

# Formación UPC - 2010

Normativas de seguridad: LOPD, LSSI,  
ISO 27001 y Esquema Nacional de  
Seguridad

# Index

- LOPD
- LSSI
- ISO 27001
- ENS
- Herramientas: magerit y pilar

# ENS con Magerit y Pilar

- MAGERIT – **M**etodología de **A**nálisis y **G**estión de **R**iesgos de los sistemas de Información de las adminis**T**raciones publicas
- ¿Qué es?
  - Es un método formal para investigar los riesgos a que están expuestos los Sistemas de Información, y para poder recomendar las medidas apropiadas que deberían adoptarse para controlar estos riesgos
- Objetivos
  - **Concienciar** a los responsables de los sistemas de información de la existencia de riesgos y de la necesidad de atajarlos a tiempo
  - Ofrecer un método sistemático para **analizar** tales **riesgos**
  - Ayudar a descubrir y planificar las **medidas oportunas** para mantener los riesgos bajo control
  - Preparar a la Organización para **procesos de evaluación, auditoría, certificación o acreditación**, según corresponda en cada caso

# ENS - Magerit

- Versiones

- Primera versión año 1997 – Centro Criptológico Nacional
- Segunda versión año 2004 – Centro Criptológico Nacional

Pertenecientes al ministerio de la presidencia

- Desarrollo

- Versión 1.0 estructurada en siete guías metodológicas:
  - Guía de Aproximación
  - Guía de Procedimientos
  - Guía de Técnicas
  - Guía para Responsables del Dominio protegible
  - Guía para Desarrolladores de Aplicaciones
  - Arquitectura de la información y especificaciones de la interfaz para el intercambio de datos
  - Referencia de Normas legales y técnicas
- Versión 2.0 estructurada en tres libros:
  - Método
  - Catálogo de elementos
  - Guía de técnicas

# MAGERIT – 1.0

- **Guía de Aproximación.** Presenta los conceptos básicos de seguridad de los sistemas de información, con la finalidad de facilitar su comprensión por **personal no especialista** y ofrece una introducción al núcleo básico de MAGERIT, constituido por las Guías de Procedimientos y de Técnicas.
- **Guía de Procedimientos.** Representa el núcleo del método, que se completa con la Guía de Técnicas. Ambas constituyen un conjunto autosuficiente, puesto que basta su contenido para **comprender la terminología** y para realizar el Análisis y Gestión de Riesgos de cualquier sistema de información.
- **Guía de Técnicas.** Proporciona las claves para comprender y seleccionar las técnicas más adecuadas para los procedimientos de análisis y gestión de riesgos de seguridad de los sistemas de información.
- **Guía para Responsables del Dominio protegible.** Explica la participación de los **directivos** "responsables de un dominio" en la realización del análisis y gestión de riesgos de aquellos sistemas de información relacionados con los activos cuya gestión y seguridad les están encomendados.
- **Guía para Desarrolladores de Aplicaciones.** Está diseñada para ser utilizada por los desarrolladores de aplicaciones, y está íntimamente ligada con la Metodología de Planificación y Desarrollo de Sistemas de Información, Métrica v2.1.
- **Arquitectura de la información y especificaciones de la interfaz para el intercambio de datos.** La interfaz para intercambio de datos posibilita que un usuario de MAGERIT establezca la comunicación con otras aplicaciones y sistemas facilitando la incorporación de sus productos a la herramienta MAGERIT y viceversa.
- **Referencia de Normas legales y técnicas.** Lista de normas en materia de seguridad a fecha 31 de Diciembre de 1996.

# MAGERIT – 2.0

- Metodología de Análisis y gestión Riesgos S.I.
  - 16.06.2005 ..... 158 páginas
- Catálogo de elementos
  - 83 páginas
  - Tipos de activos
  - Dimensiones valoración
  - Criterios de valoración
  - Amenazas
  - Salvaguardas
- Libro de técnicas
  - 73 páginas

# MAGERIT - Aplicación

- Aporta racionalidad en el conocimiento del estado de seguridad de los Sistemas de Información y en la introducción de medidas de seguridad
- Ayuda a garantizar una adecuada cobertura en extensión, de forma que no haya elementos del sistema de información que queden fuera del análisis, y en intensidad, de forma que se alcance la profundidad necesaria en el análisis del sistema.
- Incrustación de mecanismos de seguridad en sistemas de información para:
  - Paliar las insuficiencias de los sistemas vigentes
  - Asegurar el desarrollo de cualquier tipo de sistemas, reformados o nuevos, en todas las fases de su ciclo de desarrollo, desde la planificación hasta la implantación y mantenimiento

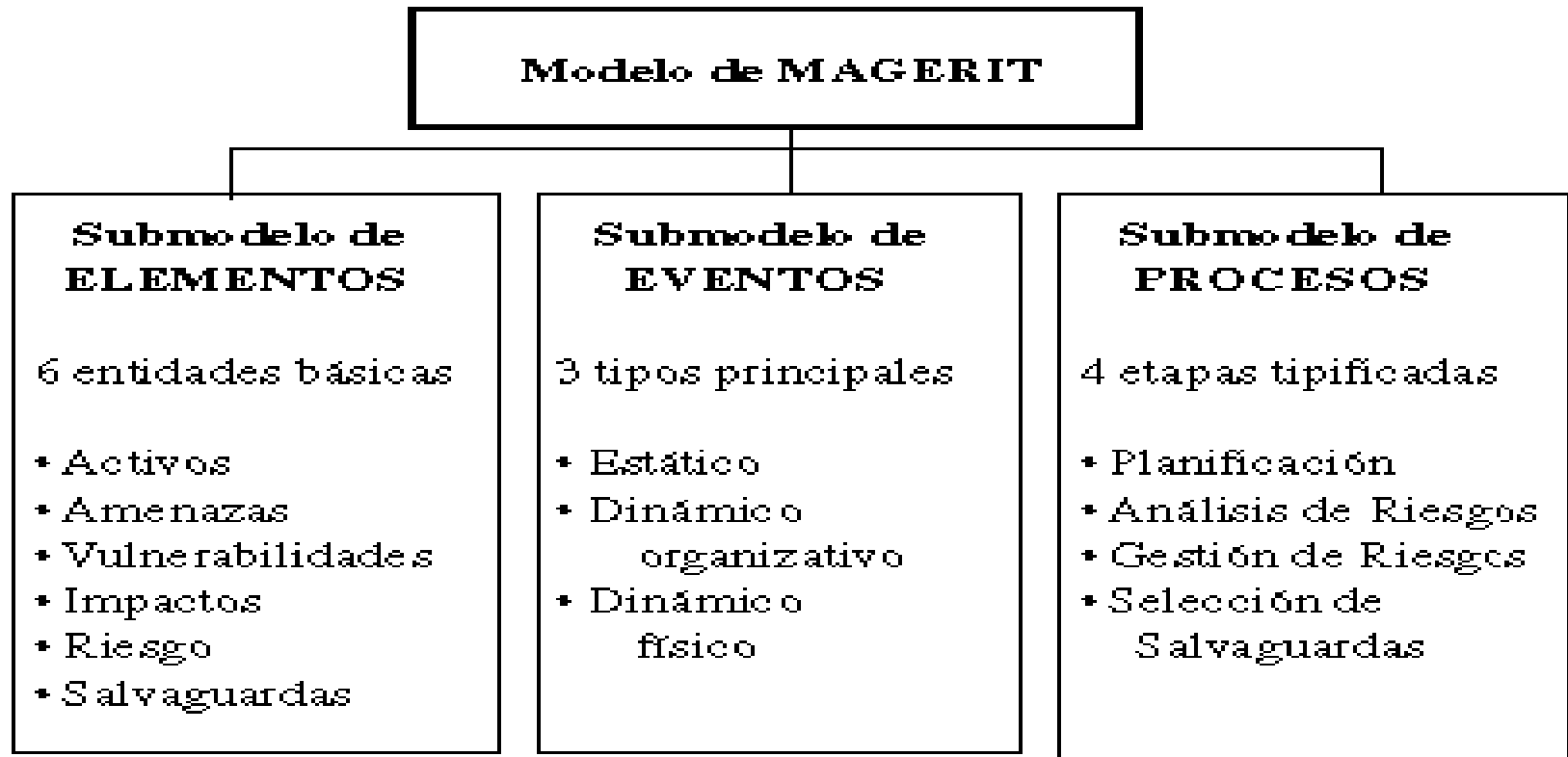
# MAGERIT – Tipos de proyectos

- MAGERIT responde a las necesidades de un espectro amplio de intereses de usuarios con un enfoque de adaptación a cada organización y a sensibilidades diferentes en Seguridad de los Sistemas de Información. Las diferencias residen en tres cuestiones fundamentales:
  - **Situación** dentro del "ciclo de estudio": marco estratégico, planes globales, análisis de grupos de múltiples activos, gestión de riesgos de activos concretos , determinación de mecanismos específicos de salvaguarda
  - **Envergadura**: complejidad e incertidumbre relativas del Dominio estudiado , tipo de estudio más adecuado a la situación (corto, simplificado, ...), granularidad adoptada
  - **Problemas específicos** que se desee solventar: Seguridad lógica, Seguridad de Redes y Comunicaciones, Planes de Emergencia y Contingencia, Estudios técnicos para homologación de sistemas o productos , Auditorías de seguridad



