



Centro  
Criptológico  
Nacional



www.oc.ccn.cni.es



# HERRAMIENTA PILAR ESQUEMA NACIONAL DE SEGURIDAD

Madrid, Abril de 2010

SIN CLASIFICAR

- FORO: VIII Foro de seguridad de Red IRIS
- SESIÓN: CCN – MAGERIT- Herramienta PILAR. Ejemplo aplicación ENS
- OBJETIVO: Presentación de la herramienta PILAR y su aplicación al Esquema Nacional de Seguridad.
- PONENTE:
  - Centro Criptológico Nacional
- FECHA: April 22, 2010

## Índice

- Centro Criptológico Nacional
  - Marco Legal / Funciones
  - CCN-CERT
- Metodología MAGERIT V2
  - Conceptos
- Herramienta PILAR
  - Desarrollo v4.4. Funcionalidades 2010
  - Perfiles de protección.
- PILAR - Esquema Nacional de Seguridad
  - Adaptación biblioteca



## Marco Legal (2)

El CCN actúa según el siguiente marco legal:



**Ley 11/2002, 6 de mayo**, reguladora del Centro Nacional de Inteligencia (CNI), que incluye al Centro Criptológico Nacional (CCN).



**Real Decreto 421/2004, 12 de marzo**, que regula y define el ámbito y funciones del CCN.



**Orden Ministerio Presidencia PRE/2740/2007, de 19 de septiembre**, que regula el Esquema Nacional de Evaluación y Certificación de la Seguridad de las Tecnologías de la Información



**Real Decreto 3/2010, de 6 de enero**, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

## Funciones

- **Elaborar y difundir** normas, instrucciones, guías y recomendaciones para garantizar la seguridad de las TIC en la Administración
- **Formar** al personal de la Administración especialista en el campo de la seguridad de las TIC
- Constituir el **organismo de certificación** del Esquema Nacional de Evaluación y Certificación de aplicación a productos y sistemas de su ámbito
- **Valorar y acreditar** capacidad productos de cifra y Sistemas de las TIC (incluyan medios de cifra) para manejar información de forma segura
- Coordinar la promoción, el desarrollo, la obtención, la adquisición y puesta en explotación y la utilización de la **tecnología de seguridad** de los Sistemas antes mencionados
- Velar por el cumplimiento normativa relativa a la protección de la **información clasificada** en su ámbito de competencia (Sistemas de las TIC)
- Establecer las necesarias **relaciones** y firmar los acuerdos pertinentes con organizaciones similares de otros países. Para el desarrollo de las funciones mencionadas, **coordinación** oportuna con las **Comisiones nacionales** a las que la leyes atribuyan responsabilidades en el ámbito de los sistema de las Tecnologías de la Información y de las Comunicaciones.



## I. DISPOSICIONES GENERALES

### MINISTERIO DE LA PRESIDENCIA

- 1330** *Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.*

Artículo 29. *Guías de seguridad.*

Para el mejor cumplimiento de lo establecido en el Esquema Nacional de Seguridad, el Centro Criptológico Nacional, en el ejercicio de sus competencias, elaborará y difundirá las correspondientes guías de seguridad de las tecnologías de la información y las comunicaciones.

### CAPÍTULO VII

#### **Respuesta a incidentes de seguridad**

Artículo 36. *Capacidad de respuesta a incidentes de seguridad de la información.*

El Centro Criptológico Nacional (CCN) articulará la respuesta a los incidentes de seguridad en torno a la estructura denominada CCN-CERT (Centro Criptológico Nacional-Computer Emergency Reaction Team), que actuará sin perjuicio de las capacidades de respuesta a incidentes de seguridad que pueda tener cada administración pública y de la función de coordinación a nivel nacional e internacional del CCN.

Artículo 37. *Prestación de servicios de respuesta a incidentes de seguridad a las Administraciones públicas.*

1. De acuerdo con lo previsto en el artículo 36, el CCN-CERT prestará a las Administraciones públicas los siguientes servicios:

### Artículo 37. Prestación de servicios de respuesta a incidentes de seguridad a las Administraciones públicas.

1. De acuerdo con lo previsto en el artículo 36, el CCN-CERT prestará a las Administraciones públicas los siguientes servicios:

a) **Soporte y coordinación para el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad** que tengan la Administración General del Estado, las Administraciones de las comunidades autónomas, las entidades que integran la Administración Local y las Entidades de Derecho público con personalidad jurídica propia vinculadas o dependientes de cualquiera de las administraciones indicadas.

El CCN-CERT, a través de su servicio de apoyo técnico y de coordinación, actuará con la máxima celeridad ante cualquier agresión recibida en los sistemas de información de las Administraciones públicas. Para el cumplimiento de los fines indicados en los párrafos anteriores se podrán recabar los informes de auditoría de los sistemas afectados.

b) **Investigación y divulgación de las mejores prácticas sobre seguridad** de la información entre todos los miembros de las Administraciones públicas. Con esta finalidad, las series de documentos CCN-STIC (Centro Criptológico Nacional-Seguridad de las Tecnologías de Información y Comunicaciones), elaboradas por el Centro Criptológico Nacional, ofrecerán normas, instrucciones, guías y recomendaciones para aplicar el Esquema Nacional de Seguridad y para garantizar la seguridad de los sistemas de tecnologías de la información en la Administración.

c) **Formación** destinada al personal de la Administración especialista en el campo de la seguridad de las tecnologías de la información, al objeto de facilitar la actualización de conocimientos del personal de la Administración y de lograr la sensibilización y mejora de sus capacidades para la detección y gestión de incidentes.

d) **Información sobre vulnerabilidades, alertas y avisos de nuevas amenazas** a los sistemas de información, recopiladas de diversas fuentes de reconocido prestigio, incluidas las propias.

2. El CCN desarrollará un **programa** que ofrezca la información, formación, recomendaciones y herramientas necesarias para que las **Administraciones públicas** puedan **desarrollar sus propias capacidades de respuesta a incidentes de seguridad**, y en el que, aquél, será coordinador a nivel público estatal.

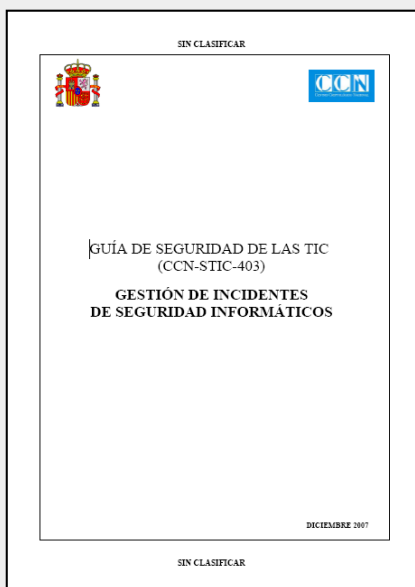




# Normativa

Elaborar y difundir normas, instrucciones, guías y recomendaciones para garantizar la seguridad de los Sistemas de las tecnologías de la información y las comunicaciones de la Administración

- CCN-STIC 000: Instrucciones/Políticas STIC
- CCN-STIC 100: Procedimientos
- CCN-STIC 200: Normas
- CCN-STIC 300: Instrucciones
- CCN-STIC 400: Guías de Gestión
- CCN-STIC 500: Guías de Entornos
- CCN-STIC 600: Guías de Configuración
- **CCN-STIC 800: Guías de Configuración de Seguridad**
- CCN-STIC 900: Informes



Datos a 31 de diciembre de 2009:

- 124 documentos pdf, 11600 páginas, 88 Mbyte

**SIN CLASIFICAR**

- PRINCIPAL
- SOBRE NOSOTROS
- INCIDENTES
- ACTUALIDAD / EVENTOS
- ALERTAS
- HERRAMIENTAS
- CCN-WINDOWS
- SERIES CCN-STIC (PÚBLICO)
- SERIES CCN-STIC
- SERIES CCN-STIC
- EAR / PILAR 4.3 (PÚBLICO)
- EAR / PILAR 4.3
- OTRAS HERRAMIENTAS
- RECURSOS
- PREFERENCIAS

PRESENTACIÓN DEL CCN-CERT EN LA COMUNIDAD VALENCIANA

Accredited by TRUSTED Introducer The European Cyber Directory EGC group

**ccn.cert** seguridad tic

capacidad de respuesta ante incidentes de seguridad de la información

NIVEL DE ALERTA MEDIO

CASTELLANO ENGLISH CATALÀ EUSKARA GALEGO VALENCIÀ

CERRAR SESIÓN

La Serie CCN-STIC-500 establece las configuraciones mínimas de seguridad de los diferentes elementos basados en la tecnología Windows.

**Serie 500: Guías de entornos Windows**

CCN-STIC-501B Seguridad en Windows XP SP2 (cliente independiente)	
VERSIÓN	Septiembre 2005 (esp) y Diciembre 2007 (eng)
CLASIFICACIÓN	SIN CLASIFICAR
DESCARGAS	<a href="#">Guía CCN-STIC-501B (esp)</a> Script (esp) <a href="#">Guía CCN-STIC-501B (eng)</a> Script (eng)
OBJETO	Proporcionar la configuración de seguridad para el sistema operativo "Windows XP Professional" con Service Pack 2 actuando como cliente independiente no integrado en un dominio.

