CCN
CENTRO CRIPTOLÓGICO NACIONAL

HERRAMIENTA PILAR
ESQUEMA NACIONAL DE SEGURIDAD

Madrid, Abril de 2010

SIN CLASIFICAR

Presentación

- 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 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica

Comisión Delegada del Gobierno para asuntos de Inteligencia. Define los objetivos del CNI.

SIN CLASIFICAR

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.

BOLETÍN OFICIAL DEL ESTADO
Núm. 25 Viernes 29 de enero de 2010 Sec. I. Pág. 8089

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.

RD 3/2010 CCN-CERT

BOLETÍN OFICIAL DEL ESTADO
Núm. 25 Viernes 29 de enero de 2010 Sec. I. Pág. 8089

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:

RD 3/2010

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.

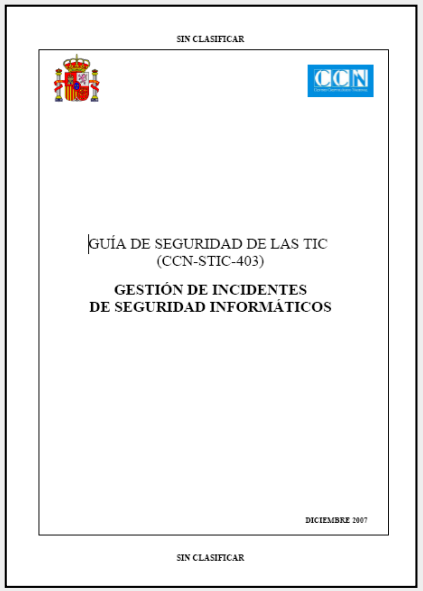
c**) Formación** destinada al personal de la Administración especialista en el campo de la seguridad de las tecnologías de la información, al objeto de facilitar la actualización de conocimientos del personal de la Administración y de lograr la sensibilización y mejora de sus capacidades para la detección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


SIN CLASIFICAR

GUÍA DE SEGURIDAD DE LAS TIC
(CCN-STIC-403)

GESTIÓN DE INCIDENTES
DE SEGURIDAD INFORMÁTICOS

DICIEMBRE 2007

SIN CLASIFICAR

- CCN-STIC 000: Instrucciones/Políticas STIC
- CCN-STIC 100: Procedimientos
- CCN-STIC 200: Normas
- CCN-STIC 300: Instrucc
- CCN-STIC 400: Guías G
- CCN-STIC 500: Guías E
- CCN-STIC 600: Guías C
- CCN-STIC 800: Guías d
- CCN-STIC 900: Informes

Datos a 31 de diciembre de 2009:

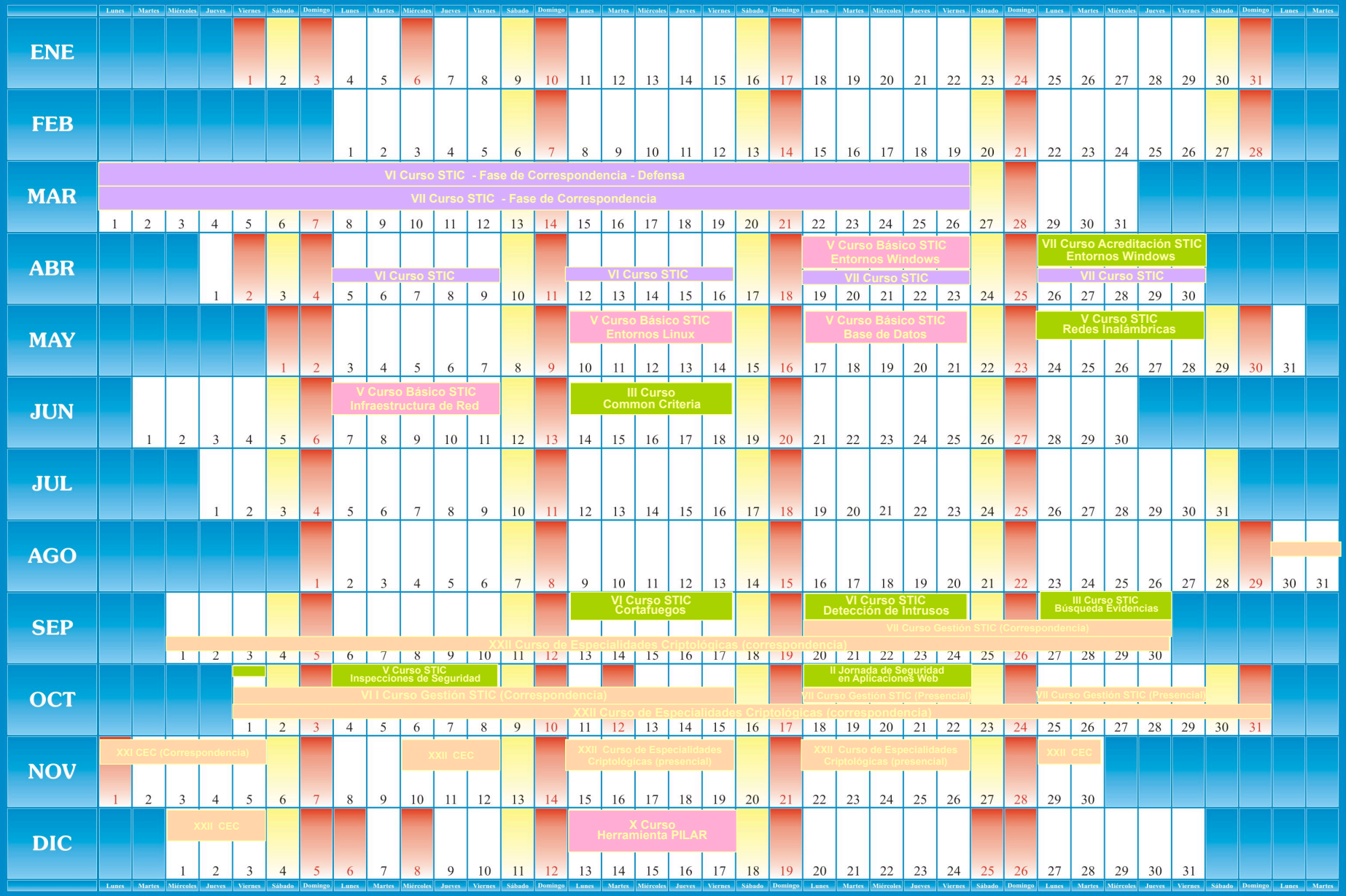
- 124 documentos pdf, 11600 páginas, 88 Mbyte

