ESQUEMA NACIONAL DE SEGURIDAD

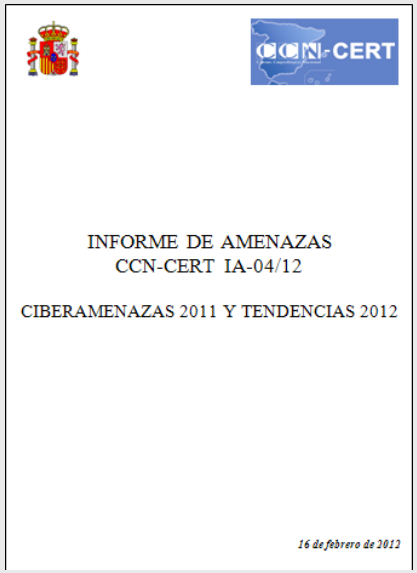
Servicios CCN-CERT

Amenazas 2011

Madrid, marzo de 2012

SIN CLASIFICAR

Índice



- Introducción
- Servicios de Alerta Temprana
  - SAT SARA / INTERNET
  - SAT CARMEN
- Formación
- Mejores prácticas
  1. Guías CCN-STIC
  2. Informes CCN-CERT
  3. PILAR
- Estudio implantación ENS / e-DNI
- Vulnerabilidades / alertas
- CONCLUSIONES
  - Ciberamenazas 2011 Tendencias 2012

Marco Legal

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

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.

CCN-CERT. www.ccn-cert.cni.es

- **MISIÓN:**
  - Ser el centro de alerta y respuesta de incidentes de seguridad, ayudando a las AAPP a responder de forma más rápida y eficiente ante las amenazas de seguridad que afecten a sus sistemas de información.
- **COMUNIDAD:**

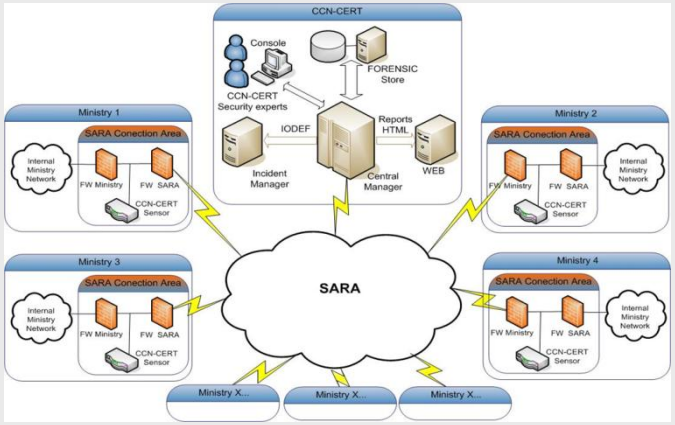
Administraciones Públicas de España

- **HITOS RELEVANTES**
  - **2006 Creación**
  - **2007 Recon. internacional**
  - **2008 EGC**
  - **2009 Sondas SARA**
  - **2010 Sondas INTERNET**

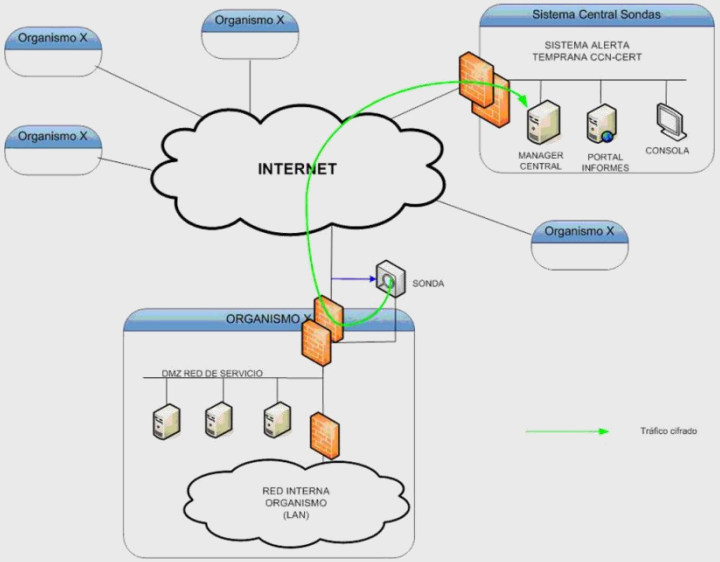
    RD 3/2010
  - **2012 CARMEN / Distribución reglas**

SISTEMAS DE ALERTA TEMPRANA

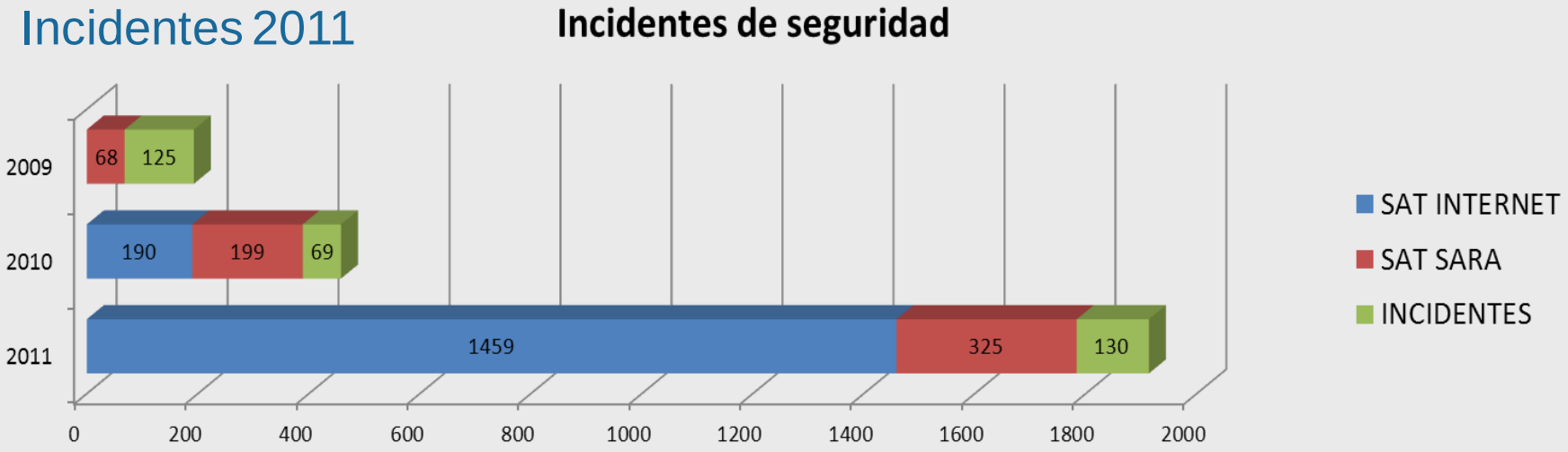
- **RED SARA:**
  - Servicio para la Intranet Administrativa
  - Coordinado con MPTAP.
  - **39**/52 sondas

