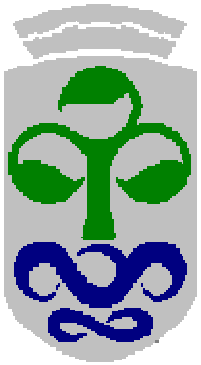
Seguridad en Internet



Cristina López Bravo

Departamento de Ingeniería Telemática

clbravo@det.uvigo.es

Contenidos

1. **Introducción a la seguridad en entornos de red**
   1. Objetivos
   2. Vulnerabilidad y amenazas
   3. Anatomía de un ataque
   4. Las 14 vulnerabilidades más importantes
   5. Política de seguridad
2. **Introducción a la criptografía**
   1. Criptografía de clave secreta
   2. Criptografía de clave pública
   3. Conexiones cifradas
3. **Protocolos de seguridad**
   1. IPSEC
   2. SSL Secure Sockets Layer
4. **Seguridad perimetral**
   1. Concepto y definiciones
   2. Routers y cortafuegos
   3. Sistemas de Detección de Intrusiones
   4. Cortafuegos personales y antivirus
   5. Ejemplos

Seguridad en Internet

1.Introducción a la seguridad en entornos de red

¿Qué es seguridad?

- La seguridad absoluta es indemostrable. Se habla de *fiabilidad*.
- Mantener un sistema seguro consiste en garantizar (*CIA: Confidentiality, Integrity, Availability*):
  - Confidencialidad: Sólo pueden acceder a los recursos de un sistema los agentes autorizados.
  - Integridad: Los recursos del sistema sólo pueden ser modificados por los agentes autorizados.
  - Disponibilidad: Los recursos del sistema tienen que estar a disposición de los agentes autorizados (contrario: denegación de servicio).

¿Qué es seguridad?

- La seguridad absoluta es indemostrable. Se habla de *fiabilidad*.
- Mantener un sistema seguro consiste en garantizar (*CIA: Confidentiality, Integrity, Availability*):
  - Confidencialidad: Sólo pueden acceder a los recursos de un sistema los **agentes autorizados**.
  - Integridad: Los recursos del sistema sólo pueden ser modificados por los **agentes autorizados**.
  - Disponibilidad: Los recursos del sistema tienen que estar a disposición de los **agentes autorizados** (contrario: denegación de servicio).

¿Qué es seguridad?

- Para determinar si un agente está o no autorizado para llevar a cabo determinadas tareas dentro del sistema, se necesitan, además, otros servicios de seguridad:
  - Autenticación: Identificación de los agentes y demostración de que un agente es “quien dice ser”.
  - Control de acceso: Especifica qué acciones pueden llevar a cabo los agentes del sistema.
  - No repudio: El emisor de un mensaje no puede negar que lo ha enviado, y el receptor de un mensaje no puede negar que lo ha recibido.
  - Auditoria: Registrar y analizar las acciones desarrolladas por los distintos agentes del sistema.

¿Qué queremos proteger?

- Los recursos del sistema
  - Hardware
  - Software
  - Datos
- Tipos de ataque a los recursos:
  - Interrupción: el recurso queda inutilizable o no disponible
  - Interceptación: captura de un recurso o acceso al mismo
  - Modificación o destrucción: Interceptación y manipulación del recurso
  - Fabricación: generación de recursos similares a los atacados

¿De qué nos queremos proteger?

- De todos aquellos agentes que puedan atacar a nuestros recursos
  - Personas: empleados, ex-empleados, curiosos, piratas, terroristas, intrusos remunerados
  - Amenazas lógicas: software defectuoso, herramientas de seguridad, puertas traseras, bombas lógicas, canales ocultos, virus, gusanos, caballos de Troya, programas conejo, técnicas salami.
  - Catástrofes naturales

¿Cómo nos podemos proteger?

1. Análisis de amenazas
2. Evaluación de (posibles) pérdidas y su probabilidad
3. Definición de una política de seguridad
4. Implementación de la política: mecanismos de seguridad
   - De prevención: durante el funcionamiento normal del sistema
   - De detección: mientras se produce un intento de ataque
   - De recuperación: tras un ataque, para retornar a un funcionamiento correcto: Análisis forense.