SIN CLASIFICAR

FORMACIÓN

CCN Centro Criptológico Nacional

Centro Criptológico Nacional 2010

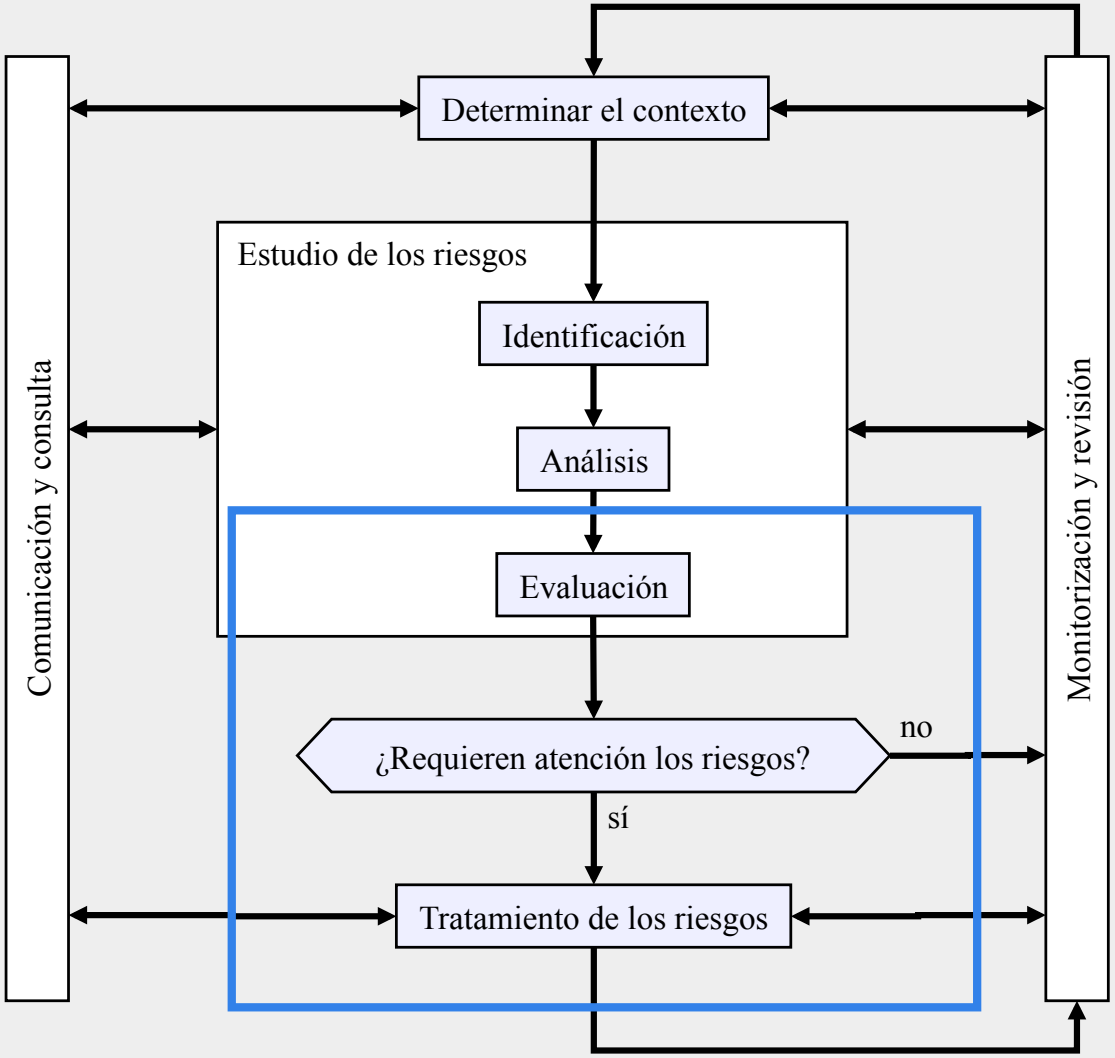


CCN-CERT …. www.ccn-cert.cni.es

En febrero 2100 usuarios registrados

SIN CLASIFICAR

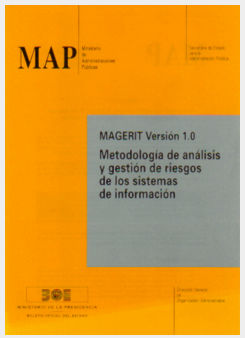
Gestión de riesgos 27005



MAGERIT

- METODOLOGIA DE ANALISIS Y GESTION DE RIESGOS DE LOS SISTEMAS DE INFORMACION DE LAS ADMINISTRACIONES PUBLICAS

AÑO 1997



MAGERIT V2

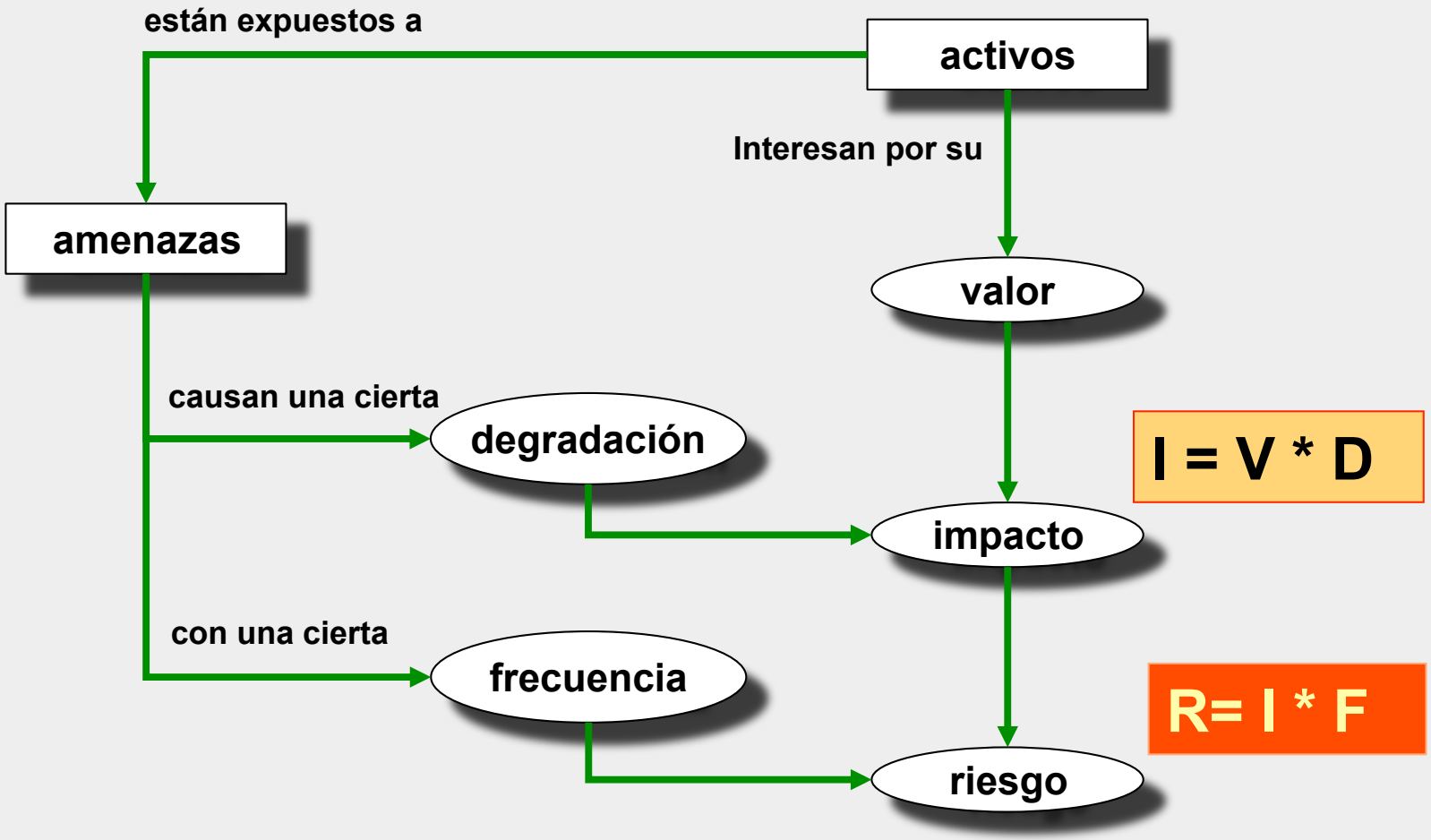
- Metodología de Análisis y gestión Riesgos S.I.
  - 16.06.2005 ….. 158 páginas
- Catálogo de elementos
  - 83 páginas
    - Tipos de activos
    - Dimensiones valoración
    - Criterios de valoración
    - Amenazas
    - Salvaguardas
- Libro de técnicas
  - 73 páginas

