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 2014

Índice

- Seguridad de la información
- Análisis de riesgos
- Tratamiento de los riesgos
- Continuidad de negocio
- Fin

dit

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

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

Los sistemas de información

- 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

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

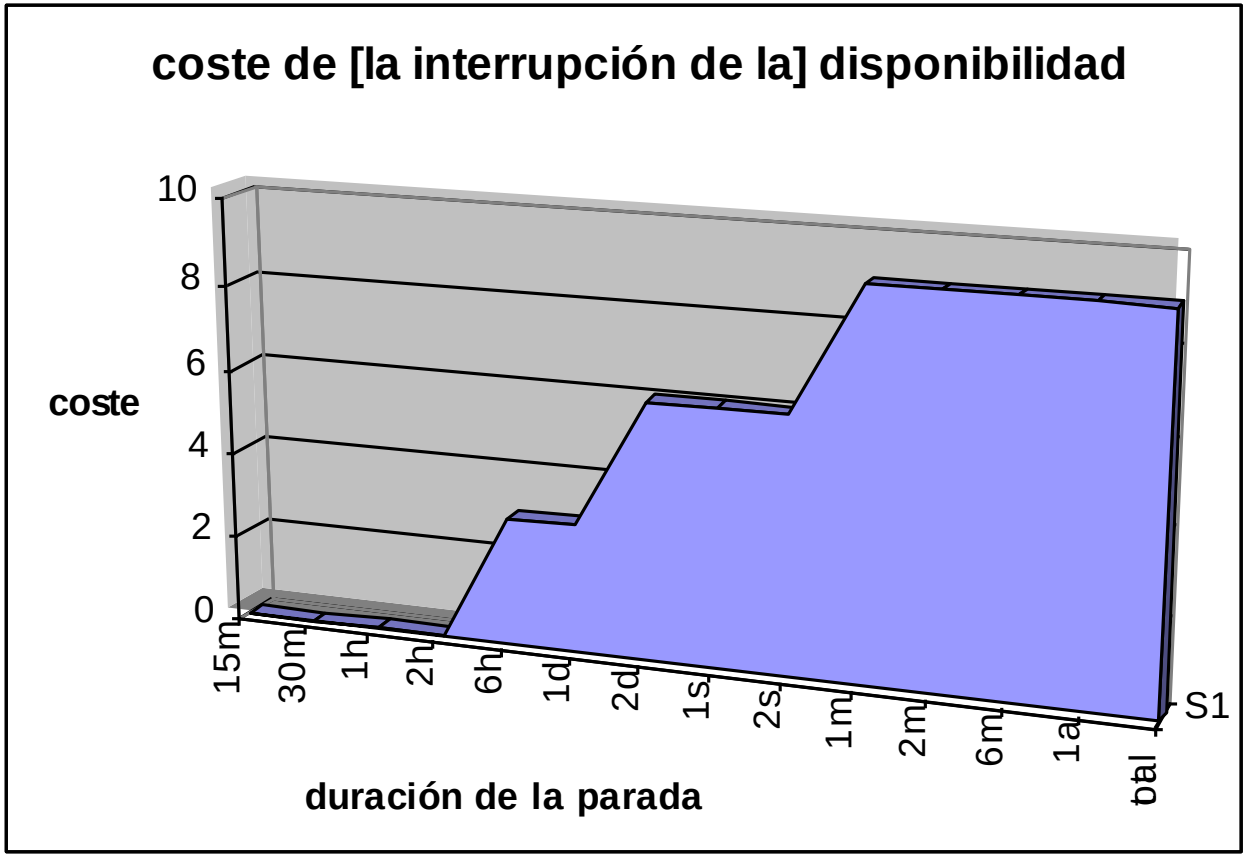
Consecuencias

- 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]

- Autenticidad = integridad [de los meta-datos]
- Trazabilidad = integridad [de los registros de actividad]

- Fallos de disponibilidad → interrupción del servicio
  - medios alternativos
  - restauración de los medios habituales

Coste de la interrupción



Asegurar todos los niveles

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

Definiciones

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

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

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

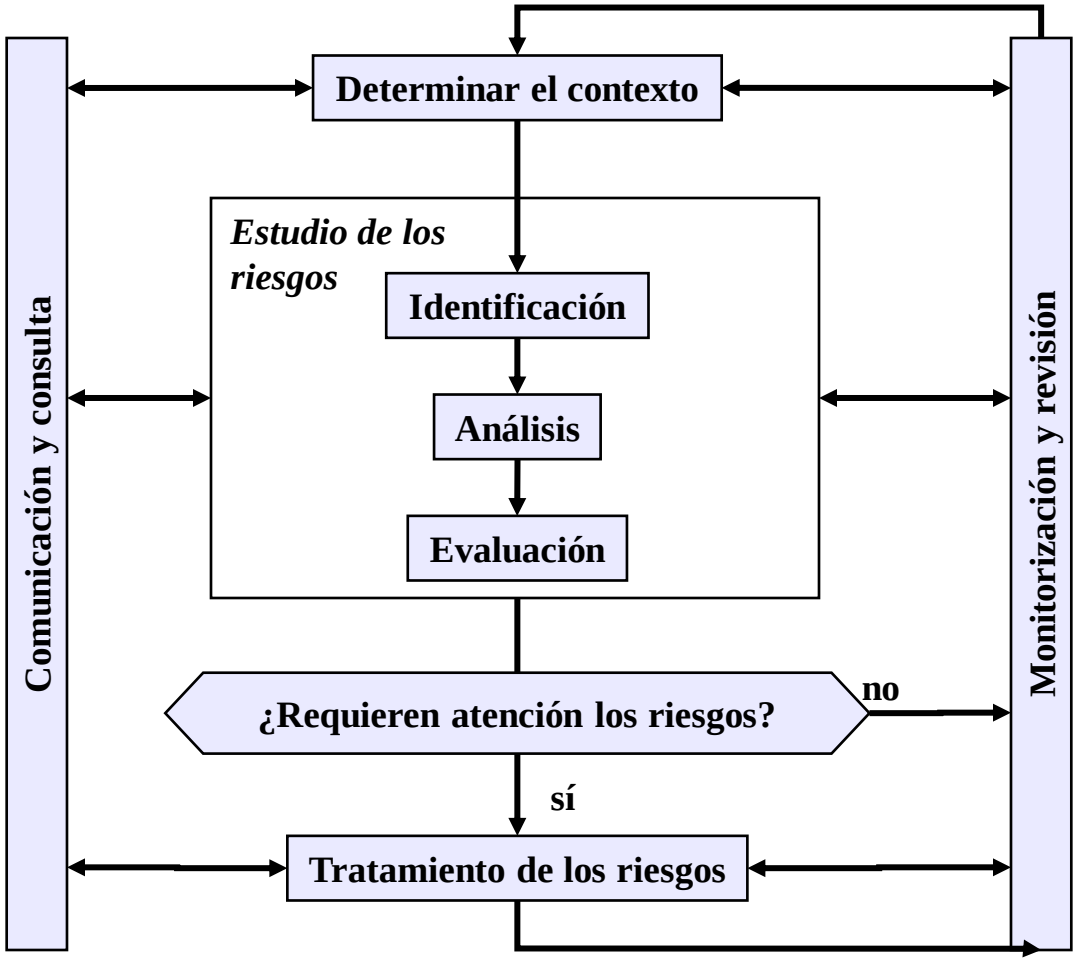
Riesgo

- 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 + aplicar medidas

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.