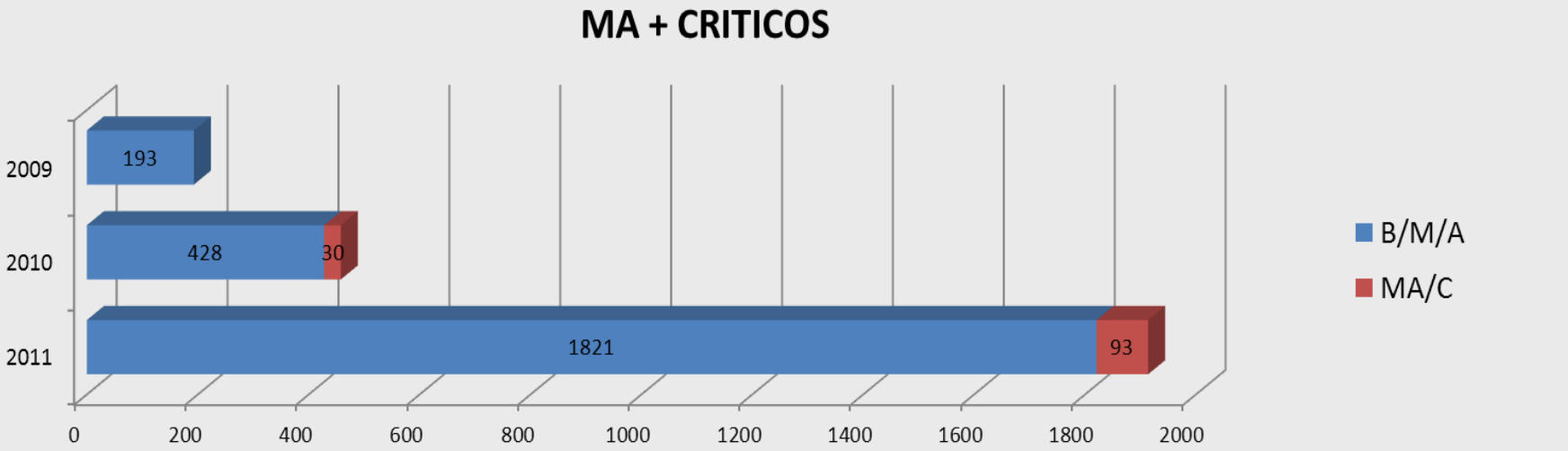


- **SONDAS SALIDAS DE INTERNET AAPP:**
  - Servicio por suscripción de los Organismos.
  - Despliegue de Sensores.
  - **31 sondas**. Previstas 35-40.



- Incidentes 2011





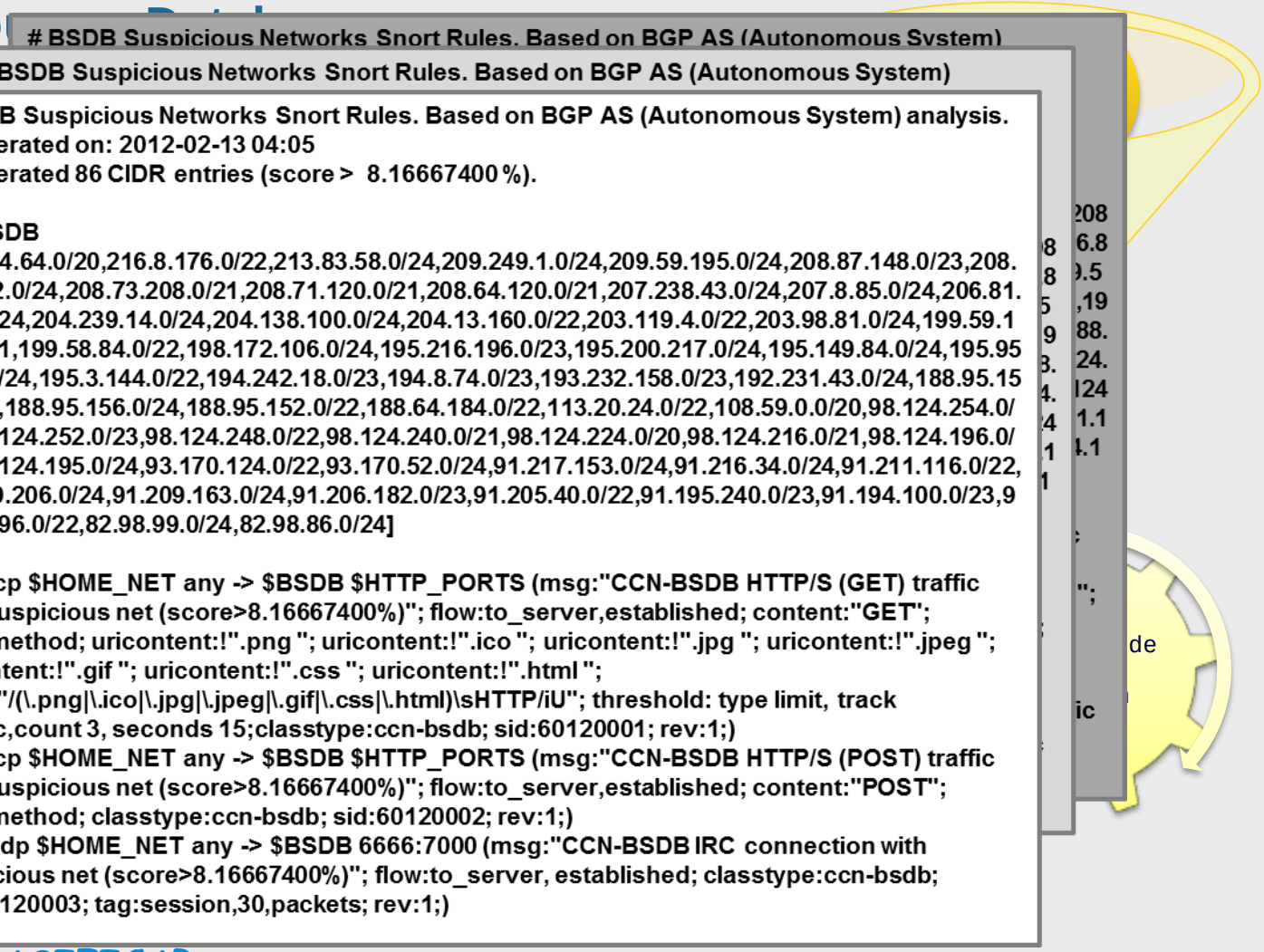
SIN CLASIFICAR

Nuevos servicios SAT INTERNET 2012:

