dit-upm

Seguridad de la Información
Análisis de Riesgos

José A. Mañas < http://www.dit.upm.es/~pepe/>
Dep. de Ingeniería de Sistemas Telemáticos
E.T.S. Ingenieros de Telecomunicación
Universidad Politécnica de Madrid

Octubre de 2015

Índice

- Gestión de riesgos
- Análisis de riesgos TIC
- Tratamiento de los riesgos TIC

riesgos

- Toda actividad está sujeta a riesgos
  - riesgo = suceso no garantizado
    puede ser positivo: éxito
    puede ser negativo: incidente
- Toda actividad basada en sistemas TIC
  está expuesta a riesgos operacionales (riesgos TIC)
- Es obligación del buen gobierno
  - prevenir los riesgos
  - estar preparados para reaccionar a lo improbable
  - maximizar la posibilidades de
    cumplir con la misión de la organización
- Gestionar los riesgos es un proceso
  cuyo primer paso es conocerlos

Gobierno de las TIC

- Las TIC son una oportunidad pero conllevan un riesgo
- Las decisiones deben equilibrar ambas caras
  - destinando recursos prudentes a los objetivos de negocio
  - destinando recursos prudentes a la protección
- Toda decisión de gobierno debe estar informada
  - la funcionalidad que queremos obtener
  - los riesgos en que incurrimos = su seguridad

dit

percepción del riesgo

nuestra subjetividad respecto del riesgo

- Hay una tendencia natural a obviar lo que no se percibe
  - “eso no me va a pasar a mi” | “eso nunca ocurre”
- Hay una tendencia natural a corregir lo que molesta
  - incluso si no tiene mayores consecuencias
- Psicología del miedo
  - el miedo paraliza
  - la paranoia es irracional
- El temor a dañar nuestra reputación nos radicaliza
  - las medidas preventivas vienen lastradas por la merma de productividad (los usuarios tienen a obviarlas)
  - las medidas reactivas son [maniqueamente] explotadas por las víctimas y sus corifeos

dueño del riesgo

risk owner

- Persona o entidad que tiene la responsabilidad y autoridad para gestionar un riesgo. [UNE Guía 73:2010]

- decide tratar o aceptar un riesgo
  ... y sufre las consecuencias de que el riesgo se materialice

- Las decisiones las debe tomar quien va a sufrir las consecuencias
  - *your business → your risk*

Puntos de vista

- 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 órganos de gobierno ven la seguridad como
  - un límite a las oportunidades que abren las TIC
- Los gestores ven la seguridad como
  - gestión de riesgos = tener los riesgos bajo control

La tecnología es amoral

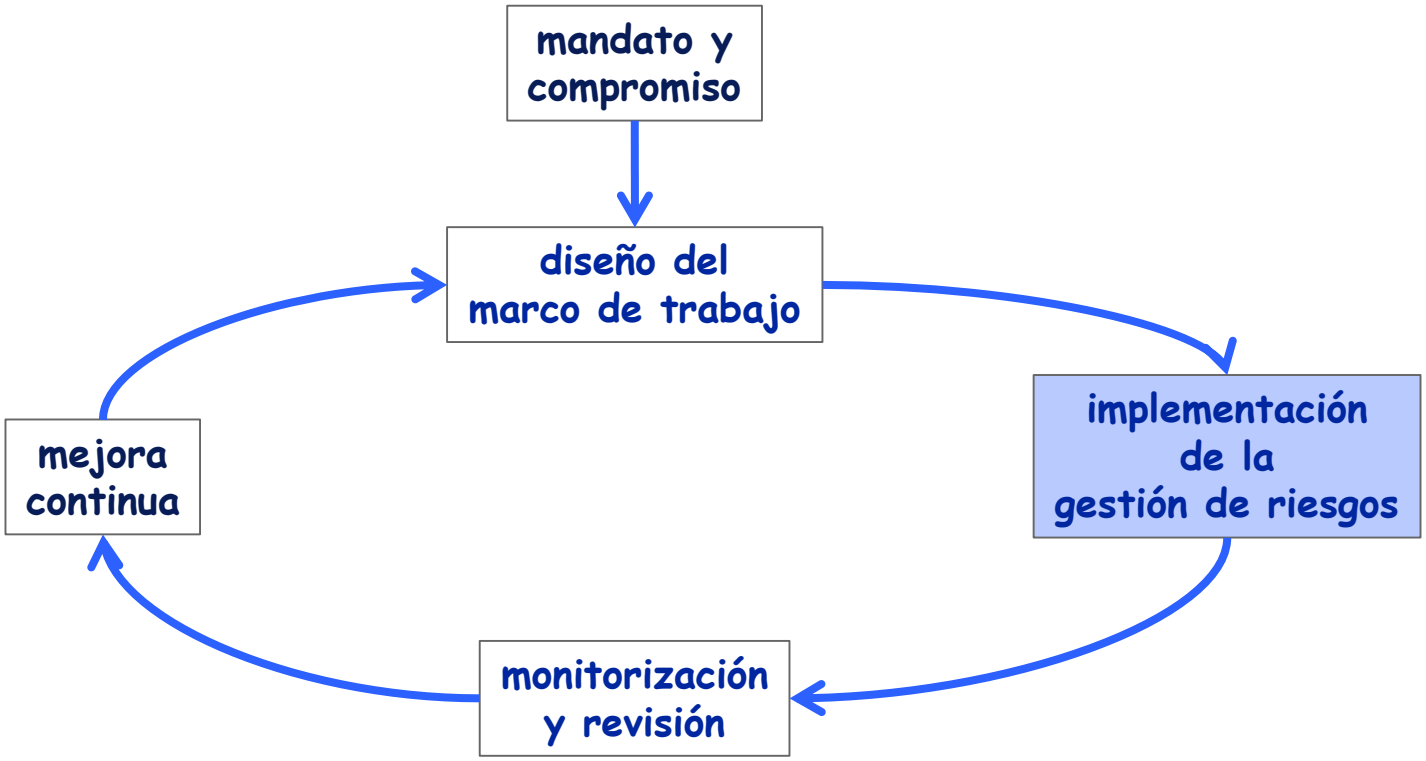
- Lo que simplifica el trabajo de los buenos
  abre oportunidades a los atacantes
- Lo que bloquea a los atacantes
  dificulta el trabajo de los buenos
- La productividad es enemiga de la seguridad

