Master

Seguridad en Internet

Propósitos del Tema

- Divulgar los conceptos de:
  - Conceptos sobre Seguridad de la información
  - Conceptos sobre TCP/IP
  - Funcionamientos de redes
  - Criptografía
  - Mecanísmos y Medios técnicos de seguridad

Seguridad: Definiciones

- "*Sabemos que es hasta que alguien nos pide que lo definamos*" (Descartes)

- ¿Qué entendemos por seguridad?
  - Real Academia de la Lengua:
    - SEGURIDAD: Cualidad de seguro
    - SEGURO: libre y exento de todo peligro, daño o riesgo
      - Cierto, indubitable y en cierta manera infalible
      - No sospechoso

Definiciones de Seguridad Informática: Consejo Superior de Informática

- Conjunto de técnicas y procedimientos que tienen como misión la protección de los bienes informáticos de una organización
- Bienes informáticos
  - Hardware
  - Datos
  - Programas

La información

ISO/IEC 17799

- La información es un activo que tiene valor para la organización y requiere una protección adecuada.
- La seguridad de la información la protege de un amplio elenco de amenazas para
  - asegurar la continuidad del negocio,
  - minimizar los daños a la organización
  - maximizar el retorno de inversiones
  - Y las oportunidades de negocios.

ISO/IEC 17799 formas información

- La información adopta diversas formas.
  - Puede estar impresa o escrita en papel,
  - Almacenada electrónicamente,
  - Transmitida por correo o por medios electrónicos,
  - Mostrada en filmes o hablada en conversación..
- Debería protegerse adecuadamente cualquiera que sea la forma que tome o los medios por los que se comparta o almacene.

ISO/IEC 17799 Características

- La seguridad de la información se caracteriza aquí por la preservación de:
  - Su confidencialidad, asegurando que solo quien está autorizado puede acceder a la información
  - Su integridad, asegurando que la información y sus métodos de procesos son exactos y completos
  - Su disponibilidad, asegurando que los usuarios autorizados tiene acceso a la información y a sus activos asociados cuando lo requieran

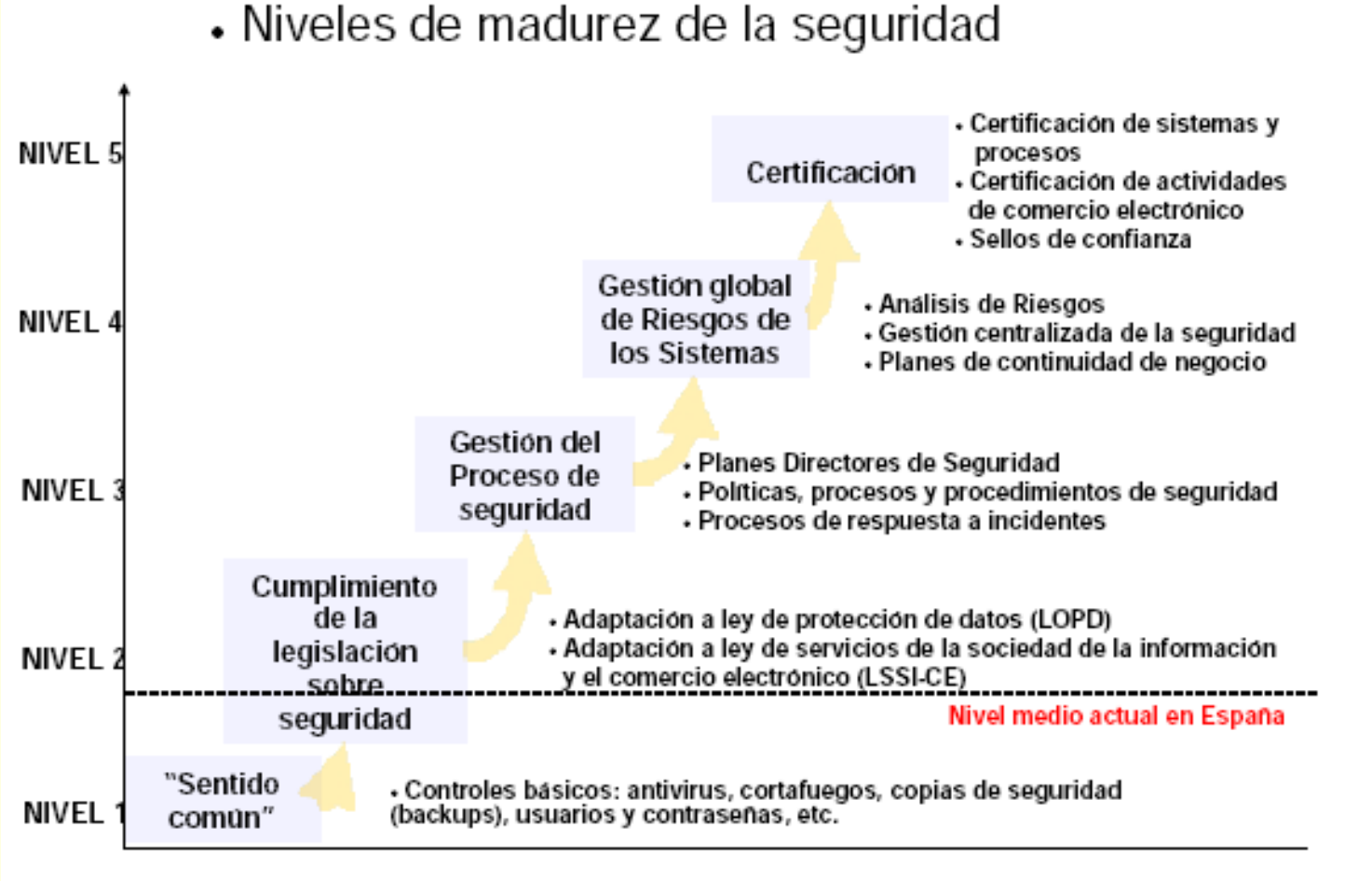
QUÉ ES SEGURIDAD

- ✓ Evitar el ingreso de personal no autorizado
- ✓ Sobrevivir aunque “algo” ocurra
- ✓ Cumplir con las leyes y reglamentaciones gubernamentales y de los entes de control del Estado
- ✓ Adherirse a los acuerdos de licenciamiento de software
- ✓ Prevención, Detección y Respuesta contra acciones no autorizadas

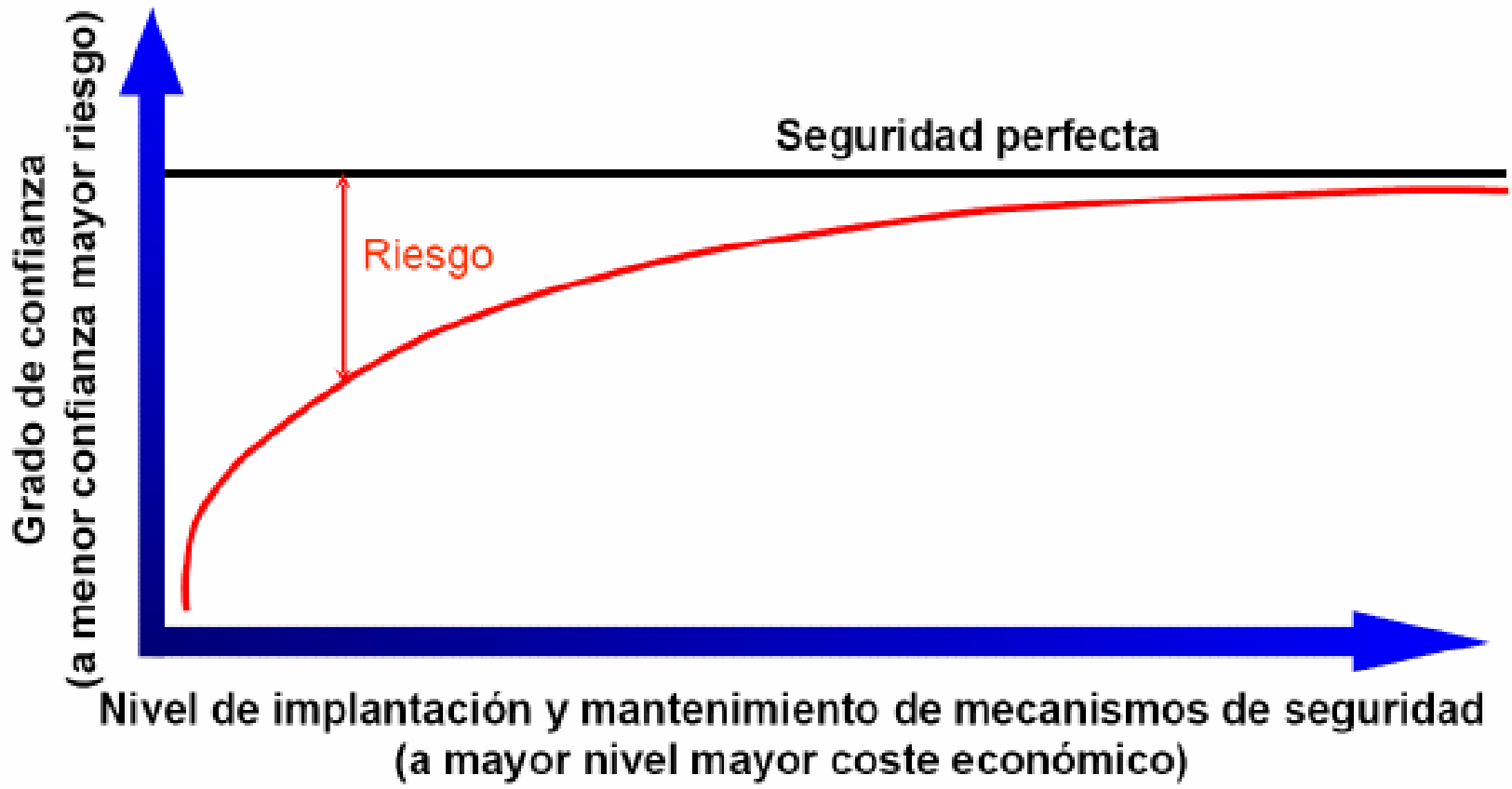
Niveles de seguridad

- Seguro estaba y se murió
- Seguridad total
  - “Queremos que no tenga éxito ningún ataque”
  - Seguridad = Invulnerabilidad
  - Imposible de alcanzar
  - La seguridad total no existe
- Existen grados de seguridad acorde con el bien a defender
  - La política de seguridad siempre es un compromiso entre el nivel de riesgo asumido y el coste requerido

Niveles de seguridad



Riesgo y seguridad



Enfoque de gestión del riesgo

- “Queremos que nuestras expectativas se cumplan”
- Seguridad = Confianza
- Posible de gestionar
- El riesgo no puede eliminarse completamente, pero puede reducirse

Análisis de riesgos

- Objetivo:
  - Identificar los riesgos
  - Cuantificar su impacto
  - Evaluar el coste para mitigarlos
  - Servir de guía para tomar decisiones
- Riesgo = Activo x Amenaza x Vulnerabilidad

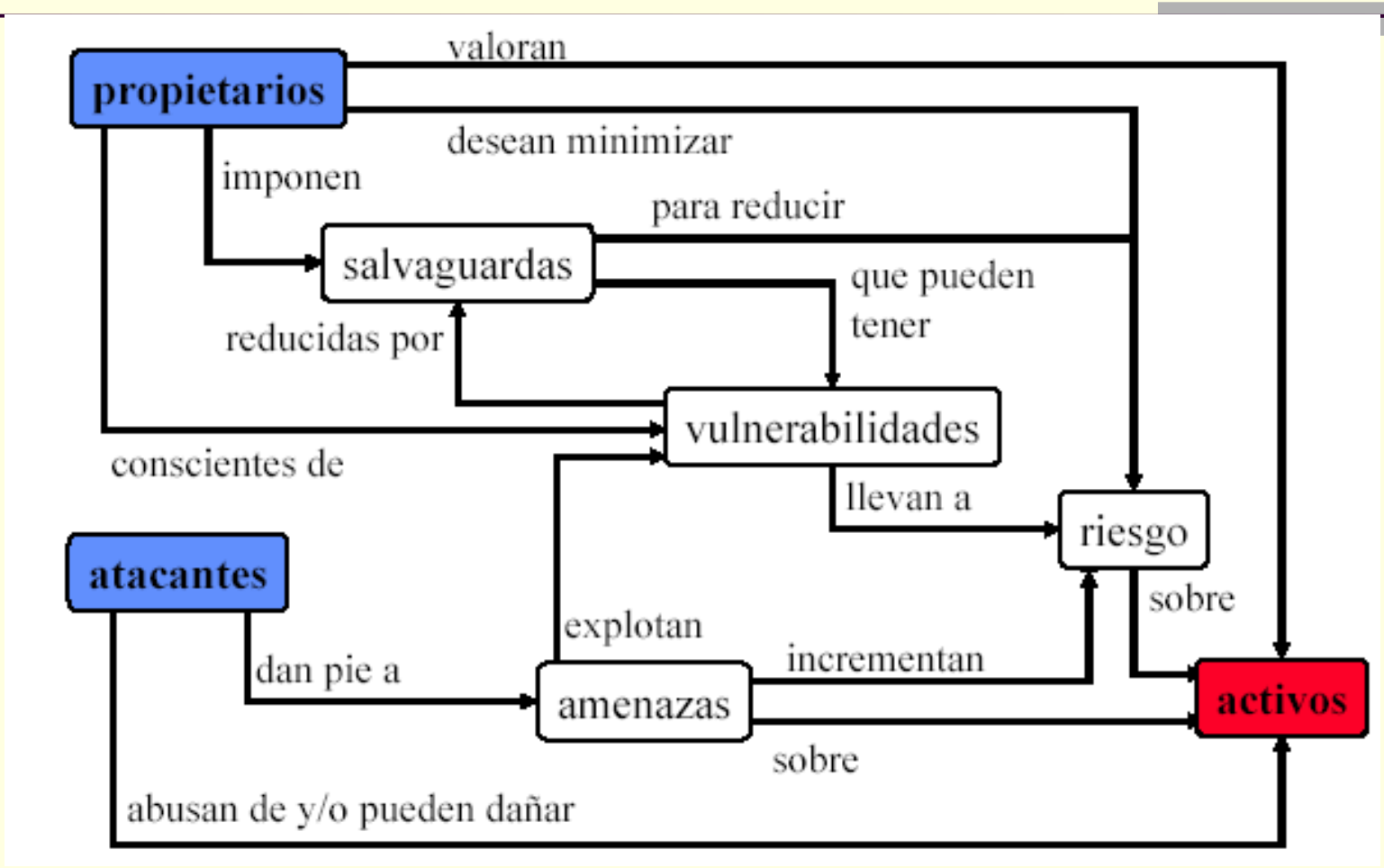
MAGERIT – versión 2

Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Definiciones

- ACTIVO:
  - Recurso del sistema de información o relacionado con éste, necesario para que la organización funcione correctamente y alcance los objetivos propuestos por su dirección.
- AMENAZA:
  - Evento que puede desencadenar un incidente en la organización, produciendo daños o pérdidas materiales o inmateriales en sus activos.
- VULNERABILIDAD:
  - debilidades que pueden permitir que una amenaza se materialice
- RIESGO:
  - Posibilidad de que una amenaza se materialice.
- IMPACTO:
  - Consecuencia sobre un activo de la materialización de una amenaza.
- CONTROL o SALVAGUARDA:
  - Práctica, procedimiento o mecanismo que reduce el nivel de riesgo.

ISO: análisis de riesgos



Gestión de riesgos

Planificar

Definir:
- Alcance
- Política
- Metodología

Identificar y analizar

Identificar:
- Activos
- Amenazas
- Vulnerabilidades

Analizar:
- Riesgos
- Coste/beneficios

Dirección

- Decidir tratamiento de riesgos
- Aceptar riesgo residual

Mitigar Riesgo

Controles:
- Seleccionar
- SOA
- Implantar

Transferir Riesgo

- Seguros
- Proveedores

Aceptar Riesgo

- No hacer nada

Evitar Riesgo

- Cese de la actividad que lo origina

Fuente: www.ISO27000.es

Valoración cuantitativa del riesgo

- B1 = beneficios_1 – gastos_1
  - si no ocurre nada
- B2 = beneficios_2 – gastos_2
  - si se materializa la amenaza
- IMPACTO = B1 – B2
  (beneficios_1 – beneficios_2) + (gastos_2 – gastos_1)

Modelo PDCA

Gestión de la seguridad: modelo

- Modelo PDCA (Plan – Do – Check – Act): Planificar, Hacer, Verificar y Actuar.

Clasificación de las medidas seguridad (I)

- Medidas técnicas
  - Seguridad física (externa)
    - Se consigue adoptando una serie de medidas físicas y administrativas
    - Aspectos:
      - Intrusos físicos (“choris”)
      - Agentes físicos externos al sistema
  - Seguridad lógica (Interna)
    - Se consigue adoptando una serie de medidas técnicas y administrativas
    - ASPECTOS:
      - De Sistemas
      - De red
      - Del software

Clasificación de las medidas seguridad (II)

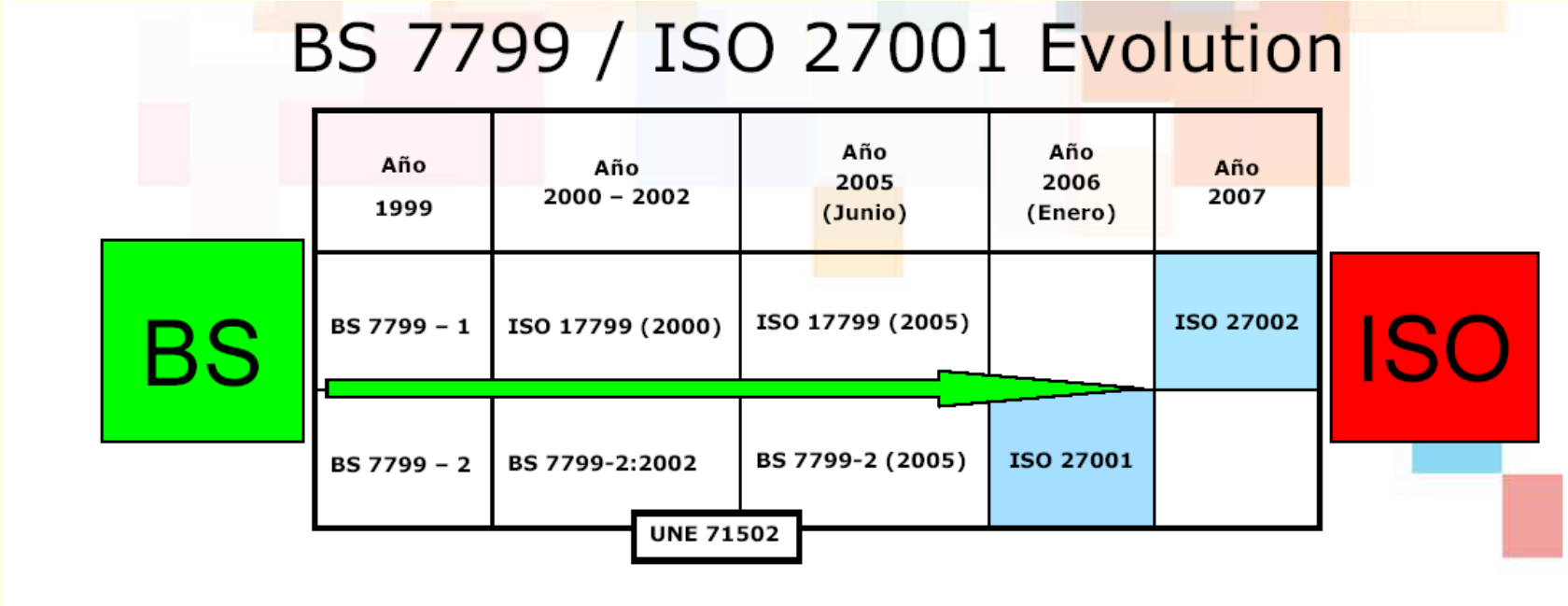
- Medidas Organizativas
  - Normas que determinan funciones como:
    - Las personas que pueden acceder.
    - Quién tiene derecho a utilizar el sistema
    - Horario etc
  - Clasificación de los usuarios
    - Administradores
    - Usuarios
    - Personas ajenas al sistema
    - Personal de mantenimiento
    - Ejecutivos de grado medio
  - Niveles
    - Todo el mundo tiene acceso a todo
    - Dos niveles: privilegiado y normal
    - Varios niveles de acceso

Medidas organizativas y legales

- Todas las normas de “organización” (NO técnicas) necesarias para llevar a cabo el plan de seguridad
- Medidas legales
  - Legislación de protección de datos
  - Normas de seguridad de obligado cumplimiento
- Metodologías de seguridad
  - Metodologías de análisis de riesgo
  - Metodologías de nacionales e internacionales de seguridad

Estándares ISO

- ISO 17799/UNE 71501
- ISO 27000
  - http://www.iso27000.es/index.html

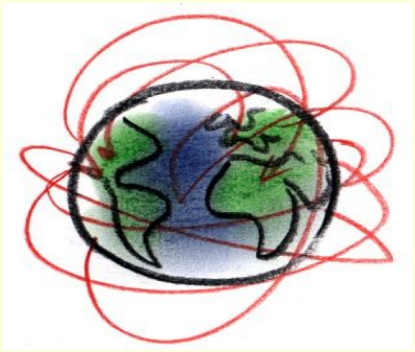


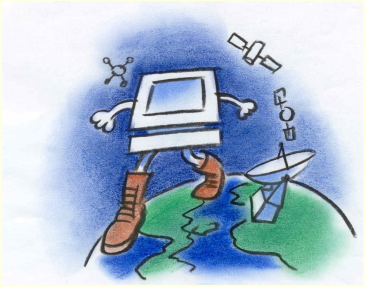
Normas ISO 27000

- NACE LA FAMILIA DE LAS NORMAS ISO 27000
- ISO/IEC 27001 (BS7799-Part 2) - 'Information Security Management System'. Due for release in November 2005. (Once ISO/IEC 27001 is released, BS7799-2:2002 will be withdrawn)
- ISO/IEC 27002 (ISO/IEC 17799 & BS7799- Part 1) - The planned 'Code of Practice' replacement for ISO/IEC 17799:2005 scheduled for April 2007
- ISO/IEC 27003 (BS7799-3) 'Risk Assessment'. No announcement has yet been made regarding ISO/IEC 27003 however, the BSI expect to release BS7799-3 in November 2005
- ISO/IEC 27004 (BS7799-4) 'Information Security Metrics and Measurement'. No launch date is available, although the BSI will publish a description in July/August 2005

¿Cómo funciona Internet?