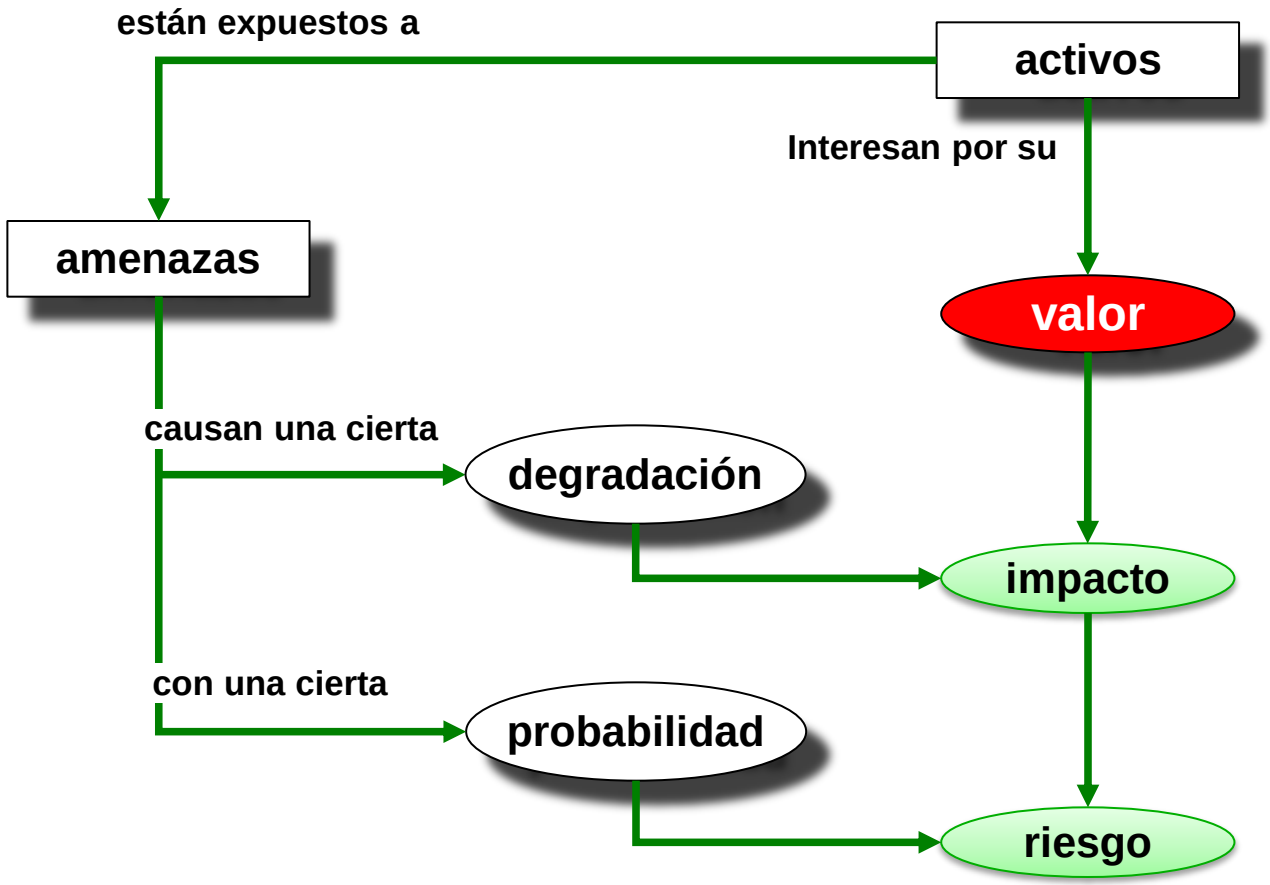
Gestión de riesgos



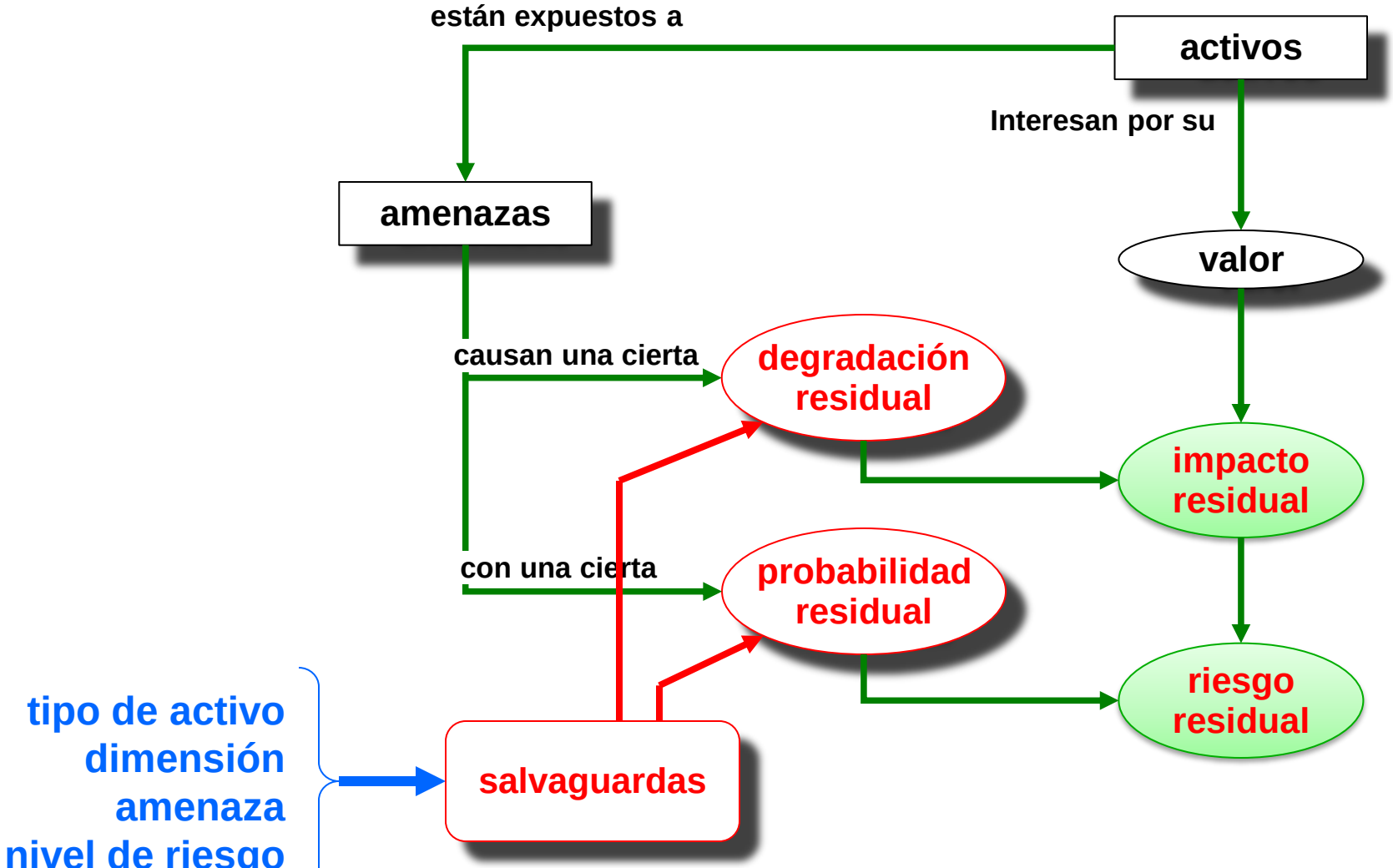
Índice

- Seguridad de la información
- Análisis de riesgos
- Tratamiento de los riesgos
- Continuidad de negocio
- Fin

Análisis (potencial)



Análisis (residual)



Roles

- El responsable de la información (N)
  - valora los requisitos de seguridad de la información
- El responsable del servicio (N)
  - valora los requisitos de seguridad del servicio
- El analista de riesgos
  - propaga requisitos
  - selecciona y evalúa salvaguardas
  - informa del riesgo
- El propietario del riesgo *(risk owner)*
  - evalúa el riesgo
  - toma las decisiones de asunción del riesgo
  - *has the accountability and authority to manage the risk*

