TEMA XIV

Concepto de seguridad

Seguridad: Definiciones

- "*Sabemos que es hasta que alguien nos pide que lo definamos*" (Descartes)

- ¿Qué entendemos por seguridad?
  - Real Academia de la Lengua:
    - SEGURIDAD: Cualidad de seguro
    - SEGURO: libre y exento de todo peligro, daño o riesgo
      - Cierto, indubitable y en cierta manera infalible
      - No sospechoso

Definiciones de Seguridad Informática: Consejo Superior de Informática

- Conjunto de técnicas y procedimientos que tienen como misión la protección de los bienes informáticos de una organización
- Bienes informáticos
  - Hardware
  - Datos
  - Programas

La información

ISO/IEC 17799

- La información es un activo que tiene valor para la organización y requiere una protección adecuada.
- La seguridad de la información la protege de un amplio elenco de amenazas para
  - asegurar la continuidad del negocio,
  - minimizar los daños a la organización
  - maximizar el retorno de inversiones
  - Y las oportunidades de negocios.

ISO/IEC 17799 formas información

- La información adopta diversas formas.
  - Puede estar impresa o escrita en papel,
  - Almacenada electrónicamente,
  - Transmitida por correo o por medios electrónicos,
  - Mostrada en filmes o hablada en conversación..
- Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

ISO/IEC 17799 Características

- La seguridad de la información se caracteriza aquí por la preservación de:
  - Su confidencialidad, asegurando que solo quien está autorizado puede acceder a la información
  - Su integridad, asegurando que la información y sus métodos de procesos son exactos y completos
  - Su disponibilidad, asegurando que los usuarios autorizados tiene acceso a la información y a sus activos asociados cuando lo requieran

Autentificación:

- ***Dar y reconocer la autenticidad de ciertas informaciones del Dominio y/o la identidad de los actores y/o la autorización por parte de los autorizadores y la verificación***
  - Que los datos, las personas y programas son auténticos
  - Verificar la identidad

Confidencialidad:

- ***Condición que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados***
- Acceso sólo entes autorizados

Disponibilidad:

- ***Grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado***
- Los bienes informáticos pueden ser utilizado cuándo y cómo lo requieran los usuarios autorizados

Integridad + disponibilidad = confiabilidad

Integridad:

- ***Condición de seguridad que garantiza que la información es modificada, incluyendo su creación y borrado, sólo por personal autorizado***
- Modificación sólo por personal autorizado

Control de acceso

- Protección de los recursos del sistema contra accesos no autorizados
  - El uso de los recursos del sistema están regulados conforme a una política de seguridad
  - Solo es permitido a las entidades autorizadas(usuarios, programas, procesos, otros sistemas..), de acuerdo a la política de seguridad

No repudiación

- No poder negar la intervención en una operación o comunicación

Auditoría de actividades

- Registro cronológico de las actividades del sistema que permitan la reconstrucción y examen de los eventos ocurridos
  - Registro de eventos