Difusión reglas SNORT / Listas negras

- En respuesta a solicitud por diversos Organismos
- Distribución mensual
- Accesibles a través del Sistema Central
  - Acceso controlado
  - Credenciales de acceso y certificados

- **Black So**
  - M
  - O



SIN CLASIFICAR

CARMEN

- **El Centro de Análisis de Registros y Minería de Eventos Nacionales (CARMEN), es una herramienta desarrollada por el CCN-CERT que permite el análisis en tiempo real de diversas fuentes de logs.**

- Basado en modelos matemáticos.
- Utilización de ingeniería de minería de datos.
- Su implementación en un Organismo es significativamente rápida.
- **Objetivo: Búsqueda APT**

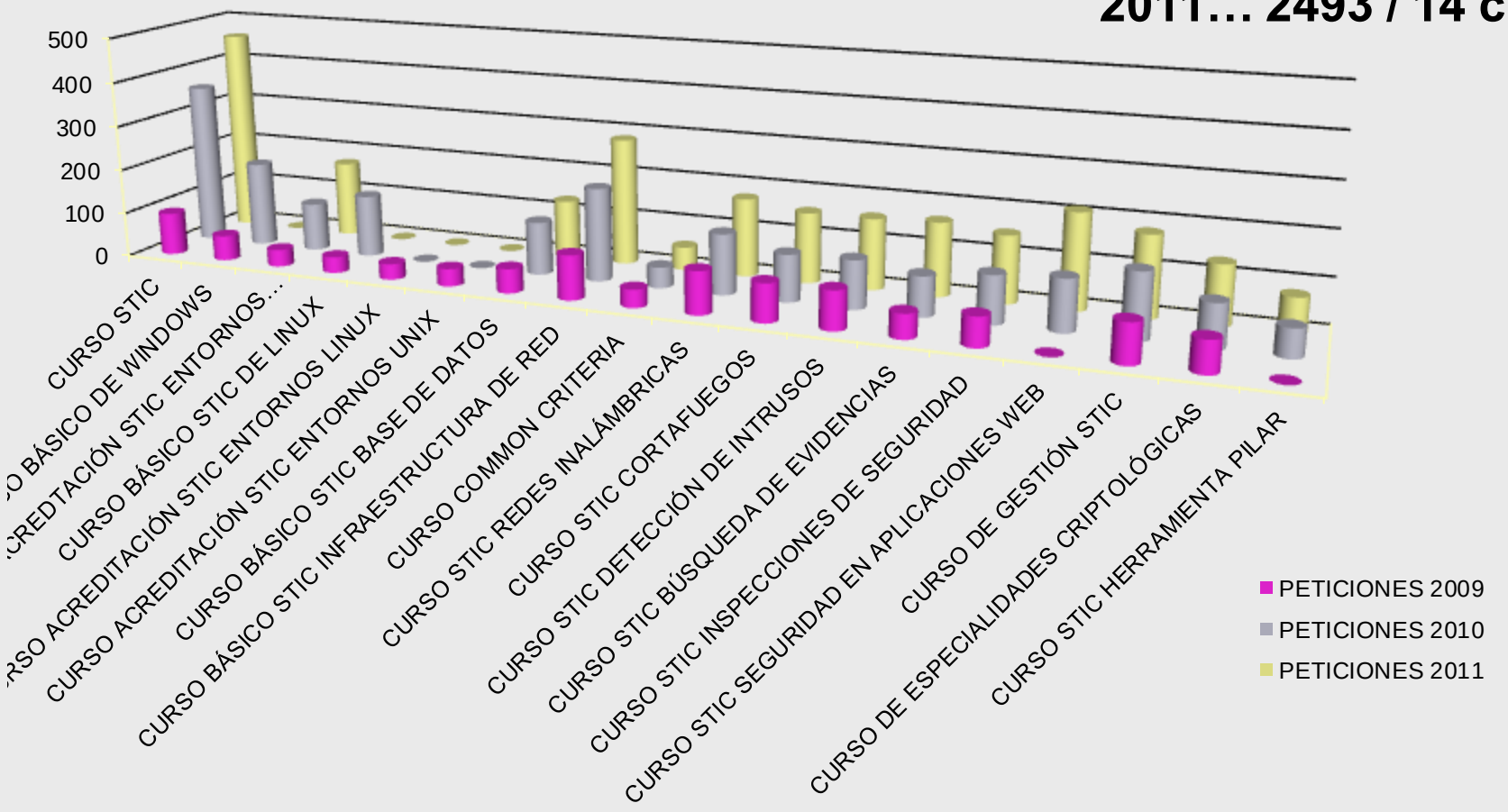
Funcionamiento básico

SIN CLASIFICAR

Formación. Estadísticas

2010… 2119 / 16 cursos

2011… 2493 / 14 cursos

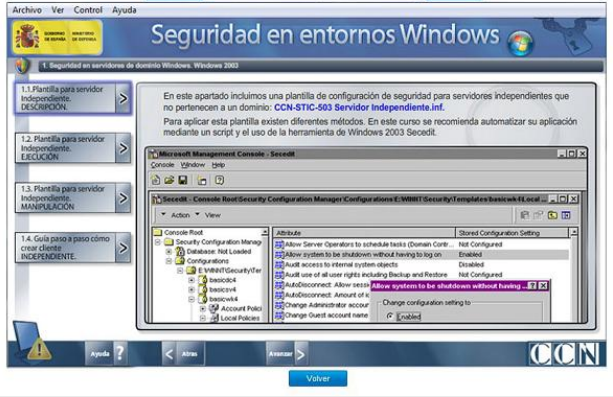


SIN CLASIFICAR

Plazas para año 2012

524 / 14 cursos

Formación



- **Cursos Online en fase de implantación:**
  - **Curso STIC fundamentos (30 horas) (fase Curso STIC)**
  - **Seguridad en entorno Linux (20 horas)**
  - **Curso PILAR** (10 horas) **(fase Curso PILAR / Gestión STIC)**
  - **Seguridad en entorno Windows (20 horas)**
  - **Curso ENS (20 horas) (fase Curso Gestión STIC)**

Cursos Online 2012:

- Curso STIC - Common Criteria. (10 horas)
- Curso Gestión de incidentes (10 horas)
- Curso PILAR (Manejo de herramienta / Funciones más usadas)
- Curso ENS. Módulo (10 horas)

SIN CLASIFICAR

Guías CCN-STIC / PILAR

- **Series CCN-STIC:**
  - 189 documentos, normas, instrucciones, guías y recomendaciones
    - (24 pendientes de aprobación)
  - Nueva serie 800: ESQUEMA NACIONAL DE SEGURIDAD
    - **14 Guías**

- **Herramienta PILAR**
  - Perfil de protección para el ESQUEMA NACIONAL DE SEGURIDAD
  - Biblioteca para infraestructuras críticas

  - Herramientas :
    - PILAR
    - MICROPILAR
    - RMAT

SIN CLASIFICAR

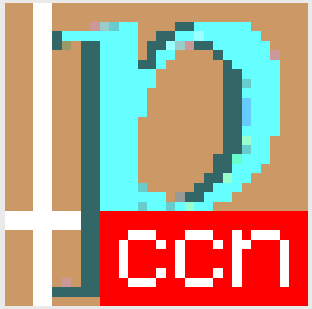
Guías desarrolladas en 2011

- 413 Auditoría de Entornos y Aplicaciones Web
- 442 Seguridad en VMWare ESXi
- **453 Seguridad en Android 2.1**
- 455 Seguridad en iPhone
- 456 Seguridad en entornos BES
- **521C y D Seguridad en Windows 2008 Server Core**
- **522A Seguridad en Windows 7 (cliente en dominio)**
- **523 Seguridad en Windows 2008 Server. Servidor de Ficheros.**
- 524 Seguridad en Bases de Datos SQL Server 2008
- 525/6 Seguridad en Microsoft Exchange Server 2007 sobre Windows 2003 /2008
- 530 Seguridad en Microsoft Office 2010
- 613 Seguridad en sistemas basados en Debian
- 615 Seguridad en entornos basados en RED HAT
- 662 Seguridad en Apache Traffic Server
- **957 Recomendaciones de Empleo de la Herramienta TrueCrypt**
- **955 Recomendaciones de Empleo de GnuPG**

SIN CLASIFICAR

Estudio de seguridad sobre cumplimiento del ENS

- Estudio sobre 34 organismos
- Empleo de microPILAR.
  - Valoración
  - Aportación evidencias documentales
- Valoración de 3 perfiles de seguridad
  - ESQ. NACIONAL DE SEGURIDAD
  - CCN-STIC 301
  - CCN-STIC 811
- Niveles de MADUREZ de PILAR



NIVEL DE MADUREZ		DESCRIPCIÓN DEL NIVEL
Nivel	%	
L0	0	**Inexistente. Esta salvaguarda no existe en este momento.**
L1	10	**Inicial/ad hoc. Se hace cuando se considera adecuado, pero no está establecido.**
L2	50	**Reproducible, pero intuitivo. Se realiza, pero no está formalizado documentalmente.**
L3	90	**Proceso definido. Se realiza y está definido documentalmente (procedimientos).**
L4	95	**Gestionado y medible. Se están gestionando y son susceptibles de ser medidas.**
L5	**100**	**Optimizado. La medida está definida, medida y se aplica proceso de mejora y optimización.**

PERFILES EMPLEADOS

- Perfil ENS. El tanto por ciento (%) de este perfil indicará el nivel de cumplimiento del ENS por parte del organismo. Se han valorado todos los aspectos del marco ORGANIZATVO, marco OPERACIONAL y MEDIDAS DE PROTECCIÓN

- Perfil CCN-STIC 301. El tanto por ciento (%) de cumplimiento de este perfil indicará el nivel de seguridad de la red corporativa haciendo especial foco en los equipos de usuarios tanto desde el punto de vista de la configuración como de la seguridad.
  - Este perfil establece los requisitos mínimos de seguridad que deben estar activos en una red clasificada DIFUSIÓN LIMITADA (equivalente a un sistema del ENS con categoría ALTA).

