

dit-upm

Análisis y Gestión de Riesgos Magerit

José A. Mañas <<http://www.dit.upm.es/~pepe/>>
Dep. de Ingeniería de Sistemas Informáticos
Universidad Politécnica de Madrid

17.5.2008

- Magerit v2 – MAP, 2005
 - Metodología de análisis y gestión de riesgos de los sistemas de información
 - <http://www.csi.map.es/csi/pg5m20.htm>
- ISO/IEC 27005, ¿2008?
 - Information security risk management

- La información
- Los procesos
- Las aplicaciones
- El sistema operativo
- El hardware
- Las comunicaciones
- Los soportes de información
- Las instalaciones
- El personal

el objeto

los medios

- Antes
 - la informática era cosa de unos pocos profesionales
 - los sistemas eran complejos y muy suyos
 - la seguridad no era un problema
- La red
 - lo cambia todo
 - no hay equipos aislados
 - los malos saben lo mismo que los buenos
- Ahora
 - las amenazas incluyen la naturaleza, la industria y el hombre
 - los sistemas son excesivamente complejos para que alguien, en singular, comprenda absolutamente todos los detalles

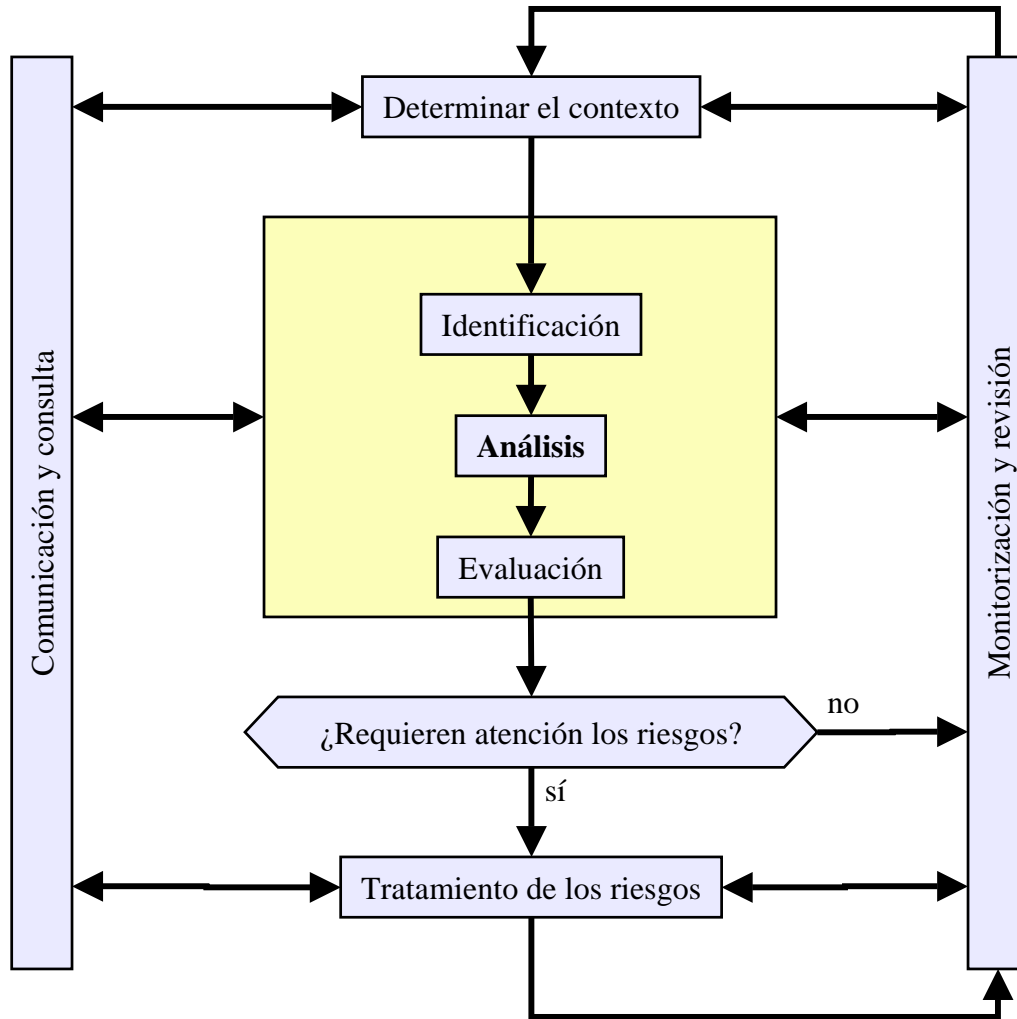
Seguridad de las redes y de la información:

la capacidad de las redes o de los sistemas de información **de resistir, con un determinado nivel de confianza,** los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, autenticidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles

*REGULATION (EC) Not 460/2004 10 OF THE EUROPEAN
PARLIAMENT AND OF THE COUNCIL of March 2004
establishing the European Network and Information Security Agency*

- Los usuarios del SI ven la seguridad como
 - confianza
- Los técnicos ven la seguridad como
 - componentes, dispositivos, software, ...
- Los atacantes ven la seguridad como
 - aquello que impide sus objetivos
- Los gestores ven la seguridad como
 - gestión de riesgos

- Mantener la **disponibilidad** de los datos almacenados, así como su disposición a ser compartidos
 - contra la interrupción del servicio
- Mantener la **integridad** de los datos ...
 - contra las manipulaciones
- Mantener la **confidencialidad** de los datos almacenados, procesados y transmitidos
 - contra las filtraciones
- Asegurar la identidad de origen y destino (**autenticidad**)
 - frente a la suplantación o engaño
- Garantizar que sabemos qué pasó (**trazabilidad**)
 - frente a la ocultación de evidencias



Análisis de riesgos

proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una organización

Evaluación de los riesgos

proceso en el que se coteja el riesgo estimado contra los criterios de la organización para determinar la importancia del riesgo

Tratamiento de riesgos

selección e implantación de salvaguardas para conocer, prevenir, impedir, reducir o controlar los riesgos identificados