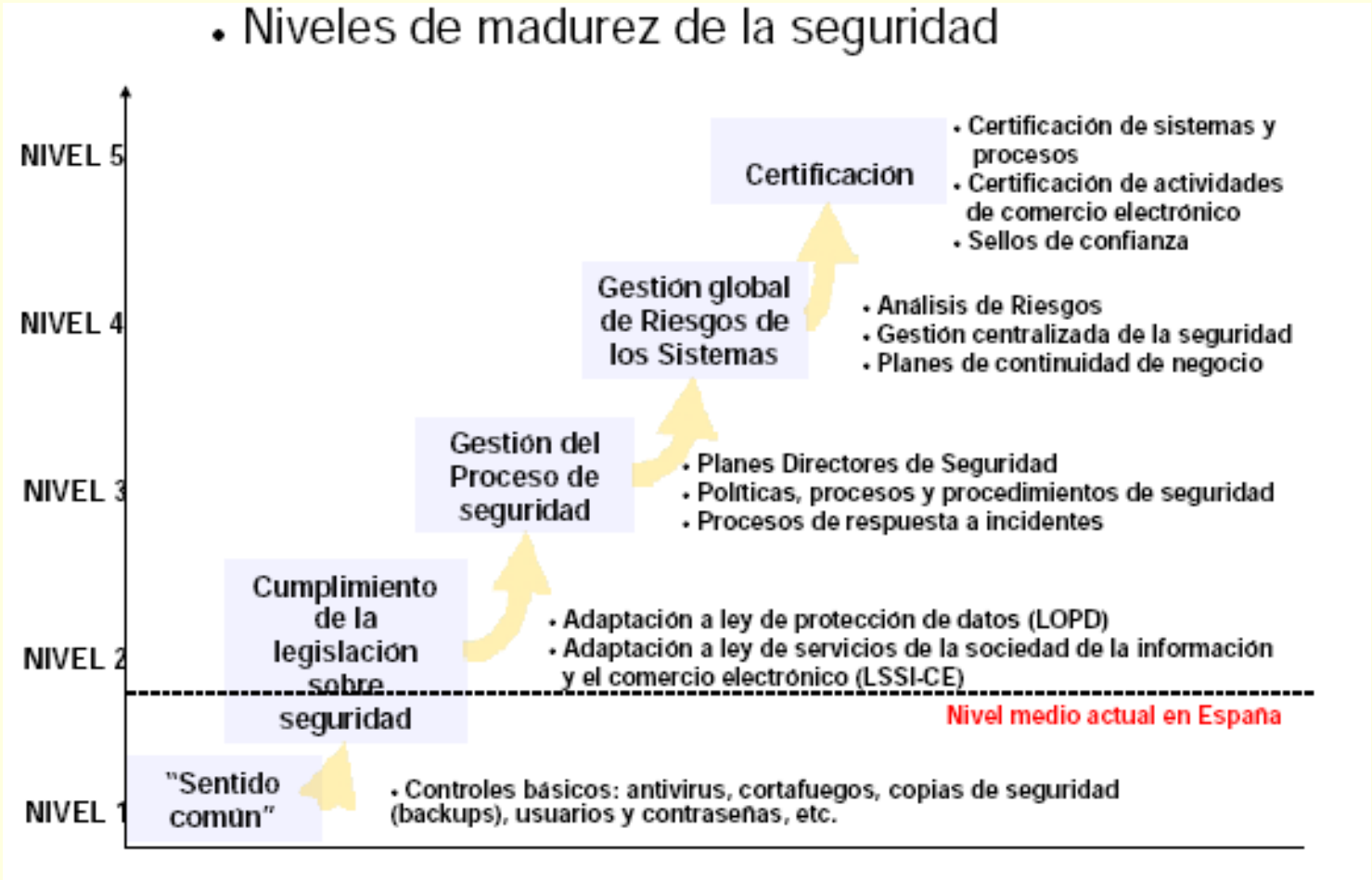
QUÉ ES SEGURIDAD

- ✓ Evitar el ingreso de personal no autorizado
- ✓ Sobrevivir aunque “algo” ocurra
- ✓ Cumplir con las leyes y reglamentaciones gubernamentales y de los entes de control del Estado
- ✓ Adherirse a los acuerdos de licenciamiento de software
- ✓ Prevención, Detección y Respuesta contra acciones no autorizadas

