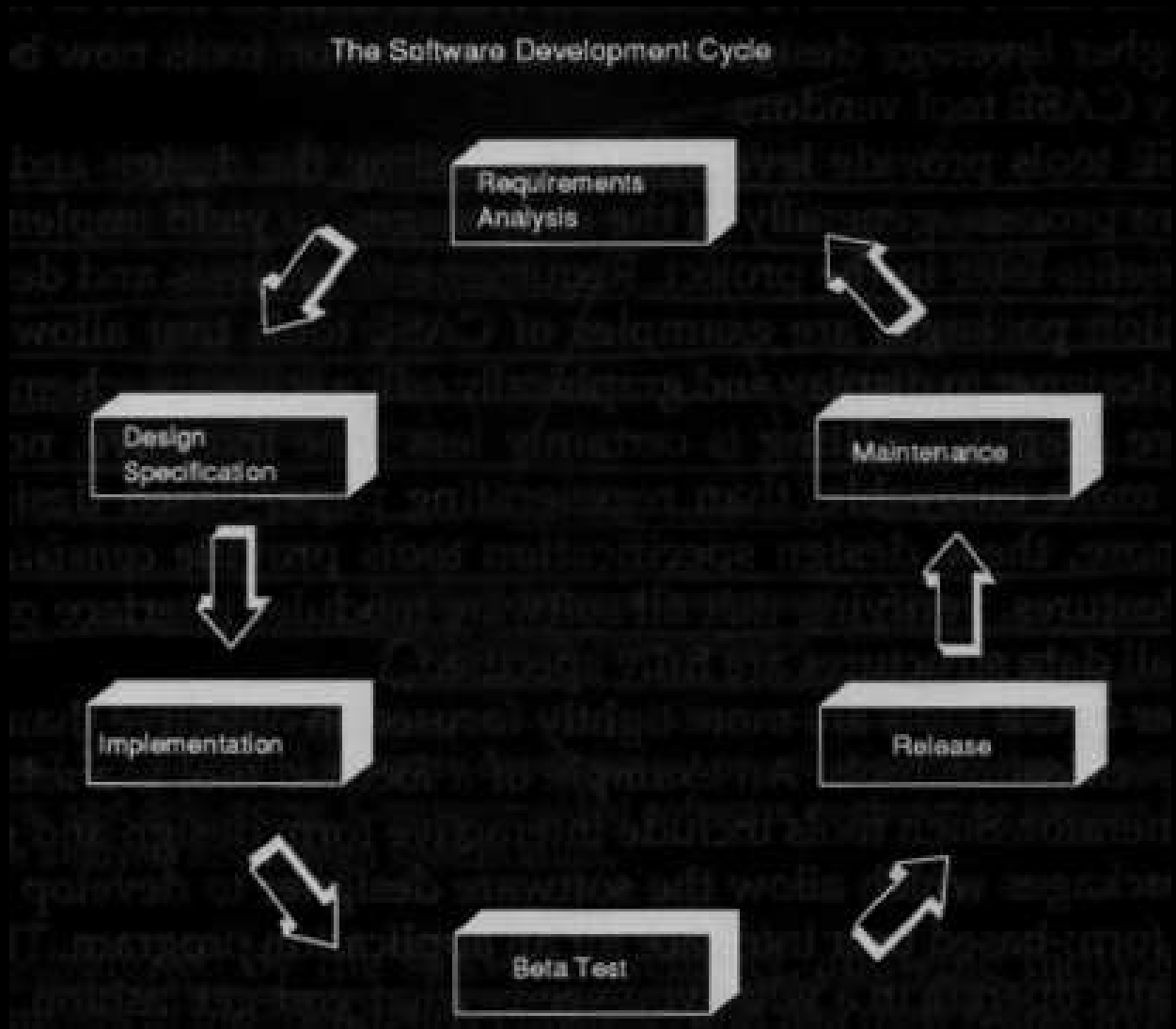
Parte II
Políticas de seguridad

Ingeniería de Seguridad I

- Ingeniería de seguridad. Modelos
- Análisis
- Diseño
- Implementacion
- Mantenimiento e incidencias.
- Referencias.