Vulnerabilidad

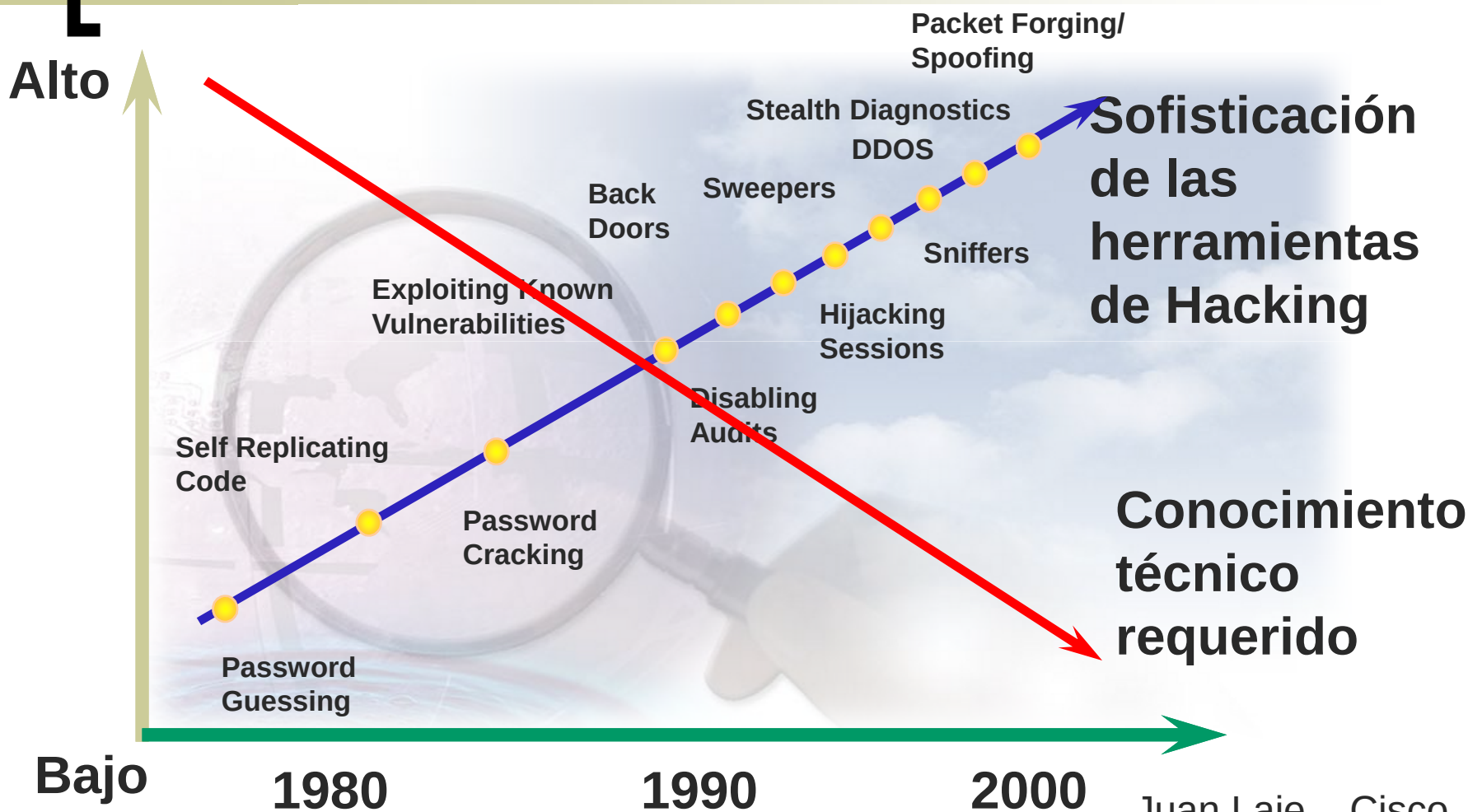
- Es un problema o error que puede ser utilizado maliciosamente para que un sistema realice funciones para los que no fue diseñado.
- La vulnerabilidad de una organización depende de:
  - El grado de publicidad de la organización
  - El coste de los ataques
  - La exposición de la organización a los ataques externos
  - La exposición de la organización ante ataques internos, o ante la facilitación de servicios (involuntaria o consciente) desde el interior
- En definitiva, depende de la:
  - Motivación: ¿Qué ventaja o provecho se puede sacar por obtener o destruir información?
  - Confianza: ¿En qué medida se puede contar con los usuarios?

