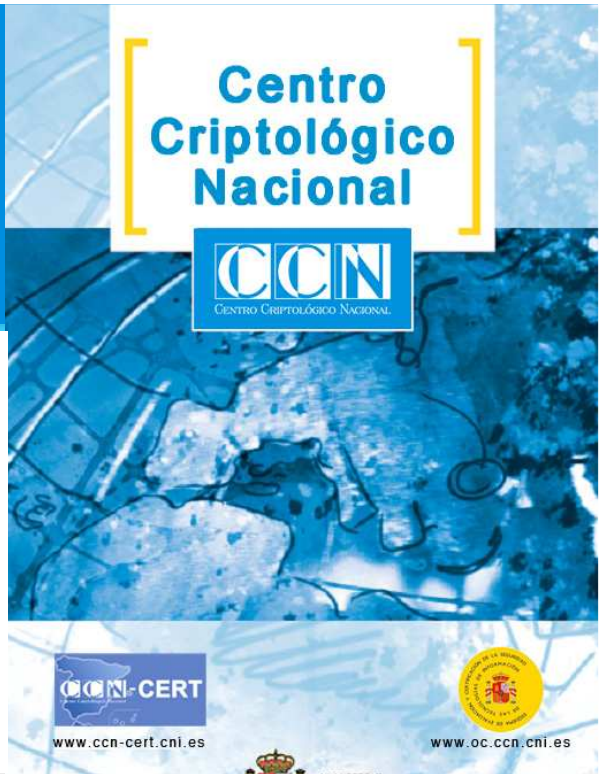


Foros DINTEL de AA.PP.