ISO

gestión de riesgos

1. análisis
2. tratamiento

MAGERIT

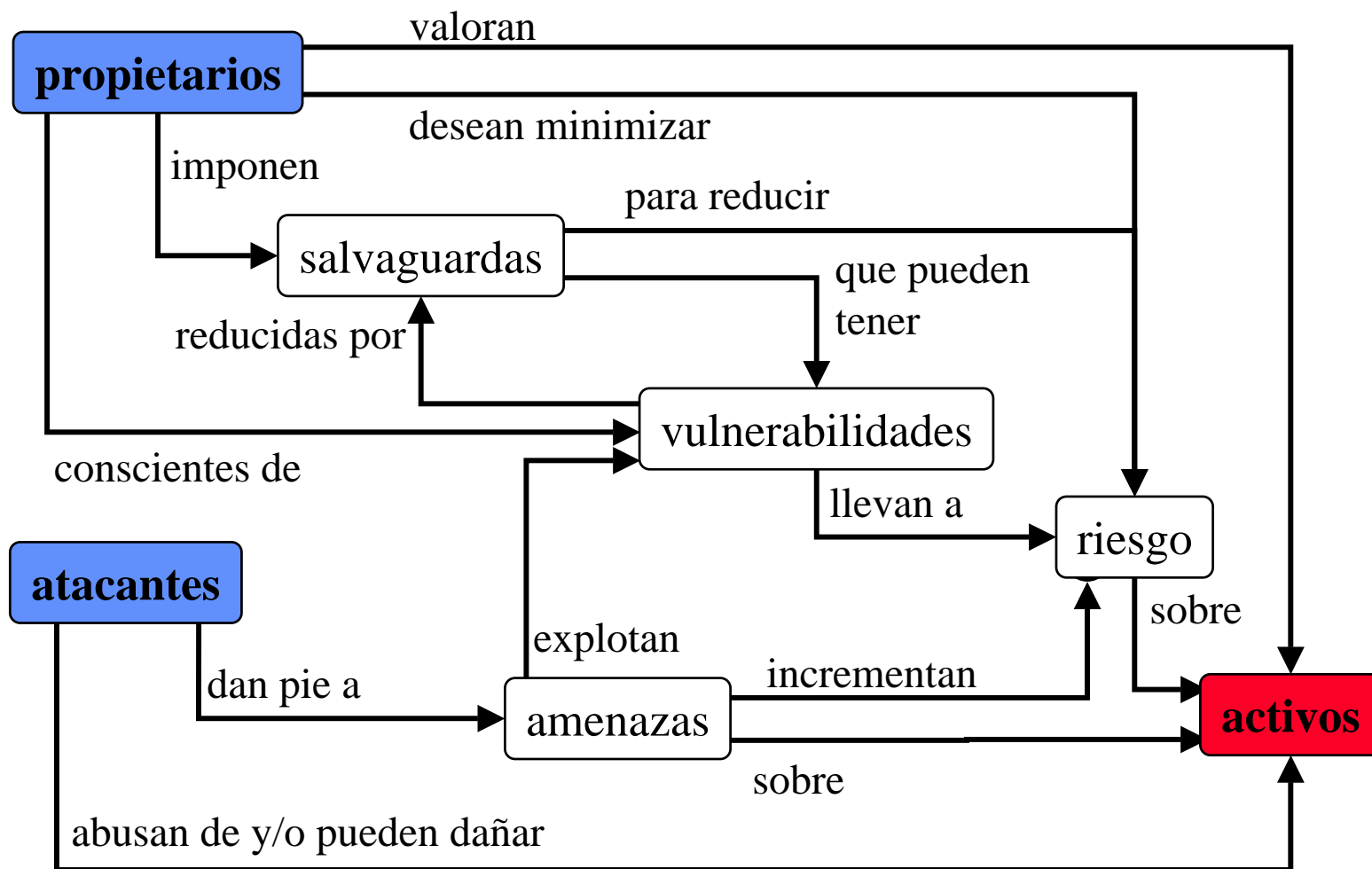
AGR – análisis y gestión de riesgos

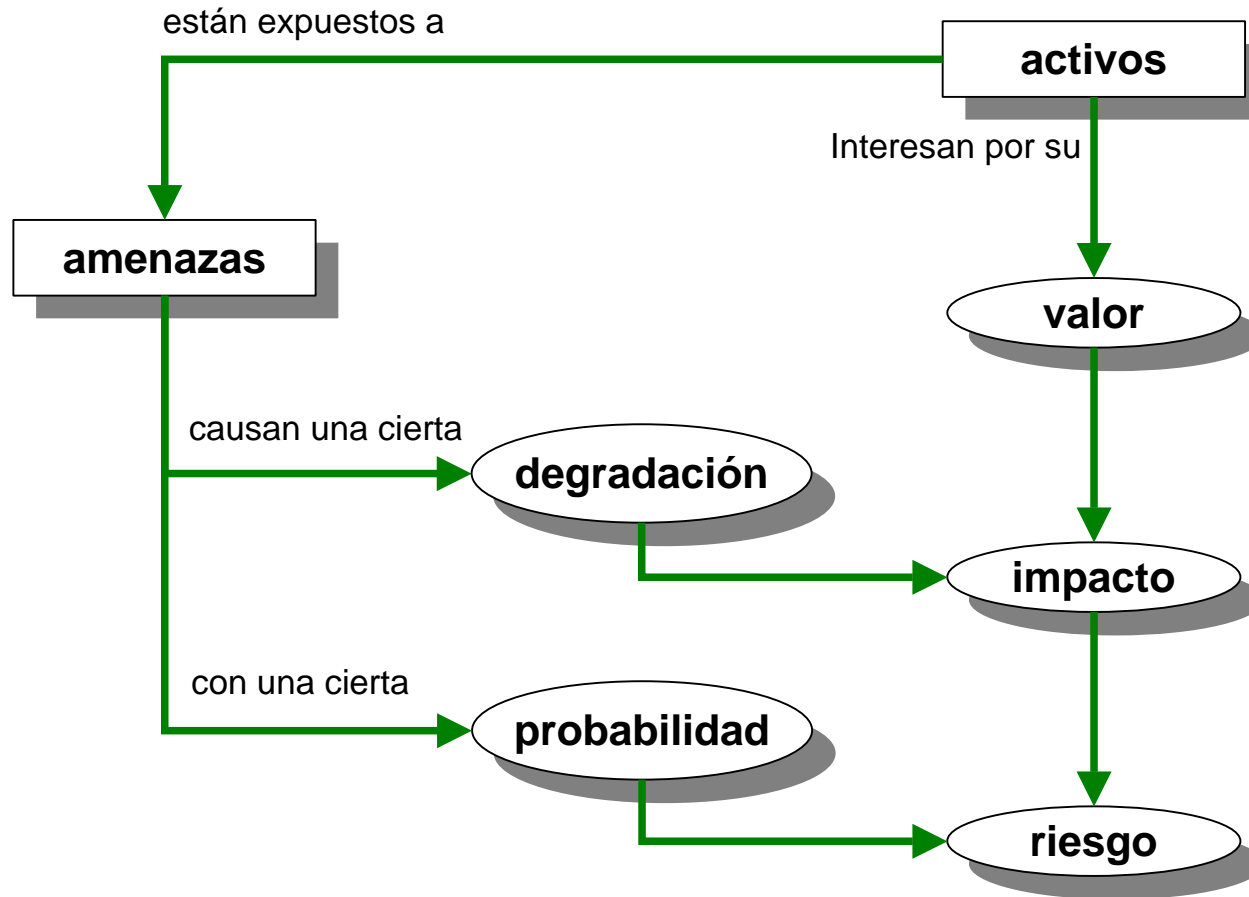
1. análisis
2. gestión

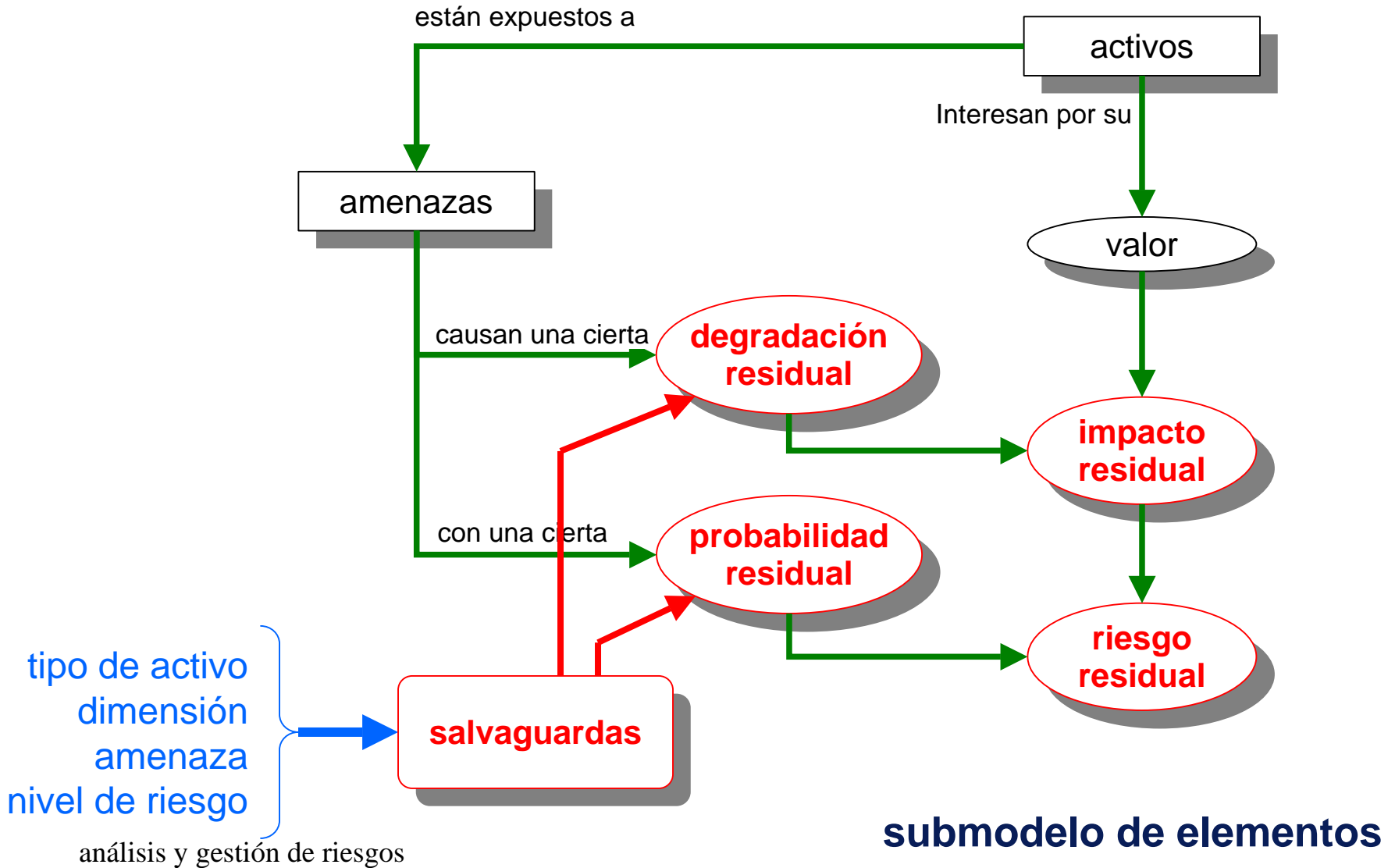
El análisis de riesgos no es simple

- Muchos activos
 - los sistemas son complejos
 - Activos de muchos tipos
 - información, servicios
 - equipamiento: aplicaciones, equipos, comunicaciones, ...
 - locales: recintos, edificios, áreas, ..., en el campo
 - personas: usuarios, operadores, desarrolladores, ...
 - Muchas amenazas
 - y muchas formas de hilvanar las amenazas
 - Muchísimas salvaguardas
 - gestión, técnicas, seguridad física, recursos humanos
- ... lleva tiempo**
... cuesta dinero
... no vale una vez y para siempre

- La complejidad se ataca metódicamente
 - una metodología es una aproximación sistemática
 - para cubrir la mayor parte de lo que puede ocurrir
 - para olvidar lo menos posible
 - para explicar a los gerentes qué se necesita de ellos
 - para explicar a los técnicos qué se espera de ellos
 - para explicar a los usuarios
 - qué un uso decente del sistema
 - qué es una respuesta urgente
 - cómo se gestionan los incidentes
 - una metodología necesita modelos
 - elementos: activos, amenazas, salvaguardas
 - métricas: impacto y riesgo







- ***Metodología de análisis y gestión de riesgos de los sistemas de información***
- Pública
 - MAP : Ministerio para las Administraciones Públicas
 - version 1.0, 1997
 - version 2.0, 2005
 - <http://www.csi.map.es/csi/pg5m20.htm>
- Recomendación para la administración pública española
 - *los funcionarios son “buena gente”
que harán un buen análisis de riesgos
... si se les ayuda a hacerlo metódicamente*

- Análisis de riesgos
 - proceso sistemático para estimar la magnitud del riesgo sobre un sistema de información

1. planificación del proyecto de análisis y gestión de riesgos

.1 oportunidad

.2 alcance

.3 planificación

.4 lanzamiento

2. análisis de riesgos

.1 activos

.2 amenazas

.3 salvaguardas

.4 estado de riesgo

3. gestión de riesgos

.1 toma de decisiones

.2 plan de seguridad

.3 ejecución del plan

- submodelo de procesos
- una guía para gestionar los riesgos, basada en su estudio