The same solution that keeps out the bad
(specially it if mutates)
will also keep out the good.
P. Herzog

Riesgo

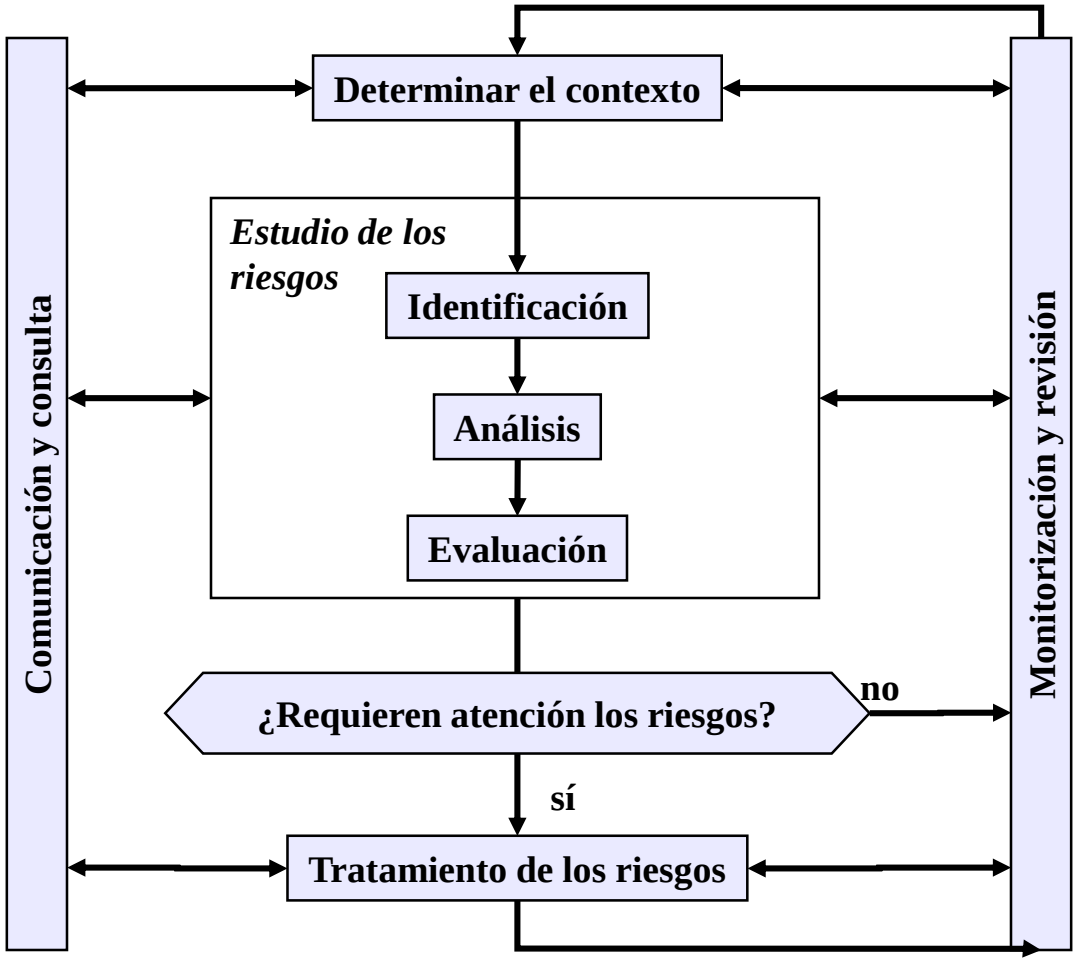
- Riesgo
  - el arte de vivir con sistemas razonablemente seguros
- Análisis de impacto
  - el arte de estimar las consecuencias de una amenaza potencial
- Análisis de riesgos
  - el arte de estimar las consecuencias recurrentes de la inseguridad residual
- Análisis de riesgos y análisis de impacto
  - proporcionan información para tomar decisiones
- Gestión de riesgos
  - analizar y actuar en consecuencia

Gestión de riesgos: el marco



ISO 31000:2009 – Risk management – Principles and guidelines

implementación de ...



Referencias

- USA : NIST SP-800-30:2002
  Risk Management Guide for Information Technology Systems
  - The only mandatory requirement under the FISMA security standards and guidance is the application of the NIST Risk Management Framework — everything else is negotiable.
- AS/NZ : AS/NZS 4360:2004
  Risk management
  - Risk management involves managing to achieve an appropriate balance between realizing opportunities for gains while minimizing losses.

Índice

- Gestión de riesgos
- Análisis de riesgos TIC
- Tratamiento de los riesgos TIC

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
  - custodiar datos
    para que puedan ser utilizados por quien debe cuando quiera
  - 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
- **Trazabilidad**: saber quién ha hecho qué en qué momento
  - para perseguir y mejorar