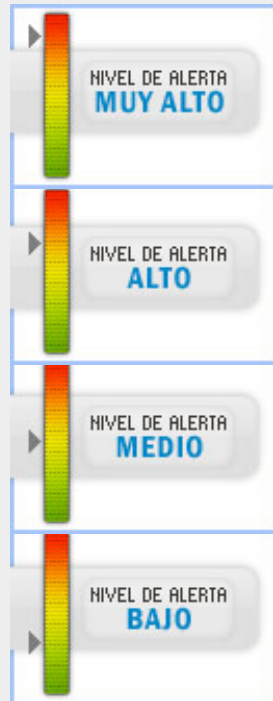
SALIR MENÚ ANTERIOR SIGUIENTE

F O R M A C I Ó N



# Centro Criptológico Nacional 2010

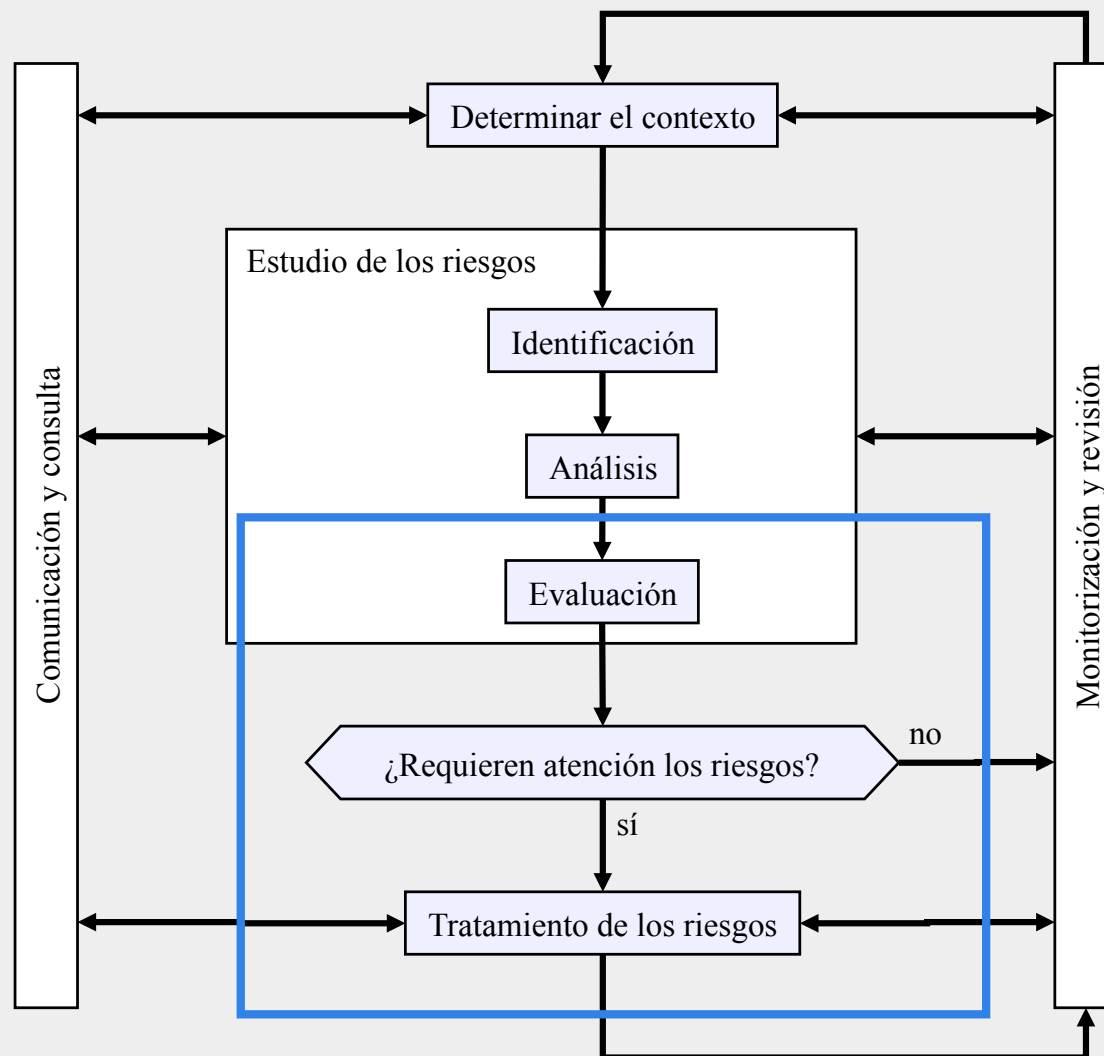
	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo	Lunes	Martes	Miércoles	Jueves	Viernes	Sábado	Domingo	Lunes	Martes					
<b>ENE</b>					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
<b>FEB</b>								1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28
<b>MAR</b>	VI Curso STIC - Fase de Correspondencia - Defensa																																		
	VII Curso STIC - Fase de Correspondencia																																		
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31				
<b>ABR</b>					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
	VI Curso STIC						VI Curso STIC						V Curso Básico STIC Entornos Windows						VII Curso STIC																
<b>MAY</b>					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	V Curso Básico STIC Entornos Linux						V Curso Básico STIC Base de Datos						V Curso STIC Redes Inalámbricas																						
<b>JUN</b>					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
	V Curso Básico STIC Infraestructura de Red						III Curso Common Criteria																												
<b>JUL</b>					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
<b>AGO</b>					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	VI Curso STIC Cortafuegos						VI Curso STIC Detección de Intrusos						III Curso STIC Búsqueda Evidencias																						
<b>SEP</b>					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	
	XXII Curso de Especialidades Criptológicas (correspondencia)																																		
<b>OCT</b>					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	V Curso STIC Inspecciones de Seguridad						II Jornada de Seguridad en Aplicaciones Web						VII Curso Gestión STIC (Presencial)																						
	VI I Curso Gestión STIC (Correspondencia)																																		
	XXII Curso de Especialidades Criptológicas (correspondencia)																																		
<b>NOV</b>	XXI CEC (Correspondencia)					XXII CEC					XXII Curso de Especialidades Criptológicas (presencial)					XXI Curso de Especialidades Criptológicas (presencial)					XXII CEC														
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30					
<b>DIC</b>					1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
	XXII CEC						X Curso Herramienta PILAR																												




The screenshot shows the CCN-CERT website with a navigation menu on the left, a main content area with sections for 'ULTIMAS VULNERABILIDADES', 'SERIES CCN-STIC', 'NOTICIAS SEGURIDAD', and 'COMUNICADOS CCN-CERT', and a right sidebar with 'CATÁLOGO DE SERVICIOS' and 'Presentación del CCN-CERT en Galicia'. A red circle highlights the 'HERRAMIENTA PILAR' section, which contains the text: 'Procedimiento Informático Lógico para el Análisis de Riesgos (Última versión)'. The alert level is set to 'MEDIO'.

En febrero 2100 usuarios  
registrados  
**SIN CLASIFICAR**

# Gestión de riesgos 27005



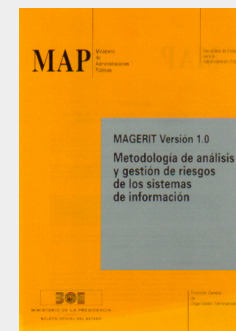


# MAGERIT

- **M**ETODOLOGIA DE **A**NALISIS Y **G**ESTION DE **R**IESGOS DE  
LOS SISTEMAS DE **I**NFORMACION DE LAS  
ADMINIS**T**RACIONES PUBLICAS