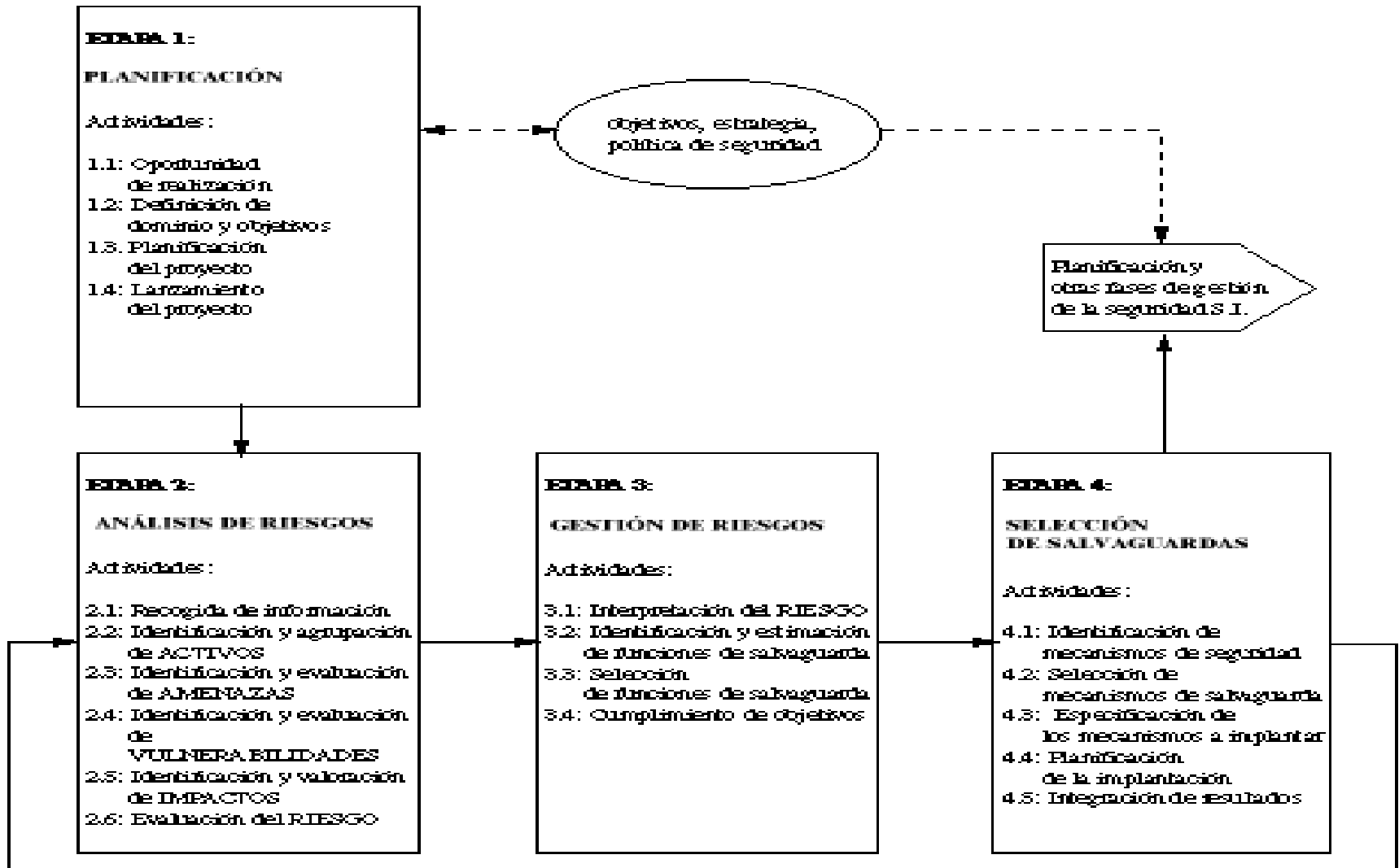
# MAGERIT - Estructura

- El modelo normativo de MAGERIT se apoya en tres submodelos: El Submodelo de Elementos proporciona los "componentes" que el Submodelo de Eventos va a relacionar entre sí y con el tiempo, mientras que el Submodelo de Procesos será la descripción funcional ("el esquema explicativo") del proyecto de seguridad a construir.



# MAGERIT - Procesos

- El Submodelo de Procesos de MAGERIT comprende 4 Etapas:



# MAGERIT - Procesos

- **Planificación del Proyecto de Riesgos.** Como consideraciones iniciales para arrancar el proyecto de Análisis y Gestión de Riesgos (AGR), se estudia la oportunidad de realizarlo, se definen los objetivos que ha de cumplir y el ámbito que abarcará, planificando los medios materiales y humanos para su realización e inicializando el propio lanzamiento del proyecto
- **Análisis de riesgos.** Se identifican y valoran las diversas entidades, obteniendo una evaluación del riesgo, así como una estimación del umbral de riesgo deseable.
- **Gestión de riesgos.** Se identifican las funciones y servicios de salvaguarda reductoras del riesgo, seleccionando los que son aceptables en función de las salvaguardas existentes y las restricciones, tras simular diversas combinaciones.
- **Selección de salvaguardas.** Se prepara el plan de implantación de los mecanismos de salvaguarda elegidos y los procedimientos de seguimiento para la implantación. Se recopilan los documentos del Análisis y Gestión de Riesgos (AGR), para obtener los documentos finales del proyecto y realizar las presentaciones de resultados a diversos niveles.

- Construcción de proyectos específicos de seguridad a partir de **interfaces de enlace de la MÉTRICA VERSIÓN 2.1. MAGERIT.**

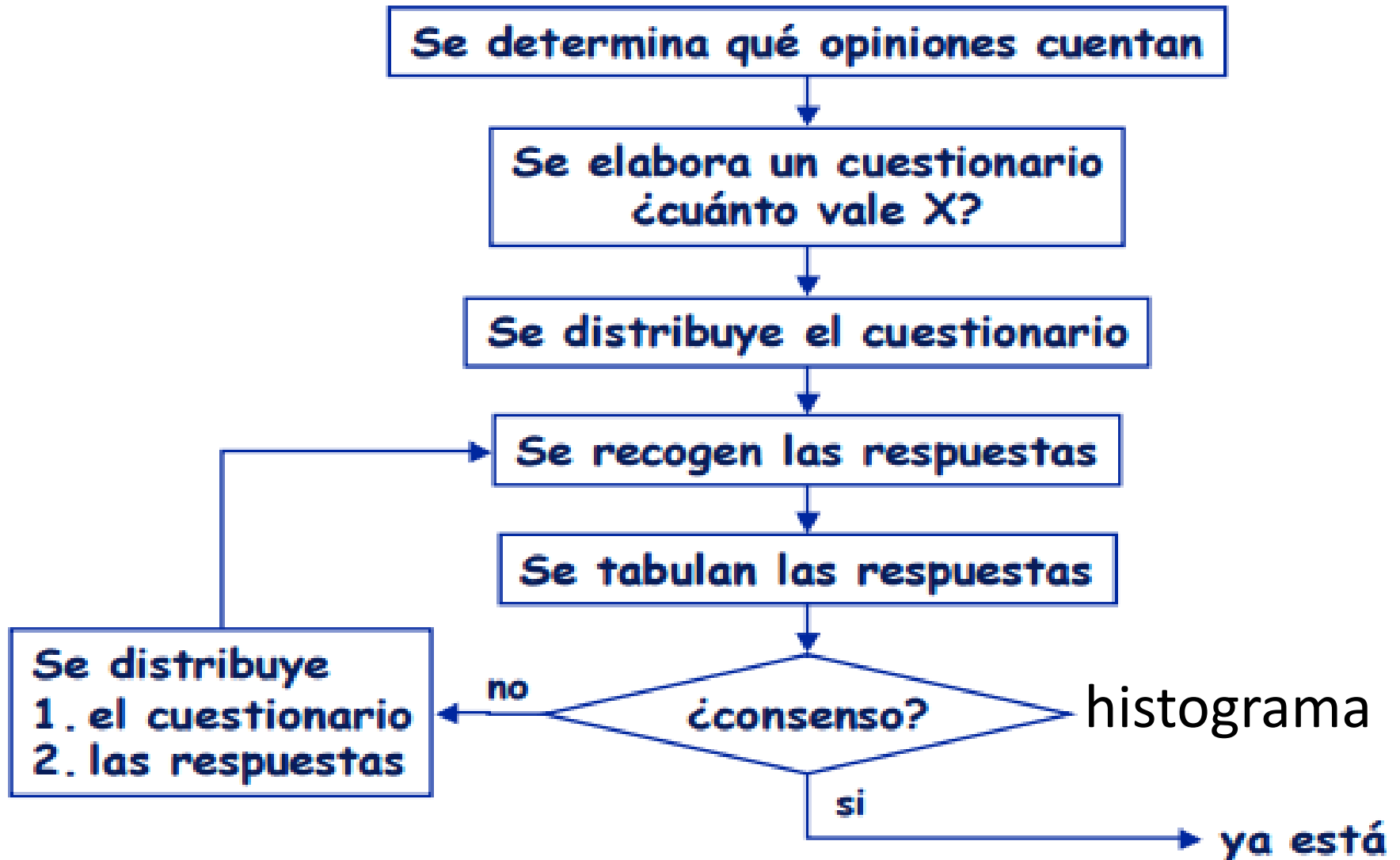
- Permite añadir durante el desarrollo del sistema, la consideración de los requerimientos de seguridad, sin interferir en los procedimientos de Métrica, pero utilizándolos para identificar y documentar los procedimientos y productos de aseguramiento.
- Tienen ventajas inmediatas: analizar la seguridad del Sistema antes de su desarrollo, incorporar defensas antes de completarlo (lo que es más barato y efectivo) y controlar su consistencia a lo largo de todo el ciclo de vida del Sistema.

# MAGERIT - Etapas

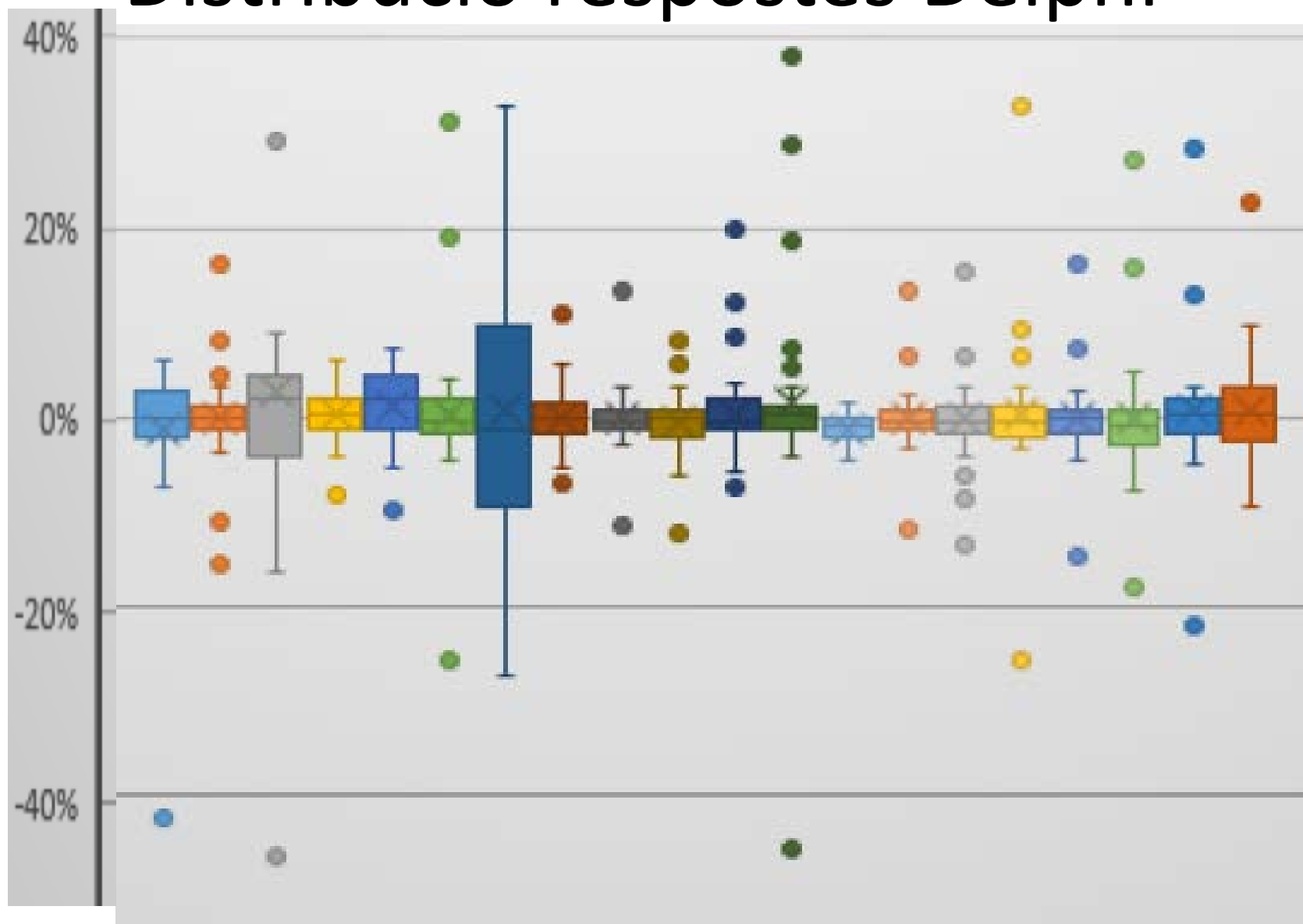
- **Modelo de Valor.** Caracterización del valor que representan los **activos** para la organización así como de las **dependencias** entre los diferentes activos.
- **Mapa de Riesgos.** Relación de las **amenazas** a que están expuestos los activos.
- **Evaluación de Salvaguardas.** Evaluación de la **eficacia** de las salvaguardas existentes en relación al riesgo que afrontan.
- **Estado de Riesgo.** Caracterización de los activos por su **riesgo residual**; es decir, por lo que puede pasar tomando en consideración las salvaguardas desplegadas
- **Informe de Insuficiencias.** Ausencia o **debilidad de las salvaguardas** que aparecen como oportunas para reducir los riesgos sobre el sistema.
- **Plan de Seguridad.** Conjunto de programas de seguridad que permiten materializar las decisiones de **gestión de riesgos**.

