



Centro
Criptológico
Nacional



www.ccn-cert.cni.es



www.oc.ccn.cni.es

Foros DINTEL de AA.PP.

Seguridad vs Ciberdelincuencia

*martes, 20 de septiembre ' 2011 * Casino de Madrid (C/ Alcalá, 15)*

SIN CLASIFICAR

CIBERDELITO

El término "ciberdelito" abarca muy diversos tipos de delitos. Los delitos reconocidos comprenden una gran variedad de infracciones, lo que dificulta su tipología o clasificación.

Un sistema de clasificación interesante está definido en el Convenio sobre la Ciberdelincuencia del Consejo de Europa en el que se distinguen cuatro tipos diferentes de infracciones:

- delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos
- delitos relacionados con el contenido
- delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines
- delitos informáticos

CIBERDELITO

- delitos contra la confidencialidad, la integridad y la disponibilidad de los datos y sistemas informáticos
 - Acceso ilícito
 - Piratería de sistemas y programas
 - Espionaje de datos
 - Intervención ilícita
 - Manipulación de datos
 - Ataques contra la integridad del sistema
- delitos relacionados con el contenido
 - Pornografía infantil
 - Racismo, lenguaje ofensivo, exaltación de la violencia
 - Juegos ilegales y juegos en línea
 - Difamación e información falsa
 - Correo basura y amenazas conexas

CIBERDELITO

- delitos relacionados con infracciones de la propiedad intelectual y de los derechos afines
 - Delitos en materia de derechos de autor
 - Delitos en materia de marcas
- delitos informáticos
 - Fraude y fraude informático (manipulación persona-máquina)
 - Falsificación informática (documentos, correos, imágenes, etc)
 - Robo de identidad
 - Utilización indebida de dispositivos

¿CIBERTERRORISMO?

Los terroristas recurren a las TIC y a Internet para los siguientes fines:

- propaganda;
- recopilación de información;
- preparación de ataques al mundo real;
- publicación de material de captación y capacitación;
- comunicaciones;
- financiación de actividades terroristas;
- ataques contra infraestructuras críticas

CIBERDELINCUENCIA. MOTIVACION

- ROBO DE INFORMACIÓN
- BENEFICIO ECONÓMICO
- PROVOCACIÓN DE DAÑOS
- MOTIVACIÓN SOCIAL O POLÍTICA

CIBERDELINCUENCIA. MOTIVACION

- **ROBO DE INFORMACIÓN**

- Robo de información de los sistemas de las AAPP o de sistemas estratégicos.
- Robo de información corporativa relevante o de propiedad intelectual de empresas e instituciones.
- Robo de información de carácter personal.
- Robo de identidades electrónicas

Todo ello mediante técnicas de Phishing, intrusión, penetración y acceso no autorizado

CIBERDELINCUENCIA. MOTIVACION

- BENEFICIO ECONÓMICO
 - Ataques a los sistemas de pago e infraestructuras bancarias.
 - ♦ Duplicación de tarjetas de pago, redireccionamiento a servidores fraudulentos
 - Ataques a los usuarios de Banca Online.
 - ♦ Troyanos tipo Zeus, SpyEye, Carberp, etc
 - Fraudes online
 - ♦ Esquemas de fraude tipo 419 Scam, Nigerian, Ponzi, etc
- PROVOCACIÓN DE DAÑOS
 - Websites defacement
 - Ataques DDoS
 - Ataques a sistemas SCADA

