Inciación a la seguridad en los Sistemas Informáticos

José Carlos Collado Machuca
Manuel Fernández Barcell
Dpto. de Lenguajes y Sistemas Informáticos

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

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

Consejo Superior de Informática

- Conjunto de medidas encaminadas al mantenimiento de la *confidencialidad,autenticidad, integridad y la disponibilidad* de los bienes informáticos

Definiciones de Seguridad: "*Internet Society*"

- Es un concepto multidimensional
- Cuando pensamos en la seguridad nos referimos a uno o más de los siguientes aspectos:
  - Autentificación
  - Control de acceso
  - Auditoría de actividades
  - Confidencialidad
  - Integridad
  - Disponibilidad
  - No repudiación

Rfc2828

ftp.isi.edu/in-notes/rfc2828.txt

Autentificación:

- ***Dar y reconocer la autenticidad de ciertas informaciones del Dominio y/o la identidad de los actores y/o la autorización por parte de los autorizadores y la verificación***
  - Que los datos, las personas y programas son auténticos
  - Verificar la identidad

Confidencialidad:

- ***Condición que asegura que la información no pueda estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados***
- Acceso sólo entes autorizados

Disponibilidad:

- ***Grado en el que un dato está en el lugar, momento y forma en que es requerido por el usuario autorizado***
- Los bienes informáticos pueden ser utilizado cuándo y cómo lo requieran los usuarios autorizados

Integridad + disponibilidad = confiabilidad

Integridad:

- ***Condición de seguridad que garantiza que la información es modificada, incluyendo su creación y borrado, sólo por personal autorizado***
- Modificación sólo por personal autorizado

Control de acceso

- Protección de los recursos del sistema contra accesos no autorizados
  - El uso de los recursos del sistema están regulados conforme a una política de seguridad
  - Solo es permitido a las entidades autorizadas(usuarios, programas, procesos, otros sistemas..), de acuerdo a la política de seguridad

No repudiación

- No poder negar la intervención en una operación o comunicación

Auditoría de actividades

- Registro cronológico de las actividades del sistema que permitan la reconstrucción y examen de los eventos ocurridos
  - Registro de eventos

ISO/IEC 17799 la información

- 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 y 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

ISO/IEC 17799 SEGURIDAD

- La seguridad de la información se consigue implantando un conjunto adecuado de controles, que pueden ser políticas, prácticas, procedimientos, estructuras organizativas y funciones software.
- Estos controles deberían establecerse para asegurar que se cumplen los objetivos específicos de seguridad de la organización

Niveles de seguridad

- Seguro estaba y se murió
  - No existe la seguridad total
- 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

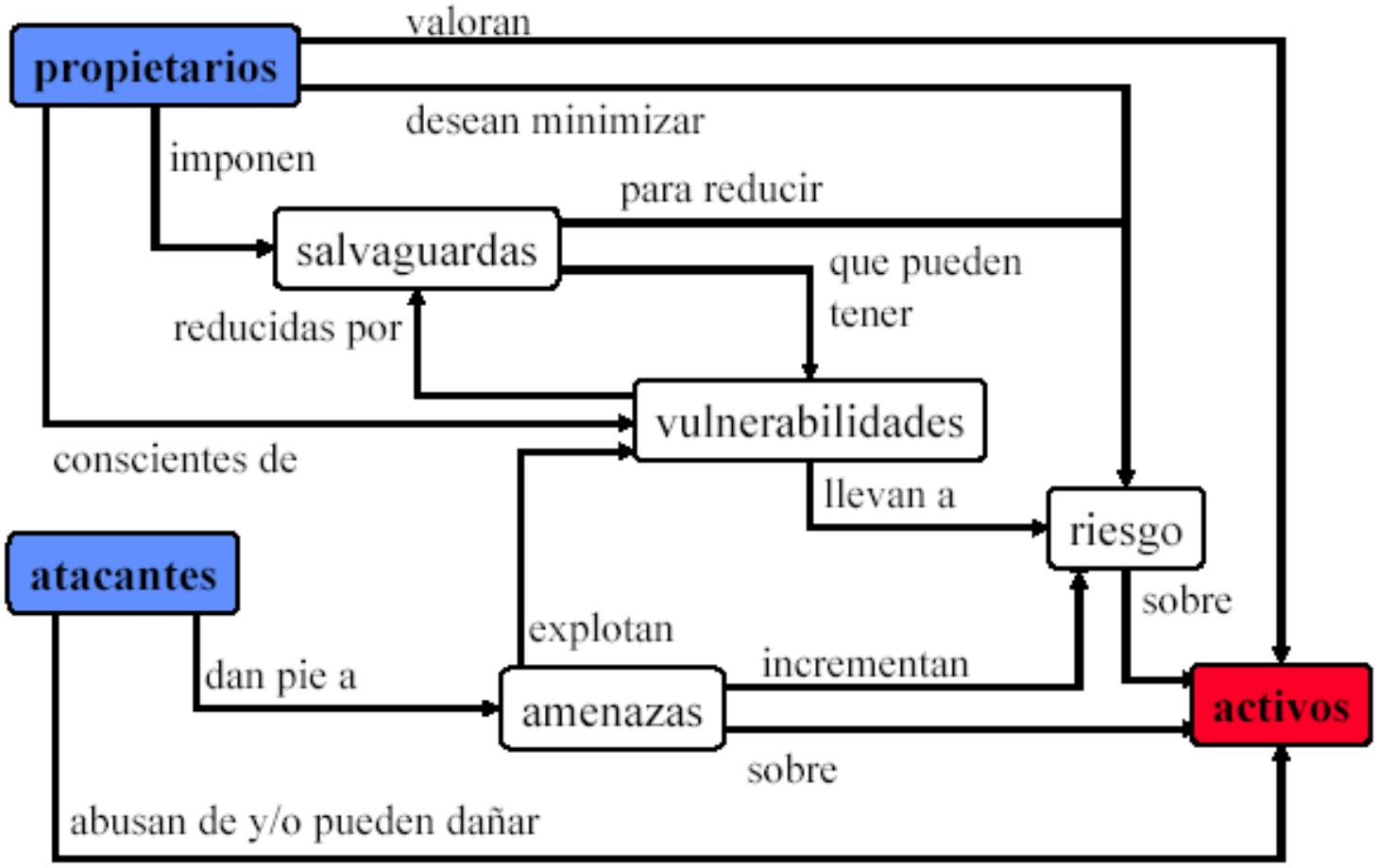
Los planes de seguridad

- Enfrentamiento con la mentalidad mediterránea

Improvisación ⟷ Planificación

- *¿Podría decirme qué camino debo tomar? Preguntó Alicia; esto depende de adonde quieras llegar, contestó el gato*
  - (Alicia en el País de las Maravillas)

ISO: análisis de riesgos

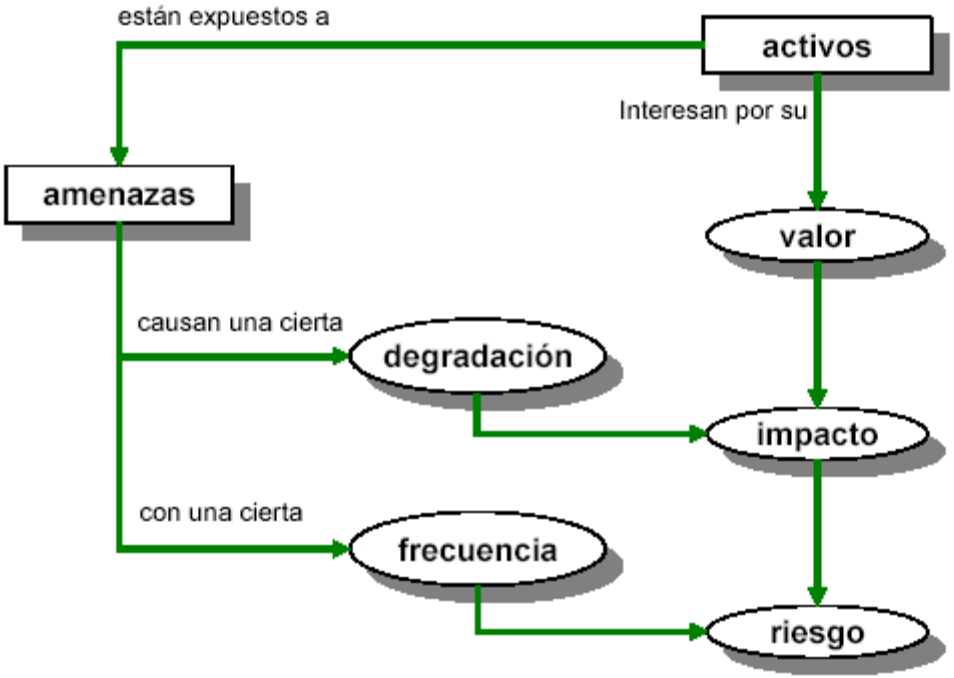


Definiciones

- 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.