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

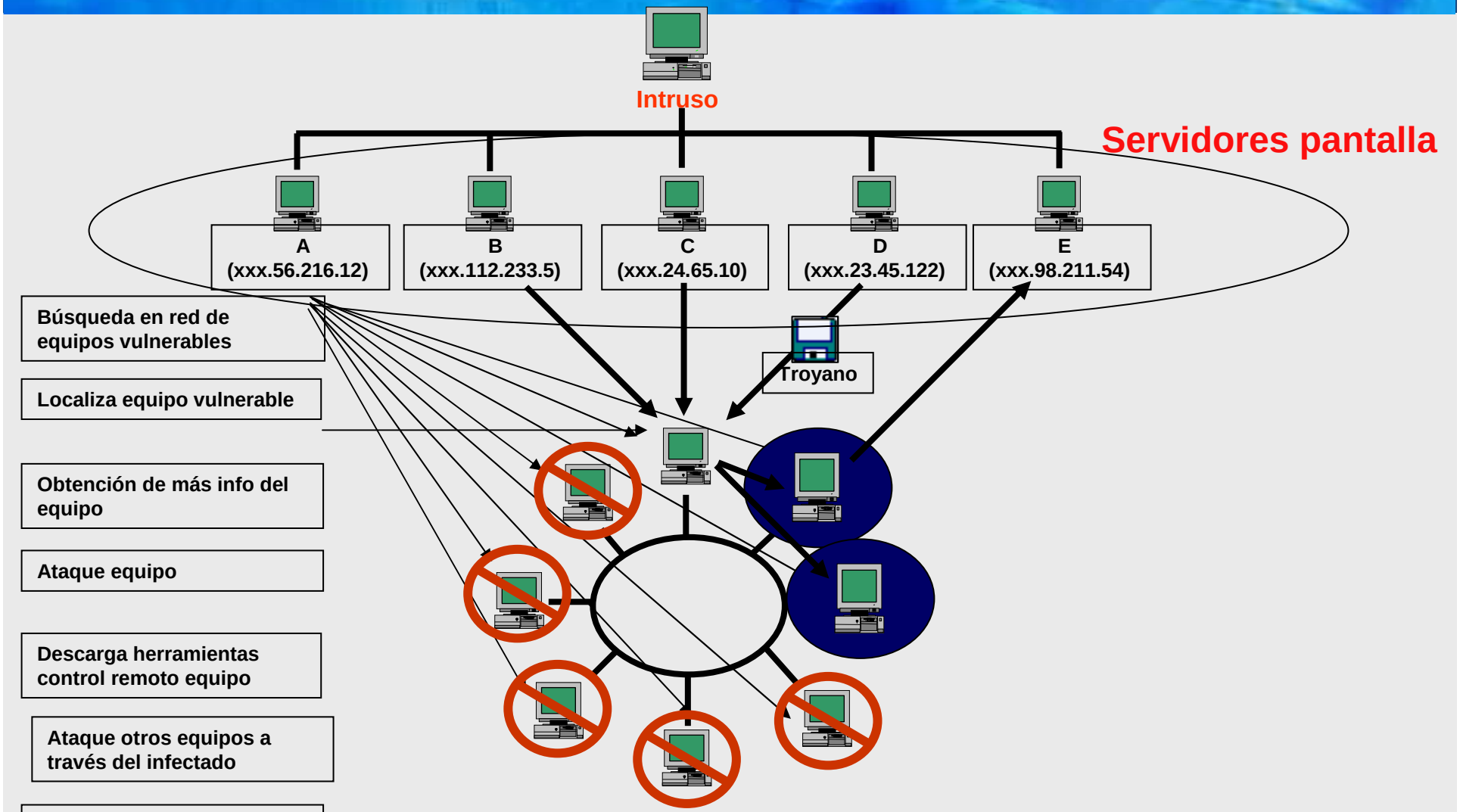
CIBERDELINCUENCIA. MOTIVACION

- 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)

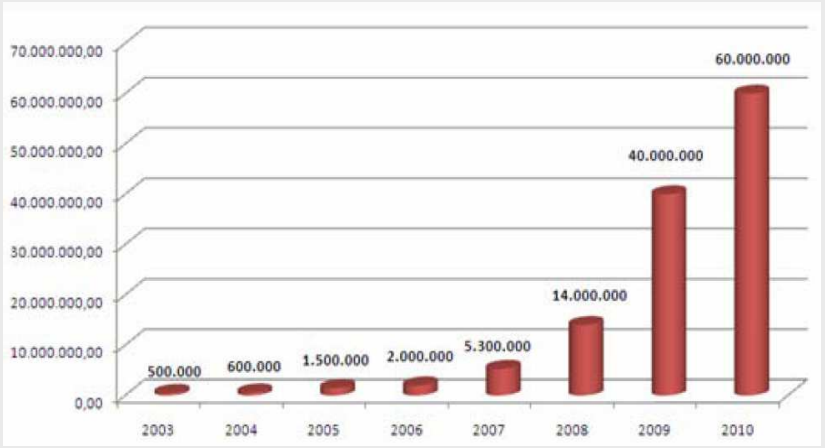
INTRUSIÓN GENÉRICA / COMO SE OCULTA EL ATACANTE



Hasta 4 saltos para evitar localización.

Amenazas 2010. Código Dañino

- **34% del código detectado en toda la historia.**
  - Rentabilidad de los ataques
  - Difícil atribución.
  - **Implicación de los gobiernos**

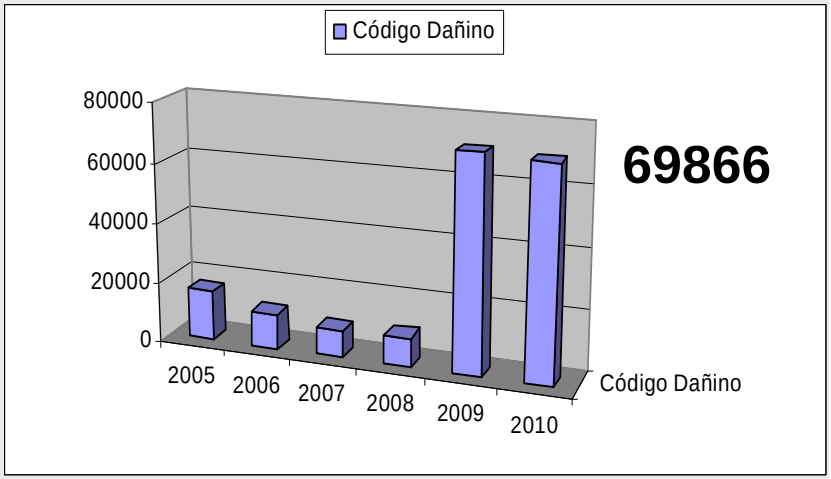


Amenaza Persistente Avanzada (APT)

