# CCN-CERT

## Setting up a Governmental CERT:

## The CCN-CERT Case Study

Sevilla, June 2007

# Presentation

- FORUM: 19th Annual FIRST Conference
- SESSION: CCN Initiative of a Governmental CERT
- OBJECTIVE: Set the scope and goals of CCN concerning with Incident Response.
- Speaker:
  - National Cryptology Center
- Date: 22th of June, 2007

# Index

- Legal Framework
- Goal and Mission
- Constituency and Authority
- Website
- CCN-CERT Services
- Sources
- Conclusions

# Legal Framework

CCN acts under the following legal framework:

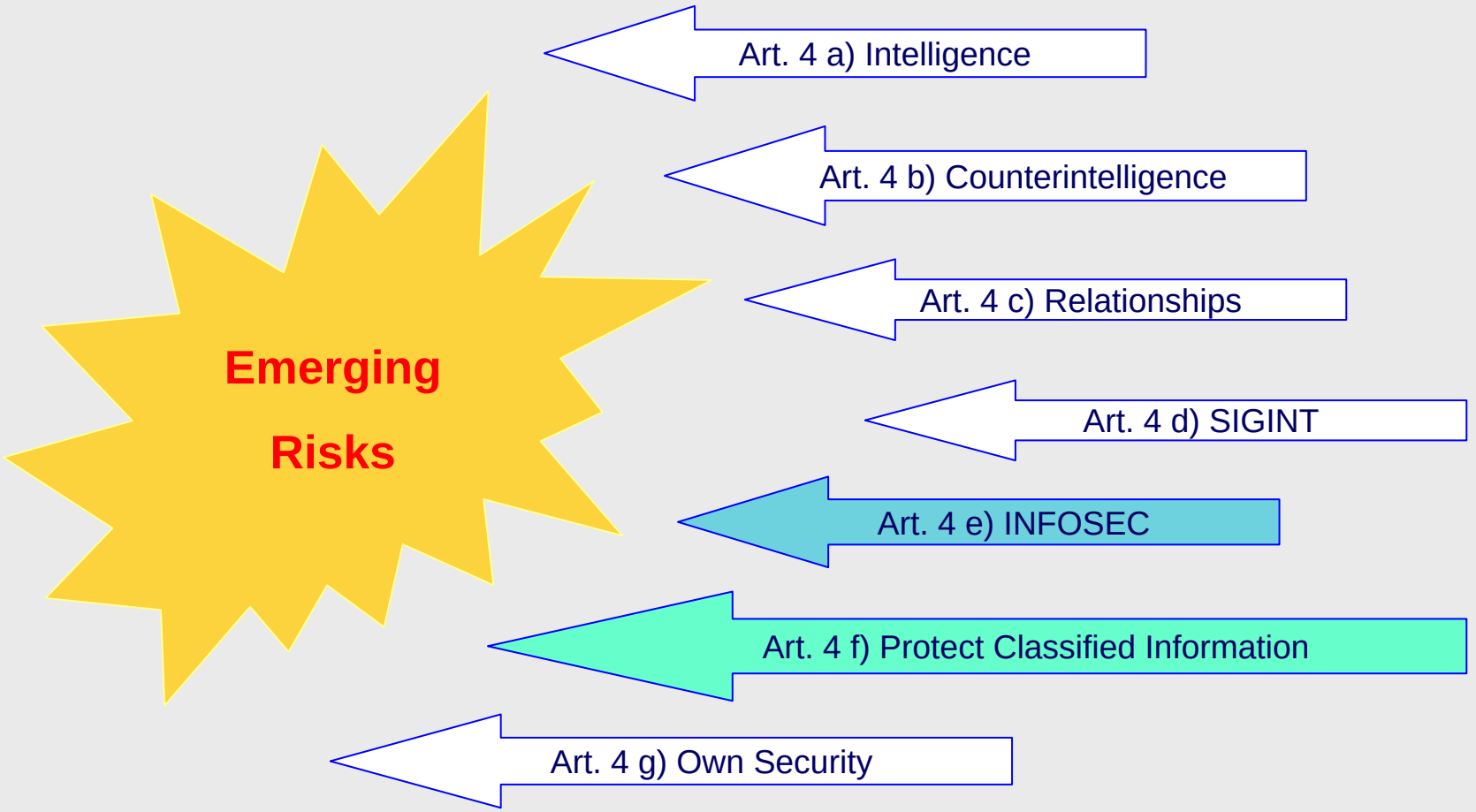
**Law 11/2002, 6th of May**, regulates the National Intelligence Center (CNI), which includes the National Cryptology Center (CCN).