- ¿Qué es Internet?
  - Internet es una red de redes Heterogénea



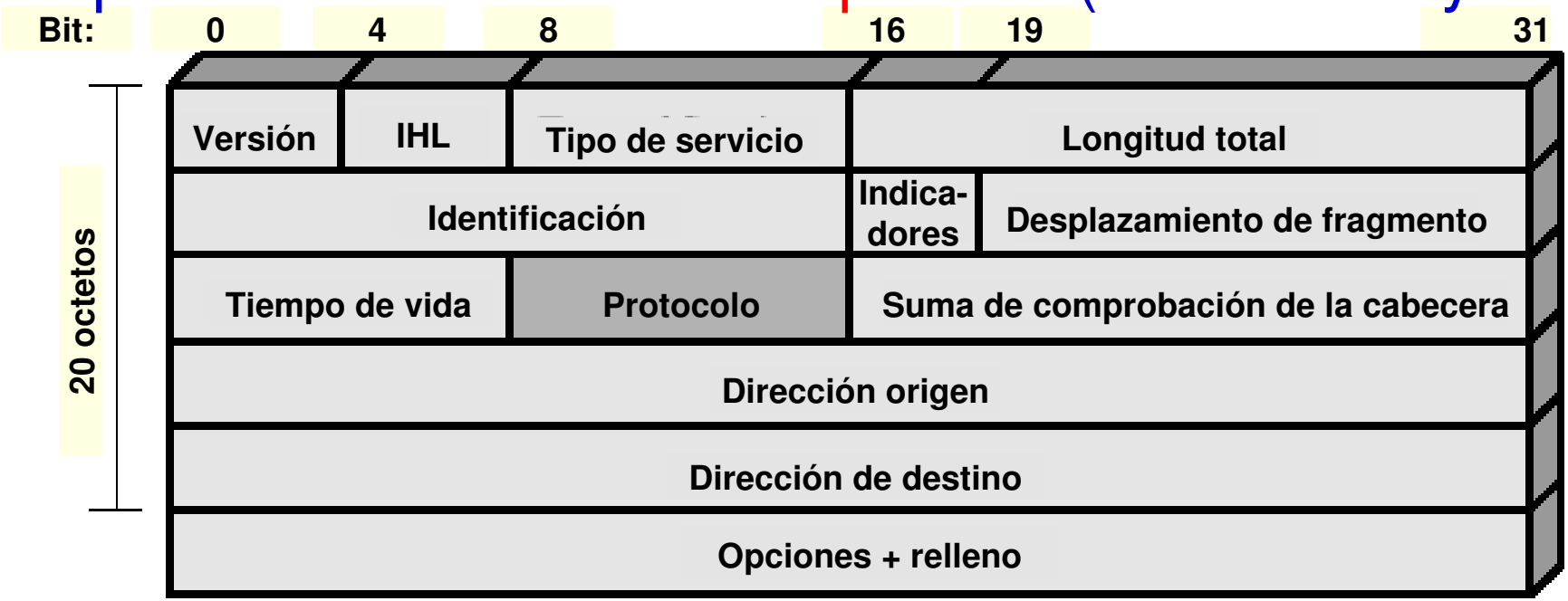


¿Que tienen en común?

- El protocolo TCP/IP
  - TCP/IP es **un conjunto de protocolos** de red capaces de soportar las comunicaciones entre equipos conectados a gran número de redes heterogéneas, independientes de un vendedor.
  - Ofrece la posibilidad de interconectar redes de diferentes arquitecturas y con diferentes sistemas operativos.
  - Se apoya en los protocolos de más bajo nivel para acceder a la red física (Ethernet, Token-Ring).
- Curso Conceptos
  - http://www.ignside.net/man/redes/index.php

¿Cómo viaja la información por la red?

Mediante unos paquetes con un formato predeterminado sin encriptación (20-65536 bytes)



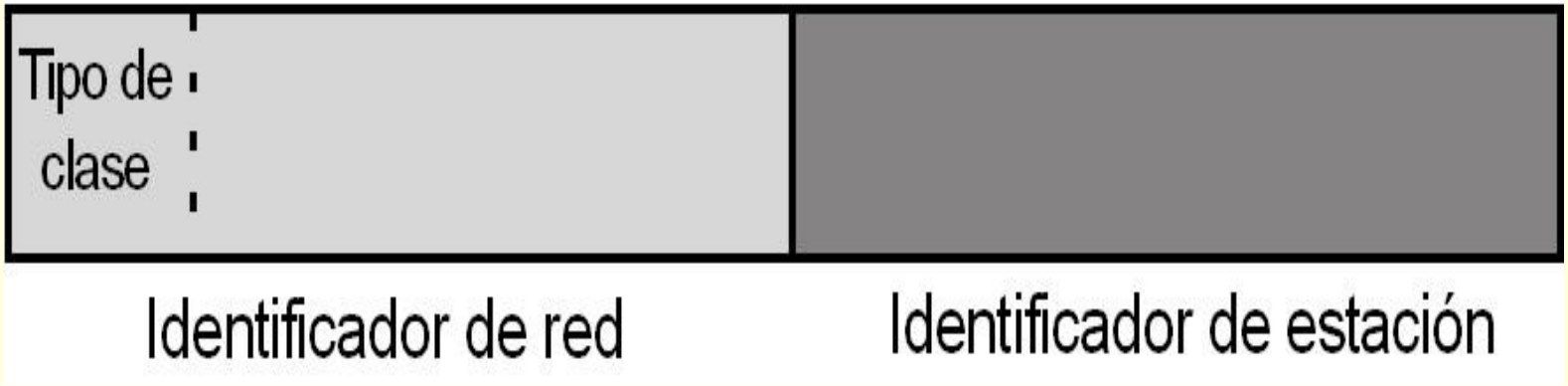
Cabecera IPv4

¿Cómo identificamos a las redes y a los ordenadores en la red?

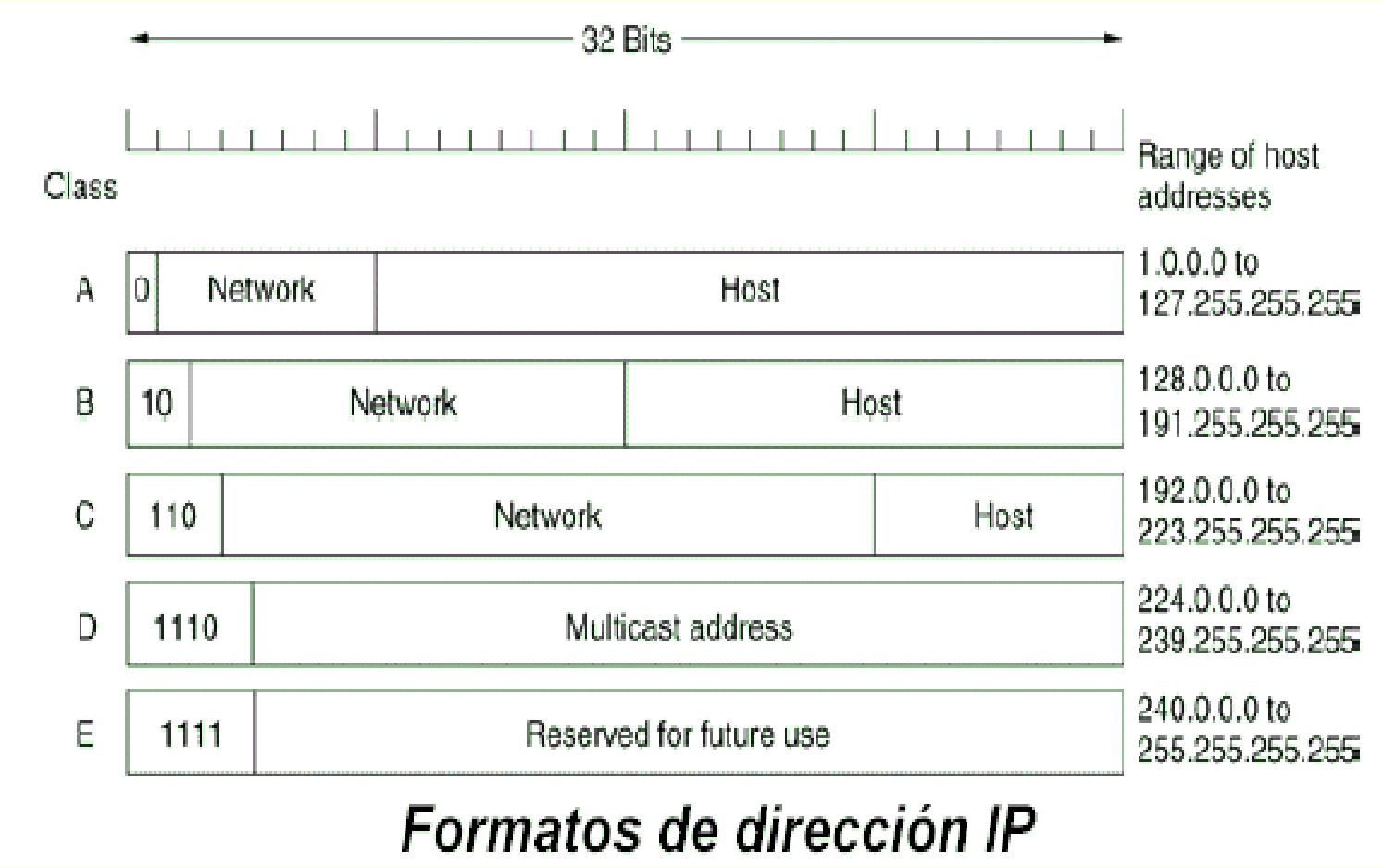
- Mediante direcciones y nombres
  - Dirección IP (identifica redes y equipos de cada red)
  - Nombre de dominio
  - Traducción nombre a dirección IP (DNS)
  - www.uca.es → 150.214.86.11
- Dirección MAC → 00-E0-7D-93-29-AB
- Traducción dirección IP a MAC

Dirección IP

Una dirección Internet consta de cuatro bytes (32 bits) que definen una conexión de la estación a la red.

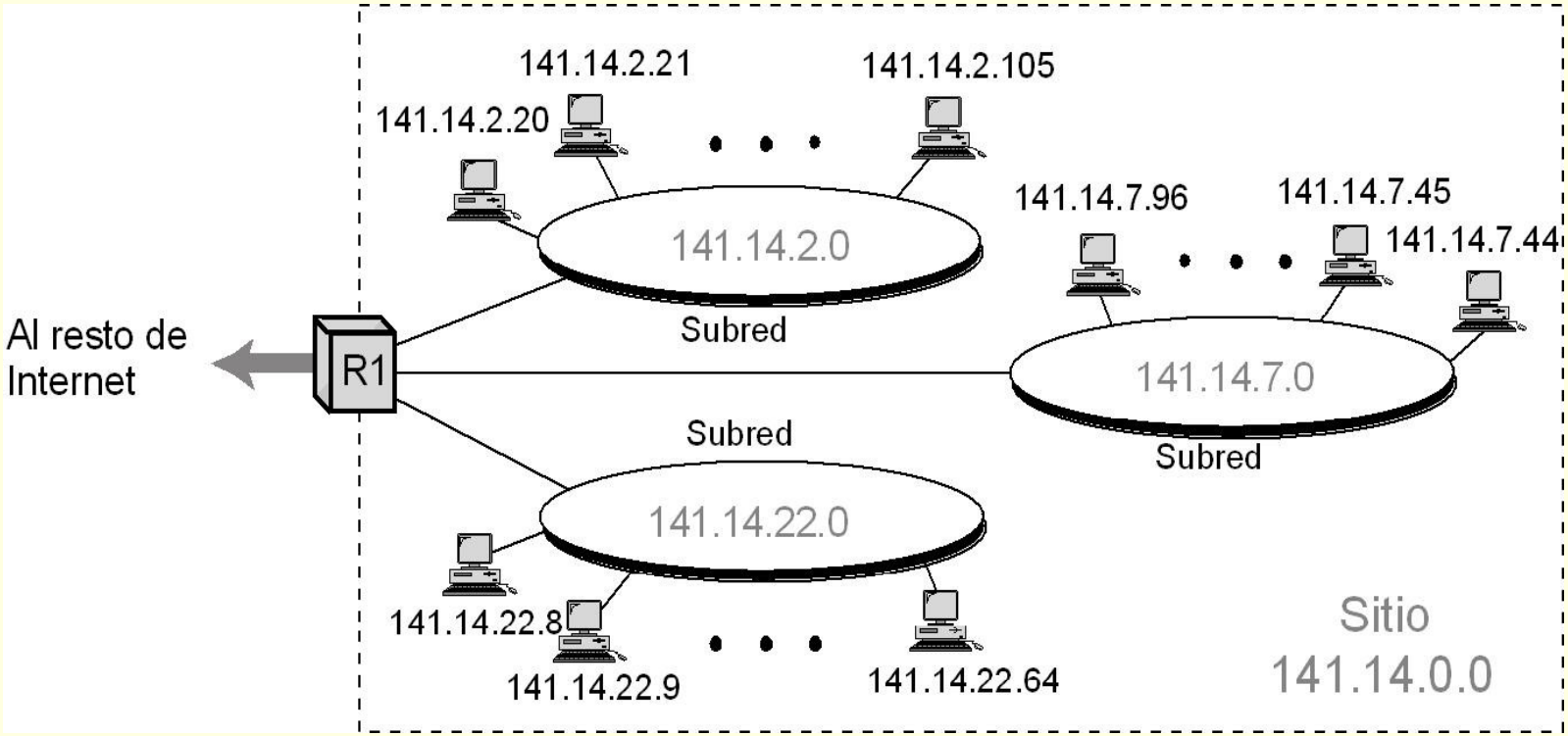


Formatos direcciones IP



Formatos de dirección IP

Una red con tres niveles de jerarquía

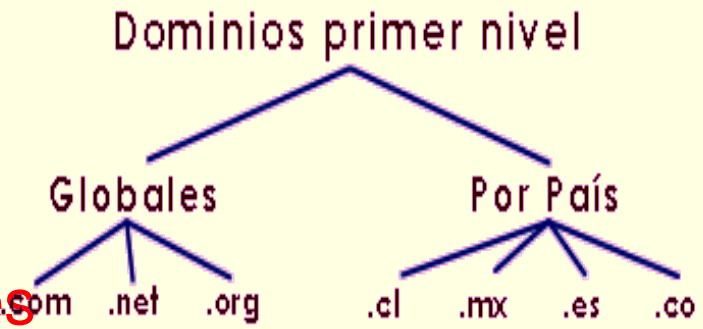


Direcciones privadas

Id. de red privada	Máscara de subred	Intervalo de direcciones IP
10.0.0.0	255.0.0.0	10.0.0.1 - 10.255.255.254
172.16.0.0	255.240.0.0	172.16.0.1 - 172.31.255.254
192.168.0.0	255.255.0.0	192.168.0.1 - 192.168.255.254

Nombre de Dominios

- La norma FQDN
  - (nombre totalmente cualificado= *Full-Qualified Domain Name*)
  - usuario@dominioN...dominio3.dominio2.dominio1
- Estilo de los dominios de primer nivel
  - Estilo genéricos gTLD
    - Tres letras (Las .com)
  - Estilo por paises ccTLD
    - Dos letras, y por países
      - .es



¿Cómo asignamos las direcciones IP a las máquinas?

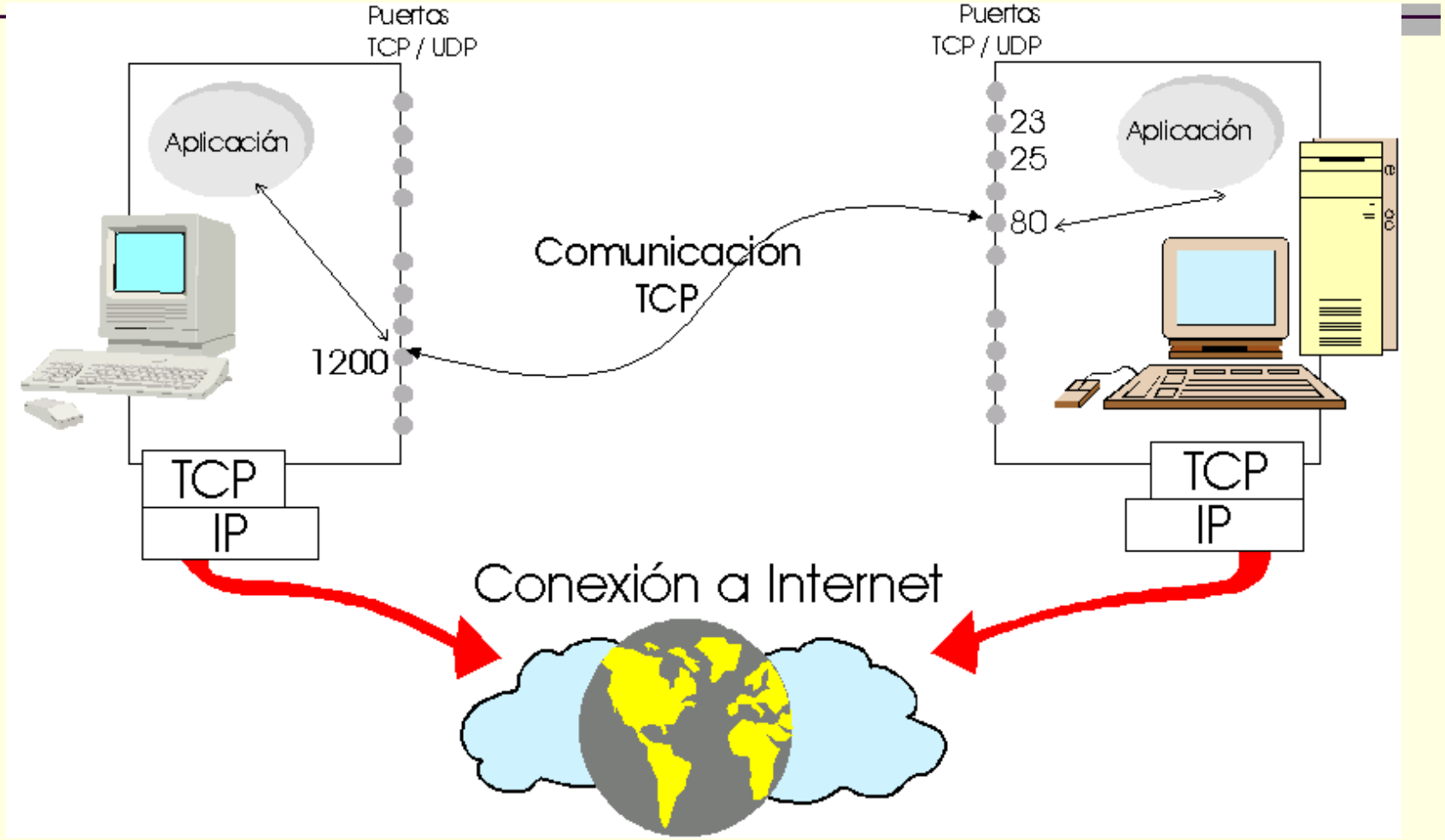
- A nuestra organización
  - Direcciones IP reales:
    - la autoridad de la región → ISP
  - Direcciones IP privadas
    - El administrador de cada red
- A nuestra máquinas
  - Direcciones fijas
  - Direcciones dinámicas (DHCP)

Puertos ¿Cómo identifico la aplicación a la que va destinada la información?

- A cada aplicación se le asigna una única dirección (puerto)
  - Cuando se produce una solicitud de conexión a dicho puerto, se ejecutará la aplicación correspondiente.