Amenazas

Una amenaza es cualquier circunstancia o evento que potencialmente puede causar un daño a una organización mediante la exposición, modificación o destrucción de información, o mediante la denegación de servicios críticos.

- ¿Los malos van a tratar de actuar sobre mi sistema?
- ¿Puede ocurrir que elementos no deseados accedan (leyendo o modificando) información importante para mi organización?
- ¿Puede ocurrir que la reputación de mi organización se vea comprometida?

Amenazas: Más peligrosas y más fáciles de usar



Tipos de amenazas

- Fallo de componentes (hardware o software). Ej. caída del cortafuegos, fallos de un protocolo.
- Exposición de la información: correo mal enrutado, salida de una impresora, grupos o listas de acceso mal configuradas...
- Utilización de la información para usos no previstos. Puede venir del exterior o del interior.
- Borrado o modificación de la información. Puede conllevar pérdidas de integridad o confidencialidad.
- Penetración: Ataques por personas o sistemas no autorizados: caballos de Troya, virus, puertas traseras, gusanos, denegación de servicios...
- Suplantación: Intentos de confundirse con un usuario legítimo para sustraer servicios, información, o para iniciar transacciones que comprometan a la organización.

Principales Amenazas

- Ingeniería Social
  - Consiste en utilizar artilugios, tretas y otras técnicas para el engaño de las personas logrando que revelen información de interés para el atacante, como ser contraseñas de acceso. Se diferencia del resto de las amenazas básicamente porque no se aprovecha de debilidades y vulnerabilidades propias de un componente informático para la obtención de información.

Principales Amenazas

- Phishing
  - Consiste en el envío masivo de mensajes electrónicos que fingen ser notificaciones oficiales de entidades/empresas legítimas con el fin de obtener datos personales y bancarios de los usuarios.

Principales Amenazas

- Escaneo de Puertos
  - Consiste en detectar qué servicios posee activos un equipo, con el objeto de ser utilizados para los fines del atacante.

Principales Amenazas

- Código Malicioso / Virus
  - Se define como todo programa o fragmento del mismo que genera algún tipo de problema en el sistema en el cual se ejecuta, interfiriendo de esta forma con el normal funcionamiento del mismo. Existen diferentes tipos de código malicioso:
    - Bombas lógicas
    - Troyanos
    - Gusanos

Principales Amenazas

- Código Malicioso / Virus
  - Cookies
    Son archivos de texto con información acerca de la navegación efectuada por el usuario en Internet e información confidencial del mismo que pueden ser obtenidos por atacantes.
  - Keyloggers
    Es una aplicación destinada a registrar todas las teclas que un usuario tipea en su computadora; algunos de ellos además registran otro tipo de información útil para un atacante, como ser, imágenes de pantalla.
  - Spyware
    Aplicaciones que recogen y envían información sobre las páginas web que más frecuentemente visita un usuario, tiempo de conexión, datos relativos al equipo en el que se encuentran instalados (sistema operativo, tipo de procesador, memoria, etc.) e, incluso, hay algunos diseñados para informar de si el software que utiliza el equipo es original o no.

Principales Amenazas

- Exploits
  - Se trata de programas o técnicas que explotan una vulnerabilidad de un sistema para el logro de los objetivos del atacante, como ser, intrusión, robo de información, denegación de servicio, etc.