AÑO 2004

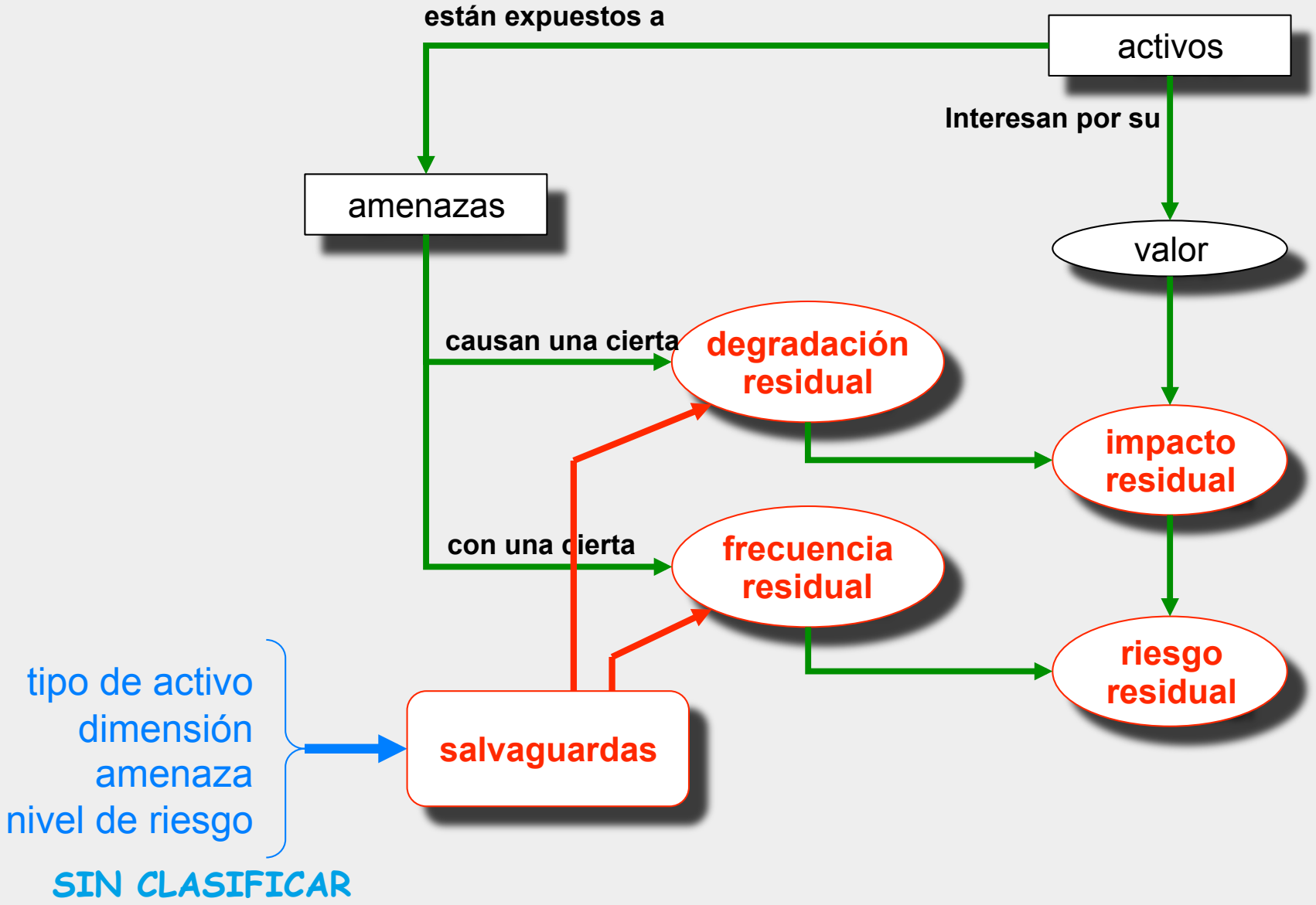
MAP, versión 2 (1.1 junio de 2006)