Tipos de activos

dit

esencial

- Datos / información
- Servicios

negocio

soporte

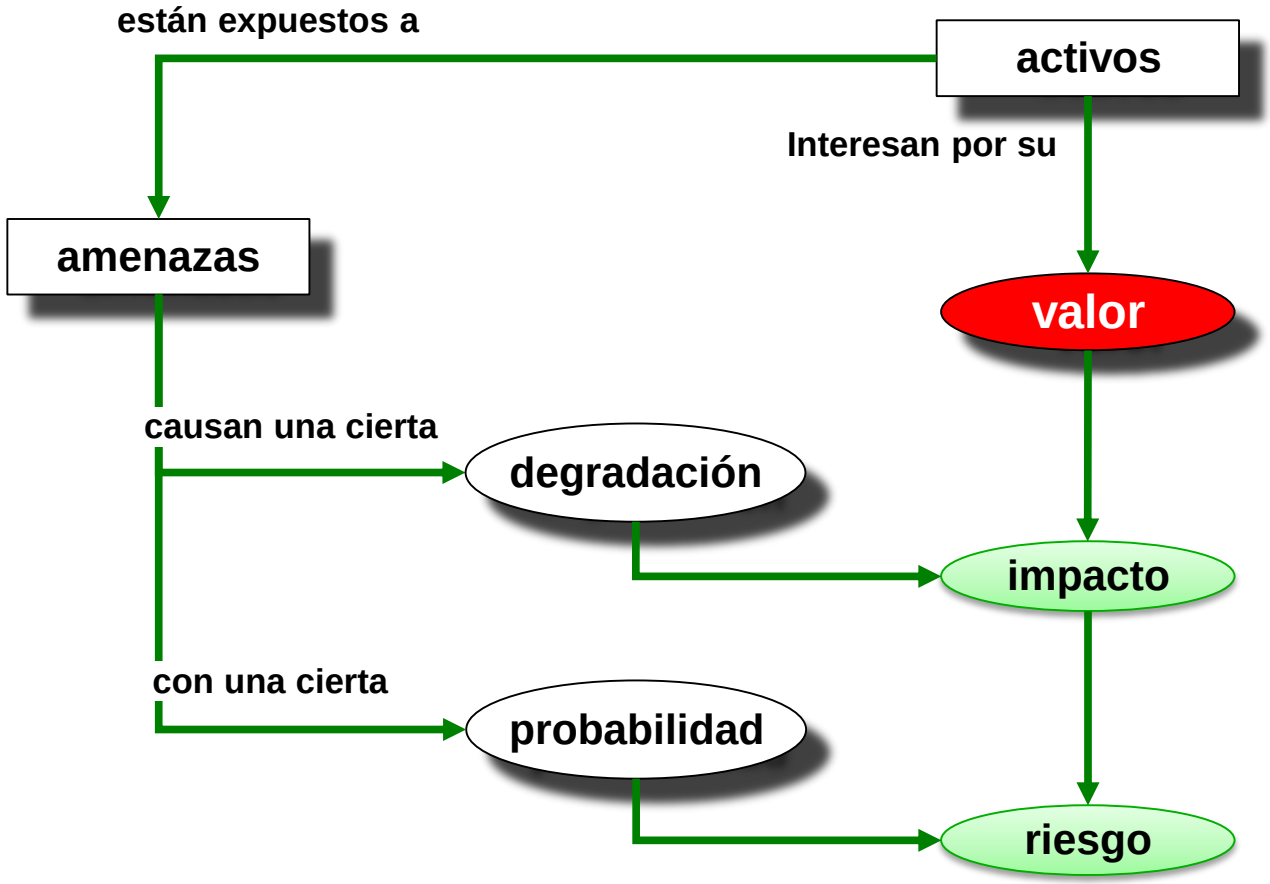
- Aplicaciones (software)
- Equipos informáticos (hardware)
- Redes de comunicaciones
- Soportes de información
- Equipamiento auxiliar
- Instalaciones (locales, etc.)
- Personal

ingeniería
aprovisionamiento

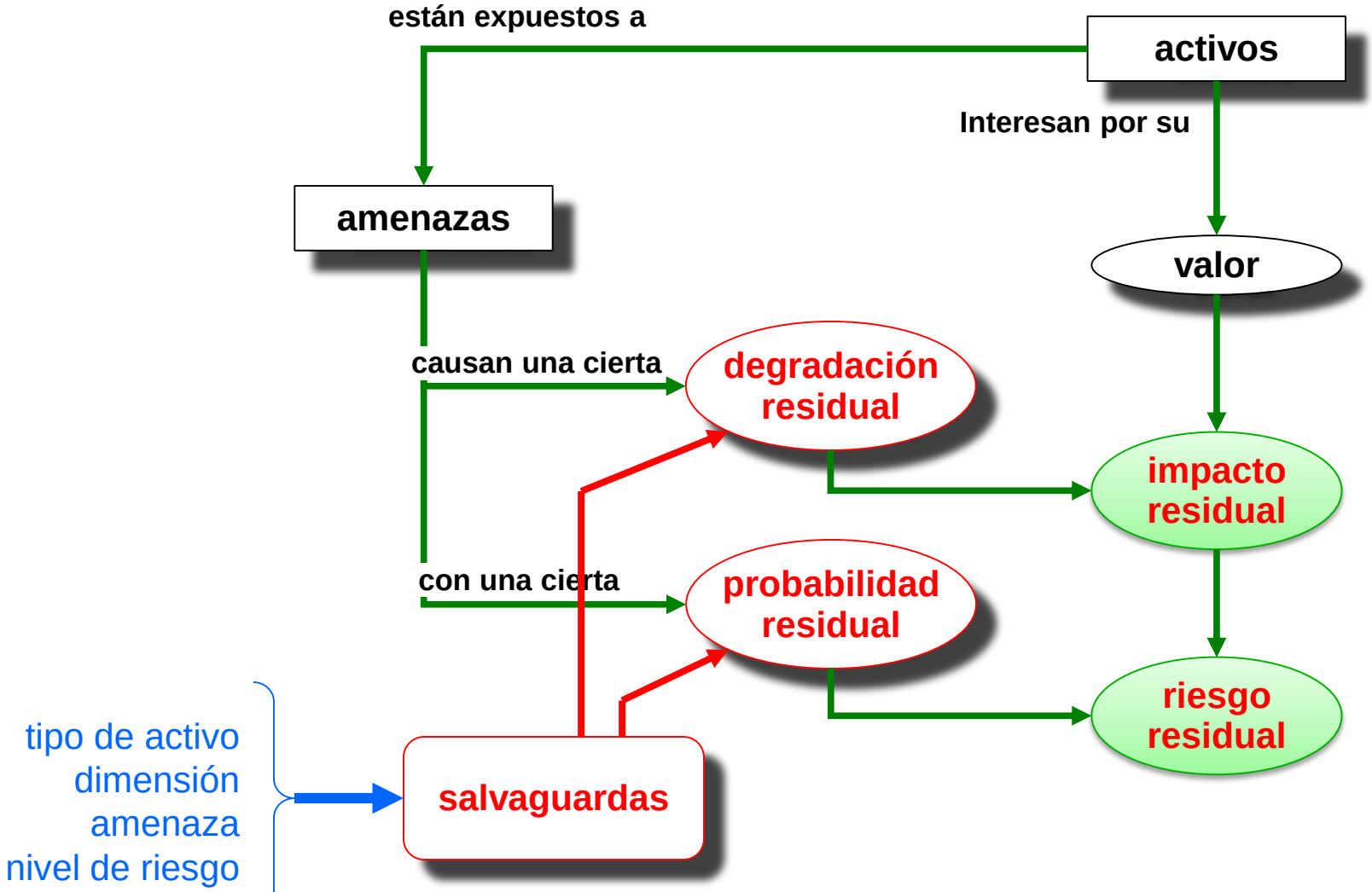
Metodología de análisis de riesgos

- 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

Análisis (potencial)



