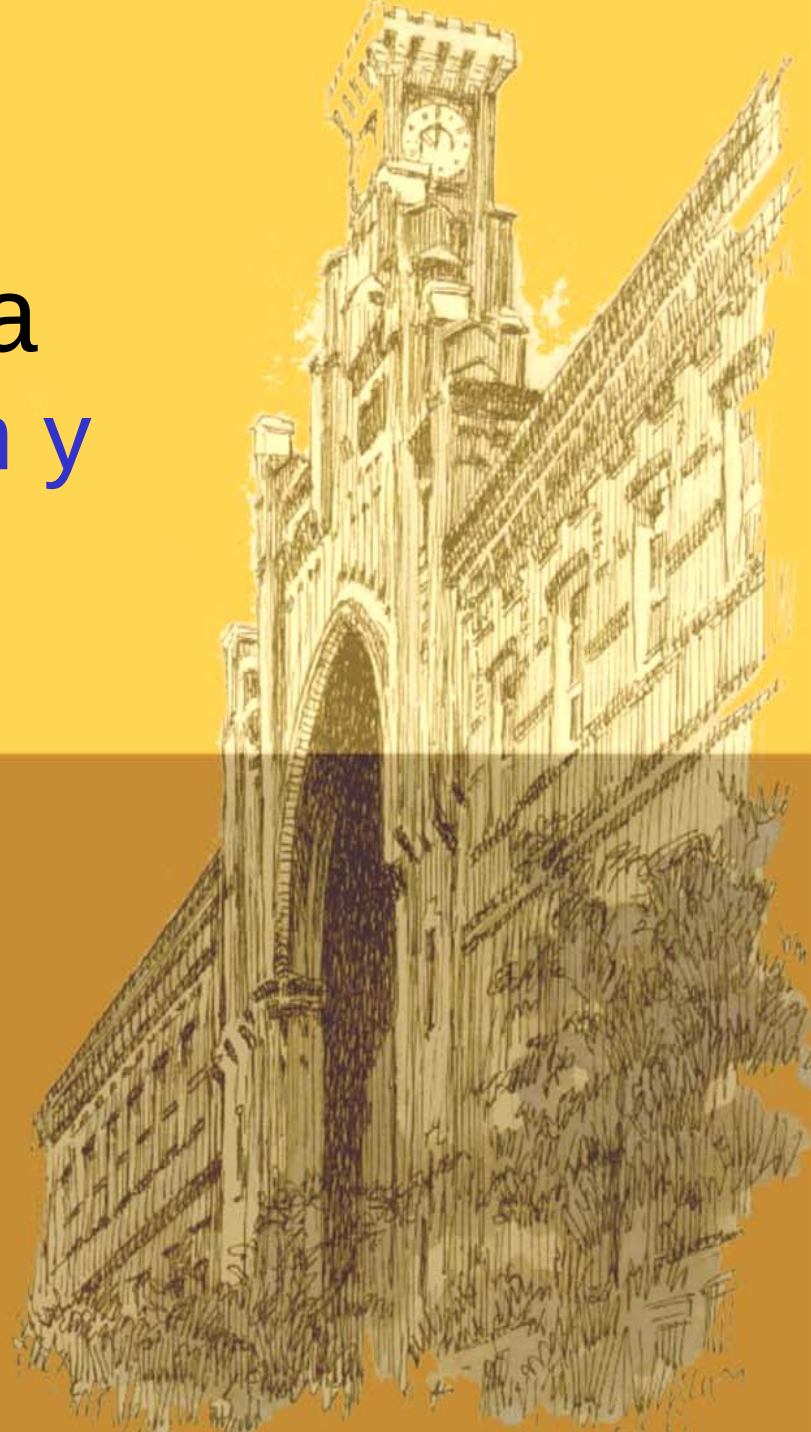
UNIVERSIDAD PONTIFICIA ICAI ICADE COMILLAS MADRID

Seguridad Informática

Capítulo 1: Introducción y conceptos básicos



Titulación: Ingeniero en Informática.
Curso 5º - Cuatrimestral (2005-2006)

Javier Jarauta Sánchez
José María Sierra
Rafael Palacios Hielscher

Conceptos Básicos

La Información

- La información es hoy en día uno de los activos más importantes de las organizaciones, y debe protegerse
- La información se encuentra en diferentes estados: Mientras se procesa, en transmisión y almacenada
- Existe en múltiples formas: papel, almacenada electrónicamente, transmitida por correo o medios electrónicos, hablada en una conversación o un vídeo, etc.
- Cada estado y forma dispone de una serie de amenazas y vulnerabilidades de diferentes niveles contra las que hay que protegerla
- Antiguamente todo era soporte papel, y la seguridad principalmente física. Actualmente lo primordial es el soporte informático y la seguridad lógica.