**AÑO 1997**

**SIN CLASIFICAR**





✘ 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

AÑO 2004

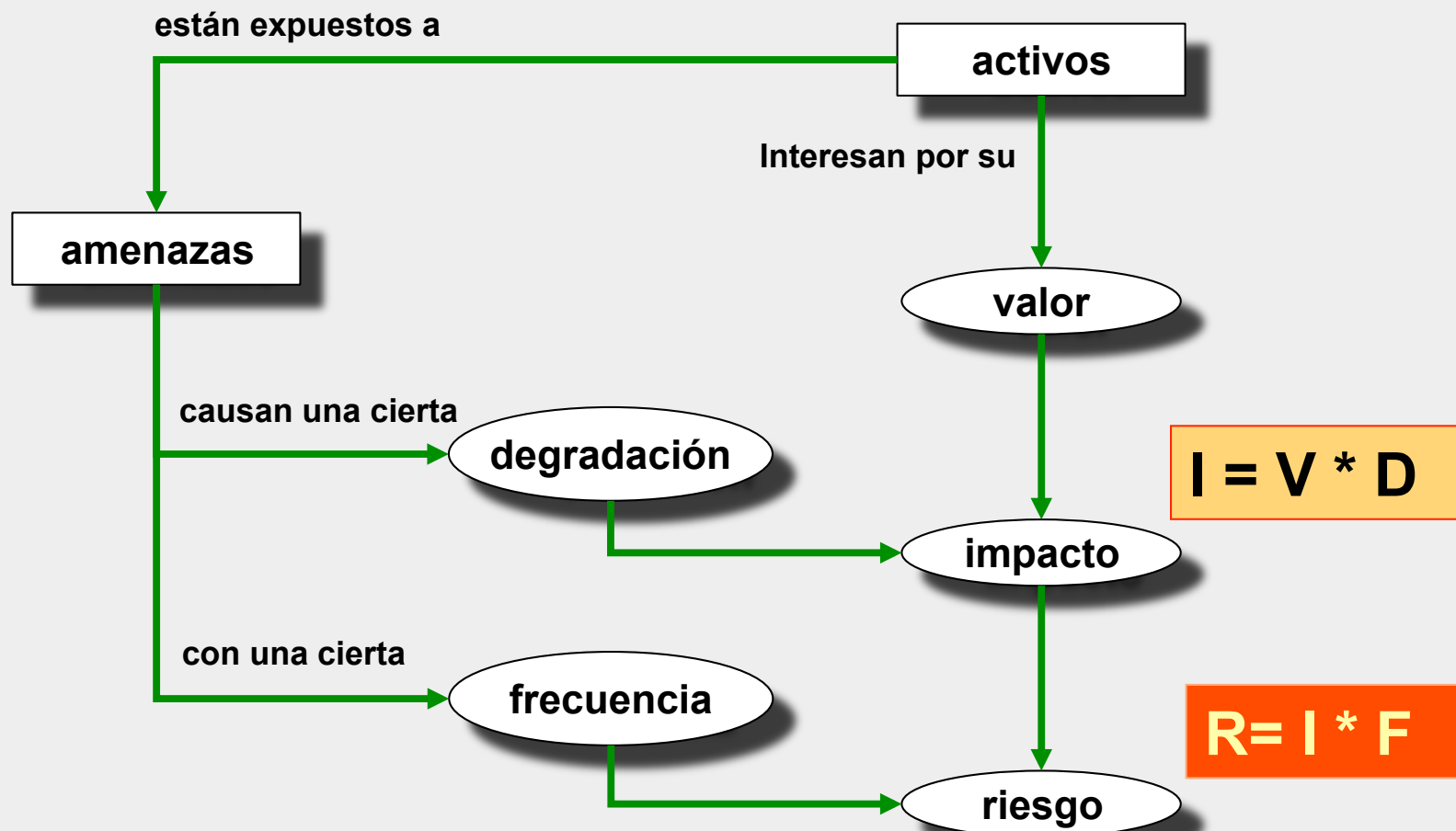
✘ Libro de técnicas

- 73 páginas

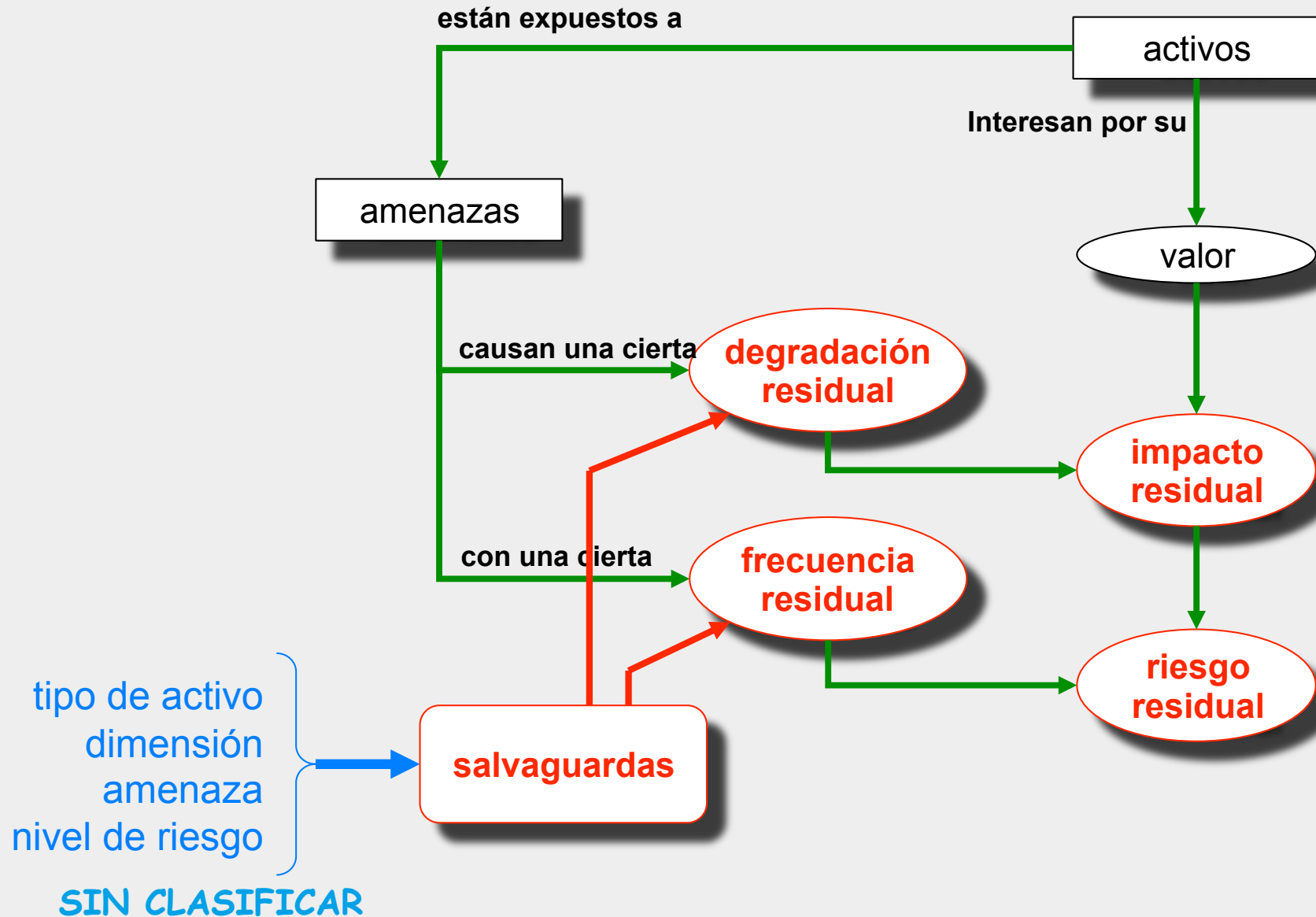
MAP, versión 2 (1.1 junio de 2006)

<http://www.csi.map.es/csi/pg5m20.htm>

# Magerit : Análisis de Riesgo



# Magerit : Gestión de Riesgo



## Evaluación de 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**

# SALVAGUARDAS

ejemplo: Eficacia de las salvaguardas - Centro Criptológico Nacional

Editar Exportar Importar Estadísticas

[base] Base Fuentes de información

aspect...	estrat...	salvaguarda	dudas	fuelle	come...	reco...	current	3m	1y	2y
T	M	[H] Protecciones Generales				10	L1	L3	L3	
G	M	[S] Protección de los Servicios				8	L1	L2	L3	
G	M	[D] 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 ó acceso a				7	L1	L3	L3	
G	M	[COMc] Seguridad Wireless (WiFi)				7	L1	L3	L3	
T	M	[COMe] KB HCOM.rdsi Seguridad RDSI				8	L1	L3	L3	
G	M	[COMf] KB COM.vpn Red privada virtual (VPN)				4	L1	L3	L3	
G	M	[AUX] Elementos Auxiliares				7	L1	L2	L3	
F	M	[L] Protección de las Instalaciones				7	L1	L2	L3	
G	M	[G] Organización				7	L1	L2	L3	

¿...?

L0 - inexistente

L1 - inicial / ad hoc

L2 - reproducible, pero intuitivo

L3 - proceso definido

L4 - gestionado y medible

L5 - optimizado

no es aplicable

¿...?

nivel - 1 + fuentes

operación sugiere

buscar >>

SIN CLASIFICAR (0-3) Interesantes (4-5) Importantes (6-7) muy importantes (8-10) criticas



# EAR-PILAR



The screenshot shows the CCN CERT website interface. At the top, there is a navigation menu with options like 'PRINCIPAL', 'SOBRE NOSOTROS', 'INCIDENTES', 'ACTUALIDAD / EVENTOS', 'ALERTAS', 'HERRAMIENTAS', 'CCN-WINDOWS', 'SERIES CCN-STIC', 'EAR / PILAR 4.3 (PÚBLICO)', 'EAR / PILAR 4.3', 'OTRAS HERRAMIENTAS', 'SISTEMA MULTIANIVIRUS', 'RECURSOS', and 'PREFERENCIAS'. Below the menu, there are logos for 'MAV', 'FIRST', 'Accredited by TRUSTED', 'Introducer The European CERT Directory', and 'EGC group'. The main content area features the 'EAR / PILAR - Entorno de Análisis de Riesgos' section, which includes a flowchart and a sidebar with a language selector and a session button.

**EAR / PILAR - Entorno de Análisis de Riesgos**

Las herramientas EAR soportan el análisis y la gestión de riesgos de un sistema de información siguiendo la metodología **Maqerit**.

The flowchart illustrates the risk analysis process:

- Activos** (Assets) and **Amenazas** (Threats) are interconnected. Threats materialize on assets, and assets have value.
- Valor** (Value) and **Degradación** (Degradation) are interconnected. Degradation allows for the estimation of value, and value allows for the estimation of degradation.
- Impacto** (Impact) and **Frecuencias** (Frequencies) are interconnected. Frequencies allow for the estimation of impact, and impact allows for the estimation of frequencies.
- Riesgo** (Risk) is derived from the combination of impact and frequencies.
- Salvaguadas** (Controls) mitigate the risk, limiting it to a value.
- Riesgo residual** (Residual Risk) is the result of the risk after controls are applied.