**Royal Decree 421/2004, 12th of March**, regulates and defines the scope and functions of CCN.

## Explanation of Reasons (Law 11/2002)

- Spanish society asks for efficient, specialized and modern Intelligence Services, able to face up to the new challenges of the present national and international scenario, ruled by the principles of control and full compliance with the legal system
- …new challenges for intelligence services that come from the emerging risks, that this law try to cover when defining the functions of the Center…

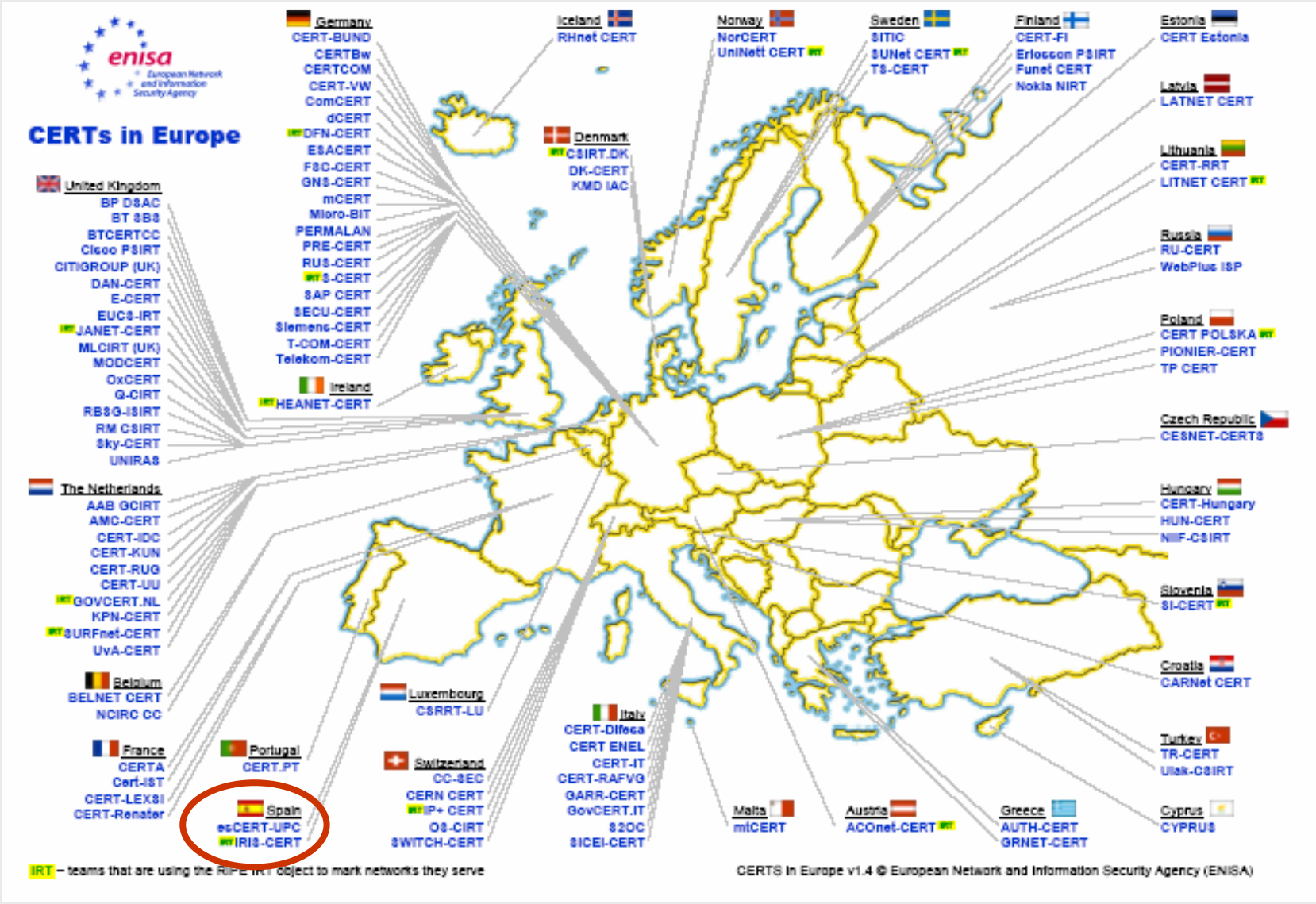
# National Intelligence Center (Law 11/2002)