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

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

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;
}
```

Activos

- 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.

Tipos de activos

- Servicios
- Datos / información

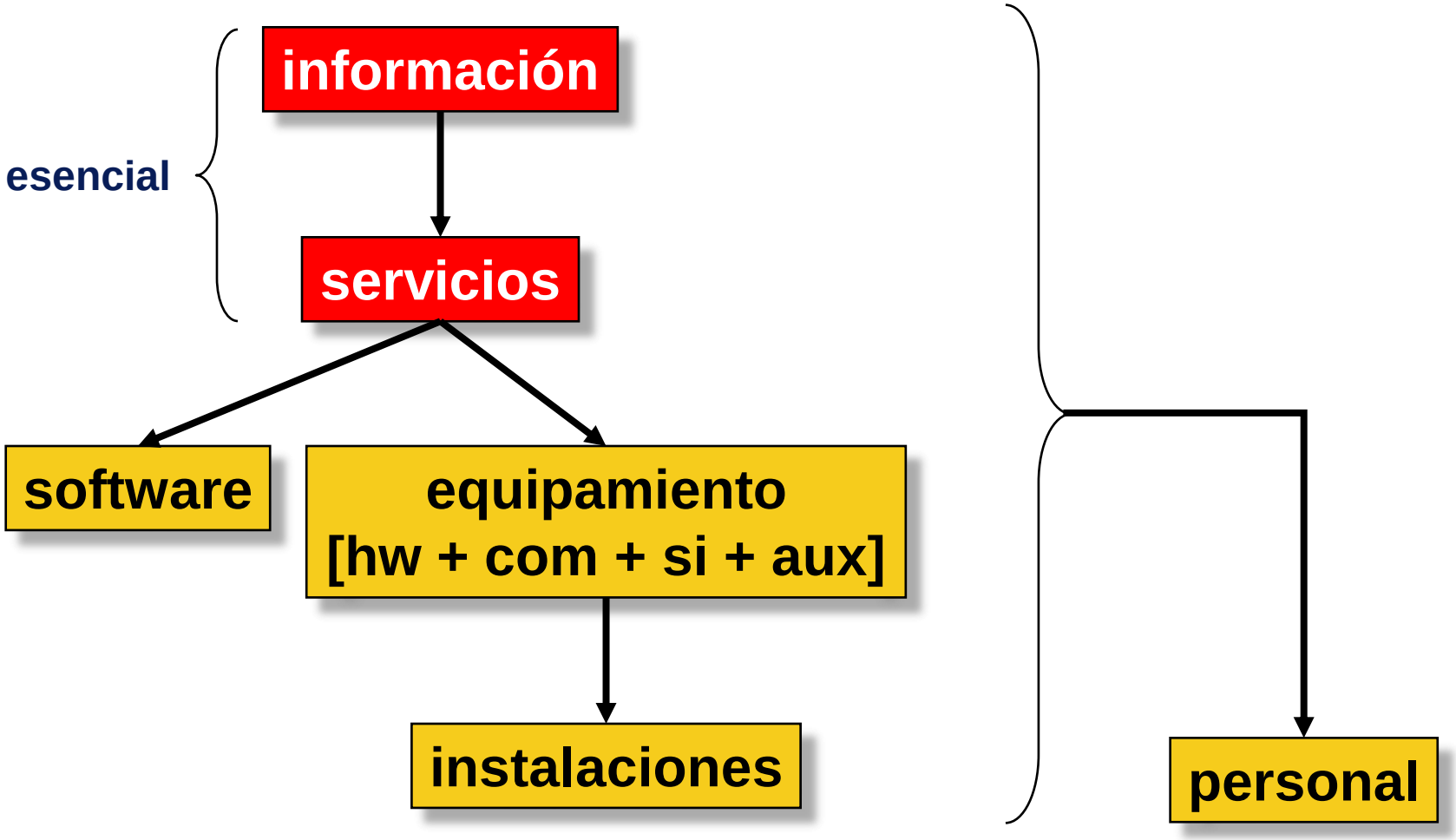
- **Datos / información**
- **Servicios**

negocio

ingeniería
aprovisionamiento

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

Unos activos dependen de otros



dit

Acumulación y repercusión

- 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

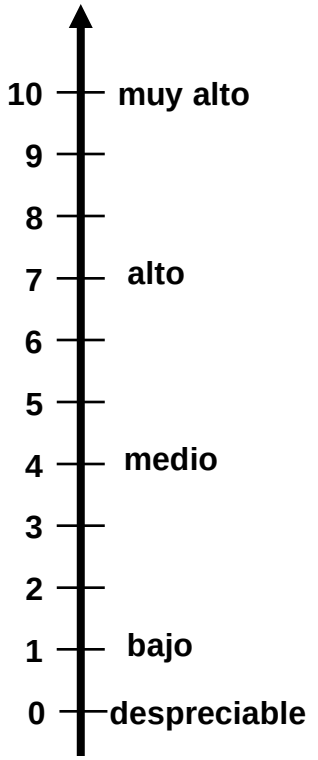
Valoración

- 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

Valor cualitativo

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

valor	*criterio*	
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	



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, ...

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
  - consecuencias [sobre el valor de los activos]
    - en magerit se llama **degradación**

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 cuantitativa

- impacto = valor $\times$ degradación
- riesgo = impacto $\times$ frecuencia

