CCN-CERT
Servicio de Respuesta a Incidentes de Seguridad para la Administración

Madrid, Abril de 2007

Presentación

- FORO: Rueda de Prensa 2007.04.24
- SESIÓN: Iniciativa del CCN del CERT Gubernamental.
- OBJETIVO: Establecer el ámbito y los objetivos del CCN en el ámbito de la respuesta incidentes.
- PONENTE:
  - Luis Jiménez
  - Centro Criptológico Nacional
- FECHA: 24 de abril de 2007

Índice

- Funciones del CNI / CCN
  - Ley 11/2002
  - RD 421/2004
- Definiciones
  - Servicios CERT
- Situación Europa
- CCN-CERT
  - Descripción proyecto
  - Servicios proporcionados
  - Plan 2007-2008
- Conclusiones

Marco Legal

El CCN actúa según el siguiente marco legal:

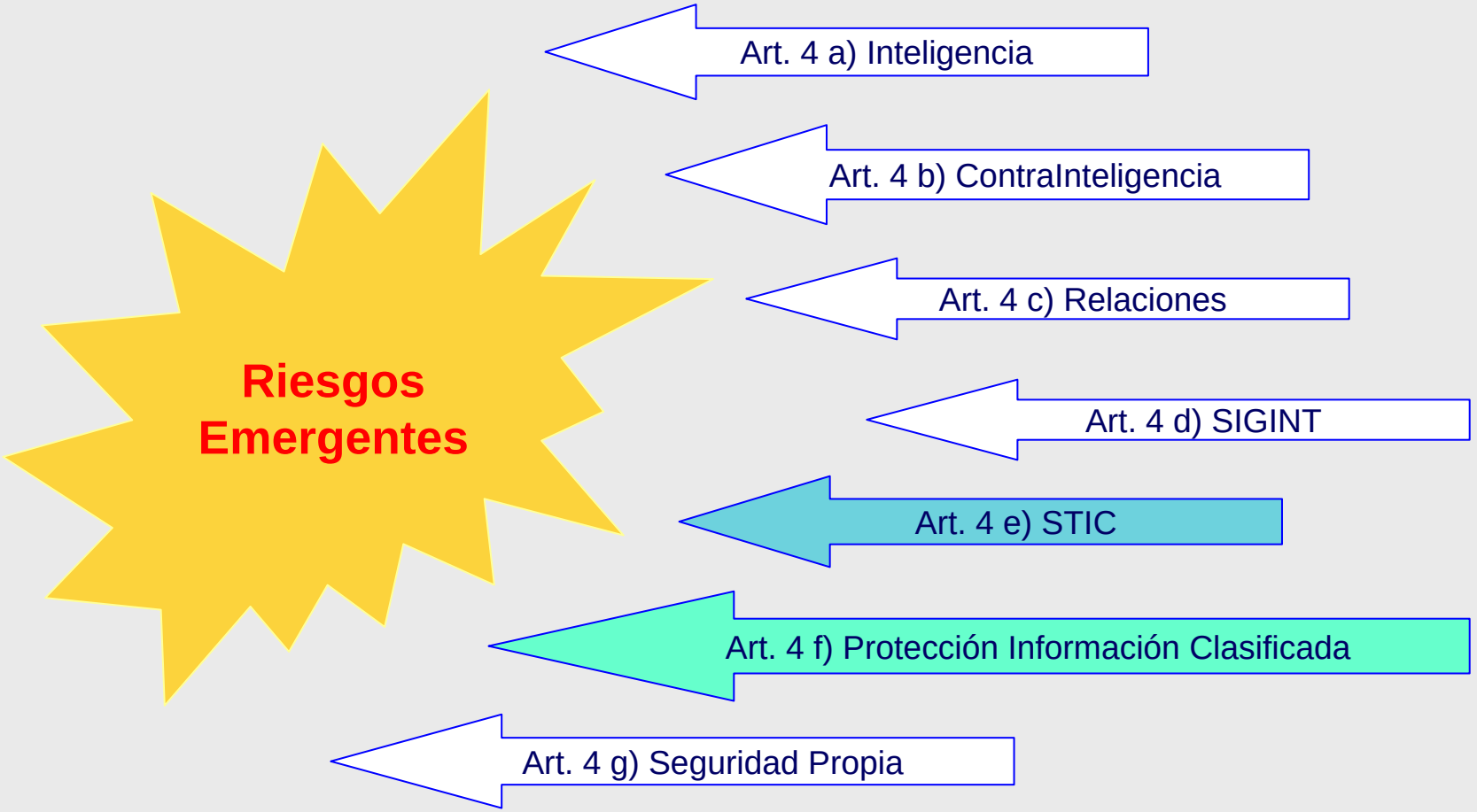
Ley 11/2002, 6 de Mayo, regula el Centro Nacional de Inteligencia (CNI), que incluye al Centro Criptológico Nacional (CCN).