Visión global de seguridad

- La información y todos los soportes que la sustentan en una organización (sistemas y redes) están sometidos cada vez a más amenazas desde más fuentes
- Las clásicas amenazas: fraude, espionaje, sabotaje, vandalismo, fuego, inundaciones, etc.
- Las nuevas amenazas: virus, hackers, negación de servicio, etc.
- Las organizaciones dependen cada día más de sus sistemas de información, y son más vulnerables
- La mayoría de los SI no han sido diseñados con criterios de seguridad (no era prioritario, ej. TCP/IP)

SOLUCION

definir requisitos e implantar soluciones técnicas y organizativas con una visión global

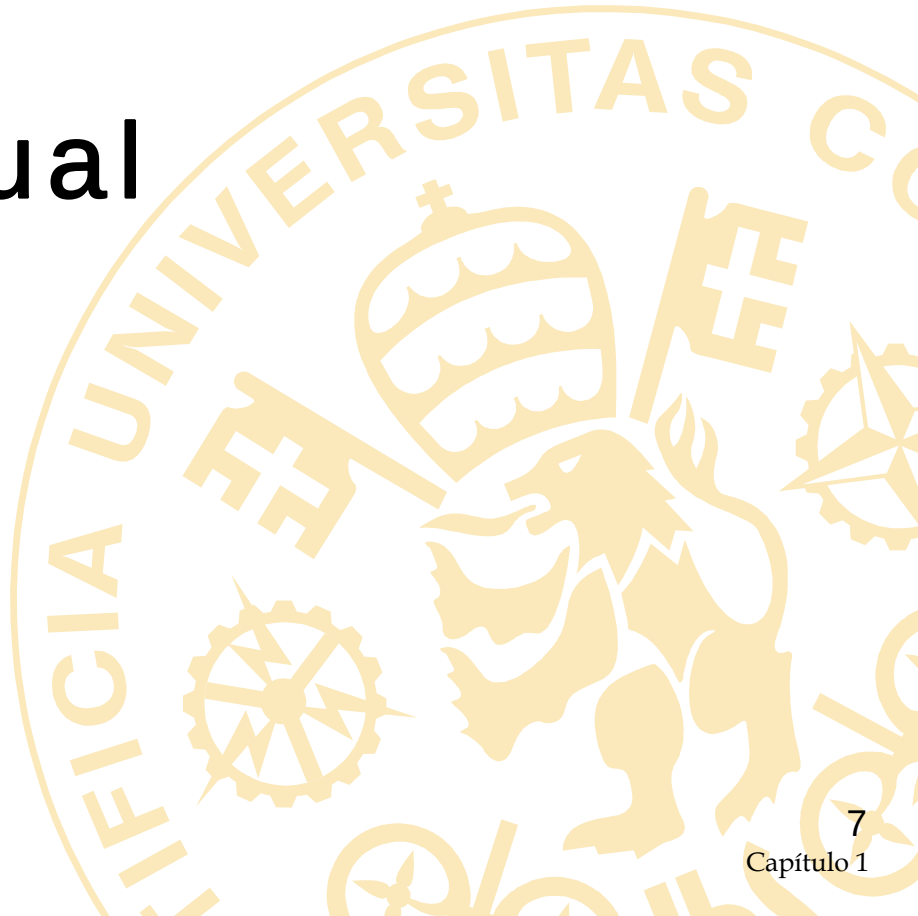
Términos básicos

- Servicios básicos de seguridad
  - Confidencialidad
  - Integridad
  - Disponibilidad
- Otros conceptos importantes de seguridad
  - Identificación / Autenticación
  - Control de accesos
  - Autorización
  - No repudio
  - Auditoría