# CCN Functions (RD 421/2004)

- **Prepare and disseminate** norms, instructions, guides and recommendations to guarantee the CIS Security of Public Authorities.
- **Train** civil servants specialized in CIS Security.
- Set the **certification body** of the Spanish Evaluation and Certification Scheme of application to products and systems under its responsability.
- **Assess and accredit** the capability of crypto products and CIS systems (that include crypto media) to deal with information in a secure way.
- Coordinate the promotion, development, acquistion, operation and use of **security technologies** of systems above-mentioned.
- Ensure for the compliance with the rules concerning with **classified information** under its competence scope (CIS Systems)
- Establish the necessary **relations** and sign the pertinent agreements with similar organizations from other countries.
- To carry out the above-mentioned functions, the necessary Coordination with the National Comissions to whom laws give the responsibilities in the area of Information and Communication Technology Systems

# CERTs in Europe



# CERTs in Spain

- **Iris-CERT**
  - Incidents affecting the security of RedIRIS network centers: Universities and other research centers.
    - Incident Response to its constituency / Forum ABUSES

- **esCERT-UPC**
  - Support to its constituency - Univer. Politécnica de Cataluña in:
    - Incident Response / Altair (Vulnerability Alert Service)
    - Education / Audit / Consultancy/ Business Solutions

- INTECO
  - Provides the following security services:
    - CERT to SMEs and Citizens / Antivirus Early Warning Center(CATA)
    - Security Observatory / Demonstration Center

## CCN-CERT – GOVERNMENTAL INCIDENT RESPONSE

- The main **Goal** of the CCN Computer Security Response Team (CCN-CERT) is to contribute to the improvement of the security level of the Information Systems in the Spanish Public Civil Service.

- Our **Mission** is to be the center of alert and security incident coordination, helping public authorities to respond to threats that affect their information systems in a fast and efficient manner.

## CCN-CERT. Constituency / Authority

- **Our *constituency* is the Spanish Public Civil Service: Central Government, Regional and Local Institutions.**

  - The CCN-CERT ***Authority*** is shared with our constituency, agreeing with them the necessary decisions and actions to fulfill our mission:
    - Royal Decree 421/2004 gives CCN the authority to take the necessary actions to solve incidents on classified systems
    - Collaboration and advice on incident responses in the Spanish Civil Service CIS Systems.

# CCN-CERT …. www.ccn-cert.cni.es

CCN-CERT

# WELCOME

CCN Computer Security

- WELCOME
- ABOUT US
- Alerts/News
- Boletines
- STATISTICS
- RESOURCES

**Destacados**

- Series CCN-STIC
- Guía CCN-STIC 401 - Glosario
- Herramientas PILAR
- Cursos STIC 2007


**Últimas Noticias**

2007-04-26 22:24:01
El CCN presenta en Madrid el CCN-CERT a los rep

2007-04-26 07:32:12
IV Congreso de la Red DerechoTICs

2007-04-25 07:57:15
Las amenazas y vulnerabilidades se incrementaron un 55% en dos años

2007-04-24 00:00:00
Presentación de la Capacidad de Respuesta ante Incidentes de Seguridad de la Información

2007-04-23 00:00:00
El Informe de Fraude Online 2006 confirma la creciente sofisticación de ataques