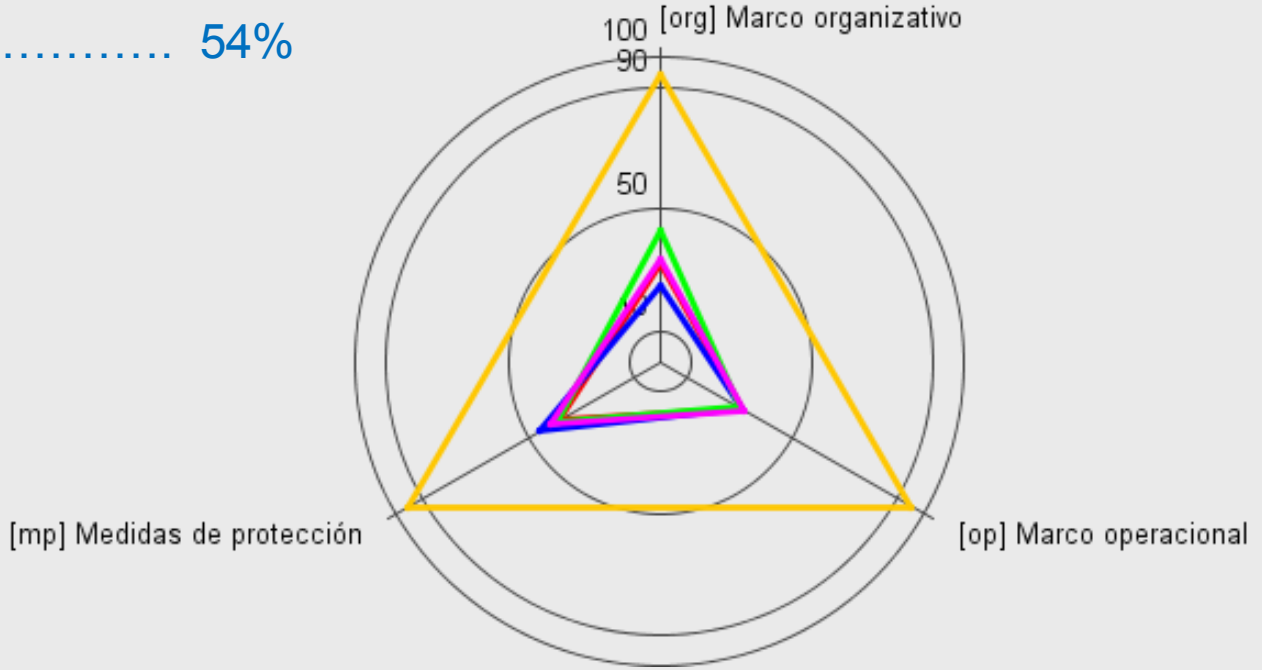
PERFILES EMPLEADOS

- Perfil ENS CCN-STIC 811. El tanto por ciento (%) de cumplimiento de este perfil indicará el nivel de seguridad en las diferentes INTERCONEXIONES y en los túneles cifrados que se establezcan en el organismo. Este perfil establece los requisitos mínimos de seguridad que deben estar activos en:
  - PROTECCIÓN PERIMETRAL. Nivel de seguridad en los diferentes dispositivos que velan por la seguridad del perímetro y eficacia en la monitorización del tráfico del organismo.
  - CON RED PÚBLICA (INTERNET). Nivel de seguridad en la conexión con INTERNET analizando los diferentes dispositivos de protección de perímetro y herramientas de seguridad que permitan detectar y/o evitar cualquier agresión a la red corporativa y sus usuarios.
    - Se consulta por las políticas de uso de INTERNET para los usuarios
  - CON RED NIVEL BAJO (SARA).
  - RED PRIVADA VIRTUAL (VPN). Nivel de seguridad en los diferentes túneles cifrados que estén activos en el organismo haciendo especial énfasis en la gestión de las claves asociadas a estos.

Estudio de seguridad sobre cumplimiento del ENS

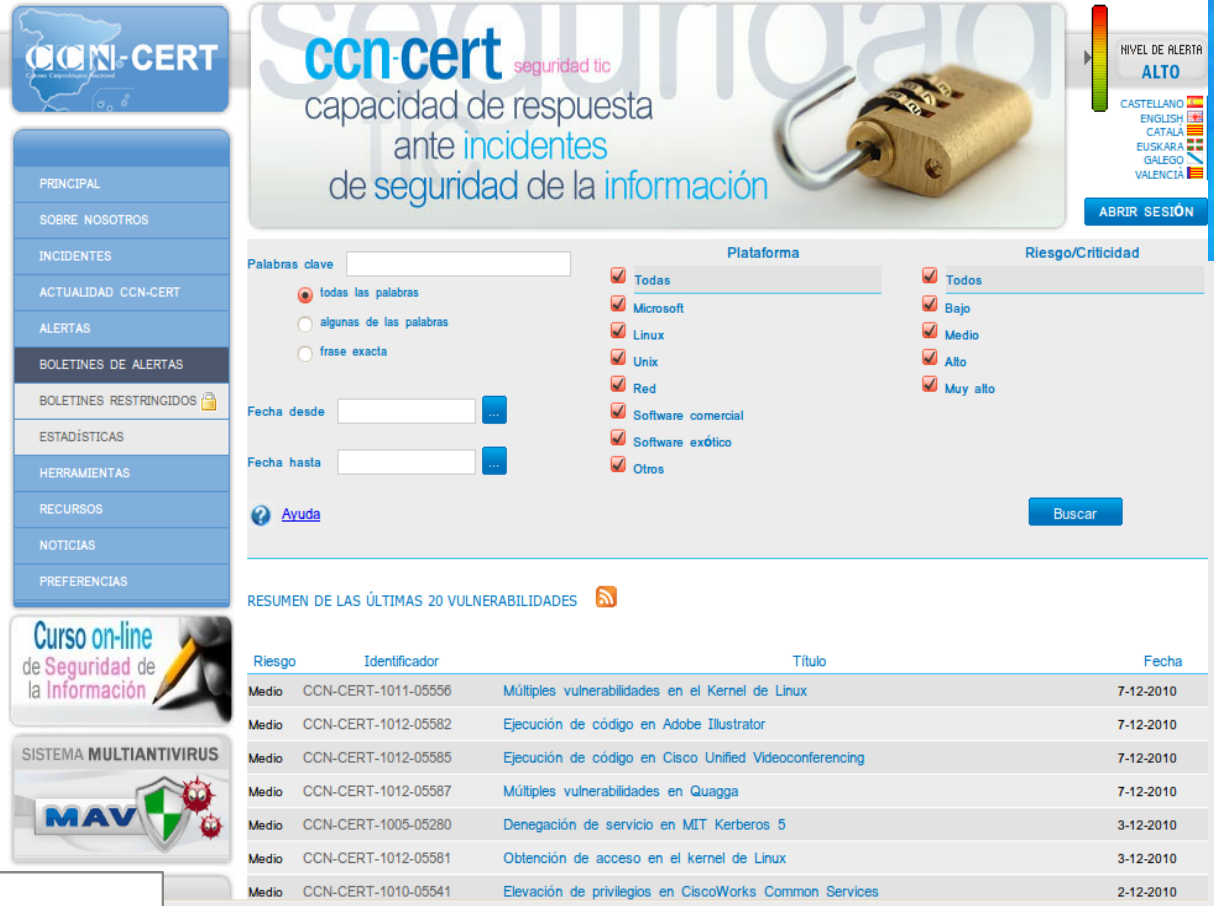
- Media de niveles de cumplimiento.
  - ESQUEMA NACIONAL DE SEGURIDAD
    - Marco organizativo …….. 34 %
    - Marco operacional …….. 32 %
    - Medidas de protección ……. 41%

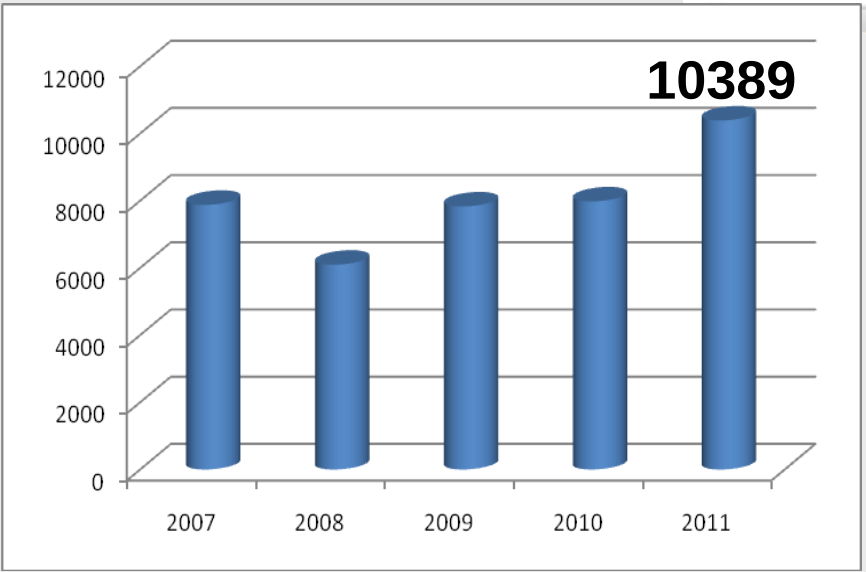
  - CCN-STIC 301 ……. 39 %
  - CCN-STIC 811 ……. 54%