Definiciones: Análisis y Gestión de Riesgos

- Análisis y Gestión de Riesgos: Definiciones
  - Activo: Componente del sistema al que la Organización le asigna un valor (Tangibles, Intangibles)
  - Amenaza: Ocurrencia de un evento que cause un impacto no deseado (Accidentales, Intencionados)
  - Riesgo: Posibilidad de que una amenaza se realice
  - Vulnerabilidad: Debilidad o ausencia de medidas de salvaguarda
  - Salvaguarda: Medida de control para reducir el riesgo asociado a una determinada amenaza
- Análisis y Gestión de Riesgos
  - Análisis de riesgos cualitativo
  - Análisis de riesgos cuantitativo
  - Procedimiento de valoración de activos
  - Selección de salvaguardas
- Metodologías: MAGERIT V2.0 (MAP) y otras

Situación Actual



Situación Actual

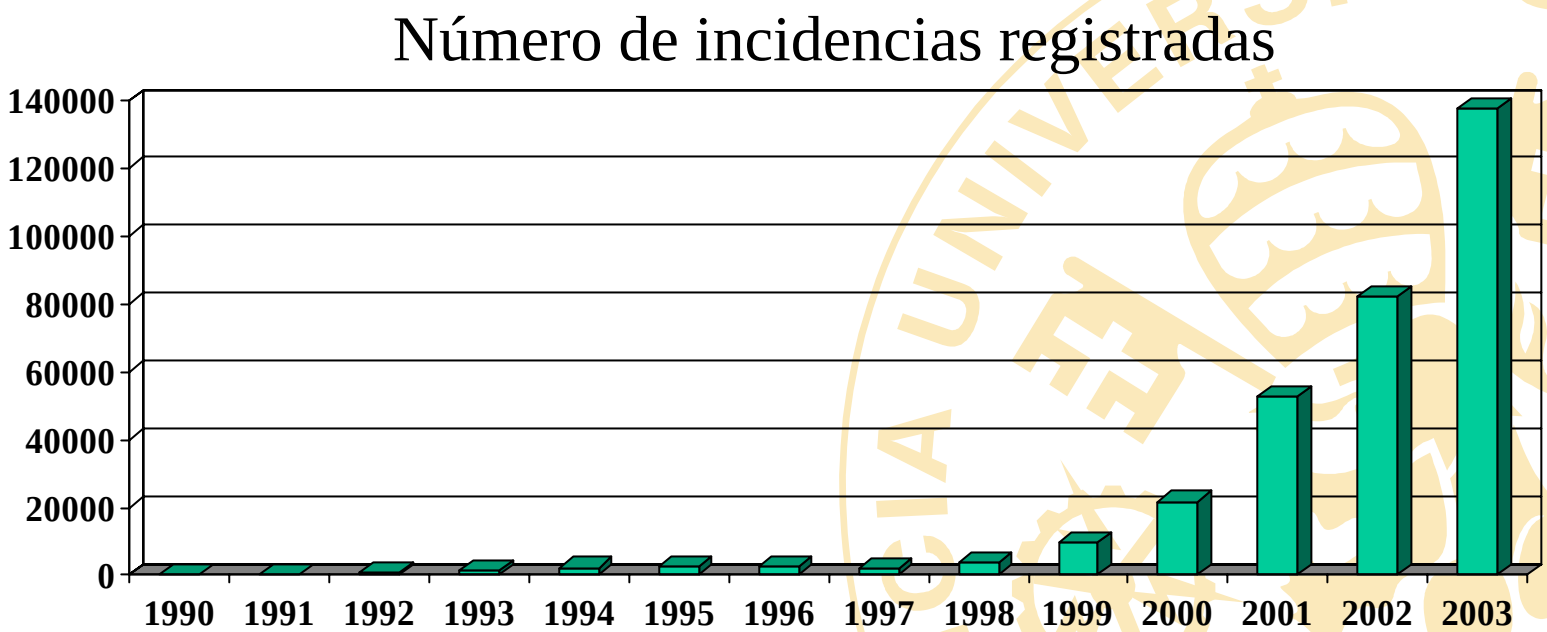
- En 2005 no se han producido las grandes epidemias de virus de años anteriores
  - LoveLetter, Sasser o Blaster
- Se ha producido un cambio a nuevas amenazas silenciosas, y cambio de motivación:
  - Fama personal versus Beneficio económico
- Tipos de malware:
  - Troyanos: Backdoor, Keylogger, con gusanos “Bot”
  - Phising, Pharming, Spyware, Spam y otros
- Vulnerabilidades continuas de todos los sistemas