Servicio o Aplicación	*Puerto*
File Transfer Protocol (FTP)	21
Telnet	23
Simple Mail Transfer Protocol (SMTP)	25
Gopher	70
Finger	79
Hypertext Transfer Protocol (HTTP)	80
Network News Transfer Protocol (NNTP)	119

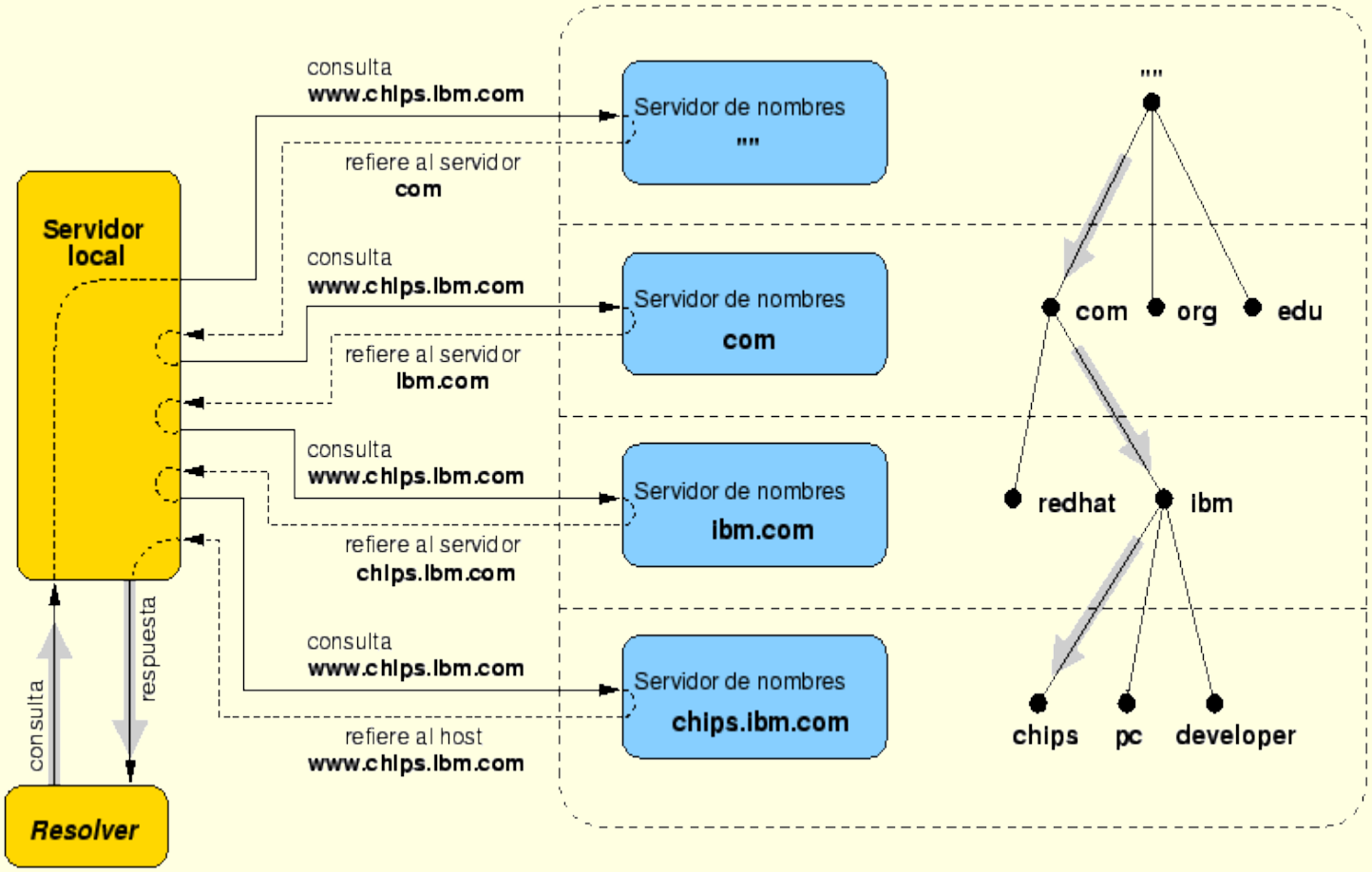
Puertos


Puertos
TCP / UDP
Aplicación
1200
Comunicación
TCP
TCP
IP
Puertos
TCP / UDP
23
25
80
Aplicación
TCP
IP
Conexión a Internet

¿Cómo traducimos los nombres de dominios a direcciones IP?

- El nombre DNS, que consta de dos partes: un nombre de host y un nombre de dominio
- Resolución de nombres
  - Resolución de nombres por difusión (NetBios)
  - Servicio de nombres Internet de Windows (*WINS, Windows Internet Naming Service*) (NetBios)
  - Resolución de nombres usando el Sistema de nombres de dominio (DNS)
  - Ficheros LMHOSTS (NetBios)
  - Fichero HOSTS (DNS)

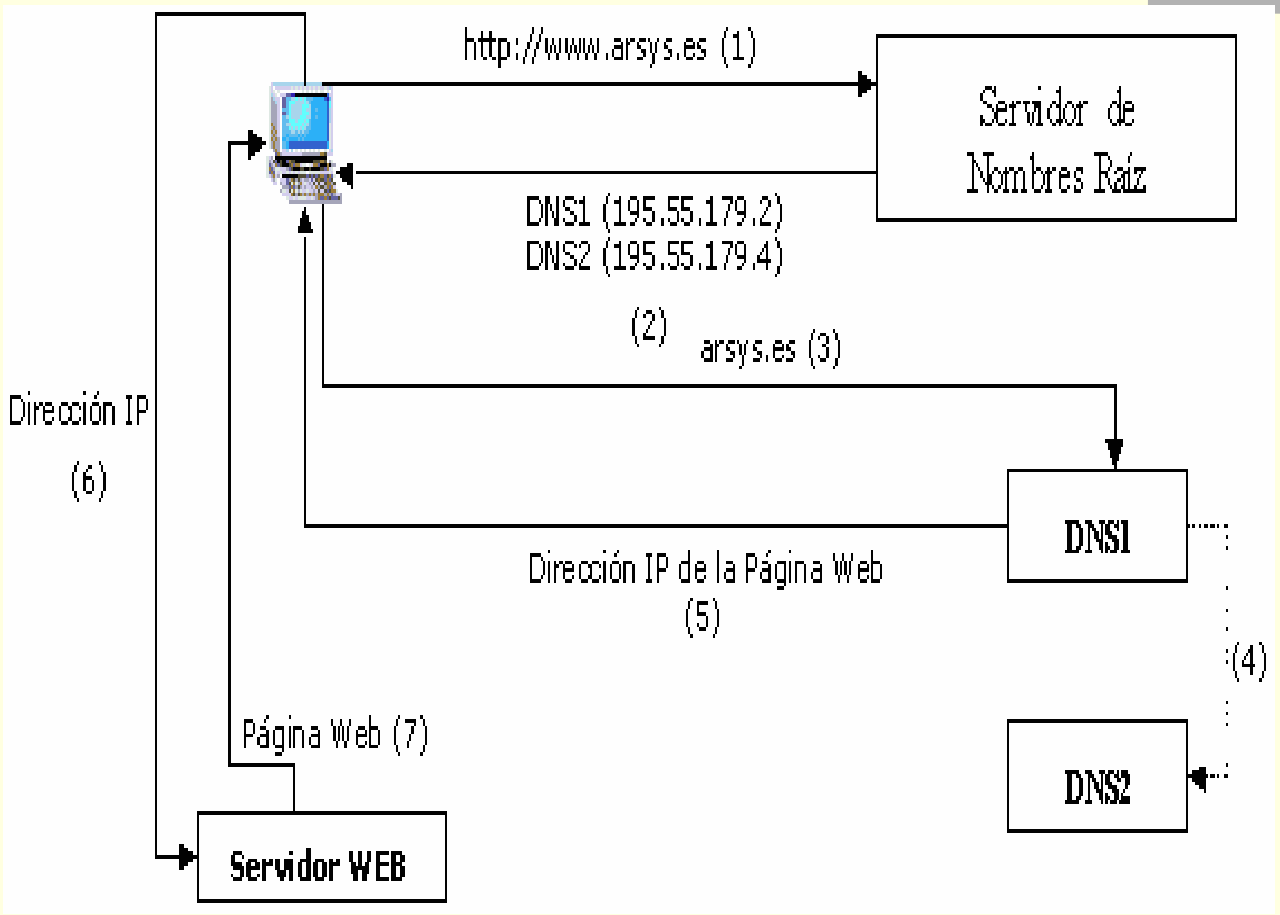
Resolución de nombres



Ejemplo

- A través de su navegador Vd. pide consultar la página web http://www.arsys.es.
- El navegador busca la información de las DNS del dominio arsys.es.
- Internet está ordenada en forma de árbol invertido, si no encuentra la información en su ordenador, irá a buscarla a su Servidor de Conexión
- De no estar, seguirá buscándola a niveles superiores, y en último lugar lo encontrará en el Servidor de Nombres Raíz

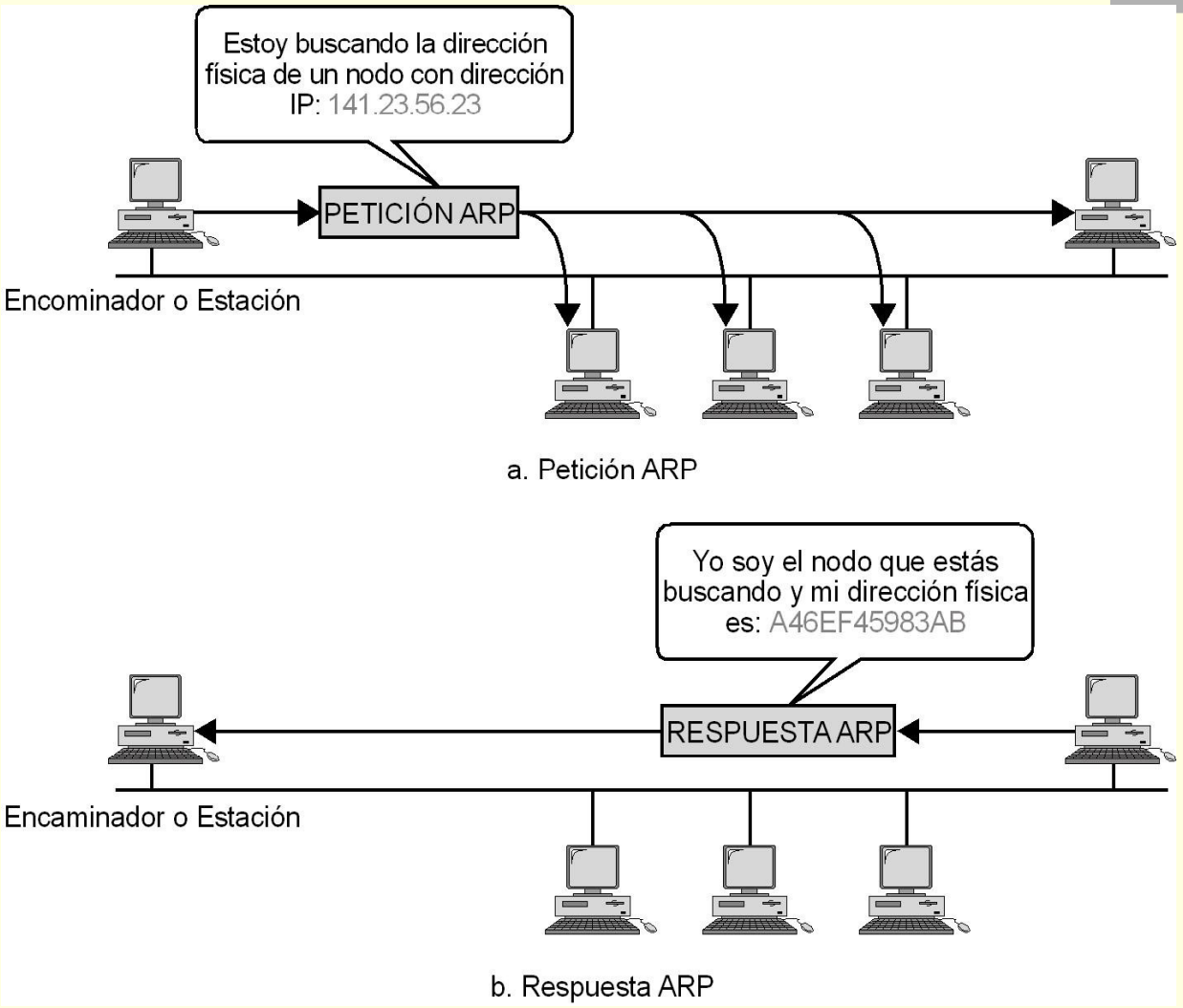
Ejemplo


http://www.arsys.es (1)
Servidor de Nombres Raíz
DNS1 (195.55.179.2)
DNS2 (195.55.179.4)
(2)
arsys.es (3)
Dirección IP
(6)
DNS1
Dirección IP de la Página Web
(5)
(4)
Página Web (7)
DNS2
Servidor WEB

Relación entre direcciones IP y direcciones físicas

- ARP:
  - Convierte una dirección IP en una dirección física
- RARP:
  - Convierte una dirección física en una dirección IP
- En cada host debe existir una tabla de encaminamiento, que está limitada a la red que pertenece
- Si la dirección IP no pertenece a la red, los paquetes IP hacia el gateway o router

ARP


Estoy buscando la dirección física de un nodo con dirección IP: 141.23.56.23
PETICIÓN ARP
Encominador o Estación
a. Petición ARP
Yo soy el nodo que estás buscando y mi dirección física es: A46EF45983AB
RESPUESTA ARP
Encaminador o Estación
b. Respuesta ARP

AMENAZAS EN INTERNET


IT / Security Managers
www.StrangeCosmos.com

QUÉ DEBE SER PROTEGIDO?

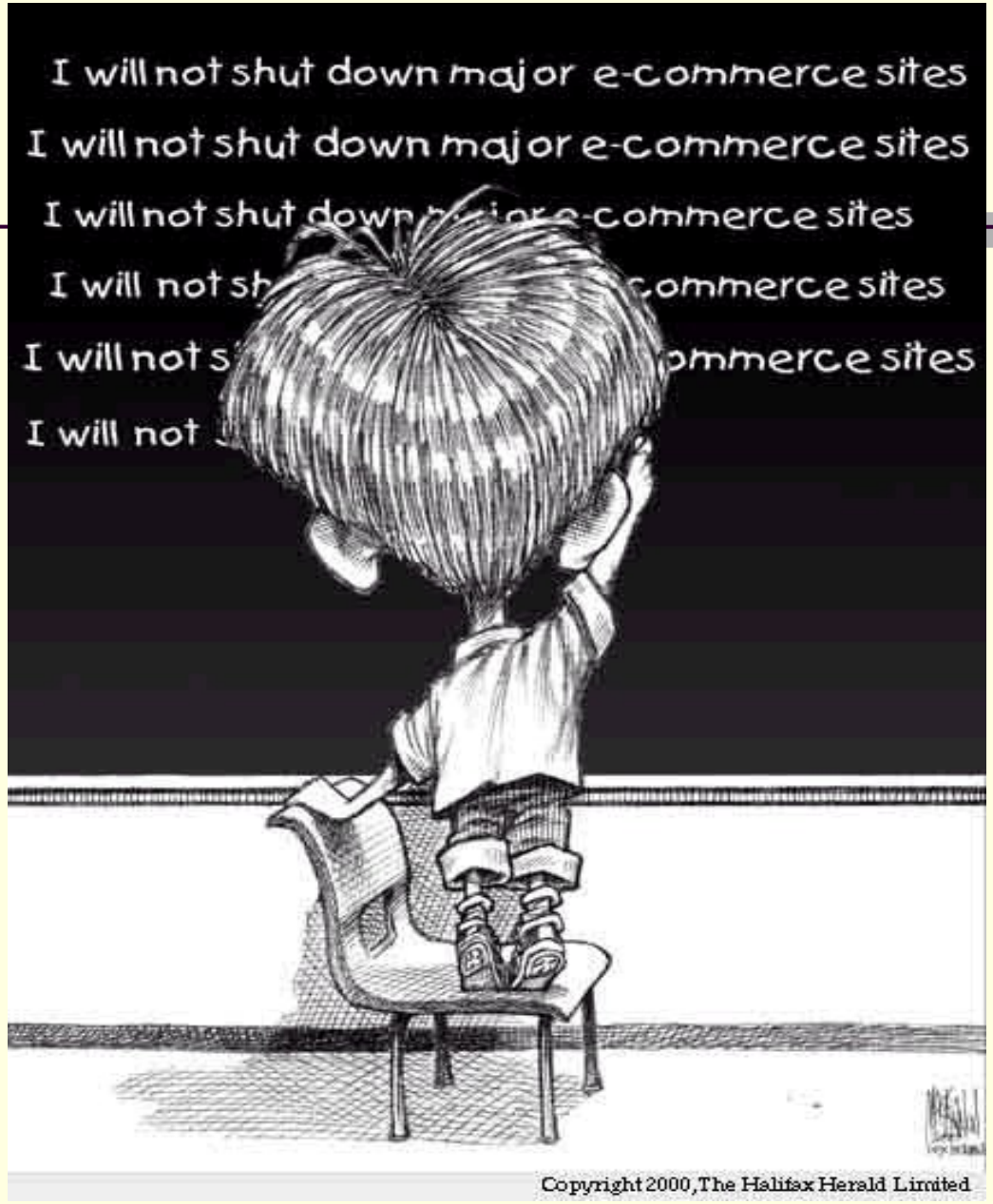
- Sus Datos
  - Confidencialidad – Quiénes deben conocer qué
  - Integridad – Quiénes deben cambiar qué
  - Disponibilidad - Habilidad para utilizar sus sistemas
- Sus Recursos
  - Su organización y sus sistemas

QUÉ DEBE SER PROTEGIDO?

- Su Reputación
  - Revelación de información confidencial
  - Realización de fraudes informáticos
  - No poder superar un desastre
  - Utilización de software ilegal

¿De Quién nos Defendemos?

- **Gente de adentro**:
  - Empleados o personas allegadas.
- **Anti gobernistas:**
  - Razones obvias para justificar un ataque.
- Un **cracker** que busca algo en específico:
  - Es problemático pues suele ser un atacante determinado. Puede estar buscando un punto de salto.


I will not shut down major e-commerce sites
I will not shut down major e-commerce sites
I will not shut down
-commerce sites
I will not sh
commerce sites
I will not s
ommerce sites
I will not
Copyright 2000, The Halifax Herald Limited

De qué nos defendemos?

- Fraude
- Extorsión
- Robo de Información
- Robo de servicios
- Actos terroristas
- Reto de penetrar un sistema
- Deterioro

De qué nos defendemos?

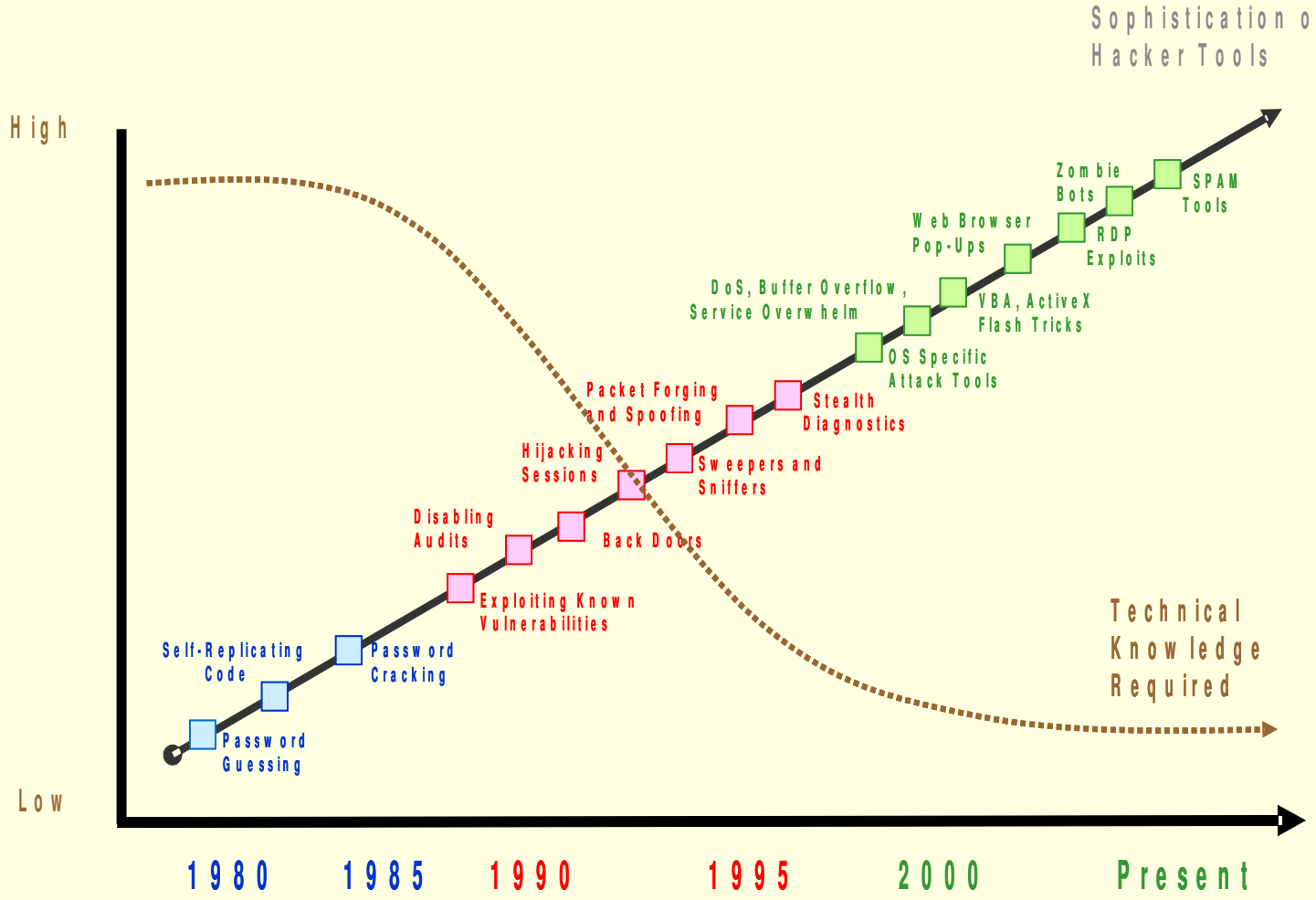
- Desastres Naturales
  - Terremotos
  - Inundaciones
  - Huracanes
  - Incendios

De qué nos defendemos?