- Entorno de Análisis de Riesgos
- PROCEDIMIENTO INFORMATICO Y LOGICO DE ANALISIS DE RIESGOS

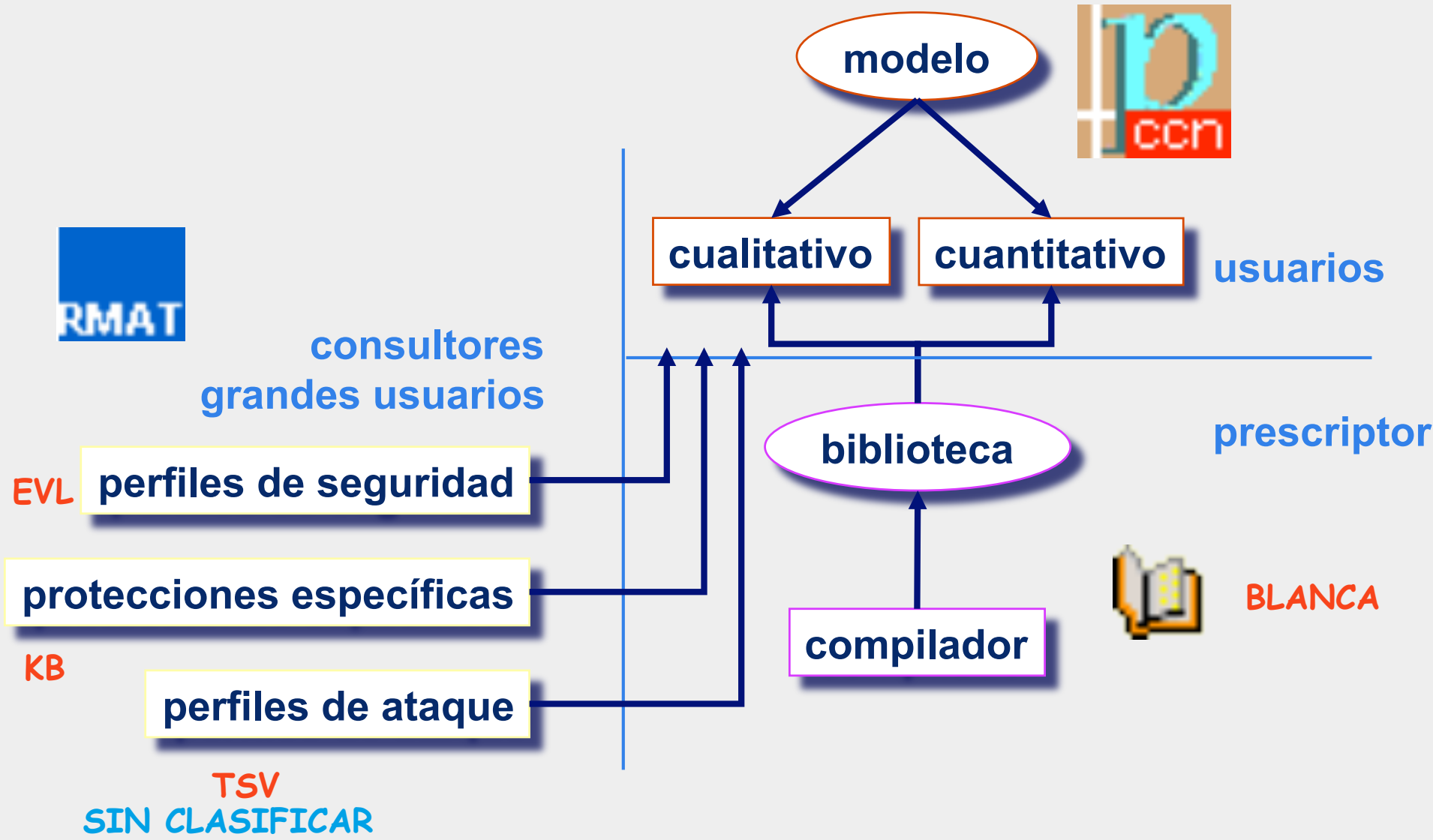
SIN CLASIFICAR

## EAR / PILAR 4.4.2

- Proyecto CCN → Desarrollador A.L.H. J. Mañas S.L.
  - ♦ PILAR: uso restringido a la administración pública / herramienta comercial
- **OBJETIVO PILAR:**
  - **FACILIDAD DE USO.**
  - **FLEXIBILIDAD.**
  - **Adaptarse a las políticas:**
    - NACIONAL / EMPRESAS
    - OTAN / UE
  - **PRIORIZACIÓN SALVAGUARDAS.**
  - **ANÁLISIS DINÁMICOS / DISTRIBUIDOS**
  - **INFRAESTRUCTURAS CRÍTICAS**
  - **APOYO ENS**
- **Multilinguaje (8 idiomas)**
  - Español / Inglés / Francés / Italiano / Alemán / Húngaro / Portugués (Brasileño) ....

**SIN CLASIFICAR**

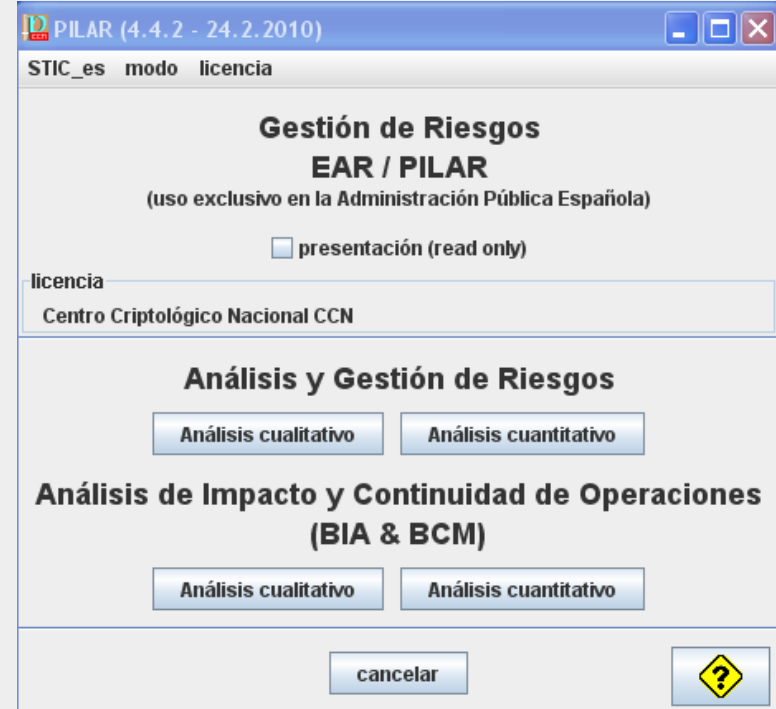
# Diseño EAR / PILAR



## Conjunto de Herramientas

- PILAR / EAR
  - ◆ Análisis de Riesgos cualitativo / cuantitativo
  - ◆ Análisis de impacto-continuidad de negocio cuantitativo / cualitativo
- Pilar BASIC
  - ◆ Análisis de riesgos para PYMES / Sistemas pequeños.
- Herramientas de personalización (RMAT)
  - EVL: perfiles de seguridad*
  - TSV: threat profiles*
  - KB: protecciones adicionales por activo*
- Creación de nuevas bibliotecas
  - BLANCA: compilador de bibliotecas*
  - (no se distribuye)*

SIN CLASIFICAR



## Marzo 2010 Herramientas de usuario final

- CCN-STIC 470 C
- CCN-STIC 472 B
  
- 2 bibliotecas
  - ◆ STIC: estándar
  - ◆ CI: Infrast críticas (CNPIC)
- N perfiles de seguridad
  - ◆ UNE ISO/IEC 17799:2005
  - ◆ Criterios de seguridad (MAP)
  - ◆ Real Decreto 994 /1720
  - ◆ OTAN / Clasificados
  - ◆ ENS
  - ◆ SP 800-53
- perfiles de amenazas: *threat profiles*
- bases de datos de conocimiento particular
  - ◆ *wifi, voip, keys, windows, email, firewalls, ...*