Notas históricas

- Kevin Mitnik, perseguido durante tres años y detenido en 1995 robó información “top secret” al FBI. Especialista en Ingeniería Social
- Vladimir Levin transfirió 10 M$ de Citibank a cuentas propias en los 90, detenido en el 95.
- Amazon, Yahoo y otros muchos caen durante horas por un ataque de Denegación de Servicio en 2000
- En marzo del 2001 se detecta el robo de más de 1 millón de datos de tarjetas por hackers, aprovechando vulnerabilidades de IIS (mafias rusas)
- Robert un estudiante austríaco de 17 años accedió en Octubre 2002 a documentos secretos del DoD del pentágono.
- U.K.suspende su servicio de Renta on-line tras detectarse un fallo que permitía a usuarios acceder a datos de otros declarantes

Situación Actual

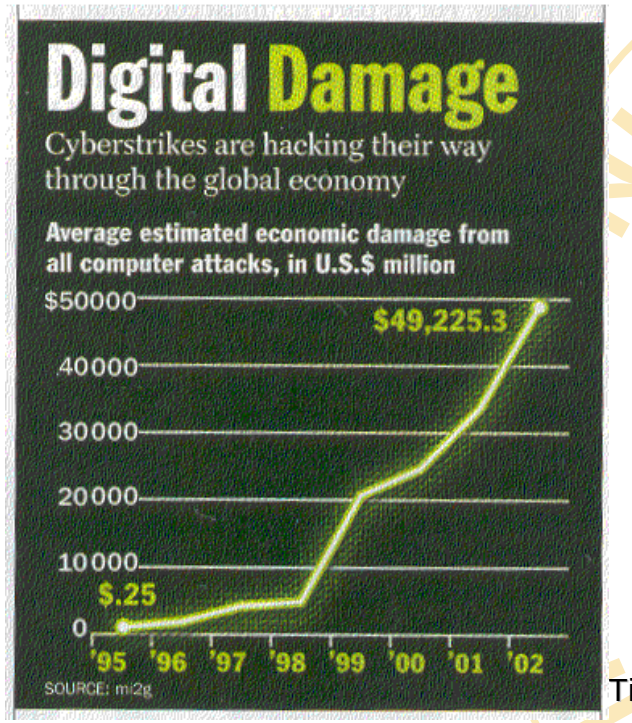
- Datos del **CERT Coordination Center**, centro de Carnegie Mellon University que coopera con el Department of Homeland Security, DOD.



*Cada incidencia puede afectar a un sitio o miles de sitios

Situación Actual

- Mi2g, compañía de seguridad informática de Londres, estima que daños económicos derivados de virus, gusanos, hackers, etc. suponen **50000 millones de dólares** (datos 2003).