Vulnerabilidades

- Parte pública portal. ESPAÑOL
  - Criticidad
  - Tecnología
- Parte privada portal. INGLÉS
  - Vulnerabilidades
  - Amenazas
  - Código dañino





•Vulnerabilidades 2011 por fabricante

2007	2008	2009	2010	2011
Novell	Novell	Oracle	Apple	Oracle
Avaya	Apple	Apple	Oracle	Microsoft
Microsoft	Sun	Novell	Vmware	Apple
Sun	Avaya	Avaya	Novell	Google
Apple	Hewlett-Packard	Microsoft	Hewlett-Packard	Adobe
Oracle	IBM	Hewlett-Packard	Microsoft	Hewlett-Packard
Silicon Graphics	Microsoft	Nortel Networks	Adobe	Novell
Hewlett-Packard	Oracle	Mozilla	Google	Vmware
IBM	Cisco	IBM	Cisco	Cisco
PHP Group	Vmware	Cisco	Mozilla	IBM

I-EXPLORER

SAFARI

CHROME

SIN CLASIFICAR

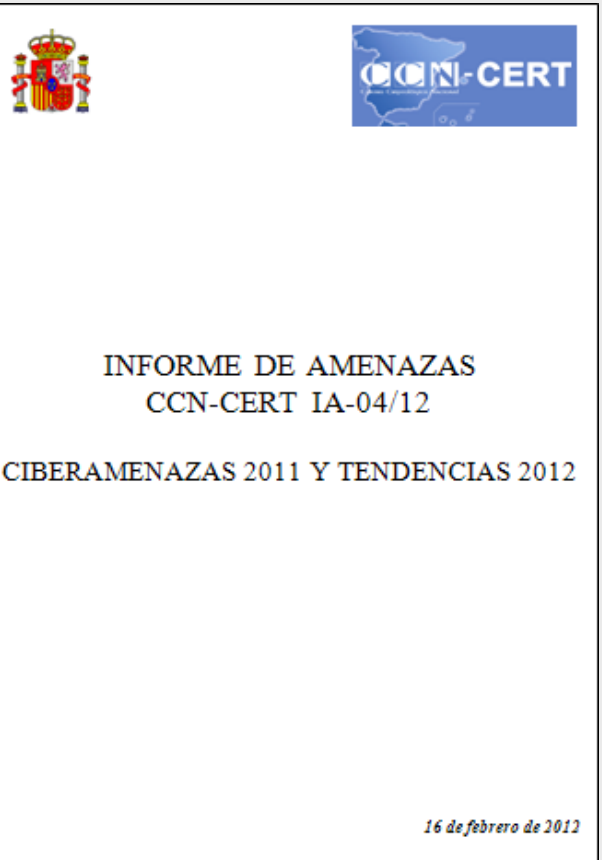
CONCLUSIONES / ACTIVIDADES PREVISTAS 2012

- FORMACIÓN / GUÍAS CCN-STIC
  - 3-4 Guías relacionadas con ENS. **(Colaboración REVISIÓN / DESARROLLO)**
  - Nuevos cursos ON LINE (relacionados con ENS)
- PILAR
  - **ESTUDIO DE SEGURIDAD PARA VALORAR NIVEL DE IMPLANTACIÓN (Art 35)**
- SISTEMAS DE ALERTA TEMPRANA
  - INTERNET / SARA… Nuevas funcionalidades.
  - CARMEN…. Despliegue de PILOTO
  - **Potenciar el intercambio de patrones**
- VULNERABILIDADES/ AMENAZAS
  - Ampliar la difusión de IA / Acceso a información de otras fuentes
- **NECESIDAD DE INTERCAMBIO / COLABORACIÓN**