Estimación cualitativa

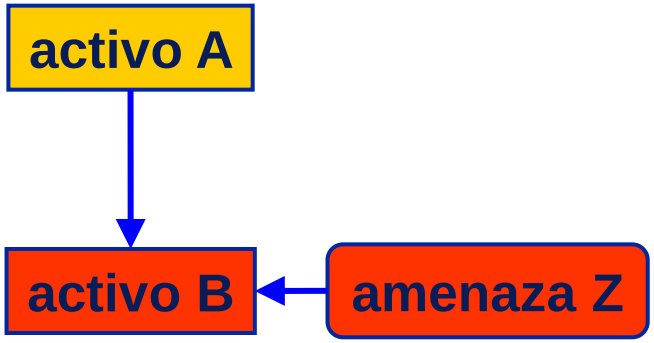
impacto						
MA	alto	muy alto	muy alto	muy alto	muy alto
A	medio	alto	alto	alto	alto
M	bajo	bajo	medio	medio	medio
B	bajo	bajo	bajo	medio	medio
MB	muy bajo	muy bajo	muy bajo	muy bajo	bajo
	PF	FN	F	MF	EF

probabilidad

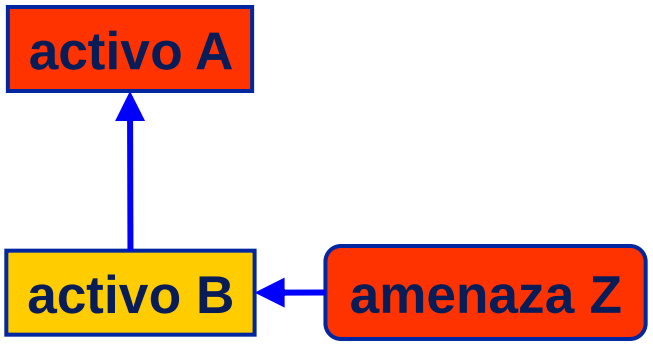
Impacto & riesgo

- 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



Salvaguardas

- 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

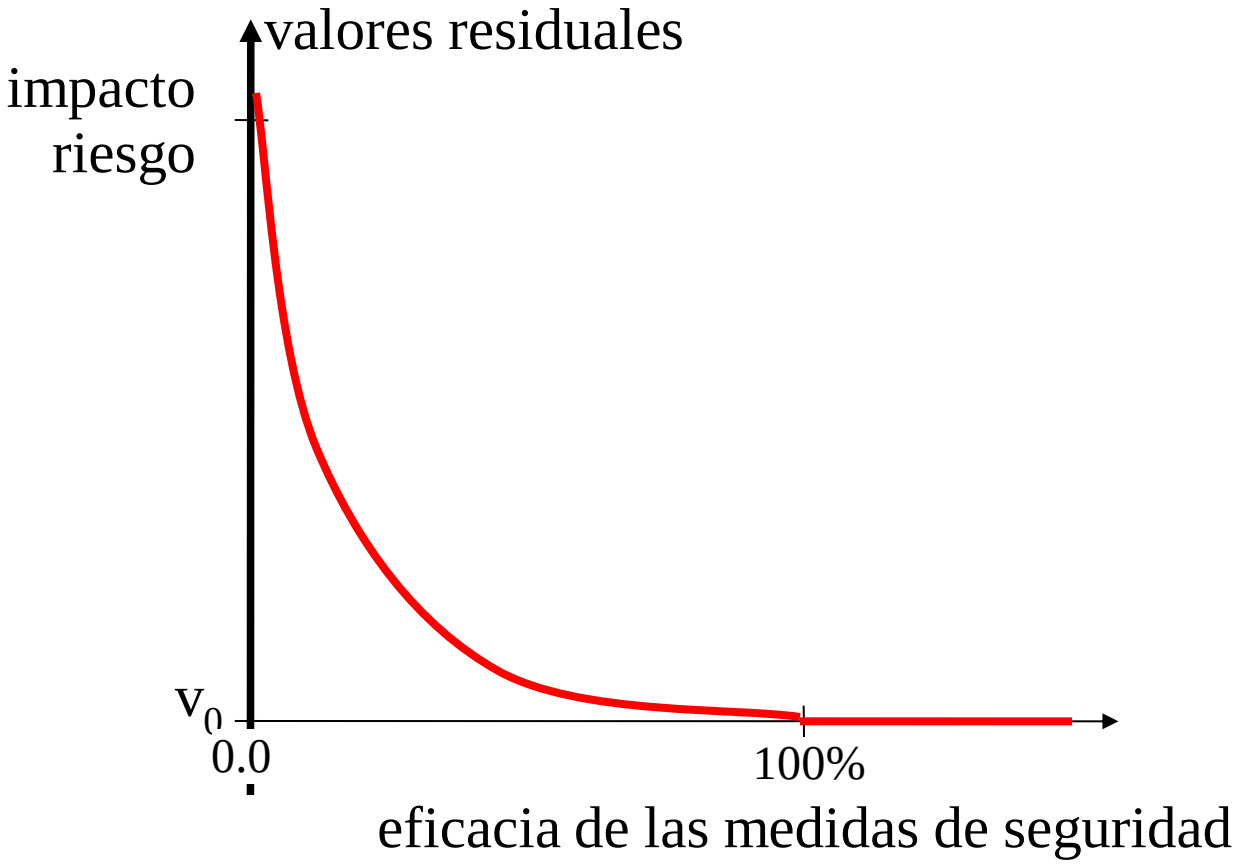
¿Qué salvaguardas se requieren?

1. Se necesita una lista de posibles salvaguardas
   - aconsejado por expertos
   - estándares (ej. **ENS**, 27002, PCI-DSS, 15408 PP, ...)
   - leyes, reglamentos, práctica sectorial
2. Hay que casar las salvaguardas con las amenazas identificadas
   - se prepara una Declaración de Aplicabilidad)
     (SoA – Statement of Applicability)
3. Se evalúa el despliegue actual:
   - existencia (o ausencia)
   - efectividad del despliegue

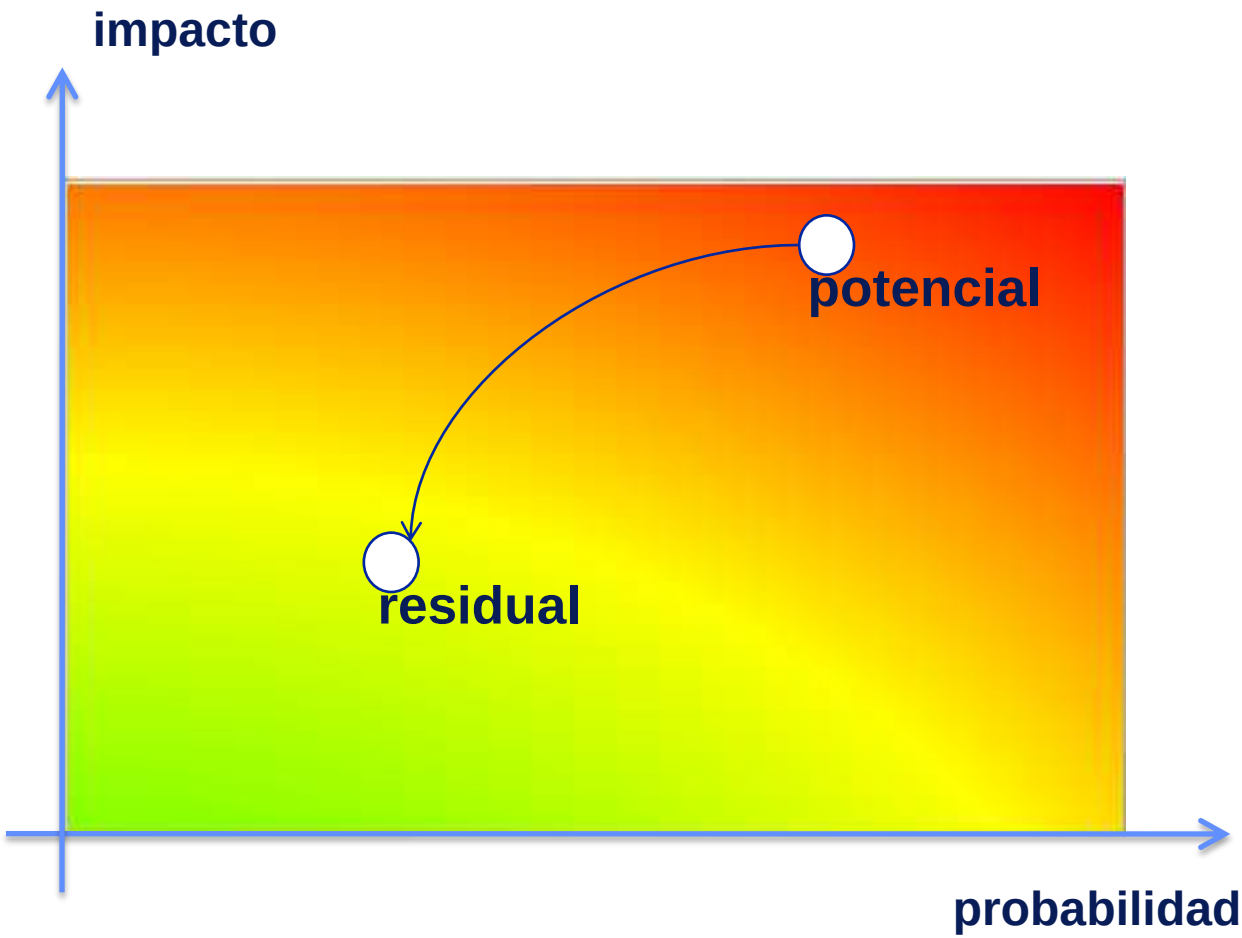
Indicadores residuales

- 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

Impacto y riesgo residuales



Mitigación de riesgos



Índice

- Seguridad de la información