Ingeniería de Seguridad II

Modelo Clásico Ing. del Software



Ingeniería de Seguridad III

Modelo ISS

Fuente: ISS.net

Ingeniería de Seguridad IV

Fuente original: CERT.org

Modelo CERT

Análisis. ¿ Que es ? (II)

- Una Politica de Seguridad no es un firewall.
  - Fallos Tecnicos: Man in the middle, spoofing, autenticación débil...
  - Fallos no tecnicos: Señora de la limpieza, fallos humanos, mal diseño, poco control en la organización....
    - Kevin Midnick

Análisis. ¿¡ QUE ES !? (III)

- ¿ Que es una política de seguridad ?
  - Confusiones varias al respecto.
  - Un conjunto de documentos, con un orden y una sistematización.
  - Describe paso a paso los distintos elementos de una politica de seguridad.
    - Detalla riesgos y peligros
    - Como protegerse frente a esos riesgos, medidas a tomar y detalles de esas medidas.
    - Que medidas tomar frente a posibles incidencias
    - Que hacer en el peor de los casos

Análisis. Que es (IV)

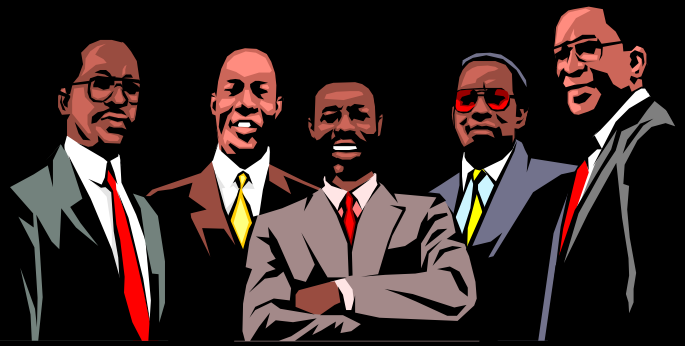
- Una Politica de Seguridad no se vende ni se compra.
  - No existen productos que hagan todo.
  - La seguridad se vende con el miedo.
  - El riesgo es real, las consecuencias diversas.
  - Figura del Consultor / Tecnico de Seguridad.

Análisis. Necesidad

- Necesidad de una Política de Seguridad en una organización.
  - Confidencialidad.
  - Integridad.
  - Disponibilidad.

Análisis. Justificación

- Justificación
  - Establece lo que se puede hacer y lo que no, de forma escrita y formal. Se puede leer y es algo escrito y aceptado.
  - Demuestra que la empresa se lo quiere tomar en serio. Implica un compromiso con los directivos.
  - Util frente a una auditoria, sobre todo si se siguen las normalizaciones.
  - Util para demostrar casos de intrusiones o delitos contra los sistemas informáticos.