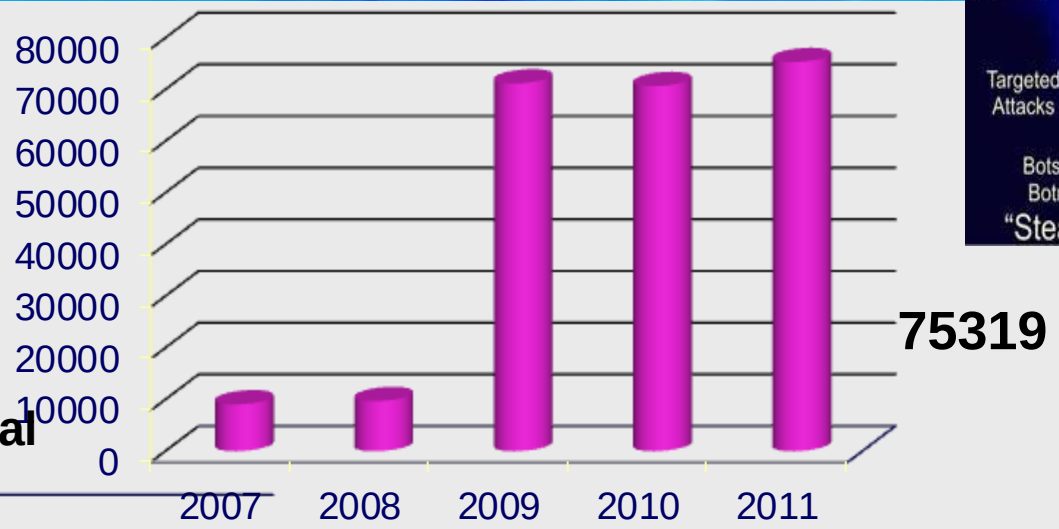
CCN
Centro Criptológico Nacional

AMENAZAS 2011
TENDENCIAS 2012

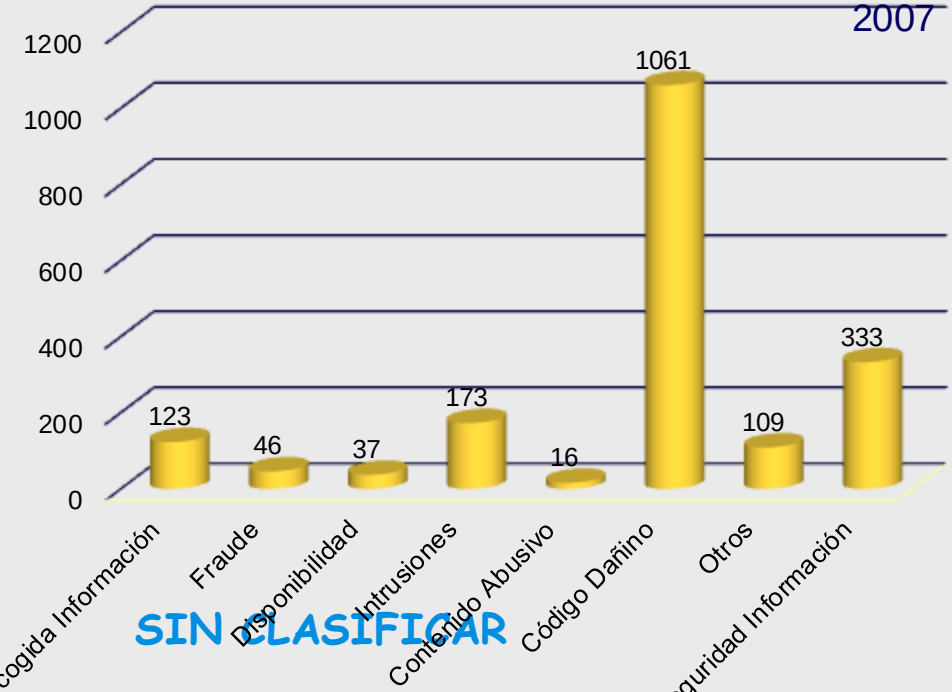
SIN CLASIFICAR

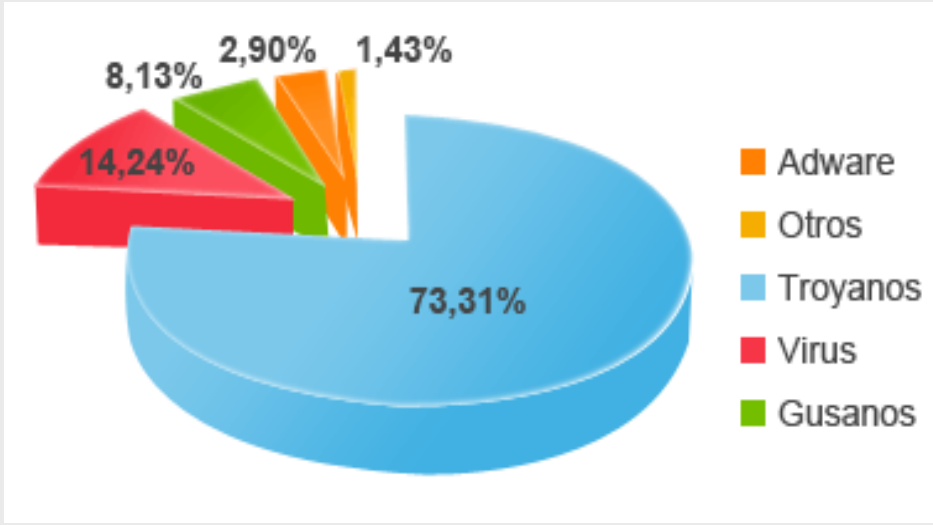


Código dañino 2011



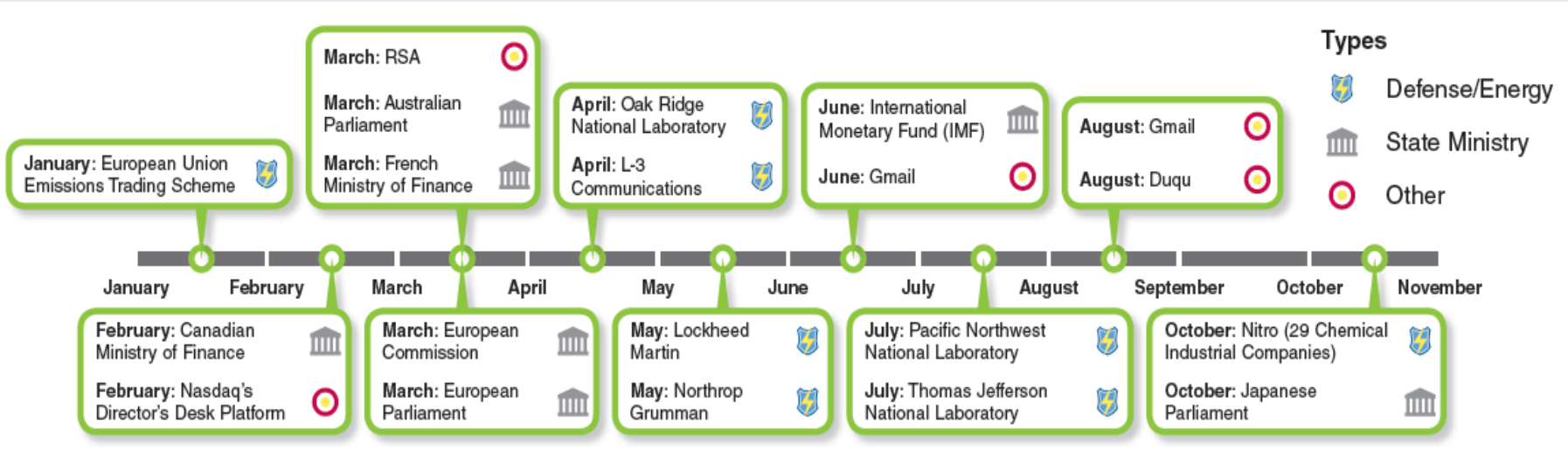
Clasificación General





Ciberamenazas. Agentes

1. Ciberespionaje
   - Estados (Servicios de Inteligencia /FFAA) / Industrias / empresas
   - Activos en formato electrónico.
   - Dificultad de atribución
   - Contra los Sectores Privado y Público.
   - Ataques dirigidos (APT) → Modelo de Confianza.
   - Contra objetivos primarios o secundarios.
   - Ventajas políticas, económicas, sociales…



Ataque Herramientas y productos de autenticación

05.2011

- Lockheed Martin
- L-3 Communications
- Northrop Grumman

- SECUR-ID EMC - RSA

03.2011

- Excel + adobe flash player
- Ataque POISON IVY

SIN CLASIFICAR

Autoridades de certificación

- Comodo
- DigiNotar (530)
- GlobalSign
- Digicert-Malasia
- KPN
- Compromiso de CA/RA

Ciberamenazas. Agentes

2. Cibercrimen
   - Robo propiedad intelectual / información de tarjetas de crédito / certificados
   - Fraude Telemático / Blanqueo de dinero / Robo de identidades…

