

Lección 11: Análisis y Gestión de Riesgos



intypedia
INFORMATION SECURITY ENCYCLOPEDIA

Dr. José A. Mañas
jmanas@dit.upm.es

Departamento de Ingeniería de Sistemas Telemáticos
Universidad Politécnica de Madrid

Definición

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*

Sistema de información

- Los ordenadores y redes de comunicaciones electrónicas, así como los datos electrónicos almacenados, procesados, recuperados o transmitidos por los mismos para su operación, uso, protección y mantenimiento

- Los sistemas tienen una o dos misiones
 1. custodiar datos
para que puedan ser utilizados por quien debe cuando quiera
 2. prestar servicios
 - administrativos
 - comerciales
 - industriales



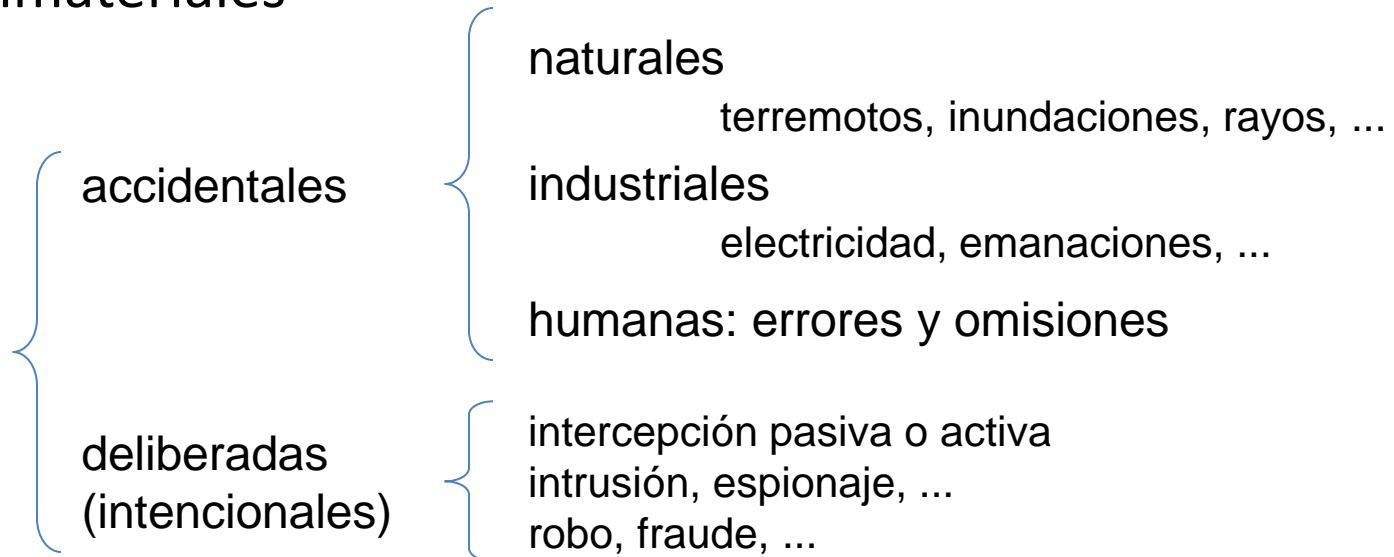
Objetivos de la seguridad

- 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
- Ser capaz de perseguir las violaciones y aprender de las experiencias
 - **trazabilidad**