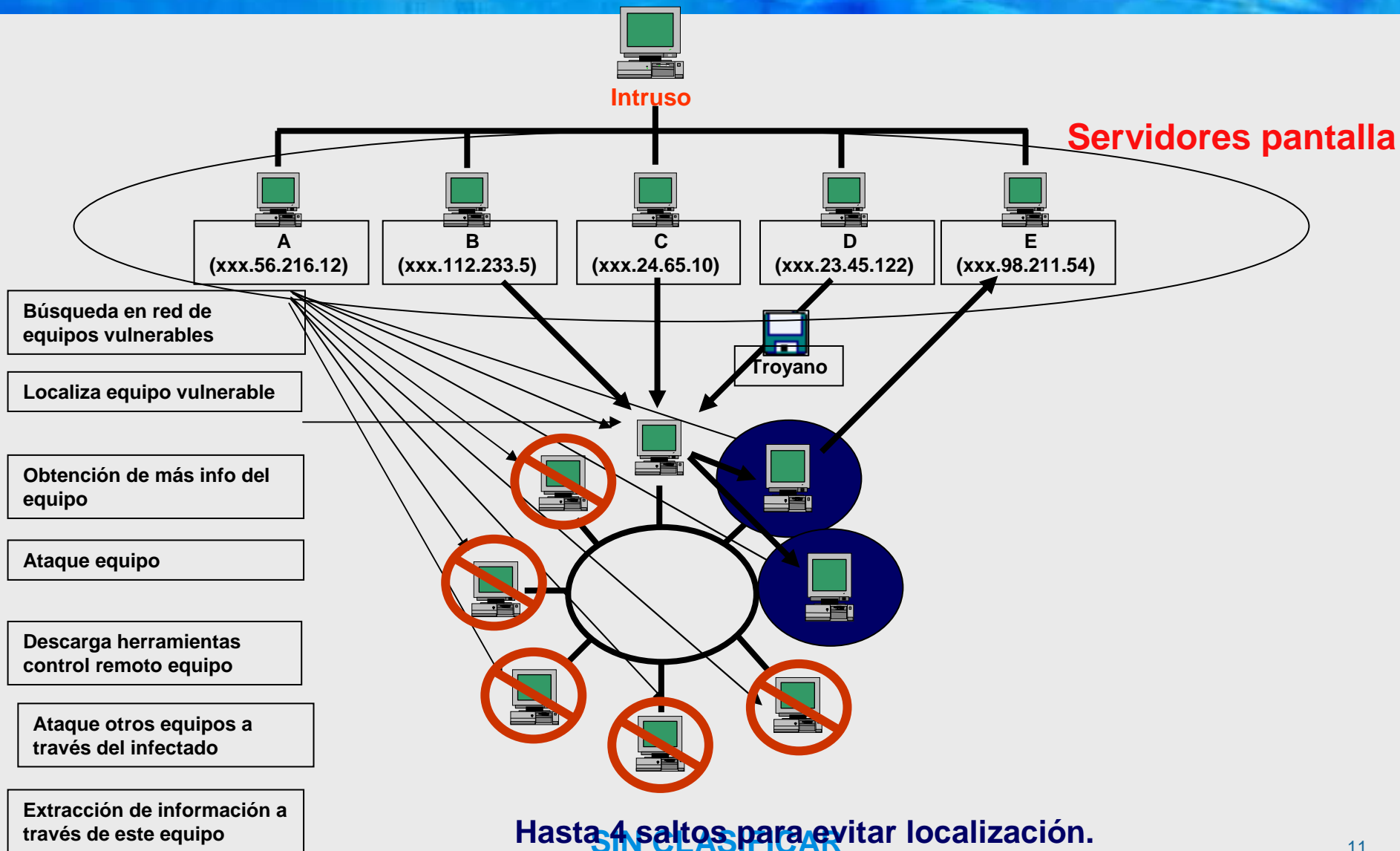
CIBERDELINCUENCIA. MOTIVACION

- MOTIVACIÓN SOCIAL O POLÍTICA
 - Protestas en red
 - ♦ Bloqueo de servicios
 - Ataques DDoS
 - Web Defacement

CIBERDELINCUENCIA. CAUSAS DEL EXITO

- Rentabilidad coste-beneficio
- Protección inadecuada e incompleta de los sistemas informáticos
- Aparición de herramientas informáticas que automatizan los ataques
- El aumento del parque de ordenadores privados a nivel mundial (zombies de redes botnets)