**SIN CLASIFICAR**



PILAR: [ejemplo] Unidad administrativa - Centro Criptológico Nacional

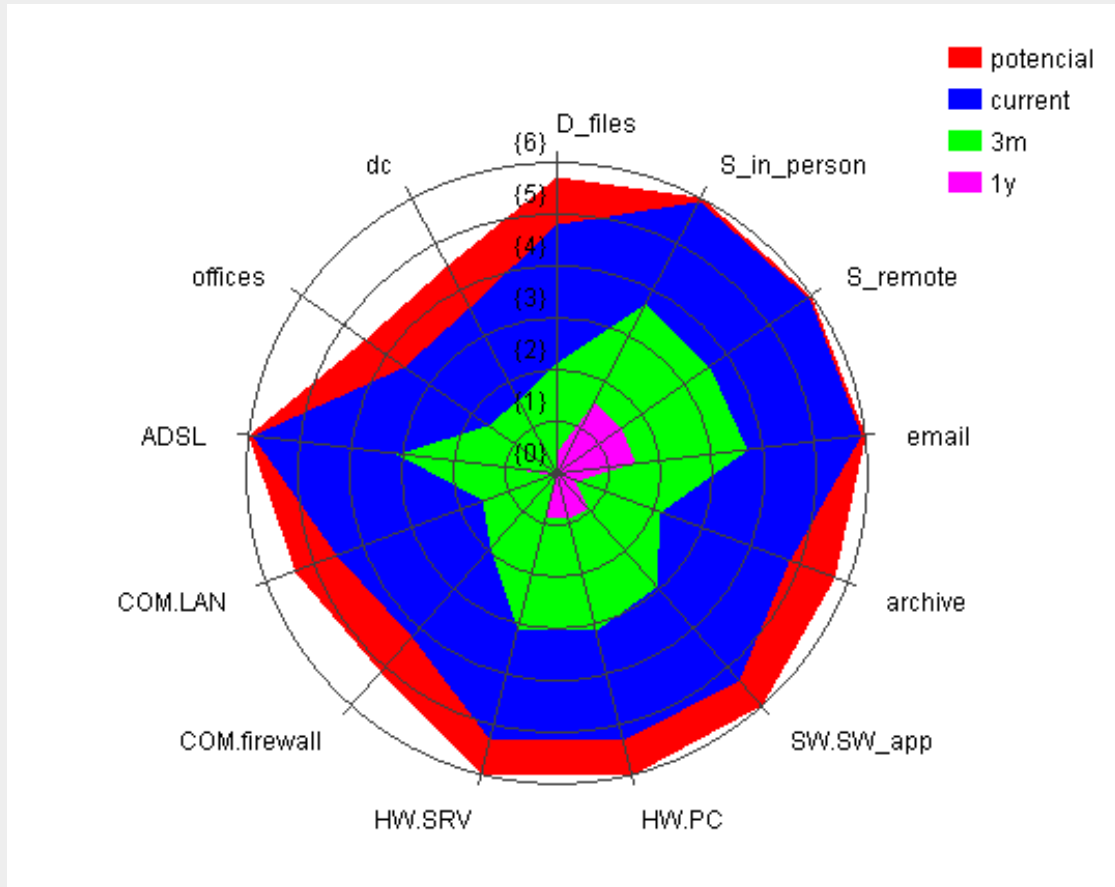
Proyecto Fichero Editar Nivel Ayuda

Análisis cualitativo

- D. Proyecto
  - A. Análisis de riesgos
    - A.1. Activos
      - A.1.1. identificación
      - A.1.2. clases de activos
      - A.1.3. valoración de los dominios
      - A.1.4. dependencias
      - A.1.5. valoración de los activos
    - A.2. Amenazas
      - A.2.1. vulnerabilidad de los dominios
      - A.2.2. identificación
      - A.2.3. valoración
    - A.3. Impacto y riesgo
      - A.3.1. impacto
      - A.3.2. riesgo
      - A.3.3. tabla
      - A.3.4. Valores repercutidos
  - T. Tratamiento de los riesgos
    - T.1. Fases del proyecto
    - T.2. Salvaguardas
      - T.2.1. identificación
      - T.2.2. valoración
      - T.2.3. específicas de activos
    - T.3. Protecciones adicionales
    - T.4. Procedimientos de seguridad
    - T.5. Impacto y riesgo residuales
  - R. Informes
  - E. Perfiles de seguridad
    - [27002:2005] Código de buenas prácticas para la Gestión de la Seguridad de la Información
    - [cscn] Criterios de seguridad, normalización y conservación
    - [ens:2010] Esquema Nacional de Seguridad
    - [policies] Normativa de seguridad
    - [RD 1720] Protección de datos de carácter personal
    - [SP800-53] Recommended Security Controls for Federal Information Systems
    - otros



# INFORMES GRAFICOS. Riesgo Residual



## Reducción del Riesgo

**Sin salvaguardas**

**Fase presente**

**Plan de Seguridad 3 meses**

**Plan de seguridad 1 año**

**SIN CLASIFICAR**

# PILAR-ENS

## Principios básicos

- a) Seguridad integral
- b) Gestión de riesgos
- c) Prevención, reacción y recuperación
- d) Líneas de defensa
- e) Reevaluación periódica
- f) La seguridad como función diferenciada

## Requisitos mínimos:

- a) Organización e implantación del proceso de seguridad
- b) Análisis y gestión de los riesgos
- c) Gestión de personal
- d) Profesionalidad
- e) Autorización y control de los accesos
- f) Protección de las instalaciones
- g) Adquisición de productos
- h) Seguridad por defecto
- i) Integridad y actualización del sistema
- j) Protección de la información almacenada y en tránsito
- k) Prevención ante otros sistemas de información interconectados
- l) Registro de actividad
- m) Incidentes de seguridad
- n) Continuidad de la actividad
- o) Mejora continua del proceso de seguridad

## Medidas de seguridad

(Protección adecuada de la información)

- a) Marco organizativo
- b) Marco operacional
- c) Medidas de protección

Artículo 6. *Gestión de la seguridad basada en los riesgos.*

1. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.

2. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

## Medidas de seguridad. Marco organizativo / OPERACIONAL

Afectadas	Dimensiones			MEDIDAS DE SEGURIDAD	
	B	M	A		
				<b>org</b>	<b>Marco organizativo</b>
categoria	aplica	=	=	org.1	Política de seguridad
categoria	aplica	=	=	org.2	Normativa de seguridad
categoria	aplica	=	=	org.3	Procedimientos de seguridad
categoria	aplica	=	=	org.4	Proceso de autorización
				<b>op</b>	<b>Marco operacional</b>
				op.pl	Planificación
categoria	n.a.	+	++	op.pl.1	Análisis de riesgos
categoria	aplica	=	=	op.pl.2	Arquitectura de seguridad
				op.acc	Control de acceso
AT	aplica	=	=	op.acc.1	Identificación
ICAT	aplica	=	=	op.acc.2	Requisitos de acceso
ICAT	n.a.	aplica	=	op.acc.3	Segregación de funciones y tareas
ICAT	aplica	=	=	op.acc.4	Proceso de gestión de derechos de acceso
ICAT	aplica	+	++	op.acc.5	Mecanismo de autenticación
ICAT	aplica	+	++	op.acc.6	Acceso local (local login)
ICAT	aplica	+	=	op.acc.7	Acceso remoto (remote login)

# Medidas de seguridad. Marco Operacional

Afectadas	Dimensiones			nn	MEDIDAS DE SEGURIDAD
	B	M	A		
					<b>Marco operacional</b>
				op.exp	Explotación
categoria	aplica	=	=	op.exp.1	Inventario de activos
categoria	aplica	=	=	op.exp.2	Configuración de seguridad
categoria	n.a.	aplica	=	op.exp.3	Gestión de la configuración
categoria	aplica	=	=	op.exp.4	Mantenimiento
categoria	n.a.	aplica	=	op.exp.5	Gestión de cambios
categoria	aplica	=	=	op.exp.6	Protección frente a código dañino
categoria	n.a.	aplica	=	op.exp.7	Gestión de incidencias
T	n.a.	n.a.	aplica	op.exp.8	Registro de la actividad de los usuarios
categoria	n.a.	aplica	=	op.exp.9	Registro de la gestión de incidencias
T	n.a.	n.a.	aplica	op.exp.10	Protección de los registros de actividad
categoria	aplica	=	+	op.exp.11	Protección de claves criptográficas
				op.ext	Servicios externos
categoria	n.a.	aplica	=	op.ext.1	Contratación y acuerdos de nivel de servicio
categoria	n.a.	aplica	=	op.ext.2	Gestión diaria
D	n.a.	n.a.	aplica	op.ext.9	Medios alternativos
				op.cont	Continuidad del servicio
D	n.a.	aplica	=	op.cont.1	Análisis de impacto
D	n.a.	n.a.	aplica	op.cont.2	Plan de continuidad
D	n.a.	n.a.	aplica	op.cont.3	Pruebas periódicas
				op.mon	Monitorización del sistema
categoria	n.a.	n.a.	aplica	op.mon.1	Detección de intrusión
categoria	n.a.	n.a.	aplica	op.mon.2	Sistema de métricas



## Medidas de seguridad. Medidas de protección

Afetadas	Dimensiones			MEDIDAS DE SEGURIDAD	
	R	M	A	mp	Medidas de protección
				mp.if	Protección de las instalaciones e infraestructuras
categoria	aplica	=	=	mp.if.1	Áreas separadas y con control de acceso
categoria	aplica	=	=	mp.if.2	Identificación de las personas
categoria	aplica	=	=	mp.if.3	Acondicionamiento de los locales
D	aplica	+	=	mp.if.4	Energía eléctrica
D	aplica	=	=	mp.if.5	Protección frente a incendios
D	n.a.	aplica	=	mp.if.6	Protección frente a inundaciones
categoria	aplica	=	=	mp.if.7	Registro de entrada y salida de equipamiento
D	n.a.	n.a.	aplica	mp.if.8	Instalaciones alternativas
				mp.per	Gestión del personal
categoria	n.a.	aplica	=	mp.per.1	Caracterización del puesto de trabajo
categoria	aplica	=	=	mp.per.2	Deberes y obligaciones
categoria	aplica	=	=	mp.per.3	Concienciación
categoria	aplica	=	=	mp.per.4	Formación
D	n.a.	n.a.	aplica	mp.per.8	Personal alternativo
				mp.eq	Protección de los equipos
categoria	aplica	+	=	mp.eq.1	Puesto de trabajo despejado
A	n.a.	aplica	+	mp.eq.2	Bloqueo de puesto de trabajo
categoria	aplica	=	+	mp.eq.3	Protección de equipos portátiles
D	n.a.	aplica	=	mp.eq.8	Medios alternativos