1. planificación del proyecto de análisis y gestión de riesgos

.1 oportunidad

.2 alcance

.3 planificación

.4 lanzamiento

2. análisis de riesgos

.1 activos

.2 amenazas

.3 salvaguardas

.4 estado de riesgo

3. gestión de riesgos

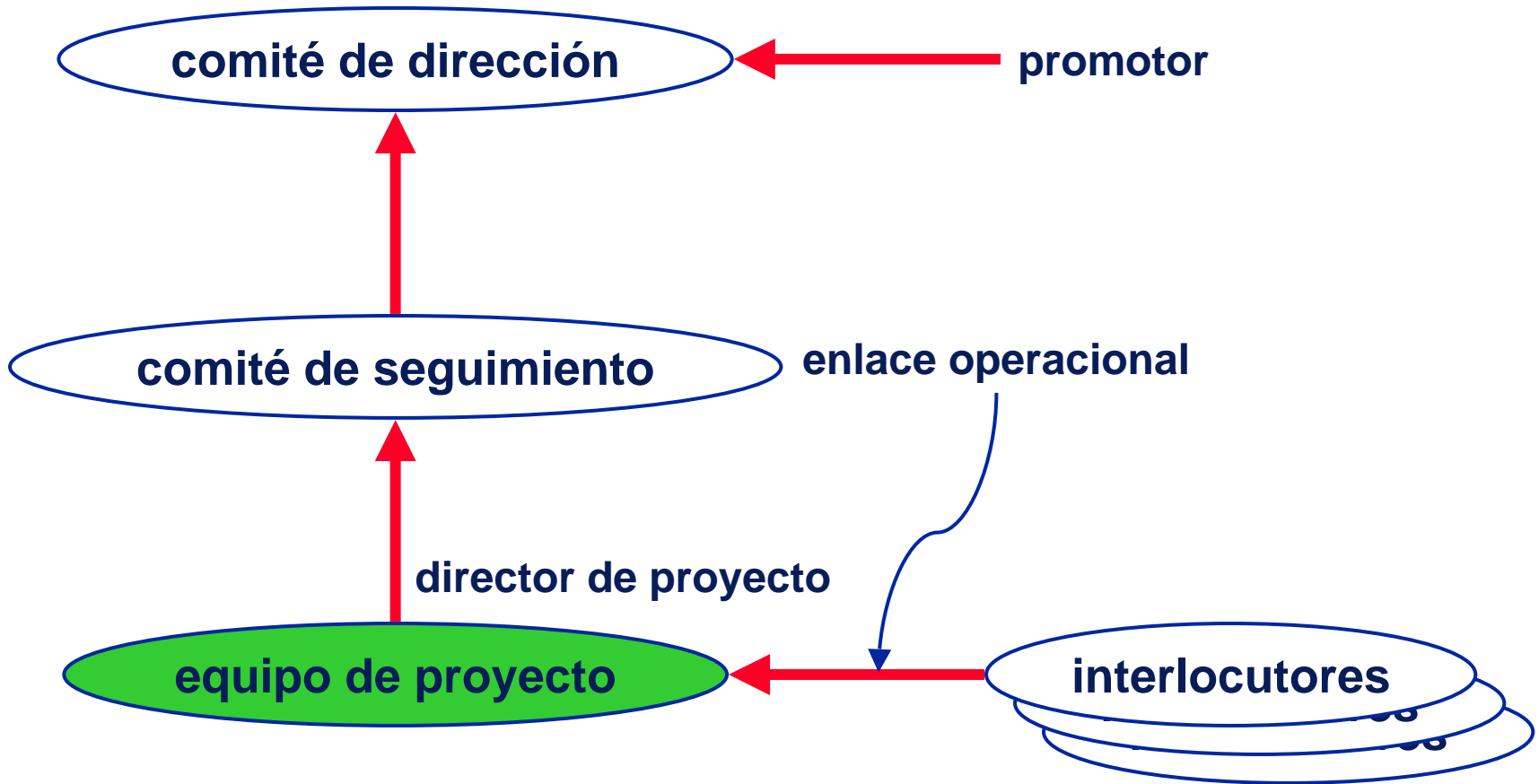
.1 toma de decisiones

.2 plan de seguridad

.3 ejecución del plan

T1.1.1. Determinar la oportunidad del proyecto

- A cargo del promotor
- Informe preliminar
- Creación del comité de seguimiento



T1.2.1. Objetivos

T1.2.2. Dominio y límites

T1.2.3. Entorno y restricciones

T1.2.4. Dimensiones y coste

- A cargo del comité de seguimiento y director del proyecto
- Marco de trabajo

T1.3.1. Plan de entrevistas a realizar

T1.3.2. Participantes a entrevistar

T1.3.3. Calendario

- Director del proyecto y equipo de proyecto

T1.4.1. Cuestionarios

T1.4.2. Criterios de valoración

T1.4.3. Recursos necesarios

T1.4.4. Sensibilización

- Equipo de proyecto y comité director

1. planificación del proyecto de análisis y gestión de riesgos

.1 oportunidad

.2 alcance

.3 planificación

.4 lanzamiento

2. análisis de riesgos

.1 activos

.2 amenazas

.3 salvaguardas

.4 estado de riesgo

3. gestión de riesgos

.1 toma de decisiones

.2 plan de seguridad

.3 ejecución del plan

T2.1.1. Identificación de activos

T2.1.2. Dependencias entre activos

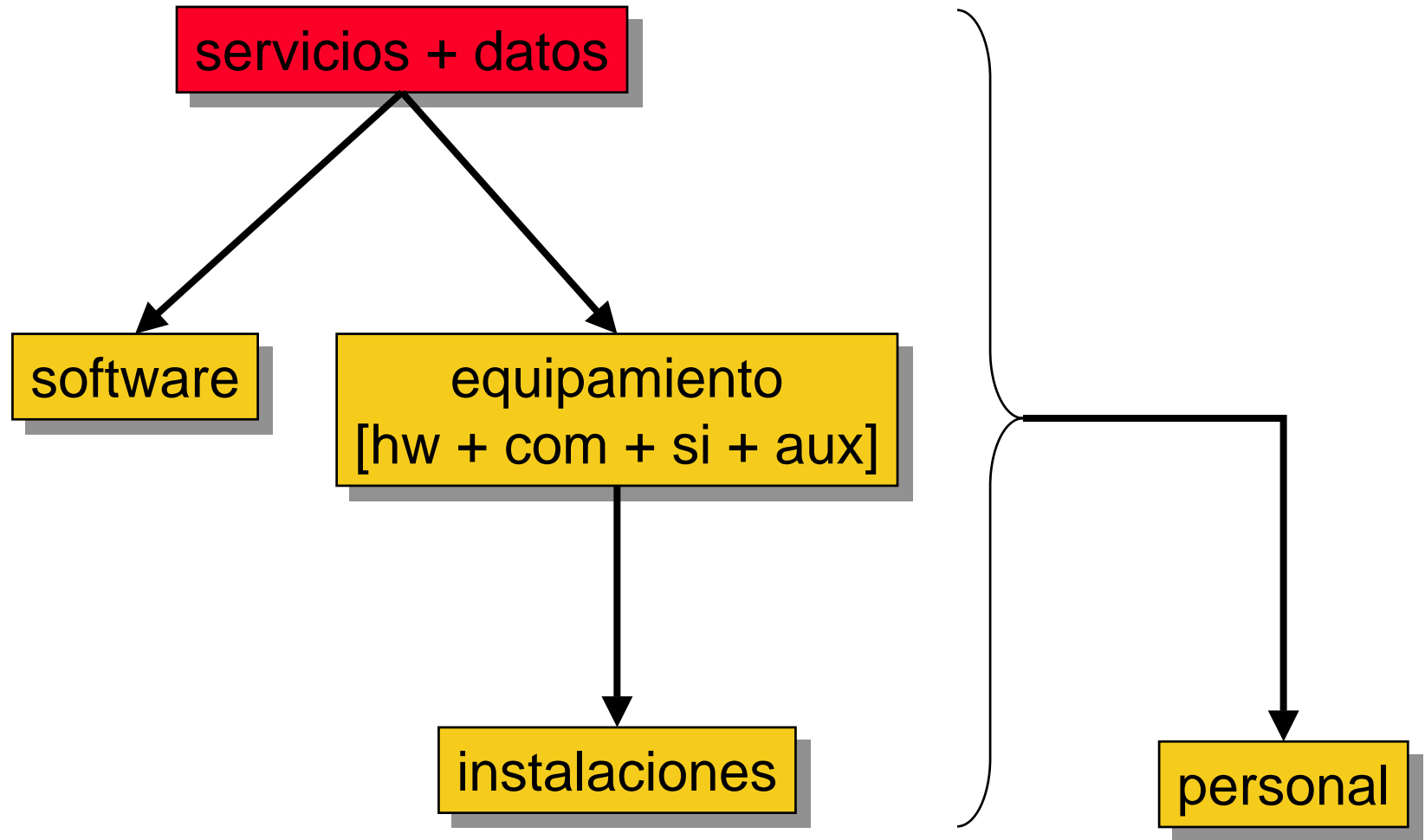
T2.1.3. Valoración

- Equipo de proyecto y grupos de interlocutores
- Salida: modelo de valor

- diagramas de flujo de datos
- diagramas de procesos

- Magerit
 - son los recursos del sistema de información, o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.
- ISO
 - **Asset.** Anything that has value to the organization.

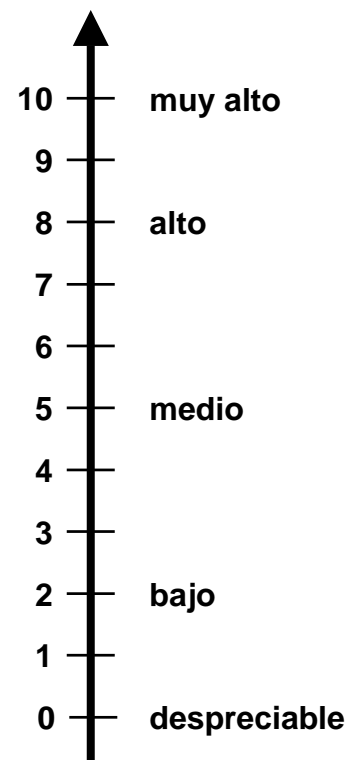
Unos activos dependen de otros



- Las dependencias crean la necesidad de proteger los activos inferiores para que cumplan su misión última
 - acumulación de responsabilidad
- Las dependencias hacen a los activos superiores víctimas pasivas de los defectos de los inferiores
 - repercusión de consecuencias

- Coste que supondría la ocurrencia de una amenaza
 - valor de reposición
 - valor de reconstrucción
 - horas perdidas de trabajo
 - lucro cesante
 - daños y perjuicios
- **No sólo importa lo que cuesta; importa [más] para qué vale**
- Para un estudio comparativo basta alguna escala sencilla:
 - 0, 1, 2, ..., 10
 - es más importante saber el valor relativo que el absoluto
- Para un estudio de costes se requiere una estimación ajustada

- Criterios homogéneos que permitan
 - relativizar entre dimensiones
 - compartir / combinar análisis realizados por separado
 - uniformidad de conocimiento



<i>valor</i>	<i>criterio</i>	
10 - muy alto	daño muy grave	
8 - alto	daño grave	repercute en otros
5 - medio	daño importante	queda en casa
2 - bajo	daño menor	
0 - despreciable	daño irrelevante	

- $B1 = \text{ingresos}_1 - \text{gastos}_1$
 - si no ocurre nada
- $B2 = \text{ingresos}_2 - \text{gastos}_2$
 - si se materializa la amenaza
- $\text{VALOR} = B1 - B2$
($\text{ingresos}_1 - \text{ingresos}_2$) + ($\text{gastos}_2 - \text{gastos}_1$)