Magerit 2: análisis de riesgo

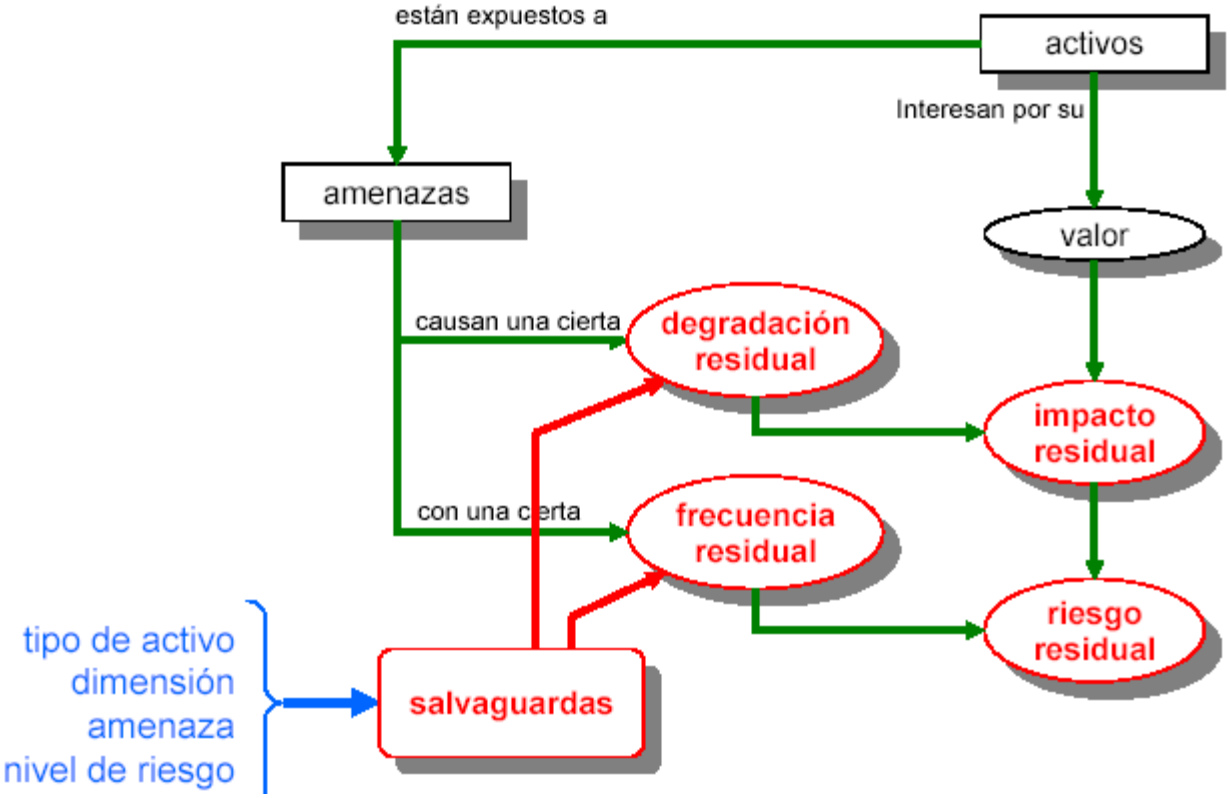
MINISTERIO DE ADMINISTRACIONES PÚBLICAS



MAGERIT – versión 2

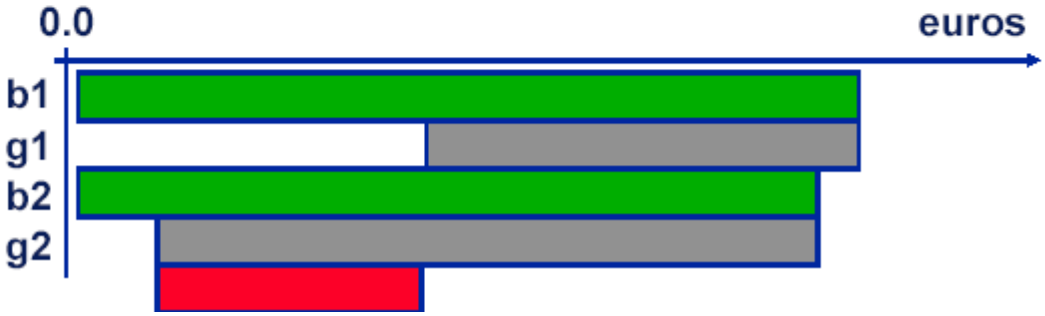
Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información

Magerit: tratamiento



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.

Ataques Pasivos

- Escuchas de las transmisiones.
  - Para obtener información.
- Divulgación del contenido del mensaje:
  - El intruso se entera del contenido de la transmisión.
- Análisis del tráfico:
  - Controlando la frecuencia y la longitud de los mensajes, incluso los cifrados, se puede adivinar la naturaleza de la conexión.

- Difíciles de detectar
- Se pueden prevenir.

Ataques Activos

- Enmascaramiento:
  - Una entidad pretende ser otra entidad diferente.
- Repetición.
- Modificación de mensajes.
- Denegación de un servicio.

•Fácil de detectar
•La detección tiene un efecto disuasivo.
•Difícil de prevenir

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 17799/UNE 71501

Seguridad física: medidas anti intrusos

Medidas anti -Intrusos sobre equipos, ordenadores y redes

Consisten en impedir el acceso físico de personas no autorizadas a las instalaciones y el equipamiento

- Medidas Físicas
  - Puertas de seguridad, cerraduras, vallas
  - Vigilancia.
  - Control de acceso
  - Alarmas, circuitos cerrados de TV

Seguridad física: anti intrusos

Muchas medidas de seguridad tienen comprometida su eficacia si no se impide el acceso físico a los equipos

- Medidas administrativas
  - Control de los visitantes
    - Acompañar al visitante hasta su destino
    - No entregar llaves
  - Restricción de acceso a zonas determinadas
  - Uso de tarjetas identificativas

Seguridad física:
Seguridad Externa Agentes físicos

Medidas dirigidas a proteger los sistemas contra accidentes, agentes ambientales o físicos como el fuego, electricidad, inundación, temperatura, humedad, ambiente sin polvo etc…

- Medidas contra incendios.
- Aire acondicionado.
- Doble suelo
- Instalación eléctrica
  - Estabilizadores
  - SAI´s

Seguridad Externa. Agentes físicos

- Directrices de construcción
  - Construcción de la sala de ordenadores por encima del primer piso
  - No debajo de conducciones de agua
  - Calidad de los materiales de construcción
- Consideraciones eléctricas
  - Suministro del panel principal
  - Independencia entre circuito ordenadores y otros equipos
  - Equipos de aislamiento eléctrico y SAI
  - Circuitos de emergencias

Seguridad física: Agentes externos

- Medidas organizativas
  - Plan de contingencia ante estos fenómenos
  - Ejemplo:
    - ¿Que hacer cuando se va la luz?

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.htr

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.

Sistemas de ficheros

- Windows
  - FAT16
  - FAT32
  - NTFS
- Unix
  - EXT2FS
  - EXTFS
  - FAT16
  - SMB
  - 9660
  - NFS
  - SWAP
  - MINIX
  - XIAF
  - Y MUCHOS MAS

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

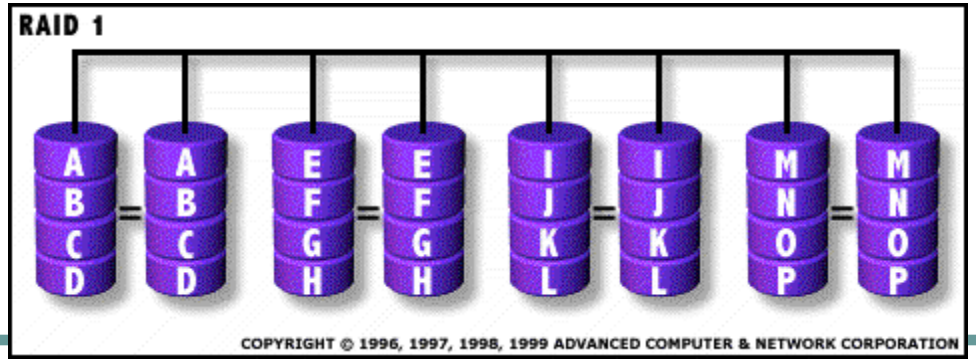
Sistemas de copias

- Medios para pequeños sistemas
  - ZIP, LS-120, grabadoras y regrabadoras de CD,DVD, Discos mageto-ópticos, sistemas de cintas DAT
- Grandes sistemas
  - Librerías robotizadas de cintas
  - SAN (*Storage Area Networks*)

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

ISO 27001

BS 7799 / ISO 27001 Evolution

	Año 1999	Año 2000 – 2002	Año 2005 (Junio)	Año 2006 (Enero)	Año 2007	
BS	BS 7799 – 1	ISO 17799 (2000)	ISO 17799 (2005)		ISO 27002	ISO
	BS 7799 – 2	BS 7799-2:2002	BS 7799-2 (2005)	ISO 27001		

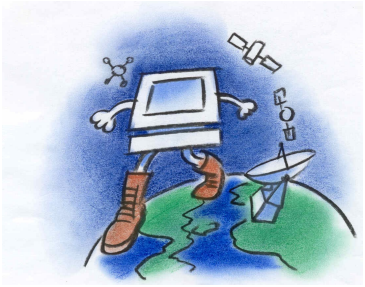
UNE 71502

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

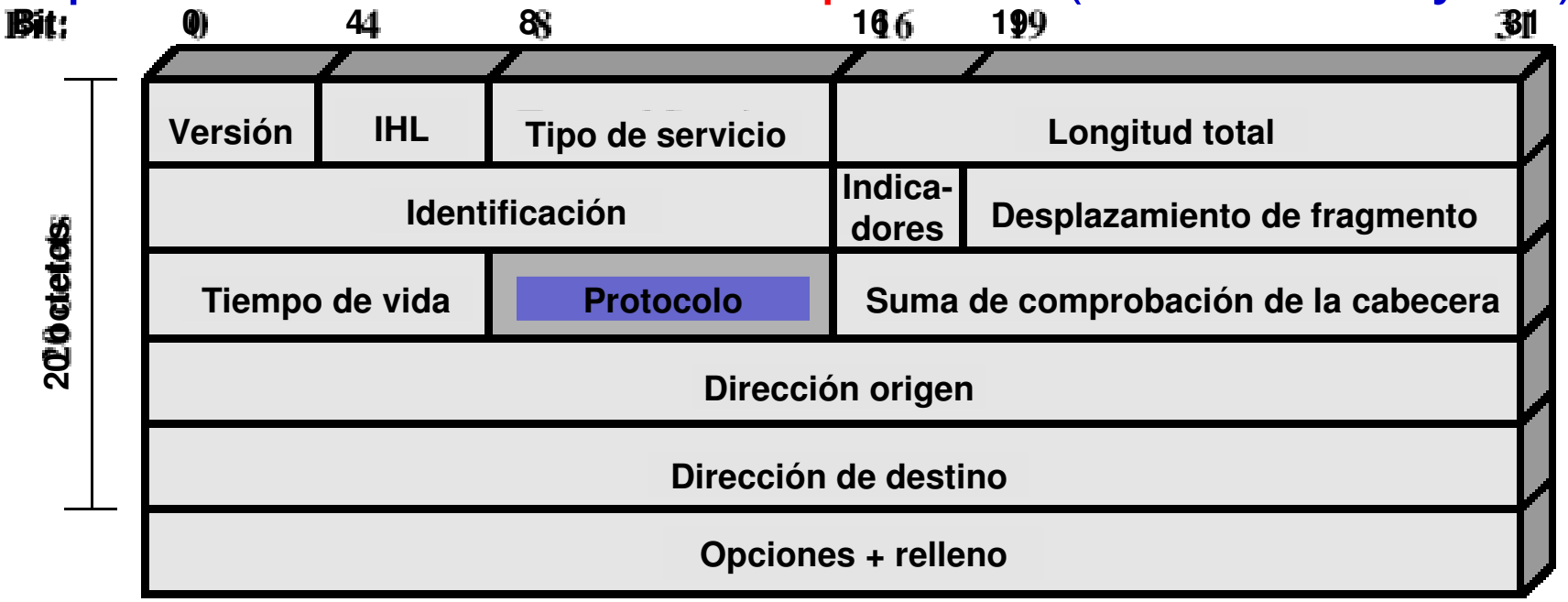


¿Que tienen en común?