SIN CLASIFICAR



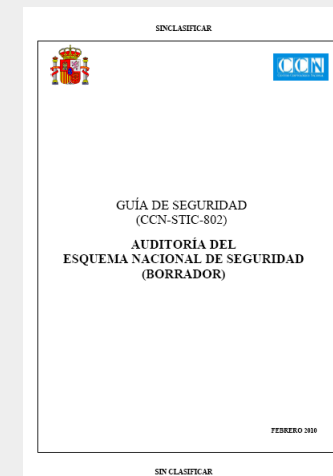
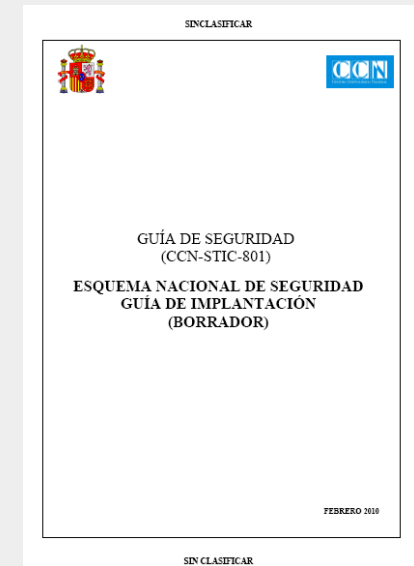
## Medidas de seguridad. Medidas de protección

Afectadas	Dimensiones				MEDIDAS DE SEGURIDAD
	B	M	A		
				mp.com	Protección de las comunicaciones
categoria	aplica	=	+	mp.com.1	Perimetro seguro
C	n.a.	aplica	+	mp.com.2	Protección de la confidencialidad
IA	aplica	+	++	mp.com.3	Protección de la autenticidad y de la integridad
categoria	n.a.	n.a.	aplica	mp.com.4	Segregación de redes
D	n.a.	n.a.	aplica	mp.com.9	Medios alternativos
				mp.si	Protección de los soportes de información
C	aplica	=	=	mp.si.1	Etiquetado
IC	n.a.	aplica	+	mp.si.2	Criptografía
categoria	aplica	=	=	mp.si.3	Custodia
categoria	aplica	=	=	mp.si.4	Transporte
C	n.a.	aplica	=	mp.si.5	Borrado y destrucción
				mp.sw	Protección de las aplicaciones informáticas
categoria	n.a.	aplica	=	mp.sw.1	Desarrollo
categoria	aplica	+	++	mp.sw.2	Aceptación y puesta en servicio
				mp.info	Protección de la información
categoria	aplica	=	=	mp.info.1	Datos de carácter personal
C	aplica	+	=	mp.info.2	Calificación de la información
C	n.a.	n.a.	aplica	mp.info.3	Cifrado
IA	aplica	+	++	mp.info.4	Firma electrónica
T	n.a.	n.a.	aplica	mp.info.5	Sellos de tiempo
C	aplica	=	=	mp.info.6	Limpieza de documentos
D	n.a.	aplica	=	mp.info.9	Copias de seguridad (backup)
				mp.s	Protección de los servicios
categoria	aplica	=	=	mp.s.1	Protección del correo electrónico
categoria	aplica	=	=	mp.s.2	Protección de servicios y aplicaciones web
D	n.a.	aplica	+	mp.s.8	Protección frente a la denegación de servicio
D	n.a.	n.a.	aplica	mp.s.9	Medios alternativos

## Herramientas cumplimiento ENS

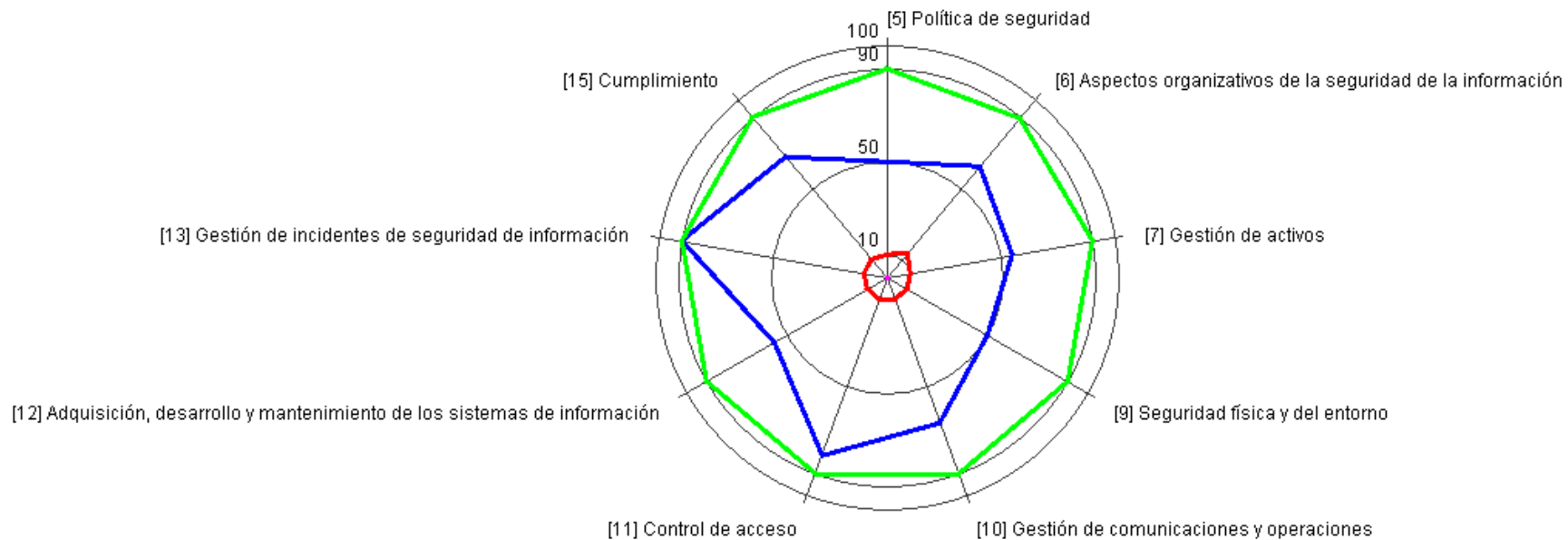
- Perfil de protección herramienta PILAR.
  - Adaptación de biblioteca
- CCN-STIC 801 Guía de implantación
  - Responsabilidades
  - Categorización
    - ♦ Criterios valoración información / servicios
  - Medidas de protección
    - ♦ Condición de aplicabilidad / Descripción
    - ♦ Referencias / Evidencias 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

SIN CLASIFICAR



# EVALUACIONES DE SEGURIDAD ... ISO 17799:2005

ejemplo: Evaluación de controles :: [17799\_2005] ISO/IEC 17799:2005



**SIN CLASIFICAR**

**Sin salvaguardas**

**Fase presente**

**Plan de Seguridad 3 meses**

**Plan de seguridad 1 año**



The screenshot shows the CCN-CERT website interface. At the top left is the CCN-CERT logo. The main header features the text "ccn-cert seguridad tic" and "capacidad de respuesta ante incidentes de seguridad de la información" next to a padlock image. On the right, there is a "NIVEL DE ALERTA BAJO" indicator and a language selection menu (Castellano, English, Català, Euskara, Galego, Valencià) with an "ABRIR SESIÓN" button.

**PRINCIPAL**

- SOBRE NOSOTROS
- INCIDENTES
- ACTUALIDAD CCN-CERT
- ALERTAS
- HERRAMIENTAS
- RECURSOS
- NOTICIAS
- PREFERENCIAS

**ÚLTIMAS VULNERABILIDADES**

- CCN-CERT-1004-05211  
Cross-Site Scripting en MoinMoin
- CCN-CERT-1004-05210  
Denegación de servicio en MIT Kerberos 5
- CCN-CERT-1004-05209  
Denegación de servicio en Linux kernel 2.6

**SERIES CCN-STIC**

- CCN-STIC-001  
Seguridad de las TIC en la Administración
- CCN-STIC-002  
Definición de Criptología Nacional
- CCN-STIC-401  
Glosario de términos

**NOTICIAS SEGURIDAD**

- Detenida una mujer que lavó 14.000 euros estafados a través de Internet - 15/04/2010
- Barcelona acoge la conferencia sobre seguridad Black Hat - 14/04/2010
- La CMT propone una nueva regulación para las AAPP que exploten redes y presten servicios de telecomunicaciones - 13/04/2010

**ÚLTIMOS INFORMES DE SEGURIDAD**

- CCN-CERT IA-02/10 - Extensiones de seguridad del sistema de nombres de dominio (dnssec)
- CCN-CERT ID-07/09 Informe de Código Dañino: Botnet Mariposa/Butterfly
- CCN-CERT IS-05/10 Informe de Actualidad STIC