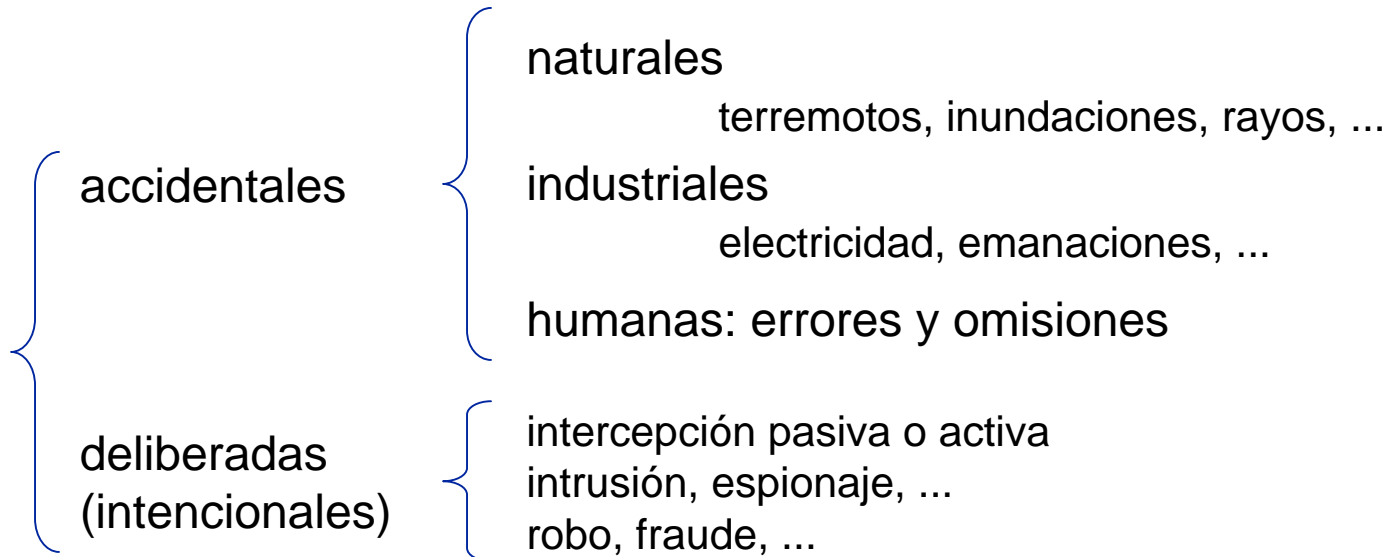
T2.2.1. Identificación

T2.2.2. Valoración

- Equipo de proyecto y grupos de interlocutores
- Salida: informe de amenazas

- historia: en casa o de fuentes exteriores
- descubrimiento y caracterización del adversario
- árboles de ataque

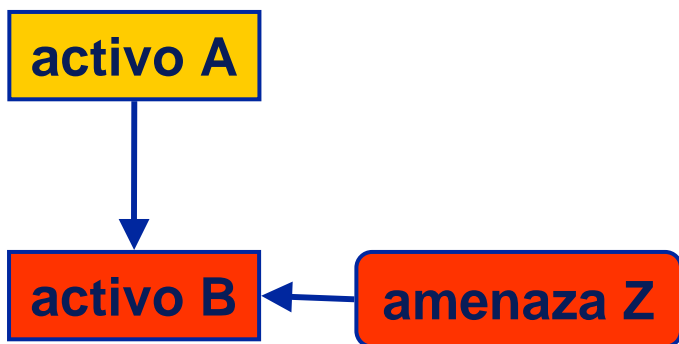
- Son los eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales



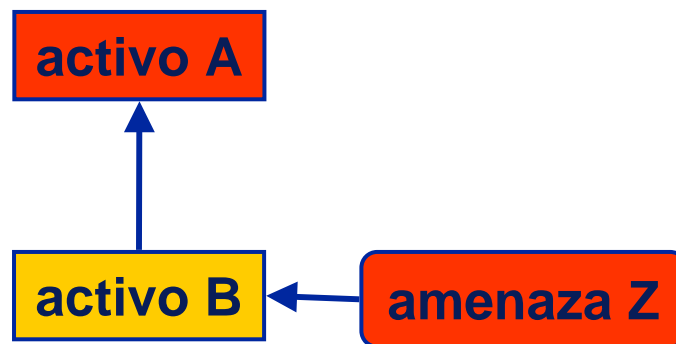
- Identificación
 - ¿qué puede ocurrir [que deba preocuparnos]?
 - por experiencia (propia o ajena)
 - por la propia naturaleza del activo (clase)
- Cuantificación - ¿vulnerabilidad?
 - frecuencia
 - probabilidad de ocurrencia
 - tasa anual de ocurrencia de incidentes
 - degradación
 - consecuencias [sobre el valor de los activos]
 - porcentaje del valor que se pierde a causa de un incidente

- Consecuencia que sobre un activo tiene la materialización de una amenaza
 - daño producido por un incidente
 - pérdida posible
- Valoración
 - cualitativa / subjetiva
 - irrelevante ... grave ... intolerable
 - cuantitativa / económica
 - coste dinerario
- Métodos
 - directos: ¿qué impacto tendría ...?
 - indirectos: valor × degradación

acumulado



repercutido

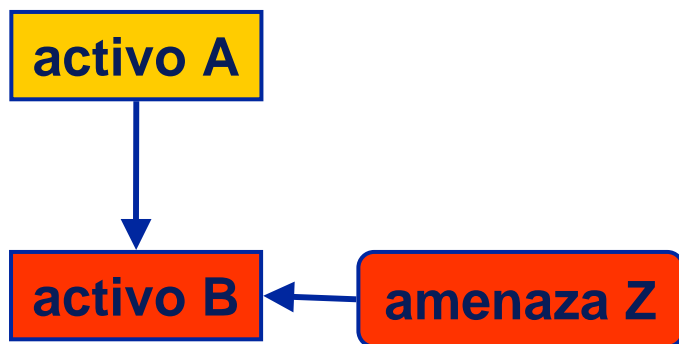


- Estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la organización
 - pérdida probable
- Valoración
 - cualitativa / subjetiva
 - irrelevante ... grave ... intolerable
 - cuantitativa / económica
 - coste dinerario
- Métodos
 - cualitativos: tabulares
 - cuantitativos: impacto × frecuencia

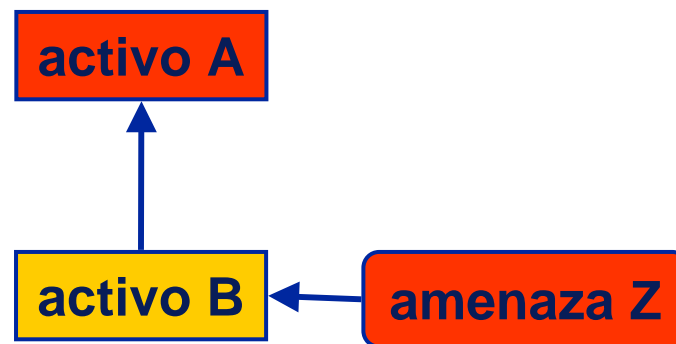
- $\text{impacto} = \text{valor} \times \text{degradación}$
- $\text{riesgo} = \text{impacto} \times \text{frecuencia}$

impacto	MA	alto	muy alto	muy alto	muy alto	muy alto
	A	medio	alto	alto	alto	alto
	M	bajo	bajo	medio	medio	medio
	B	bajo	bajo	bajo	medio	medio
	MB	muy bajo	muy bajo	muy bajo	muy bajo	bajo
		PF	FN	F	MF	EF
						probabilidad

acumulado



repercutido



- **T2.3.1. Identificación de salvaguardas presentes**
- **T2.3.2. Valoración de su efectividad**

- Equipo de proyecto y grupos de interlocutores
- Varias evaluaciones
 - auto-evaluación | inspección | auditoría
- Salida:
 - declaración de aplicabilidad
 - evaluación de las salvaguardas
 - informes de insuficiencias

- MAGERIT
 - procedimiento o mecanismo tecnológico que reduce el riesgo
 - sinónimos: contra medidas, controles
- ISO
 - **Safeguard.** A practice, procedure or mechanism that reduces risk
 - synonyms: countermeasures, controls
- EBIOS
 - **Mesure de sécurité.** Moyen destiné à améliorer la sécurité, spécifié par une exigence de sécurité et à mettre en oeuvre pour la satisfaire. Il peut s'agir de mesures de prévision ou de préparation, de dissuasion, de protection, de détection, de confinement, de "lutte", de récupération, de restauration, de compensation...