Amenazas

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

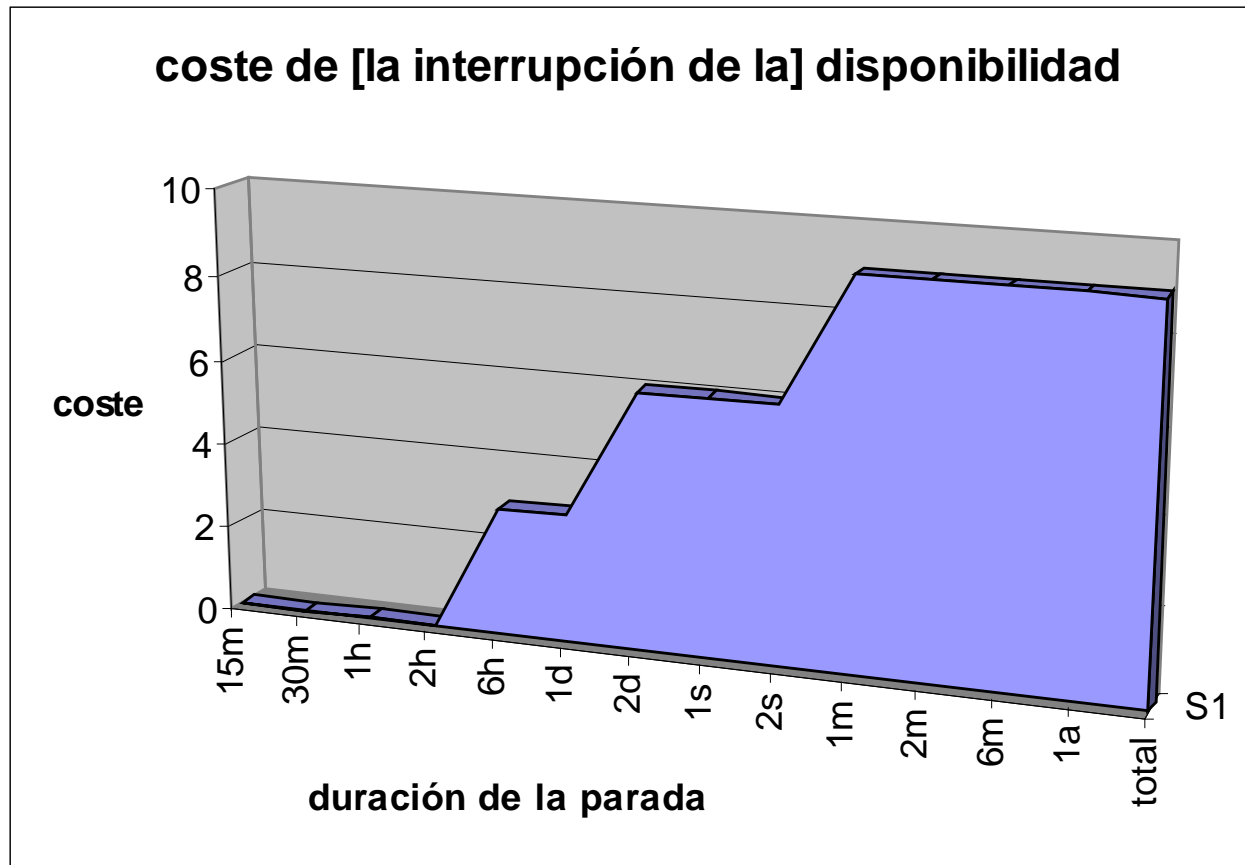


Consecuencias

- Fallos de confidencialidad ☐ fugas de información
 - no hay reparación posible
 - si se detecta, tenemos la opción de perseguir (disuasorio)
- Fallos de integridad ☐ datos manipulados
 - si se detecta, tenemos la opción de recuperar [de otra fuente]
- Fallos de disponibilidad ☐ interrupción del servicio
 - medios alternativos
 - restauración de los medios habituales
- Autenticidad = integridad [de los meta-datos]
- Trazabilidad = integridad [de los registros de actividad]