Tarjetas de crédito	Desde 2$ hasta 90$
Tarjetas de crédito físicas	Desde 180$ + coste de los datos
Máquinas duplicadoras de tarjetas	Desde 200 hasta 1.000 $
Cajeros automáticos falsos	Hasta 3.500$
Credenciales bancarias	Desde 80 y hasta 700$ (con garantía de saldo)
Transferencias bancarias y cobro de cheques	Entre el 10 y el 40% del total a transferir o cobrar
Cuentas de tiendas online y pasarelas de pago	Entre 80 y 1.500$ con saldo verificado
Diseño e implementación de falsas tiendas online	Según proyecto (sin especificar)
Compra y envío de productos	Entre 30 y 300$ (dependiendo producto)
Alquiler envío de spam	A partir de 15$
Alquiler SMTP	A partir de 20$. 40$ para uso durante 3 meses
Alquiler VPN	20$ para utilización para 3 meses

Costes del Ciberdelito	Coste neto total del ciberdelito	388.000 M. dólares
	El valor del tiempo perdido por las víctimas de los ciberdelitos	274.000 M. dólares
	Coste directo (cantidades sustraídas – dedicadas a la resolución de los ciberdelitos)	114.000 M. dólares

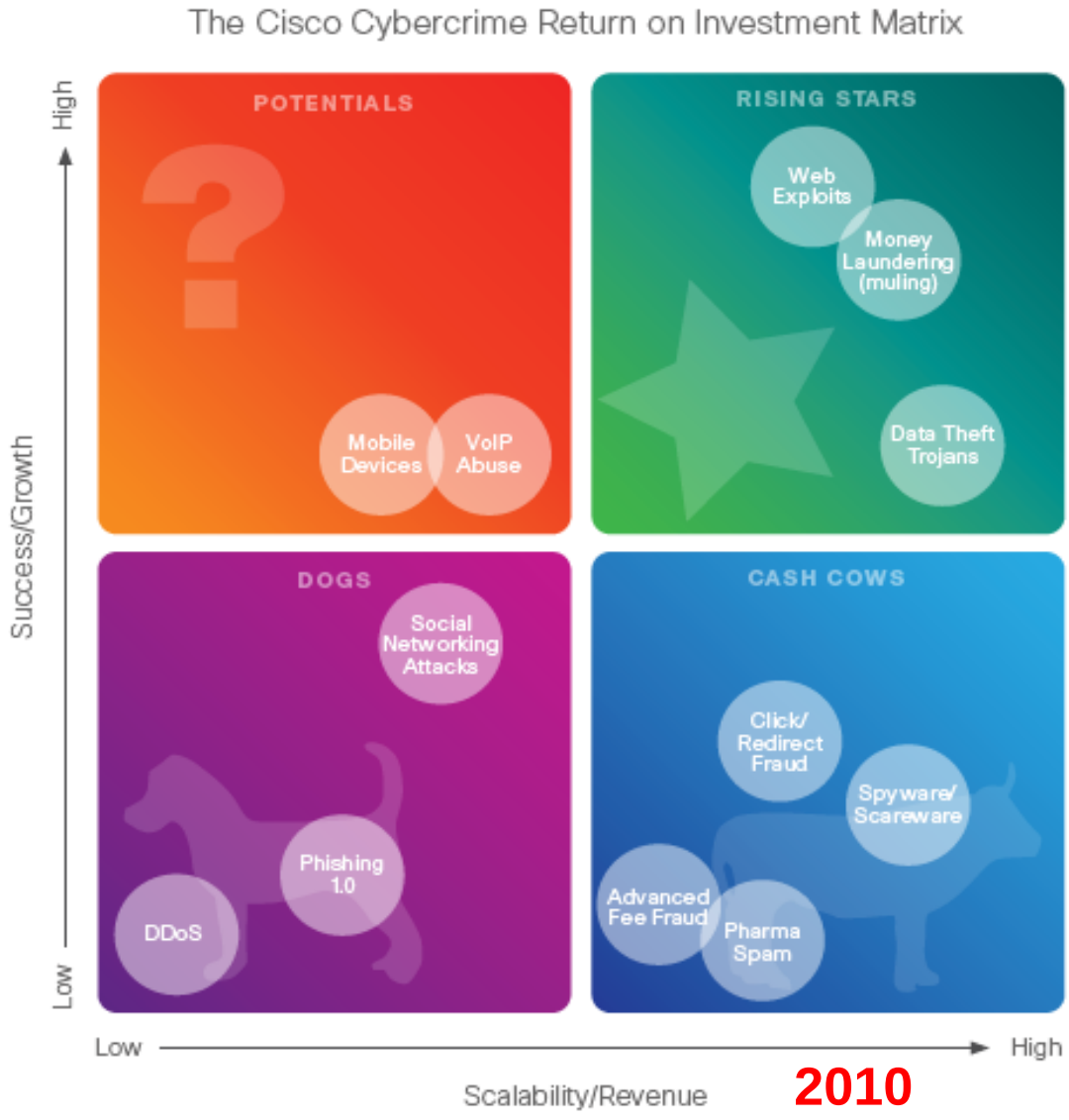
SIN CLASIFICAR

ESPAÑA	Coste neto total del ciberdelito	5.900 millones de euros (8.300 millones de dólares)
	El valor del tiempo perdido de las víctimas de los ciberdelitos	5.500 millones de euros (7.600 millones de dólares)
	Coste directo (cantidades sustraídas – dedicadas a la resolución de los ciberdelitos)	482 millones de euros (670,2 millones de dólares)

Ciberamenazas. Agentes

- 3. Hacking Político / Patriótico
  - China- Japón; India-Pakistán; Irán-Israel…
  - ANONYMUS /LUZSEC / Antisec
  - Progresiva vertebración de sus estructuras.
  - Grupos organizados (por países, regiones, …)
  - Nivel organizativo / nivel ejecutivo.
  - Ataques / divulgación de información.
  - Pre-selección de objetivos.
  - Hacktivismo tecnológico y físico → juntos.
  - Peligro → radicalización.

TENDENCIAS 2012



2010

2011

Gracias

- **CÓMO CONTACTAR:**
  - ccn@cni.es
  - **INCIDENTES**
    - incidentes@ccn-cert.cni.es
  - **SISTEMAS ALERTA TEMPRANA**
    - sondas@ccn-cert.cni.es
    - redsara@ccn-cert.cni.es
    - carmen@ccn-cert.cni.es
  - **GENERAL**
    - info@ccn-cert.cni.es
    - ens@ccn-cert.cni.es

SIN CLASIFICAR