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

Magerit : Análisis de Riesgo



Magerit : Gestión de Riesgo



Evaluación de salvaguardas

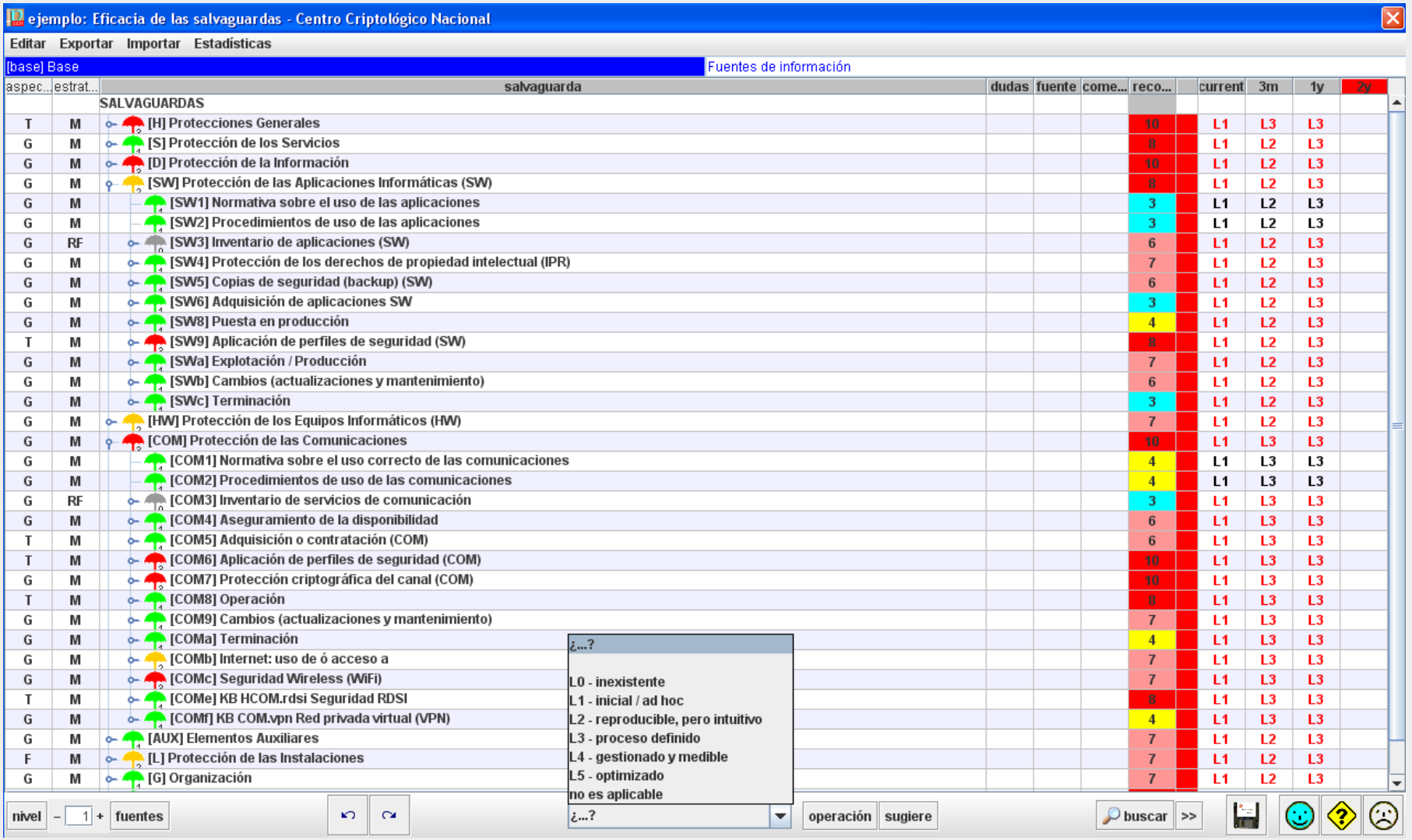
- Estimación de su eficacia:
  - NA : no aplica
  - 0% L0 inexistente
  - 10% L1 inicial / ad hoc
  - 50% L2 reproducible, pero intuitivo
  - 90% L3 proceso definido
  - 95% L4 gestionado y medible
  - 100% L5 optimizado

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**

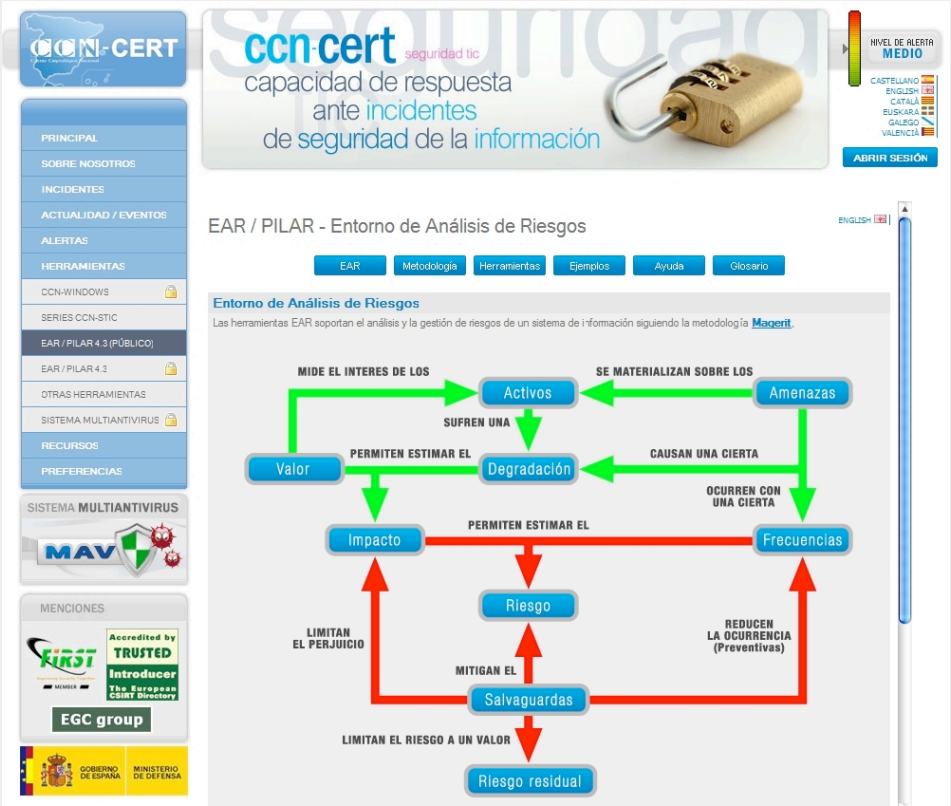
- **COSTE..... *N / B / M / A***

SALVAGUARDAS



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

EAR-PILAR



- 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

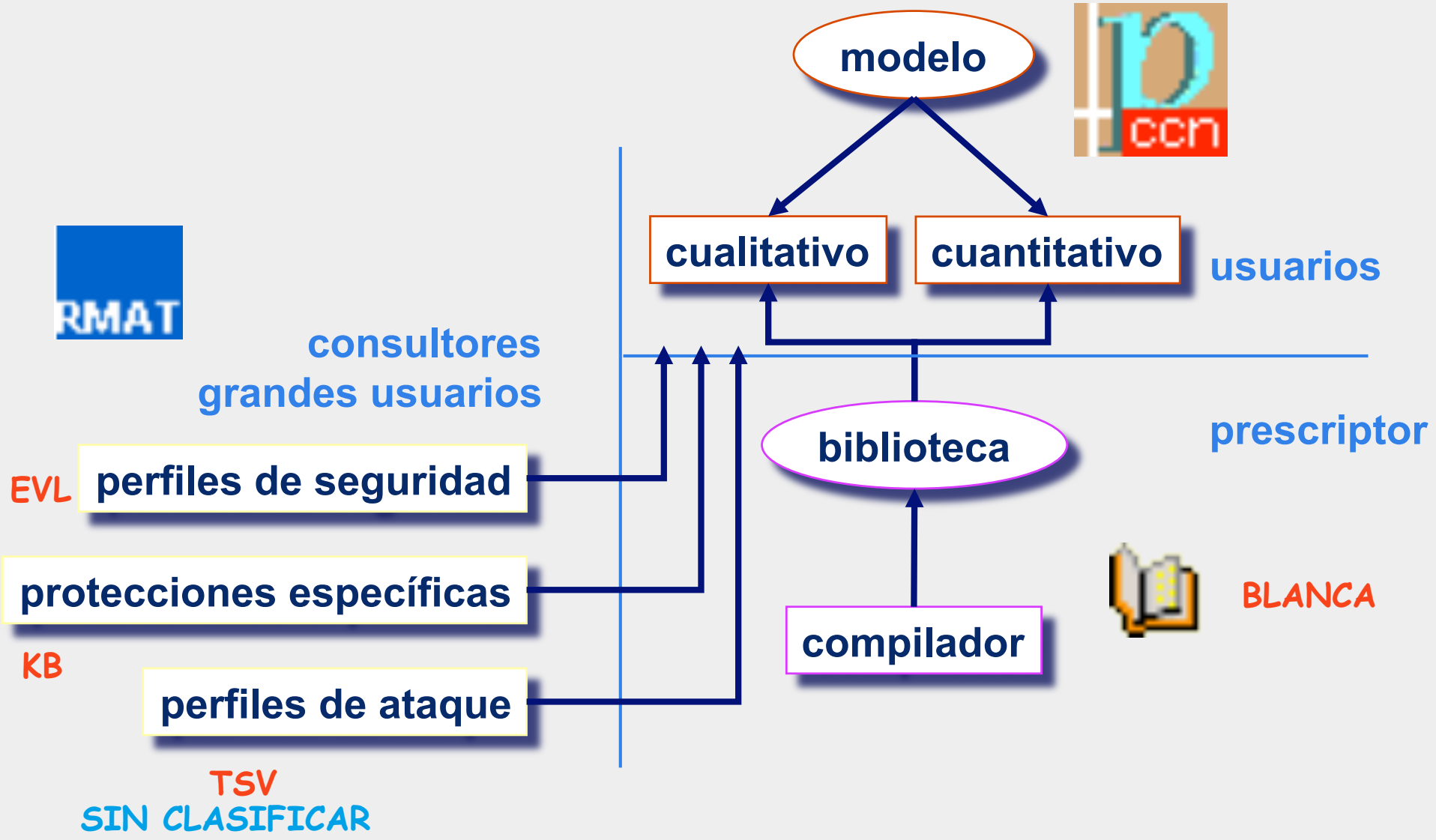
- **OBJETIVO PILAR:**
  - **FACILIDAD DE USO.**
  - **FLEXIBILIDAD.**
  - **Adaptarse a las políticas:**
    - **NACIONAL / EMPRESAS**
    - **OTAN / UE**
  - **PRIORIZACIÓN SALVAGUARDAS.**