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

Exposición de Motivos (Ley 11/2002)

- La sociedad española demanda unos Servicios de Inteligencia eficaces, especializados y modernos, capaces de afrontar los nuevos retos del actual escenario nacional e internacional, regidos por los principios de control y pleno sometimiento al ordenamiento jurídico.
- … los nuevos retos que para los servicios de inteligencia se derivan de los llamados riesgos emergentes, que esta Ley afronta al definir las funciones del Centro …

Centro Nacional de Inteligencia (Ley 11/2002)



Funciones del CCN (RD 421/2004)

- **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.

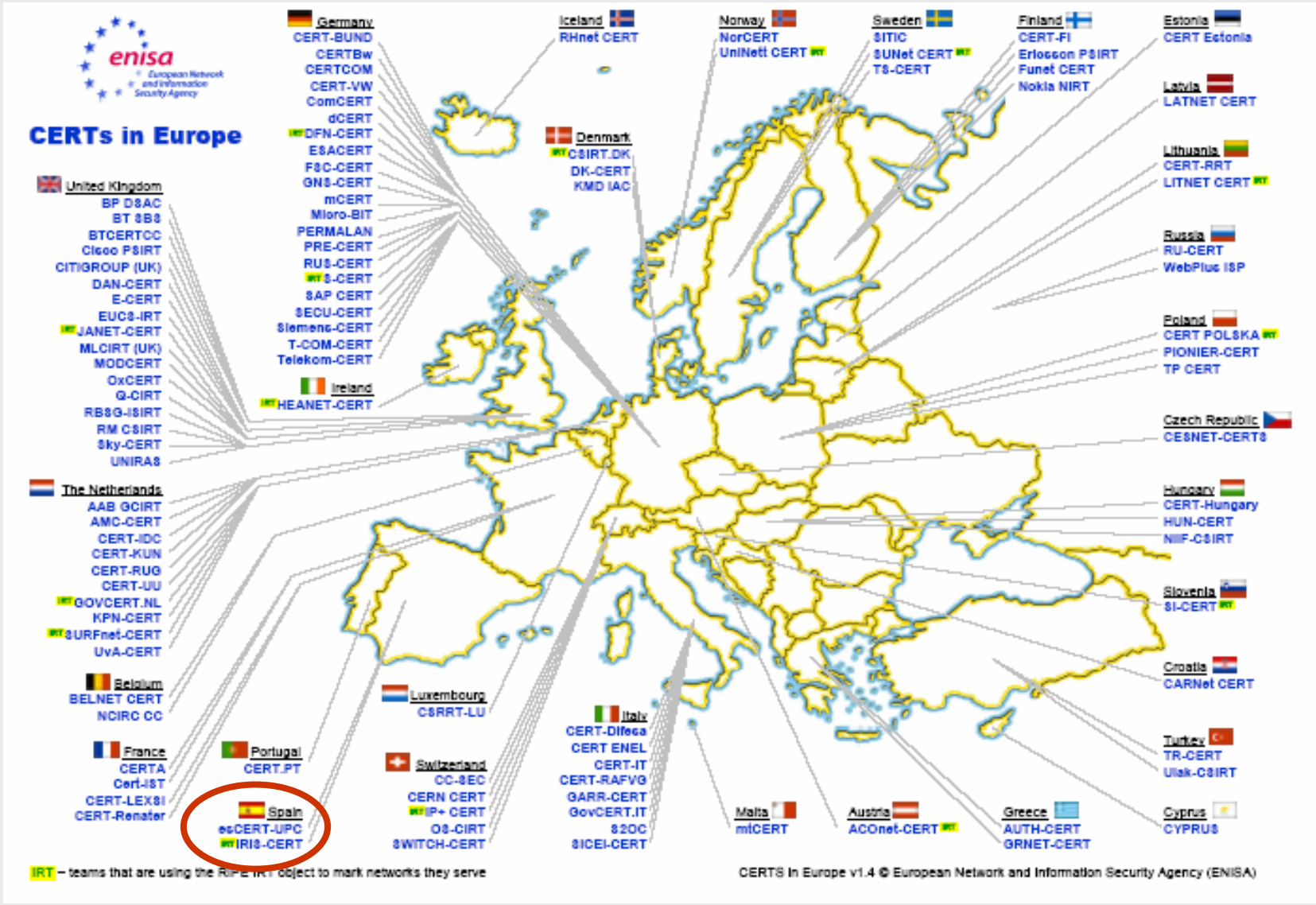
CERT / CSIRT

- **CERT**
  - **C**omputer **E**mergency **R**esponse **T**eam
  - Es una organización que estudia la seguridad de las redes y ordenadores para proporcionar servicios de respuesta ante incidentes a víctimas de ataques, publicar alertas relativas a amenazas y vulnerabilidades y para ofrecer información que ayude a mejorar la seguridad de estos sistemas.
    - It´s an organisation that studies computer and network security in order to provide incident response services to victims of attacks, publish alerts concerning vulnerabilities and threats, and to offer other information to help improve computer and network security.
  - **SERVICIOS REACTIVOS**

- **CSIRT**
  - **C**omputer **S**ecurity and **I**ncident **R**esponse **T**eam….. Final 90 completar concepto de CERT.
  - Completa los servicios proporcionados incluyendo servicios preventivos y de gestión de seguridad (valor añadido)

- (CERT y CSIRT) se utilizan de forma similar,

CERTs en Europa



CCN-CERT RESPUESTA A INCIDENTES EN LA ADMINISTRACION