**HERRAMIENTA PILAR**

Procedimiento Informático Lógico para el Análisis de Riesgos (Última versión)

**CURSOS CCN-STIC**

- VII Curso de Gestión STIC del 1 de marzo al 30 de abril
- V Curso Básico STIC - Entornos Windows del 19 al 23 de abril
- VII Curso Acreditación STIC - Entornos Windows del 26 al 30 de abril

**COMUNICADOS CCN-CERT**

- El Esquema Nacional de Evaluación y Certificación del CCN se incorpora al acuerdo europeo SOGIS MRA v3. - 31/03/2010
- La coordinación nacional e internacional y la respuesta a incidentes funciones del CCN fijadas en el nuevo Esquema Nacional - 26/02/2010
- El CCN, en colaboración con la Xunta de Galicia, presenta en Santiago su Servicio de Respuesta a Incidentes - 30/12/2009

**DESTACADO**

- Servicios S.A.T. CCN-CERT Sistema de Alerta Temprana
- Esquema Nacional de Seguridad

**MENCIONES**

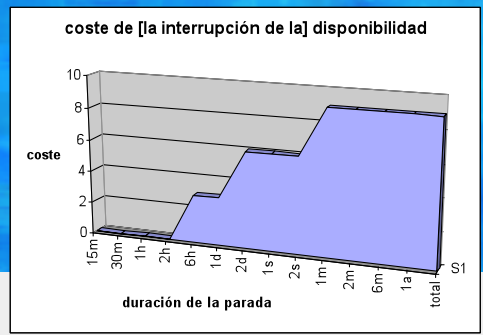
- FIRST Accredited by TRUSTED Introduce The European CSIRT Directory
- EGC group

**AVISO LEGAL - CONTACTO - MAPA WEB - DECLARACIÓN DE ACCESIBILIDAD**  
© 2010 Centro Criptológico Nacional - CI/Argenta s/n 28023 MADRID

- 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



# Análisis de Impacto y Continuidad de Negocio



BCM: [ejemplo] Unidad administrativa - AGENCIA

Proyecto Edita Nivel Ayuda



## Análisis cualitativo

- ☐ D. Proyecto
  - ☐ D.0. Datos del proyecto
  - ☐ D.1. Fuentes de información
  - ☐ D.2. Escalones de interrupción
  - ☐ D.3. Subconjunto de amenazas
  - ☐ D.4. Modelado de las amenazas
- ☐ A. Análisis de riesgos
  - ☐ A. Análisis de riesgos
  - ☐ A.2. Amenazas
  - ☐ A.3. Impacto y riesgo
- ☐ T. Tratamiento de los riesgos
  - ☐ T.1. Fases del proyecto
  - ☐ T.B. Equipamiento de respaldo
- ☐ S. Salvaguardas
  - ☐ S.0. identificación
  - ☐ S.1. valoración
  - ☐ S.1+. específicas de activos
- ☐ Impacto y riesgo residuales
  - ☐ Plan de recuperación de desastres
- ☐ R. Informes
  - ☐ R.r. textuales
    - ☐ Modelo de valor (corto)
    - ☐ Modelo de valor (largo)
    - ☐ Informe de amenazas
    - ☐ Evaluación de las salvaguardas
    - ☐ Informe de insuficiencias
    - ☐ Análisis de impacto
    - ☐ Estado de riesgo
  - ☐ R.g. gráficas



activo	now	3m	1y
☐ [FS] Funciones del sistema de información			
☐ [S_T_presencial] Tramitación presencial			
☐ [S_T_remota] Tramitación remota			
☐ [D_exp] Expedientes en curso			[1d]
☐ [SI] Servicios internos			
☐ [email] Mensajería electrónica			
☐ [archivo] Archivo histórico central			
☐ [E] Equipamiento			
☐ [sw] [SW_exp] Tramitación de expedientes			
☐ [hw] [PC] Puestos de trabajo	[1d]	[1d]	[20m]
☐ [SRV] Servidor			
☐ [network] [firewall] Cortafuegos			
☐ [LAN] Red local			
☐ [ADSL] Conexión a Internet			
☐ [L] Instalaciones			
☐ [oficinas] Oficinas			
☐ [cpd] Sala de equipos			

[hw.PC] Puestos de trabajo :: [3m] plan de remedios urgentes: a 3 meses

escalón de interrupción

comentario

- ☐ equipamiento de respaldo
  - ☐ [S] Servicios (S)
  - ☐ [D] Datos / Información (D)
  - ☐ [SW] Aplicaciones informáticas (SW)
  - ☐ [HW] Equipos (HW)
    - ☐ [HW.prp] Equipo alternativo propio
      - ☐ [HW.prp.cluster] arquitectura redundante (always on)
      - ☐ [HW.prp.stored] dedicado (almacenado)
      - ☐ [HW.prp.stolen] en otras funciones: desarrollo, etc.
    - ☐ [HW.cont] Equipo alternativo contratado
    - ☐ [HW.agreed] Equipo alternativo acordado
    - ☐ [HW.sla\_new] Acuerdo de reposición (SLA)
    - ☐ [HW.sla\_old] Acuerdo de reparación (SLA)
    - ☐ [HW.prov] Proveedor preferente
  - ☐ [COM] Redes de comunicaciones (COM)

# Planes de Continuidad de Negocio / Recuperación

## - Funcionalidades

1. modelar el coste de la interrupción del servicio
2. identifica elementos críticos
3. permite incorporar equipamiento de respaldo
4. permite calificar las salvaguardas
5. permite estimar el impacto y riesgo residuales
6. permite diseñar un plan de recuperación

activo	comentario	[0s]	[15m]	[1h]	[4h]	[1d]	[2d]	[7d]
		[0]	[3]	[5]	[5]	[5]	[7]	[7]
		[0]	[3]	[3]	[3]	[4]	[5]	[7]
<b>ACTIVOS</b>								
☞ [FS] Funciones del sistema de información								
A [S_T_presencial] Tramitación presencial			listo					
A [S_T_remota] Tramitación remota			objetivo					
A [D_exp] Expedientes en curso			requerido			objetivo		
☞ [SI] Servicios internos								
A [email] Mensajería electrónica			requerido					
A [archivo] Archivo histórico central			requerido			requerido		
☞ [E] Equipamiento								
☞ [sw]								
A [SW_exp] Tramitación de expedientes			requerido			requerido		
☞ [hw]								
A [PC] Puestos de trabajo			requerido		objetivo	requerido		
A [SRV] Servidor			requerido			requerido		
☞ [network]								
A [firewall] Cortafuegos			requerido			requerido		
A [LAN] Red local			requerido			requerido		
A [ADSL] Conexión a Internet			requerido			requerido		
☞ [L] Instalaciones								
A [oficinas] Oficinas			requerido		requerido	requerido		
A [cpd] Sala de equipos			requerido			requerido		

Gracias

SIN CLASIFICAR



**CCN CERT** seguridad de capacidad de respuesta ante incidentes de seguridad de la información

**CERTIFICACIÓN CRIPTOLÓGICA**  
Productos capaces de proteger la información clasificada Nacional

**CERTIFICACIÓN TEMPEST**  
Equipos y sistemas protegidos frente a las emisiones electromagnéticas.

**CERTIFICACIÓN FUNCIONAL**  
En base a criterios establecidos y reconocidos como estándar internacional (CC)

**CENTRO Criptológico NACIONAL**

Inicio Normas Certificación Acreditación Formación Gestión de Incidentes

**SERIES CCN-STIC**

- Serie 000 Políticas
- Serie 100 Procedimientos STIC
- Serie 200 Normas STIC
- Serie 300 Instrucciones Técnicas STIC
- Serie 400 Guías Generales
- Serie 500 Guías entornos Windows
- Serie 600 Guías otros entornos
- Serie 900 Informes Técnicos

**CURSOS CCN-STIC**

El Centro Criptológico Nacional tiene la potestad de formar al personal de la Administración especialista en el campo de la seguridad de las Tecnologías de la Información. Por este motivo, anualmente, el CCN oferta a todo el personal de las administraciones públicas diversos cursos, presenciales y a distancia, englobados en cuatro categorías:

- Cursos Informativos y de Concienciación en Seguridad
- Cursos básicos de seguridad
- Cursos específicos de gestión de seguridad
- Cursos de especialización en seguridad