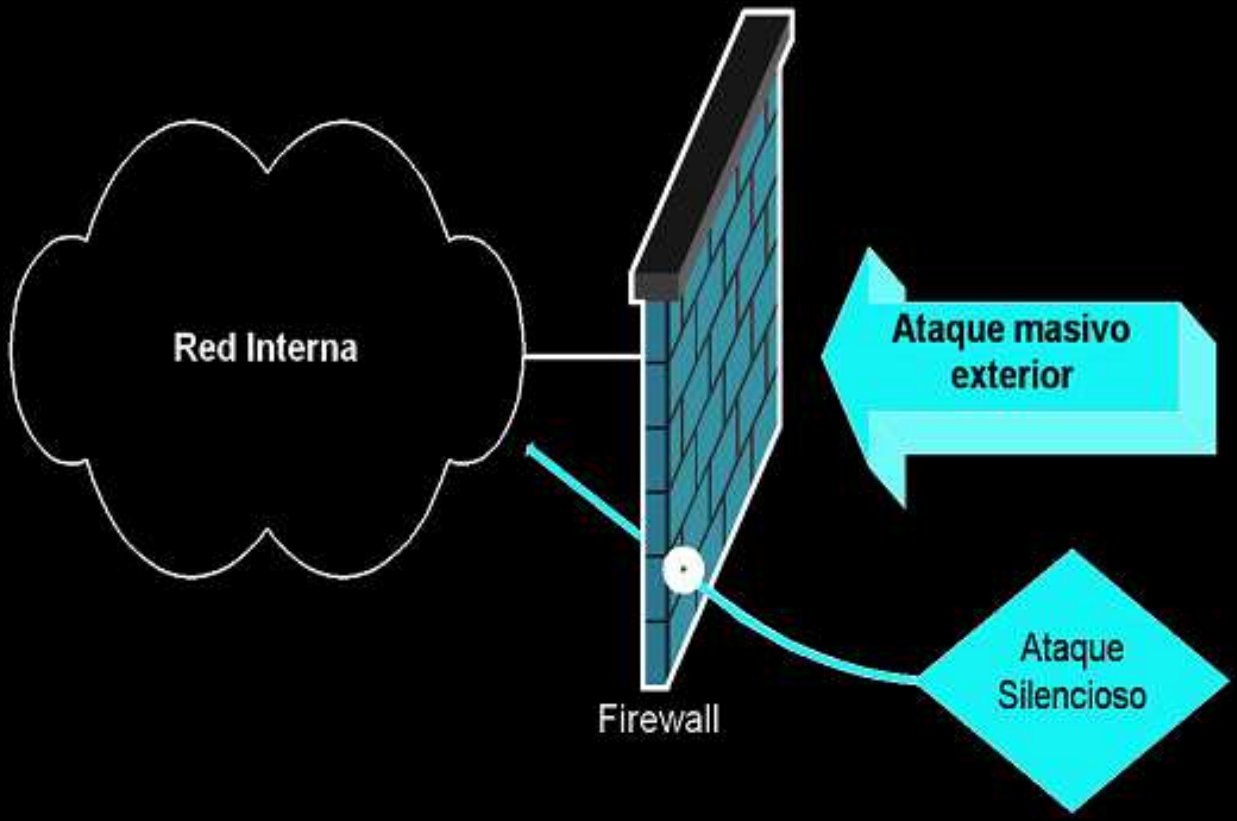


Analisis. Normalización I

- Normalización y método. ISO 17799, BS7799, RFC 2196
  - Standard y certificación
  - Rigurosidad y Método
  - Hacking ”etico”