- Tecnología
  - Fallos en procedimientos
  - Fallos en el software aplicativo
  - Fallos en el software Operativo
  - Fallos en el hardware
  - Fallos en los equipos de soporte
  - Paros, huelgas

History of Hacking Tools

¿Debemos preocuparnos?



Una madrecita
Aprendiendo a
"Hackear".

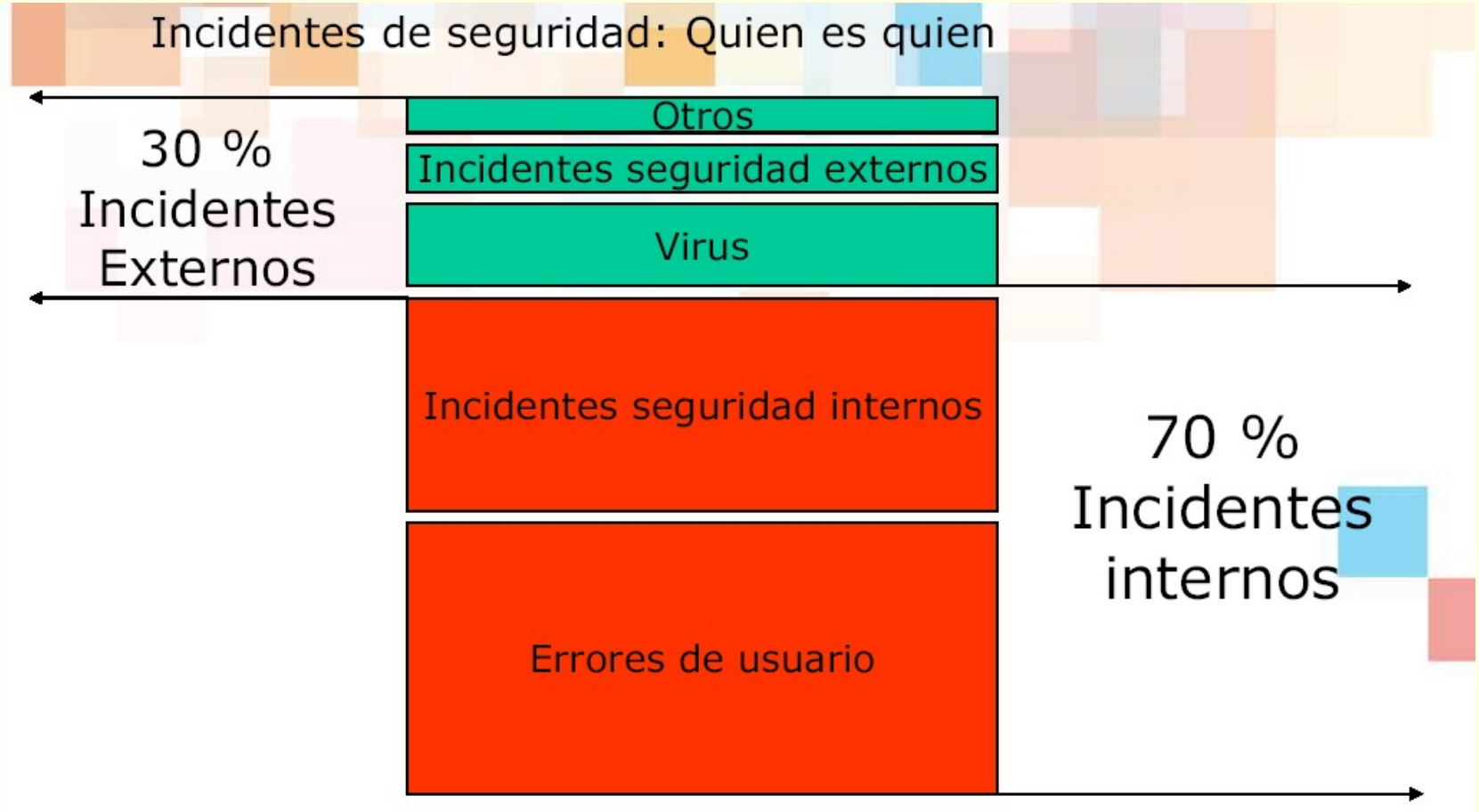
¿De qué amenazas debe defenderse un sistema seguro?

- Interrupción
  - Los recursos del sistema son destruidos, o no están disponibles o están inservibles.
  - Afecta a la disponibilidad del sistema.
    - Ejemplo: Destrucción de un elemento del *hardware* del sistema.
- Intercepción
  - Un elemento no autorizado accede a un recurso del sistema.
  - Afecta a la privacidad del sistema.
    - Ejemplo: Pinchar una línea de comunicación de la red

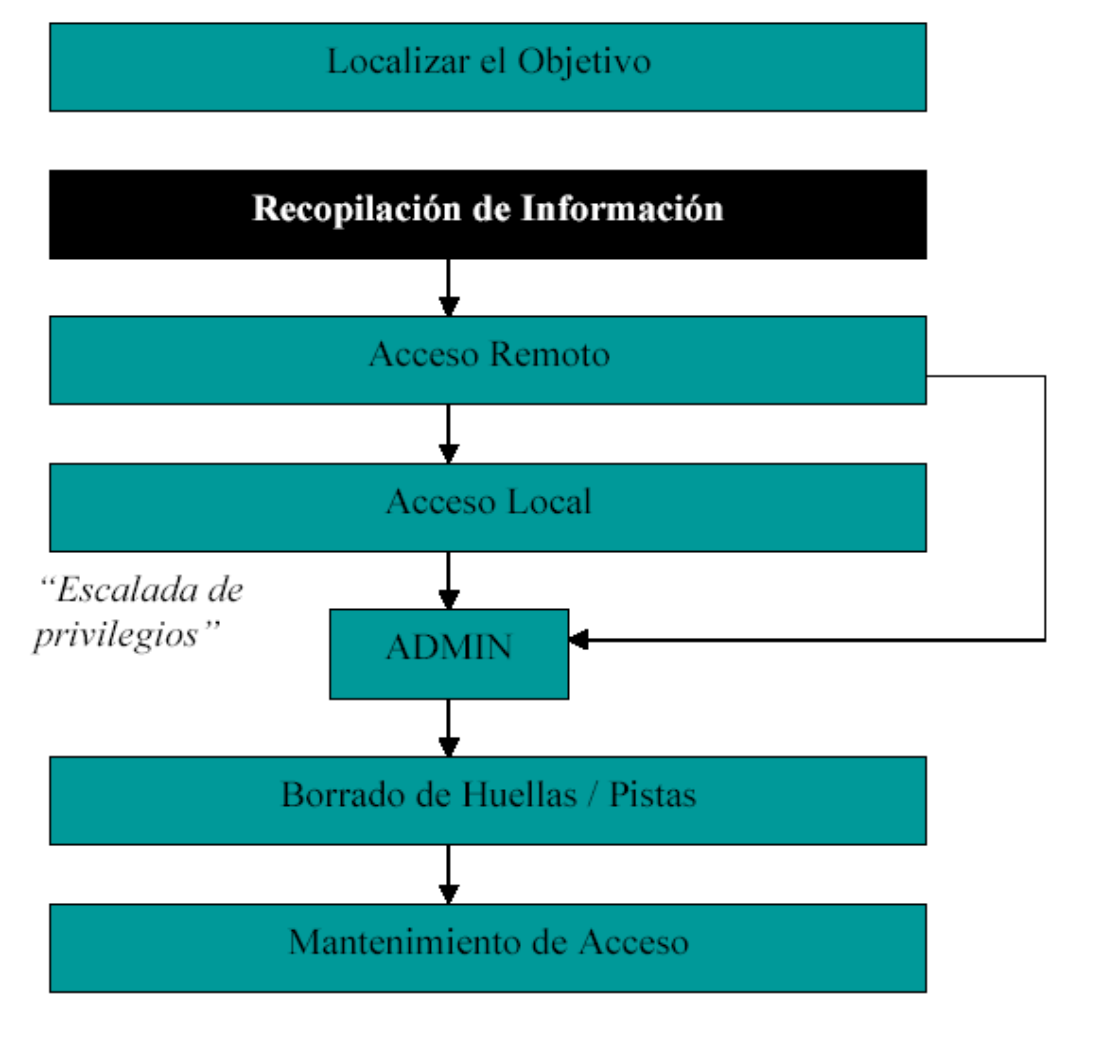
Tipos de amenazas (II)

- Modificación
  - Acceso y modificación de un recurso del sistema
  - Afecta a la integridad del sistema
    - Ejemplo: Modificación de un programa o fichero.
- Fabricación
  - Inserción de elementos ajenos al sistema
  - Afecta a la integridad del sistema
    - Ejemplo: Añadir un registro a un fichero o generar un mensaje en la red

Fuente de los incidentes



¿Cómo nos atacan?
Anatomía de un ataque



Spoofing

- *Uso de técnicas de suplantación de identidad*
- IP SPOOFING:
  - Suplantación de IP. Consiste básicamente en sustituir la dirección IP origen de un paquete TCP/IP por otra dirección IP a la cual se desea suplantar
- ARP SPOOFING:
  - Suplantación de identidad por falsificación de tabla ARP
    - Cambiar la dirección origen por una que es aceptada por el filtro
- DNS SPOOFING:
  - Suplantación de identidad por nombre de dominio. Se trata del falseamiento de una relación "Nombre de dominio-IP" ante una consulta de resolución de nombre
- WEB SPOOFING:
  - Suplantación de una página web real
- MAIL SPOOFING:
  - Suplantación en correo electrónico de la dirección e-mail de otras personas o entidades. es tan sencilla como el uso de un servidor SMTP configurado para tal fin

Ataques

- Hijacking
  - Significa "Secuestro" en inglés y en el ámbito informático hace referencia a toda técnica ilegal que lleve consigo el adueñamiento o robo de algo (generalmente información) por parte de un atacante
    - Introducirse en la comunicación aprovechando una sesión abierta por un usuario con privilegio
- DoS Denegación de servicios con paquetes UDP o ICMP
  - Destruye paquetes
- Pharming (Ataques al DNS)
  - Modifica la memoria cache del DNS (IP/nombre)
  - Los ataques mediante pharming pueden realizarse de dos formas: directamente a los servidores DNS, con lo que todos los usuarios se verían afectados.
  - O bien atacando a ordenadores concretos, mediante la modificación del fichero "hosts" presente en cualquier equipo que funcione bajo Microsoft Windows o sistemas Unix.

Estafas on line

- Estafas piramidales
- “premios” llamando a numeros de tarifación especial
- Subastas o ventas ficticias
- Comercios ficticios
- Solicitud a entidades bancarias de tarjetas de créditos (con DNI y nóminas falsas)
- CARDING:
  - Compra con números de tarjetas válidas (programa generador de números)
- SCAM o cartas nigerianas
  - Captación de “mulas” o intermediarios para blanquear dinero (Wester Union, PayPal)

Picaresca (ingeniería social)

- Objetivo: entrar en redes u obtener secretos, engañando a la gente para que revelen contraseñas y otra información confidencial
- Apelan a las inclinaciones más profundas de la persona: el miedo, el deseo, la codicia o incluso la bondad
- Aplicaciones:
  - Timos
  - Phishing
  - Bulos


CYBER CRIME
Hijacking the Net
Protect

Qué es el Phishing

- Suplantación de páginas o sitios web, que permite al estafador, mediante engaño, conocer los datos privados y personales que se utilizan en operaciones económicas
  - Correo + spam + ingeniería social + secuestro DNS + dominios similares
- Nueva forma de fraude
- Se basa en la picaresca (ingeniería social)
- Objetivo: Robo de identidad digital
  - Phishing8.swf

Phishing: Procedimiento

- Un atacante (el phisher) se hace pasar por una compañía o institución financiera de reconocido prestigio
- Envía mensajes de forma masiva (el primer cebo), habitualmente a través del correo electrónico, aunque podrían utilizarse otros canales
- Los mensajes están dirigidos a potenciales clientes (phish, el pescado) de la organización suplantada
- Si muerden el anzuelo son redirigidos a un sito web idéntico al original (el segundo cebo)
- Recolecta la información personal
- Una vez robada la identidad de la víctima, el atacante podrá suplantarla ante el servicio legítimo
- 5% de los clientes alcanzados pican 2,5 millones de mensajes en un día

Impacto del Phishing

- Pérdidas directas: dinero robado, emisión de nuevas tarjetas, soporte telefónico, gastos judiciales
- Pérdidas indirectas motivadas por la erosión de la confianza: vuelta a canales tradicionales de comunicación, daño a la imagen, pérdida de clientes
- Amenaza a las relaciones a través del canal electrónico

NORMAS PARA EVITAR EL PHISHING

- http://www.seguridadpymes.es/
- No atienda a correos electrónico escritos en idiomas que no hable: su entidad financiera no se dirigirá a Ud en ese idioma si antes no lo han pactado previamente
- No atienda a correos enviados por entidades de las que no es cliente en los que le pidan datos íntimos o que afecten a su seguridad
- No atienda a sorteos u ofertas económicas de forma inmediata e impulsiva
- No atienda a correos que le avisen del cese de actividades financieras recibidos por primera vez y de forma sorpresiva
- No atienda a correos de los que sospeche sin confirmarlos telefónica o personalmente con la entidad firmante

Medidas

- No acceder a entidades financieras mediante enlaces
- Evitar conectarse en sitios públicos (ciber)
- Comprobar que la conexión es HTTPS
- Finalizar mediante la función “SALIR”
- Desactivar las funciones de almacenamiento de claves en cache

Herramientas anti phishing

- Microsoft IE 7
- NetCraft Toolbar:
  - disponible Internet Explorer y Firefox
- Google Safe browsing:
  - disponible para Firefox
- Ebay Toolbar:
  - disponible para Internet Explorer
- Earthlink Scamblocker:
  - Disponible para Internet Explorer y Firefox
- Geotrust Trustwatch
  - Disponible para Internet Explorer, Firefox, y Flock
- Site Advisor
  - http://www.siteadvisor.com/
- http://www.antiphishing.org/

Spam

- Correo electrónico no deseado ni justificado
  - Vehículo de: Phishing, Virus, Timos, Bulos (Hoax)
- Spim
  - Mensajes no deseados en la mensajería instantánea

Anti spam

- Sistema para servidores anti spam
  - http://www.spamcop.net/
  - http://www.ordb.org/
- Consejos antispam
  - http://www.aui.es/contraelspam/consejos_usuarios.htm
- Protocolos anti-spam
  - **SPF** (Convenio de Remitentes, del inglés ***Sender Policy Framework***)
    - Identifica, a través de los registros de nombres de dominio (DNS), a los servidores de correo SMTP autorizados para el transporte de los mensajes.
    - http://www.openspf.org/
  - DomainKeys
    - Firmas electrónicas del emisor
    - http://antispam.yahoo.com/domainkeys
    - http://ar.antispam.yahoo.com/domainkeys

Antispam

- G-Lock SpamCombat:
  - www.glocksoft.com/sc
- K9:
  - www.keir.net/k9.html
- Outlook Security Agent:
  - www.outlooksecurityagent.com

SpamFighter:

- www.spamfighter.com

- Spamihilator:
  - www.spamihilator.com
- SpamPal:
  - www.spampal.org
- Spamina
- http://www.spamina.com/
- SpamGuard Yahoo_
  - http://antispam.yahoo.com/tools?tool=1

Otros ataques

- Hombre en el medio (MITM)
- Ofuscación de URL
- XSS
- Fijación de sesión
- Maquillaje
- Espionaje del usuario

Zombies

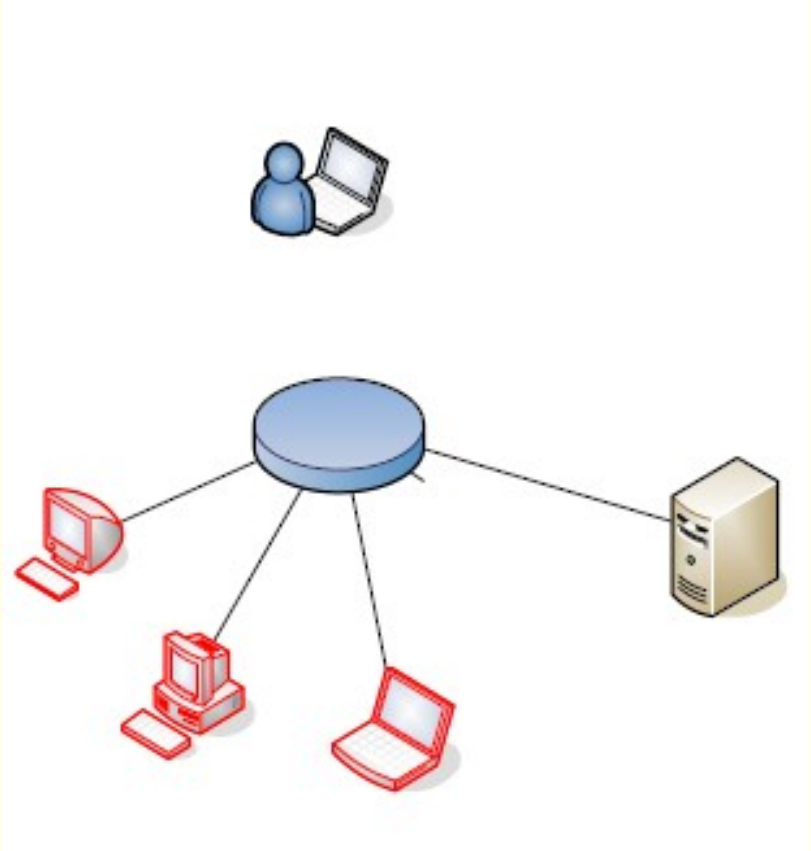
- Equipos comprometidos al servicio de usuarios maliciosos, que utilizan las plataformas corruptas con el total desconocimiento de los propietarios y/o administradores
- Entre las tareas que realizan
  - Envío de spam
  - Servir pornografía
  - Servidores de fraude y phishing
  - Distribución de malware
- Las máquinas zombie se aglutinan en botnets

Hombre en el medio (MITM) Intersección

- un ataque man-in-the-middle (MitM, u hombre en el medio, en castellano) es un ataque en el que el enemigo adquiere la capacidad de leer, insertar y modificar a voluntad, los mensajes entre dos partes sin que ninguna de ellas conozca que el enlace entre ellos ha sido violado (wikipedia)
  - Proxies transparentes
  - Envenenamiento de caché DNS
  - Ofuscación de URL
  - Configuración del proxy del navegador
  - Manipulación del archivo HOSTS

Botnets

- Botnets
  - Redes de ordenadores zombies
  - Sniffer
- Mass Scanning



Ofuscación de URL

- Nombres de dominio similares
- Utilización del login para simular nombre de dominio: desactivado en las últimas versiones de los navegadores
  - http://www.gruposantander.es:login.jsp?
- CodigoActivacionSeguridad=@3368601800
- URL abreviados
  - http://tinyurl.com/3erp1

Cross-Site Scripting (XSS)

- El hiperenlace conduce al sitio verdadero
- Todo es auténtico
- Los certificados digitales también
- Se inserta código para que el formulario se envíe al sitio web del phisher
- Videos de hispaset
  - http://www.hispasec.com/directorio/laboratorio/

Fijación de sesión

- El hiperenlace conduce al sitio verdadero
- Todo es auténtico
- Los certificados digitales también
- Se crea una sesión para que al autenticarse la víctima utilice el mismo testigo
- Conocido el testigo, se puede acceder a sus datos