# Método Delphi

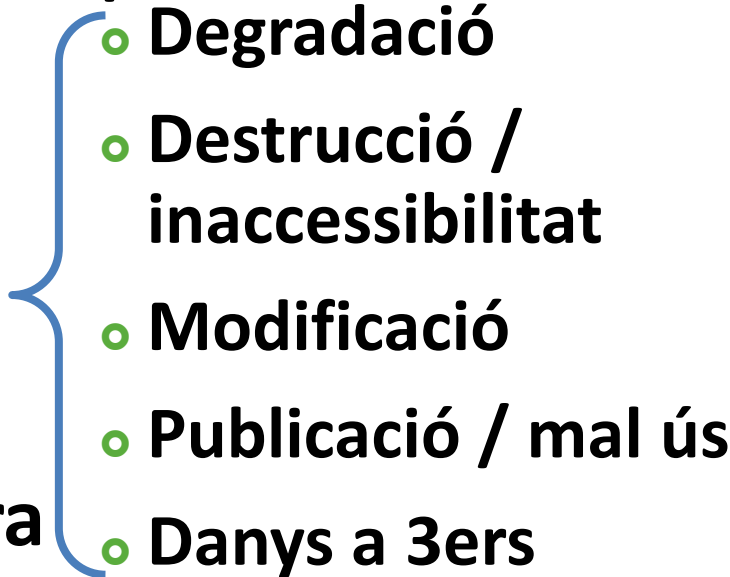
Es una técnica netamente cualitativa



# Distribució respostes Delphi



# Tipus d'impacte

- **DICTA**
  - **Serveis**
  - **Dades / Informació**
  - **Operació**
  - **Equips / Infraestructura**
  - **Reputació**
  - **Personal: Equips, temps, productivitat**
  - **Legals**
  - **Ciutadans**
  - **(Dispon. Integr. Confid. Trustworth. Account.)**
- 
- ◉ **Degradació**
  - ◉ **Destrucció / inaccessibilitat**
  - ◉ **Modificació**
  - ◉ **Publicació / mal ús**
  - ◉ **Danys a 3ers**

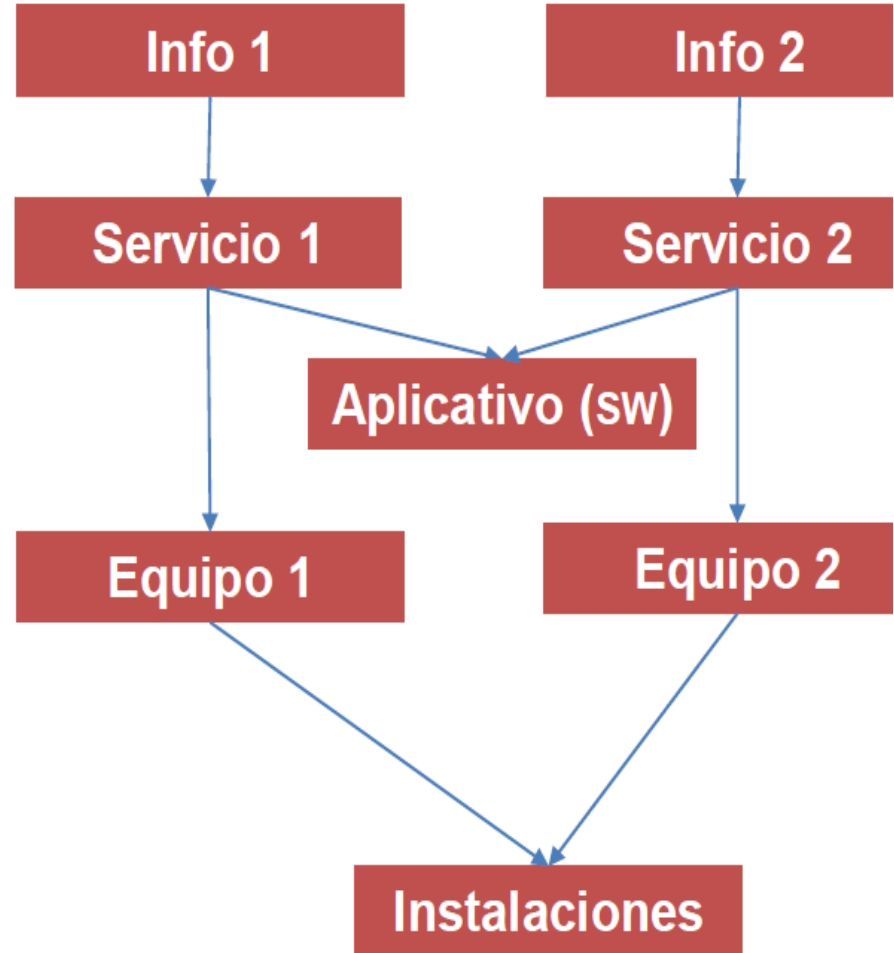
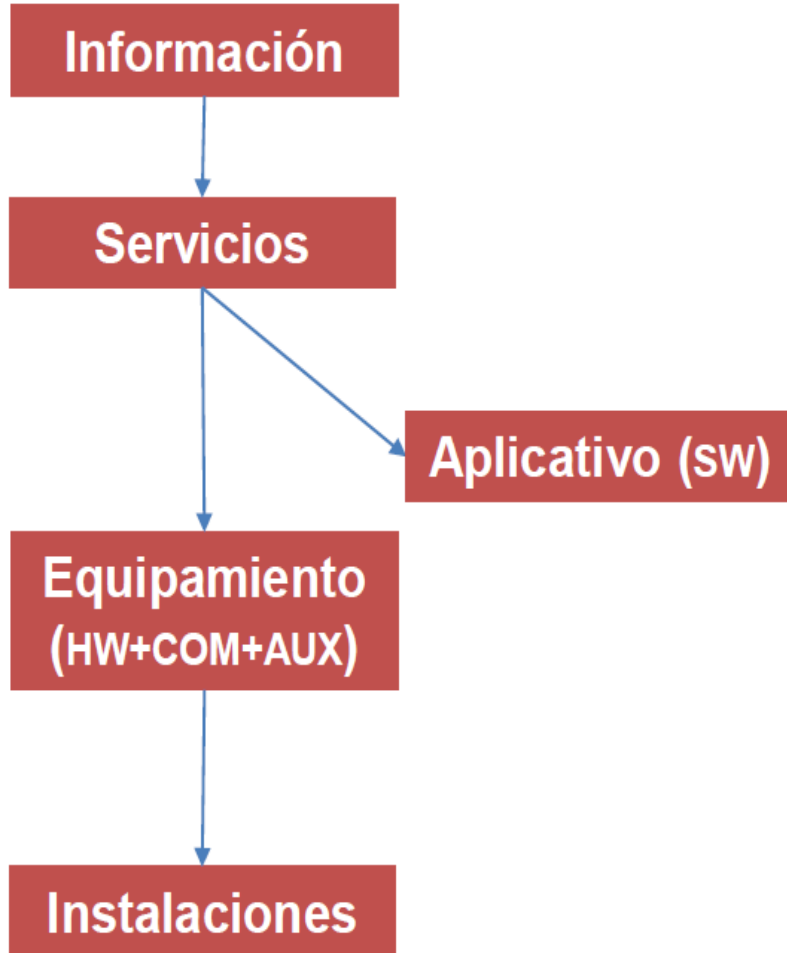
# estimar impacte i probabilitat

- Dependències
- Acumular valor actiu més dependents
- Acumular amenaces
- Acumular degradacions en totes les dimensions
- Escenari: Intrínsec o Residual
- Metodologia: Qualitativa o Quantitativa o Econòmica
- Categoritzar:
  - Amenaça: Accés, Origen, motivació, resultat
  - Impacte: Reputació, Econòmic, Eficiència, Multa, Seguretat, Altres
  - Avaluar valor i confiança



# Dependències funcionals

- Determinar grau (%)



# Metodologies d'Anàlisi i Gestió de Risc

- MAGERIT (MAP): Econòmic, ROSI
- CRAMM (UK, Siemens): qualitatiu numèric
- ISO 27005
- OCTAVE (CERT/CC): qualitatiu pur, simplificat
- NIST SP 800-30

# Valoración de amenazas. Probabilidad

- Se puede calcular de forma cualitativa:

Tipos de Escalas			
MA	Muy alta	Casi seguro	Fácil
A	Alta	Muy alto	Medio
M	Media	Posible	Difícil
B	Baja	Poco probable	Muy difícil
MB	Muy baja	Muy raro	Extremadamente difícil

- Se puede calcular numéricamente

Tipos de Escalas			
MA	100	Muy frecuente	A diario
A	10	Frecuente	Mensualmente
M	1	Normal	Una vez al año
B	1/10	Poco frecuente	Cada varios años
MB	1/100	Muy poco frecuente	siglos