INTRUSIÓN GENÉRICA / COMO SE OCULTA EL ATACANTE



SIN CLASIFICAR

Amenazas 2010. Código Dañino

• **34% del código detectado en toda la historia.**

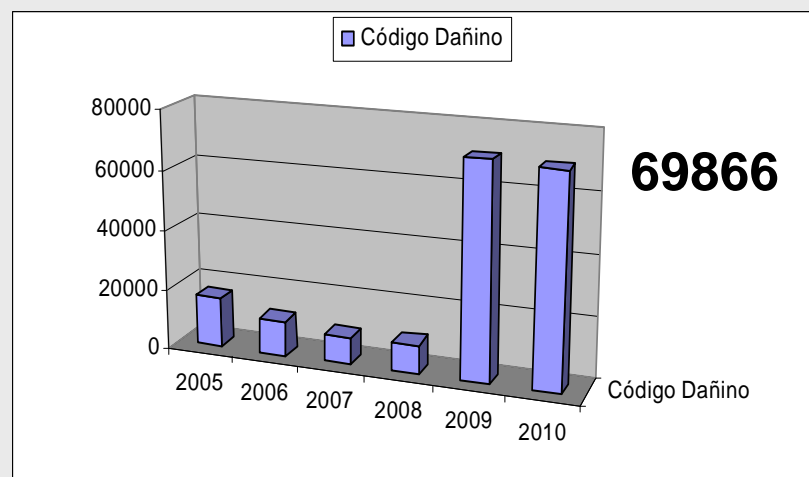
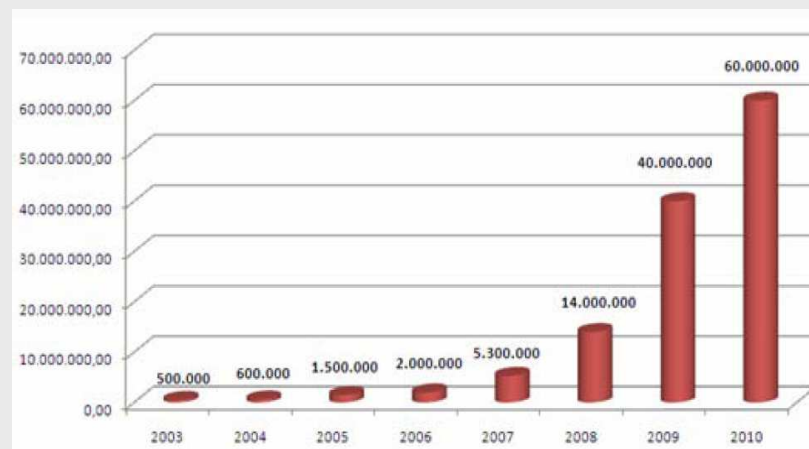
- Rentabilidad de los ataques
- Difícil atribución.
- **Implicación de los gobiernos**

Amenaza Persistente Avanzada (APT)

- ◆ Operación Aurora (Enero 2010)
- ◆ Stuxnet (Julio 2010)

Mcafee:

Targeted cyberespionage or cybersabotage attack that is carried out under the sponsorship of a nation-state for something other than a pure financial/criminal reason or political protest



Características APT (Advanced Persistent Threat)

- **Patrón de ataque**

- Escaso número de objetivos (10-100)

- Objetivos seleccionados. Ingeniería social

- Emplean exploits basados en vulnerabilidades recientes / día cero

- No es detectado por el SW antivirus / IDS / Firewall de los equipos
(No dispone de firma)

- Empleo de mecanismos de cifra resistentes al análisis

- Permanece sin ser detectado por MESES. Para la explotación / actualización usa **protocolos autorizados**

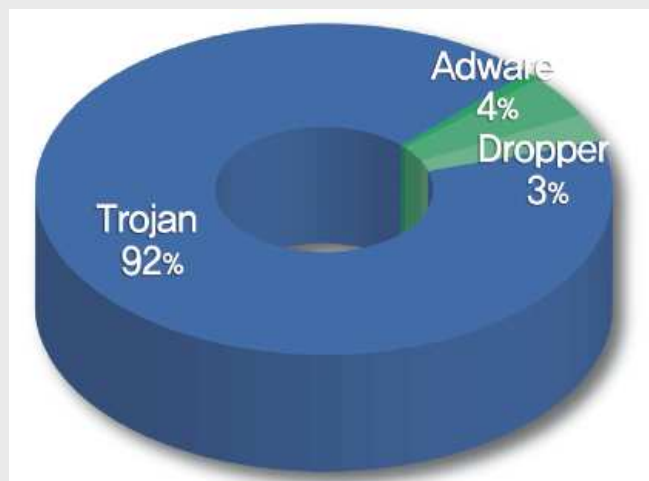


Capacidad de defensa ante APT

- Nivel de detección no superior al 25%
- Reacción lenta en la actualización
- Solo detectan lo que ven.
 - ◆ APT no reportado. No dispone de firma.
 - ◆ Parecen aplicaciones legítimas