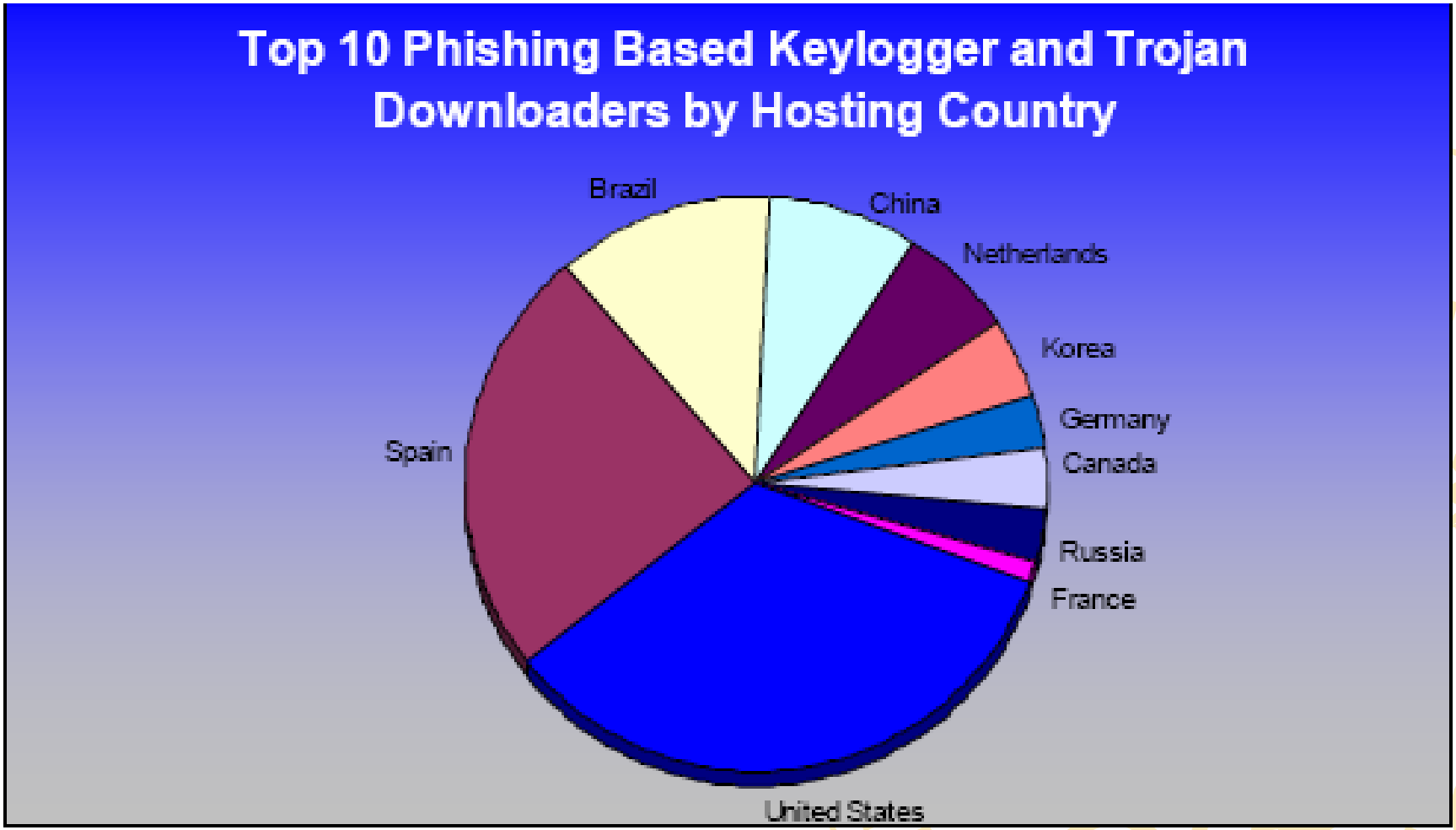
Time, Feb 10th, 2003

Situación Actual

- Federal Trade Commision (www.ftc.gov)
  - 516.740 reclamaciones en el año 2003.
  - Las reclamaciones relacionadas con Internet suponen el 55% de los fraudes reportados
  - La pérdida media de los fraudes por Internet es de $195
  - 645.000 en 2004
  - Pérdidas económicas de $565 million

Situación Actual

- Phishing Activity Trends Report. Nov 2005



Situación Actual

- En 2006 se despliega el DNI electrónico
  - Tarjeta chip para todos los españoles
  - Certificados digitales para autenticación y firma electrónica reconocida legalmente
  - 15/Febrero/2006 celebrada la Ceremonia de Generación de Claves del DNIe
  - 2/Marzo/2006 Se emite el primer DNIe en Burgos
- Durante los próximos años se emitirán a razón de 6-8 millones al año
- Proyecto líder a nivel mundial, liderado por la Dirección General de la Policía.