Maquillaje

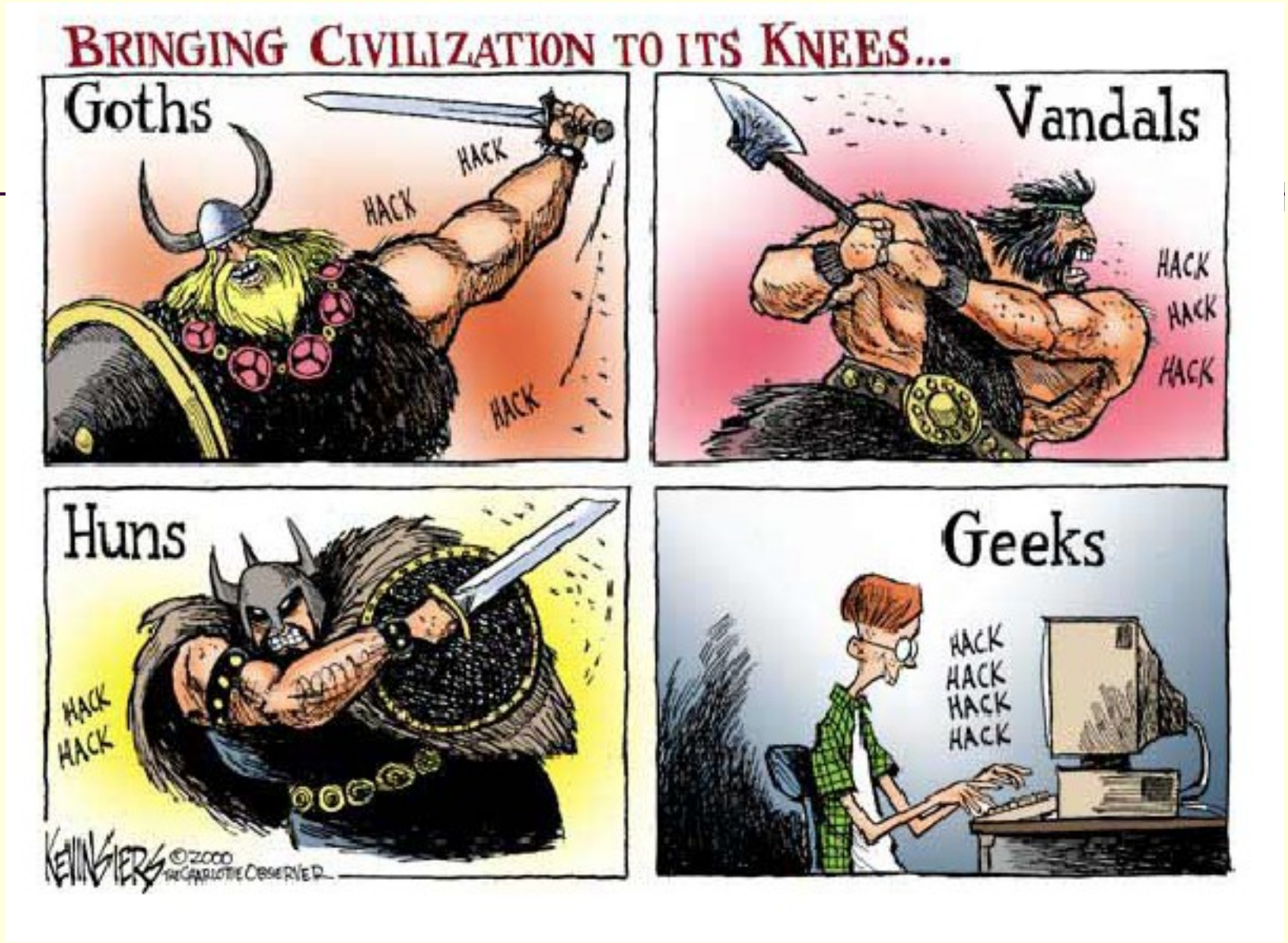
- Manipulación del aspecto del navegador que ve el usuario:
  - Marcos ocultos
  - Sobrescritura del contenido
  - Substitución gráfica

Herramientas de seguridad WEB

- Herramientas gratuitas
  - Paros:
    - www.parosproxy.org
  - Wikto
    - www.sensepost.com/research/wikto
- Herramientas comerciales
  - WebInspect de SPI Dynamics
    - www.spidynamics.com

Hackers

- ¿Qué tengo de valor para un hacker?
  - Espacio de disco
  - Ancho de banda
- ¿Cómo puede encontrarme?
  - Dirección IP


BRINGING CIVILIZATION TO ITS KNEES...
Goths
HACK
HACK
HACK
Vandals
HACK
HACK
HACK
Huns
HACK
HACK
Geeks
HACK
HACK
HACK
HACK
KEVIN SIERS
©2000 THE CHARLOTTE OBSERVER

Privacidad

- Rastro del uso de Internet:
  - Dirección IP
  - Navegador
  - Sistema Operativo
  - Dirección de correo electrónico
  - Páginas visitadas, fotos vistas, documentos leídos,
  - Formularios rellenos
  - Cookies: hábitos de navegación, gustos, etc.

Herramientas de búsqueda de información

- http://johnny.ihackstuff.com/
- google

- http://www.foundstone.com/
- Whois directo e inverso
  - http://www.dnsystem.com/herramientas/index.php
  - http://cqcounter.com/whois/
  - http://www.atomintersoft.com/products/alive-proxy/whois/
- Navegación anónima
  - http://www.all-nettools.com/toolbox

Auditoría Caja Negra

- Se realiza desde fuera
- Ofrece la visión de un hacker
- No puede ser ejecutada desde dentro
- No garantiza “Servidor Seguro”
- No todos los escáner ofrecen los mismos resultados
- SSS, Nessus, GFI Languard, Retina, ISS Real Secure, etc…

Herramientas verificación de seguridad

- Exploración de puertos: superScan
- Whois (Sam Spade www.samspade.org)
- NSLookup y dig
- Rastreo de pila (nmap)
- Trazas (SolarWinds: barridos de ping)
- Captura de cabeceras (wfetch)
- Cheops
- Ettercap
- Nessus
  - http://www.nessus.org

Vulnerabilidades

- Satan, Saint, Sara
- ShadowSecurity Scanner
  - http://www.safety-lab.com
- GFI LanguardNetwork Security scanner
  - http:///www.gfihispana.com
- Retina
  - http://www.eeye.com
- NetBrute, R3X

Vulnerabilidades

- Sans
  - http://www.sans.org/top20/
  - http://www.sans.org/top20/#w1

Auditoría Caja Blanca

- Se realiza internamente
- Con privilegios y visualización completa del sistema
- Se utilizan herramientas proporcionadas por el fabricante o propias
  - MBSA
  - EXBPA
  - MOM 2005….

MBSA

- Ayuda a identificar sistemas Windows vulnerables.
- Escanea buscando actualizaciones no aplicadas y fallos en la configuración del software.
- Escanea distintas versiones de Windows y distintas aplicaciones.
- Escanea en local o múltiples máquinas en remoto vía GUI o línea de comandos.
- Genera informes XML sobre los resultados de cada equipo.
- Corre en Windows Server 2003, Windows 2000 y Windows XPSe
- integra con SMS 2003 SP1, con SUS y WSUS

Escáneres de Vulnerabilidades y Sistemas de Gestión de Parches

- El Microsoft Baseline Security Analyzer puede ser usado para identificar sistemas Windows vulnerables.
  - http://www.microsoft.com/technet/security/tools
- Programa para recuperar paswword
  - http://home.eunet.no/pnordahl/ntpasswd/
- Análisis de seguridad de tu ordenador windows
  - http://onecare.live.com/site/es-es/default.htm

Problemas de protección

- Terminal con sesión abierta
- Puerta secreta (back door)
  - El diseñador del *software* deja una puerta para poder usarla cuando quiera.
- Búsqueda de basura.
  - Información sensible borrada que queda en el dispositivo y puede ser husmeada y reconstruida con las herramientas adecuadas (pc-tools)

Fallos software y hardware

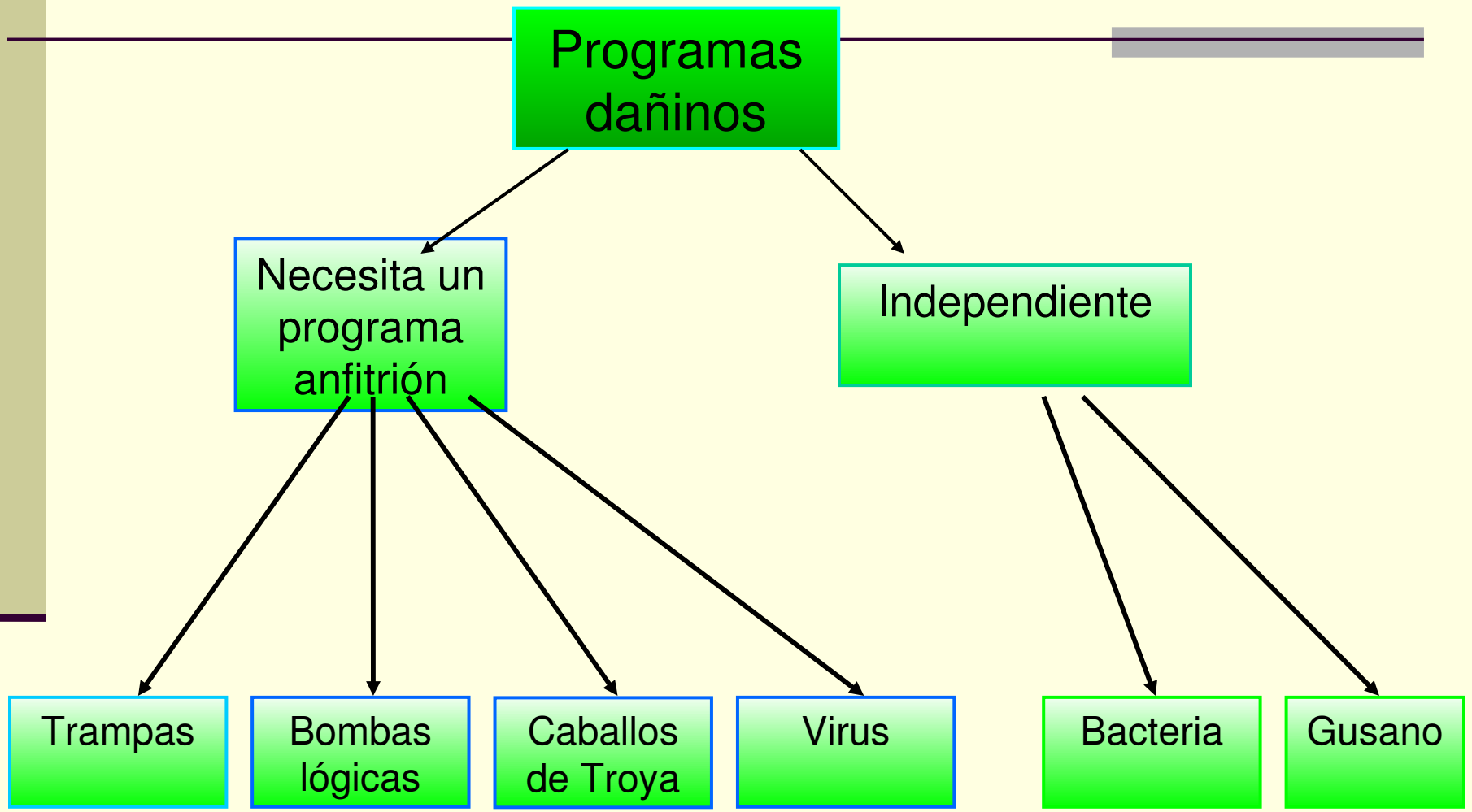
- Tolerancia a fallos
  - Suministro eléctrico: SAI, regletas
  - Conectividad: líneas redundantes, Wifi con vecinos, 3G
  - Hardware: equipos de reserva
- Recuperación de sistemas
  - Copias de seguridad
- Plan de continuidad

Seguridad de menores

- Contenidos indebidos: sexo, violencia
- Revelación de información
- Juegos de azar
- Subastas
- Chat, mensajería, foros

Malware

Taxonomía de los programas dañinos (malware)



Gusanos y bacterias

- Gusanos
  - un programa que se reproduce a través de la red (normalmente se transmite por los mensajes del correo electrónico o por los documentos adjuntos (por ejemplo, los virus de macro).
  - Se autopropagan sin intervención humana
  - Explotan vulnerabilidades en sistemas: Nimda,Blaster, etc.
- Una “bacteria”
  - se reproduce hasta que llena todo el espacio del disco o los ciclos de CPU.

Virus

- Virus: código que se reproduce en otros programas.
  - Capacidad de replicación y destrucción
  - Necesitan del usuario para propagarse
  - Diversos métodos de infección:
    - sector de arranque,
    - archivos ejecutables,
    - MBR, multipartitos,
    - macro (Word, Excel, Access, Lotus)

Dialers y Troyanos

- Dialers
  - Conexión vía modem a números tarificación especial
  - Sin consentimiento ni conocimiento de la víctima
  - Generan gasto telefónico
- Troyanos
  - instrucciones en un buen programa que hace que se produzcan efectos perjudiciales (enviando datos o contraseñas a un atacante a través de la red).
  - Realizan tareas encubiertas
  - Disfrazados de programas útiles
  - Algunos permiten control remoto del equipo

Spyware

- Software espía instalado sin el conocimiento del usuario
- Normalmente explotan vulnerabilidades en IE
- Presente en algún software gratuito (e incluso de pago)

Definiciones

- Carga útil:
  - los efectos perjudiciales que lleva a cabo el programa dañino, después de que haya tenido tiempo de extenderse.
- Bomba lógica:
  - código dañino que se activa con un acontecimiento (por ejemplo, una fecha concreta).
- Trampas:
  - punto de entrada sin documentar escrito en código para depurar y que puede permitir la entrada de usuarios no deseados.
- Huevo de Pascua (easter egg):
  - código extraño que lleva a cabo algo “interesante”. Es una forma de mostrar que los programadores controlan el producto.

¿Que podemos hacer?

- Diseñar nuestra **política** de seguridad
  - Diccionario de R.A.L: Política:
    - Orientaciones o directrices que rigen la actuación de una persona o entidad en un asunto o campo determinado
- Implementar los **mecanismos** de seguridad para realizar la política diseñada
  - Mecanismo:
    - Especifica cómo llevar a la práctica las políticas de seguridad y cómo hacerlas cumplir en un sistema determinado.

Primera medida: autentificación

Poner una cerradura y tener la llave

Métodos de autentificación (validación de la identidad)

- El objetivo de la validación es:
  - Permitir el acceso a los usuarios legítimos del sistema y denegarlo a los no autorizados.
- La validación se basa en una combinación de tres conjuntos de elementos
  - Algo que tú sabes
    - Nombre de usuario y contraseña
  - Algo que tú tienes
    - Certificados X.509 en el ordenador o en
    - tarjetas inteligentes
  - Algo que tú eres
    - Escáner de huellas o de retina

'En Internet nadie sabe que eres un perro'

Ataques a las contraseñas

- Con acceso al fichero
  - Diccionario
    - Con 8 caracteres $128^8 = 7{,}2 * 10^{16}$
    - Un diccionario solo centenares de miles
  - Prueba y ensayo (*task force*)
- Caballos de Troya
- Keylogger
- Espías en la red (*sniffer*)
- Ingeniería social
  - Mirar el teclado, los post-tip...
- Bugs o errores en los programas

Espionaje del usuario

- Registro de la actividad del usuario
- Keyloggers: hardware y software
- Screengrabbers

Curiosidad Fraude en cajeros

Fraude

Banca electrónica

- Para operaciones de consulta
  - Nombre de usuario + contraseña
- Para operaciones
  - 2ª clave de operaciones dinerarias
  - Tarjeta de coordenadas
  - Teclados virtuales en pantalla e introducir sólo algunos dígitos de la clave de modo aleatorio

Consejos

- No utilizar formularios no seguros para introducir datos de identificación (que no sean HTTPS)
- Configurar el navegador para:
  - Que no guarde las claves
  - Que no utilice caché

Medios de pagos

para el e-commerce

Tarjetas 3 D secure

- Verified by visa
  - http://www.visaeu.com/spainvbv/
- Mastercard secure code
  - http://www.mastercard.com/us/personal/es/serv

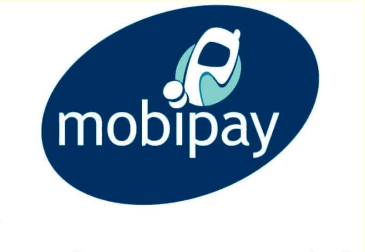
Vini paga

- Solo Internet explorer
- http://www.coit.es/publicac/publbit/bit1

Medios de pago

- Paypal
  - Comprar sin compartir información financiera
  - http://www.paypal.es/es

Mobipay



- Pago por teléfono móvil
  - http://www.mobipay.es

Características del sistema Mobipay

- Los medios de pago activados podrán ser tarjetas existentes o ser medios de pagos que las entidades diseñen específicamente para este canal.
- El usuario solo puede activar/desactivar medios de pagos a través de su entidad emisora.
- Existe un “Número de Identificación Personal” (NIP) por cada medio de pago que es gestionado por la entidad emisora.
- Sólo es conocido por el titular.
- El usuario autoriza cada transacción mediante la introducción del NIP correspondiente al medio de pago utilizado, siendo equivalente a la firma manuscrita.
- En cada transacción, Mobipay permitirá que el usuario elija pagar con cualquiera de los medios de pago que tiene activados en su cartera y son admitidos en el establecimiento.
- Mobipay aporta funcionalidad para gestionar de forma fácil los medios de pago dentro de la cartera.

Compra presencial: identificativos de cartera

Emisor 1

Emisor 2

Emisor 3

Emisor 4

Emisor 5

CARTERA MOBIPAY

El cliente puede activar su cartera mediante cualquiera de los siguientes identificadores:

- **El número de teléfono: 6XX 12 34 56**
- **El PAN mobipay: código equivalente a un número de tarjeta.**
- **El código de barras para establecimientos que tengan scanner instalado en el terminal**

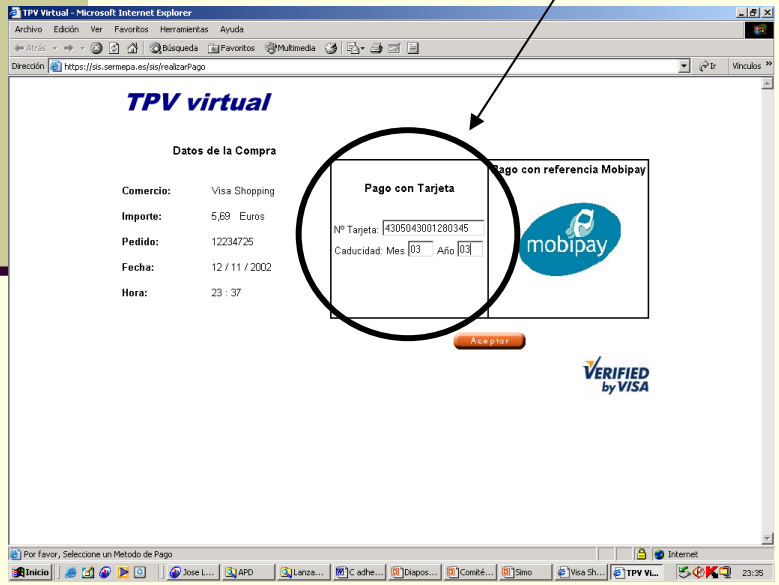
Pago / compra por referencia en internet: propuesta de valor

- Usuario
  - No introduce ningún dato relativos a sus medios de pago en internet.
  - Autoriza cada transacción mediante la introducción de su número secreto personal.
  - No requiere contar con un software especial en el PC.
  - Operativa homogénea con el resto de compras mobipay.
- Comercio:
  - Garantiza el no repudio de la transacción.