- 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).

¿Cómo viaja la información por la red?

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



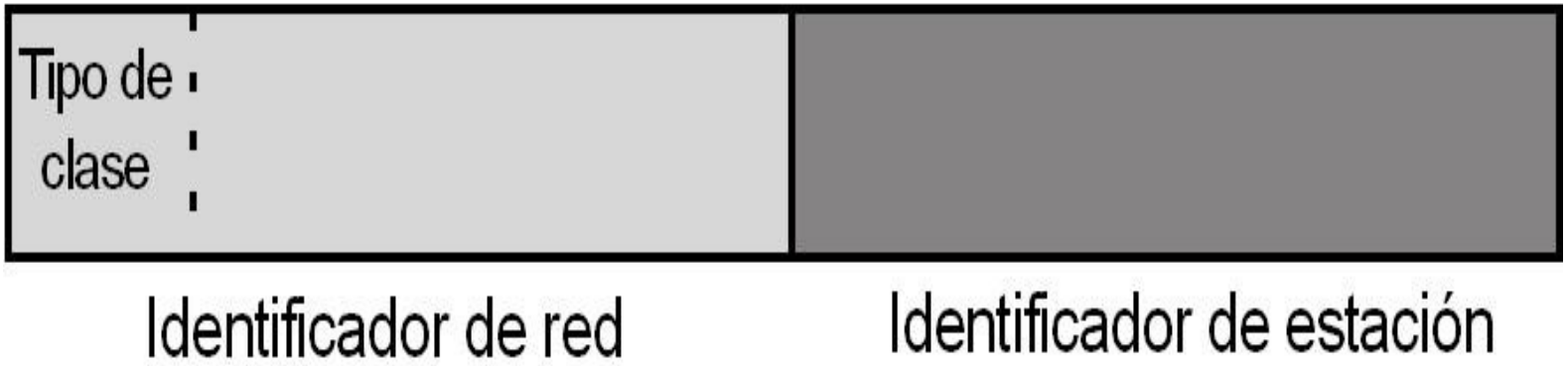
Cabecera IPv4

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

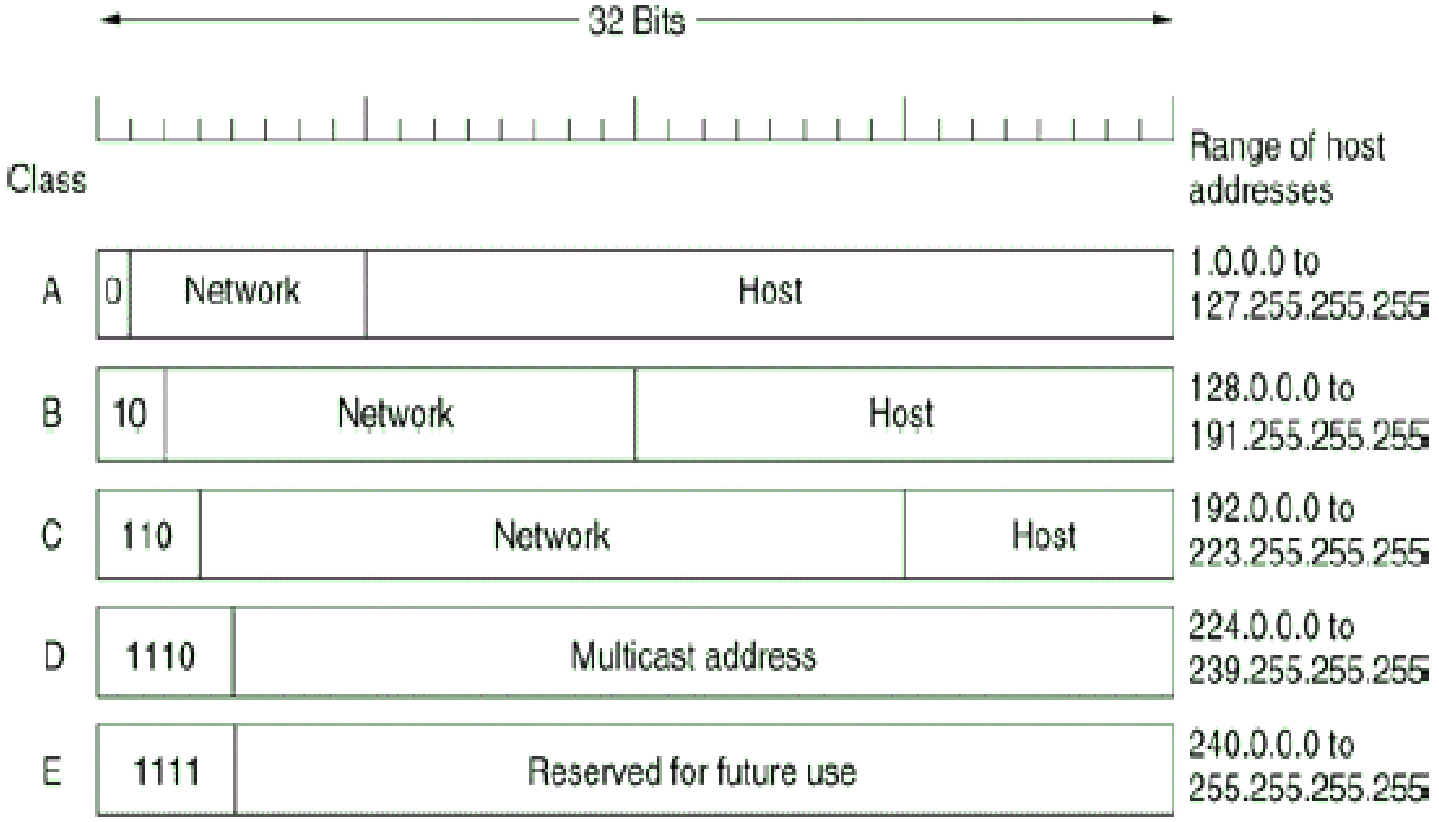
- Mediante direcciones y nombres
  - Dirección IP (identifica redes y equipos de cada red)
  - Nombre de dominio
  - Traducción nombre a dirección IP (DNS)
  - www.uca.es → 150.214.86.11
- Dirección MAC → 00-E0-7D-93-29-AB
- Traducción dirección IP a MAC

Dirección IP

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

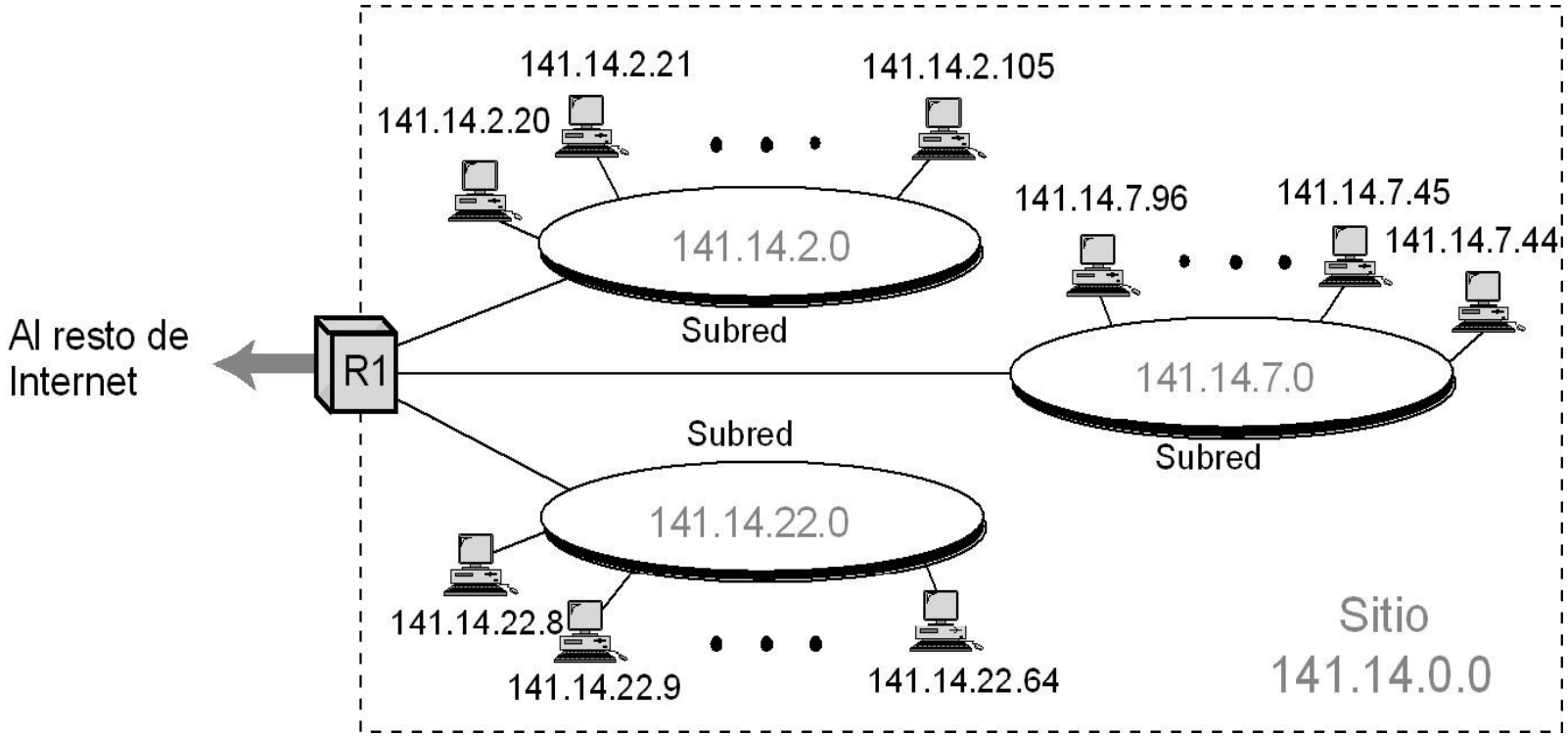


Formatos direcciones IP



Formatos de dirección IP

Una red con tres niveles de jerarquía

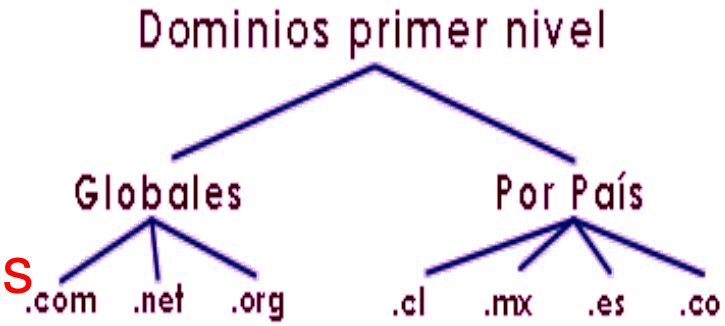


Direcciones privadas

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
    - Tres letras (Las .com)
  - Estilo por paises
    - Dos letras, y por países
      - .es