Principales Amenazas

- Ataques de Contraseña
  - Consiste en la prueba metódica de contraseñas para lograr el acceso a un sistema, siempre y cuando la cuenta no presente un control de intentos fallidos de logueo. Este tipo de ataques puede ser efectuado:
    - Por diccionario: existiendo un diccionario de palabras, una herramienta intentará acceder al sistema probando una a una las palabras incluidas en el diccionario.
    - Por fuerza bruta: una herramienta generará combinaciones de letras números y símbolos formando posibles contraseñas y probando una a una en el login del sistema.

Principales Amenazas

- Eavesdropping
  - El eavesdropping es un proceso por el cual un atacante capta de información (cifrada o no) que no le iba dirigida. Existen diferentes tipos de técnicas que pueden utilizarse:
    - Sniffing
      Consiste en capturar paquetes de información que circulan por la red con la utilización de una herramienta para dicho fin, instalada en un equipo conectado a la red; o bien mediante un dispositivo especial conectado al cable. En redes inalámbricas la captura de paquetes es más simple, pues no requiere de acceso físico al medio.

Principales Amenazas

- Eavesdropping
  - VLAN hopping
    Las VLANs son redes LAN virtuales las cuales se implementan para generar un control de tráfico entre las mismas, de forma que los equipos conectados a una VLAN no posean acceso a otras. Este tipo de ataque pretende engañar a un switch (sobre el cual se implementan VLANs) mediante técnicas de Switch Spoofing logrando conocer los paquetes de información que circulan entre VLANs.
  - STP manipulation
    Este tipo de ataque es utilizado en topologías que cuentan con un árbol de switches que implementan el protocolo Spanning Tree Protocol para coordinar su comunicación. El equipo atacante buscará convertirse en la “raíz” de dicho árbol, con el objeto de poder tener acceso a los paquetes de información que circulan por todos los switches.

Principales Amenazas

- Eavesdropping
  - Desbordamiento de CAM
    Se trata de inundar la tabla de direcciones de un switch con el objeto de bloquear la capacidad que éste posee de direccionar cada paquete exclusivamente a su destino. De esta forma el atacante podrá efectuar sniffing de los paquetes enviados por un switch, cuando en condiciones normales un switch no es vulnerable a este tipo de ataques.

Principales Amenazas

- Man-in-the-middle
  - El atacante se interpone entre el origen y el destino en una comunicación pudiendo conocer y/o modificar el contenido de los paquetes de información, sin esto ser advertido por las víctimas. Esto puede ocurrir en diversos ambientes, como por ejemplo, en comunicaciones por e-mail, navegación en Internet, dentro de una red LAN, etc..

Principales Amenazas

- Defacement
  - Consiste en la modificación del contenido de un sitio web por parte de un atacante.

Principales Amenazas

- IP Spoofing - MAC Address Spoofing
  - El atacante modifica la dirección IP o la dirección MAC de origen de los paquetes de información que envía a la red, falsificando su identificación para hacerse pasar por otro usuario. De esta manera, el atacante puede asumir la identificación de un usuario válido de la red, obteniendo sus privilegios.

Principales Amenazas

- Repetición de Transacción
  - Consiste en capturar la información correspondiente a una transacción efectuada en la red interna o en Internet, con el objeto de reproducirla posteriormente. Esto cobra real criticidad en transacciones monetarias.

Principales Amenazas

- Backdoors
  - También denominados “puertas traseras”, consisten en accesos no convencionales a los sistemas, los cuales pueden permitir efectuar acciones que no son permitidas por vías normales. Generalmente son instalados por el atacante para lograr un permanente acceso al sistema.

Principales Amenazas

- DHCP Starvation
  - El atacante busca reemplazar al servidor DHCP que se encuentra funcionando en la red, de forma que pueda asignar a los clientes direcciones IP y otra información (como ser el servidor Gateway) de acuerdo a su conveniencia. De esta forma podría luego simular ser el Gateway e interceptar la información que los clientes envíen, con el tipo de ataque Man-in-the-middle.

Principales Amenazas

- Trashing o basureo
  - Consiste en la búsqueda de información dentro de la basura. Esto puede representar una amenaza importante para usuarios que no destruyen la información crítica o confidencial al eliminarla.