SEVILLE SPAIN JUNE 2007 19th Annual FIRST Conference
Conference Speaker

FIRST
Improving Security Together

**Solicitud de registro**

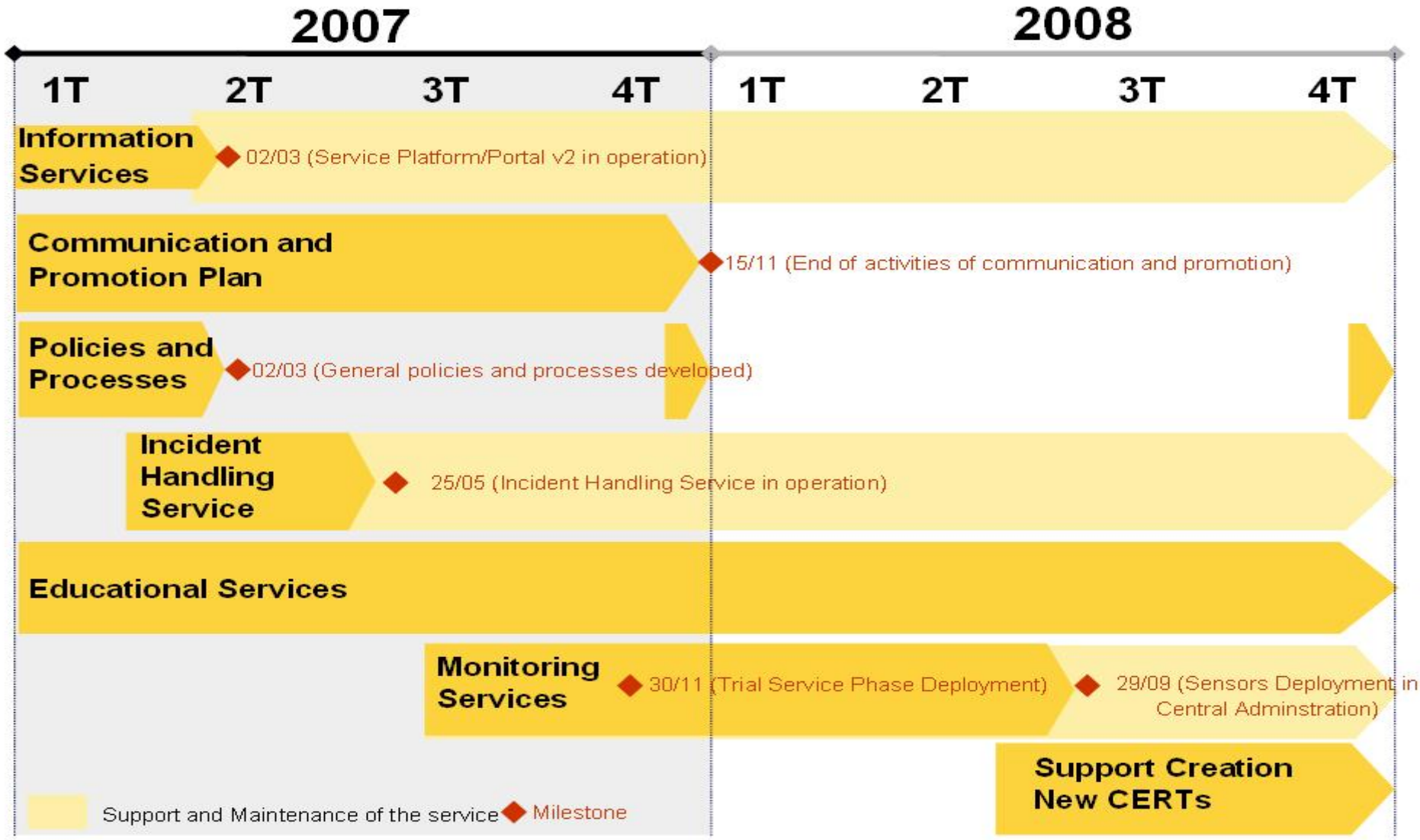
Por favor, cumplimente el siguiente formulario para proceder a su registro en nuestro portal.
CCN-CERT estudiará posibilidad de concederle acceso a la parte restringida.

| | |
|---|---|
| Escriba su nombre: | |
| Escriba sus apellidos: | |
| Provincia: | Álava |
| Cargo: | |
| Organismo: | |
| Tipo: | Local |
| Dirección: | |
| Teléfono: | |
| E-Mail: | |
| Clave: | |
| Verificar clave: | |
| Texto imágen | |