Coste de la interrupción



Términos

– Impacto

- evaluación de las consecuencias de una amenaza

– Riesgo

- impacto, teniendo en cuenta la probabilidad de la amenaza

– Análisis

- identificación y valoración

– Evaluación

- cómo el impacto y el riesgo afectan al negocio

– Gestión

- organizarse y actuar



Estimación tabular

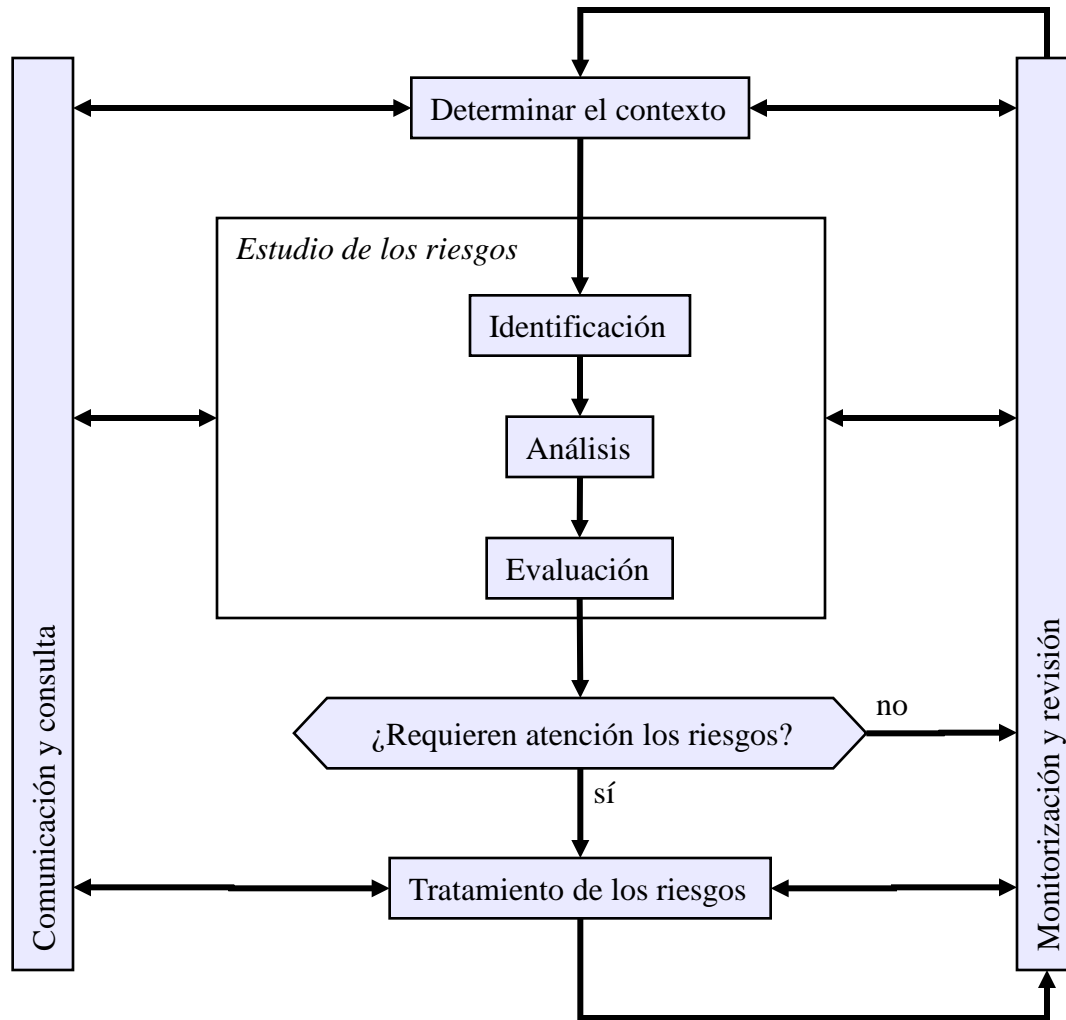
impacto	MA	alto	muy alto	muy alto	muy alto	muy alto
	A	medio	alto	alto	alto	alto
	M	bajo	bajo	medio	medio	medio
	B	bajo	bajo	bajo	medio	medio
	MB	muy bajo	muy bajo	muy bajo	muy bajo	bajo
		XS	S	M	L	XL
					probabilidad	

Riesgo

- Riesgo
 - el arte de vivir con sistemas **razonablemente seguros**
- Análisis de impacto
 - el arte de estimar las consecuencias de una amenaza potencial
- Análisis de riesgos
 - el arte de estimar las consecuencias recurrentes de la inseguridad residual
- Análisis de riesgos y análisis de impacto
 - proporcionan información para tomar decisiones
- Gestión de riesgos
 - Risk management involves managing to achieve an appropriate balance between realizing opportunities for gains while minimizing losses. [AS/NZS 4360:2004]



Gestión de riesgos



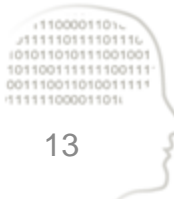
Marco para la gestión del riesgo



ISO 31000:2009 – Risk management – Principles and guidelines

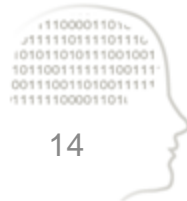
Marco

- Criterios para evaluar la información y los servicios
 - ej. clasificación de la información
 - ej. niveles de servicio
- Metodología para analizar los riesgos
 - e.g. ISO/IEC 27005:2008
- Criterios para evaluar los riesgos
- Criterios para decidir el tratamiento de los riesgos