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

Mcafee:

Targeted cyberespionge 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



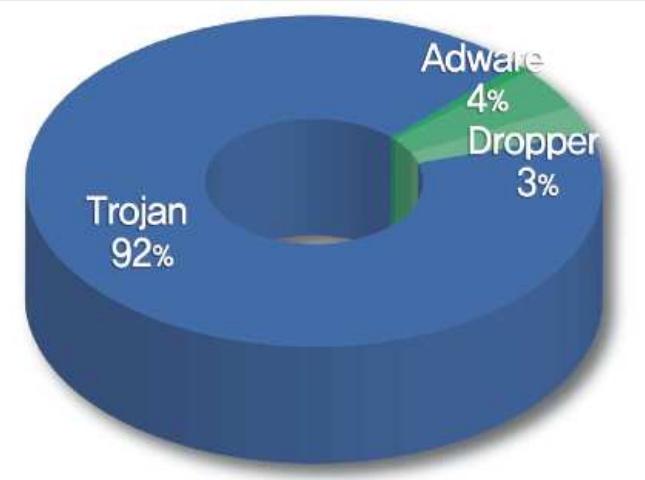
Características APT (Advanced Persistent Threat)

- **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**

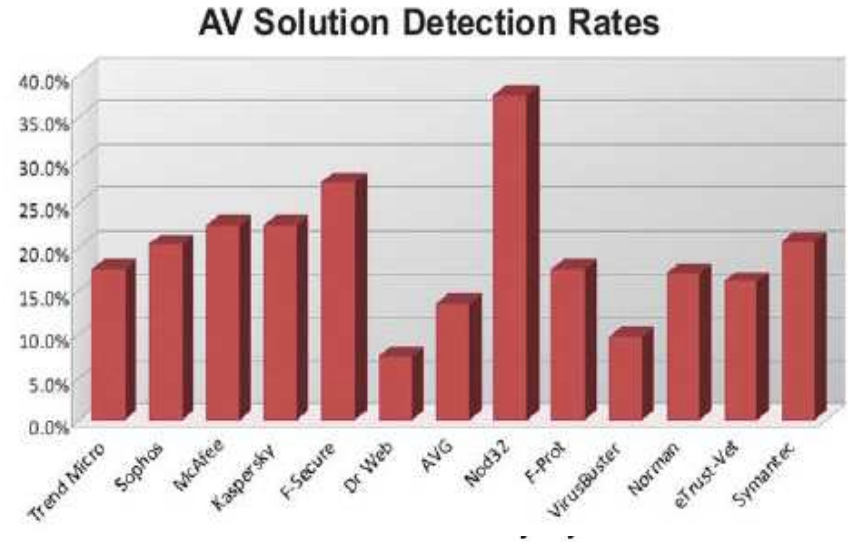
Capacidad de defensa ante APT

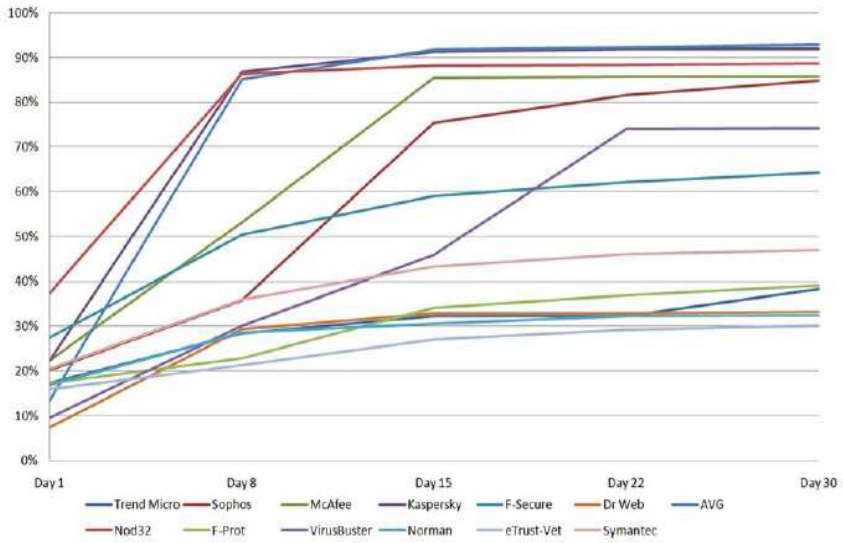
- Nivel de detección no superior al 25%
- Reacción lenta en la actualización
- Solo detectan lo que ven.
  - APT no reportado. No dispone de firma.
  - Parecen aplicaciones legítimas