Ejemplos (1)

Ejemplo de fallo hardware

- 08/nov/2002, 09:00 UTC: Problema eléctrico
  - Incendio por sobrecarga eléctrica en la central mundial de Iberia. La Muñoza (Madrid)
  - Avería en los sistemas informáticos de Iberia que provocó retrasos en todos los vuelos de la compañía y varias cancelaciones.
  - Paralización de las operaciones de facturación y embarque
  - En este centro se gestiona también el sistema de distribución de reservas Savia-Amadeus, utilizado por el 96% de las agencias de viajes y los turoperadores

Ejemplos (2)

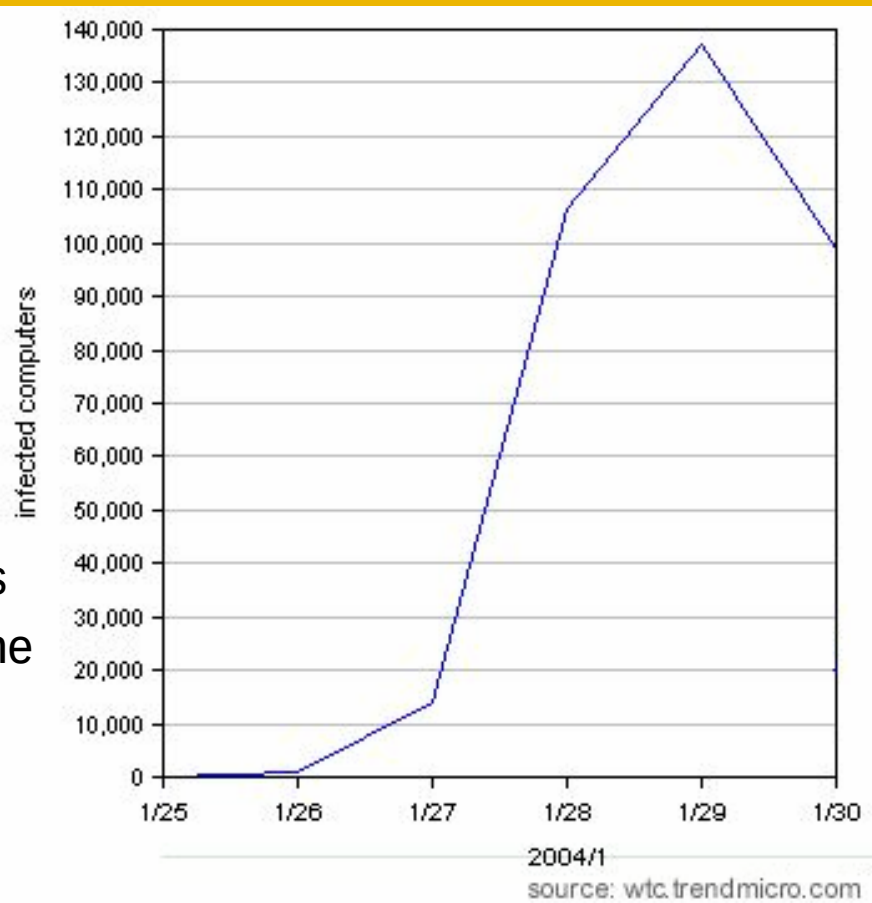
Ejemplo de ataque por Internet

- 25/ene/2003, 5:30 AM UTC: Slammer
  - Internet worm contra Microsoft SQL server
  - En pocas horas 700.000 servidores web afectados
    - American Express network
    - 13000 cajeros automáticos de Bank of America
    - Tráfico telefónico en Finlandia
  - Coste estimado a la economía mundial: 1.000 millones de dólares. (Costes de productividad y oportunidad de negocio).
  - El parche estaba disponible desde julio/2002

Ejemplos (3)

Expansión de Virus rápida

- 26/ene/2004, MyDoom worm
  - Internet worm contra sistemas Microsoft Windows
  - Correo electrónico basado en ingeniería social
    - Mensajes localizados en 142 países
    - Hasta uno de cada 3 mensajes tiene el virus (CNN)
    - > 400.000 ordenadores afectados
  - Ataques DoS programados:
    - 1/Feb/2004: www.sco.com
    - 3/feb/2004: www.microsoft.com