Análisis (residual)



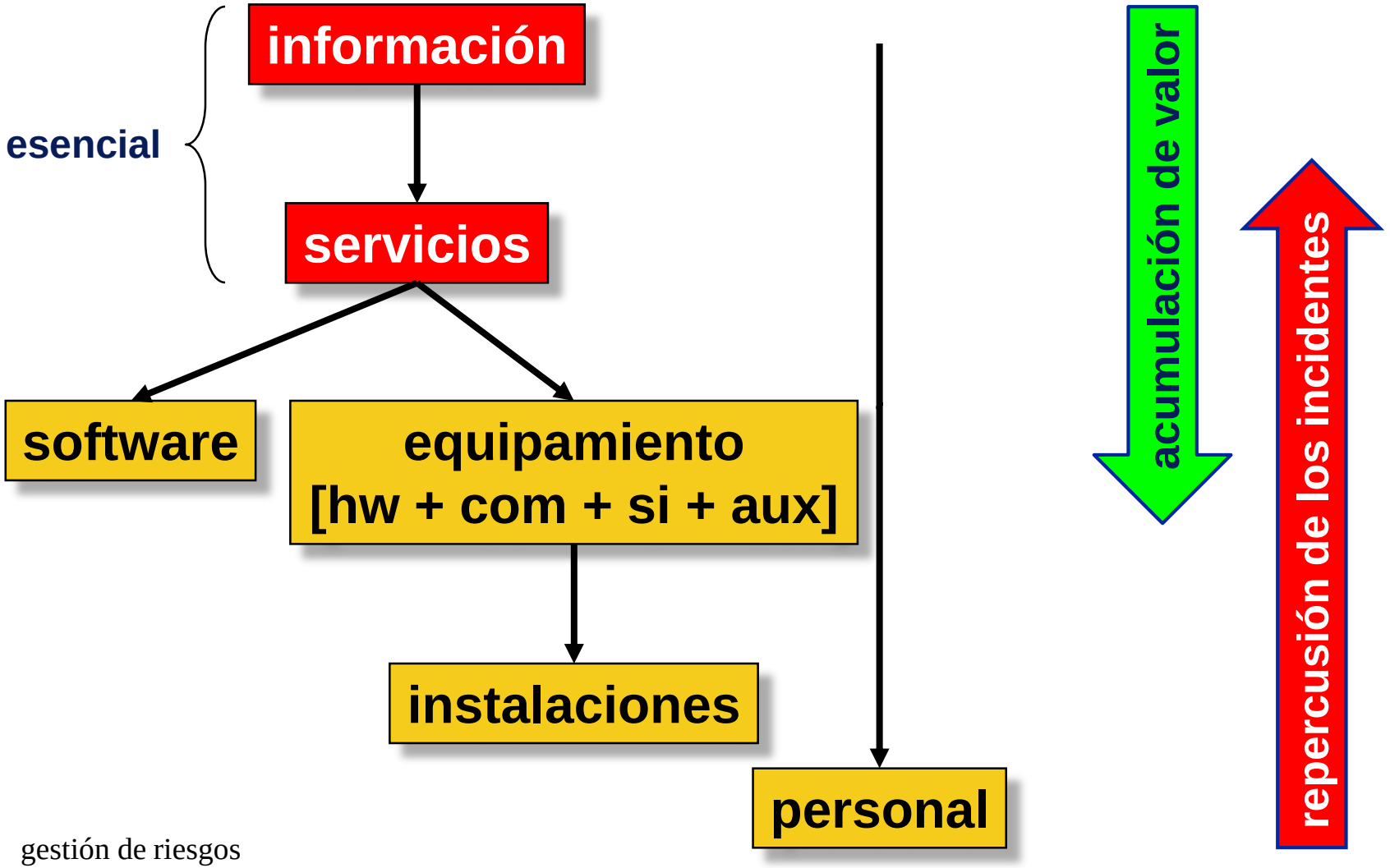
Metodología Magerit / PILAR

```
análisisRiesgos (SistemaInformación si) {
    Contexto contexto= establecerContexto (si);
    Set<Activo> activos= getModeloValor(si);
    Set<Amenaza> amenazas= getMapaAmenazas(si, activos);
    Riesgo potencial= calcula(activos, amenazas);
    Set<Salvaguarda> salvaguardas= necesidad(activos, amenazas);
    evaluaEstadoActual(salvaguardas);
    Riesgo residual= calcula(activos, amenazas, salvaguardas);
}
```

Metodología Magerit / PILAR

```
Set<Activos> getModeloValor(SistemaInformación si) {
    do {
        Set<Activo> activos= descubrimiento(si);
        relaciones(activos, si);
        valoración(activos, si);
    } until (dirección.aprueba(activos));
    dirección.firma(informe(activos));
    return activos;
}
```

Unos activos dependen de otros



Valoración

- Coste que supondría la ocurrencia de una amenaza
  - valor de reposición; reconstrucción
  - 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

Amenazas

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

accidentales

- **naturales**
  terremotos, inundaciones, rayos, ...
- **industriales**
  electricidad, emanaciones, ...
- **humanas**
  errores y omisiones

deliberadas (intencionales)

- intercepción pasiva o activa
- intrusión, espionaje, ...
- robo, fraude, ...

dit

Análisis de amenazas

- Identificación
  - ¿qué puede ocurrir [que deba preocuparnos]?
  - por experiencia (propia o ajena)
  - por la propia naturaleza del activo (clase)
- Cuantificación
  - probabilidad de ocurrencia
    - es difícil predecir el futuro (¿subjetivo?)
    - ARO – Annual Rate of Occurrence
      tasa anual: 0.1 - 1 - 10 - 100
  - consecuencias [sobre el valor de los activos]
    - es fácil imaginar el daño
    - 0% - 1% - 10% - 100%