Principales Amenazas

- Denegación de Servicio
  - Su objetivo es degradar considerablemente o detener el funcionamiento de un servicio ofrecido por un sistema o dispositivo de red. Existen diferentes técnicas para la explotación de este tipo de ataques:
    - Envío de paquetes de información mal conformados de manera de que la aplicación que debe interpretarlo no puede hacerlo y colapsa.
    - Inundación de la red con paquetes (como ser ICMP - ping, TCP – SYN, IP origen igual a IP destino, etc.) que no permiten que circulen los paquetes de información de usuarios.
    - Bloqueo de cuentas por excesivos intentos de login fallidos.
    - Impedimento de logueo del administrador.

Principales Amenazas

- Denegación de Servicio Distribuída
  - Su objetivo es el mismo que el perseguido por un ataque de denegación de servicio común, pero en este caso se utilizan múltiples equipos para generar el ataque.

Principales Amenazas

- Fraude Informático
  - Se trata del perjuicio económico efectuado a una persona mediante la utilización de un sistema informático, ya sea, modificando datos, introduciendo datos falsos o verdaderos o cualquier elemento extraño que sortee la seguridad del sistema.

Principales Amenazas

- Software Ilegal
  - Consiste en la instalación de software licenciado sin contar con la licencia correspondiente que habilita su uso, o mediante la falsificación de la misma.

Principales Amenazas

- Acceso a Información Confidencial Impresa
  - Ocurre cuando información confidencial impresa es obtenida por personal no autorizado debido a que la misma no es resguardada adecuadamente mediante por ejemplo, una política de limpieza de escritorios.

Principales Amenazas

- Daños Físicos al Equipamiento
  - Los daños físicos pueden ser ocasionados por:
    - Acciones intencionadas
    - Negligencia de los usuarios (ej.: derrame de líquidos, golpes, etc.)
    - Catástrofes naturales (ej.: fallas eléctricas, incendio, inundación, falta de refrigeración, etc.)

Principales Amenazas

- Robo de Equipos o Componentes
  - El robo puede involucrar todo un equipo o de parte del mismo, ej.: un disco rígido. Puede ocurrir por un deficiente control de acceso establecido al centro de cómputos (o recinto donde residen los equipos: servidores, routers, switches, etc.), así como a las propias instalaciones del Organismo.