OCTAVE

CRAMM

# Anàlisi de les dades (impacte a l'organització)

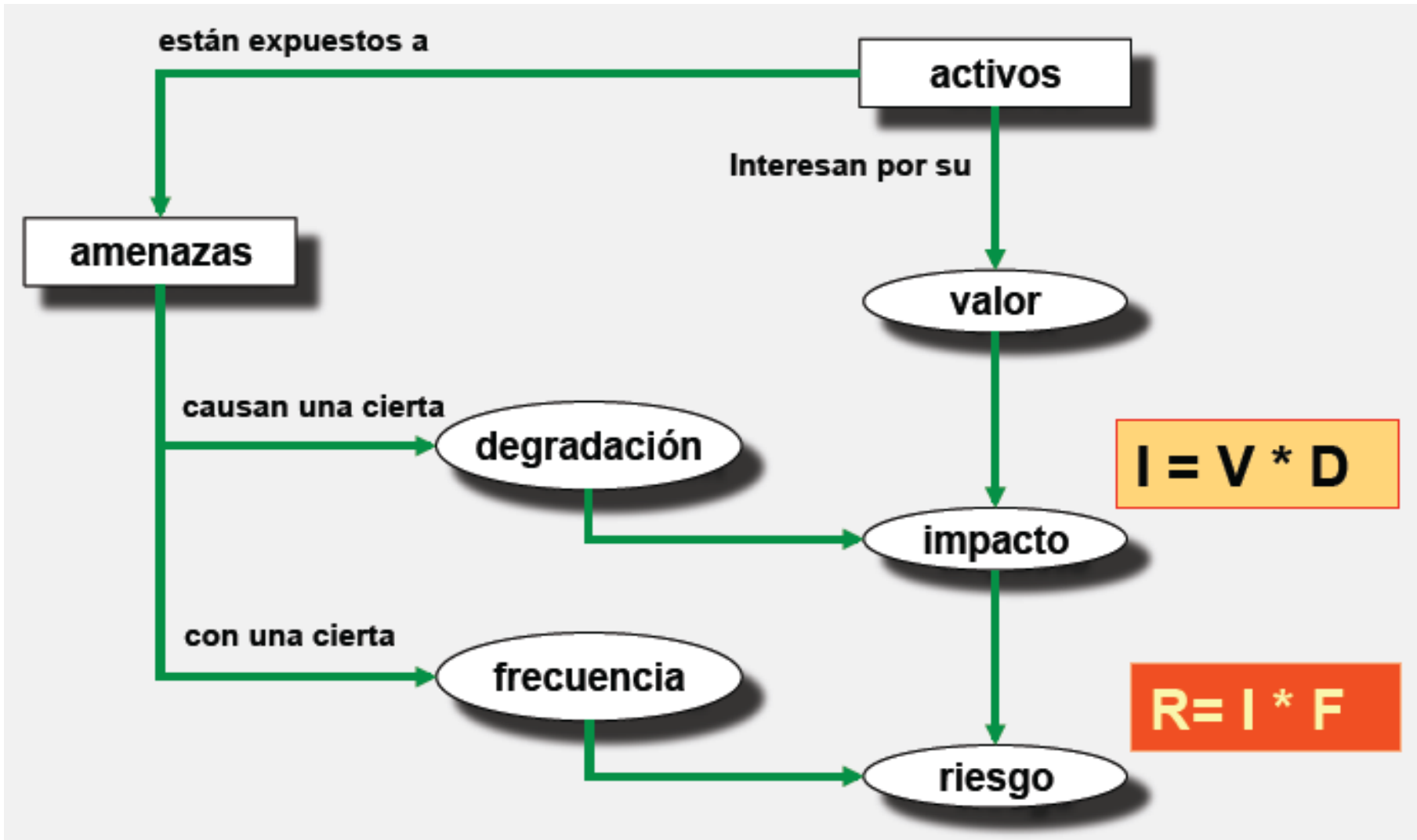
Preguntes que hauríem de respondre:

- Correlació entre el nombre d'incidents i creixement econòmic
  - Impacte de la resposta a incidents en l'economia?
- Cost d'un incident?
  - En termes econòmics: 0.4% PIB, volum de negoci
  - En persona.hora
  - Social / Reputacional / Bursàtil
- Correlació entre creixement dels usuaris d'internet i nombre d'incidents
  - Comparar amb habilitats de la població
- Quantes persones afecta un incident?
- Vida mitja d'un lloc de phishing (compromís)?

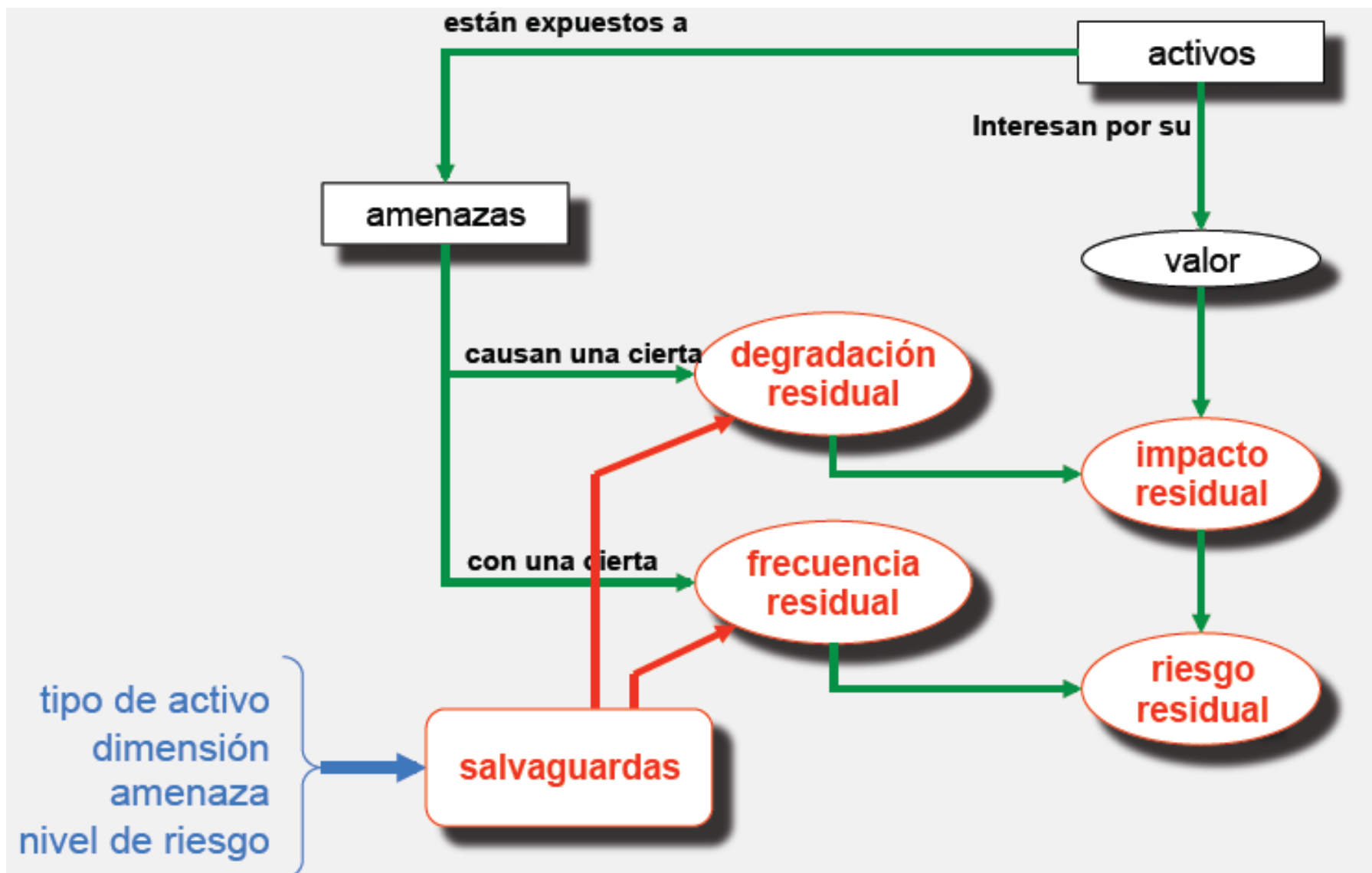
# Definició de l'estratègia de gestió del risc

- Dimensions:
  - Confidencialitat, Integritat, Disponibilitat
- Complementaris:
  - Autenticitat (exactitud),
  - Auditabilitat/Traçabilitat us (Acreditació)/accès (Registres)
- Estratègia de protecció:
  - Preventiva: Probabilitat (eliminació)
  - Reactiva: Impacte (minimització, restauració, recuperació)
  - Ambivalents / Consolidació: Conscienciació, administració, monitorització, detecció

# MAGERIT – Gestión de Riesgo



# MAGERIT – Gestión de Riesgo



# Avaluant Controls de Seguretat

- Risc Inicial Inherent  $R_i$  vs.  
Risc Acceptat  $R_a$ 
  - Cost seguretat inicial =  $R_i = \text{Prob}_i * \text{Impact}_i$
- Risc Residual  $R_r$  = Risc post-controls de mitigació
  - $R_r = \text{Prob}_r * \text{Impact}_r$
  - $C_f = \text{Cost Seg. Final} = R_r + \text{Depreciat} (\text{Instal} \cdot \text{lat} / \text{Anys Vida}) + \text{Manten.} + \text{Operació}$
  - Cost Final Seg.  $\leq$  Cost seguretat inicial



# Avaluació Controls de seguretat

- Actiu valorat en 1,000.000€
- Impacte degrada 80%:  $1,000.000 * .8 = 800.000$
- Probabilitat 10%
- Risc Inherent inicial  $R_i = 800.000 * 0,1 = 80.000€$
- Risc Acceptat  $R_a$  50.000
- Eficàcia de la salvaguarda redueix 50% la probabilitat
- Risc Residual  $R_r = (10% * 50%) * 800.000 = 40.000€$
- $C_f = \text{Cost Final Seg.} = 40.000 + 20.000/5 + 2.000 + 1.000$   
 $R_r = 47.000€ < R_a < R_i$