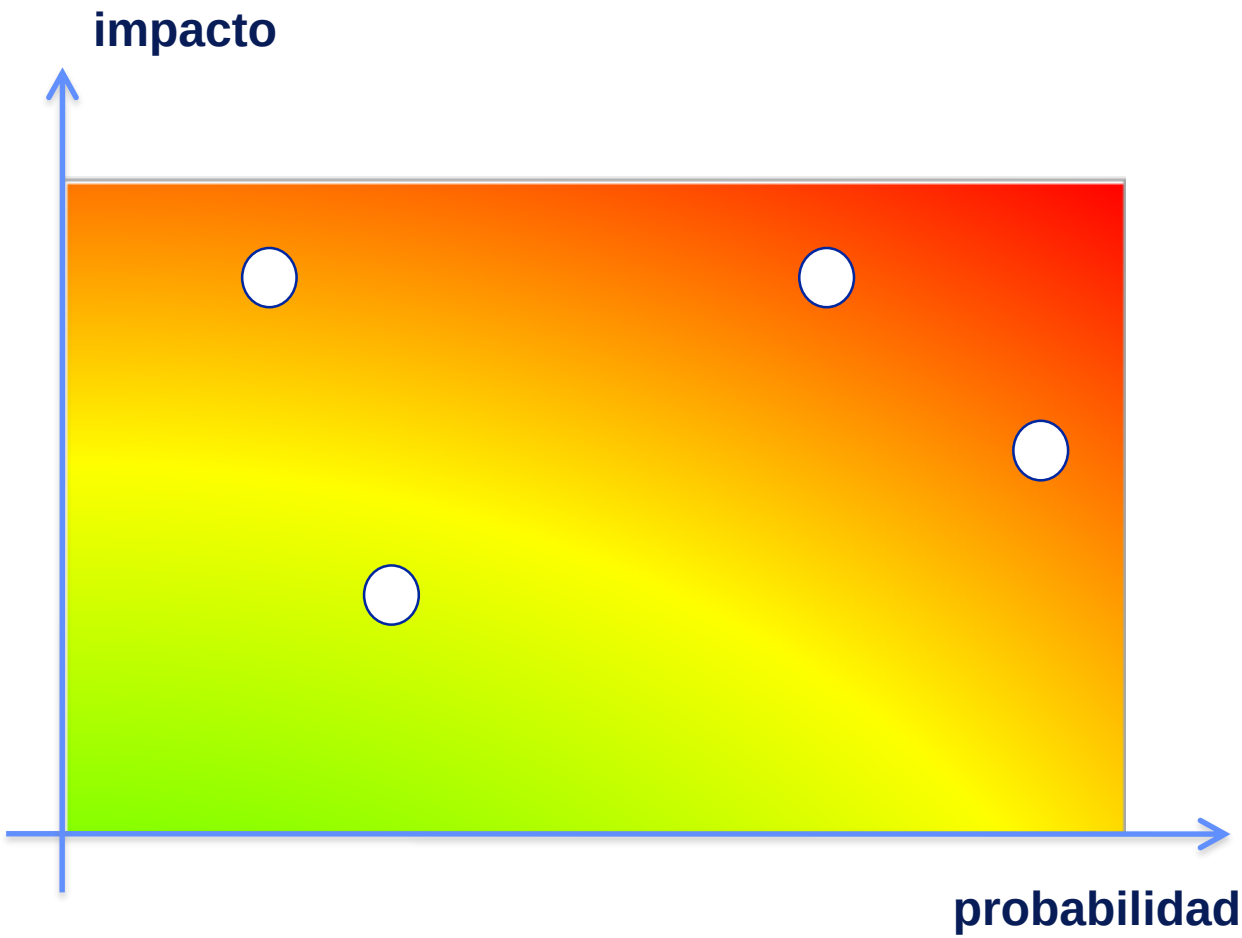
Impacto (indicador)

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

Riesgo (indicador)

- 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

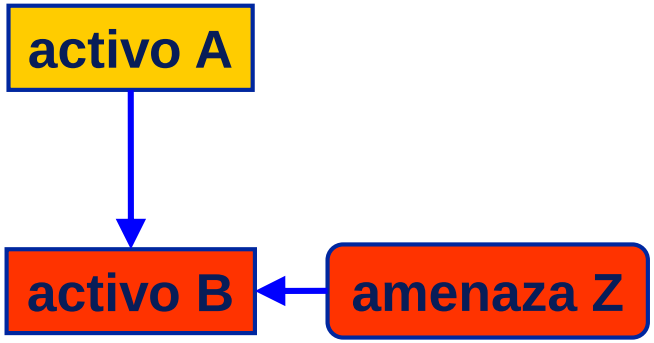
Estimación cualitativa



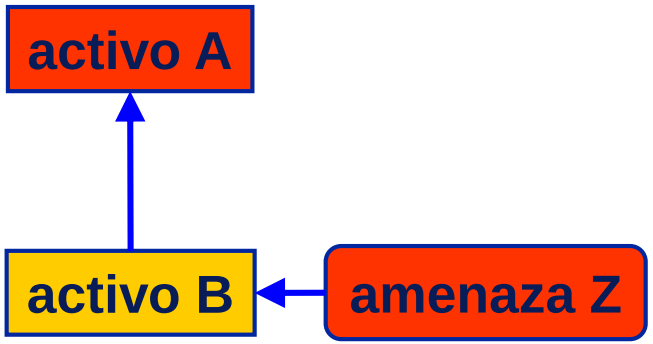
Impacto & riesgo

- Si el activo A depende del activo B,
  el valor de A se acumula en B
  en la proporción en que A depende de B