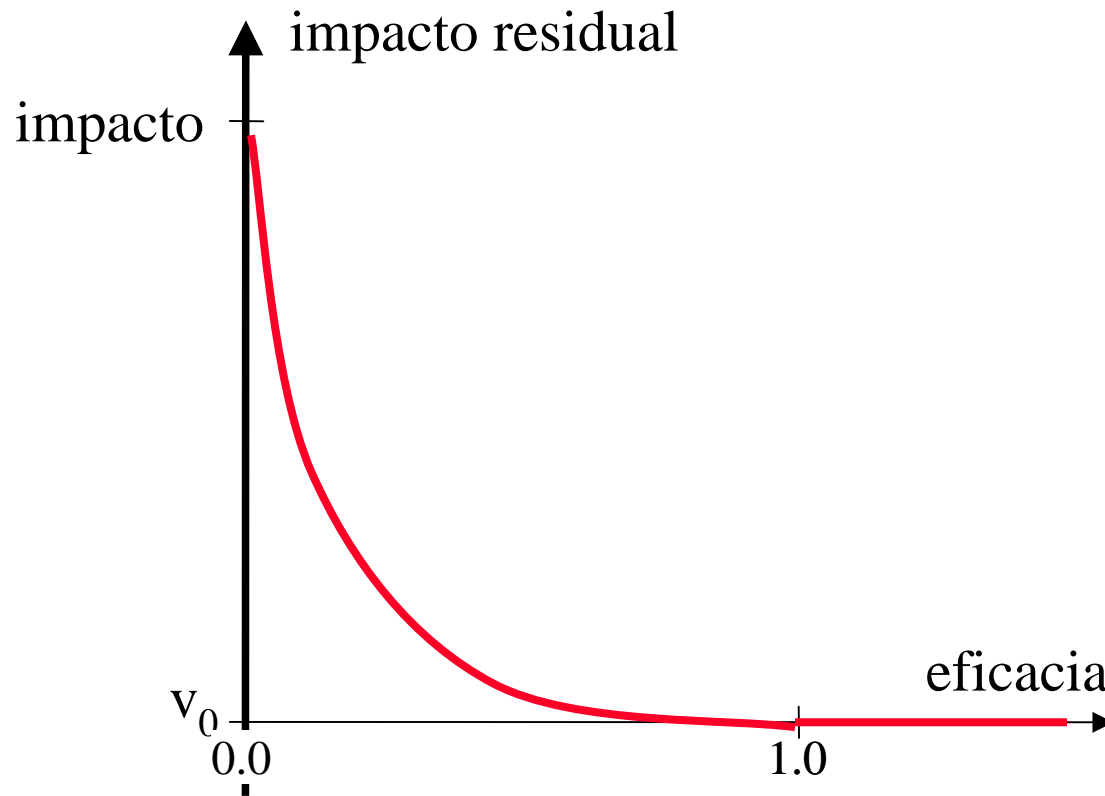
- E: Eficacia
 - medida en que la salvaguarda está implantada y es efectiva frente al riesgo al que se enfrenta
 - opinión cualificada (de un experto)
- La eficacia se reparte entre
 - reducción de oportunidades
 - limitación del impacto

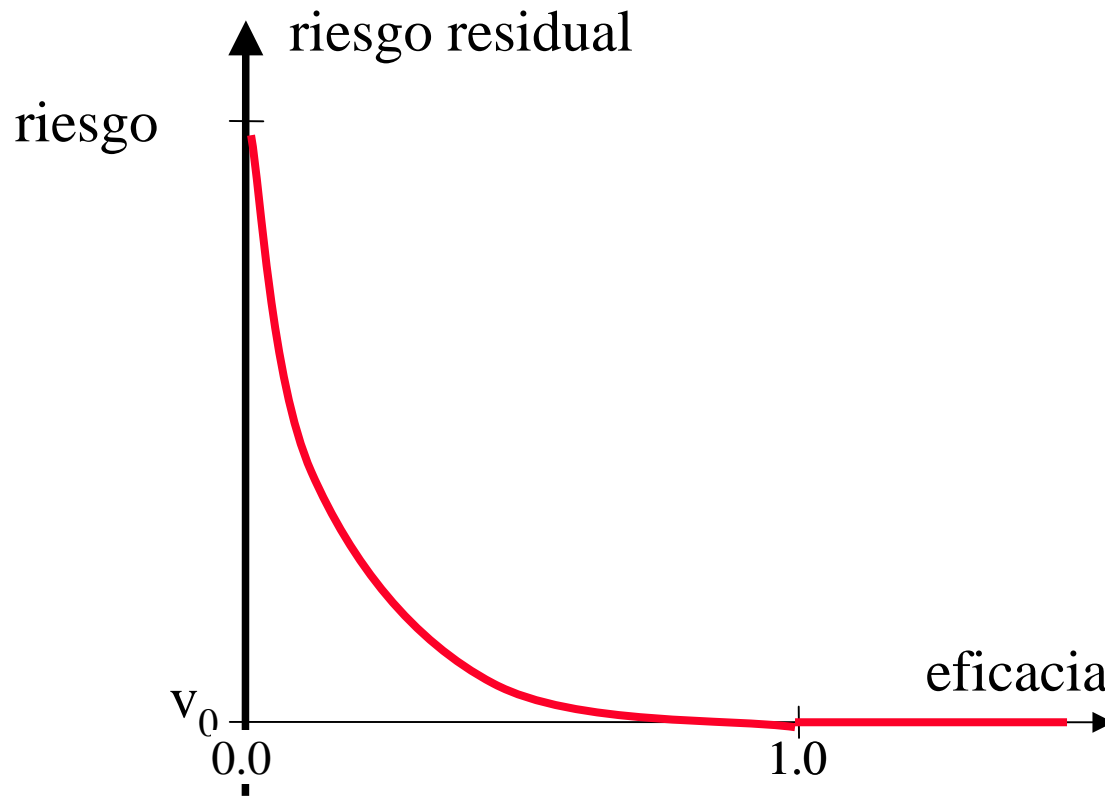
- T2.4.1. Estimación del impacto
- T2.4.2. Estimación del riesgo
- T2.4.3. Interpretación de los resultados

- Equipo de proyecto
- Salida: estado de riesgo

estimaciones

- potencial (teórico)
- residual (actual)