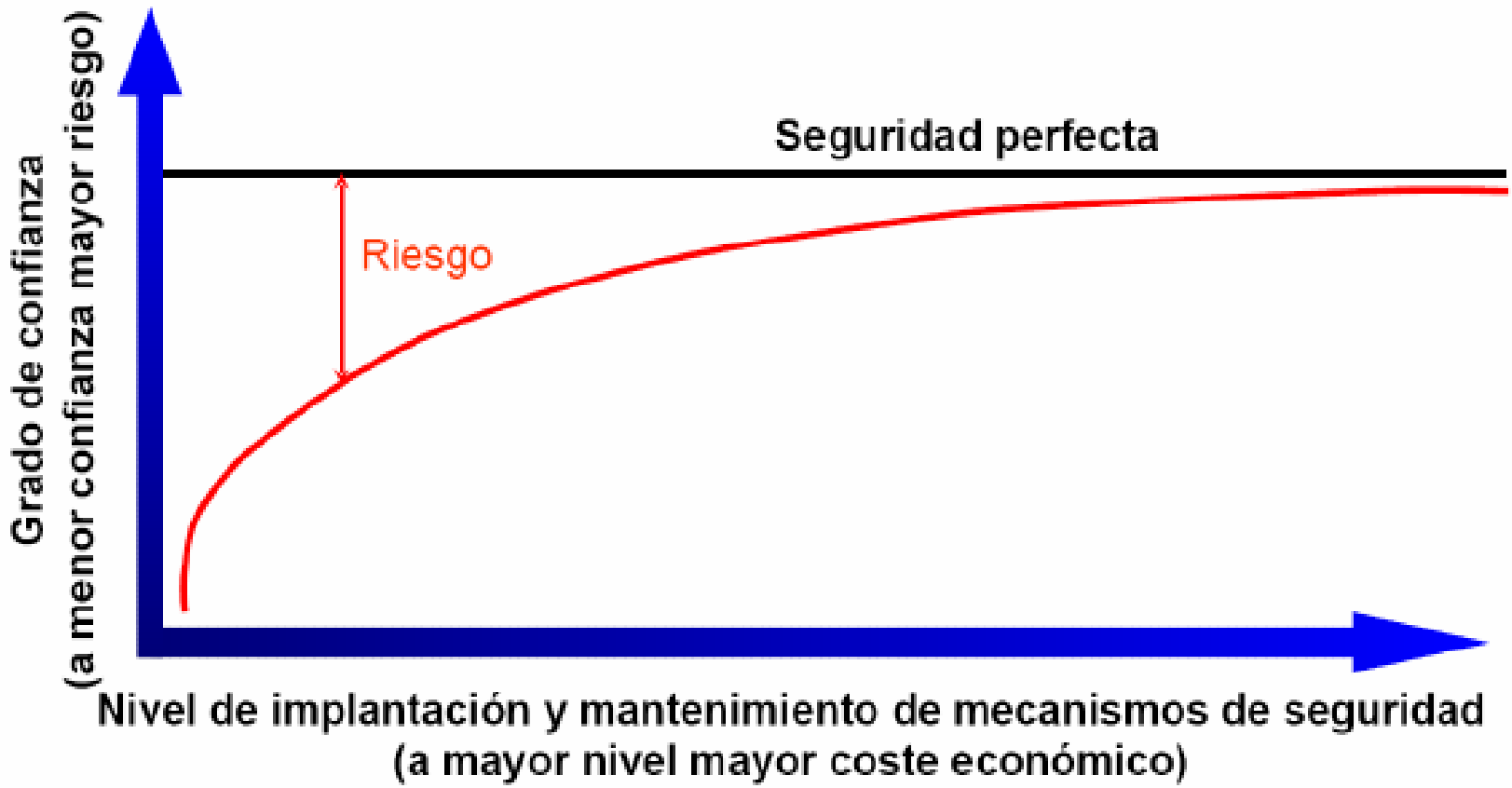
Niveles de seguridad

- Seguro estaba y se murió
- Seguridad total
  - “Queremos que no tenga éxito ningún ataque”
  - Seguridad = Invulnerabilidad
  - Imposible de alcanzar
  - La seguridad total no existe
- Existen grados de seguridad acorde con el bien a defender
  - La política de seguridad siempre es un compromiso entre el nivel de riesgo asumido y el coste requerido

niveles de seguridad



Riesgo y seguridad



Enfoque de gestión del riesgo

- “Queremos que nuestras expectativas se cumplan”
- Seguridad = Confianza
- Posible de gestionar
- El riesgo no puede eliminarse completamente, pero puede reducirse