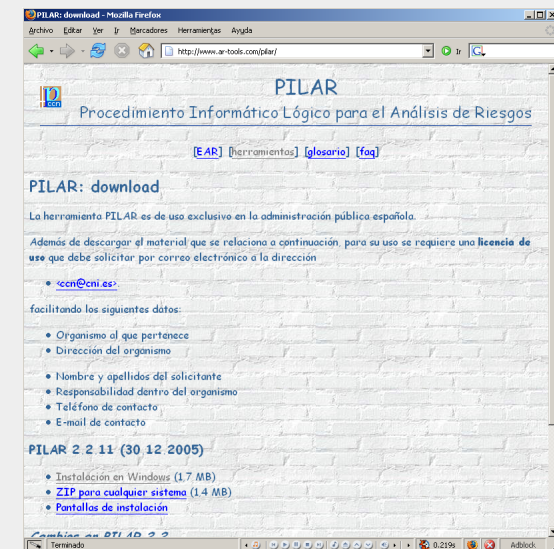
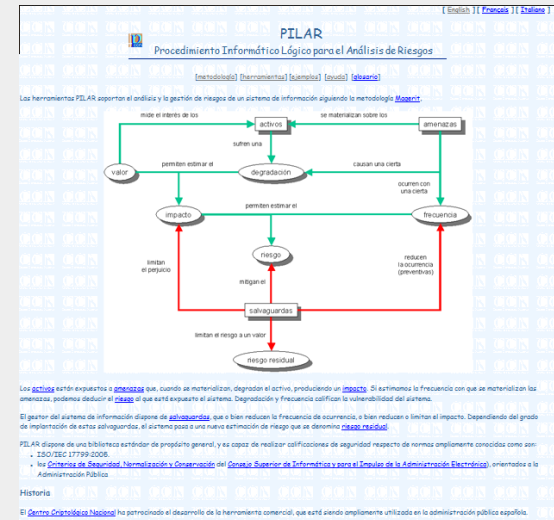
Copyright © 2009 Centro Criptológico Nacional. Todos los derechos reservados. C/Argentina s/n 28023 MADRID

AVISO LEGAL | CONTACTAR | MAPA WEB

## MAS INFORMACION

- <http://www.ccn.cni.es>
- Consulta sobre la herramienta
  - [formacion.ccn@cni.es](mailto:formacion.ccn@cni.es)
    - ◆ **Distribuciones de PILAR**
- Descarga de la herramienta CCN
  - [www.ccn-cert.cni.es](http://www.ccn-cert.cni.es)
    - ◆ **Publica: 4.4.2**
    - ◆ **Privada:**
      - 4.4.3
      - Actualizaciones
      - Perfil
  - **Solicitud de cursos**
  - [formacion.ccn@cni.es](mailto:formacion.ccn@cni.es)
- Entrega de licencia
  - [ccn@cni.es](mailto:ccn@cni.es)

SIN CLASIFICAR





# SERVICIOS DE INFORMACIÓN - BOLETINES

- Boletín de Noticias de Seguridad
- Boletines de Alertas - Sección Pública
- Boletines Restringidos - Sección Privada



PREFERENCIAS
DETALLES DE USUARIO
ASOCIAR DNIE A CUENTA
SUSCRIPCIÓN A BOLETINES
SUSCRIPCIÓN A LISTAS

RESUMEN DE LAS ÚLTIMAS 20 VULNERABILIDADES 

Riesgo	Identificador	Título	Fecha
Medio	CCN-CERT-907-04718	Denegación de servicio en Linux kernel	10-11-2009

<b>Palabras clave</b> <input type="text"/> <input checked="" type="radio"/> todas las palabras <input type="radio"/> algunas de las palabras <input type="radio"/> frase exacta	<b>Plataforma</b> <input checked="" type="checkbox"/> Todas <input checked="" type="checkbox"/> Microsoft <input checked="" type="checkbox"/> Linux <input checked="" type="checkbox"/> Unix <input checked="" type="checkbox"/> Red <input checked="" type="checkbox"/> Software comercial <input checked="" type="checkbox"/> Software exótico <input checked="" type="checkbox"/> Otros	<b>Riesgo/Criticidad</b> <input checked="" type="checkbox"/> Todos <input checked="" type="checkbox"/> Bajo <input checked="" type="checkbox"/> Medio <input checked="" type="checkbox"/> Alto <input checked="" type="checkbox"/> Muy alto
---	--	--

Fecha desde    
 Fecha hasta  

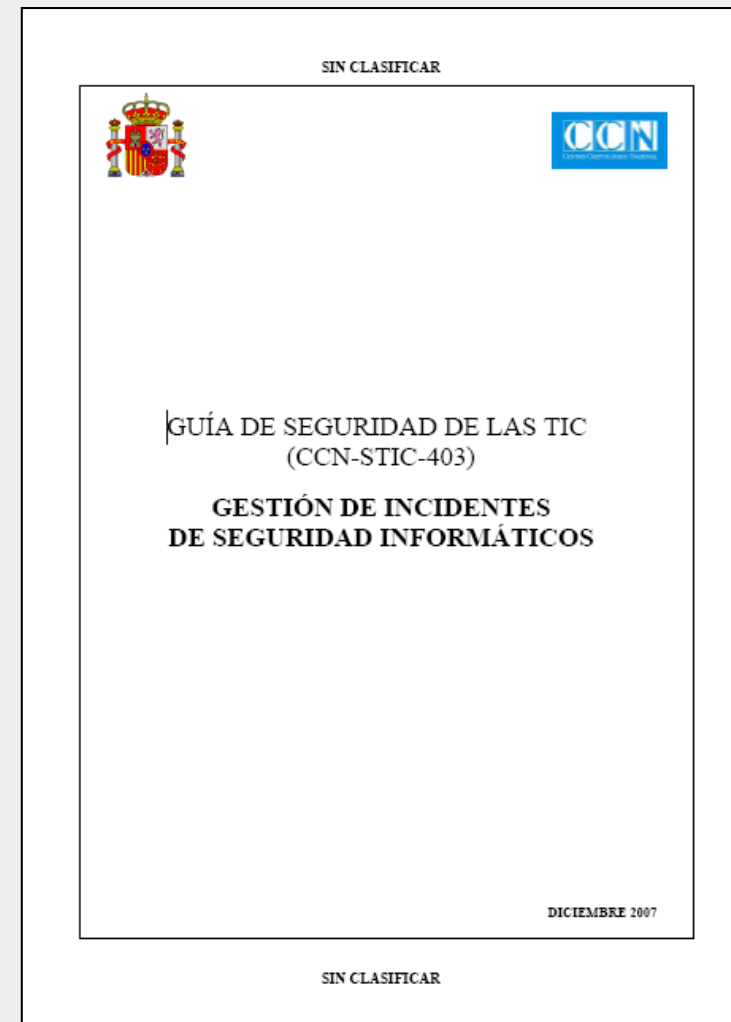
[Ayuda](#) [Buscar](#)

Medio	CCN-CERT-812-04391	Múltiples vulnerabilidades en Moodle	3-11-2009
Medio	CCN-CERT-907-04747	Múltiples vulnerabilidades en Apache2	3-11-2009
Medio	CCN-CERT-908-04802	Ejecución remota de código en Apache Portable Runtime	3-11-2009
Medio	CCN-CERT-909-04873	Cross-Site Scripting en Ruby on Rails	3-11-2009
Medio	CCN-CERT-909-04884	Desbordamiento de búfer en Newt	3-11-2009
Bajo	CCN-CERT-910-04901	Múltiples vulnerabilidades en PostgreSQL	3-11-2009
Bajo	CCN-CERT-910-04908	Múltiples vulnerabilidades en Samba	3-11-2009

## CCN-STIC 403: Gestión de Incidentes Informáticos

- Otros foros CERTs / CSIRTs
- Qué esperar de un CERT
- Respuesta a Incidentes - Check Lists:
  - Caso General
  - Intentos de Intrusión
  - Ataque con Malware
  - Phishing
  - Ataque DDOS
- Contactar con FCSE

SIN CLASIFICAR





- **Informes de Amenazas STIC**
  - ◆ Seguridad en la nube (“Cloud computing”)
  - ◆ Seguridad Móvil
  - ◆ DNSSec
  - ◆ Amenazas y vulnerabilidades 2009. Tendencias 2010, etc...
- **Informes de Actualidad STIC**
  - ◆ Noticias STIC
  - ◆ Artículos sobre Ciberseguridad
  - ◆ Estado del Hack
- **Informes de Código Dañino**
  - ◆ Troyanos:
    - KoobFace, Capircinius, Gumblar, Beladen,
    - Zeus, Waledac, Butterfly bot, etc
  - ◆ Caso práctico de análisis forense.

RECURSOS
CURSOS STIC 2009 - LISTA
CURSOS STIC 2009
CURSOS STIC 2008
CURSO ON-LINE
ENLACES DE INTERÉS
PRESENTACIÓN EN CLM
I JORNADA STIC CCN-CERT
II JORNADA STIC CCN-CERT
III JORNADA STIC CCN-CERT
9 NATO WORKSHOP
PUBLICACIONES
INFORMES DE AMENAZAS
INFORMES DE ACTUALIDAD
INFORMES CÓDIGO DAÑINO

## Gestión de Incidentes

- Incidentes prioritarios para CCN-CERT



### **Incidentes prioritarios para CCN-CERT**

Priority incident for the CCN-CERT

- » Incidentes que afecten a información «clasificada»  
» [Activities that affect "classified" information](#)
- » Ataques contra infraestructuras de Internet de las administraciones públicas  
» [Attacks against Public Administration's Internet infrastructures](#)
- » Ataques distribuidos y automáticos contra sitios de Internet  
» [Distributed and automatic attacks against Internet sites](#)
- » Nuevos tipos de ataques o nuevas vulnerabilidades  
» [New types of attacks or new vulnerabilities](#)
- » Ataque con código dañino  
» [Attack with malicious code](#)
- » Análisis Forense de equipos comprometidos  
» [Forensic analysis of compromised machine](#)
- » Ataque a Sistemas CIS de Infraestructuras Críticas  
» [Attacks against Critical Infrastructures Systems](#)