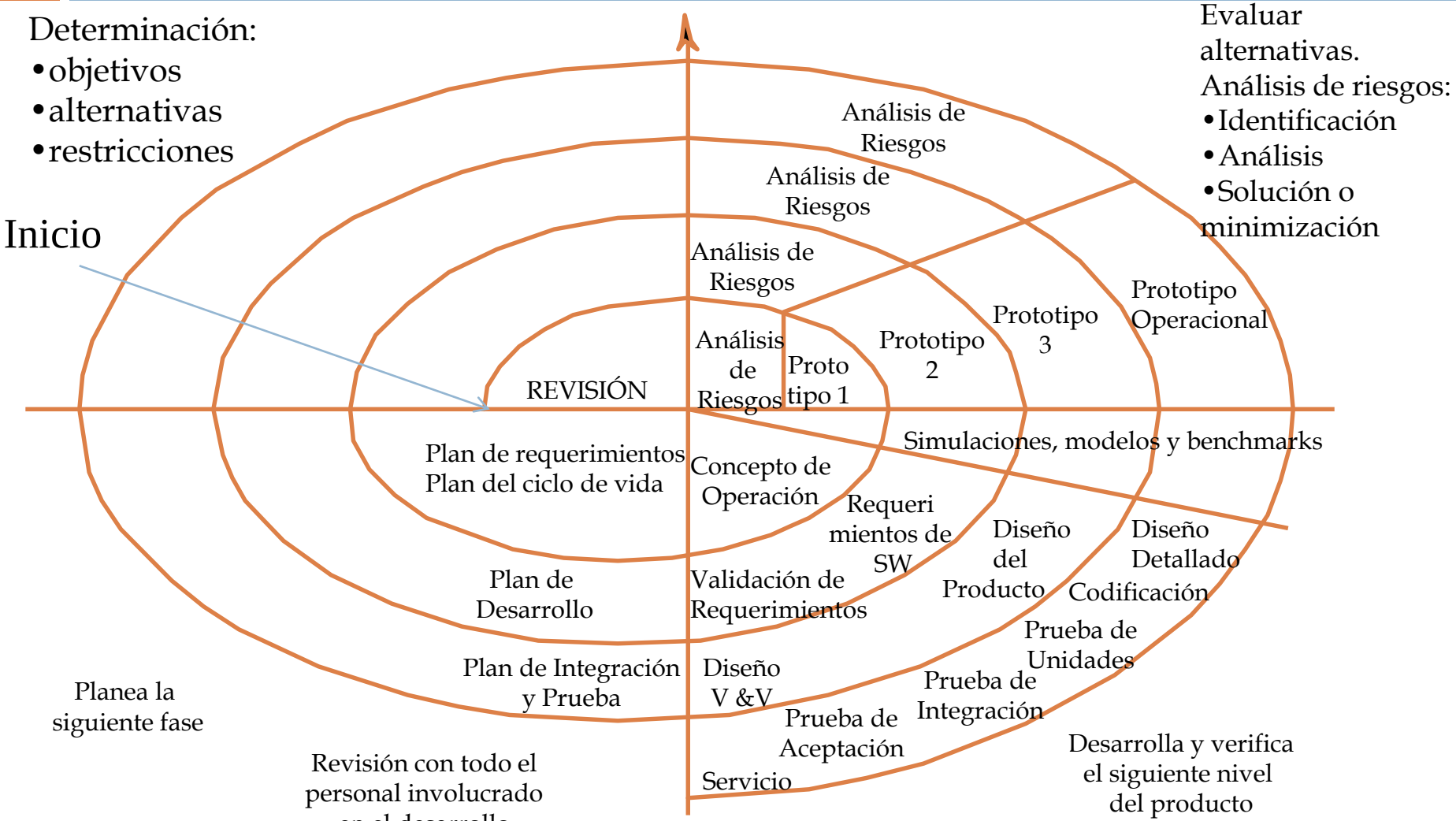
Glosario

- El modelo en espiral
- Definiciones
- Activos
- Amenazas
- Plan de riesgos

Modelo en Espiral



Análisis de riesgos: Definiciones

DEFINICIONES:

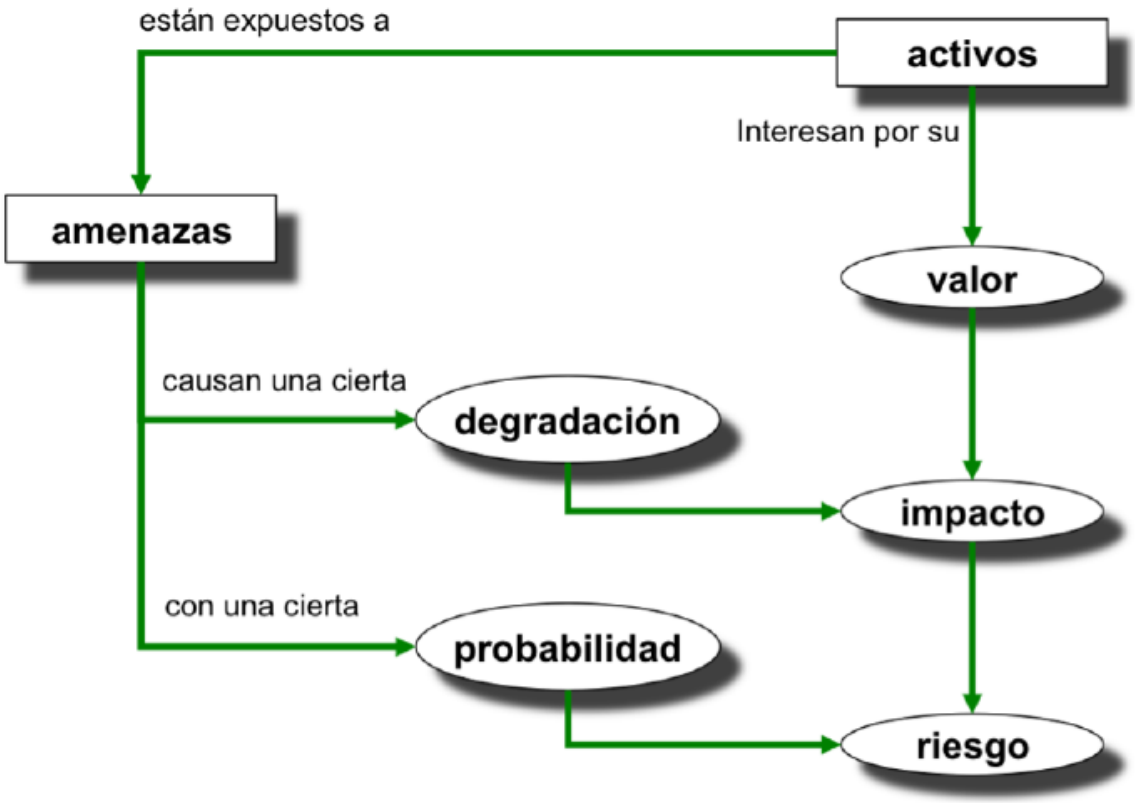
- **Activos,** son los elementos del sistema de información que soportan la misión de la Organización
- **Amenazas,** que son cosas que les pueden pasar a los activos causando un perjuicio a la Organización
- **Salvaguardas** (o contramedidas), que son medidas de protección desplegadas para que aquellas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

Análisis de riesgos: Definiciones

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 de riesgos: Definiciones



MAGERIT *Elementos del análisis de riesgos potenciales*

Análisis de riesgos: Activos

- ACTIVOS

Componente o funcionalidad de un sistema de información **susceptible de ser atacado** deliberada o accidentalmente **con consecuencias para la organización.** [UNE 71504:2008]

Análisis de riesgos: Activos

- 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 y prestar servicios
  - **Las instalaciones** que acogen equipos informáticos y de comunicaciones.
  - **Las personas** que explotan u operan todos los elementos anteriormente citados.

Análisis de riesgos: Activos

- 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

Análisis de riesgos: Activos

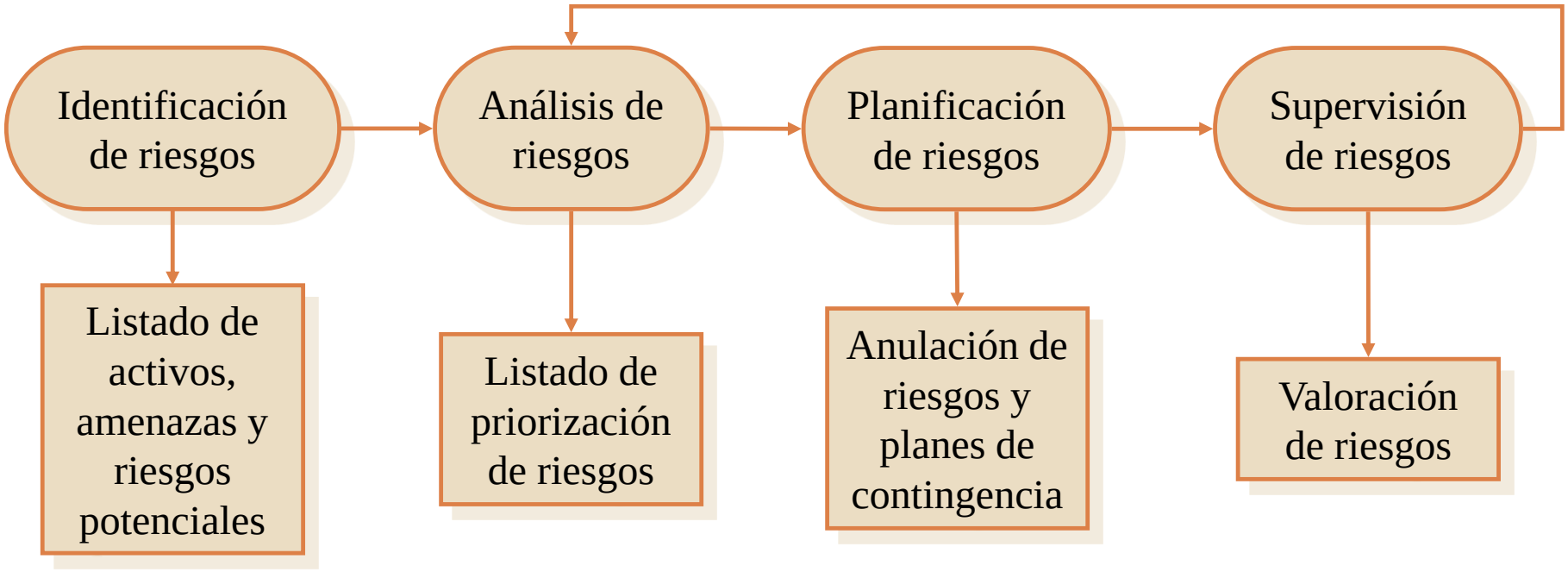
- Dimensiones de los servicios:
  - la **autenticidad:** ¿qué perjuicio causaría no saber exactamente quién hace o ha hecho cada cosa?
  - la **trazabilidad** del uso del servicio: ¿qué daño causaría no saber a quién se le presta tal servicio? Es decir, ¿quién hace qué y cuándo?
  - la **trazabilidad**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