Análisis. Normalización II

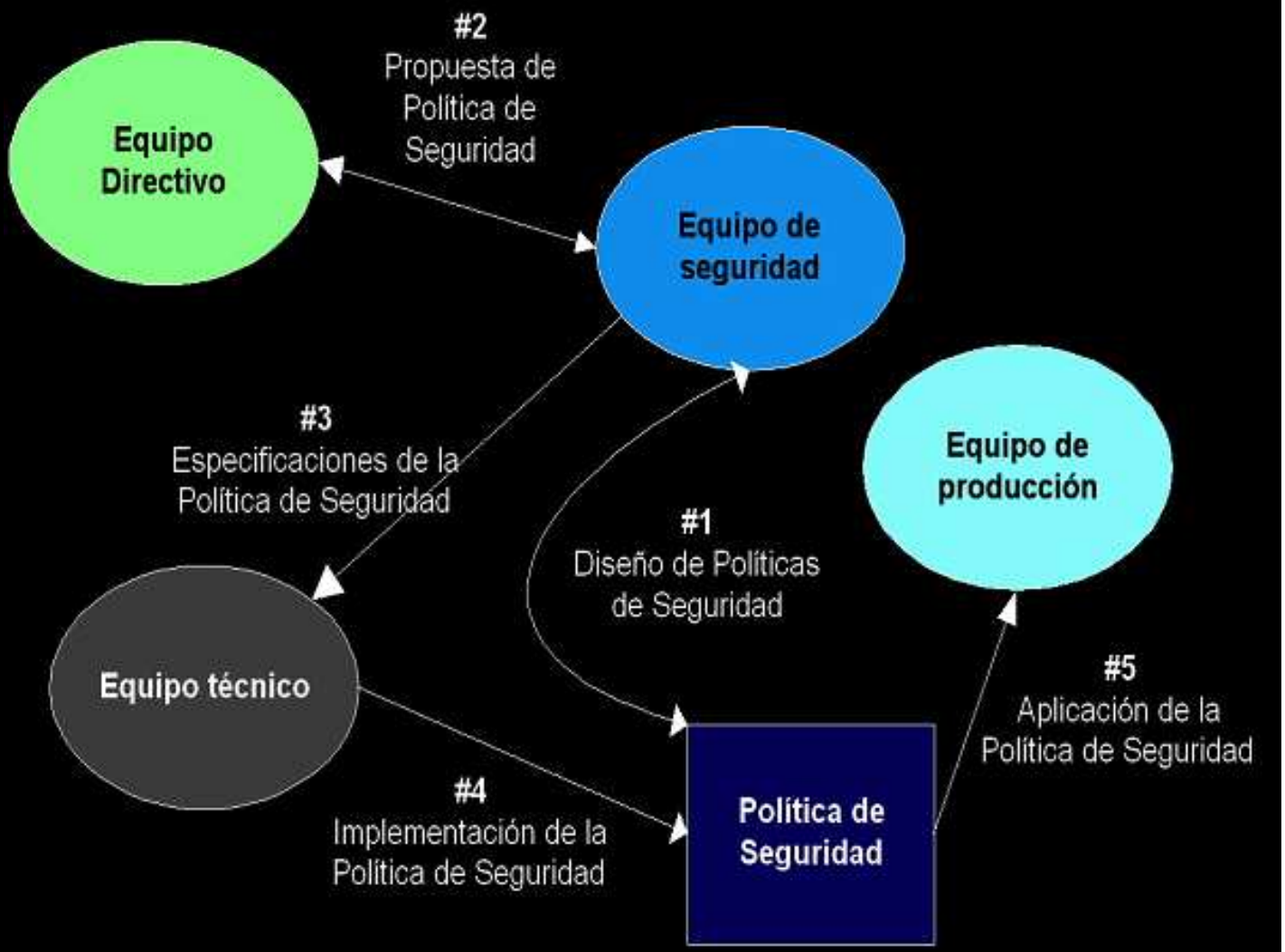
- Normalización y método II
  - Hacker vs Administrador
    - Teoría de la “presa”



Análisis. Ámbitos

- Personas implicadas y responsabilidades en el proyecto.
  - Equipo de seguridad
  - Dirección de la organización
  - Personal técnico
  - Personal no técnico

Análisis. Ambitos (II)



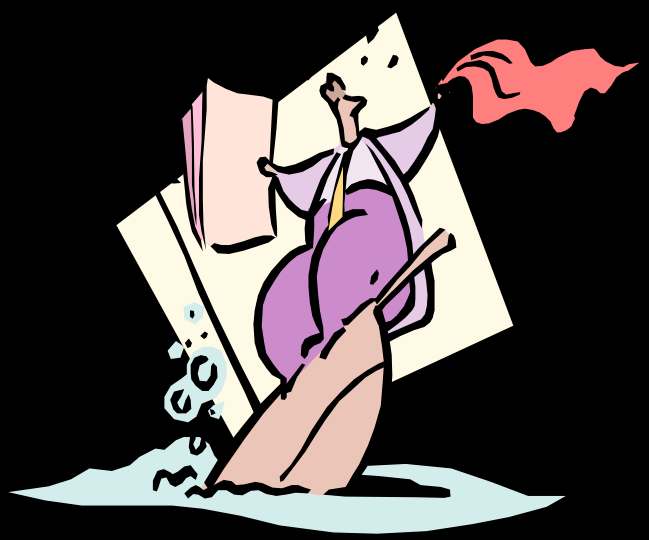
Análisis. Riesgos (I)