Roles

- Responsable de la información
 - establece sus requisitos de seguridad
- Responsable del servicio
 - establece sus requisitos de seguridad
- Analista de riesgos
 - traslada los requisitos a los medios TIC
 - selecciona y evalúa medidas de protección
 - reporta sobre el riesgo residual
- *Propietario del riesgo*
 - evalúa el riesgo en términos de negocio
 - toma decisiones de tratamiento del riesgo
 - *es la autoridad responsable de la gestión del riesgo*



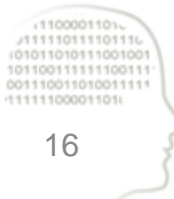
Gestión de riesgos

1. Analizar
2. Preparar una declaración de aplicabilidad
- Gestionar para cumplimiento
 - aplicar medidas hasta satisfacer los controles requeridos
- Para seguridad real [estática]
 - aplicar tratamientos hasta que el riesgo es aceptado
- Para seguridad real [dinámica]
 1. analizar qué consecuencias implican los cambios en el sistema, en su entorno, las vulnerabilidades descubiertas y las intrusiones detectadas
 2. reaccionar en consecuencia

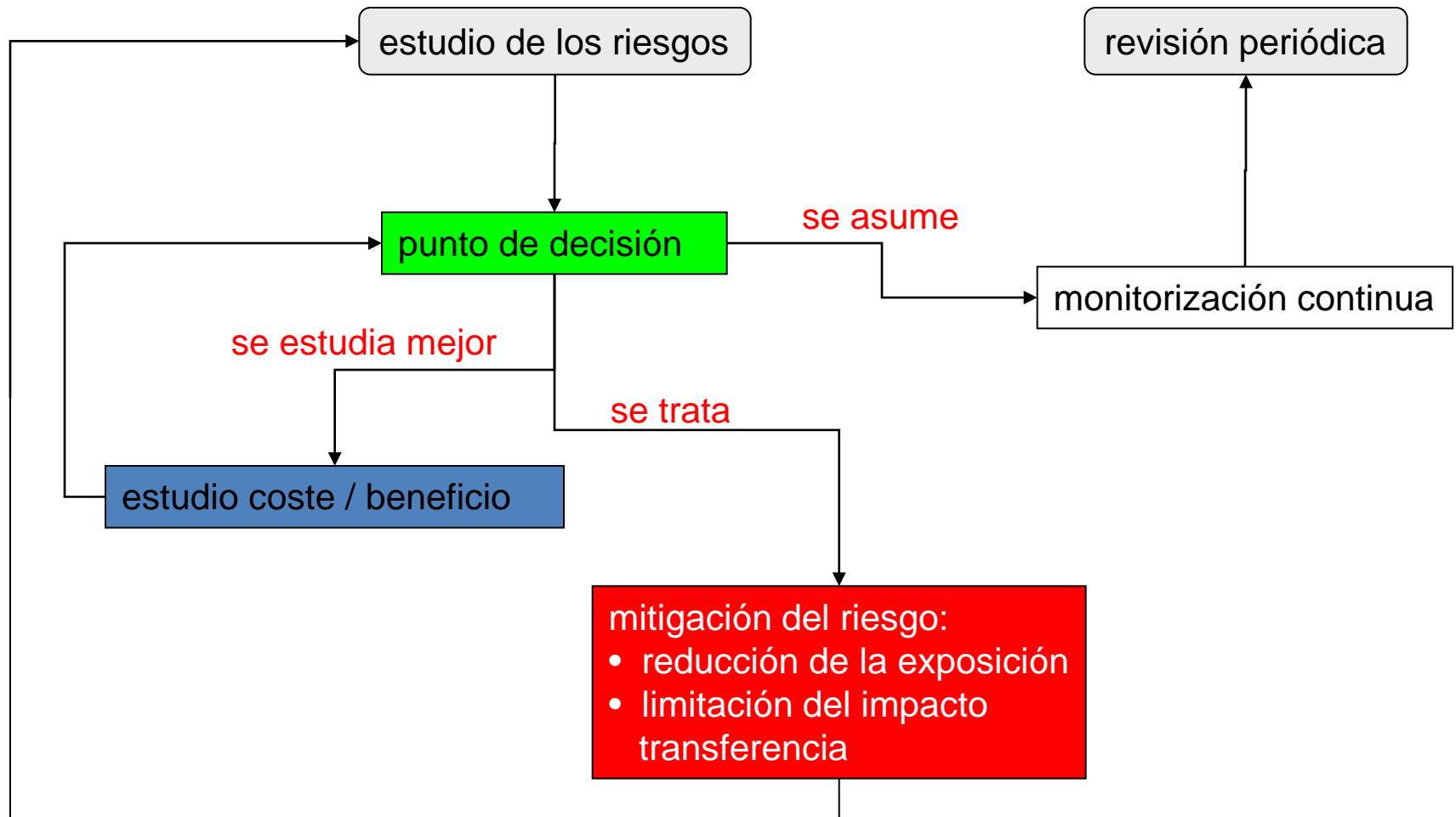


Opciones de tratamiento

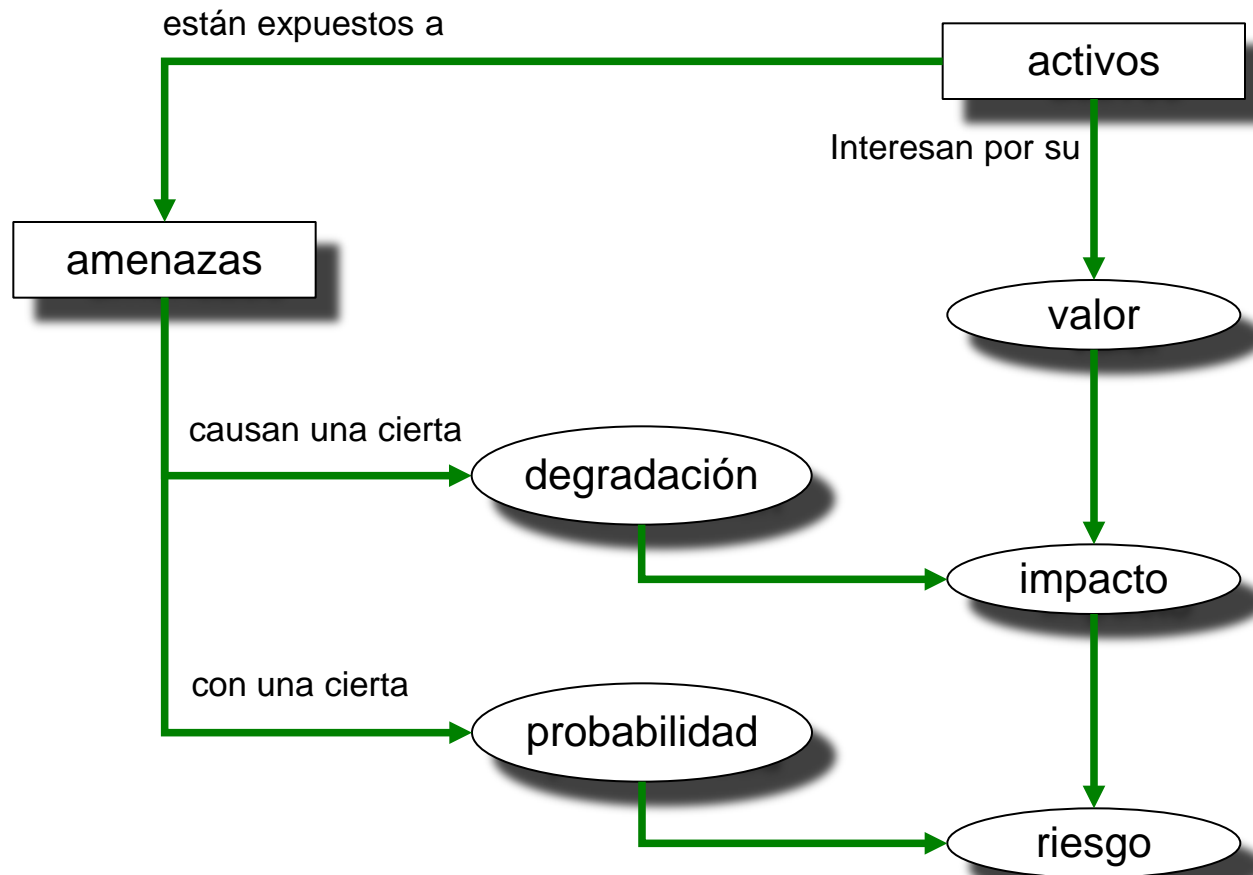
- Evitar
 - eliminar información / servicios / activos
- Mitigar
 - prevenir / reaccionar / recuperar
- Transferir o compartir
 - en términos cualitativos (externalización)
 - en términos cuantitativos (seguros)
- Aceptar
 - el riesgo es parte del negocio