- **MONITORIZACIÓN DE SISTEMA**
  - **Despliegue de IDS.**
  - **Firewall / Proxy**
  - **Análisis de protocolos autorizados**



SIN CLASI





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 anÃ¡lisis al fichero the right.pdf:

MOTOR	RESULTADO
AhnLab-V3	CÃ³digo malicioso no detectado
Avast	PDF:CVE-2010-0188
AVG	CÃ³digo malicioso no detectado
BitDefender	Exploit.PDF-Name.Gen
eTrust-Vet	CÃ³digo malicioso no detectado
ClamAV	CÃ³digo malicioso no detectado
DrWeb	CÃ³digo malicioso no detectado
eSafe	CÃ³digo malicioso no detectado
Fortinet	CÃ³digo malicioso no detectado
F-Prot	CÃ³digo malicioso no detectado
Ikarus	Exploit.JS.Pdfka
Kaspersky	Exploit.JS.Pdfka.bzh
McAfee	CÃ³digo malicioso no detectado
NOD32	CÃ³digo malicioso no detectado
Norman	CÃ³digo malicioso no detectado
Panda9	CÃ³digo malicioso no detectado
CAT-QuickHeal	CÃ³digo malicioso no detectado
Rising	CÃ³digo malicioso no detectado
Sophos	Mal/PDFEx-D
Sunbelt	CÃ³digo malicioso no detectado
TheHacker	CÃ³digo malicioso no detectado
VBA32	CÃ³digo malicioso no detectado
VirusBuster	CÃ³digo malicioso no detectado

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

MOTOR	RESULTADO
AhnLab-V3	CÃ³digo malicioso no detectado
Avast	CÃ³digo malicioso no detectado
AVG	CÃ³digo malicioso no detectado
BitDefender	CÃ³digo malicioso no detectado
eTrust-Vet	CÃ³digo malicioso no detectado
ClamAV	CÃ³digo malicioso no detectado
DrWeb	CÃ³digo malicioso no detectado
eSafe	CÃ³digo malicioso no detectado
Fortinet	CÃ³digo malicioso no detectado
F-Prot	CÃ³digo malicioso no detectado
Ikarus	CÃ³digo malicioso no detectado
Kaspersky	CÃ³digo malicioso no detectado
McAfee	CÃ³digo malicioso no detectado
NOD32	CÃ³digo malicioso no detectado
Norman	CÃ³digo malicioso no detectado
Panda9	Suspicious file
CAT-QuickHeal	Suspicious) - DNASca
Rising	CÃ³digo malicioso no detectado
Sophos	Troj/Agent-MSC
Sunbelt	CÃ³digo malicioso no detectado
TheHacker	CÃ³digo malicioso no detectado
VBA32	CÃ³digo malicioso no detectado
VirusBuster	CÃ³digo malicioso no detectado

- **Se ha detectado un incremento considerable de los ataque con código dañino**
  - **Dirigido a objetivos seleccionados**
  - **Difícil detección (empleo de protocolos autorizados)**
    - **Externas … Navegación Web**
    - **Internas …..SMB / 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

CIBERSEGURIDAD

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

CENTRO CRIPTOLÓGICO NACIONAL

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 CLASIF