- El **objetivo** principal del equipo de respuesta a incidentes del CCN (CCN-CERT) es contribuir a la mejora del nivel de seguridad de los sistemas de información de las AA.PP. de España.

- **Misión** es 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.

CCN-CERT. Comunidad / Autoridad

- **Nuestra comunidad serán las Administraciones Públicas de España: Administración General, Autonómica y Local**

  - La Autoridad del CCN-CERT es compartida con los organismos de nuestra comunidad, consensuando con ellos las acciones necesarias para cumplir con la misión CCN-CERT:
    - Se tiene potestad para realizar todas las acciones necesarias para resolución del incidente en sistemas clasificados
    - Colaboración y asesoramiento en resolución de incidentes de sistemas de la administración general, autonómica y local

CCN-CERT …. www.ccn-cert.cni.es

Visión general del Proyecto

I. Servicios de Información

II. Servicios de Formación

III. Plan de Comunicación y Promoción

IV. Desarrollo de Políticas y Procedimientos

V. Servicios de Gestión de Incidentes

VI. Servicios de Monitorización

VII. Soporte a la creación de nuevos CERT's

I. Servicios de Información

- Funcionalidades principales PORTAL WEB:
  - Servicios públicos:
    - Boletines de vulnerabilidades propios
    - Estadísticas e indicadores de propios / terceros
    - Notas de prensa / Publicaciones / Herramientas
    - Descarga herramienta PILAR / Glosario (CCN-STIC 401)
  - Servicios restringidos AAPP:
    - Series CCN-STIC / Contenidos cursos STIC…
  - Mecanismos de publicación no Web:
    - Publicación de noticias por listas de distribución de correo electrónico
    - Publicación de estadísticas y otros contenidos por hilos RSS