1. planificación del proyecto de análisis y gestión de riesgos

.1 oportunidad

.2 alcance

.3 planificación

.4 lanzamiento

2. análisis de riesgos

.1 activos

.2 amenazas

.3 salvaguardas

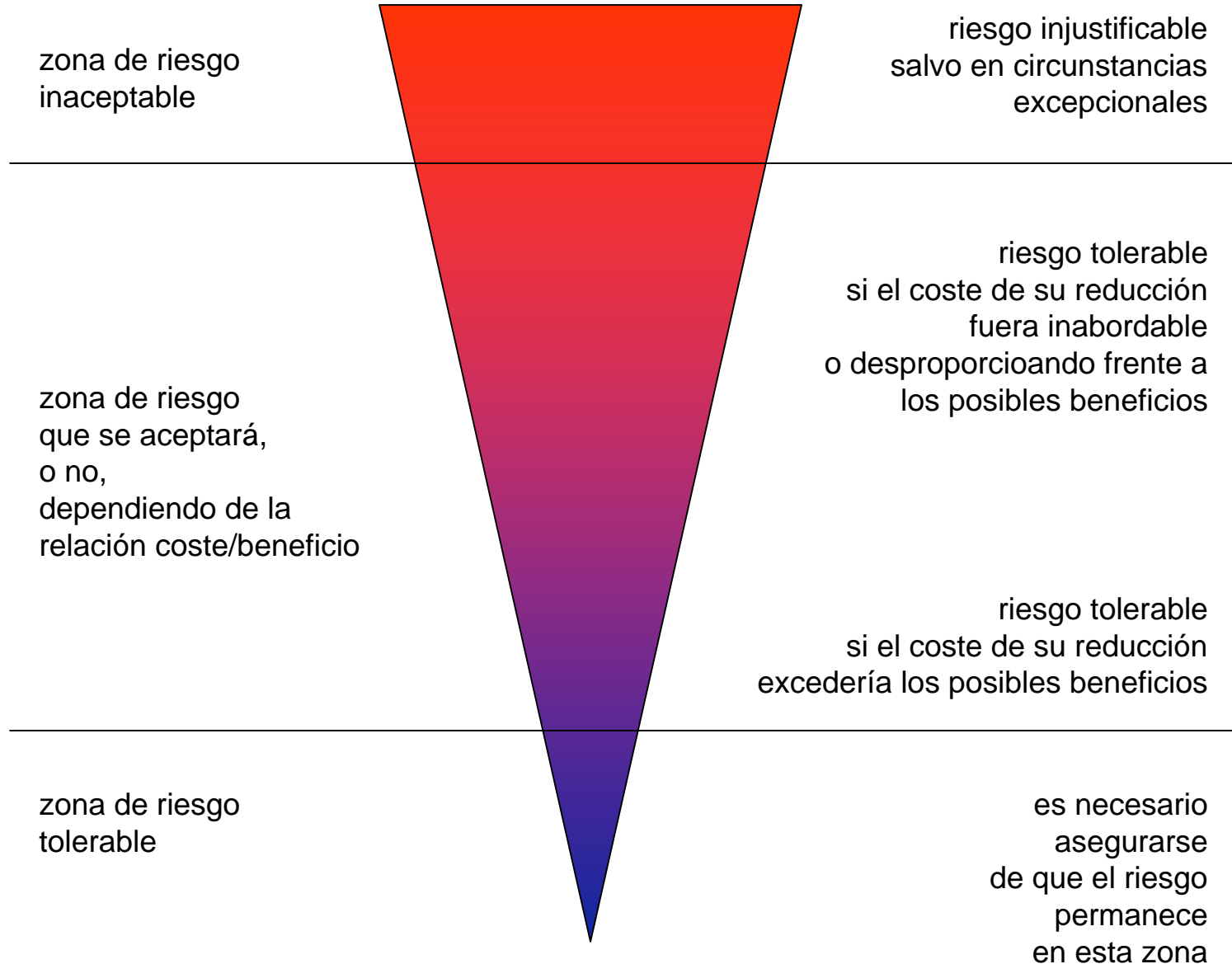
.4 estado de riesgo

3. gestión de riesgos

.1 toma de decisiones

.2 plan de seguridad

.3 ejecución del plan



1. planificación del proyecto de análisis y gestión de riesgos

.1 oportunidad

.2 alcance

.3 planificación

.4 lanzamiento

2. análisis de riesgos

.1 activos

.2 amenazas

.3 salvaguardas

.4 estado de riesgo

3. gestión de riesgos

.1 toma de decisiones

.2 plan de seguridad

.3 ejecución del plan

- O cómo pasar de la situación de riesgo actual a la situación de riesgo asumible por la organización
- Es un conjunto de programas / proyectos que mejoran la calificación de salvaguardas
- Identifica áreas de actuación
 - adquisición / implantación de equipos / servicios
 - desarrollos propios
 - proyectos específicos

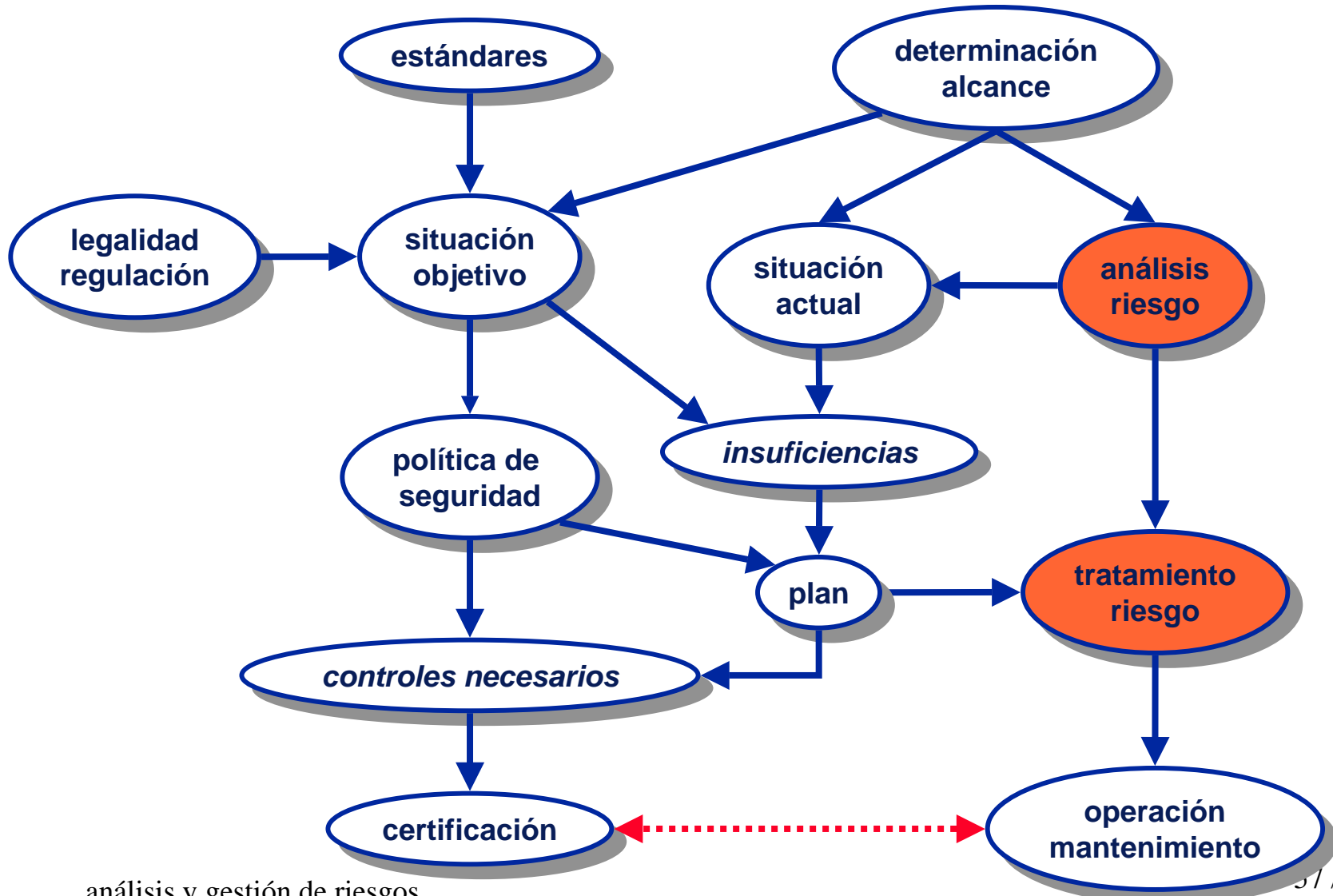
- El plan en curso
 - dedicado a la gestión de programas y proyectos
 - [desviaciones de] hitos
 - [desviaciones de] coste
- Planes para el siguiente periodo [financiero]
 - provisión de recursos
- Plan Director (strategic plan)
 - garantiza que al final todas las piezas encajan
 - garantiza que la foto final es equilibrada
 - no hay debilidades manifiestamente descompensadas