Toma de decisiones



Análisis (potencial)

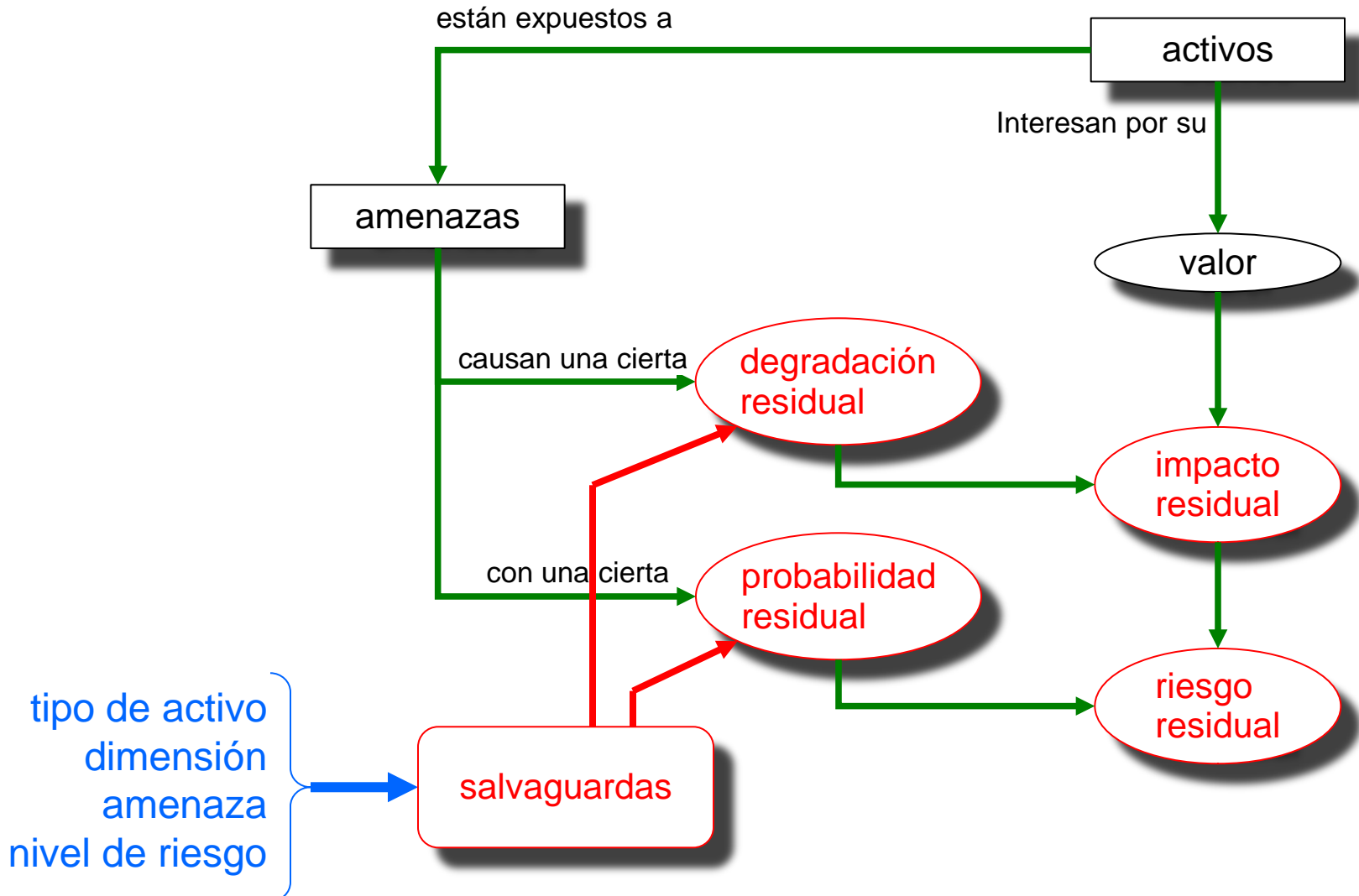


Asegurar todos los tipos de activos

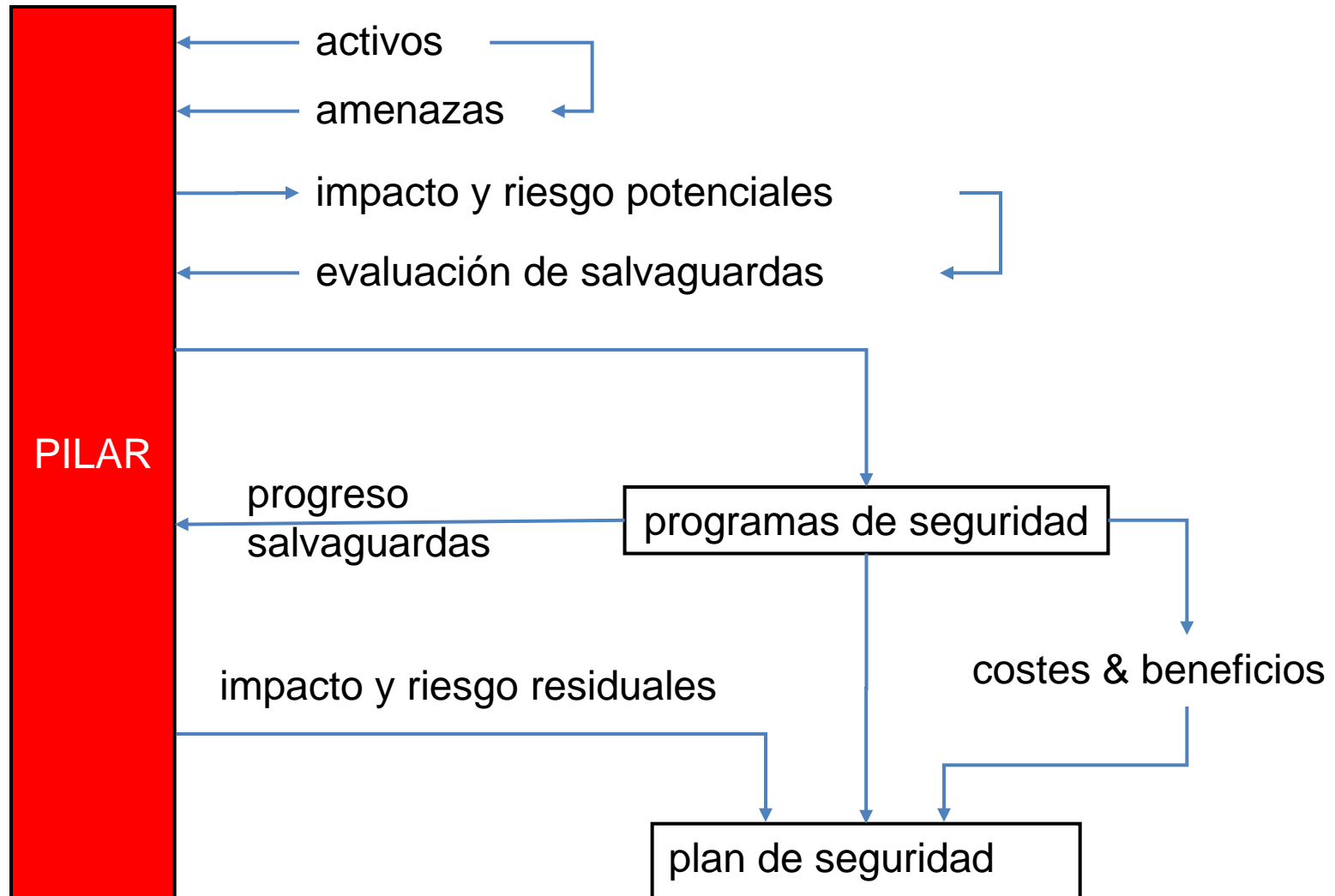
- La información
- Los procesos
- Las aplicaciones
- El sistema operativo
- El hardware
- Las comunicaciones
- Los soportes de información
- Las instalaciones
- El personal



Análisis (residual)



Soporte en herramientas



La herramienta PILAR

— EAR / PILAR

- procedimiento informático-lógico para el análisis del riesgo
entorno de análisis de riesgos
- proyecto CNI → A.L.H. J. Mañas (2003)
- especificación: CCN
Ministerio de Defensa, España
- comité validación: CCN + MAP + FNMT
- parcialmente financiado por el CCN
comercializado como producto independiente





intypedia

INFORMATION SECURITY ENCYCLOPEDIA