Análisis de riesgos

- Objetivo:
  - Identificar los riesgos
  - Cuantificar su impacto
  - Evaluar el coste para mitigarlos
  - Servir de guía para tomar decisiones
- Riesgo = Activo x Amenaza x Vulnerabilidad

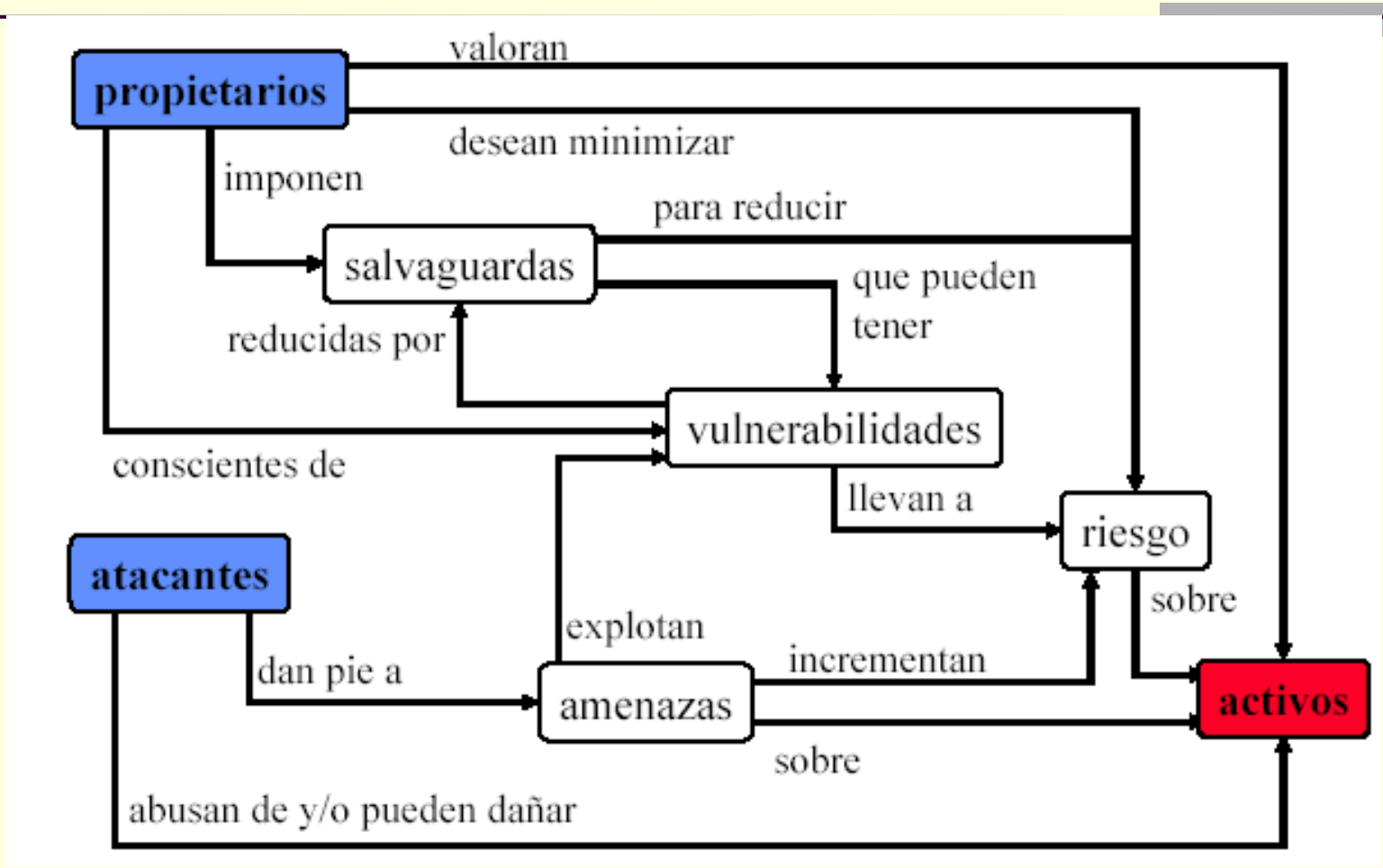
MAGERIT – versión 2

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Definiciones

- ACTIVO:
  - Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.
- AMENAZA:
  - Evento que puede desencadenar un incidente en la organización, produciendo daños o pérdidas materiales o inmateriales en sus activos.
- VULNERABILIDAD:
  - debilidades que pueden permitir que una amenaza se materialice
- RIESGO:
  - Posibilidad de que una amenaza se materialice.
- IMPACTO:
  - Consecuencia sobre un activo de la materialización de una amenaza.
- CONTROL o SALVAGUARDA:
  - Práctica, procedimiento o mecanismo que reduce el nivel de riesgo.

ISO: análisis de riesgos



Gestión de riesgos

Planificar

Definir:
- Alcance
- Política
- Metodología

Identificar y analizar

Identificar:
- Activos
- Amenazas
- Vulnerabilidades

Analizar:
- Riesgos
- Coste/beneficios

Dirección

- Decidir tratamiento de riesgos
- Aceptar riesgo residual

Mitigar Riesgo

Controles:
- Seleccionar
- SOA
- Implantar

Transferir Riesgo

- Seguros
- Proveedores

Aceptar Riesgo

- No hacer nada

Evitar Riesgo

- Cese de la actividad que lo origina

Fuente: www.ISO27000.es

Valoración cuantitativa del riesgo

- B1 = beneficios_1 – gastos_1
  - si no ocurre nada
- B2 = beneficios_2 – gastos_2
  - si se materializa la amenaza
- IMPACTO = B1 – B2
  (beneficios_1 – beneficios_2) + (gastos_2 – gastos_1)

Modelo PDCA

Gestión de la seguridad: modelo

- Modelo PDCA (Plan – Do – Check – Act): Planificar, Hacer, Verificar y Actuar.

Clasificación de las medidas seguridad (I)

- Medidas técnicas
  - Seguridad física (externa)