# Criteria d'èxit en estimació de Risc

- Qualitatiu

HIGH	MED	HIGH	VERY HIGH
MED	LOW	MED	HIGH
LOW	VERY LOW	LOW	MED
	LOW	MED	HIGH

- Quantitatiu

- Pèrdua esperada (€) =

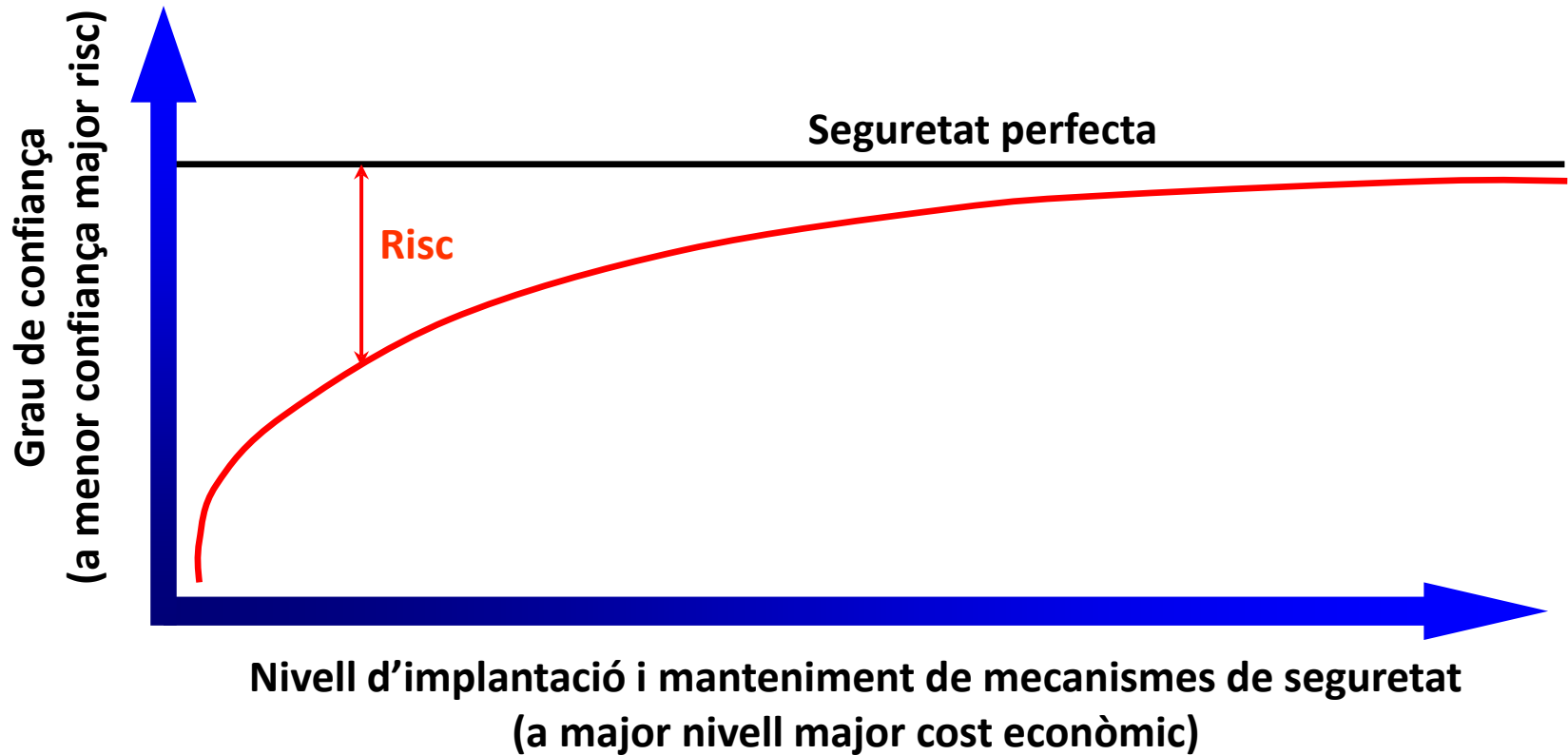
- Probabil. D'atac amb èxit (%) \* Impacte a l'actiu (€)

- Valor actiu, pèrdua productivitat o intangible, ...

# Analitzant els riscos: CRAMM

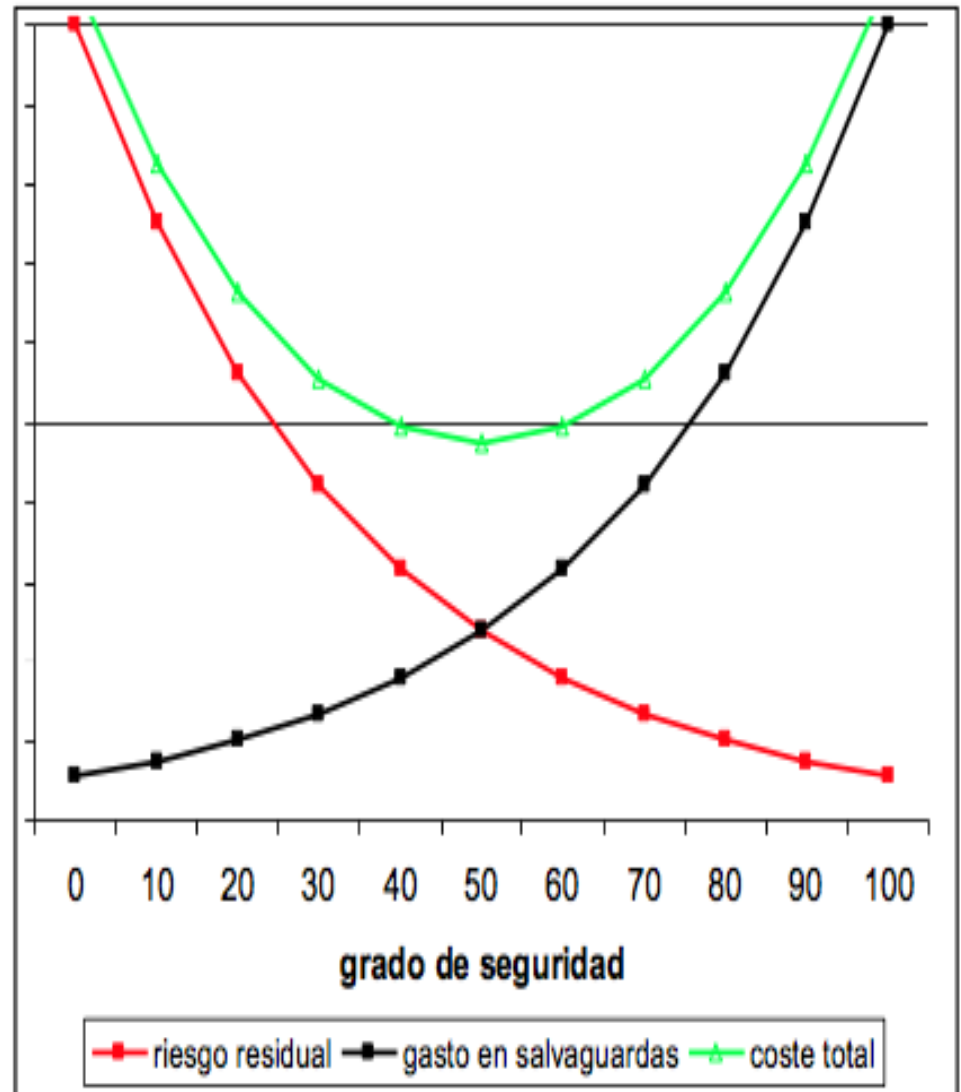
Probabilidad	1					2					3					4					5				
Impacte	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
Valor																									
1	3	4	5	6	7	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11
2	4	5	6	7	8	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12
3	5	6	7	8	9	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13
4	6	7	8	9	10	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13	10	11	12	13	14
5	7	8	9	10	11	8	9	10	11	12	9	10	11	12	13	10	11	12	13	14	11	12	13	14	15
de 3 a 7	Control no necessari																								
de 8 a 10	Control recomenat																								
de 11 a 15	Control obligatorio																								

# Analitzant els riscos: ROSI



# Gestió del risc: Equilibri

- Motivació:
  - Magnitud del risc
  - Reglaments sectorials
  - Obligacions legals
  - Contractes organitzatiu



# MAGERIT – Estimación salvaguardas

## - Estimación de su eficacia:

- ♦ NA : no aplica
- ♦ 0% L0        inexistente
- ♦ 10% L1       inicial / ad hoc
- ♦ 50% L2       reproducible, pero intuitivo
- ♦ 90% L3       proceso definido
- ♦ 95% L4       gestionado y medible
- ♦ 100% L5      optimizado

### Estrategia de mitigación del Riesgo:

- (RF) Reducción de frecuencia (Preventiva)
- (RI) Reducción Impacto o degradación (Correctiva)
- (M) Mixta. RI+RF
- (R) Recuperación tras catástrofe
- (D) Detección. Permite reacción temprana

• **COSTE..... N / B / M / A**

# MAGERIT - Salvaguardas

ejemplo: Eficacia de las salvaguardas - Centro Criptológico Nacional

Editar Exportar Importar Estadísticas

[base] Base Fuentes de información

aspec...	estrat...	salvaguarda	dudas	fuer...	come...	reco...	current	3m	1y	2y
SALVAGUARDAS										
T	M	[H] Protecciones Generales				10	L1	L3	L3	
G	M	[S] Protección de los Servicios				8	L1	L2	L3	
G	M	[I] Protección de la Información				10	L1	L2	L3	
G	M	[SW] Protección de las Aplicaciones Informáticas (SW)				8	L1	L2	L3	
G	M	[SW1] Normativa sobre el uso de las aplicaciones				3	L1	L2	L3	
G	M	[SW2] Procedimientos de uso de las aplicaciones				3	L1	L2	L3	
G	RF	[SW3] Inventario de aplicaciones (SW)				6	L1	L2	L3	
G	M	[SW4] Protección de los derechos de propiedad intelectual (IPR)				7	L1	L2	L3	
G	M	[SW5] Copias de seguridad (backup) (SW)				6	L1	L2	L3	
G	M	[SW6] Adquisición de aplicaciones SW				3	L1	L2	L3	
G	M	[SW8] Puesta en producción				4	L1	L2	L3	
T	M	[SW9] Aplicación de perfiles de seguridad (SW)				8	L1	L2	L3	
G	M	[SWa] Explotación / Producción				7	L1	L2	L3	
G	M	[SWb] Cambios (actualizaciones y mantenimiento)				6	L1	L2	L3	
G	M	[SWc] Terminación				3	L1	L2	L3	
G	M	[HW] Protección de los Equipos Informáticos (HW)				7	L1	L2	L3	
G	M	[COM] Protección de las Comunicaciones				10	L1	L3	L3	
G	M	[COM1] Normativa sobre el uso correcto de las comunicaciones				4	L1	L3	L3	
G	M	[COM2] Procedimientos de uso de las comunicaciones				4	L1	L3	L3	
G	RF	[COM3] Inventario de servicios de comunicación				3	L1	L3	L3	
G	M	[COM4] Aseguramiento de la disponibilidad				6	L1	L3	L3	
T	M	[COM5] Adquisición o contratación (COM)				6	L1	L3	L3	
T	M	[COM6] Aplicación de perfiles de seguridad (COM)				10	L1	L3	L3	
G	M	[COM7] Protección criptográfica del canal (COM)				10	L1	L3	L3	
T	M	[COM8] Operación				8	L1	L3	L3	
G	M	[COM9] Cambios (actualizaciones y mantenimiento)				7	L1	L3	L3	
G	M	[COMa] Terminación				4	L1	L3	L3	
G	M	[COMb] Internet: uso de o acceso a				7	L1	L3	L3	
G	M	[COMc] Seguridad Wireless (WiFi)				7	L1	L3	L3	
T	M	[COMe] KB HCOMLrdsi Seguridad RDSI				8	L1	L3	L3	
G	M	[COMf] KB COMApn Red privada virtual (VPN)				4	L1	L3	L3	
G	M	[AUX] Elementos Auxiliares				7	L1	L2	L3	
F	M	[I] Protección de las Instalaciones				7	L1	L2	L3	
G	M	[G] Organización				7	L1	L2	L3	

nivel - 1 + fuentes

operación sugiere

buscar >>

¿...?