acumulado



repercutido

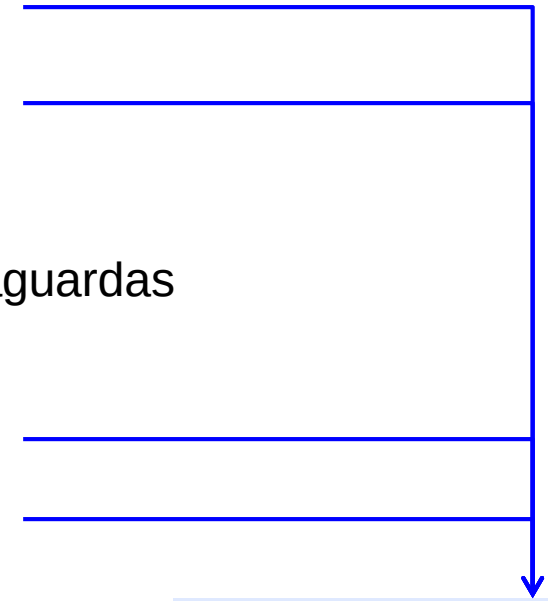


Índice

- Gestión de riesgos
- Análisis de riesgos TIC
- Tratamiento de los riesgos TIC

Opciones de tratamiento

- Se evita
  - eliminando activos
  - cambio de arquitectura
- Se mitiga
  - poniendo o mejorando salvaguardas
- Se transfiere | se comparte
  - cualitativo: externalizació
  - cuantitativo: seguro
- Se acepta
  - ... monitprización + reacción
  - hay que cuidar la reputación:
    - departamento de comunicación
    - departamento legal



hay que analizar otro sistema

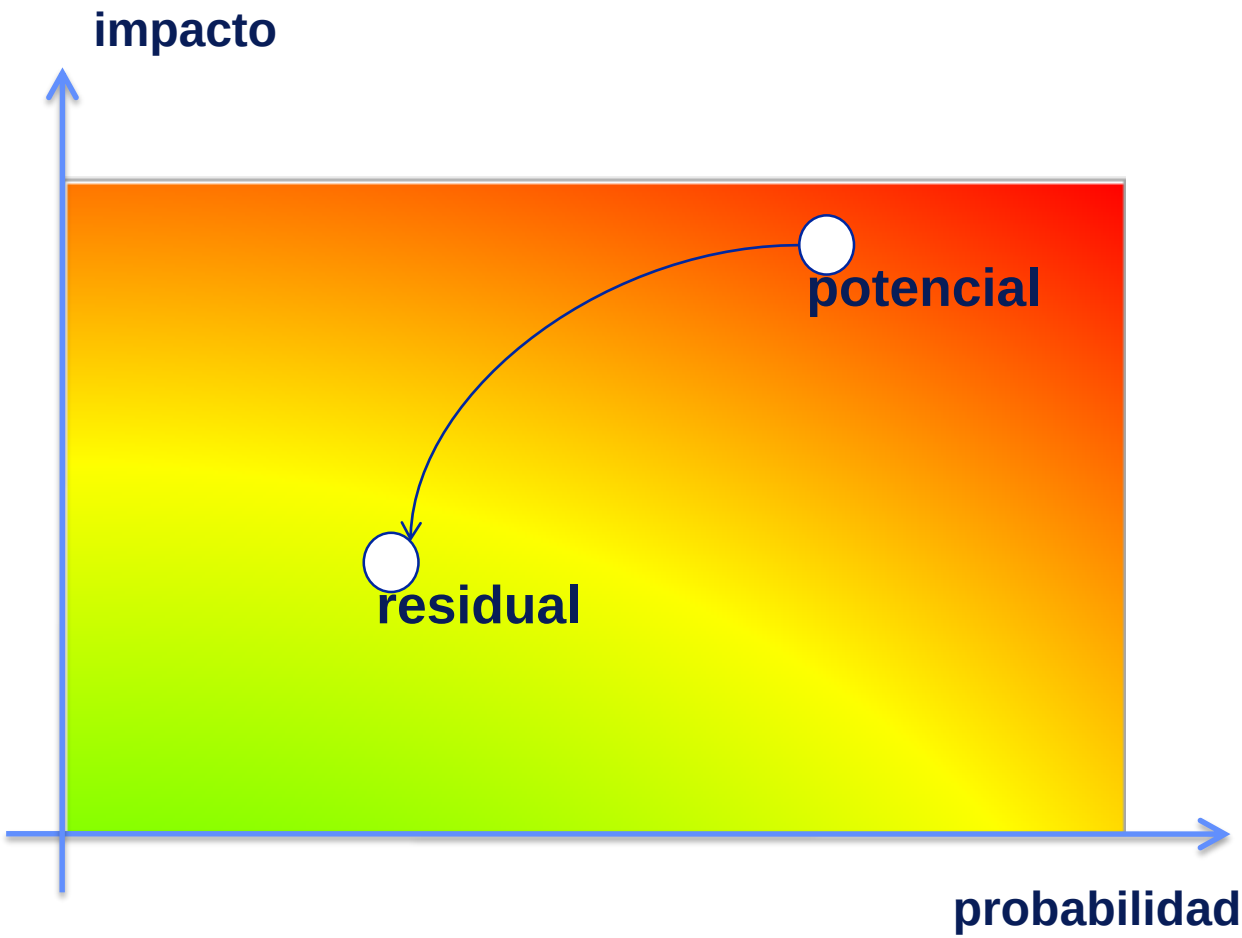
Salvaguardas

- MAGERIT
  - procedimiento o mecanismo tecnológico que reduce el riesgo
  - sinónimos: medidas de seguridad, contra medidas, controles
- ISO
  - Safeguard. A practice, procedure or mechanism that reduces risk
  - synonyms: security measures, countermeasures, controls