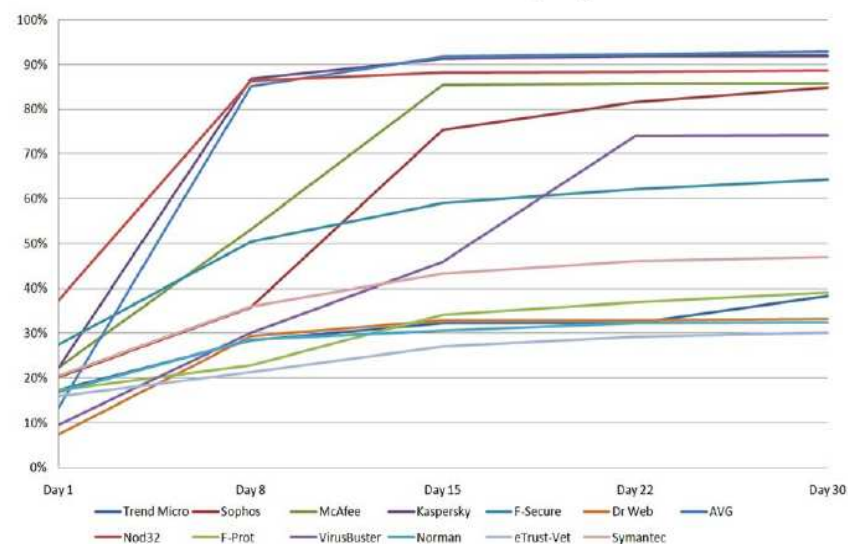
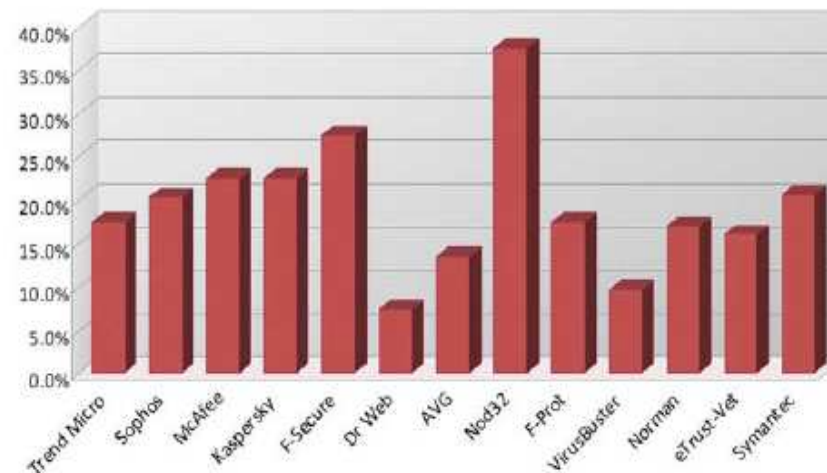
- MONITORIZACIÓN DE SISTEMA

- ◆ Despliegue de IDS.
- ◆ Firewall / Proxy
- ◆ Análisis de protocolos autorizados



SIN CLASI

AV Solution Detection Rates



Ejemplo ataque troyano adaptado objetivo

- 24.04.2010. Ataque con troyano dirigido
 - **From: 'zhanat shaimerdenov <shaimerdenov@hotmail.com>'**
 - **To:**
 - ♦ **@maec.es**
 - ♦ **@oc.mde.es**
 - ♦ **@presidencia.gob.es**
- Características:
 - No detectable por antivirus..... (22%)
 - Vulnerabilidad próxima a día CERO
 - Adjunto ADOBE