  - **ANALISIS DINÁMICOS / DISTRIBUIDOS**
  - **INFRAESTRUCTURAS CRÍTICAS**
  - **APOYO ENS**

- Multilenguaje (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

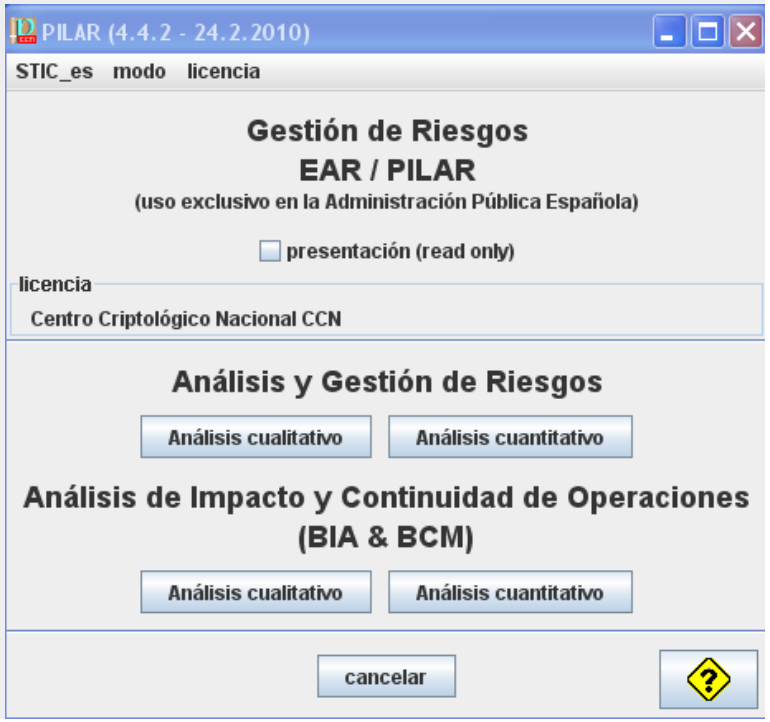
  TSV: threat profiles

  KB: protecciones adicionales por activo

- Creación de nuevas bibliotecas

  BLANCA: compilador de bibliotecas

  (no se distribuye)