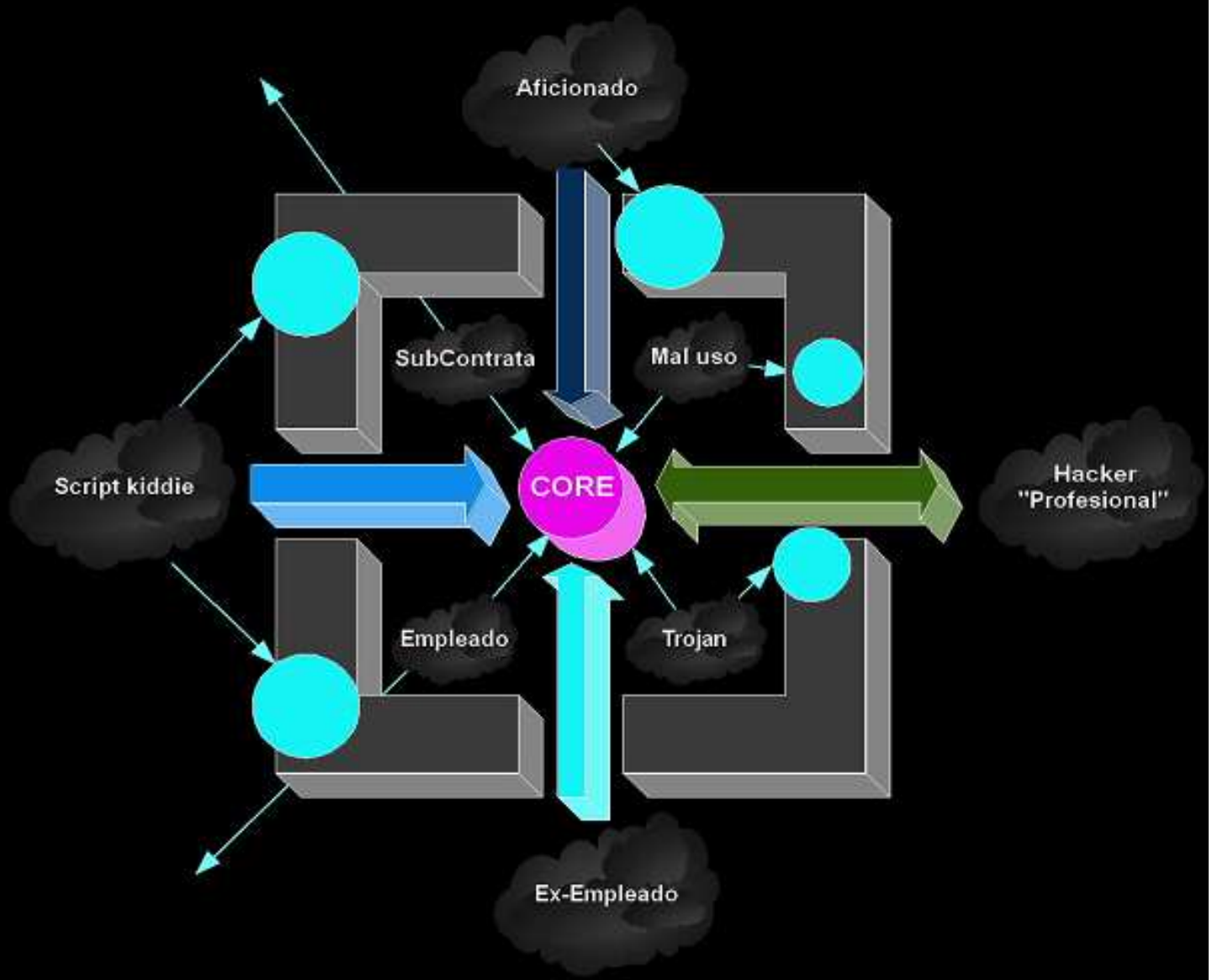
- Administrador vs Hacker. Teoria de la presa.
- Identificar peligros. Checklist.
  - Confidencialidad
  - Integridad
  - Disponibilidad
- Clasificación en niveles de seguridad. Normalizaciones.