L0 - inexistente  
L1 - inicial / ad hoc  
L2 - reproducible, pero intuitivo  
L3 - proceso definido  
L4 - gestionado y medible  
L5 - optimizado  
no es aplicable

(0-3) Interesantes (4-5) Importantes (6-7) muy importantes (8-9) críticas

# ENS – EAR-PILAR

Entorno de **Análisis de Riesgos** -

**Procedimiento Informático y Lógico de Análisis de Riesgos**

- ¿Qué es?
  - Herramienta automatizada de análisis de riesgos utilizada en la Administración española, siguiendo la metodología MAGERIT.
- Objetivos
  - Facilidad de uso
  - Flexibilidad
  - Adaptarse a las políticas
    - Nacional / Empresa
    - OTAN / UE
  - Priorización de salvaguardas
  - Análisis dinámicos y distribuidos
  - Infraestructuras críticas
  - Apoyo ENS



# PILAR – Conjunto de herramientas

- PILAR / EAR
  - Análisis de Riesgos cualitativo / cuantitativo
  - Análisis de impacto-continuidad de negocio cuantitativo /cualitativo
- Pilar BASIC
  - Análisis de riesgos para sistemas pequeños.
- Herramientas de personalización (RMAT) (Risk Management Additional Tools)
  - *EVL* - Perfiles de protección: Criterios de evaluación/acreditación específicos
  - *TSV* - Perfiles de amenazas: Estableciendo la vulnerabilidad típica de los activos frente a las amenazas en diferentes entornos de operación.
  - *KB* - Protecciones adicionales: Detallando protecciones adicionales. Se puede llegar a dar instrucciones al administrador del activo.
- Creación de nuevas bibliotecas
  - *BLANCA*: compilador de bibliotecas (no se distribuye)

# PILAR - EAR

- Herramienta de Análisis y gestión de riesgo



- **Análisis cualitativo.** Las valoraciones de los elementos (activos, amenazas y salvaguardas) se realiza por niveles, desde la irrelevancia hasta la máxima importancia o criticidad. Esto hace un **análisis rápido del que lo más importante es la relativización de impactos y riesgos.**
- **Análisis cuantitativo.** Las valoraciones son numéricas, típicamente en términos dinerarios. Esto hace el **análisis mucho más preciso, si se consigue validar los datos empleados.** El análisis puede llegar a **ofrecer resultados de recuperación de la inversión en salvaguardas,** en términos de riesgo menguante.

# PILAR - EAR

- Las herramientas emplean el concepto de “**categoría de activos**” para organizar el inventario y para ayudar al analista en la identificación de amenazas y salvaguardas relevantes. Las herramientas pueden hacer sugerencias al analista, basándose en la categoría de los activos involucrados.
- También se soporta la presentación del **riesgo como acumulado sobre los activos de soporte o repercutido en los servicios prestados**, como se explicó anteriormente.
- La herramienta busca un amplio espectro de utilización. En su vertiente más ejecutiva (casi con toda seguridad, cualitativa) se busca poder **levantar un primer plano de riesgos en una jornada**, con resultados al menos orientados en la dirección correcta. La captura de datos y automatización permite que aquel esbozo rápido pueda ser refinado y mantenido capturando una caracterización más precisa (probablemente cuantitativa) de la organización.

# PILAR – Análisis y gestión de riesgos

- Se analizan los riesgos en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y auditabilidad (*accountability*).
  - Para tratar el riesgo se proponen:
    - normas de seguridad (preventivas y formativas)
    - procedimientos de seguridad (operativos y reactivos)
    - salvaguardas (o contra medidas)
  - Se analiza el riesgo residual a lo largo de diversas etapas de tratamiento.
- Análisis de Impacto y Continuidad de Operaciones
  - Se analiza el efecto de las interrupciones de servicio informático en los procesos de negocio, teniendo en cuenta la duración de la interrupción.
  - Para minimizar el impacto se proponen:
    - salvaguardas (o contra medidas)
    - elementos de respaldo (*back up*)
    - planes de recuperación de desastres, hasta funcionalidad operativa mínima (resiliencia)
    - Procedimientos de restauración de servicios hasta el 100%
  - Se analiza el impacto residual sobre diversas etapas de tratamiento.