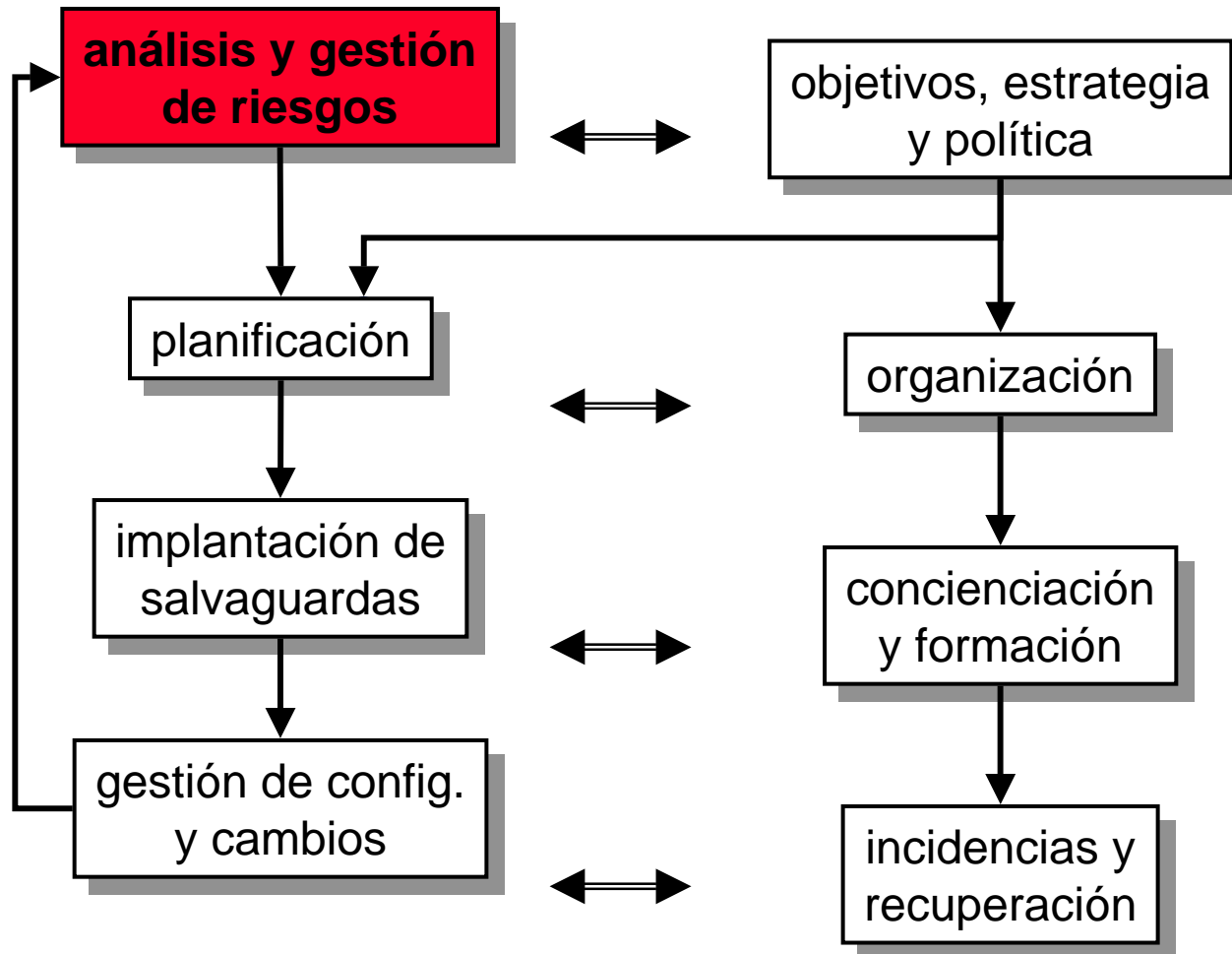
- Salvaguardas
 - normativa
 - procedimientos
 - componentes técnicos, si los hubiera
- Plan de
 - adquisición / contratación / desarrollo
 - implantación & formación
 - operación & gestión de incidencias
- Controles de eficacia
- Controles de eficiencia
- Indicadores de impacto y riesgo residuales



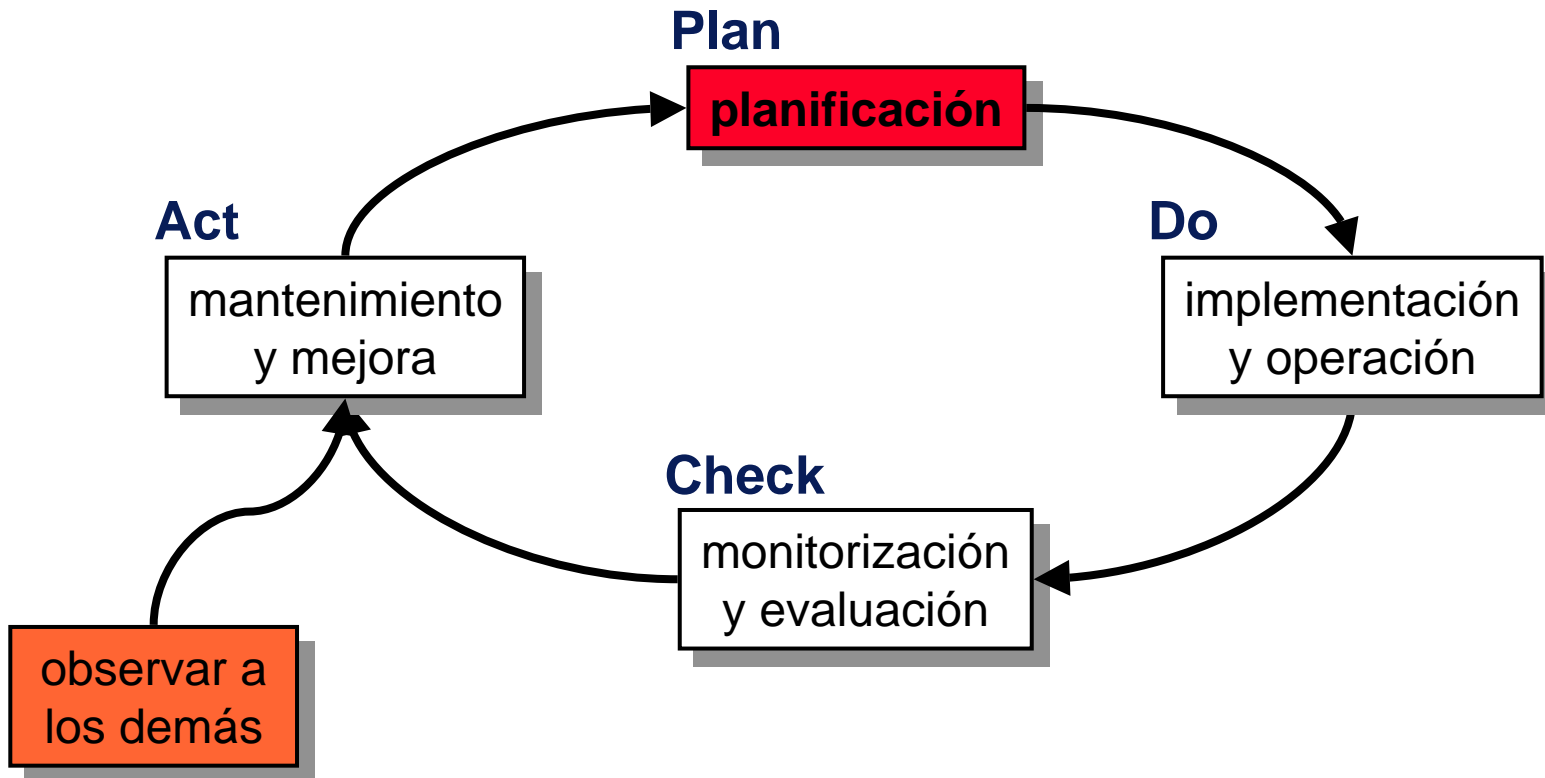
- Cuantificar el riesgo y demostrar que está bajo control
 - es necesario
 - es laborioso
 - es recurrente
- Es el fundamento de la gestión de la seguridad

- El análisis de riesgo muestra su máxima eficacia cuando se realiza antes del despliegue de un sistema
 - y las salvaguardas se incorporan al diseño de la solución
- Es necesario cuando
 - un sistema se hace cargo de nuevas o más importantes misiones que aquellas para las que fue diseñado
 - morir de éxito
 - cambia el perfil de vulnerabilidad
 - ej. exposición a Internet





Sistema de Gestión de la Seguridad de la Información



- Elementos
 - activos (y su valor para la organización)
 - amenazas (y su probabilidad y consecuencias)
 - salvaguardas
- Indicadores
 - impacto (daño potencial)
 - riesgo (daño probable)
- Tratamiento
 - minimización de los perjuicios posibles
 - maximización de los beneficios posibles