Genéricos

com	Organizaciones comerciales (DEC, Convex, IBM..).
gov	Organismo gubernamental (NASA...).
edu	Institución educacional (MIT...).
int	Organización internacional.
mil	Organización militar.
net	Organismo de redes.
org	Otras organizaciones.

https://www.interdominio.com/html/index.htr

https://www.nic.es/index.html

http://www.red.es/

Nuevos dominios

TLD	Who can register	Example	
biz	Registrations in the .biz TLD must be used or intended to be used primarily for bona fide business or commercial purposes.	www.companyname.biz	Accredited
info	There are no restrictions on who may register a .info domain name.	www.example.info	
name	Intended for personal use by Individuals.	www.john.smith.name	
pro	Restricted to certified professionals such as lawyers, accountants etc.	www.johnsmith.law.pro	
coop	Restricted to bona-fide cooperatives.	www.orgname.coop	
museum	Restricted to verified museums.	www.natgallery.us.museum	
aero	Restricted to organizations within the air transport industry sector.	www.boeing.aero www.london.uk.aero	

Por países

Dominio	País	Dominio	País	Dominio	País
ar	Argentina	fo	Islas Faroe	jp	Japón
at	Austria	fr	Francia	ki	Kiritabi
au	Australia	uk	Gran Bretaña	mx	México
be	Bélgica	bg	Bulgaria	nl	Holanda
gr	Grecia	bn	Brunei Darussalam	se	Suecia
u	Hungría	br	Brasil	de	Alemania
ie	Irlanda	ca	Canadá	dk	Dinamarca
in	India	ch	Suiza	es	España
it	Italia	cl	Chile	fi	Finlandia

¿Quién administra los dominios y las direcciones IP?

- Información sobre dominios
  - http://www.iana.org/
- Información sobre los dominios por paises
  - http://www.iana.org/cctld/cctld-whois.htm
- Qué es ICANN Internet Corporation for Assigned Names and Numbers
  - Es una organización internacional, responsable de:
    - Asignar espacio de direcciones numéricas de protocolo de Internet (IP),
    - Administración del sistema de nombres de dominio de primer nivel
  - http://www.icann.org/
  - http://www.icann.org/tr/spanish.html

¿Quién administra las direcciones IP y los dominios en España?

- Dominios en España
  - www.red.es
  - https://www.nic.es/index.html
- FAQS: https://www.interdominio.com/PortalServlet?pagi

¿Cómo asignamos las direcciones IP a las máquinas?

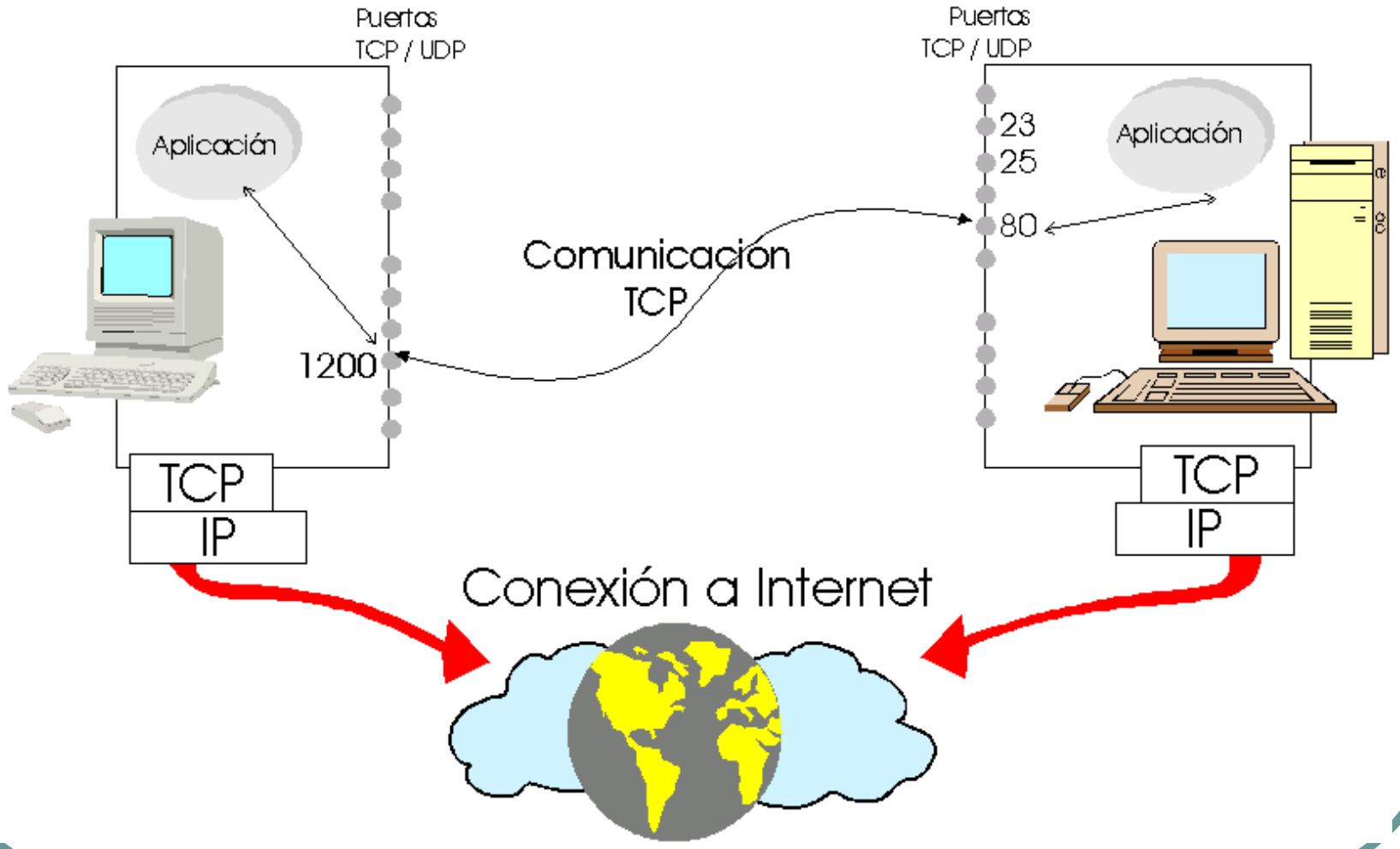
- A nuestra organización
  - Direcciones IP reales:
    - la autoridad de la región → ISP
  - Direcciones IP privadas
    - El administrador de cada red
- A nuestra máquinas
  - Direcciones fijas
  - Direcciones dinámicas (DHCP)

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

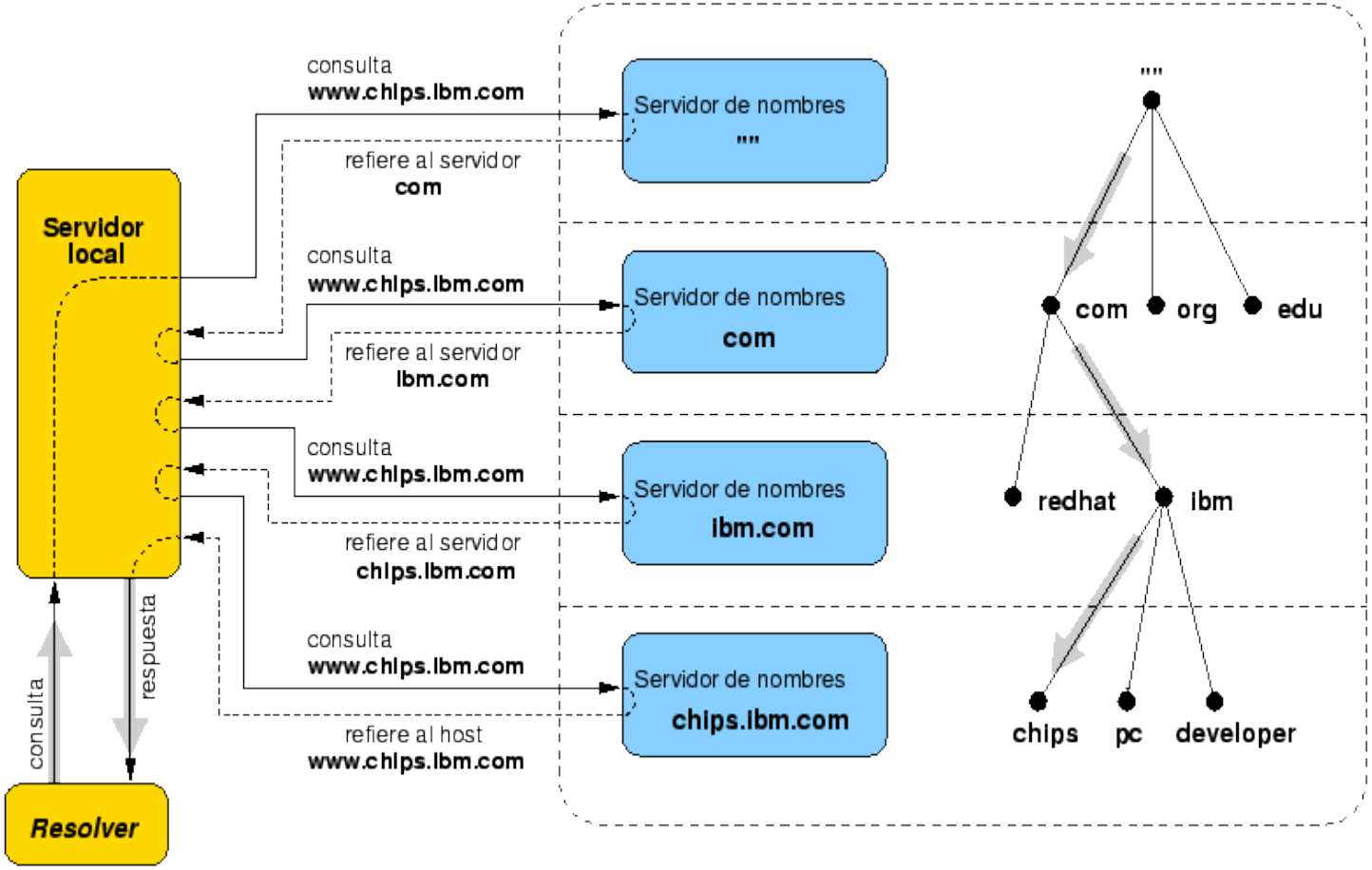
Puertos


Puertos
TCP / UDP
Aplicación
1200
TCP
IP
Comunicación
TCP
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)