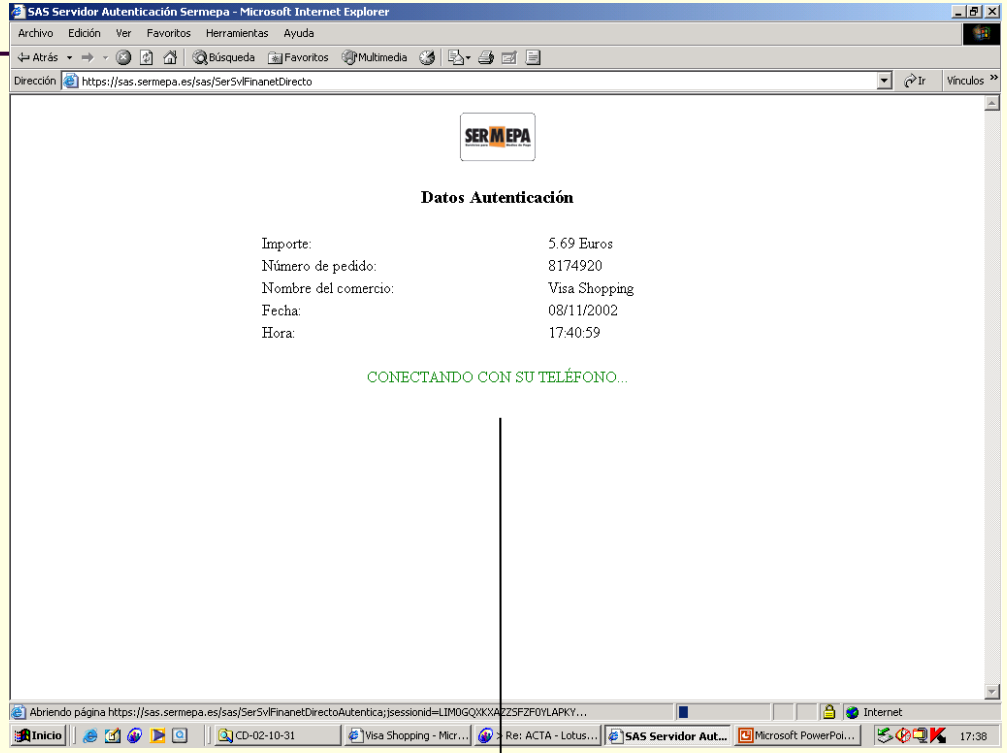
Mobipay como mecanismo para hacer compra segura en internet fija: autenticación 3D Secure.

Paso 1: Selección de los artículos

Paso 2: Introducción del Nº de la Tarjeta y fecha de caducidad



Paso 3: El Sistema pide la autenticación del cliente a través de Mobipay



“CONECTANDO CON SU TELÉFONO”

Mobipay como mecanismo para hacer compra segura en internet fija: autenticación 3D Secure.

Paso 4: El teléfono móvil pide la autenticación mediante la introducción del NIP correspondiente al medio de pago

MOBIPAY.
5,69 EUR
1 VISA BBVA
Autorice con NIP

Paso 5: El teléfono móvil informa de la confirmación del pago

MOBIPAY.
5,69 EUR
1 VISA BBVA
Operación Realizada

Paso 5bis: El comercio informa de la confirmación del pago.

Compra en internet mediante referencia mobipay.

Paso 1: Tecleo en el móvil del código de operación y del número de referencia que indica el TPV Virtual

*145*1* 518464#

Paso 2: El teléfono móvil presenta los datos de la compra (comercio e importe) y solicita medio de pago y clave secreta.

COMPRA REF.
VISA SHOPPING
5,69 EUR
1 VISA BBVA
Autorice con NIP
Elija MP con 99

Paso 3: El teléfono móvil informa de la confirmación del pago

COMPRA REF.
VISA SHOPPING
5,69 EUR
1 VISA BBVA
Operación Realizada

Paso 3bis: El comercio informa de la confirmación del pago.

- http://checkout.google.com

¿Cómo funciona Ukash?

- Compre en efectivo un cupón o tarjeta Ukash en su tienda más próxima o en tiendas o puntos de venta Telecor o en oficinas de Correos.
- Después utilice el número único Ukash de 19 dígitos de su cupón o tarjeta para comprar bienes y servicios en Internet.
- Obtener Ukash es instantáneo:
  - no es necesario esperar a recibir una tarjeta del banco o registrarse en ningún sitio.
  - http://www.ukash.com/es-es

epagado

- https://www.epagado.com/www/es-es/
- Correos
- ebankinter

Autentificación fuerte

- OTP (one time password)
  - dispositivo generador de contraseñas de un solo uso
- Certificados digitales
- Sistemas biométricos
- EMV

Tarjetas chip **EMV**

- **EMV** es un acrónimo de **E**uropay, **M**astercard y **V**isa
- EMV es un standard para interoperar de IC cards ("Chip cards") y IC capable POS terminals, para autentificación de tarjetas de crédito y débito
- Se aplica a **tarjetas chip**
  - http://emission.rtspain.com/
  - http://www.fnmt.es/es/html/tage/sc_tage.asp

*E*uropay
*M*astercard
*V*isa

Contraseña (I) normas

- Requerir que el usuario normas para proteger la contraseña
- Los problemas de la contraseña están relacionados con la dificultad de mantenerla secreta.
  - Deben de ser largas
  - No se deben de anotar
  - Posibles de recordar
  - Deben de evitarse: Nombres familiares, fechas familiares, DNI, nombre de la novia/novio, del perro o del canario (pájaro)
  - Deben de caducar obligando al usuario a cambiarla
  - Intercalar números, letras y signos de puntuación
  - NO USAR LA MISMA CONTRASEÑA PARA DISTINTOS SISTEMAS

Autentificación con objeto físico (*Tokens*)

- Tarjetas magnéticas
- Tarjetas Chip
- Memorias EPROM o Flash
- Pequeños ordenadores
- Estos sistemas complementan otros sistemas de acceso:
  - Contraseña, biométricos o certificados digitales
- Problema de la pérdida del objeto

Sistemas biométricos

- Utilizan características físicas del usuario
- Las características deben ser únicas y que no cambien
- Ventajas
  - Son Intransferibles
  - Muy seguros
  - No necesitan gestión
- Inconvenientes
  - Necesitan electrónica adicional
  - Rechaso del usuario
  - Costo (100 dólares por contraseña)

Tipos de sistemas biométricos

- Medidas de acierto
  - FAR (*False Acceptence Rate*) % malos dados por buenos
  - FRR (*False Rejet Rate*) % buenos dados por malos
  - SR (*Succes Rate*) = 100 - (FAR+FRR)
- Emisión de calor o termograma
- Huellas dactilares FRR= 0,001 %
- Mano
- Iris del ojo. FAR 0,006 % FRR 0,0007 %
- Retina FAR 0 % FRR 12 %
- Firma
- Voz
- Reconocimiento facial.

Autentificación con certificados digitales

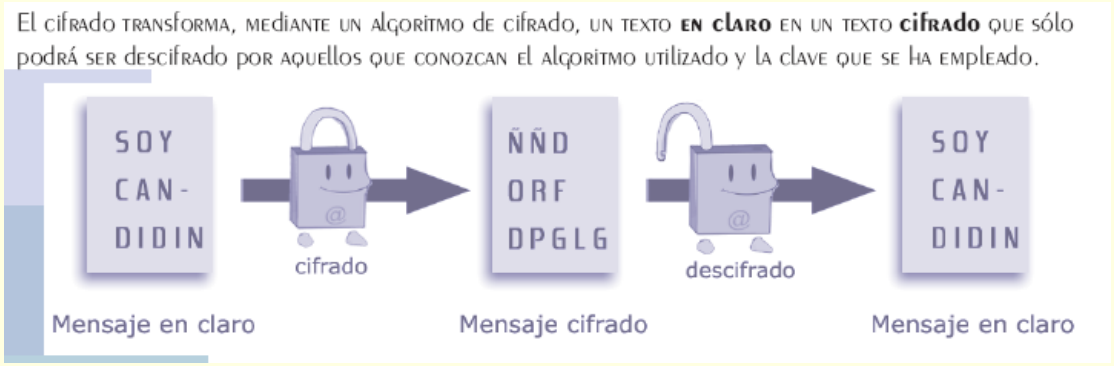
- Utiliza criptografía
- Es un objeto lógico, no físico
- El usuario debe tener
  - Un a clave privada de algún algoritmo asimétrico
  - Un certificado digital con la clave pública pareja de la privada y firmado digitalmente por el servidor
- Ejemplo: declaración de la renta por Internet

Segunda medida: cifrado de datos

Esconder las cosas de valor

Criptografía

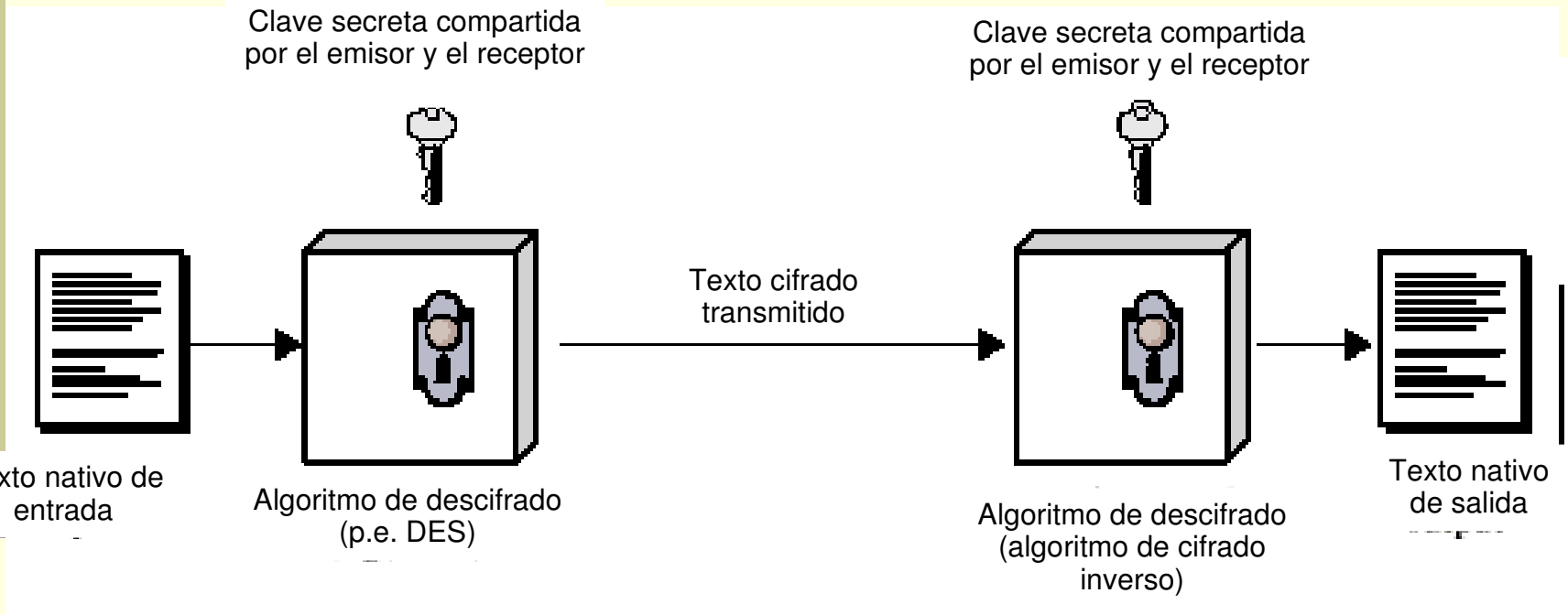
- El conjunto de técnicas que permiten asegurar que un mensaje solo es entendible por aquel al que va dirigido
  - Es el arte de escribir en clave
  - Protege la información del acceso de quien no está autorizado a conocerla
- La criptografía oculta datos
  - Cifrado: ocultación de datos
  - Descifrado: liberación de datos
- Elementos:
  - clave y algoritmos



Clases de Criptografía

- Criptografía de clave privada: la información se cifra con una clave privada que tienen tanto el remitente como el receptor (simétrica DES)
- Criptografía de clave pública: dos claves separadas pero relacionadas una pública y otra privada (asimétrica)

Cifrado convencional



Ingredientes

- Texto nativo.
- Algoritmo de cifrado.
- Clave secreta.
- Texto cifrado.
- Algoritmo de descifrado.

Requisitos de seguridad

- Algoritmo de cifrado robusto:
  - Incluso si conoce el algoritmo, no debería ser capaz de descifrar el texto o describir la clave.
  - Incluso si posee un determinado número de textos cifrados junto con los textos nativos que produce cada texto.
- El emisor y el receptor deben haber obtenido las copias de la clave secreta de una forma segura.
- Una vez que se conoce la clave, todas las comunicaciones que utilicen esta clave pueden ser leídas.

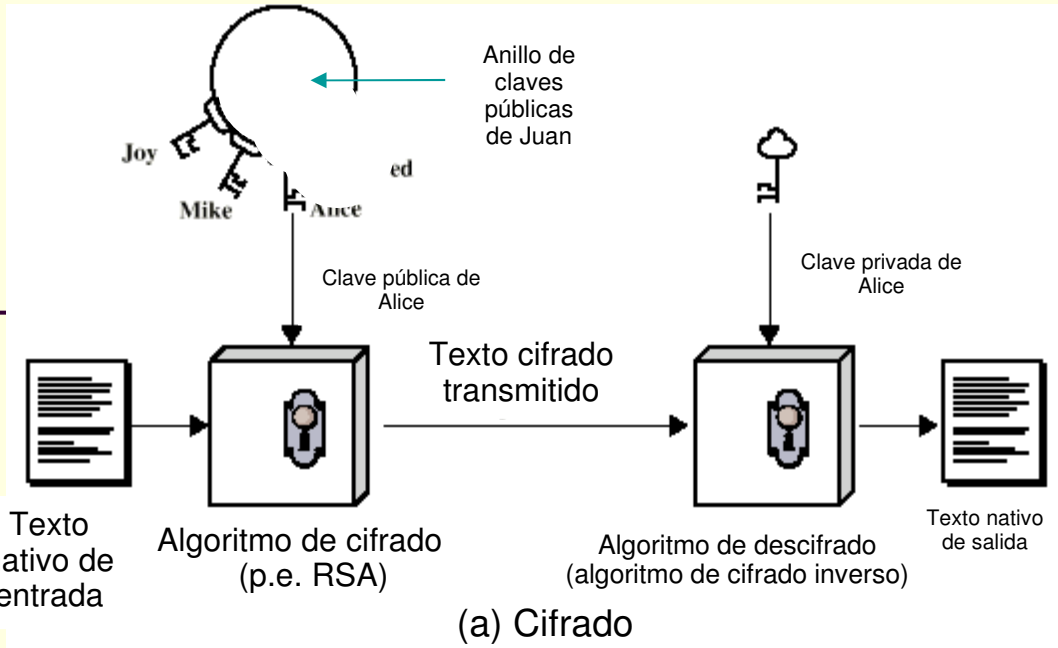
Ataques al cifrado convencional

- Criptoanálisis:
  - Se basa en la naturaleza del algoritmo más algún conocimiento de las características generales del texto nativo.
  - Intento de deducir un texto nativo o la clave.
- Fuerza bruta:
  - Intentar cada clave posible hasta que se obtenga una traducción inteligible del texto nativo.

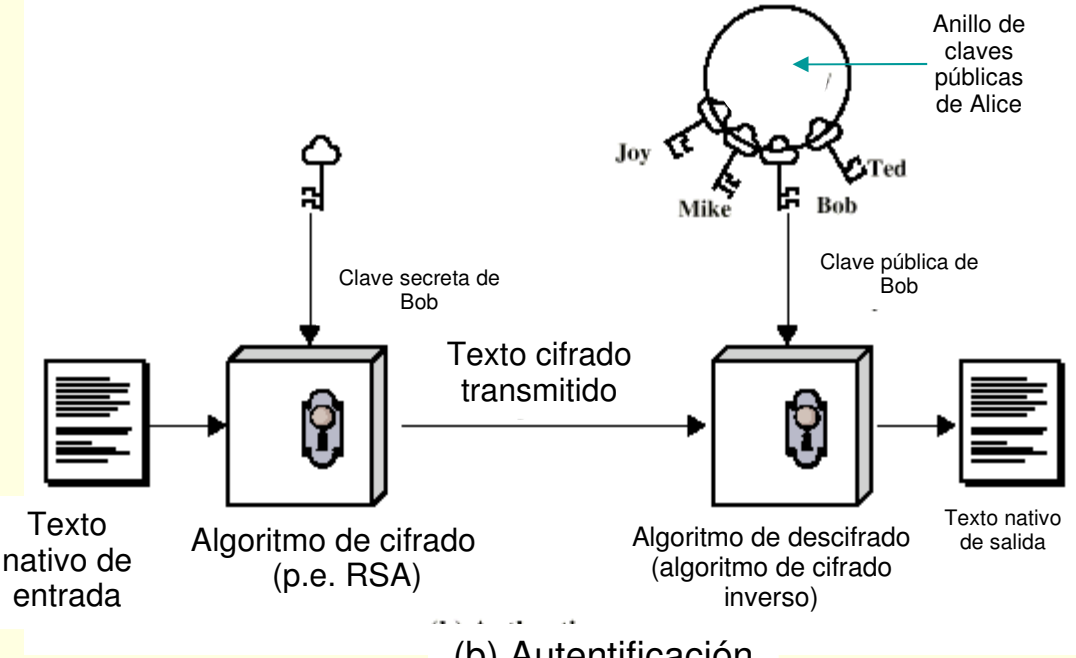
Cifrado de clave pública

- Se basa en funciones matemáticas.
- Asimétrica:
  - Usa dos claves independientes.
- Ingredientes:
  - Texto nativo.
  - Algoritmo de cifrado.
  - Clave pública y privada.
  - Texto cifrado.
  - Algoritmo de descifrado.

Cifrado Clave Pública



(a) Cifrado



(b) Autentificación

Técnica de Cifrado de Clave Pública

- Una clave se hace pública:
  - Se usa para el cifrado.
- Otra clave se mantiene privada:
  - Se usa para el descifrado.
- No es factible determinar la clave de descifrado dadas la clave de cifrado y el algoritmo.
- Cualquiera de las claves se puede usar para cifrar, la otra para descifrar.

Pasos

- Cada usuario genera un par de claves.
- Cada usuario publica una de las dos claves.
- Para enviar un mensaje al usuario, se cifra el mensaje utilizando la clave pública.
- El usuario descifra el mensaje utilizando su clave privada.

Protocolos Estándares

- SSL (*Secure Socket Layer*)
  - Establece un canal seguro de intercambio de información
- SET (*Secure Electronic Transaction*)
  - Además impide la manipulación de la información en los extremos
  - No muy usado en la actualidad (obsoleto)
- EMV (sustituye a SET)
- PGP (*Pretty Good Privac)*
  - Correo electrónico)
- IPsec

SSL *Secure Socket Layer*

- Proporciona:
- Cifrado de datos
- Autenticación de servidores
- Integridad de mensajes
- Autenticación de clientes
- EJEMPLO:
  - Correo electrónico para los alumnos en https://webmerlin.uca.es

SSL pasos para crear un canal seguro

- 1 Elección de algoritmo
  - DES, RC2,RC4..
- 2 Autenticación
  - intercambio certificado x.509v3
- 3 Generación de clave de sesión
- 4 Verificación de canal seguro

SSL

- Si el sitio es seguro:
  - Aparece un candado cerrado
  - El protocolo es *https*
  - Pinchando sobre el candado aparece información sobre el sitio y su certificado

Infraestructuras de Clave Pública (ICPs o PKIs, Public Key Infrastructures).

- El modelo basado en Terceras Partes Confiables
- Es un conjunto de protocolos, servicios y estándares que soportan aplicaciones basadas en criptografía de clave pública.
- Algunos de los servicios
  - Registro de claves: emisión de un nuevo certificado para una clave pública.
  - Revocación de certificados: cancelación de un certificado.
  - Selección de claves: publicación de la clave pública
  - Evaluación de la confianza: determinación sobre si un certificado es válido
  - Recuperación de claves: posibilitación de recuperar las claves de un usuario.
- Las ICPs están compuestas por distintas terceras partes en los que todos los demás usuarios de la infraestructura confían:·
  - Autoridad de Certificación·
  - Autoridad de Registro·
  - Otras Terceras Partes Confiables como por ejemplo las Autoridades de Fechado Digital.

¿Qué es un certificado?