- Análisis de riesgos
- Tratamiento de los riesgos
- Continuidad de negocio
- Fin

¿Qué hacer con el riesgo?

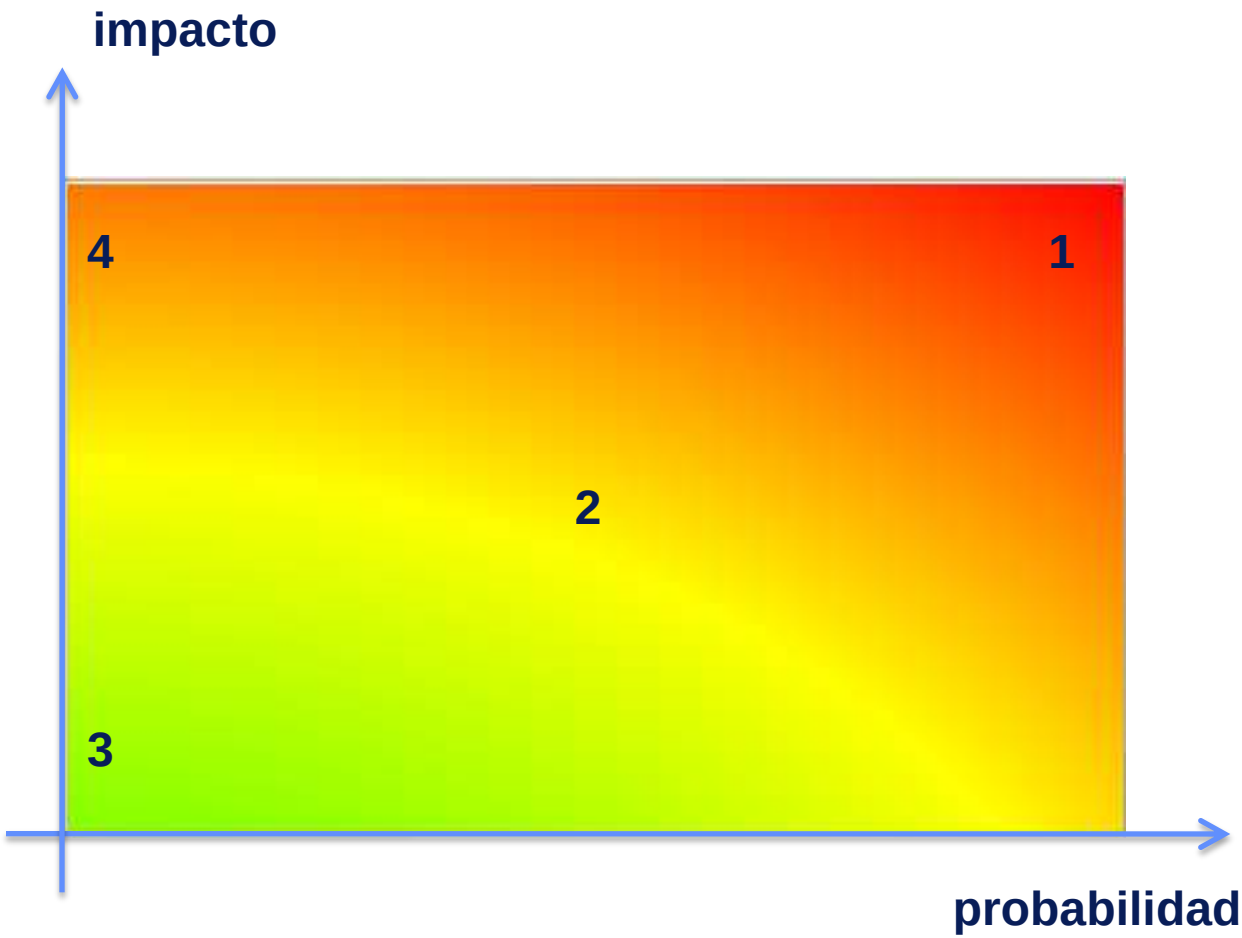
- Se evita
  - si se puede ... es la solución ideal
  - prescindir de activos
- Se reduce | se mitiga
  - ocurre menos
  - impacto limitado
- Se transfiere | se comparte
  - se le pasa a otra organización
  - ya no es [sólo] “mi problema”
- Se asume | se acepta
  - pasa a contabilizarse como gasto operacional
  - puede ser una oportunidad

Opciones de tratamiento

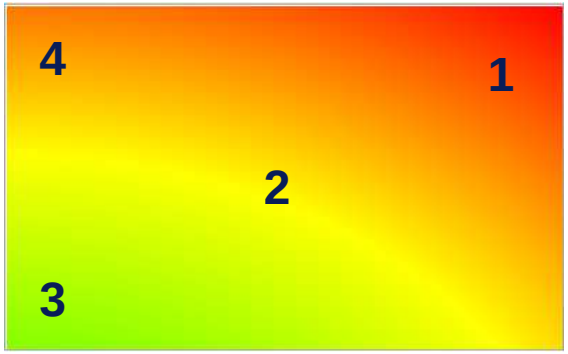
- Se evita
  - eliminando activos
  - cambio de arquitectura
- Se mitiga
  - poniendo o mejorando salvaguardas
- Se transfiere | se comparte
  - cualitativo: externalizació
  - cuantitativo: seguro
- Se acepta
  - ... monitprización + reacción
  - hay que cuidar la reputación:
    - departamento de comunicación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

hay que analizar otro sistema

Evaluación en términos de negocio



Acciones



- Zona 1
  - debemos atender a estos riesgos, sacándolos de la zona 1
- Zona 2
  - podemos negociarlo
  - ¿cómo está la competencia?
- Zona 3
  - podemos olvidarnos o asumir más riesgo
- Zona 4