SIN CLASIFICAR

Marzo 2010 Herramientas de usuario final

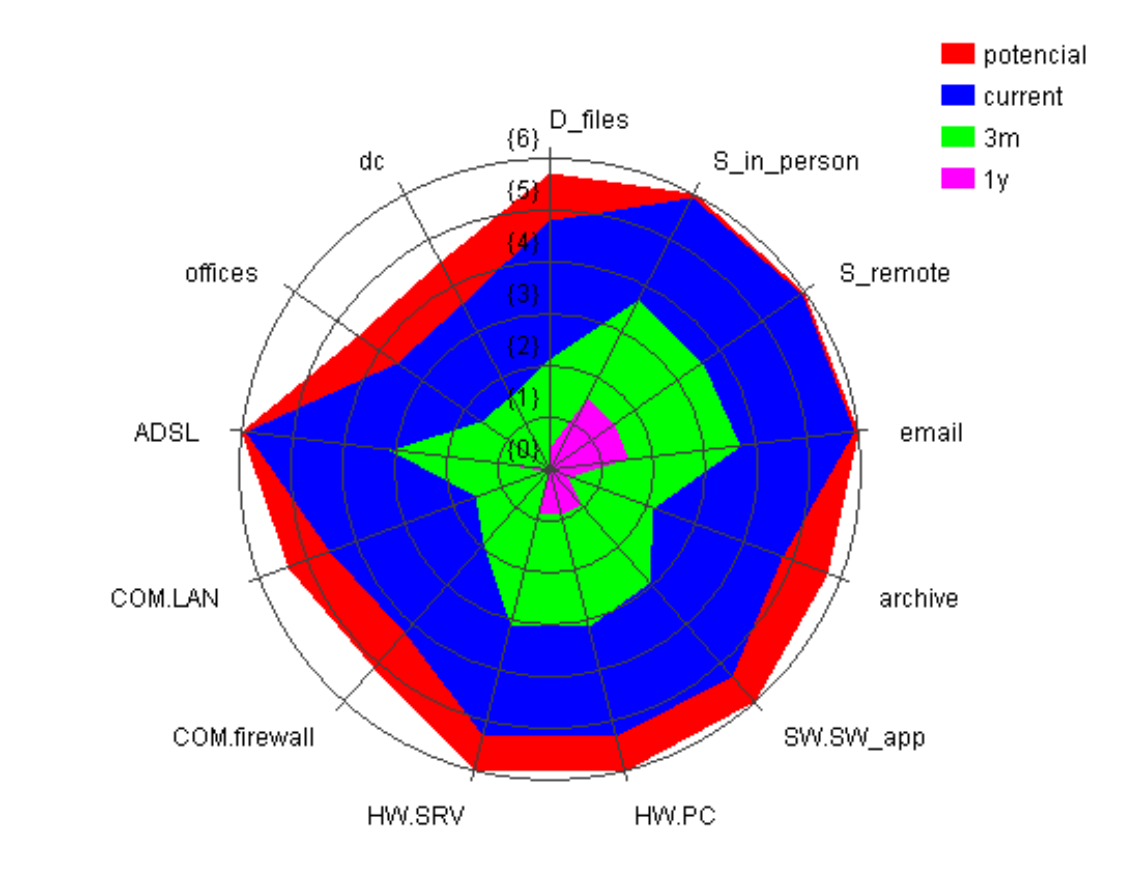
Nivel | Ayuda
básico
medio
experto

- 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

INFORMES GRAFICOS. Riesgo Residual

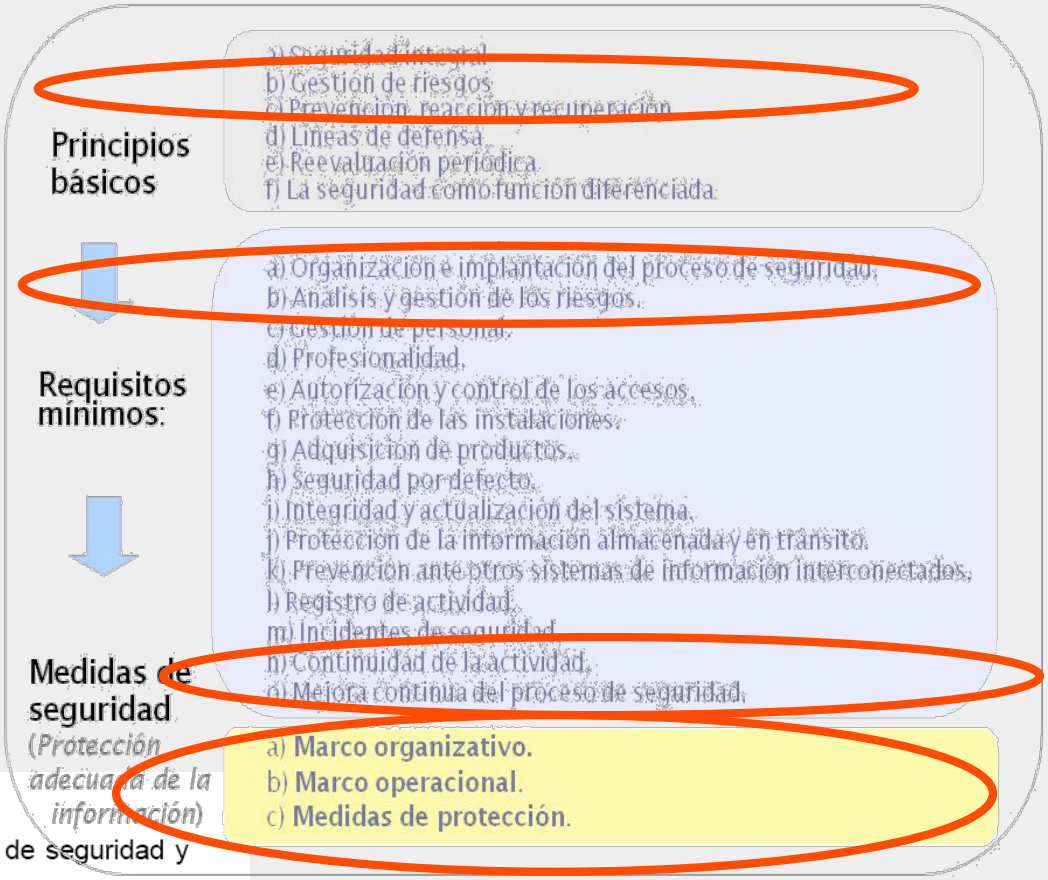


Reducción del Riesgo

- Sin salvaguardas
- Fase presente
- Plan de Seguridad 3 meses
- Plan de seguridad 1 año

SIN CLASIFICAR

PILAR-ENS



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.

SIN CLASIFICAR

Medidas de seguridad. Marco organizativo / OPERACIONAL

Dimensiones Afectadas	B	M	A	MEDIDAS DE SEGURIDAD	
				org	**Marco organizativo**
categoría	aplica	=	=	org.1	Política de seguridad
categoría	aplica	=	=	org.2	Normativa de seguridad
categoría	aplica	=	=	org.3	Procedimientos de seguridad
categoría	aplica	=	=	org.4	Proceso de autorización
				op	**Marco operacional**
				op.pl	Planificación
categoría	n.a.	+	++	op.pl.1	Análisis de riesgos
categoría	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 logon)
ICAT	aplica	+	=	op.acc.7	Acceso remoto (remote login)

SIN CLASIFICAR

Medidas de seguridad. Marco Operacional

Dimensiones Afectadas	B	M	A	MEDIDAS DE SEGURIDAD op	Marco operacional
				op.exp	Explotación
categoría	aplica	=	=	op.exp.1	Inventario de activos
categoría	aplica	=	=	op.exp.2	Configuración de seguridad
categoría	n.a.	aplica	=	op.exp.3	Gestión de la configuración
categoría	aplica	=	=	op.exp.4	Mantenimiento
categoría	n.a.	aplica	=	op.exp.5	Gestión de cambios
categoría	aplica	=	=	op.exp.6	Protección frente a código dañino
categoría	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
categoría	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
categoría	aplica	=	+	op.exp.11	Protección de claves criptográficas
				op.ext	Servicios externos
categoría	n.a.	aplica	=	op.ext.1	Contratación y acuerdos de nivel de servicio
categoría	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
categoría	n.a.	n.a.	aplica	op.mon.1	Detección de intrusión
categoría	n.a.	n.a.	aplica	op.mon.2	Sistema de métricas

SIN CLASIFICAR

Medidas de seguridad. Medidas de protección

Dimensiones Afectadas	B	M	A	MEDIDAS DE SEGURIDAD mp	Medidas de protección
				mp.if	Protección de las instalaciones e infraestructuras
categoría	aplica	=	=	mp.if.1	Áreas separadas y con control de acceso
categoría	aplica	=	=	mp.if.2	Identificación de las personas
categoría	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
categoría	aplica	=	=	mp.if.7	Registro de entrada y salida de equipamiento
D	n.a.	n.a.	aplica	mp.if.9	Instalaciones alternativas
				mp.per	Gestión del personal
categoría	n.a.	aplica	=	mp.per.1	Caracterización del puesto de trabajo
categoría	aplica	=	=	mp.per.2	Deberes y obligaciones
categoría	aplica	=	=	mp.per.3	Concienciación
categoría	aplica	=	=	mp.per.4	Formación
D	n.a.	n.a.	aplica	mp.per.9	Personal alternativo
				mp.eq	Protección de los equipos
categoría	aplica	+	=	mp.eq.1	Puesto de trabajo despejado
A	n.a.	aplica	+	mp.eq.2	Bloqueo de puesto de trabajo
categoría	aplica	=	+	mp.eq.3	Protección de equipos portátiles
D	n.a.	aplica	=	mp.eq.9	Medios alternativos