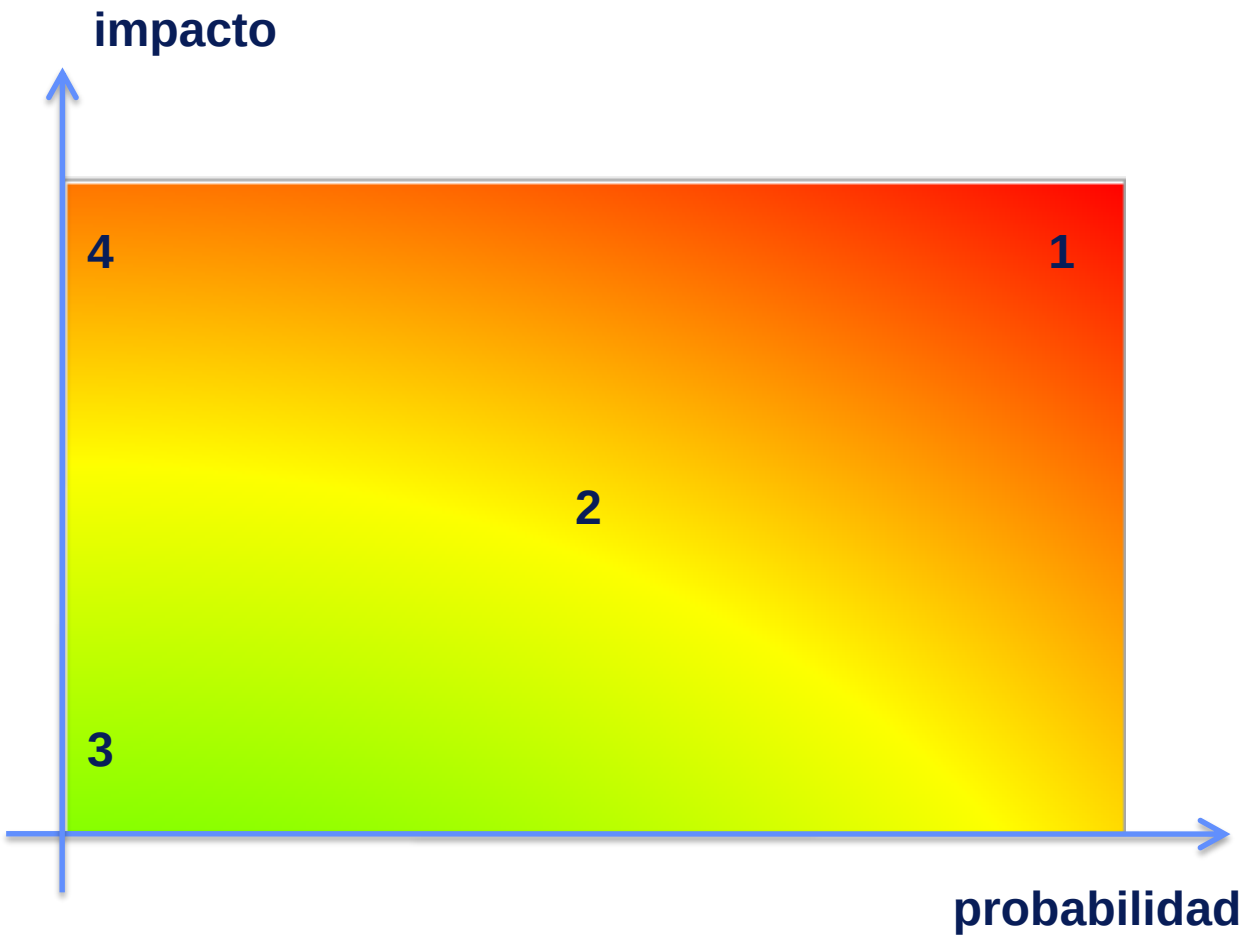
Indicadores residuales

- Impacto
  - lo que puede pasar
- Impacto residual
  - el que queda tras contabilizar las medidas de seguridad adoptadas
- Riesgo
  - lo que probablemente pase
- Riesgo residual
  - el que queda tras contabilizar las medidas de seguridad adoptadas