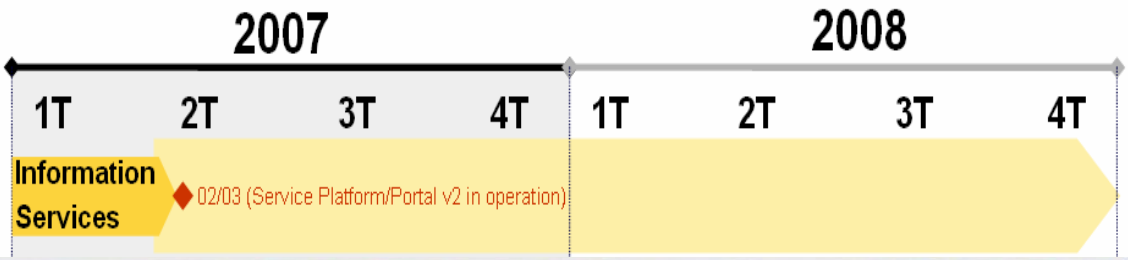
Enviar

Medio

# Roadmap 2007-2008



# I. Information Services




- WEB PORTAL – Main Features:
  - Public Services:
    - Own Vulnerabilities Bulletins
    - Own and Third-party Statistics and Measures
    - Press Releases/ Publications / Tools
    - PILAR Risk Analysis Tool/ Glossary (CCN-STIC 401)
  - Restricted Services for the constituency:
    - CCN-STIC Series / INFOSEC Courses…
    - Incident Notification Interface
    - Restricted Alerts and Vulnerabilities
    - CCN-CERT Monthly Reports
  - Non-Web Publication Media:
    - News disclosure through e-mailing lists
    - Statistics and Other Contents by RSS threads

# CCN-CERT ….

- WELCOME
- ABOUT US
- Alerts/News
- Boletines
- STATISTICS
- RESOURCES

Destacados

- Series CCN-STIC
- Guía CCN-STIC 401 - Glosario
- Herramientas PILAR
- Cursos STIC 2007

SEVILLE SPAIN JUNE 2007 19th Annual FIRST Conference Conference Speaker

FIRST Improving Security Together

## CCN-STIC-600 Guides for Other Environments

- CCN-STIC-601 Hardening (HP-UX 10.20)
- CCN-STIC-602 Hardening (HP-UX 11i)
- CCN-STIC-610 Hardening (Red Hat Linux)
- CCN-STIC-611 Hardening (SuSE linux)
- CCN-STIC-612 Hardening (Debian)
- CCN-STIC-614 Hardening (RedHat Enterprise AS 4 y Fedora 5)
- CCN-STIC-621 Hardening (Sun Solaris 8.0)
- CCN-STIC-622 Hardening (Sun Solaris 9.0/Oracle 8.1.7)
- CCN-STIC-623 Hardening (Sun Solaris 9.0/Oracle 9i)
- CCN-STIC-624 Hardening (Sun Solaris 10/Oracle 9.2)
- CCN-STIC-625 Hardening (Sun Solaris 10/Oracle 10g)
- CCN-STIC-631 Hardening (Oracle 8.1.7/Solaris)
- CCN-STIC-641 Hardening (Routers CISCO)
- CCN-STIC-641 Template for Hardening Routers CISCO
- CCN-STIC-642 Hardening (Switches Enterasys)
- CCN-STIC-642 Template for Hardening Switches Enterasys
- CCN-STIC-671 Hardening (Web Server Apache)
- CCN-STIC-681 Hardening Mail Server (Postfix)

## CCN-STIC-900 Technical Reports

- CCN-STIC-903 Hardening PDA (HP IPAQ 6340)
- CCN-STIC-951 Recommendations for using Ethereal Tool
- CCN-STIC-952 Recommendations for using Nessus Tool
- CCN-STIC-954 Advanced NMAP guide

Search

es

les en PHP

les en

en

# CCN-CERT …. Vulnerability Bulletins

## 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<br>Mozilla Firefox < 1.5.0.11<br>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.