SIN CLASIFICAR

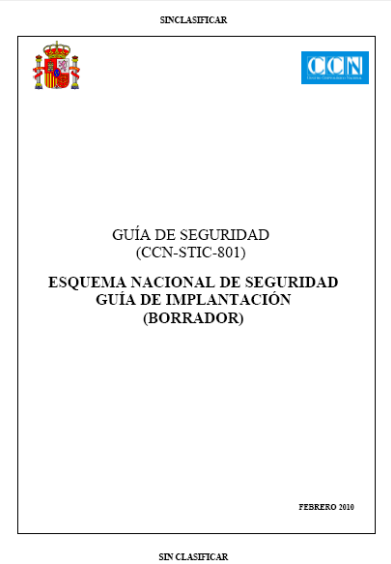
Medidas de seguridad. Medidas de protección

Dimensiones Afectadas	B	M	A		MEDIDAS DE SEGURIDAD
				mp.com	Protección de las comunicaciones
categoría	aplica	=	+	mp.com.1	Perímetro seguro
C	n.a.	aplica	+	mp.com.2	Protección de la confidencialidad
I A	aplica	+	++	mp.com.3	Protección de la autenticidad y de la integridad
categoría	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
I C	n.a.	aplica	+	mp.si.2	Criptografía
categoría	aplica	=	=	mp.si.3	Custodia
categoría	aplica	=	=	mp.si.4	Transporte
C	n.a.	aplica	=	mp.si.5	Borrado y destrucción
				mp.sw	Protección de las aplicaciones informáticas
categoría	n.a.	aplica	=	mp.sw.1	Desarrollo
categoría	aplica	+	++	mp.sw.2	Aceptación y puesta en servicio
				mp.info	Protección de la información
categoría	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
I A	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
categoría	aplica	=	=	mp.s.1	Protección del correo electrónico
categoría	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

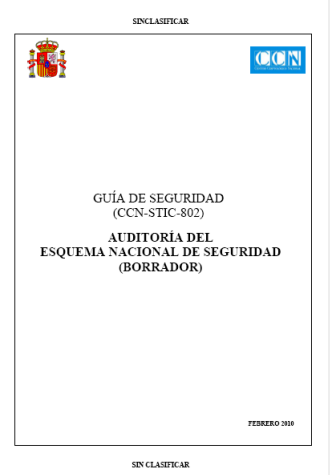

SINCLASIFICAR

GUÍA DE SEGURIDAD
(CCN-STIC-801)

ESQUEMA NACIONAL DE SEGURIDAD
GUÍA DE IMPLANTACIÓN
(BORRADOR)

FEBRERO 2010

SIN CLASIFICAR


SINCLASIFICAR

GUÍA DE SEGURIDAD
(CCN-STIC-802)

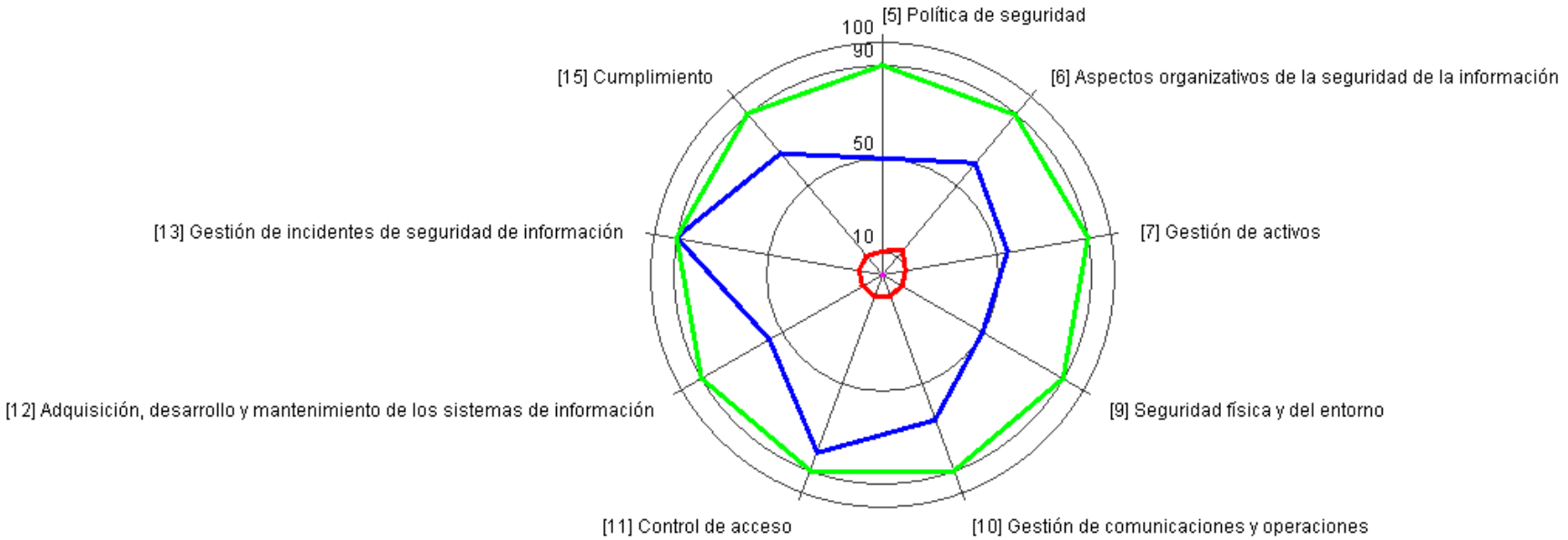
AUDITORÍA DEL
ESQUEMA NACIONAL DE SEGURIDAD
(BORRADOR)

FEBRERO 2010

SIN CLASIFICAR

EVALUACIONES DE SEGURIDAD … ISO 17799:2005

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



Sin salvaguardas

Fase presente

Plan de Seguridad 3 meses

Plan de seguridad 1 año

SIN CLASIFICAR

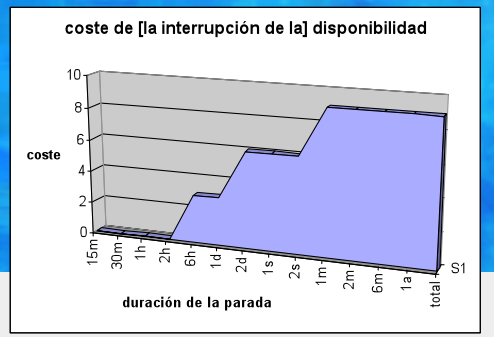
Espacio ENS en www.ccn-cert.cni.es

SIN CLASIFICAR

PILAR | EAR - 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

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

[example] Administration unit: Service interruption steps - CENTRO CRI...