Análisis de riesgos: Amenazas

- **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

Análisis de riesgos: Plan de riesgos

- Administración del riesgo:



Análisis de riesgos: Plan 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, Technical Reports SEI
      - Del negocio: afectan a la organización responsable del desarrollo
      - Del proyecto: afectan a la calendarización o recursos.
      - Del producto: afectan a la calidad o desempeño del software
      - Tecnológicos
      - Personales
      - De la organización
      - En las herramientas
      - En los requisitos
      - En la estimación
  - **Análisis de riesgos**
  - **Planificación del riesgo**
  - **Supervisión de riesgos**

Análisis de riesgos: Plan de riesgos

- Administración del riesgo:
  - **Identificar los riesgos.**
  - **Análisis de riesgos**
    - Para cada riesgo, evaluamos:
      - La probabilidad de que ocurra: Baja, Moderada, Alta y
      - Su Impacto, consecuencias, o degradación: Catastrófico, Grave, Tolerable, Insignificante.
  - **Planificaci**
  - **Supervisió**

Matriz de riesgos

	TOLERABLE	SERIO	CRÍTICO
BAJA		R4, R19, R26, R32, R33	R5, R8, R13, R34
MODERADA	R6, R15,R16, R18, R28, R29,R30,	R2, R3, R12, R17, R21, R23, R25, R27,R31	R1, R7, R9, R11
ALTA	R24, R10	R14, R20, R22	

Análisis de riesgos: Plan de riesgos

- Administración del riesgo:
  - **Identificar los riesgos.**
  - **Planificación del riesgo**
    - Prevención, o evitación: reducimos la probabilidad de aparición
    - Minimización: reducimos el impacto de la amenaza
    - Planes de contingencia: tratamos de llevar a nuestra organización al estado anterior a la ocurrencia del riesgo, siguiendo un plan preconcebido.
    - Transferencia: subcontratamos expertos que nos gestionen (y se responsabilicen) de la gestión de un riesgo (porque son expertos en ello)
  - **Supervisión de riesgos**

Análisis de riesgos: Plan de riesgos

- Administración del riesgo:
  - **Identificar los riesgos.**
  - **Análisis de riesgos**
  - **Planificación del riesgo**
  - **Supervisión/Monitorización 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
    - Buscaremos indicadores que puedan ser monitorizados en el tiempo (de forma continua o discreta), estableciendo umbrales de alerta que podrían desencadenar acciones de reanálisis del riesgo

Análisis de riesgos: Ejemplo de prácticas

Identificador	Categoría	Amenaza	Activos
R3	C1	Inseguridad en el entorno labora	1, 2, 4, 11, 12

Descripción	Probabilidad de aparición	Impacto
Estado físico de las instalaciones en el cual el empleado puede sufrir algún tipo de accidente debido a las deficiencias en el entorno de trabajo.	Moderada	Serio

Riesgos
Para este riesgo se ha elegido la estrategia de transferencia. La acción a desarrollar será la contratación de una empresa especializada en la seguridad en el entorno de trabajo que acudirá y realizará periódicamente revisiones sobre el estado de las instalaciones.

Seguimiento de riesgos
Se tendrá en cuenta el número de accidentes laborales mensuales poniendo como límite 3 accidentes.