# PILAR – Etapas del análisis de riesgos

- Metodología MAGERIT

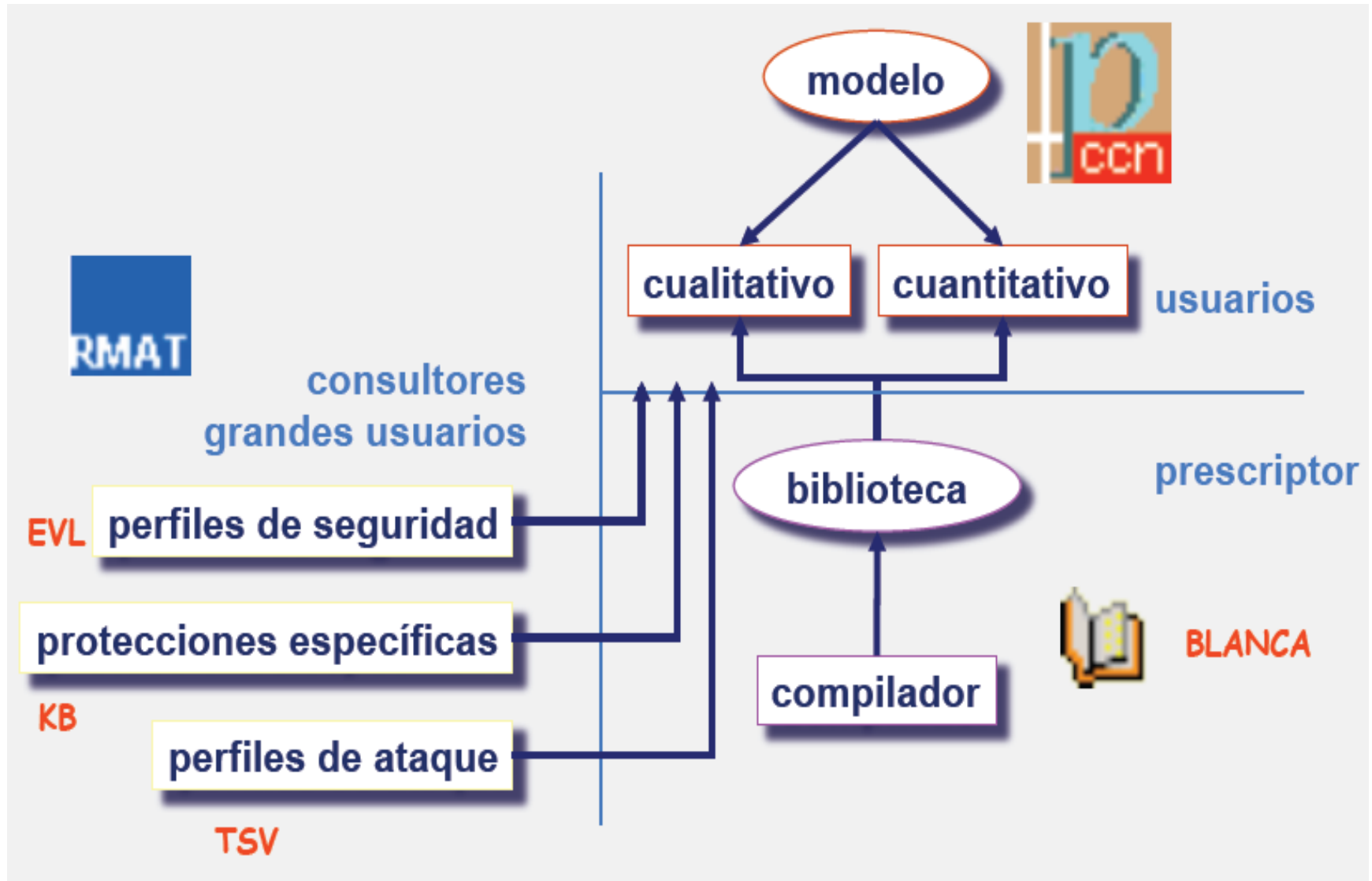


# PILAR – Etapas del análisis de riesgos

- Metodología MAGERIT



# PILAR - Diseño



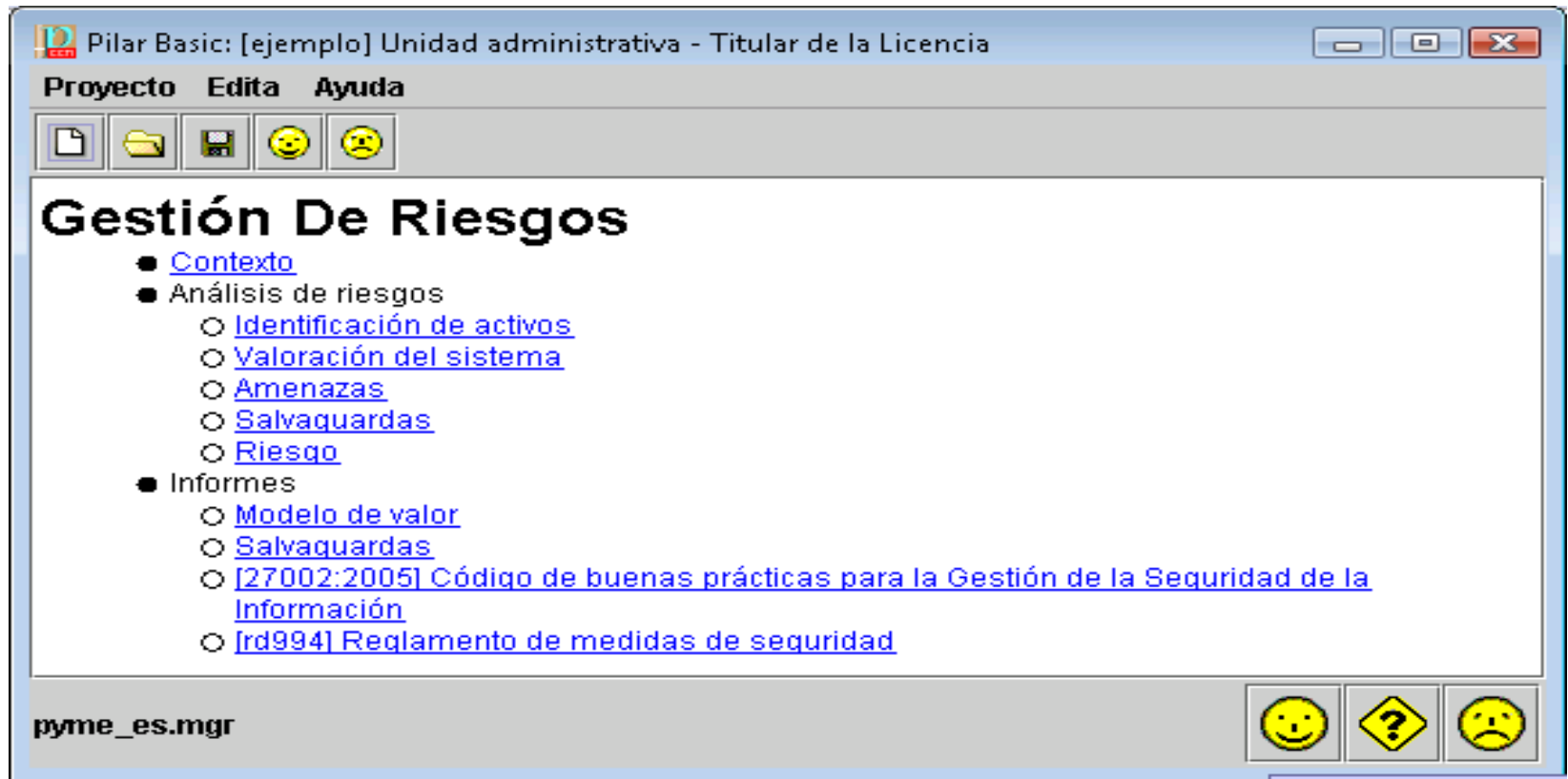
# PILAR - Bibliotecas

- Entorno adaptable. Se puede trabajar con diferentes marcos, estando dentro de lo parametrizable
  - **categorías de activos**
  - dimensiones de **valoración** de los activos (típicamente, disponibilidad, integridad, confidencialidad y autenticidad; pero hay casos más simples y más complejos)
  - colección de **amenazas**
  - **niveles de valoración cualitativa** de activos y amenazas
  - **clasificación de salvaguardas**, unas **técnicas**, otras de tipo **organizativo**; pero todas ellas con un **efecto** sobre el riesgo
- En el desarrollo actual se trabaja con tres **bibliotecas**
  - **criterios** de seguridad que es una guía de recomendaciones y obligaciones para proteger los activos empleados por la **administración pública**
  - **UNE-ISO/IEC 17799 (ISO 27001)** que es una guía ampliamente difundida internacionalmente, y base de los protocolos de certificación 7799-2 y 71502, antes citados
  - **defensa**, que es una biblioteca específica del Ministerio de Defensa para material clasificado
- Se está trabajando en **nuevas librerías**, concretamente para afrontar
  - **protección de datos de carácter personal**, que permita analizar el estado de seguridad de los datos a la vista de las medidas de seguridad implantadas, más allá del mero cumplimiento de las obligaciones legales
  - **criterios comunes** que permita tanto la elaboración de **perfiles de protección** como una evaluación del **riesgo efectivo** cuando se satisfacen perfiles de certificación



# PILAR - BASIC

- Versión sencilla para PYME y Administración local



- Se **analizan los riesgos** en varias dimensiones: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad (*accountability*).
- Para tratar el riesgo se **proponen salvaguadas** (o contra medidas), analizándose el **riesgo residual** a lo largo de diversas etapas de tratamiento.

# PILAR - RMAT

- RMAT (Risk Management Additional Tools) - Personalización de las herramientas
  - Herramientas de personalización (RMAT)
    - *EVL: perfiles de seguridad.* Criterios de evaluación/acreditación específicos de ciertos sectores o de puntos de vista específicos. Por ejemplo: leyes nacionales de protección de datos personales.
    - *TSV: threat profiles.* Estableciendo la vulnerabilidad típica de los activos frente a las amenazas en diferentes entornos de operación.
    - *KB: protecciones adicionales por activo.* Detallando protecciones adicionales sobre ciertos tipos de activos. Se puede llegar a dar instrucciones al administrador del activo.
  - Estas herramientas permiten **preparar y mantener personalizaciones**, que se incorporan dinámicamente a la biblioteca, extendiéndola para **adaptarse** a un determinado **contexto**.
  - Las herramientas de personalización no están previstas para usuarios finales, sino para consultores y grandes organizaciones.

# PILAR - BLANCA

- Las bibliotecas EAR incorporan a título de conocimiento empotrado, una serie de clases de activos:
  - **amenazas** típicas
  - **salvaguardas** normalizadas
  - **ítems** estándar para una **política** de seguridad
  - **procedimientos** estándar de seguridad
  - conocimiento de cuán buena es una salvaguarda **mitigando** una amenaza
- Estas bibliotecas permiten:
  - Al Usuario de la herramienta
    - concentrarse en la identificación y valoración de activos, amenazas y salvaguardas
  - Al Receptor de los informes
    - usar una terminología común y comparar diferentes análisis de riesgos
  - Auditor
    - leer el informe con una terminología estandarizada
- Las herramientas de gestión de bibliotecas no son para el usuario final, sino para elaborar y mantener bibliotecas normalizadas.

# PILAR – Herramientas de usuario final

- CCN-STIC 470 C
- CCN-STIC 472 B
- 2 bibliotecas
  - STIC: estándar
  - CI: Infraestructuras críticas (CNPIC)
- N perfiles de seguridad
  - UNE ISO/IEC 17799:2005 (ISO/IEC 27002 – 2013)
  - Criterios de seguridad (MAP)
  - LOPD: Ley Organica 15/1999 (Directiva 95/46/CE) (Reglam. antiguo 994/1999) + Reglamento RD 1720/2007
  - OTAN / Clasificados
  - ENS
  - SP 800-53
- Perfiles de amenazas: *threat profiles*
- Bases de datos de conocimiento particular
  - *wifi, voip, keys, windows, email, firewalls, ...*

# ISO/IEC 27000

- [ISO/IEC 27000](#) — Information security management systems — **Overview and vocabulary**<sup>[6]</sup>
- [ISO/IEC 27001](#) IT- Security Techniques - ISMS— **Requirements**. [ISO/IEC 27001:2005](#) relied on Plan-Do-Check-Act cycle; [ISO/IEC 27001:2013](#) does not, but has been updated in other ways to reflect changes in technologies and in how organizations manage information.
- [ISO/IEC 27002](#) — **Code of practice** for information security management
- [ISO/IEC 27003](#) — Information security management system **implementation** guidance
- [ISO/IEC 27004](#) — Information security management — **Measurement**<sup>[7]</sup>
- [ISO/IEC 27005](#) — Information security **risk management**<sup>[8]</sup>
- [ISO/IEC 27006](#) — **Requirements for bodies providing audit and certification** of information security management systems
- [ISO/IEC 27007](#) — **Guidelines** for information security management systems **auditing** (focused on the **management** system)
- [ISO/IEC TR 27008](#) — Guidance for **auditors on ISMS controls** (focused on the information security controls)
- [ISO/IEC 27010](#) — Information security management for **inter-sector and inter-organizational** communications
- [ISO/IEC 27011](#) — Information security management guidelines for **telecommunications organizations**
- [ISO/IEC 27013](#) — Guideline on the **integrated implementation of ISO/IEC 27001 & ISO/IEC 20000-1**
- [ISO/IEC 27014](#) — Information security **governance**.<sup>[9]</sup> Mahncke assessed this standard in the context of Australian e-health.<sup>[10]</sup>

# ISO/IEC 27000

- ISO/IEC TR 27015 — Information security management guidelines for **financial services**
- ISO/IEC 27017 — Code of practice for information security controls for **cloud services**
- ISO/IEC 27018 — Code of practice for protection of **personally identifiable information (PII) in public clouds acting as PII processors**
- ISO/IEC 27031 — Guidelines for information and communication technology readiness for **business continuity**
- ISO/IEC 27032 — Guideline for **cybersecurity**
- ISO/IEC 27033-1 — **Network** security - Part 1: **Overview** and concepts
- ISO/IEC 27033-2 — **Network** security - Part 2: Guidelines for the **design and implementation** of network security
- ISO/IEC 27033-3 — **Network** security - Part 3: Reference networking **scenarios - Threats, design techniques and control issues**
- ISO/IEC 27033-5 — **Network** security - Part 5: Securing communications across networks using **Virtual Private Networks (VPNs)**
- ISO/IEC 27034-1 — **Application** security - Part 1: **Guideline** for application security
- ISO/IEC 27035 — Information security **incident management**
- ISO/IEC 27036-3 — Information security for **supplier relationships** - Part 3: Guidelines for **information and communication technology [supply chain security](#)**
- ISO/IEC 27037 — Guidelines **for identification, collection, acquisition and preservation of digital evidence**
- ISO 27799 — Information security management in **health**. how to protect personal health info.

# PILAR - BCM

- Variante de PILAR | EAR
  - comparte activos, dependencias, amenazas (D) y salvaguardas (D)
  - introduce escalones de interrupción, equipamiento de respaldo
- Busca:
  - identificar los elementos críticos
  - evaluar impacto y riesgo residual
    - impacto: tiempo máximo de parada
    - riesgo: de que ocurra
  - ayuda a evaluar costes

# PILAR – Cumpliendo el ENS

- Perfil de protección herramienta PILAR.
  - Adaptación de biblioteca
- CCN-STIC 801 Guía de implantación
  - Responsabilidades
  - Categorización
    - Criterios valoración información / servicios
  - Medidas de protección
    - Condición de aplicabilidad / Descripción
    - Referencias / Evidencias de cumplimiento
  - Tabla de relación
    - ISO 27002 / RD 1720 / CSNC/NIST SP 800-53
- CCN-STIC 802 Auditorias en el ENS
- Herramientas de apoyo:
  - Herramientas de controles
  - Herramientas de requisitos mínimos



# PILAR - Conclusiones

- Realizar un análisis de riesgos y gestionar el riesgo residual para tomar decisiones de inversión en seguridad de las TIC
- Actividad larga y costosa cuyos resultados deben mantenerse actualizados con el paso del tiempo
- Soporte de programas que permitan crear un modelo de análisis en un contexto adecuado y mantenerlo de forma incremental en el tiempo

# Resumen de metodologías mundiales

- **MAGERIT** (Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información). Elaborada por el Consejo Superior de Administración Electrónica de España, es una metodología de carácter público, perteneciente al Ministerio de Administraciones Públicas. Tiene como objetivo estudiar los riesgos que soporta un sistema de información y el entorno asociado a él. Está conformada por una serie de técnicas específicas para el análisis de riesgos, análisis mediante tablas, análisis algorítmico, árboles de ataque, técnicas generales, análisis costo-beneficio, entre otros.
- **EBIOS** (Expression des Besoins et Identification des Objectifs de Sécurité - Expresión de las Necesidades e Identificación de los Objetivos de Seguridad). Es promovido por la Dirección Central de Seguridad de Sistemas de Información (DCSSI-Francia) como norma internacional. Es un software de asistencia bajo **licencia libre**. Su enfoque simple y modular le permite adaptarse a todos los contextos y a distintas acciones de seguridad. Permite apreciar y tratar los riesgos relativos a la seguridad de los sistemas de información (SSI).