    - Se consigue adoptando una serie de medidas físicas y administrativas
    - Aspectos:
      - Intrusos físicos (“choris”)
      - Agentes físicos externos al sistema
  - Seguridad lógica (Interna)
    - Se consigue adoptando una serie de medidas técnicas y administrativas
    - ASPECTOS:
      - De Sistemas
      - De red
      - Del software

Clasificación de las medidas seguridad (II)

- Medidas Organizativas
  - Normas que determinan funciones como:
    - Las personas que pueden acceder.
    - Quién tiene derecho a utilizar el sistema
    - Horario etc
  - Clasificación de los usuarios
    - Administradores
    - Usuarios
    - Personas ajenas al sistema
    - Personal de mantenimiento
    - Ejecutivos de grado medio
  - Niveles
    - Todo el mundo tiene acceso a todo
    - Dos niveles: privilegiado y normal
    - Varios niveles de acceso

Medidas organizativas y legales

- Todas las normas de “organización” (NO técnicas) necesarias para llevar a cabo el plan de seguridad
- Medidas legales
  - Legislación de protección de datos
  - Normas de seguridad de obligado cumplimiento
- Metodologías de seguridad
  - Metodologías de análisis de riesgo
  - Metodologías de nacionales e internacionales de seguridad

Normas de seguridad

- Pregunta:
  - ¿Hay alguna norma sobre seguridad de los sistemas de información para las Administraciones Públicas?
- Respuesta:
  - si
    - Magerit
    - Métrica V3

Seguridad MAGERIT: definición

- EL Consejo Superior de Informática ha elaborado:
- Metodología de Análisis y GEstión de los Riesgos de los sistemas de Información de las AdminisTraciones Públicas
- MAGERIT

Seguridad MAGERIT: Objetivos

- Objetivos
  - Estudiar los riesgos que soporta un sistema de información y el entorno asociable con él
  - Recomendar las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados

Guía de Aproximación a la Seguridad de los sistemas de información

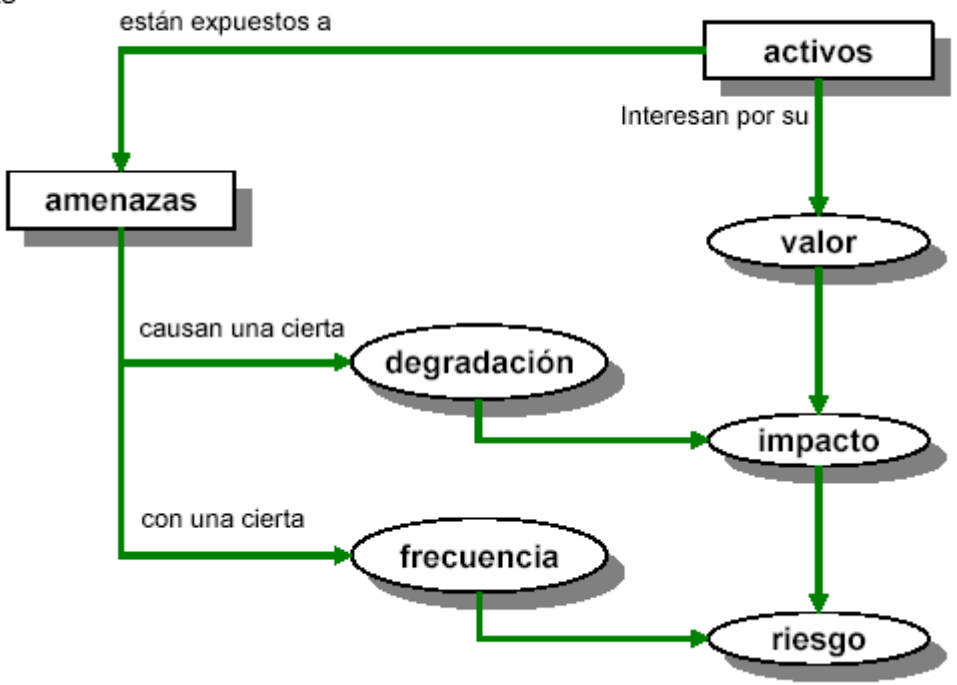
- ¿Donde conseguirla?:URL:http://www.map.es/csi
- Elementos de MAGERIT
  - **Un conjunto de Guías**, compuesto básicamente por:
    - Guía de Aproximación
    - Guía de Procedimientos
    - Guía de Técnicas
    - Guía para Desarrolladores de Aplicaciones
    - Guía para Responsables del Dominio protegible
    - Referencia de Normas legales y técnicas
  - **Un panel de herramientas de apoyo**, con sus correspondientes Guías de Uso y con la Arquitectura de Información y Especificaciones de la Interfaz para el Intercambio de datos.

Salvaguardas preventivas mínimas de seguridad

- 1. Documentación de políticas de seguridad de la información
- 2. Asignación de funciones y responsabilidades de seguridad
- 3. Responsabilidades del usuario en el acceso al sistema
- 4. Educación y formación en la seguridad de la información
- 5. Comportamiento ante incidentes de seguridad
- 6. Controles físicos de seguridad
- 7. Gestión de la seguridad del Equipamiento
- 8. Cumplimiento de las obligaciones y restricciones jurídicas vigentes
- 9. Protección, transporte y destrucción de la Información
- 10. Gestión Externa de servicios