Ejemplo ataque troyano adaptado objetivo

Informe realizado por el Sistema Multiantivirus del Portal CCN-CERT.
Resultado del análisis al fichero the right.pdf:

MOTOR	RESULTADO
AhnLab-V3	Código malicioso no detectado
Avast	PDF:CVE-2010-0188
AVG	Código malicioso no detectado
BitDefender	Exploit.PDF-Name.Gen
eTrust-Vet	Código malicioso no detectado
ClamAV	Código malicioso no detectado
DrWeb	Código malicioso no detectado
eSafe	Código malicioso no detectado
Fortinet	Código malicioso no detectado
F-Prot	Código malicioso no detectado
Ikarus	Exploit.JS.Pdfka
Kaspersky	Exploit.JS.Pdfka.bzh
McAfee	Código malicioso no detectado
NOD32	Código malicioso no detectado
Norman	Código malicioso no detectado
Panda9	Código malicioso no detectado
CAT-QuickHeal	Código malicioso no detectado
Rising	Código malicioso no detectado
Sophos	MalVPDFEx-D
Sunbelt	Código malicioso no detectado
TheHacker	Código malicioso no detectado
VBA32	Código malicioso no detectado
VirusBuster	Código malicioso no detectado

Informe realizado por el Sistema Multiantivirus del Portal CCN-CERT.
Resultado del análisis al fichero 705c17b8612bf422bea47db383c639a8:

MOTOR	RESULTADO
AhnLab-V3	Código malicioso no detectado
Avast	Código malicioso no detectado
AVG	Código malicioso no detectado
BitDefender	Código malicioso no detectado
eTrust-Vet	Código malicioso no detectado
ClamAV	Código malicioso no detectado
DrWeb	Código malicioso no detectado
eSafe	Código malicioso no detectado
Fortinet	Código malicioso no detectado
F-Prot	Código malicioso no detectado
Ikarus	Código malicioso no detectado
Kaspersky	Código malicioso no detectado
McAfee	Código malicioso no detectado
NOD32	Código malicioso no detectado
Norman	Código malicioso no detectado
Panda9	Código malicioso no detectado
CAT-QuickHeal	Suspicious file
Rising	Suspicious) - DNASca
Sophos	Código malicioso no detectado
Sunbelt	TrojAgent-MS
TheHacker	Código malicioso no detectado
VBA32	Código malicioso no detectado
VirusBuster	Código malicioso no detectado

- **Se ha detectado un incremento considerable de los ataques con código dañino**
 - ◆ Dirigido a objetivos seleccionados
 - ◆ Difícil detección (empleo de protocolos autorizados)
 - Externas ... Navegación Web
 - InternasSMB / RPC
 - ◆ Evolución constante (cambio continuo de firmas)
 - ◆ Difícil / imposible localización del origen
 - ◆ Capacidad de colonización de la red objetivo

- **Deficiente monitorización de la actividad de la red desde el punto de vista de seguridad.**
 - ◆ Escaso análisis de registros
 - ◆ Escasa monitorización del tráfico en búsqueda de código dañino

- **Escasa concienciación de los usuarios.**

- **Valorar el riesgo del manejo de información sensible en redes con conexión a INTERNET. Implantar salvaguardas adicionales.**

Actividad de código dañino por País

Overall Rank	Country	Overall Proportion	Malicious Code Rank	Spam Host Rank	Command and Control Server Rank	Phishing Host Rank	Bot Rank	Attack Rank
1	United States	31%	1	1	1	1	2	1
2	China	10%	3	2	4	8	1	2
3	Germany	7%	7	3	3	2	4	3
4	France	4%	9	4	14	4	3	4
5	United Kingdom	4%	4	13	9	3	6	6
6	South Korea	4%	12	9	2	9	11	9
7	Canada	3%	5	23	5	7	10	5
8	Spain	3%	13	5	15	16	5	7
9	Taiwan	3%	8	11	6	6	7	11
10	Italy	3%	2	8	10	14	12	10

Table 2. Malicious activity by country

Source: Symantec Corporation

La lucha contra el ciberdelito exige un enfoque global.