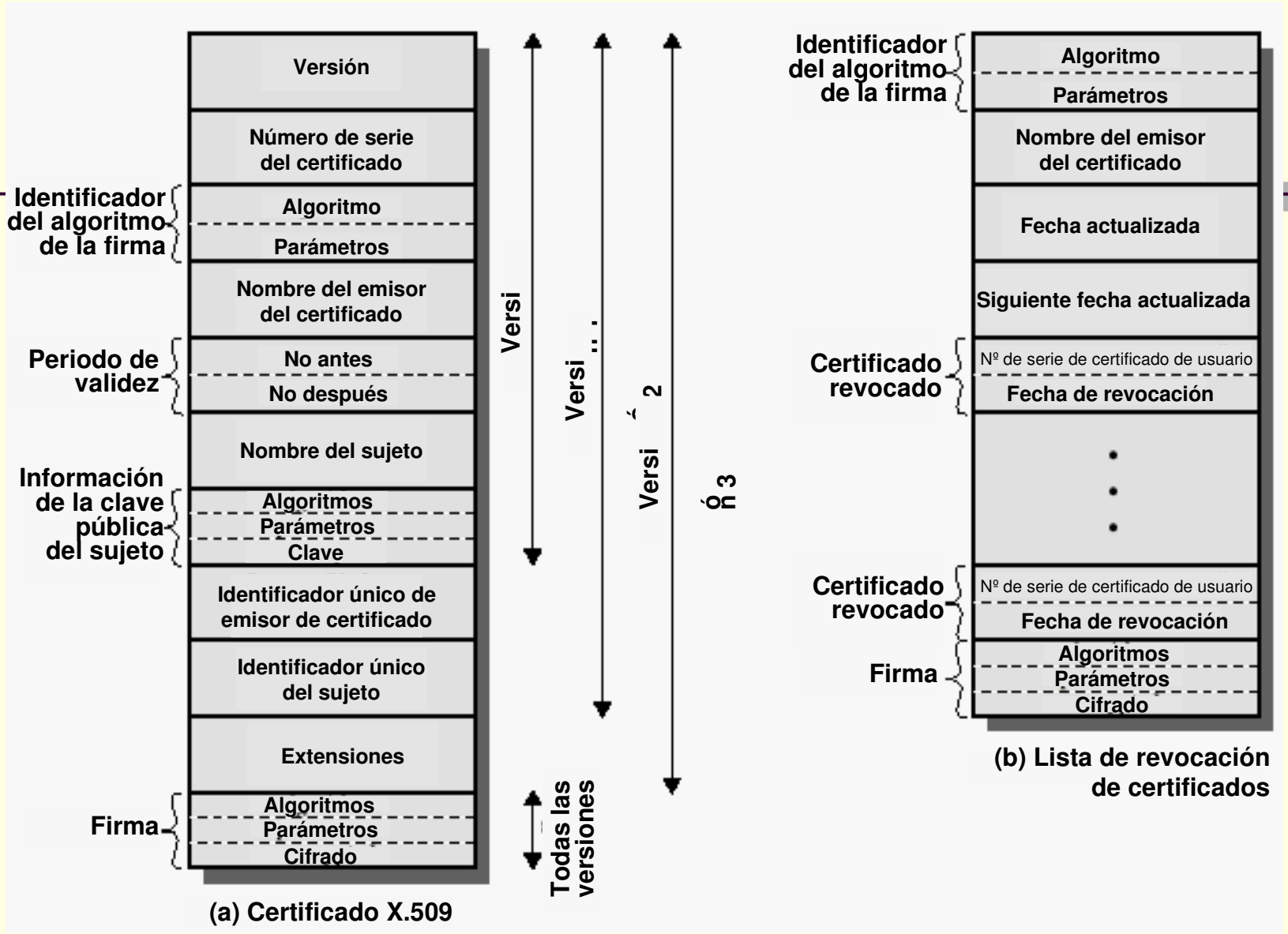
- Un certificado en un documento emitido y firmado por la Autoridad de Certificación que identifica una clave pública con su propietario.
- Cada certificado está identificado por un número de serie único y tiene un periodo de validez que está incluido en el certificado.

¿Qué es un certificado raíz?

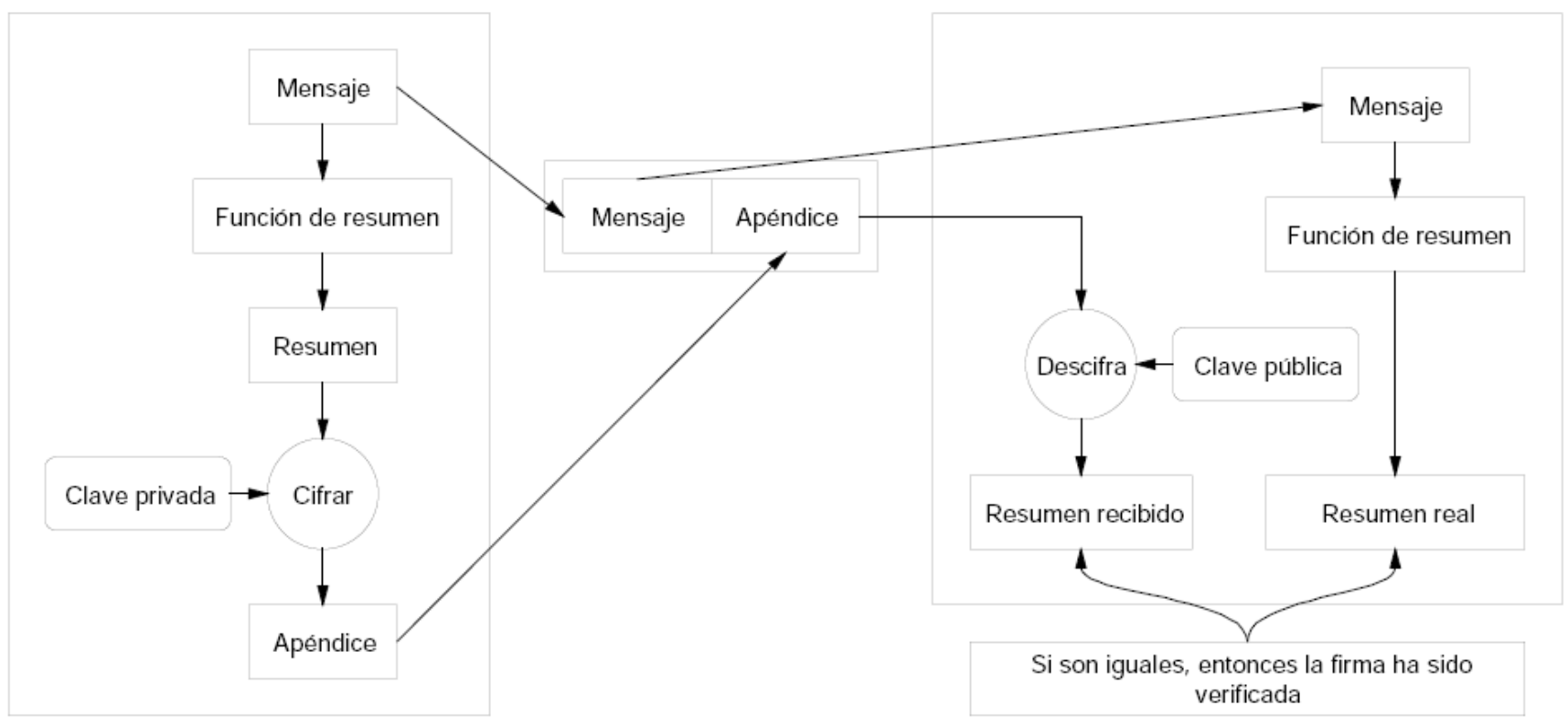
- Un certificado raíz es un certificado emitido por la Autoridad de Certificación para sí misma.
- En este certificado consta la clave pública de la Autoridad de Certificación y por tanto será necesario para comprobar la autenticidad de cualquier certificado emitido por ella.
- Es el certificado origen de la cadena de confianza.

¿Qué información contiene un certificado ?

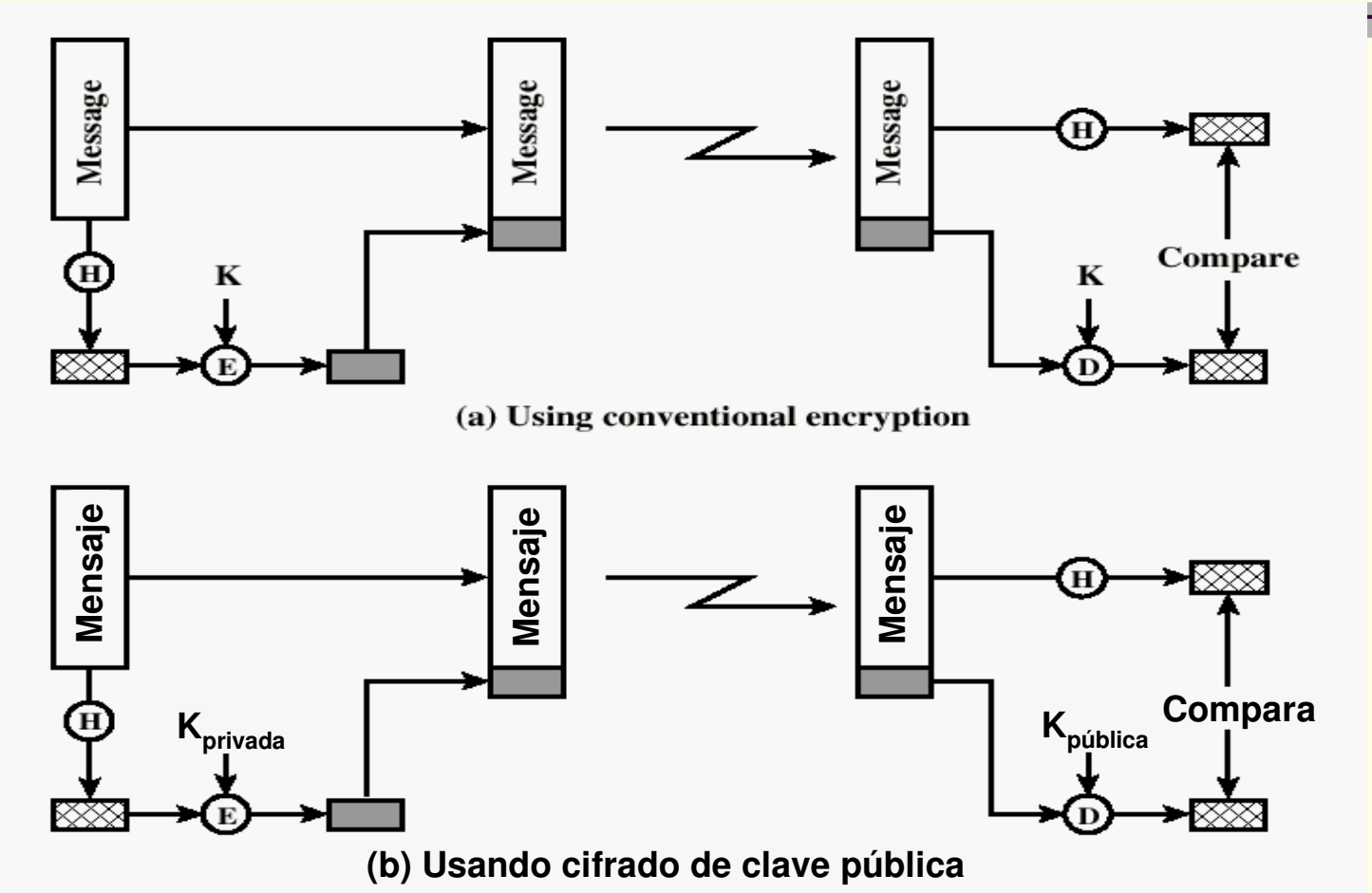
- **Nombre habitual del propietario de la clave de firma**
- **Identificador único del propietario**
- **Clave pública correspondiente a la clave privada de firma**
- **Identificación de los algoritmos de clave pública**
- **Número del certificado**
- **Nombre de la Entidad Certificadora**
- **Limitaciones de aplicación de las claves**
- **Capacidad de representación por terceras partes**
- **Fecha y hora de emisión y aceptación del certificado**
- **Fecha y hora de expiración del certificado**
- **Firma de la Autoridad Pública de Certificación como emisora del certificado**
- **Versión de la DPC bajo la cual se haya emitido el certificado**


Versión
Número de serie del certificado
Identificador del algoritmo de la firma
Algoritmo
Parámetros
Nombre del emisor del certificado
Periodo de validez
No antes
No después
Nombre del sujeto
Información de la clave pública del sujeto
Algoritmos
Parámetros
Clave
Identificador único de emisor de certificado
Identificador único del sujeto
Extensiones
Firma
Algoritmos
Parámetros
Cifrado
Versi
Versi
Versi
ó n 3
Todas las versiones
(a) Certificado X.509
Identificador del algoritmo de la firma
Algoritmo
Parámetros
Nombre del emisor del certificado
Fecha actualizada
Siguiente fecha actualizada
Certificado revocado
Nº de serie de certificado de usuario
Fecha de revocación
Certificado revocado
Nº de serie de certificado de usuario
Fecha de revocación
Firma
Algoritmos
Parámetros
Cifrado
(b) Lista de revocación de certificados

firma digital



Enfoque típico de firma digital

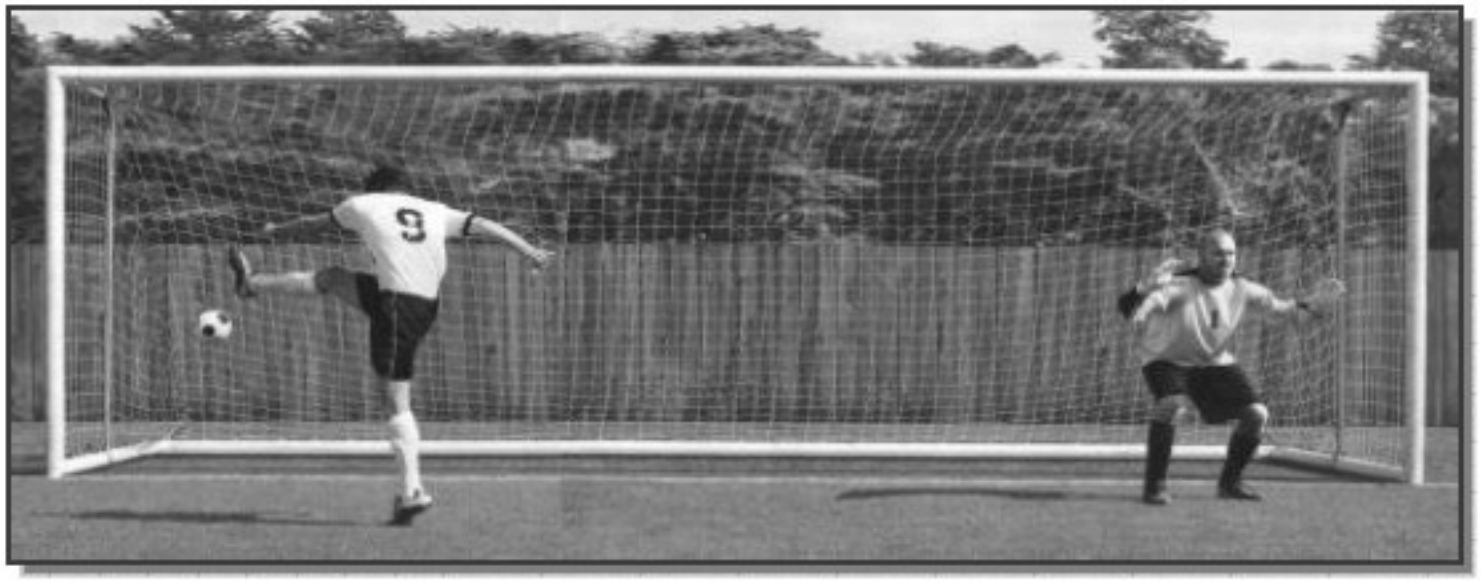


Medidas de seguridad

- Cortafuegos
- Antivirus
- Actualizaciones de software
- Listas de control de acceso
- Cifrado de los archivos del disco
- Copias de respaldo
- Anonimato
- Control de contenidos
- http://alerta-antivirus.red.es/

What does Perimeter mean?

Take care of your perimeter !!!

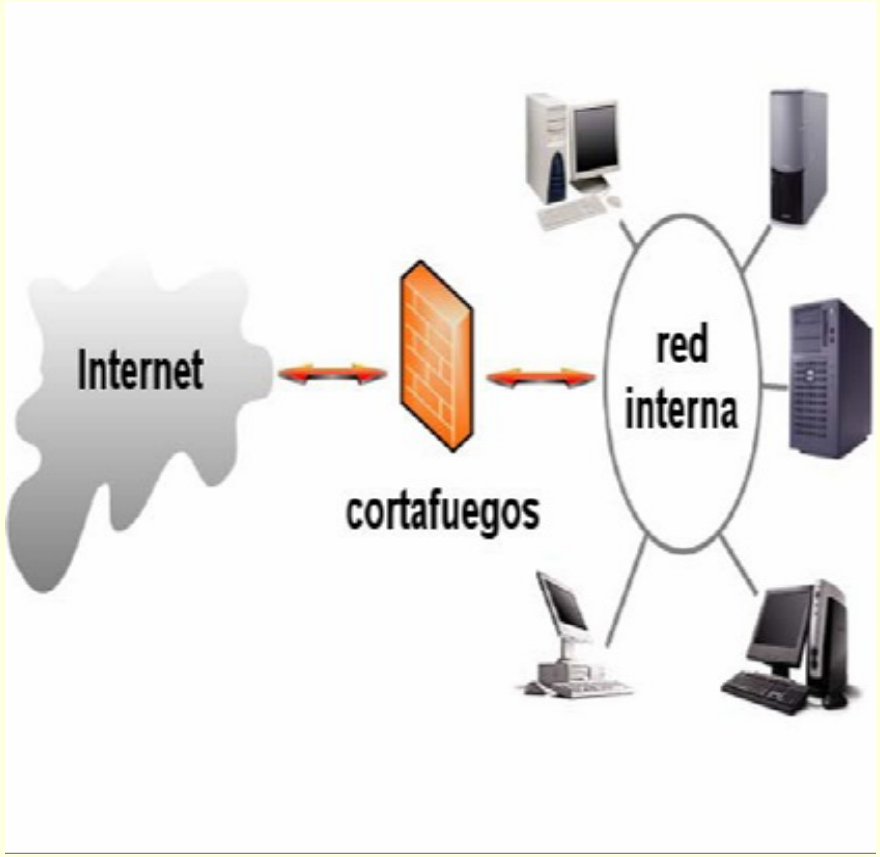


carlos@jessland.net

More information at: http://www.jessland.net

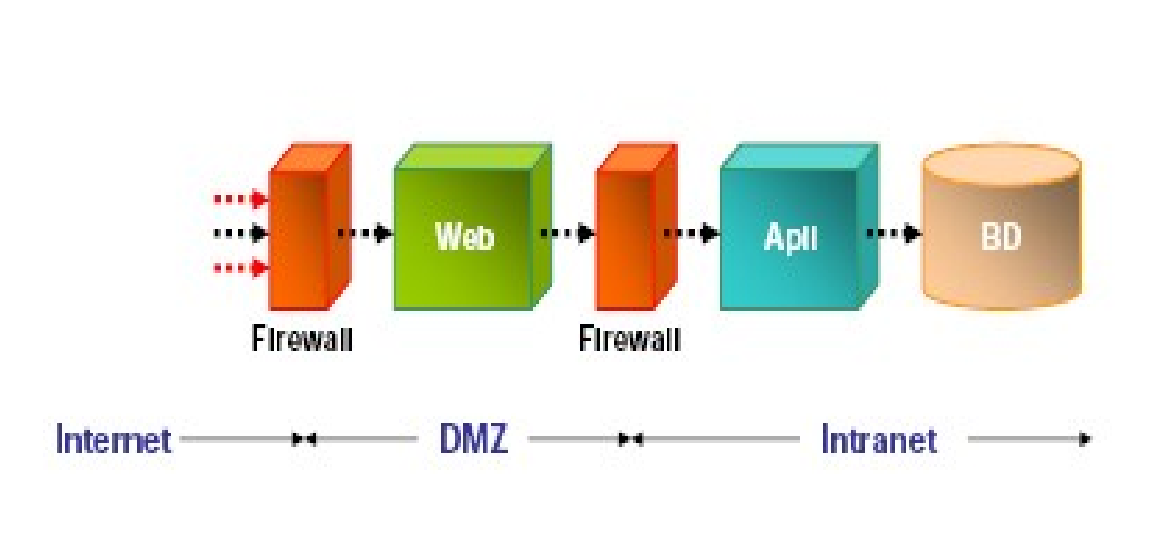
Cortafuegos

- Aislamiento de Internet
  - Bloquea la entrada y salida
- Detección de intrusos
  - Detecta aplicaciones que intentan acceder a Internet
- Auditoría y registro de uso
  - Registra conexiones y ayuda a detectar intrusiones



Cortafuegos

- ZoneAlarm:
  - http://download.zonelabs.com/bin/free/es/down
- Outpost: www.outpost-es.com
- Comodo: www.personalfirewall.comodo.com



Antivirus

- AVG Free Edition:
  - www.grisoft.com/doc/productsavg-anti-virus-fre
  - http://free.grisoft.com/doc/1
- BitDefender Free Edition v7:
  - www.bitdefender-es.com/PRODUCT-14-es--Bit
- AntiVir Personal Edition:
  - www.free-av.com
- Free avast! 4 Home Edition:

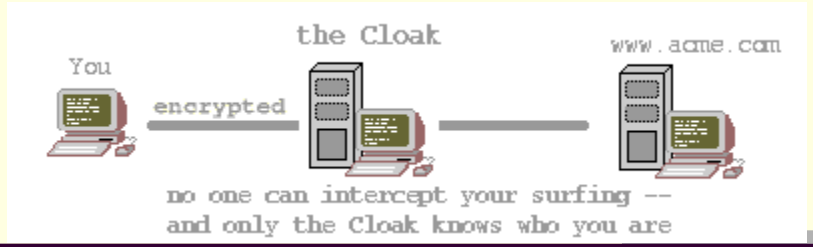
Antispyware

- Windows Defender:
  - www.microsoft.com/spain/athome/security/spyw
- AdAware:
  - http://www.lavasoft.com/products/ad-aware_se
- Spybot Search & Destroy (S&D):
  - http://www.spybot.info/es/index.html
  - www.safernetworking.org/es/home/index.html

Cifrado de los archivos del disco

- Permite cifrar el contenido de cualquier carpeta o archivo
- Solución altamente segura, integrada con el sistema de archivos, totalmente transparente para el usuario y con la capacidad de recuperar datos cifrados
- Se basa en el uso de criptografía de clave pública y de algoritmos de cifrado simétrico

Anonimato



- CGI o anonimizadores
  - @nonymouse: anonymouse.ws
  - Megaproxy: www.megaproxy.com
  - The Cloak: www.the-cloak.com
- Proxies HTTP
  - HiProxy: www.hiproxy.com
  - Multiproxy: www.multiproxy.org
  - Privoxy: www.privoxy.org
- SOCKS
  - SocksCap: www.socks.permeo.com

Control de contenidos

- Controlar por dónde navegan los suyos
  - Filtro de contenidos del navegador
  - Programas especializados:
    - Cyber Patrol: www.cyberpatrol.com
    - Cybersitter: www.cybersitter.com
    - Net Nanny: www.netnanny.com
    - SurfControl: www.surfcontrol.com

Información Microsoft

- Información o Seguridad en el hogar:
  - http://www.microsoft.com/spain/seguridad/defa
- Windows Defender
  - www.microsoft.com/spain/athome/security/defa
  - http://www.microsoft.com/spain/technet/seguric

Scanner en línea

- http://www.dslreports.com/scan

Recomendaciones usuarios finales

- Por Bruce Schneier (schneier@counterpane.com)
- Traducido por José Manuel Gómez (jmg@kriptopolis.com)

Recomendaciones

- Contraseñas
- Antivirus, cortafuegos (malware)
- Correo electrónico
- Navegación en Internet
- Aplicaciones
- Copias de seguridad
- Seguridad en portátiles
- Cifrado

1. Contraseñas

- Las contraseñas suficientemente buenas no son fáciles de memorizar
- Cree contraseñas largas y aleatorias, y anótelas.
  - Guárdelas en su cartera, o en un programa como Password Safe.
  - Guárdelas como haría con su dinero.
- No deje que los navegadores web almacenen sus contraseñas por usted.
- No transmita contraseñas (o PINs) mediante formularios web o correos sin cifrar.
- Asuma que todos los PINs pueden romperse fácilmente, y actúe en consecuencia.