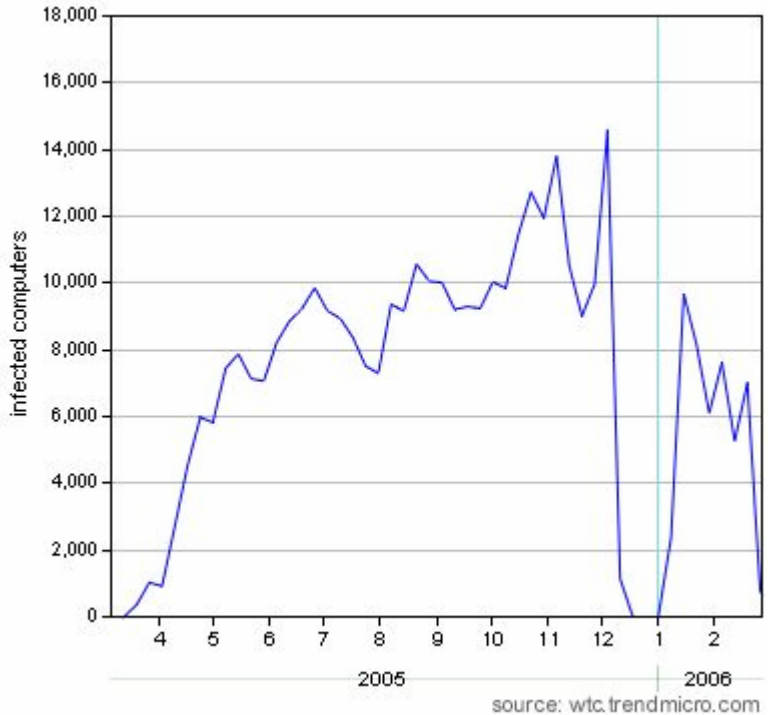


Ejemplos (4)

Expansión lenta

- 24/mar/2005, SPYW_DASHBAR
  - Entra por Internet Explorer sin acción del usuario.
  - Instala un toolbar de búsqueda

  - Casi 400.000 ordenadores infectados



Ejemplos (5)

Virus en la lista de alerta del Ministerio CyT

- 31/ene/2004, worm Sober.C
  - Fallo de configuración de la lista de correo de alertas del Centro de Alerta Temprana Antivirus.
  - Centro dependiente del Ministerio de Ciencia yTecnología a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información.
  - Están reforzando la seguridad e incluirán firma electrónica en los mensajes.

Soluciones

Cómo abordar la seguridad en los SI

- La seguridad es un proceso, no un producto
- Se utilizan medidas de varios tipos:
  - Adoptar políticas y procedimientos
  - Implantar medidas técnicas con productos
  - Gestionar todos los incidentes de seguridad
  - Auditorias continuas
- Abordarla desde un punto de vista global
  - Diagnóstico inicial de la seguridad
  - Plan director de seguridad
  - Abordar proyectos parciales

Norma UNE-ISO/IEC 17799:2002

Código de buenas prácticas en Seguridad de la Información (contenido)

Introducción a los conceptos de gestión de la seguridad.

10 secciones

36 objetivos de seguridad

127 controles de seguridad

Especificaciones / / Guía / / Referencias

Cubre aspectos de Gestión, Jurídicos y Técnicos

Norma UNE-ISO/IEC 17799:2002

Código de buenas prácticas en Seguridad de la Información (secciones)

3 .- Política de Seguridad.

4.- Aspectos organizativos para la Seguridad.

5.- Clasificación y control de activos

6.- Seguridad ligada al personal

7.- Seguridad física y del entorno

8.- Gestión de Comunicaciones y Operaciones

9.- Control de accesos

10.- Desarrollo y mantenimiento de sistemas.

11.- Gestión de Continuidad del negocio.

12.- Conformidad (cumplimiento con la legislación vigente)

Norma UNE 71502:2004 - SGSI

Sistema de Gestión de la Seguridad de la Información (SGSI – ISMS)