Principales Amenazas

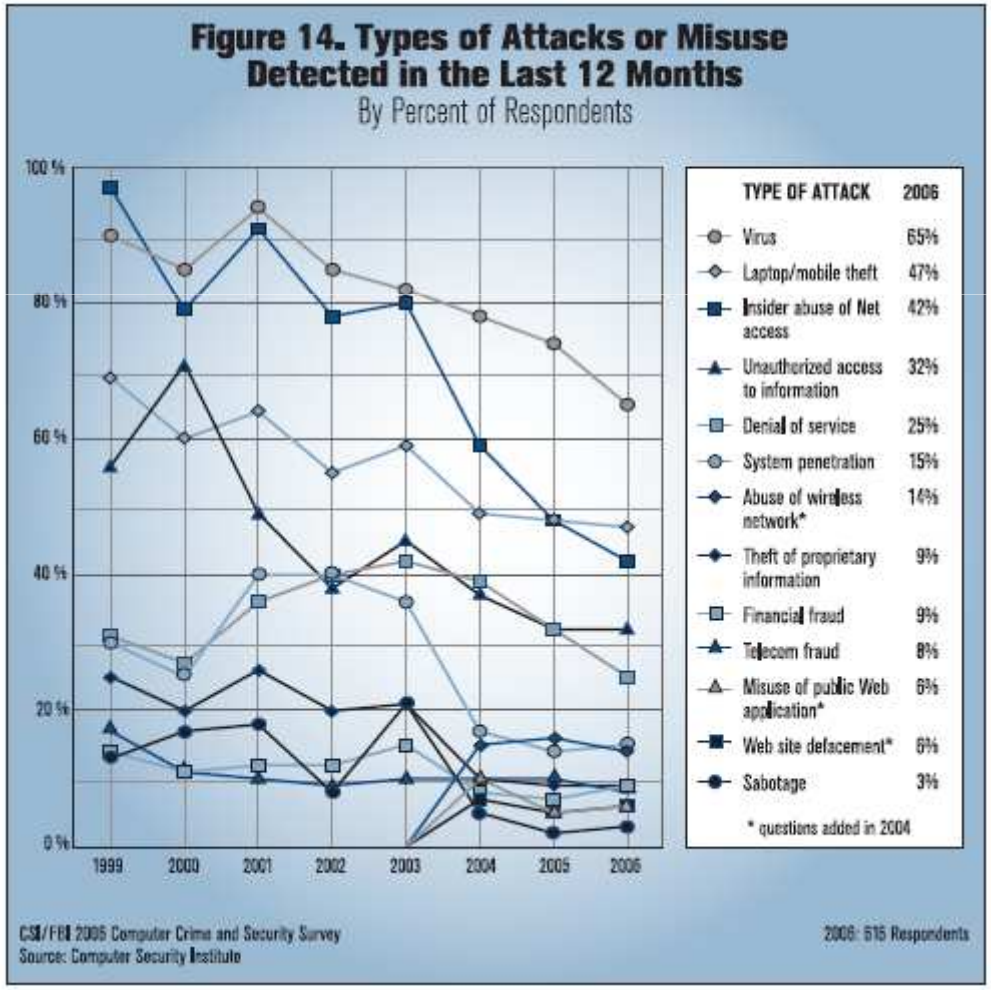
Pérdida de Copias de Resguardo

Si no existen adecuadas medidas de seguridad física para las copias de resguardo, las mismas pueden dañarse, por ejemplo, en caso de ser afectadas por **desastres** como un **incendio, inundación, o incluso por robo**. Asimismo, una administración inadecuada de los medios físicos de almacenamiento puede provocar la **obsolescencia** de los mismos (ej.: reutilización excesiva de cintas).

Por otra parte, se debe tener en cuenta la obsolescencia tecnológica de los medios de almacenamiento con el paso del tiempo, de manera de actualizarlos adecuadamente para permitir su restauración en caso de ser necesaria.