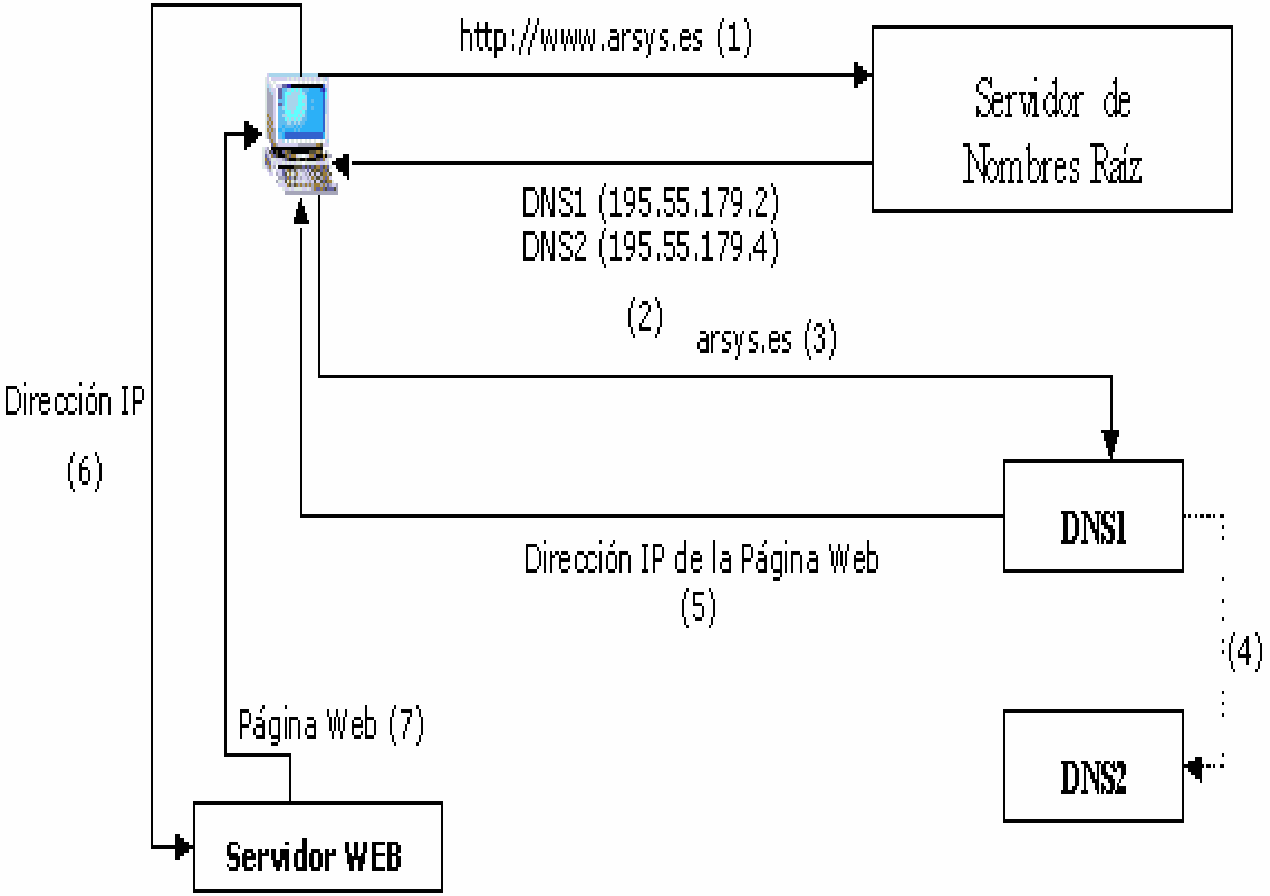
Resolución de nombres



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

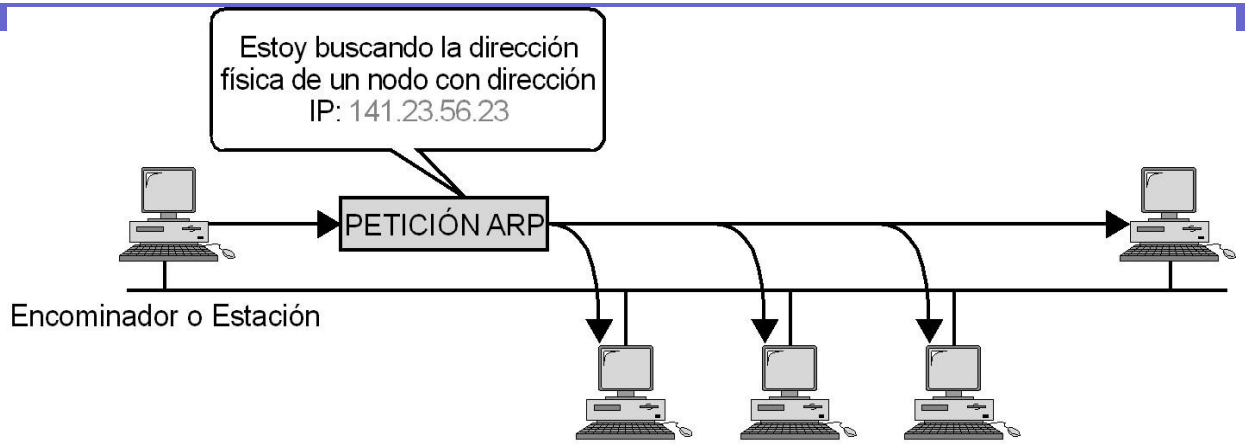
Ejemplo


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)
DNS2
Página Web (7)
Servidor WEB

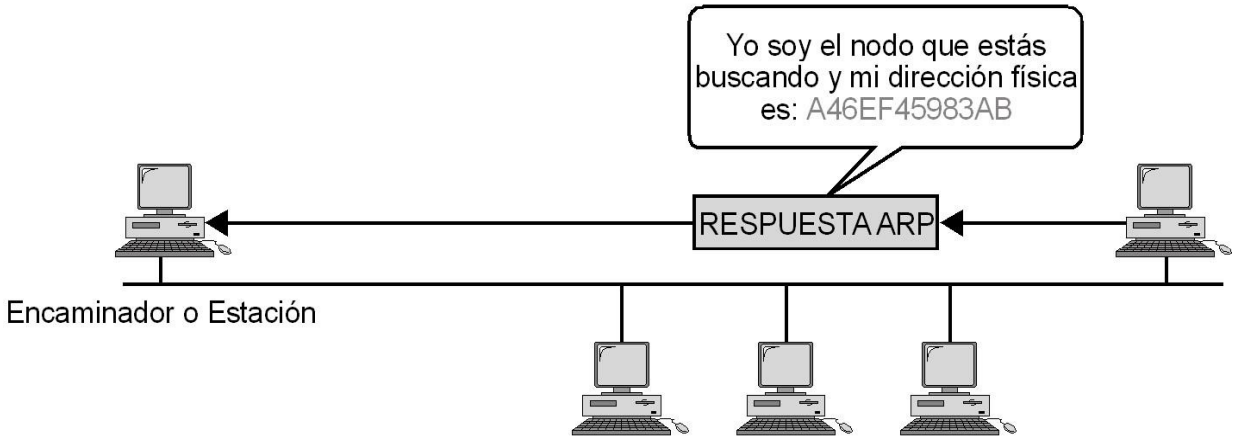
Relación entre direcciones IP y direcciones físicas

- 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



a. Petición ARP



b. Respuesta ARP

AMENAZAS EN INTERNET

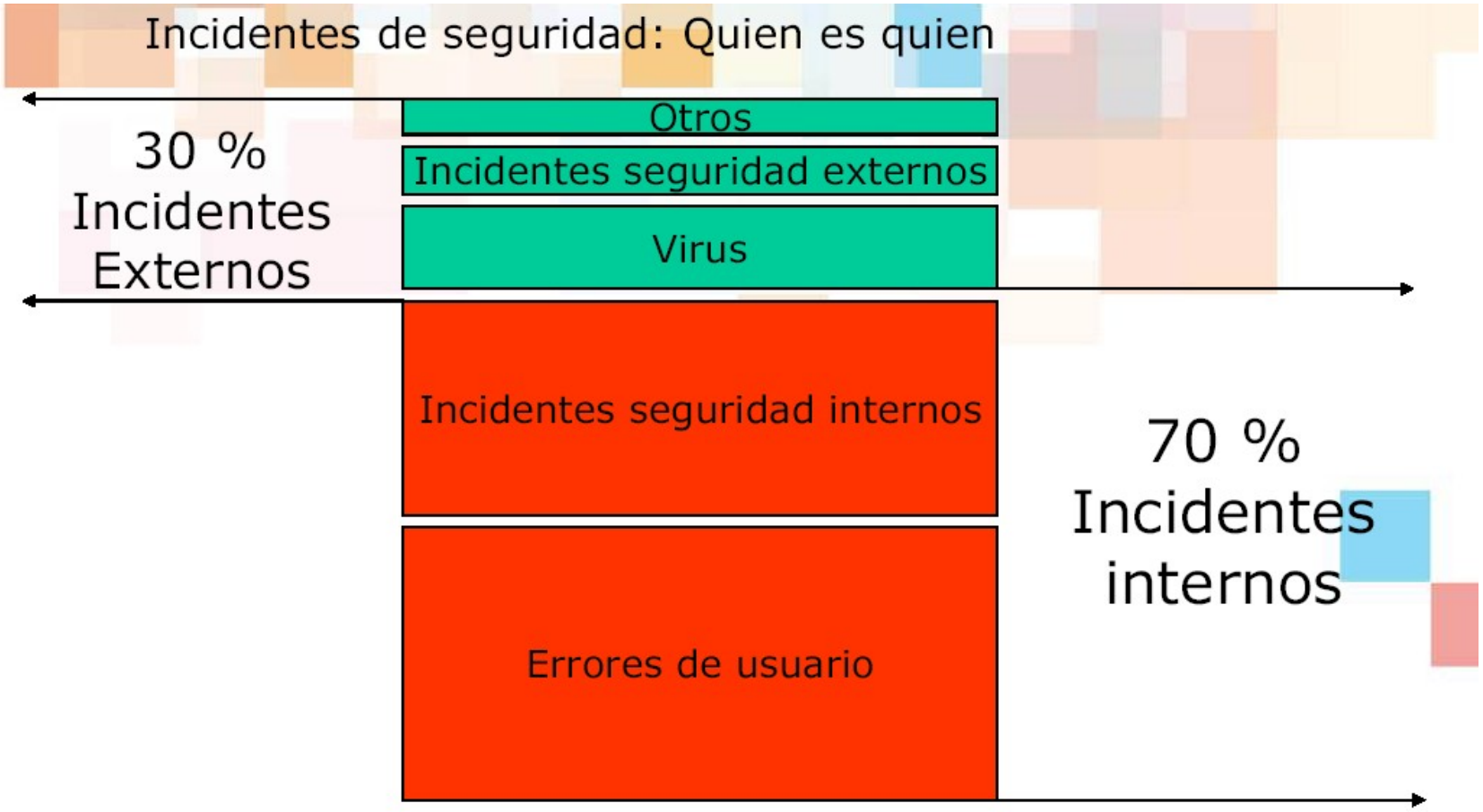
¿De qué amenazas debe defenderse un sistema seguro?