Servicio de publicación de vulnerabilidades

Boletines de Vulnerabilidades

Utilización de Firefox como escáner de puertos

Clasificación de la vulnerabilidad

Propiedad	Valor
Riesgo	Medio
Nivel de Confianza	Oficial
Impacto	Integridad
Dificultad	Experto
Requerimientos del atacante	Acceso remoto sin cuenta a un servicio exotico

Información sobre el sistema

Propiedad	Valor
Plataforma afectada	Networking
Software afectado	Mozilla Firefox < 2.0.0.3 Mozilla Firefox < 1.5.0.11 Mozilla SeaMonkey

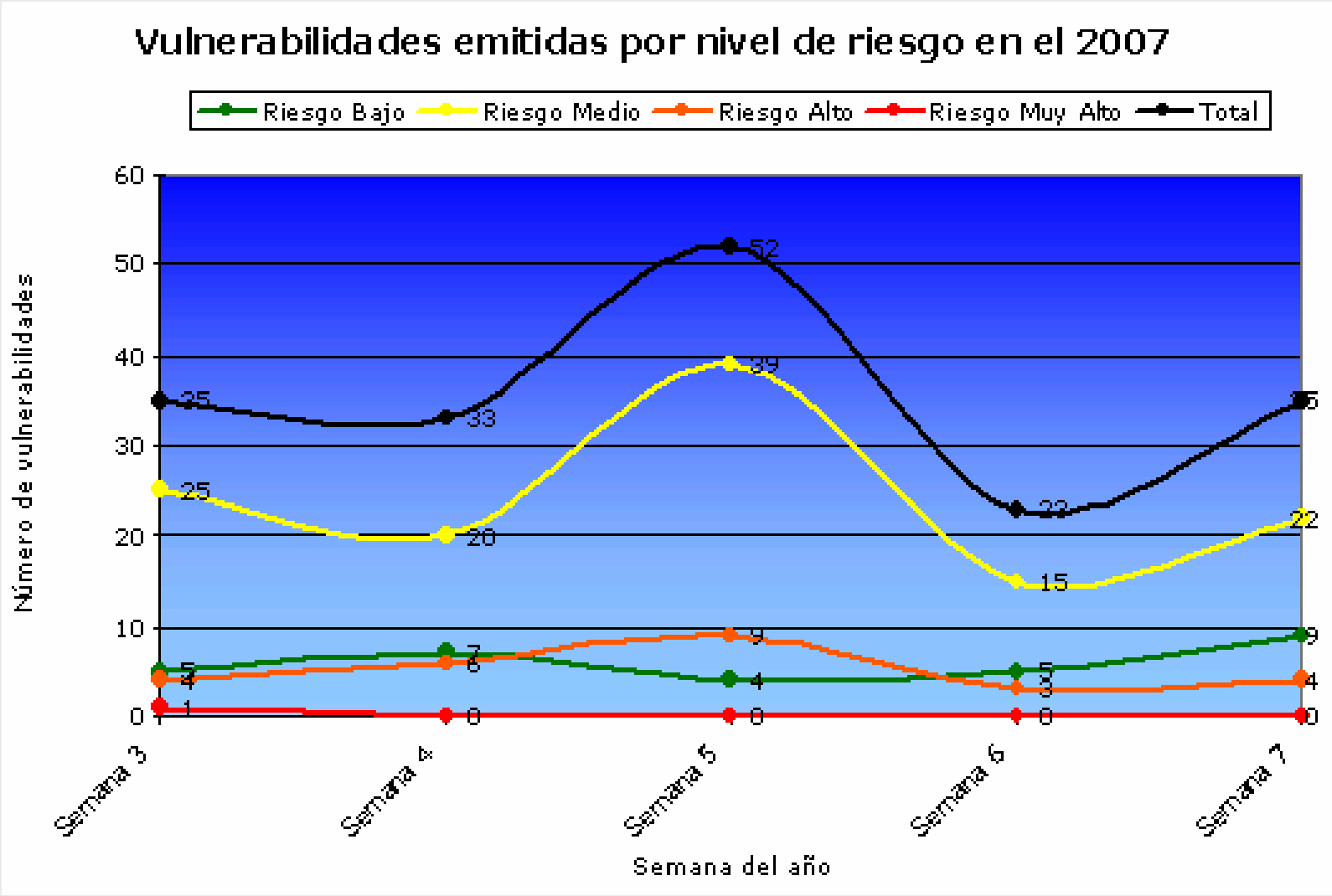
Descripción

Se ha descubierto una vulnerabilidad en Mozilla Firefox y en Mozilla SeaMonkey. La vulnerabilidad reside en un error en el comando PASV que es usado por Firefox para hacer la petición de un puerto alternativo para los datos.

Un atacante remoto podría utilizar esta vulnerabilidad para realizar un escaneo de puertos a las máquinas que hayan detrás del firewall de la víctima.

Solución

Notificación de incidentes / Estadísticas



III. Plan de Comunicación

2007 | **2008**

1T 2T 3T 4T | 1T 2T 3T 4T

Plan de Comunicación y Promoción

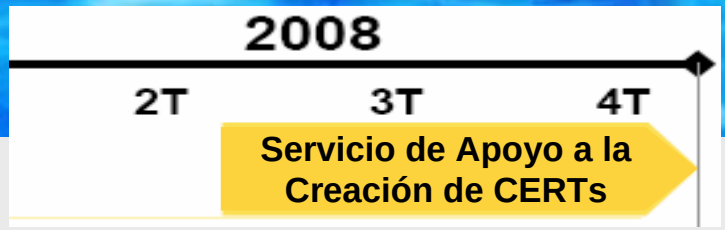
15/11 (Fin actividades de comunicación y promoción)

Hitos significativos 2007:

- Fin Diseño del Plan de Integración con Organismos Internacionales: **01/2007**
- Fin Ejecución del Plan de Integración
  - Fin Integración a nivel europeo (TERENA TF-CSIRT) : **06/2007**
  - Fin Integración a nivel internacional (FIRST) : **06/2007**
- Fin Ejecución Plan de Comunicación y Promoción: **11/2007**