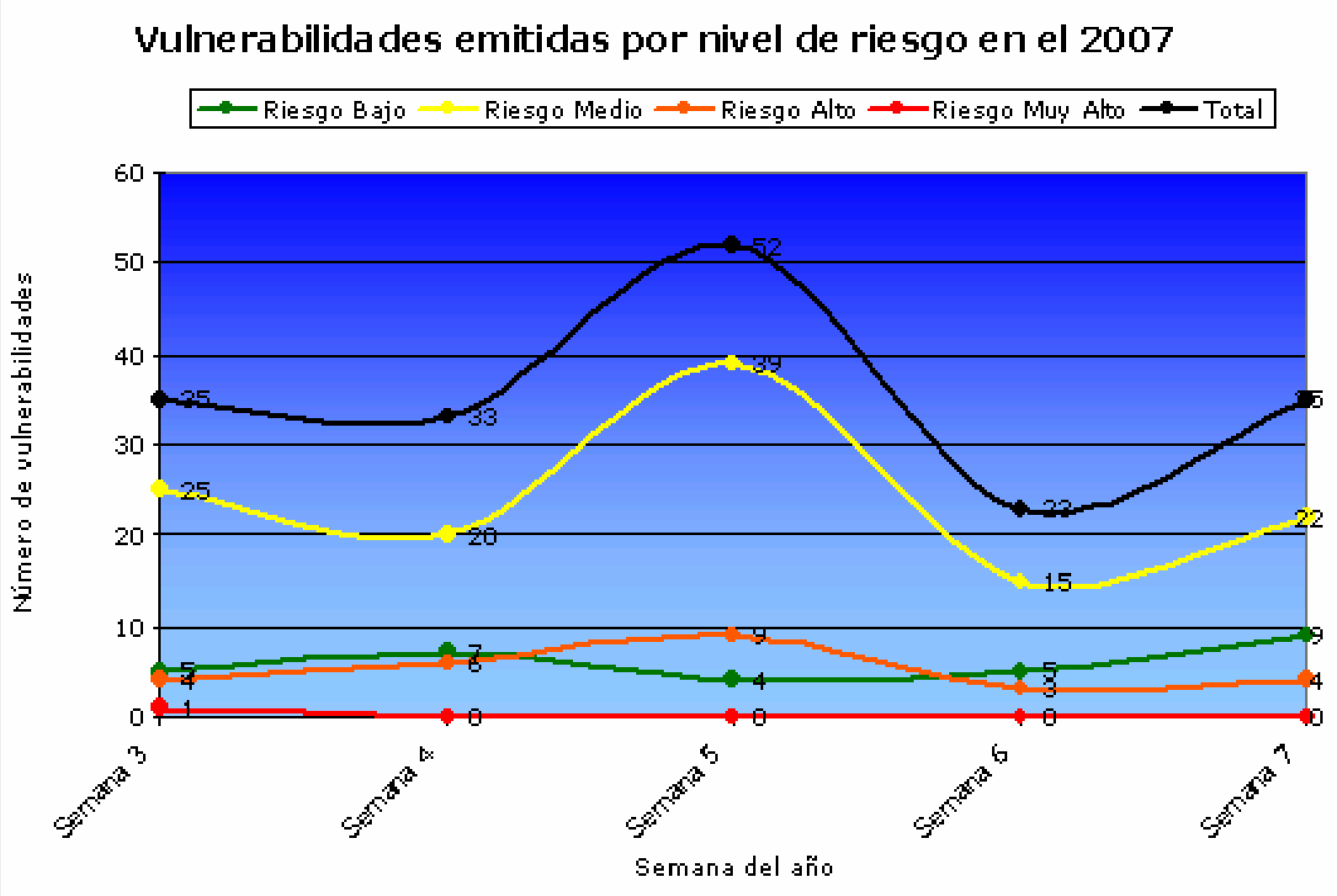
Un atacante remoto podría utilizar esta vulnerabilidad para realizar un escaneo de puertos a las máquinas que hayan detrás del firewall de la víctima.

#### Solución

# EAR / PILAR

- **E**ntorno de **A**nálisis de **R**iesgos (Environment for the Analysis of Risks)
- **PROCEDIMIENTO INFORMATICO Y LOGICO DE ANALISIS DE RIESGOS** (Computer and Logic Procedure for Analysis of Risks)
  - CCN Project→ Developer A.L.H. J. Mañas
  - Validation Commitee: CCN + MAP + FNMT + CCAA…
    - PILAR: exclusive use to public administration / business tool
- **PILAR OBJECTIVE:**
  - **EASY TO USE. Help to unskilled users.** *Suggestions.*
  - **FLEXIBILITY. Adaptable to policies:**
    - **NATIONAL**
    - **ENTERPRISES**
    - **NATO**
    - **EU**
  - **PRIORITIZATION OF SAFEGUARDS.**
- Multilanguage
  - Spanish / English / French / Italian

# Statistics Tables




## CURSOS STIC 2007

Cursos Informativos y de Concienciación en Seguridad:

**III Curso STIC**
- Fechas:
- Fase por Correspondencia: del 5 de marzo al 4 de abril
- Fase de Presente: del 9 al 20 de abril

Cursos Básicos de Seguridad

**II curso Básico STIC - Entornos Windows**
- Fechas: del 7 al 11 de mayo

**II curso Básico STIC - Entornos Linux**
- Fechas: del 21 al 25 de mayo

**II curso Básico STIC - Base de Datos**
- Fechas: del 25 al 29 de junio

**II curso Básico STIC - Infraestructura de Red**
- Fechas: del 2 al 6 de julio

Cursos Específicos de Gestión de Seguridad:

**IV curso de gestión STIC**
- Fechas:
- Fase por Correspondencia: del 17 de septiembre al 11 de octub
- Fase de Presente: del 15 al 26 de octubre

**XIX Curso de Especialidades Criptológicas (CEC)**
- Fechas:
- Fase por Correspondencia: del 4 de septiembre al 10 de noviem
- Fase de Presente: del 12 al 30 de noviembre

Cursos de Especialización en Seguridad:

**IV Curso Acreditación STIC - Entornos UNIX**
- Fechas: del 13 al 22 de junio

**IV Curso Acreditación STIC - Entornos Windows**
- Fechas: del 23 al 27 de abril

**II Curso Acreditación STIC - Entornos Linux**
- Fechas: del 30 de mayo al 8 de junio

**II Curso Acreditación STIC - Redes Inalámbricas**
- Fechas: del 3 al 7 de septiembre

**III Curso Acreditación STIC - Cortafuegos**
- Fechas: del 10 al 14 de septiembre

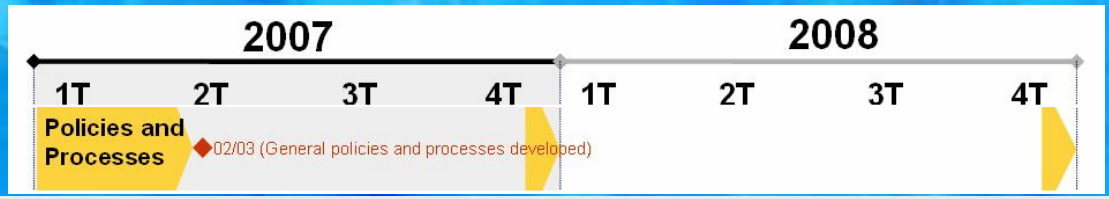
**III Curso Acreditación STIC - Detección de Intrusos**
- Fechas: del 17 al 21 de septiembre

**II Curso Acreditación STIC - Herramientas de Seguridad**
- Fechas: del 24 al 28 de septiembre

**II Curso Acreditación STIC - Inspecciones de Seguridad**
- Fechas: del 1 al 5 de octubre

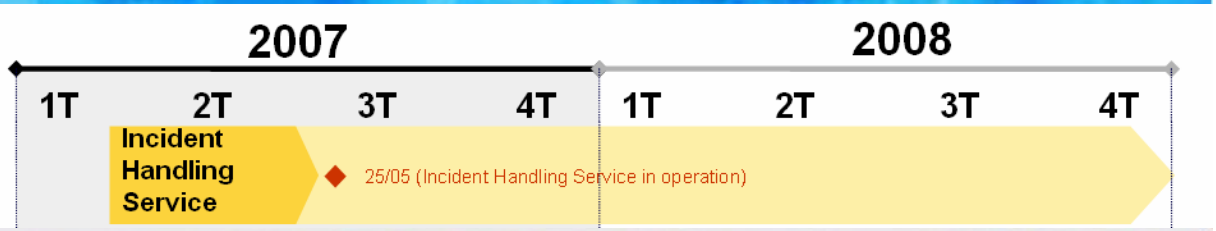
# III. Communication Plan

# IV. Policies and Procedures



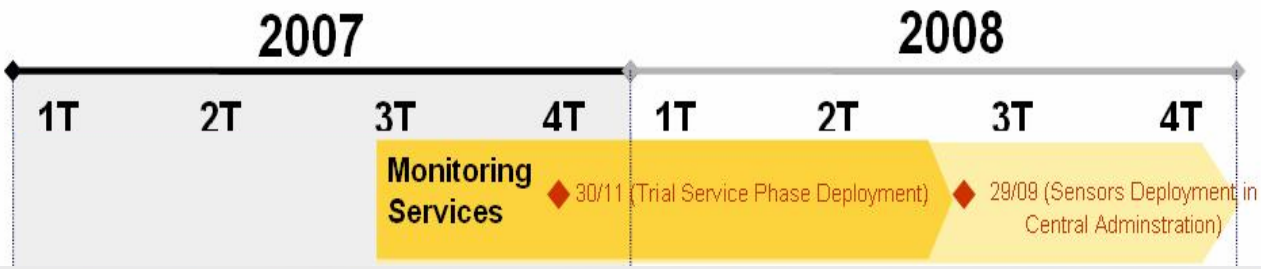

- Main Policies
  - Security Policy
  - Conduct Policy
  - Information Classification
  - Disclosure Policy / Information Dissemination
  - Media Policy
  - Policy versus Human Errors
  - Monitoring Policy
- Main Procedures
  - Operating Procedure of the Handling Incident Platform and applications