- 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

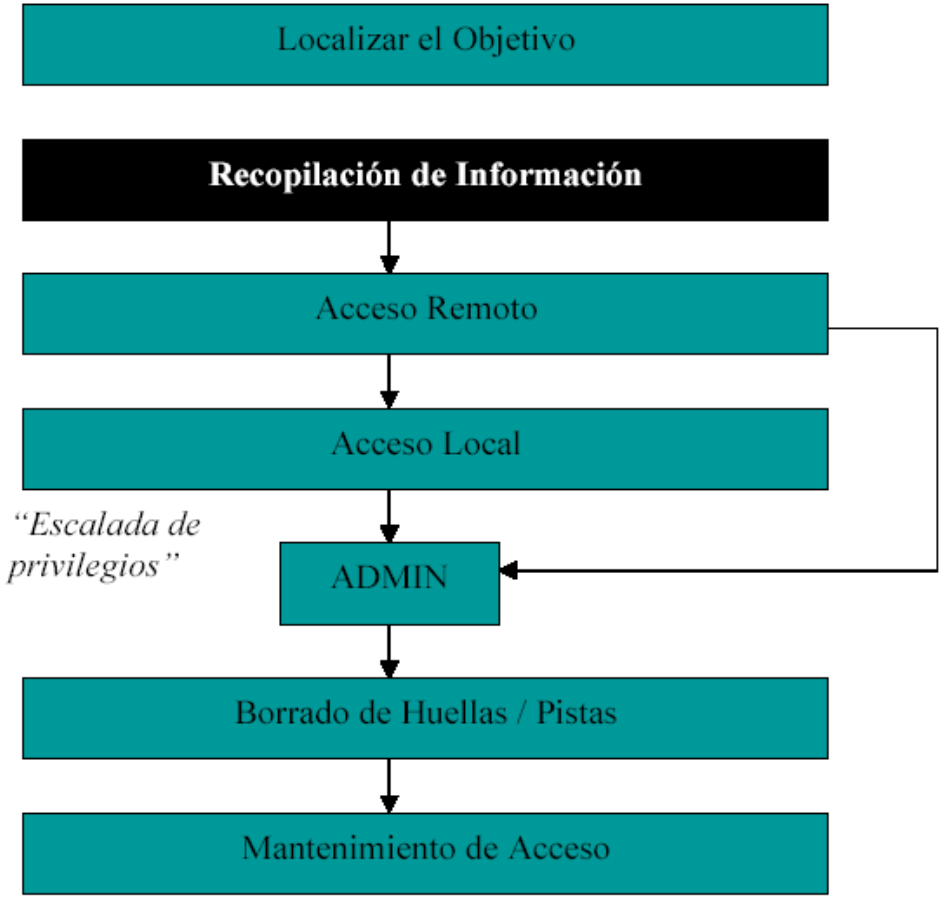
Tipos de amenazas (II)

- 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

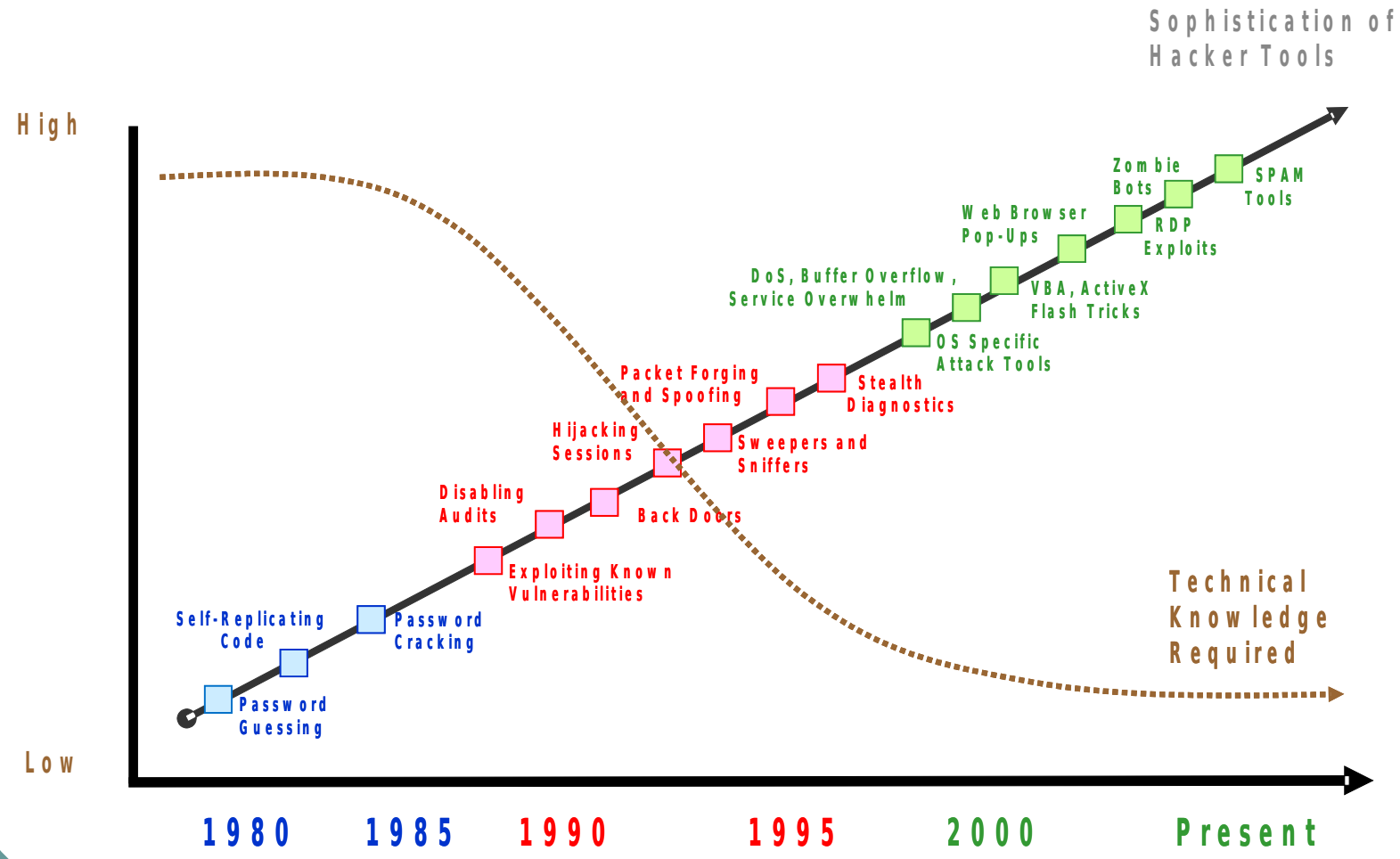
Fuente de los Incidentes



Anatomía de un ataque



History of Hacking Tools



Atáques

- *Spoofing*
  - Cambiar la dirección origen por una que es aceptada por el filtro
- *Hijacking*
  - Introducirse en la comunicación aprovechando una sesión abierto 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)

Amenazas

- Sniffer
- Ingeniería social

Spam

- correo no deseado ni justificado
  - 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

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)