Análisis. Riesgos (II)

- ¿Que proteger?
  - Acceso a Informacion comprometida o confidencial
    - Planes de negocio, nominas, contratos, listados passwords, informacion de clientes.
  - Acceso a Informacion valiosa
    - Documentacion, desarrollos de I+D, historicos y archivos.
  - Acceso a Inversiones e infraestructura
    - Configuraciones, logs, backups, bbdd, webs, intranets, Acceso a servidores, electrónica y hardware costoso.

Análisis. Riesgos (III)





Análisis. Riesgos (IV)

- Peligros contra la confidencialidad.
  - Accesos no autorizados a información confidencial
  - Accesos públicos a informacion confidencial, por error, mala configuracion o descuido.
  - Suplantación de usuarios.
  - Acceso a servicios confidenciales (correo, bbdd, servidores de acceso, etc).
  - Instalación de caballos de troya.
  - Acceso fisico a material restringido.

Análisis. Riesgos (V)

- Peligros contra la integridad
  - Modificación indebida de datos (fallo de permisos)
  - Falta de integridad (borrado o modificación) de datos.
  - Imposibilidad de idenficar fuente de datos.
  - Fallo en la integridad de bases de dato (corrupcion).
  - Modificación en archivos de sistema (configuraciones, logs, etc)
  - Destrucción o corrupción de backups.
  - Virus.
  - Acceso fisico a material restringido.

Análisis. Riesgos (VI)

- Peligros contra la disponibilidad.
  - Caida de servicios externos. (DoS)
  - Agotamiento de recursos (ancho de banda, disco, socket, etc). (DoS o mala config.)
  - Fallo de infraestructuras generales de red (routing, switches, etc). (DoS, fallo, mala configuración o sabotaje)
  - Destrucción de configuraciones o servicios. (DoS o Sabotaje)
  - Acceso fisico a infraestructura básica. Sabotaje.

Análisis. Riesgos (VII)

- DoS
  - Casos historicos: Yahoo, Amazon, eBay, etc. Perdidas.
  - Tecnicas varias.
    - Fallos especificacion protocolo.
    - Programacion deficiente (buffer overflow).
    - Flood.
    - Acceso a los servicios: Fuerza bruta, trojan, otros.
    - Spoofing vario (IP, DNS, etc).
    - Session hijacking.
    - Ingenieria social y acceso fisico.
    - DDoS y gusanos

Análisis. Riesgos (VII)

- Resumen de riesgos:
  - Acceso a informacion sensible.
  - DoS y fallos de programación.
  - Mal uso de recursos.
- ¿ Era un firewall suficiente ?
- ¿ Existe algo suficiente por si mismo para garantizar la seguridad ?

Diseño. Introducción

- Diseño.
  - Como llevar esto a la práctica
- Uso de herramientas
  - ISO 17799 y BS 7799
  - RFC 2196
  - Orange Book (DoD EEUU)
  - CERT Security Guidelines
  - Otras guías

Diseño. Vamos allá (I)

- Organizando subpoliticas
- Las mas importantes y comunes
  - Uso de los recursos del sistema (*)
  - Política de cuentas de usuario (*)
  - Política de protección de la información (*)
  - Política legal (*)
  - Política de seguridad general de los sistemas informáticos en producción (*)
  - Política de backup (*)
  - Política de control de accesos (*)
  - Política de accesos y permisos (*)
  - Política de seguridad física (*)

Diseño. Vamos allá (II)

- Otras subpolíticas.
  - Política de Accesos remotos.
  - Política de educación en el ámbito de la seguridad.
  - Política de prevencion y detección de virus.
  - Plan de continuidad de negocio.
  - Política de passwords.
  - Política de seguridad perimetral de los sistemas informáticos.

Diseño. Vamos allá (III)

- Otras subpolíticas (continuación)
  - Política de seguridad perimetral interna de los sistemas informáticos.
  - Política de intervenciones.
  - Política de incidencias.
  - Política de alta disponibilidad y redundancia.
  - Política de guardias 24x7
  - Politica de gestion de recursos informáticos.
  - Política de monitorización.
  - Política de encriptación y ocultación de información.