SERVICE INTERRUPTION STEPS

- [15m]
- [1h]
- [4h]
- [1d]
- [2d]
- [7d]

ejemplo: Equipamiento de respaldo - AGENCIA DE PROTECCION DE DATOS

activo	now	3m	1y
ACTIVOS			
[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)

SIN

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

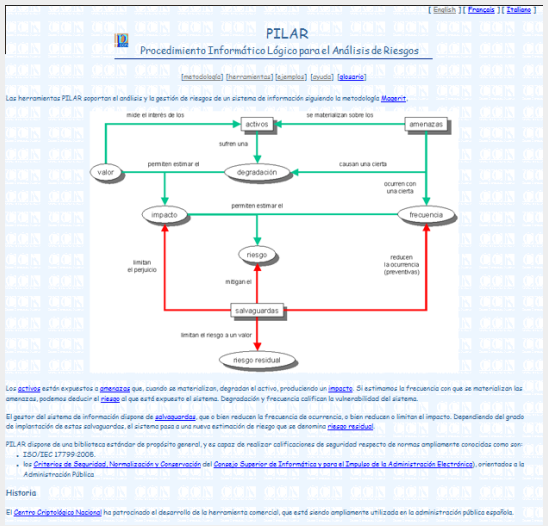
CENTRO CRIPTOLÓGICO NACIONAL

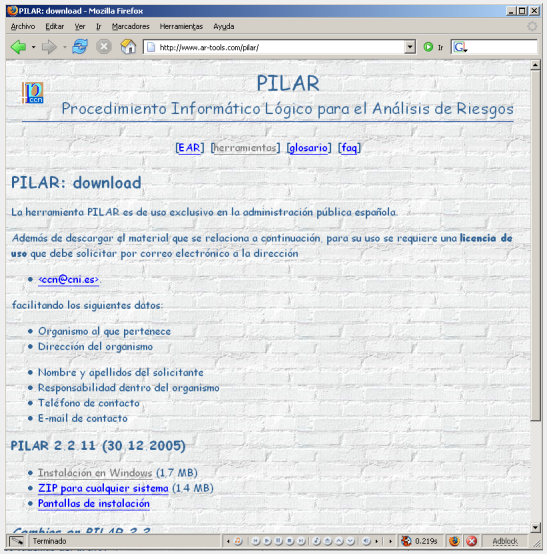
Gracias

SIN CLASIFICAR

MAS INFORMACION

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





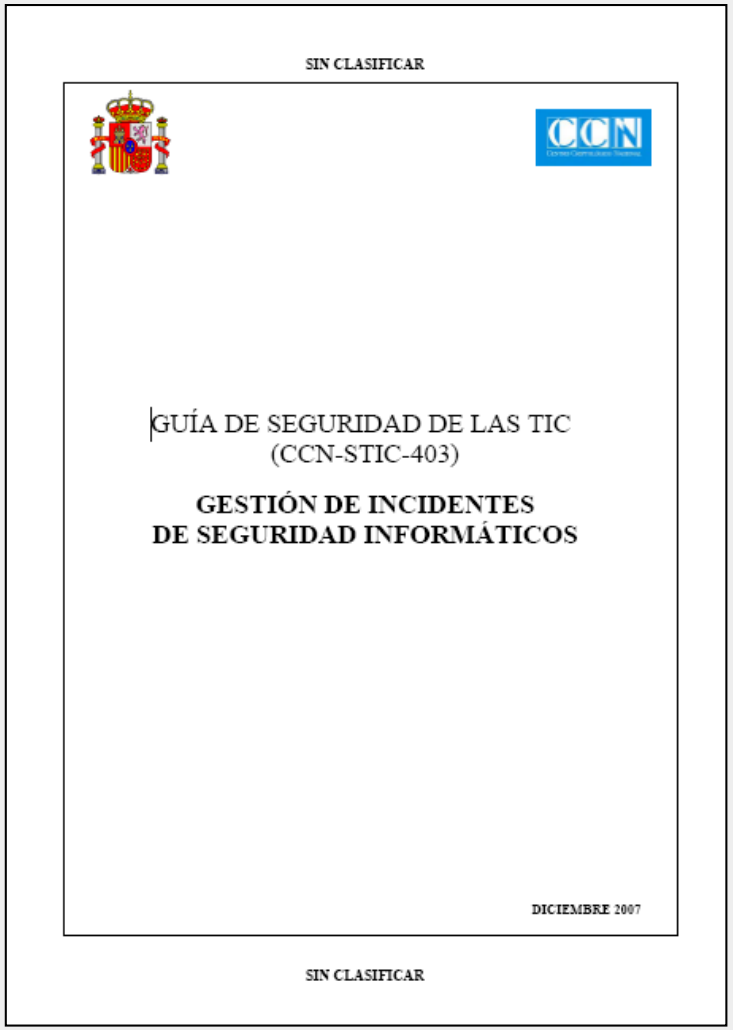
SIN CLASIFICAR

SERVICIOS DE INFORMACIÓN - BOLETINES

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

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

GUÍA DE SEGURIDAD DE LAS TIC
(CCN-STIC-403)

GESTIÓN DE INCIDENTES
DE SEGURIDAD INFORMÁTICOS

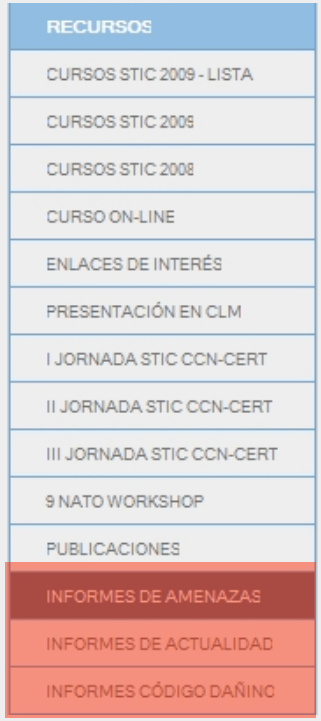
DICIEMBRE 2007

SIN CLASIFICAR

SIN CLASIFICAR

INFORMES CCN-CERT

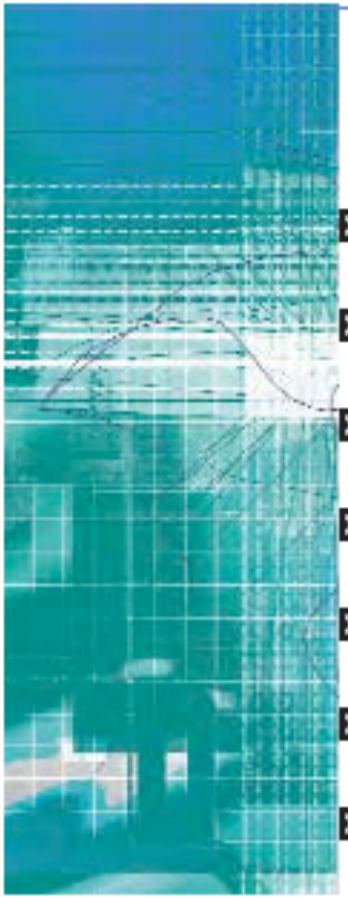
- **Informes de Amenazas STIC**
  - Seguridad en la nube (“Cloud computing”)
  - Seguridad Móvil
  - DNSSec
  - Amenazas y vulnerabilidades 2009. Tendencias 2010, etc…
- **Informes de Actualidad STIC**
  - Noticias STIC
  - Artículos sobre Ciberseguridad
  - Estado del Hack
- **Informes de Código Dañino**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



SIN CLASIFICAR

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