  - probablemente las medidas preventivas sean irrelevantes
  - hay que estar preparados para detectar y reaccionar con presteza, limitando el impacto
    o tener un plan alternativo

Tiempos

- Todo lo que podamos prevenir ...
  - ... si se justifica el coste
- Escenarios de desastre previstos
  - si es que el incidente es previsible
- Gestión de crisis
  - indicadores predictivos
  - detección
    y escalado de la alarma
  - gestión de los afectados
    sistemas, negocio, clientes, sociedad
  - recuperación
    business as usual?

esto es aplicable en riesgos
que admiten una
disminución de probabilidad

esto es aplicable en riesgos
de alto impacto

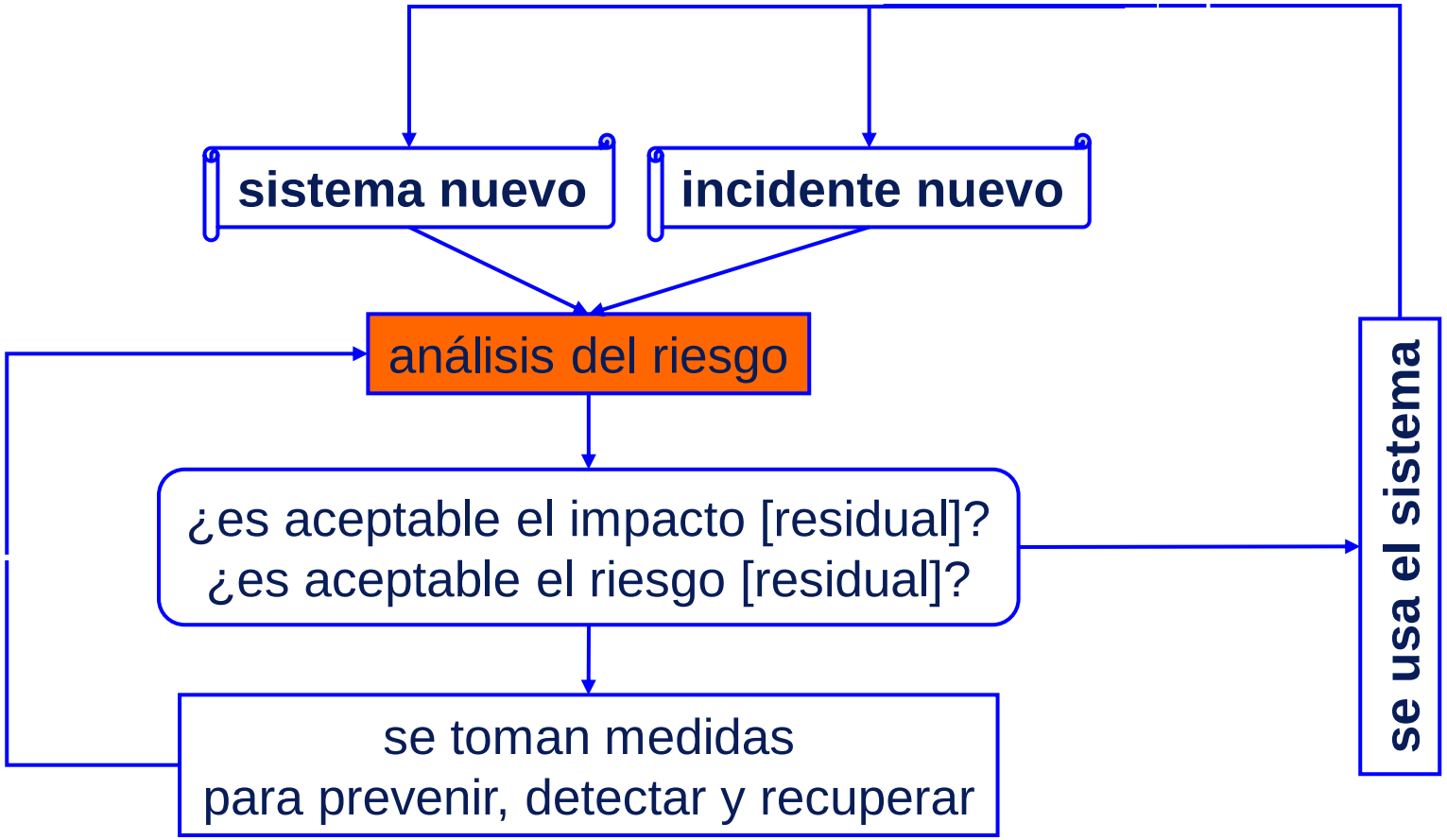
hay que dedicarle tanto más estudio
cuanto mayor es el impacto potencial

Regulación & cumplimiento

- Son respuestas ‘rápidas’ frente a escenarios que quizás nunca más se darán
  - calman la alarma social
  - ¿evitan organizaciones suicidas?
  - es difícil validar su efecto
    - se trata de una intervención “rápida” en un proceso impredecible
- Algunas medidas se toman por miedo al incumplimiento
  - quedar fuera del mercado
  - acabar en prisión

lo que no puede ser es que te pillen con los deberes sin hacer