Para lograr CIBERSEGURIDAD se deben realizar esfuerzos en las cinco áreas de trabajo siguientes:

- 1) medidas legales
- 2) medidas técnicas y de procedimiento
- 3) estructuras institucionales
- 4) creación de capacidades
- 5) cooperación internacional



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

SIN CLASIFI

CCN CENTRO CRIPTOLÓGICO NACIONAL

Inicio Normas Certificación Acreditación Formación Gestión de Incidentes

CCN

- ¿Quiénes Somos?
- Carta del SED
- Ámbito de actuación
- Contactar

Organismo de Certificación

Capacidad de Respuesta a Incidentes

RELACIONES INSTITUCIONALES

redtrabaj@

CERTIFICACIÓN CRIPTOLÓGICA
Productos capaces de proteger la información clasificada Nacional

CERTIFICACIÓN TEMPEST
Equipos y sistemas protegidos frente a las amenazas electro magnéticas.

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

NORMAS INSTRUCCIONES GUÍAS RECOMENDACIONES

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

tion Scheme operates the Act 11/2002, Act the Royal Decree

olic parties that may ll as under request of to certify the security subject to be included

se of the requirements ablished in Chapter three tion security

ogy products in llowing the evaluation es for the security

bro. s/n. 28023-MADRID. smo.certificacion@cni.es

CCN-CERT seguridad tic

capacidad de respuesta ante incidentes de seguridad de la información

PRINCIPAL
SOBRE NOSOTROS
INCIDENTES
ACTUALIDAD
ALERTAS
HERRAMIENTAS
RECURSOS
NOTICIAS
PREFERENCIAS

Curso on-line de Seguridad de la Información

SISTEMA MULTANTIVIRUS MAV

MENCIONES

Accredited by TRUSTED

EGC group

ÚLTIMAS VULNERABILIDADES

- CCN-CERT-1001-05047 Múltiples vulnerabilidades en Kerberos
- CCN-CERT-1001-05046 Múltiples vulnerabilidades en PowerDNS Recursor
- CCN-CERT-1001-05045 Múltiples vulnerabilidades en Linux kernel

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

Los ataques sortos, víctimas propicias a los ataques de phishing - 22/01/2010

IPv4 se agota y la llegada de IPv6 se convierte en urgente - 21/01/2010

Microsoft lanzará un parche de emergencia para Internet Explorer 6 - 20/01/2010

El CCN-CERT no se hace responsable del contenido de las noticias aquí publicadas. Al tratarse de enlaces externos, la información recogida depende exclusivamente de la fuente de la noticia o del autor de la misma.

ÚLTIMOS INFORMES DE SEGURIDAD

- CCN-CERT IA-03/09 Seguridad en la nube ("Cloud computing")
- CCN-CERT ID-07/09 Informe de Código Dañino: Botnet Mariposa/Butterfly
- CCN-CERT IS-23/09 Informe de Actualidad STIC

HERRAMIENTA PILAR

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

CURSOS CCN-STIC

- VI Curso de Gestión STIC del 21 de septiembre al 30 de octubre
- II Curso STIC - Búsqueda de Evidencias y Control de Integridad del 29 de septiembre al 2 de octubre
- XXI Curso de Especialidades Criptológicas (CEC) del 31 de agosto al 4 de diciembre

COMUNICADOS CCN-CERT

El CCN, en colaboración con la Xunta de Galicia, presenta en Santiago su Servicio de Respuesta a Incidentes - 30/12/2009

Más de sesenta personas provenientes de la AAPP asistieron a la III Jornada STIC organizada por el CCN-CERT - 18/12/2009

El CCN-CERT amplía su oferta educativa para el personal de la AAPP con una nueva plataforma de e-learning - 28/10/2009

CATÁLOGO DE SERVICIOS

descárgate aquí CCN-CERT

Presentación del CCN-CERT en Galicia

III Jornada STIC CCN-CERT Las AAPP ante las nuevas amenazas

¿Por qué debería registrarme?

¿Quieres notificar un incidente?

AVISO LEGAL CONTACTO MAPA WEB DECLARACIÓN DE ACCESIBILIDAD

© 2009 Centro Criptológico Nacional - C/Argentina s/n 28023 MADRID