# Resumen de metodologías mundiales

- **OSSTMM** (Open Source Security Testing Methodology Manual). Manual de metodología Abierta de Testeo de Seguridad es una metodología para realizar análisis de vulnerabilidad que está basada en entregar resultados cuantificables y que ha sido desarrollada dentro de un proyecto de comunidad **Open Source**. Es la respuesta cuando un analista de seguridad informática se pregunta por dónde empezar, qué y cómo analizar, cómo presentar los resultados.
- **OWASP** (Open Web Application Security Project). Es un organismo sin ánimo de lucro creado en Estados Unidos y que cuenta con más de 60 capítulos locales repartidos en todo el mundo. Su objetivo es ayudar a las empresas a entender y mejorar la seguridad de sus aplicaciones y servicios Web. El proyecto crea documentación, herramientas y estándares Open Source sobre seguridad en Aplicaciones Web gracias a expertos de la comunidad internacional que, de forma voluntaria, colaboran en los distintos proyecto.

# ISO27001 e ENS – Otras herramientas

- GlobalSGSI
- ISOTools (?)
- e-PULPO
- Octave
- CRAMM
- CORBA

# Global SGSI

- Que es?
  - Herramienta de gestión integral de la norma ISO 27001 que cumple con el ciclo completo de la misma, desde las fases de inicio y planificación del proyecto hasta el mantenimiento, pasando por el análisis de riesgos y el cuadro de mandos.
- Objetivo
  - Herramienta para gestionar de forma global el ciclo completo de la norma ISO 27001.
  - Ayuda a acompañar el proyecto de realización de un SGSI desde su nacimiento. Apoyándolo y asistiéndolo durante todo el proyecto, como la implantación, controles automáticos, centralizando y controlando la información, etc...
  - Uso de metodologías para la seguridad, el control y el aseguramiento de la calidad de las infraestructuras y procesos TIC en las organizaciones: ITIL, ISO 20000, ISO 27001, CobiT, CMMI..
- A quien va dirigido
  - Toda persona que desea abordar la implantación de un proyecto de ISO 27001. No es necesario ser experto en la norma puesto que la herramienta apoya el proceso de implantación y establece un camino guiado sobre todos los hitos del proyecto.
  - Adaptado al Esquema Nacional de Seguridad. Las Administraciones Públicas pueden implantar y adaptarse a dicho Esquema. La Licencia Premium permite configurar y adaptar la metodología de implantación y mantenimiento del sistema para cualquier tipo de Administración Pública, ya sea de la Administración General del Estado, Autonómica, etc.
  - Las Administraciones Públicas pueden implantar proyectos ISO 27001.

## Propiedades

- Definición de alcance
- Análisis diferencial
- Inventario de activos
- Análisis de riesgos (con ayudas a la hora de definir amenazas y vulnerabilidades)
- Gestión de riesgos (con ayudas a la hora de identificar controles de seguridad)
- Declaración de aplicabilidad
- Cuadro de mandos
- Auditorías, incidencias, soportes, usuarios, etc
- Documentación centralizada
- Gráficos, informes y plantillas para una mejor visualización

# ISO Tools

- Producto comercial
- Poca información disponible

# e-PULPO

- **Que es?**
  - Plataforma de **Unificación Lógica** de los **Procesos Organizativos (e-PULPO)**, que integra una serie de herramientas Open Source , para cubrir todo el abanico de necesidades relativas a la gestión de la seguridad de la información.
- **Objetivo**
  - **e-PULPO** es una herramienta software que permite la gestión completa de un Departamento de Tecnologías de la Información (TI) y que esta sea más eficiente y efectiva
- **A quien va dirigido**
  - Cualquier institución pública o privada
  - Cualquier institución pública o privada
- **Propiedades**
  - **Repositorio Único de Usuarios**
  - **Identificación Única de Usuarios:** SSO.
  - **Inventario de Activos:** Inventario automático a través de SNMP, mediante el despliegue de agentes en los equipos informáticos (identifica hardware y software) o mediante el escaneo de la red. Inventariado manual para activos tanto materiales como inmateriales. Integración con la Herramienta PILAR de Análisis y Gestión de Riesgos.
  - **Gestión de Activos:** Administración y gestión del inventariado de activos, proveedores, contratos y reservas. Registro, control y gestión de incidencias centralizado, notificadas a través de Web o correo electrónico. Proporciona una CMDB<sup>1</sup>.
  - **Análisis y Gestión de Riesgos:** Mediante la herramienta PILAR, basada en la metodología MAGERIT.
  - **Análisis de Impacto y Continuidad de Operaciones:** Mediante la herramienta PILAR.
  - **Gestión de Planes de Acción:** Planificación y ejecución de proyectos y planes para el tratamiento de riesgos.
  - **Cuadro de Mandos:** Métricas e indicadores para la medición de planes y objetivos.
  - **Gestión Documental:** Gestión de la documentación, definición de responsabilidades y accesos, workflow para tramitación, aprobación y difusión de documentos.
  - **Comunicación de Equipos de Trabajo:** Foros.
  - **Formación:** Plataforma de concienciación y tele formación, cuestionario de evaluación y exámenes de acreditación.
  - Cubre las recomendaciones básicas de las mejores prácticas de **ITIL**
  - Gestión de los requisitos legales (**LOPD** -Ley 15/1999 y RD 1720/2007-, **ENS** -RD 3/2010-).
  - Gestión de los requisitos normativos (**SGSI** -ISO 27001 e ISO 27002-, **SGTI** -ISO 20000-).

# e-Pulpo

- Cubre las recomendaciones básicas de las mejores prácticas de **ITIL**
- Gestión de los requisitos legales (**LOPD** -Ley 15/1999 y RD 1720/2007-, **ENS** -RD 3/2010-).
- Gestión de los requisitos normativos (**SGSI** -ISO 27001 e ISO 27002-, **SGTI** -ISO 20000-).

Módulo	SGSI	ENS	LOPD	ITIL
Activos	Activos con valor (desde sistemas hasta servicios)	Activos con valor (desde sistemas hasta servicios)	Ficheros con DCP <sup>6</sup>	Sistemas (HW y SW)
Documentación	Política, Normativa, Procedimientos	Política, Normativa, Procedimientos	Documento de Seguridad	Procedimientos
Incidencias	Incidencias de seguridad	Incidencias de seguridad	Restauración de backup, etc.	Incidencias de sistemas, solicitudes
Formación	Difusión SGSI	Formación del personal involucrado	Aceptación de los responsables	Difusión procedimientos
Indicadores	Métricas e indicadores	Sistema de métricas		SLA <sup>7</sup>
Auditoría	Anual (ISO 27001)	Bienal	Bienal	Anual (ISO 20000)





# Octave

- Que es?
  - Es un conjunto de herramientas, técnicas y métodos para la seguridad de la información estratégica basada en la evaluación y planificación de riesgos
- Objetivo
  - Desarrollo de una perspectiva de seguridad dentro de una organización, teniendo en cuenta perspectivas de todos los niveles para asegurar que las soluciones puedan implementarse con facilidad.
- A quien va dirigido
  - Cualquier institución pública o privada
- Propiedades
  - Fase 1- Identificación de activos críticos, áreas importantes, requerimientos de seguridad, actual estrategia de protección, vulnerabilidades. Se identifica la información a nivel general. Se organizan los perfiles de amenazas a los activos críticos (información consolidada)
  - Fase 2- Determinar sistemas importantes para activos críticos, vulnerabilidades de los componentes críticos, componentes claves y se evalúan dichos componentes.
  - Fase 3- Identificar riesgos sobre activos críticos, acciones, planes y estrategias de protección. Se realiza un análisis de riesgos y se desarrolla una estrategia de protección para luego revivir y aprobar la estrategia

# CRAMM

- Que es?
  - Cramm (CCTA Risk Analysis and Management Method - Método de Análisis y Gestión de Riesgos) fue creado en 1987 por el Centro de Informática y Telecomunicaciones Agencia (CCTA) del gobierno del Reino Unido. Cramm es actualmente en su quinta versión, CRAMM versión 5.0.
- Objetivo
  - Se compone de tres etapas, cada una con el apoyo de cuestionarios y directrices. Etapas de identificación y análisis de riesgos para el sistema y recomendaciones sobre la administración de estos riesgos.
- A quien va dirigido
  - OTAN, fuerzas armadas neerlandesas y las empresas que trabajan activamente en la seguridad, como Unisys, RAC, etc.
- Propiedades
  - Etapa 1: establecimiento de los **objetivos** de la seguridad:
    - Definición del límite de estudio
    - Identificación y valoración de los activos físicos que forman parte del sistema
    - La determinación del valor de los datos en poder de entrevistas con los usuarios acerca de los impactos de negocios potenciales que podrían derivarse de la no disponibilidad, la destrucción, la divulgación o modificación,
    - Identificación y valoración de los activos de software que forman parte del sistema
  - Etapa 2 La **evaluación de los riesgos** para el sistema propuesto y los requisitos para la seguridad:
    - Identificar y evaluar el tipo y el nivel de amenazas que pueden afectar al sistema
    - Evaluar el alcance de las vulnerabilidades del sistema a las amenazas detectadas
    - La combinación de la amenaza y la vulnerabilidad con los valores de activos para calcular las medidas de riesgos
  - Etapa 3 **Identificación y selección de las medidas** que sean proporcionales a las medidas de riesgos calculados en la Etapa 2. Cramm contiene una biblioteca muy grande de contramedida que consiste de más de 3000 contramedidas detallada organizados en más de 70 agrupaciones lógicas.

# COBRA

- Que es?
  - COBRA es un consultor de riesgos que ofrece un servicio completa en este ámbito.
- Objetivo
  - Análisis y gestión de riesgos: evaluación de la importancia relativa de todas las amenazas y vulnerabilidades así como la generación de recomendaciones y soluciones adecuadas. Los informes proporcionan una evaluación por escrito y a la medida del riesgo, o nivel, para cada categoría de riesgo.
- A quien va dirigido
  - Cualquier institución pública o privada
- Propiedades
  - Compatible con la mayoría de las metodologías reconocidas (cualitativos y cuantitativos).
  - Cuestionario del sistema y amplia base de conocimientos.
  - Identificación de amenazas y vulnerabilidades.
  - Medida del grado actual de riesgo de cada area o aspecto del sistema y su potencial impacto asociado al negocio (financieros, la pérdida de clientes, etc).
  - Solucion detallada y recomendaciones para reducir riesgos, así como informes técnicos.
  - Cumplimiento ISO17799 / BS7799

# Referencias

- VIII Foro de seguridad de RedIRIS, 22 de Abril, sesión CCN – MAGERIT – Herramienta PILAR. Ejemplo aplicación ENS. Ponencia del Centro Criptológico Nacional. <https://ccn-cert.cni.es>
- <http://www.csae.map.es/csi/pg5m20.htm>
- [http://www.csae.map.es/csi/pdf/2008\\_Magerit\\_AEMET.pdf](http://www.csae.map.es/csi/pdf/2008_Magerit_AEMET.pdf)
- <http://www.nexusasesores.com/docs/ISO%2027001-gestion-de-riesgos.pdf>