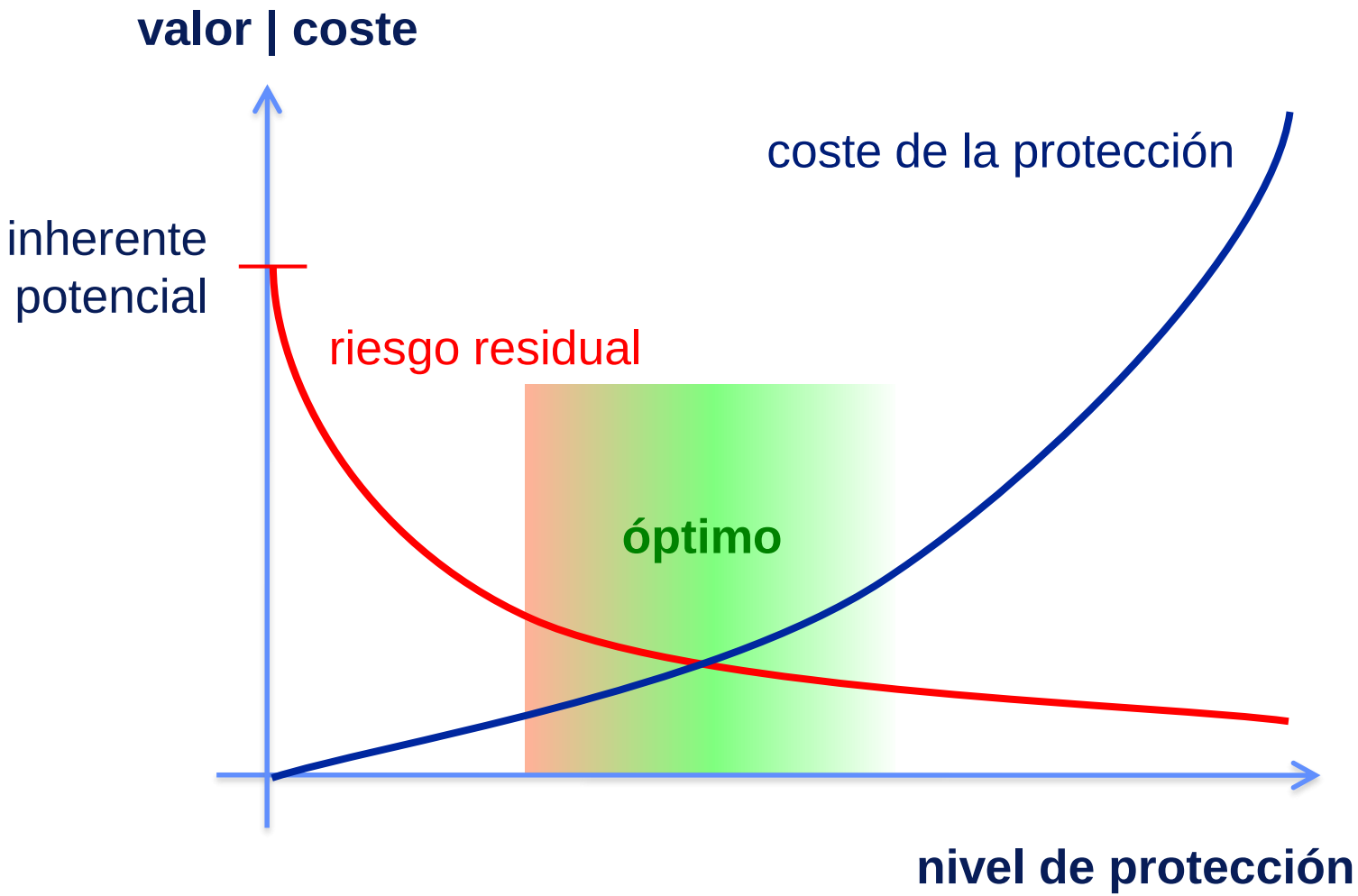
Mitigación de riesgos



Evaluación en términos de negocio



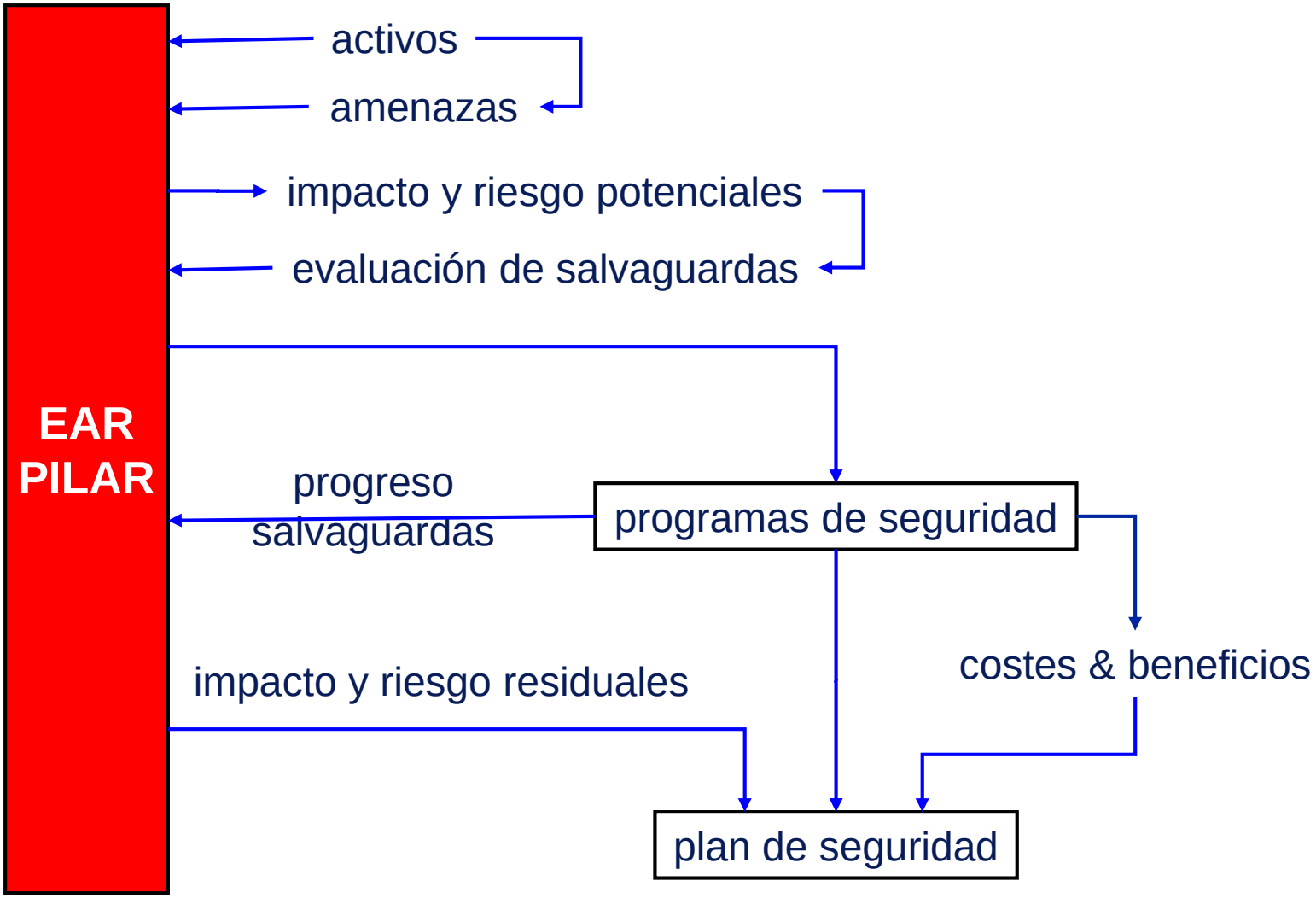
equilibrio valor-coste



Aceptación del riesgo

- Es una opción
  - honrada y necesaria
  - pero peligrosa
    - el análisis dice cuán peligrosa
- Debe ser tomada EXPLÍCITAMENTE por negocio
  - nunca puede ser una decisión técnica

Soporte en herramientas



Conclusiones

- 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 riesgos no es simple

... lleva tiempo
... cuesta dinero
... no vale una vez y para siempre

- Muchos activos
  - los sistemas son complejos
- Activos de muchos tipos
  - información, servicos
  - 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

¿Cuándo?

- 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

Interés de un análisis del riesgo

- Conciencia a [los miembros de] la organización
  - a la dirección y a los empleados
- Identifica activos, amenazas y controles
  - modelo de valor de la organización
  - mapa de riesgos
  - estado de riesgo
- Base razonada para tomar decisiones
  - juicio sobre la eficacia de los controles, actuales y futuros
  - DRES: requisitos específicos de seguridad
- Justificación del gasto en seguridad

Bibliografía

- Magerit v3 - 2012
  - Metodología de análisis y gestión de riesgos de los sistemas de información
  - http://administracionelectronica.gob.es/
- PILAR
  - implementación de magerit++
  - http://www.pilar-tools.com/es/