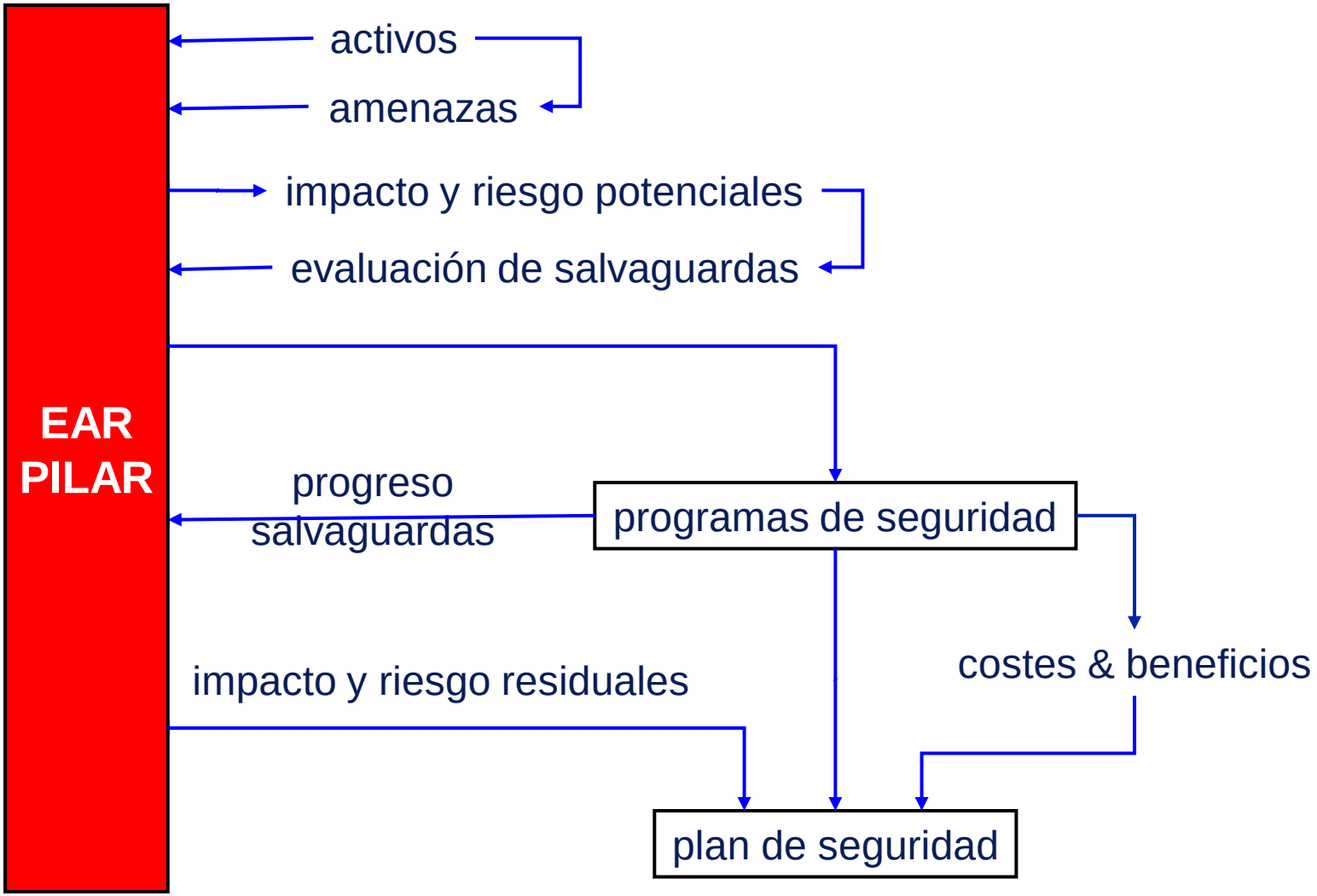
Ciclos de gestión de riesgos



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



Índice

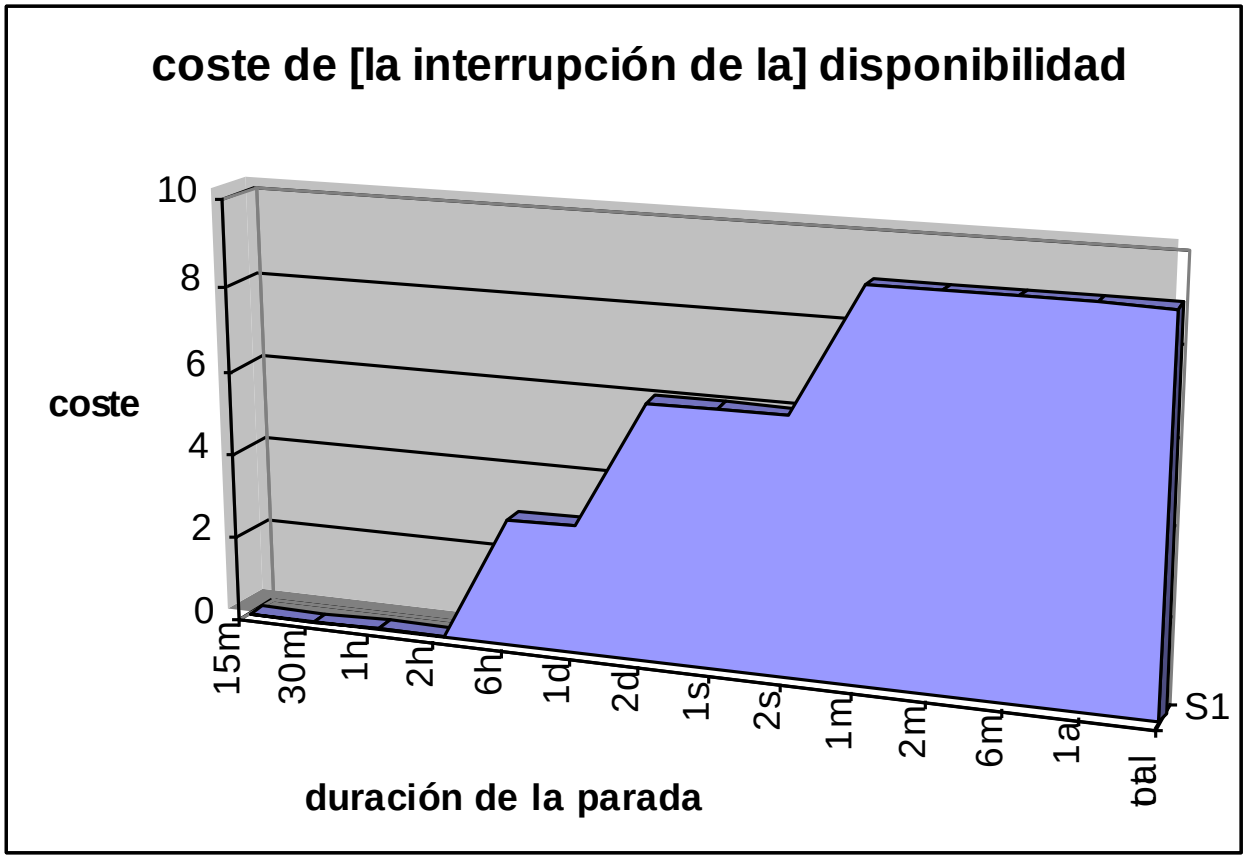
- Seguridad de la información
- Análisis de riesgos
- Tratamiento de los riesgos
- Continuidad de negocio
- Fin

dit

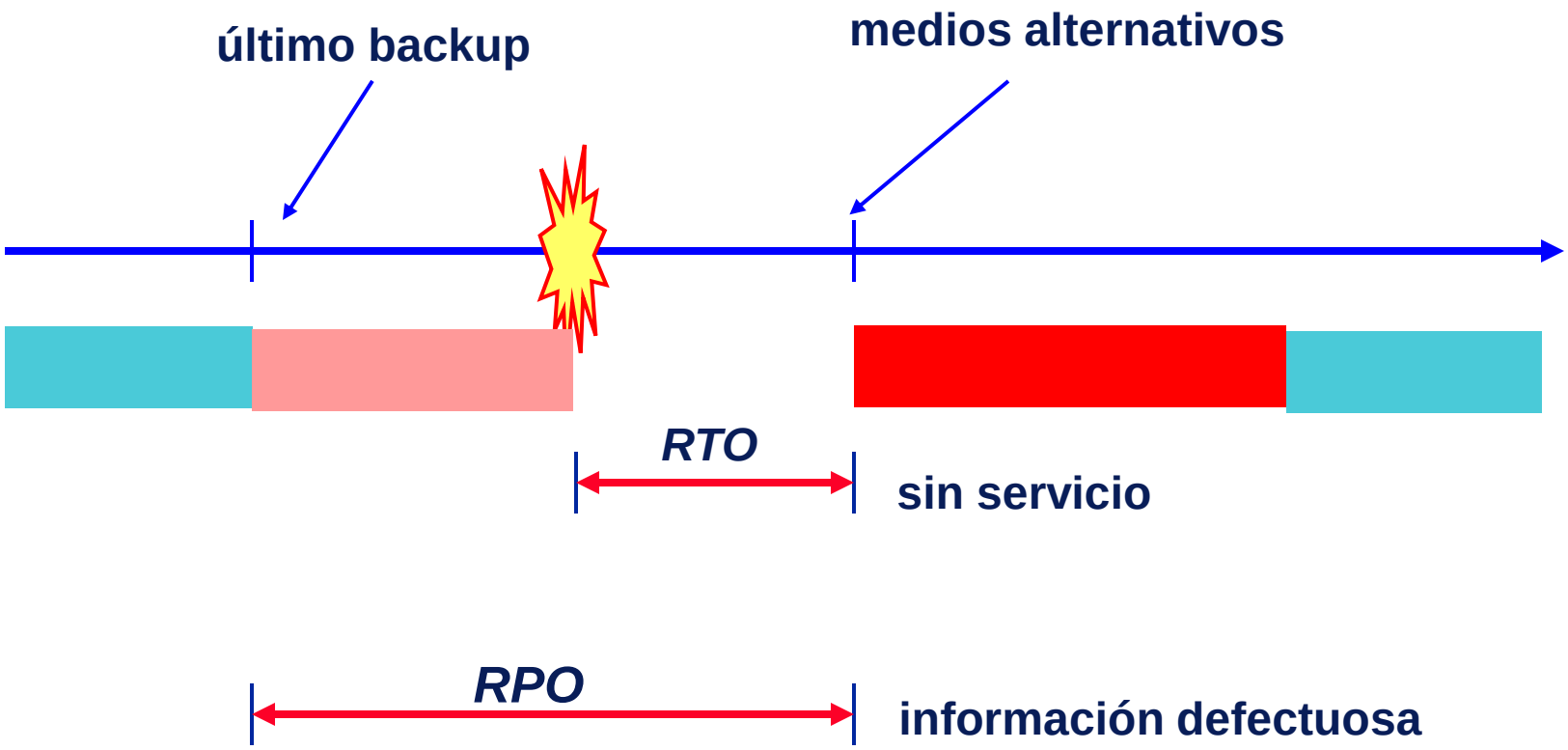
Continuidad de negocio

- Es improbable un desastre; pero somos muy vulnerables
  - dependencia creciente de la tecnología
  - interdependencia de los proveedores
    - su problema es mi problema
  - un acto individual puede tener consecuencias planetarias
  - la competencia [feroz] no perdona detenciones prolongadas o, simplemente, apreciables por los usuarios
  - por obligación legal
    o por regulación sectorial

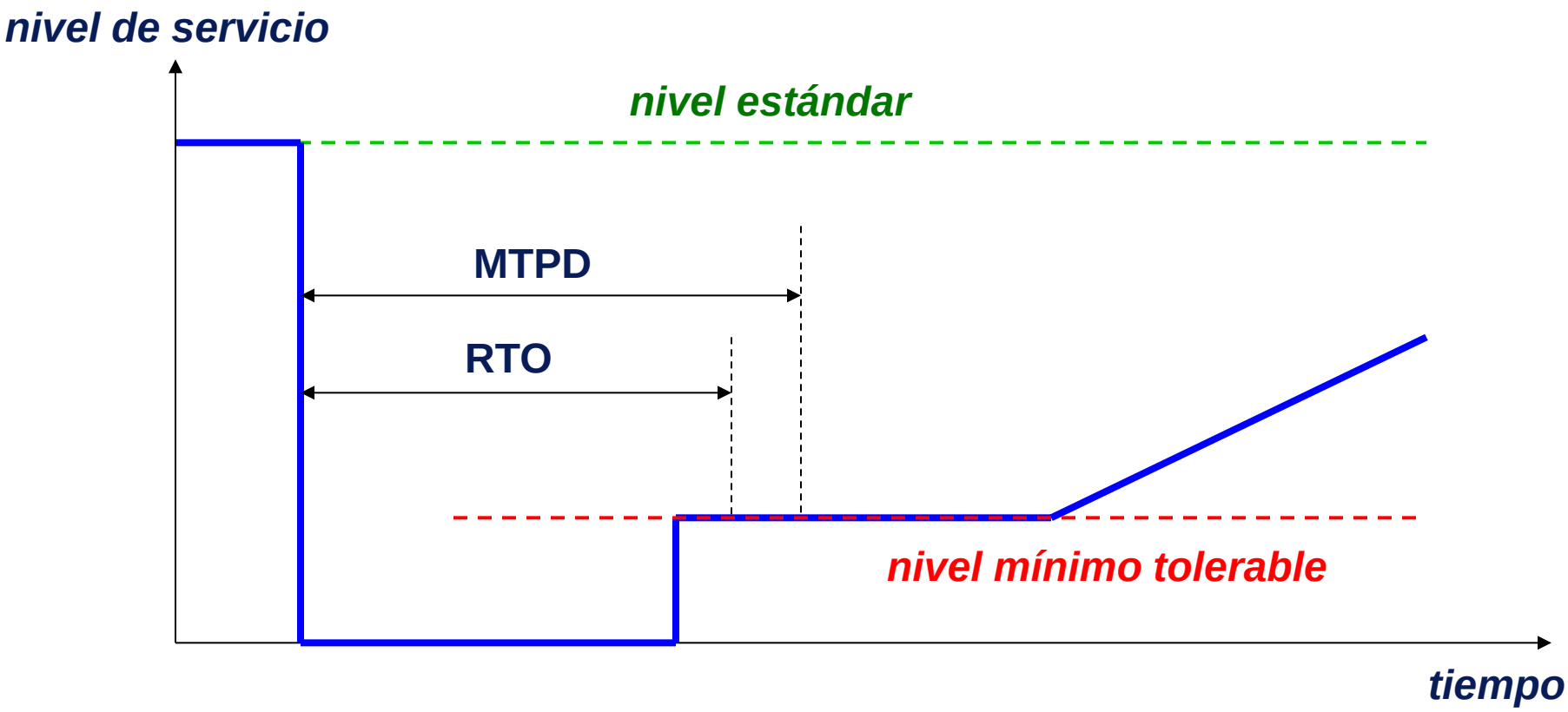
Coste de la interrupción



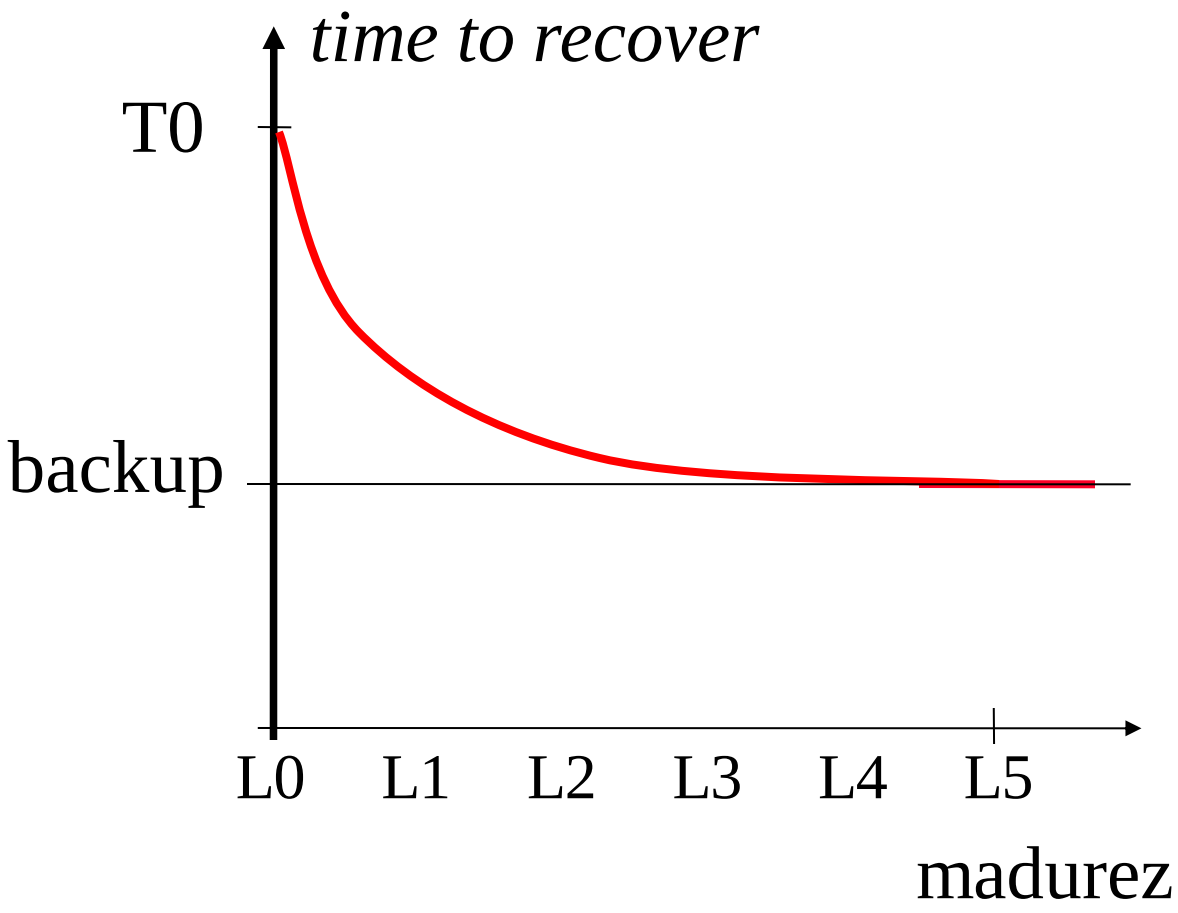
Tiempos


último backup
medios alternativos
RTO
sin servicio
RPO
información defectuosa

MTPD / RTO


nivel de servicio
nivel estándar
MTPD
RTO
nivel mínimo tolerable
tiempo

Impacto residual



Desarrollo de un plan

1. Definir una política (formal)
2. BIA – análisis del impacto en el negocio