- NACIONAL:
  - Abril 2007
    - Cartas a AA.PP.
    - CSAE
    - Nota/Rueda de Prensa
    - SECURMATICA
  - Mayo 2007
    - Admin General Estado
    - Comunidad Madrid
  - TECNIMAP 2007 (Nov)
  - Junio-Diciembre 2007
    - J. Andalucia / Cataluña / Galicia / C. Valencia / G. Baleares / G. Aragón / P. Vasco

VII. Promoción de otros CERT,s



- Objetivos
  - Ofrecer información, formación y herramientas para que la comunidad pueda desarrollar sus propios CERTs, permitiendo al CCN-CERT actuar de catalizador y coordinador de CERTs a nivel gubernamental
- Actividades principales
  - Plan de desarrollo de CERTs
    - Diseño de guías y herramientas de implantación y operación
    - Diseño y desarrollo de sección en el portal para la comunidad
  - Plan de formación
    - Realización de cursos de creación y gestión de CERTs

CCN-CERT. Conclusiones

- **Del conocimiento y experiencia del CCN en STIC …**
  - ... Mejorar la seguridad de los sistemas de la Administración
  - … Capacidad de Respuesta ante incidentes Gubernamental
    - CCN-CERT
- **Resolución de Incidentes de Seguridad mediante:**
  - Servicios de Información
  - Investigación, Formación y Divulgación
  - Soporte Respuesta a Incidentes
- **Relaciones:**
  - Organismos de la Administración
  - CERTs
  - ISPs, Hosting, DNS,...

Gracias

- Correos electrónicos
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - organismo.certificacion@cni.es
- Páginas Web:
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - www.oc.ccn.cni.es