# V. Handling Incidents



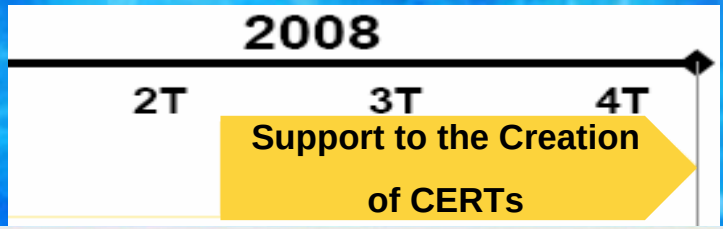

- Procedures:
  - Incident Response Plan (IRP)
  - Incident Handling Processes:
    - Reception and Evaluation
    - Register / Identification and Analysis
    - Notification / Escalation / Contention
    - Collect Evidences
    - Recovery
  - Post-incidents Procedures
  - IRT Platform Operating Procedures
- Incident Research Platform
  - Artifact Analysis
  - Forensic Analysis
- Incident Handling Tool

# VI. Monitoring Services




- 2007… Types of sensors assessment to deploy.
  - 3 sensors
  - Types of sensors:
    - Logs Analysis Agents.
    - IDS Appliances…Traffic Analysis.
- 2008… Sensors Deployment
  - Roadmap coordinated with Civil Service Ministry…. Central and Regional Governments
  - Access to the INTERNET / INTRANET of Central Government
  - Benefits:
    - Own statistics and measures
    - Attack Detections

# VII. Promoting new CERT,s




- Objectives
  - Offer information, training and tools in order to our constituency could set up their own CERTs, allowing CCN-CERT to operate as a coordinator of CERTs at governmental level
- Main Activities
  - CERTs Deployment Plan
    - Design guides and tools to set and operate CERTs
    - Design and development of a section in the web portal to our constituency
  - Educational Plan
    - Creating and Managing CERTs Course

# CCN-CERT SERVICES

## REACTIVE SERVICES

- ALERTS AND ADVISORIES.
- INCIDENT HANDLING
  - Classified Systems
- VULNERABILITY HANDLING
- MALCODE ANALYSIS

## MANAGEMENT SERVICES

- RISK ANALYSIS
- SECURITY CONSULTING
- AWARNESS AND TRAINING:.
  - STIC Courses
  - Seminaries / workshops
  - Discussion Forums
- PRODUCT EVALUATION AND CERTIFICATION:
  - COMMON CRITERIA / TEMPEST / CRYPTO.

## PROACTIVE SERVICES

- ANNOUNCEMENTS. Only authorized users.
- SECURITY AUDITS OR ASSESSMENTS
  - Classified Systems
- CONFIGURATION AND MAINTENANCE OF SECURITY ELEMENTS
- DEVELOPMENT OF SECURITY TOOLS
- INTRUSION DETECTION SYSTEMS
- SECURITY-RELATED INFORMATION DISSEMINATION.
- QUALITY CERTIFICATION

RD
2006
2007
200?

## CCN-CERT. Sources

- Open Sources
- Other Organism Sources
  - FIRST /TERENA TF-CSIRT
  - Other CERT,s
    - CPNI (UNIRAS) / CERTA / NCIRC
    - esCERT /IRIS-CERT / INTECO
  - Other companies / forums
    - SANS / SECURITY FOCUS / HISPASEC / TB-SECURITY / S21SEC / GARTNER …
  - Other services
- Own Sources
  - Incident Notifications
  - **Sensors Deployment**

# CCN-CERT. Conclusions

- **From CCN knowledgment and expertise on CIS Security …**
  - ... Improve security on CIS Government Systems
  - … Government Capability on Incident Response
    - CCN-CERT
- **Handling Computer Incidents by:**
  - Security-Related Information Services
  - Research, Training and Awareness
  - Support on Incident Response
- **Relationships:**
  - Public Civil Service Organisms
  - CERTs
  - ISPs, Hosting, DNS,...


# Thank you

- E-Mails
  - info@ccn-cert.cni.es
  - ccn@cni.es
  - organismo.certificacion@cni.es
- Websites:
  - www.ccn.cni.es
  - www.ccn-cert.cni.es
  - www.oc.ccn.cni.es