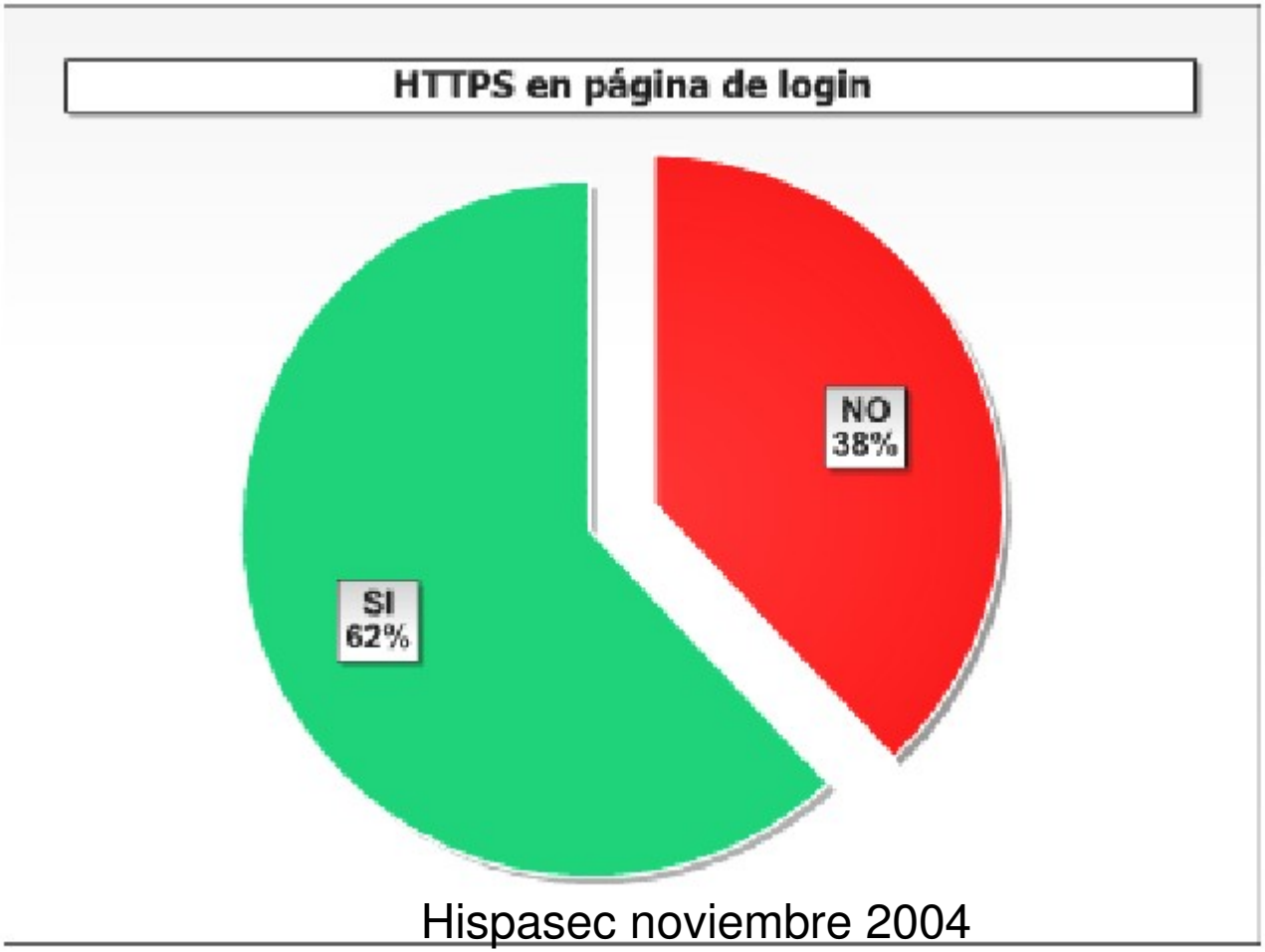
SCAM o cartas nigerianas

- Captación de “mulas” o intermediarios para blanquear dinero (Wester Union, PayPal)
- ejemplos

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

Phishing



Hispasec noviembre 2004

Hispasec noviembre 2004

CINCO NORMAS PARA EVITAR EL PHISHING

- http://www.seguridadpymes.es/
- 1.- 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
- 2.- 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
- 3.- No atienda a sorteos u ofertas económicas de forma inmediata e impulsiva
- 4.- No atienda a correos que le avisen del cese de actividades financieras recibidos por primera vez y de forma sorpresiva
- 5.- 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
- Comprobar que la conexión es HTTPS
- Finalizar mediante la función “SALIR”
- Desactivar las funciones de almacenamiento de claves en cache

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.aui.es/contraelspam/aui_dns.htm
- http://www.atomintersoft.com/products/alive-proxy/whois/
- http://www.all-nettools.com/toolbox navegación anónima

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

Vulnerabilidades

- Sans
- http://www.sans.org/top20/2005/top20-v6

Internet Explorer

- Los problemas más críticos son los que permiten la ejecución de código remoto sin ninguna interacción del usuario cuando éste visita una página web maliciosa o lee un correo electrónico.
- Internet Explorer contiene muchas vulnerabilidades que pueden llevar a la corrupción de la memoria, spoofing y a la ejecución de secuencias de comandos arbitrarios

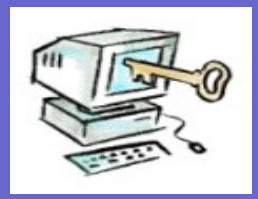
Escáneres de Vulnerabilidades y Sistemas de Gestión de Parches

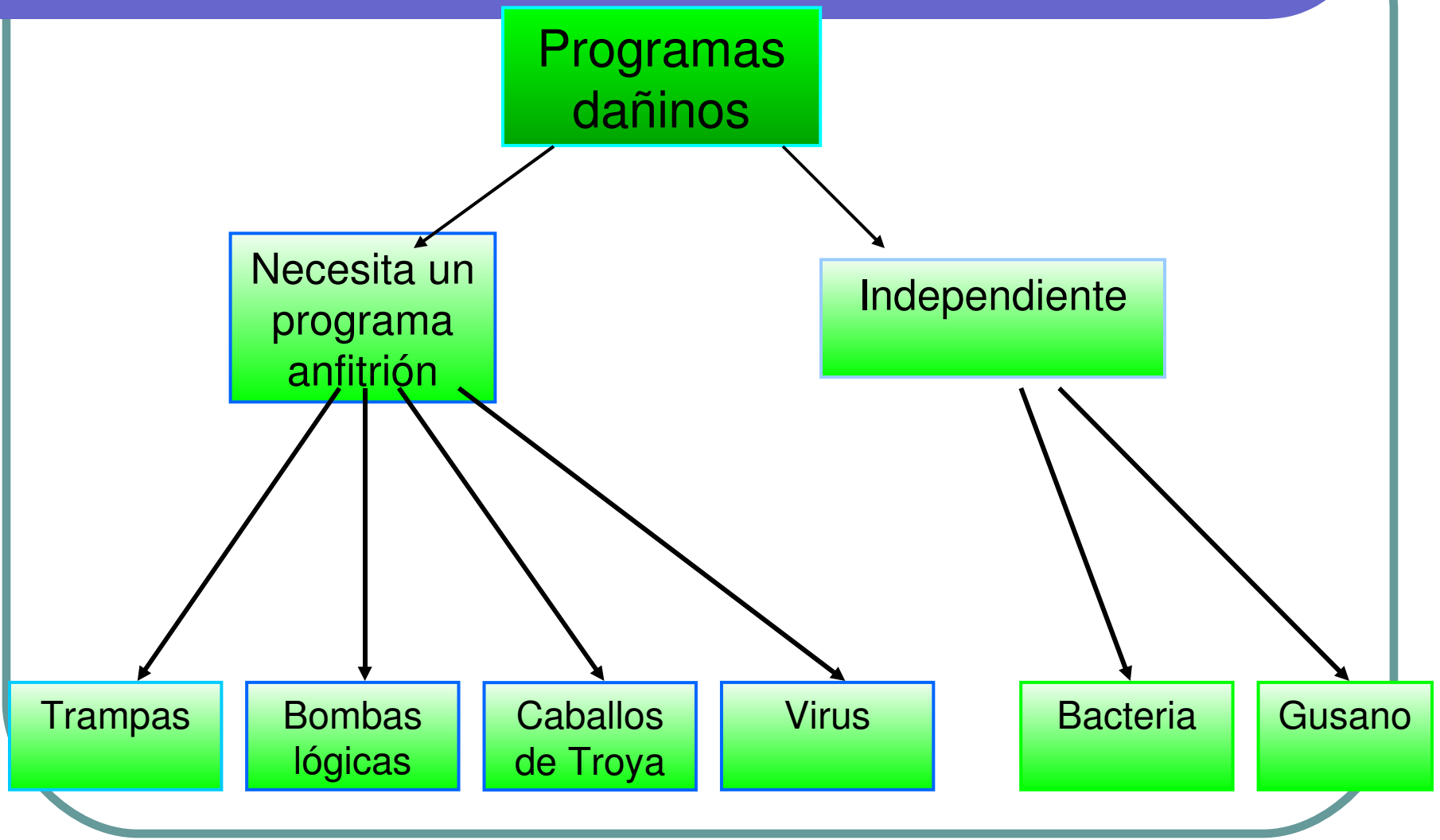
- El Microsoft Baseline Security Analyzer puede ser usado para identificar sistemas Windows vulnerables.
- http://www.microsoft.com/technet/security/tools/mbsahome.mspx

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)

Taxonomía de los programas dañinos (malware)





Definiciones

- Virus: código que se reproduce en otros programas.
- Una "bacteria" se reproduce hasta que llena todo el espacio del disco o los ciclos de CPU.
- Carga útil: los efectos perjudiciales que lleva a cabo el programa dañino, después de que haya tenido tiempo de extenderse.
- Gusano: 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).

Definiciones

- Caballos de Troya: instrucciones en un buen programa que hace que se produzcan efectos perjudiciales (enviando datos o contraseñas a un atacante a través de la red).
- 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

Validación de la identidad (autentificación)

- El objetivo de la validación es:
  - Permitir el acceso a los usuarios legítimos del sistema y denegarlo a los no autorizados.

Métodos de autentificación

- 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

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

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

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/bit128/k

Medios de pago

- Mobipay
  - Pago por teléfono móvil
  - http://www.mobipay.es/
- Paypal
  - Comprar sin compartir información financiera
  - http://www.paypal.es/es

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 is a standard for interoperation of IC cards ("Chip cards") and IC capable POS terminals, for authenticating credit and debit card payments
- Se aplica a **tarjetas chip**
  - http://emission.rtspain.com/
  - http://www.fnmt.es/es/html/tage/sc_tage.asp

Europay
Mastercard
Visa

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

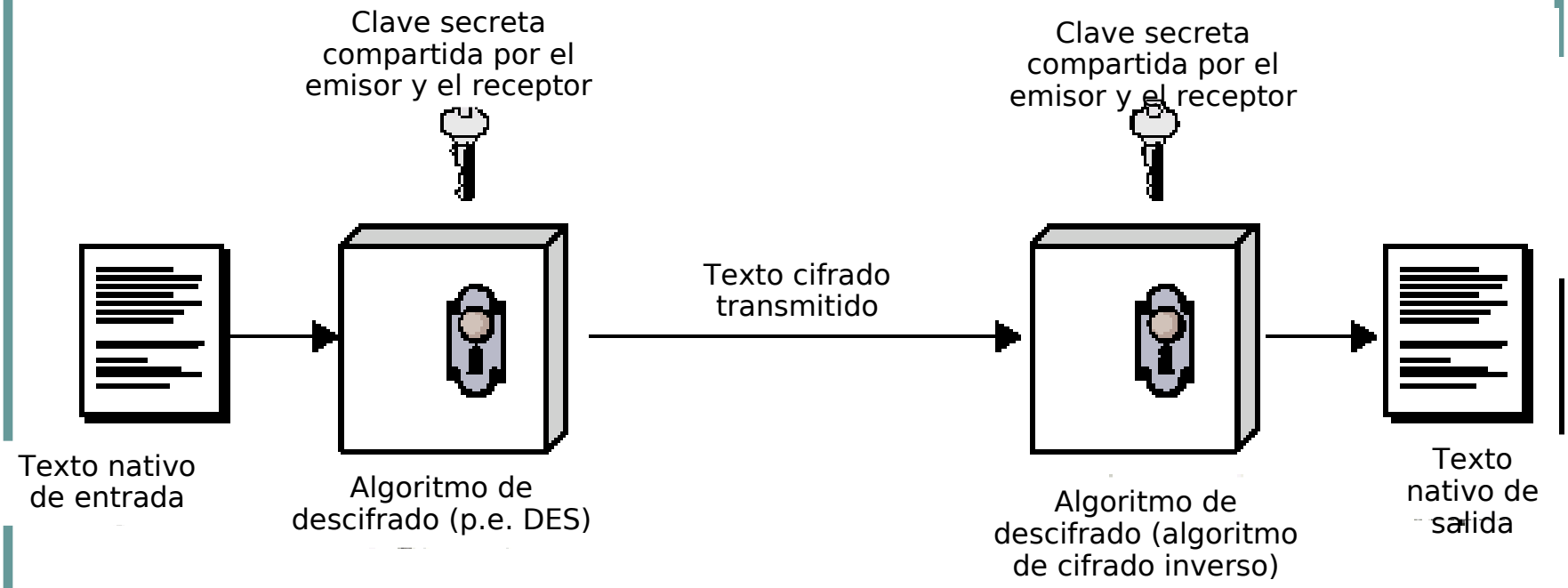
Criptografía

- 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.