Norma certificable

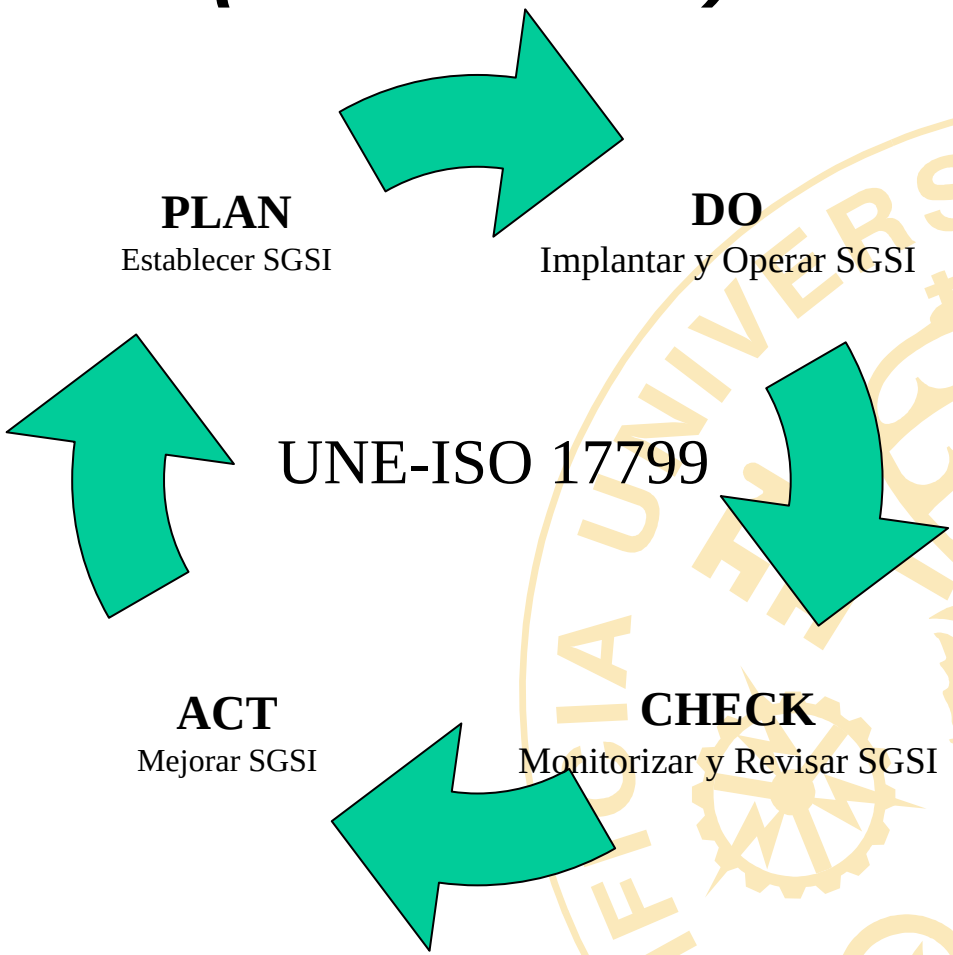
Sistema de gestión que comprende la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de la seguridad

Es la herramienta de que dispone la Dirección para llevar a cabo las políticas y objetivos de seguridad

Proporciona mecanismos para la salvaguarda de los activos de información

Norma UNE 71502:2004 - SGSI

Sistema de Gestión de la Seguridad de la Información (Modelo PDCA)



Plan Director de Seguridad

- Fase 1: Diagnóstico de la situación
  - Conocer la organización, áreas funcionales y procesos de negocio
  - Identificar activos, realizar entrevistas
  - Evaluar la seguridad de comunicaciones, sistemas, aplicaciones
- Fase 2: Análisis de riesgos
  - Análisis de las amenazas y vulnerabilidades
  - Identificación, cálculo y clasificación de los riesgos
- Fase 3: Grado de cumplimiento UNE/ISO 17799
  - Informe de cumplimiento de cada un de los 10 capítulos
- Fase 4: Plan de proyectos de seguridad
  - Agrupar las vulnerabilidades y definir proyectos a acometer
  - Clasificar y valorar proyectos a corto, medio y largo
- Fase 5: Gestión de los riesgos
  - Disminuir con proyectos, externalizar con seguros o asumir.

Seguridad de la Información

- **Seguridad**:
  - Protección de la CONFIDENCIALIDAD, INTEGRIDAD y DISPONIBILIDAD de la información, según el nivel requerido para los objetivos de negocio de la organización

- **Información**:
  - ACTIVO de información tangible o intangible que tiene VALOR para los procesos de negocio de la organización.