2.Antivirus

- Utilícelo.
- Descargue e instale las actualizaciones cada dos semanas, y en cualquier momento en que lea algo sobre un nuevo virus en los medios de comunicación.
- 3.Cortafuegos personales.
  - Utilícelos. Habitualmente no existe ninguna razón para permitir conexiones entrantes de nadie.

4.- Correo electrónico (I)

- Borre el spam (correo basura) sin leerlo.
- No abra, y borre inmediatamente, mensajes con ficheros adjuntos, a menos que sepa lo que contiene.
- No abra, y borre inmediatamente, viñetas, vídeos y ficheros del tipo "bueno para echar unas risas" enviados por bienintencionados amigos.
- Desactive el correo HTML. No utilice Outlook ó Outlook Express.
- Si debe utilizar Microsoft Office, active la protección frente a virus de macro;

4.- Correo electrónico (II)

- en Office 2000 cambie el nivel de seguridad a "Alto" y no confíe en ninguna fuente a menos que tenga que hacerlo.
- Si está utilizando Windows, desactive la opción "Ocultar extensiones de fichero para tipos de fichero conocidos"; esa opción permite que los troyanos se hagan pasar por otros tipos de ficheros.
- Desinstale "Windows Scripting Host" si puede pasar sin ello. Si no puede, al menos cambie sus asociaciones de ficheros, para que los ficheros de script no sean enviados automáticamente al Scripting Host si se hace doble click sobre ellos.

5.Sitios web.

- SSL no proporciona ninguna seguridad sobre si el comerciante es fiable o si su base de datos de información de clientes es segura.
- Piensélselo antes de hacer negocios con un sitio web.
- Limite los datos personales y financieros que envíe a los sitios web; no proporcione ninguna información a no ser que lo considere imprescindible.
- Si no quiere dar información personal, mienta.
- No acepte recibir anuncios de marketing.
- Si el sitio web le da la opción de no almacenar su información para usos posteriores, márquela.

6.Navegación

- Limite el uso de cookies y applets a esos pocos sitios que le dan servicios que necesita.
- Limpie con regularidad sus carpetas de cookies y ficheros temporales
- Si eso no es posible, no utilice Microsoft Internet Explorer.

7.Aplicaciones

- Limite los programas en su máquina.
- Si no lo necesita, no lo instale.
- Si no va a necesitarlo más, desinstálelo.
- Si lo necesita, compruebe con regularidad si hay actualizaciones e instálelas.

8. Copias de Seguridad

- Hágalas regularmente.
- Haga copias al disco, cinta o CD-ROM
- Guarde por lo menos un juego de copias fuera de su ordenador (una caja de seguridad es un buen lugar) y al menos un juego en el ordenador.
- Recuerde destruir las copias antiguas; destruya físicamente los discos CD-R.

9. Seguridad en portátiles

- Mantenga su portátil con usted siempre que no esté en casa; piense en él como si fuera su cartera o su bolso.
- Elimine regularmente los ficheros de datos que ya no necesite.
- Lo mismo puede aplicarse a los dispositivos Palm; la gente tiende a dejar en ellos incluso más datos personales, incluyendo contraseñas y PINs, que en los portátiles.

10. Cifrado

- Instale un cifrador de correo y ficheros (como PGP).
- Cifrar todo su correo no es realista, pero algún correo es demasiado sensible para enviarlo sin cifrar.
- De igual forma, algunos ficheros de su disco duro son demasiado sensibles para dejarlos sin cifrar.

11. General

- Apague su ordenador cuando no lo utilice, sobre todo si tiene una conexión permanente a Internet.
- Si es posible, no utilice Microsoft Windows.
- Sinceramente, todo esto resulta difícil. Ni siquiera puedo decir que yo siga escrupulosamente mis propios consejos. Pero sigo la mayoría, y probablemente eso ya resulta suficiente. Y "probablemente suficiente" es casi lo mejor que se puede obtener hoy en día.

Seguridad en red

- 1.- No comparta recursos si no es necesario
- 2.- Si necesita compartirlo hágalo con una buena contraseña
- 3.- Siempre que sea posible compártalo como “solo lectura”
- 4.- NUNCA comparta su disco duro con privilegio de escritura ni siquiera con contraseña.

Sitios con medidas y consejos de seguridad

- http://alerta-antivirus.red.es/portada
- http://www.seguridadenlared.org/es/index.php
- http://www.internautas.org/html/
- http://www.seguridadpymes.es/

Herramientas de seguridad

- 75 herramientas de seguridad
  - http://www.insecure.org/tools.html
  - http://www.linuxdata.com.ar/index.php?idmanual=75segurida
- http://www.ush.it/free-services/security-tools/
- http://www.ausejo.net/seguridad/intrusiones.htm
- http://www.itsafe.gov.uk/index.html
- curso del antiespia de microsoft
  - http://www.seguridad.unam.mx/doc/?ap=tutorial&id=13

Direcciones

- Recomendaciones de seguridad
  - http://www.rediris.es/cert/doc/docu_rediris/recon
    - recomendaciones.pdf
    - rainbow-series
- Definición de una política de seguridad:
  - http://www.rediris.es/cert/doc/docu_rediris/poliseg.es.html#o14

Conclusiones

- Amplio abanico de herramientas de seguridad gratuitas
- Un pequeño esfuerzo eleva drásticamente el nivel de seguridad
- La concienciación es fundamental

Kit de supervivencia

- 1. Cortafuegos
- 2. Antivirus
- 3. Actualizaciones
- 4. Concienciación
- 5. antiespias
- 6. limpiadores de registro

Seguridad lógica

- Se consigue adoptando una serie de medidas técnicas y administrativas
- Afectan a la configuración de los sistemas operativos
- La implementación dependerá de cada sistema operativo:
  - UNIX
  - Windows
- Ver documento de recomendaciones de seguridad para encontrar medidas concretas
  - http://www.rediris.es/cert/doc/
  - Redes inalámbricas
    - http://www.rediris.es/cert/doc/reuniones/fs2006/archivo.es.h

Seguridad lógica

- ASPECTOS:
  - De Sistemas
    - Autentificación
      - Políticas de contraseñas
      - Políticas de cuentas
    - Control de acceso
    - Seguridad en los sistemas de ficheros
    - Configuración de equipos y servidores
    - Configuración de servicios (www, FTP, correo, DNS, Servidores de ficheros)
    - Monitorización
    - Actualizaciones de software
  - De red
    - Intranets
    - Internet
  - Recomendaciones para usuarios finales
  - De diseño del software

Seguridad del sistema de ficheros

- La pérdida de la información contenida en un sistema de ficheros puede ser irreparable y de costo infinito.
  - Un ordenador que se quema puede ser sustituido con la compra de otro. La información que contenía no.
- El control de acceso en un sistema de ficheros permite que el usuario determine quién y cómo puede acceder a sus ficheros.
- Un sistema orientado a la protección ofrece medios para distinguir entre uso autorizado y no autorizado.

Copias de seguridad

Disponibilidad del sistema de ficheros

- Un sistema de ficheros puede ser dañado por problemas de hardware:
  - Errores de lectura
  - Cortes o sobrecarga de corriente.
  - Choque de las cabezas
  - Polvo
  - Temperatura
  - Vandalismo

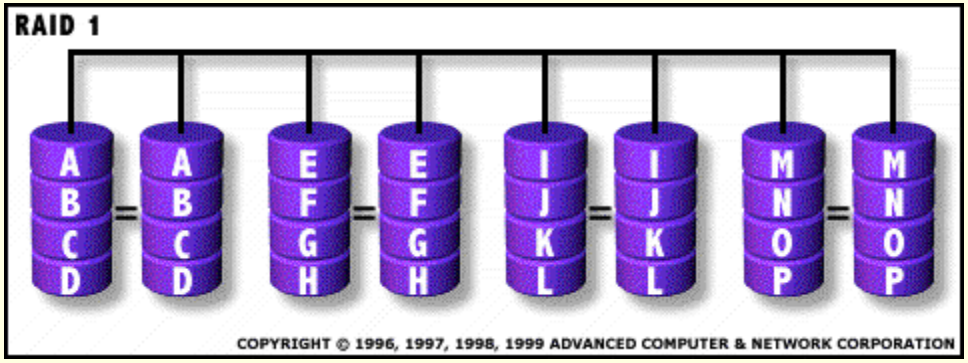
Sistemas de copias (respaldo)

- Medios para pequeños sistemas
  - ZIP, grabadoras y regrabadoras de CD,DVD, Discos mageto-ópticos, sistemas de cintas DAT
  - Disco duro externo (NAS)
- Grandes sistemas
  - Librerías robotizadas de cintas
  - SAN (*Storage Area Networks*)
- Online:
  - www.xdrive.com
  - www.idrive.com

Sistemas RAID

(redundant array of independent [inexpensive] disks)

- El RAID mejora el rendimiento y la disponibilidad
- Hay muchos tipos de RAID (0-7, 10, 53)
- Se basan en las bandas (striping), redundancia (Discos espejos) y control de errores (CCR)



Copias de seguridad

- Tipos de copias
  - Normales
  - Incrementales
  - Diferenciales (no marca como copiado)
- Sistemas de bases de datos
  - Registro de transacciones.
  - Ficheros de versión múltiple
- Gestión de soportes
- Sistemas de copia padre, hijo, nieto

Sistemas tolerantes a fallos

- Sigue funcionando aunque falle alguno de sus componentes.
- El aspecto fundamental es la redundancia
- Se emplean en instalaciones críticas
  - Líneas aéreas.
  - Bancos.
  - Central nuclear.
- Degradación paulatina.
- Sustituir y reparar en caliente

Escaneado y firma digital de los soportes

Recepción

- Recepción de soportes.
- Comprobación de integridad.
- Tratamiento del papel.

Escaneado

- Color, 200 dpi.
- TIFF multipágina.
- 50 ppm.

Generación metadatos

- Formato XML.
- Código de proceso interno.
- Datos del propio interesado.

Gestión documental

- Integración en el sistema de información.
- Análisis estadístico.

Firma digital

- Certificado digital.
- Generación fichero de firma.
- Proceso automático.

Destrucción

- Garantía de confidencialidad.

NAT estático

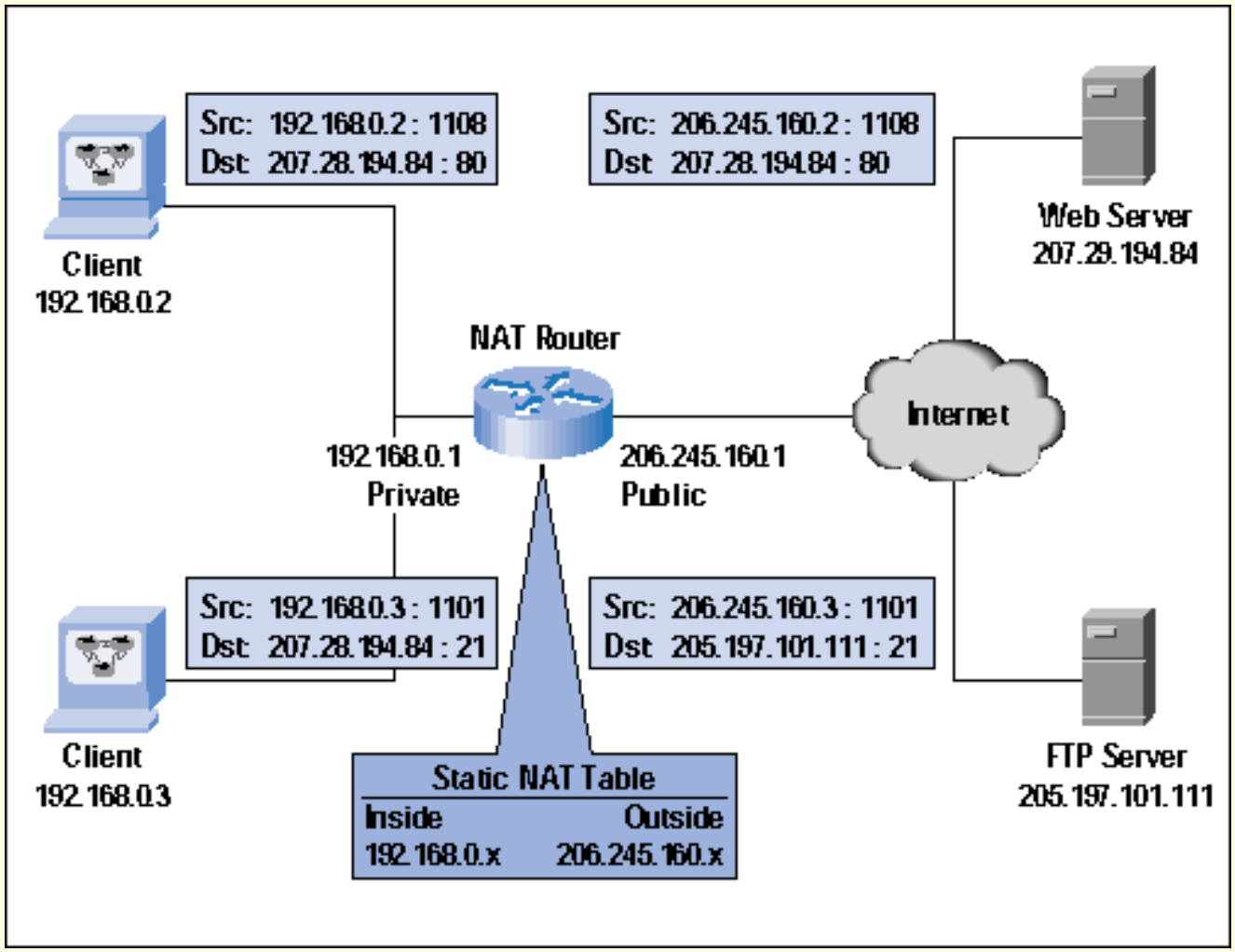
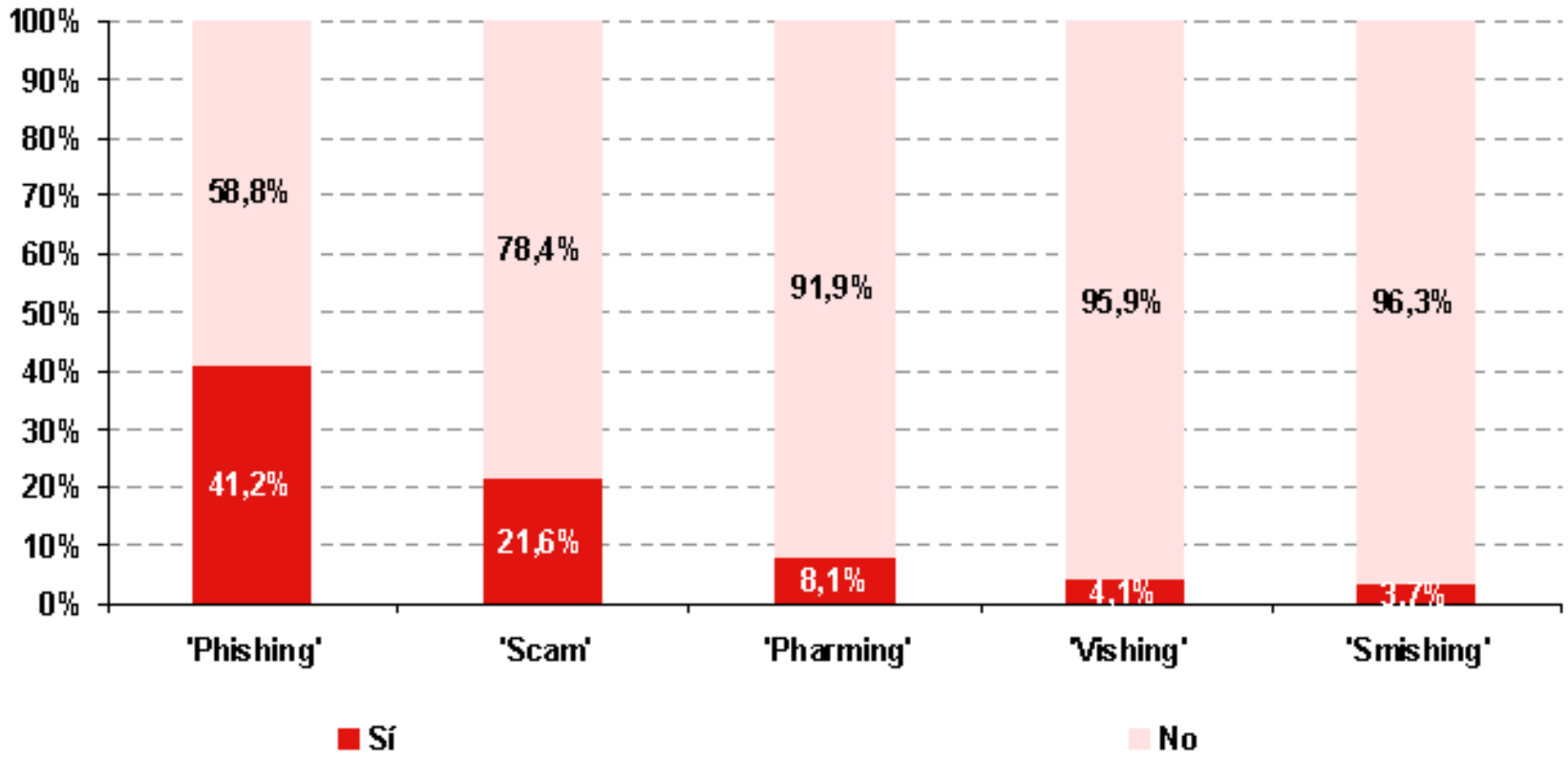


Gráfico 1: Nivel de conocimiento declarado sobre términos relacionados con el fraude online. (%)



Phishing: *Acto de adquirir fraudulentamente información sensible de carácter personal de forma online.*
Scam: *Oferta de trabajo online de carácter fraudulento.*
Pharming: *Evolución tecnológica del phishing que se concreta en el envenenamiento del sistema DNS (Domain Name Service).*

Smishing: *Tipo de phishing telefónico que utiliza los mensajes sms de los teléfonos móviles.*
Vishing: *Tipo de phishing telefónico que utiliza voces grabadas para solicitar los dígitos y la fecha de caducidad de las tarjetas de crédito, produciéndose a continuación las operaciones fraudulentas.*

Fuente: INTECO

- http://www.confianzaonline.org/
- http://sans.org/

Enlaces

- http://www.confianzaonline.org/
- http://sans.org/
- Guía de seguridad de Microsoft
  - http://www.microsoft.com/security/protect
- Página de seguridad de Microsoft
  - http://www.microsoft.com/security/
- Internet Storm Center
  - http://www.dshield.org/clients/windows_xp_firev
  - http://www.dshield.org/howto.php
- Sala de lectura de SANS
  - http://www.sans.org/rr

Enlaces

- Formación de SANS Institute: Protección de Windows
  - http://www.sans.org/conference/bytrack.php#t5
  - http://isc.sans.org
- Guías de seguridad de la NSA
  - http://nsa.gov/snac/index.html
- Center for Internet Security
  - http://www.cisecurity.org
- Hispasec
  - http://www.hispasec.com