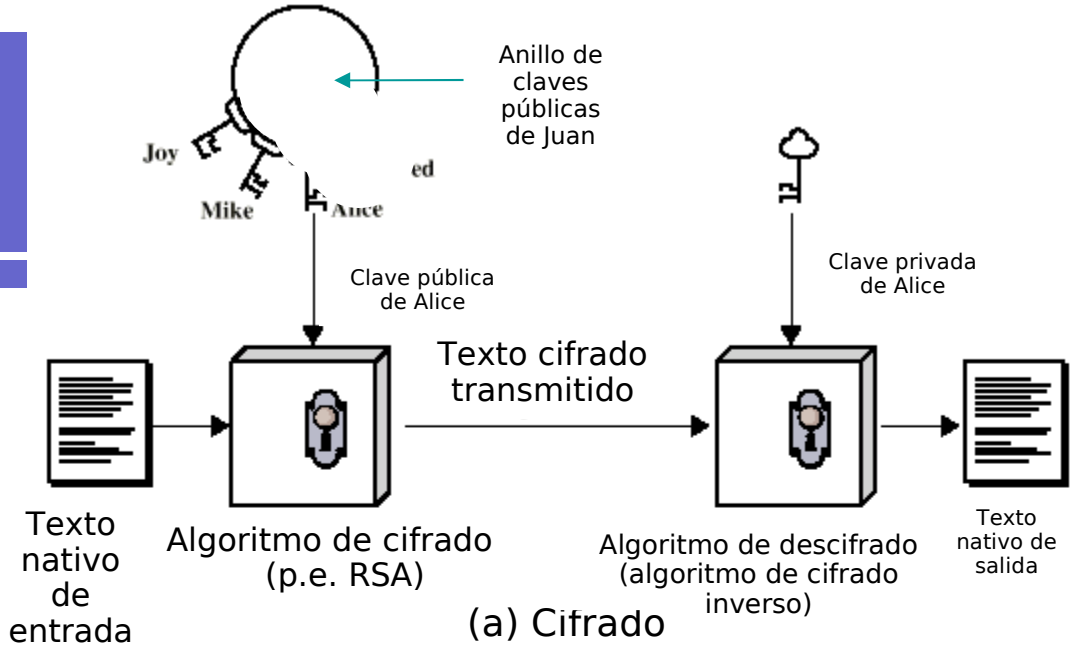
Ataques al cifrado convencional

- 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.

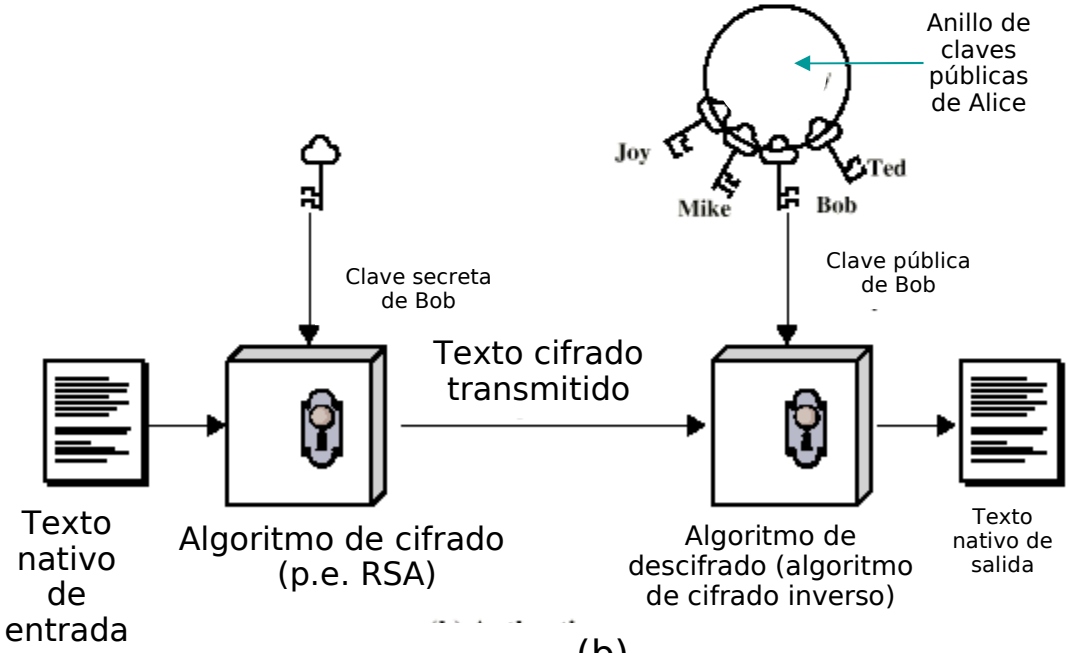
Cifrado de clave pública

- 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



(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
- 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.

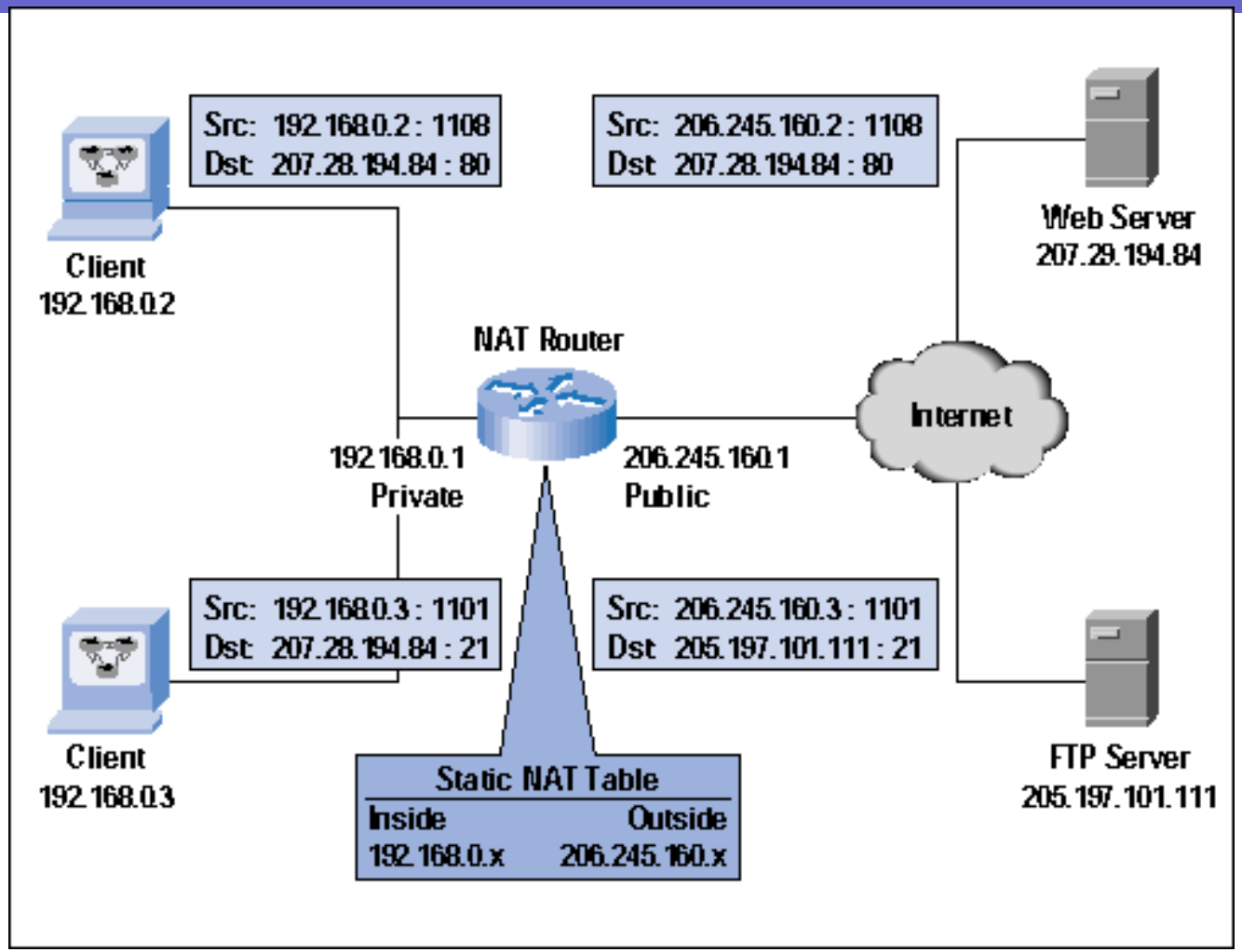
¿Qué información contiene un certificado ?

- **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**

Demostraciones

- Redes inalámbricas
- Sniffer
- Phishing

NAT estático



Scanner en línea

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

Recomendaciones

Haz lo que te diga, no lo que yo haga

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

- http://www.insecure.org/tools.html

75 herramientas de seguridad

- http://www.linuxdata.com.ar/index.php?idmanual=75seguridad.htm&manuale=1
- http://www.ush.it/free-services/security-tools/
- http://www.ausejo.net/seguridad/intrusiones.htm
- http://www.itsafe.gov.uk/index.html
- http://www.seguridad.unam.mx/doc/?ap=tutorial&id=131 curso del antiespia de microsoft

Direcciones

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

Denuncias

- http://194.179.107.38/
- http://www.gdt.guardiacivil.es/ guardia civil, delitos telemáticos
- http://www.policia.es/bit/index.htm Brigada de investigación tecnológica
- https://www.agpd.es/ Agencia de protección de datos
- www.apdcm.es