3. Identificación de medidas de seguridad
4. Selección de medios alternativos
5. Escribir un plan
6. Auditoría, pruebas, entrenamiento
7. Mantenimiento regular
   - tenemos más
   - sabemos más

dit

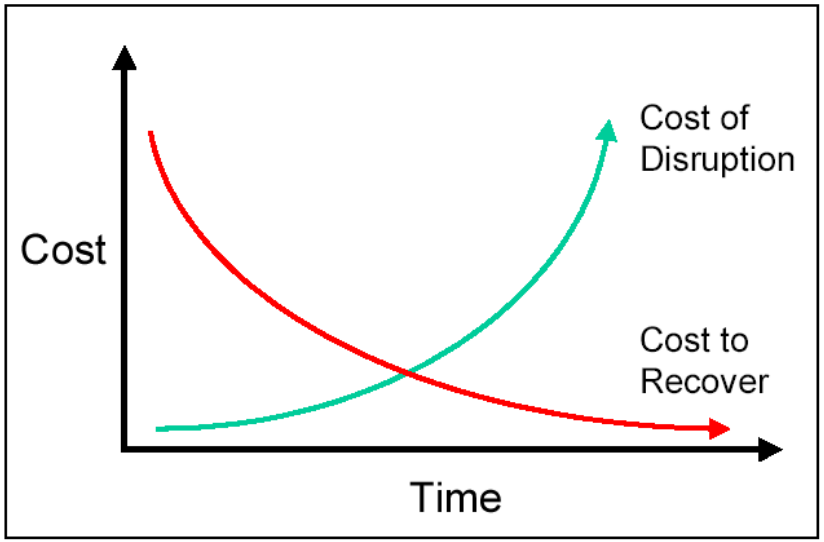
BIA: business impact analysis

1. Determinación de las funciones críticas
   - de producción
   - de responsabilidad legal y contractual
2. Determinación de recursos críticos para funciones críticas
3. Determinación del coste por hora de indisponibilidad

4. Identificación de
   - activos que requieren una alternativa
   - tiempo crítico de puesta en marcha

Estrategias de supervivencia

- ... de los servicios
- ... de la información
- ... de las aplicaciones
- ... de los equipos
- ... de las instalaciones
- ... del personal



criterios
- **impacto a tratar**
- **coste**
- **tiempo de entrada en acción**
- **localización**

Índice

- Seguridad de la información
- Análisis de riesgos
- Tratamiento de los riesgos
- Continuidad de negocio
- Fin

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

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

¿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

dit

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/