Magerit 2: análisis de riesgo

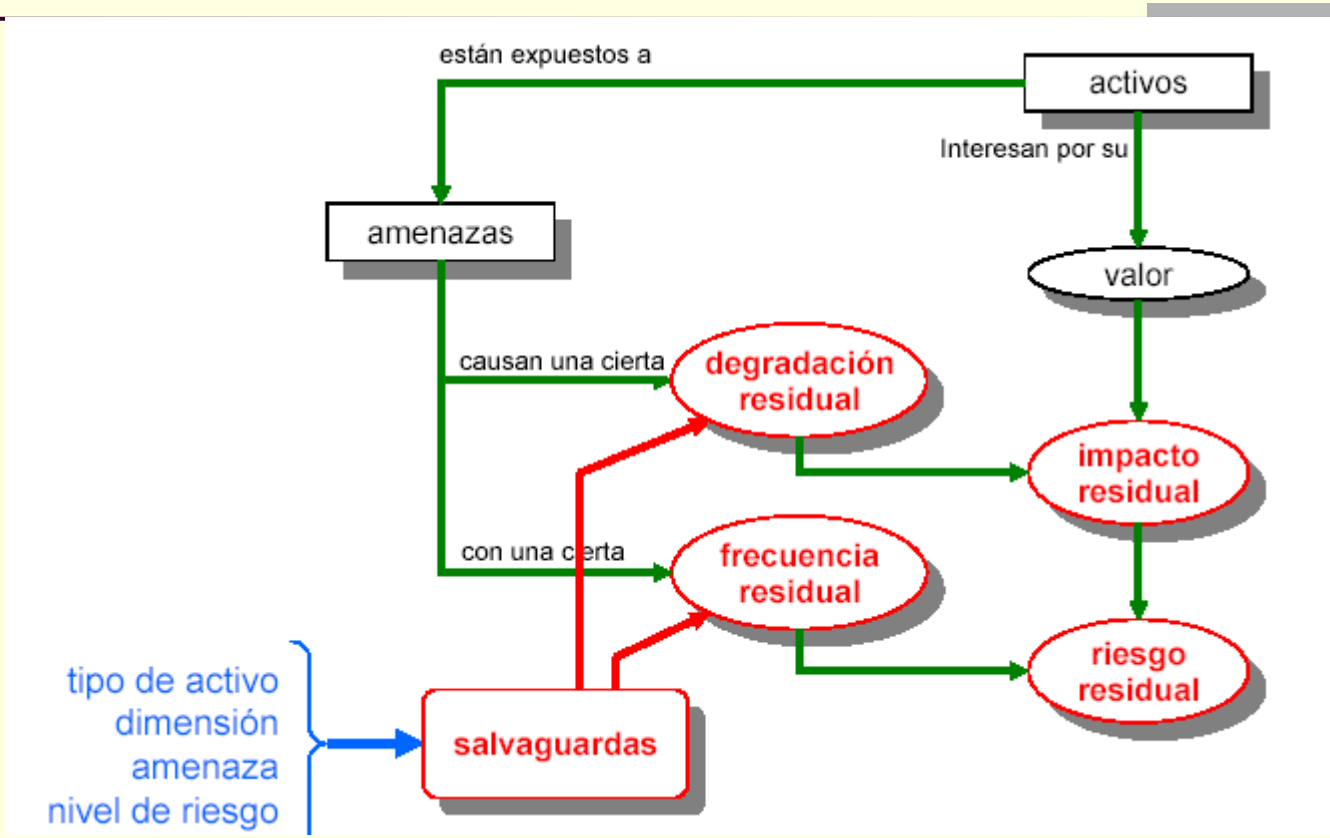
MINISTERIO DE ADMINISTRACIONES PÚBLICAS



MAGERIT – versión 2

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Magerit: tratamiento

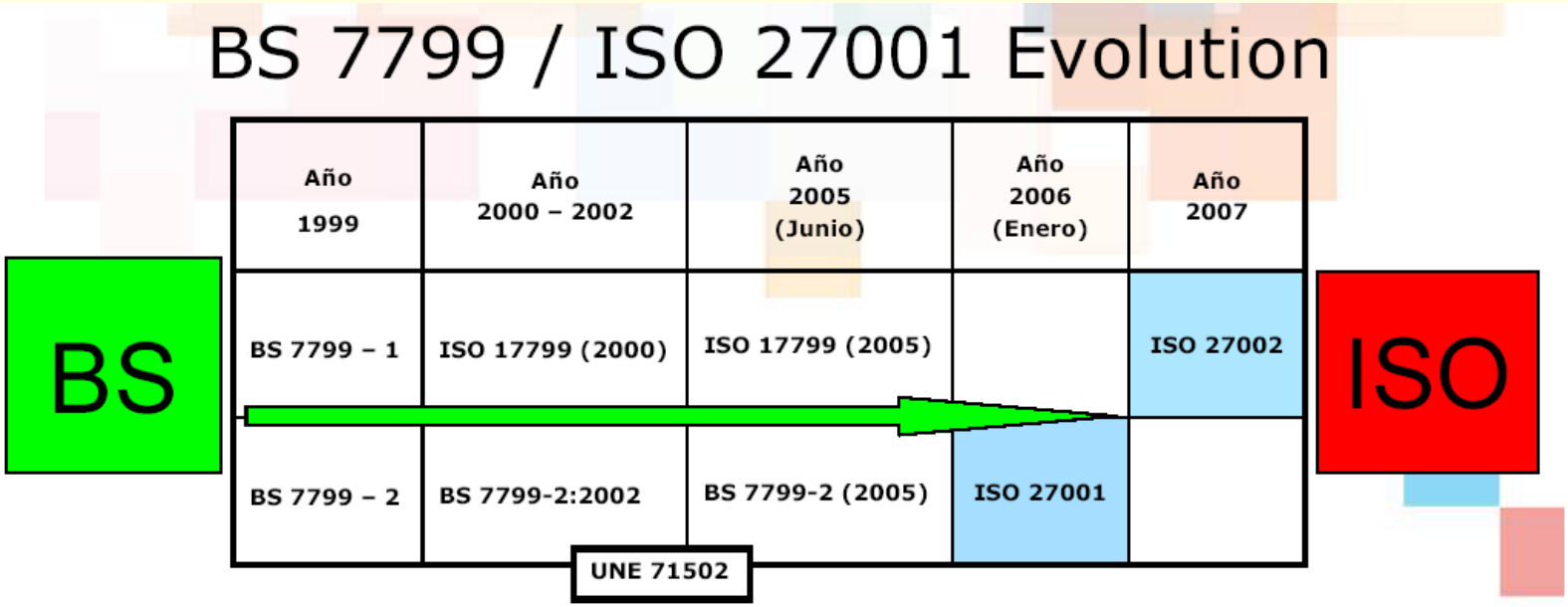


Métrica versión 3 (octubre 1999)

- Metodología de planificación y desarrollo de sistemas de Información
- Autor: Consejo Superior de Informática
- Fase1
- Interfaz de seguridad
- El objetivo de la interfaz de seguridad MAGERIT – Métrica V.3 es
  - Ayudar en la consideración de los requisitos de seguridad de los sistemas de información durante todas los procesos que cubre la metodología Métrica V.3:
    - Planificación de Sistemas de Información, Estudio de Viabilidad, Análisis, Diseño, Construcción, Implantación y Aceptación del sistema de información.

Estándares ISO

- ISO 17799/UNE 71501
- ISO 27000
  - http://www.iso27000.es/index.html



Normas ISO 27000

- NACE LA FAMILIA DE LAS NORMAS ISO 27000
- ISO/IEC 27001 (BS7799-Part 2) - 'Information Security Management System'. Due for release in November 2005. (Once ISO/IEC 27001 is released, BS7799-2:2002 will be withdrawn)
- ISO/IEC 27002 (ISO/IEC 17799 & BS7799- Part 1) - The planned 'Code of Practice' replacement for ISO/IEC 17799:2005 scheduled for April 2007
- ISO/IEC 27003 (BS7799-3) 'Risk Assessment'. No announcement has yet been made regarding ISO/IEC 27003 however, the BSI expect to release BS7799-3 in November 2005
- ISO/IEC 27004 (BS7799-4) 'Information Security Metrics and Measurement'. No launch date is available, although the BSI will publish a description in July/August 2005