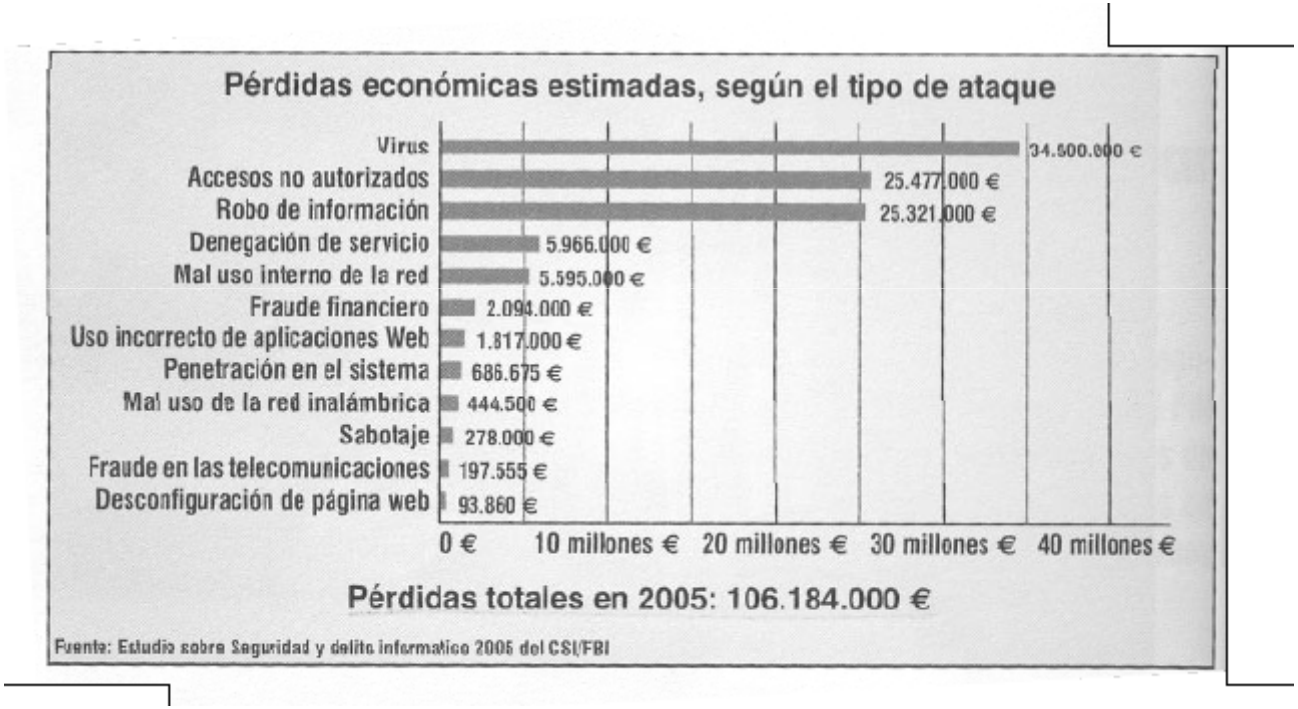
Estadísticas de la amenaza

- Fuente: Estudio del CSI/FBI de 2006 (www.gocsi.com)



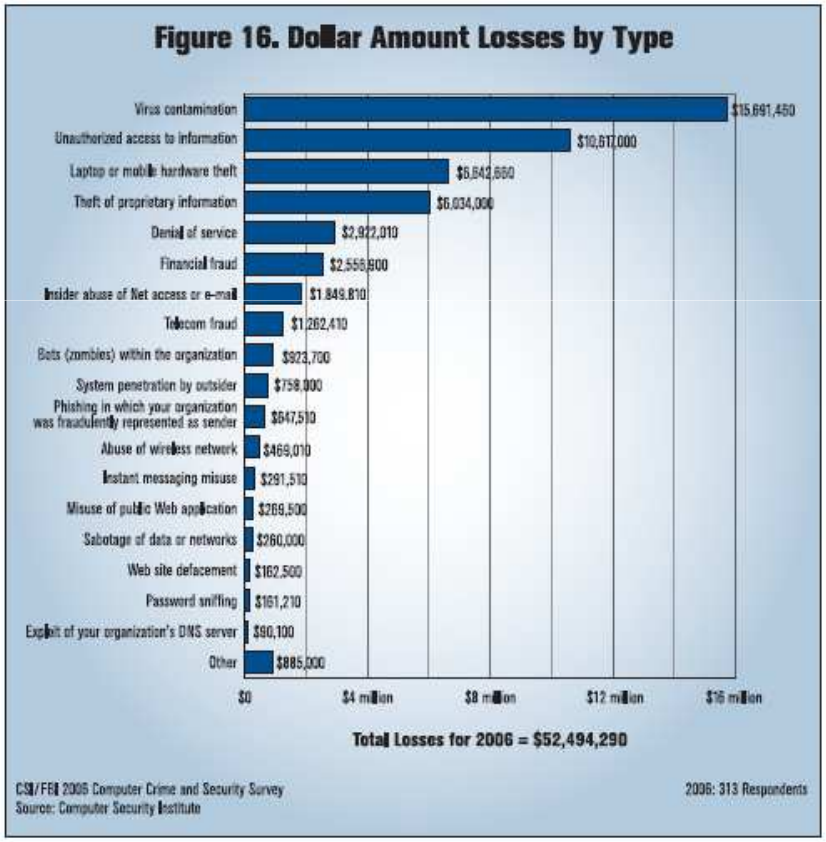
Estadísticas de la amenaza

- Fuente: Revista SIC



Estadísticas de la amenaza

- Fuente: Estudio del CSI/FBI de 2006 (www.gocsi.com)



Estadísticas de la amenaza

- HoneyPots-HoneyNets

- Estas “trampas de red” son sistemas que se activan con la finalidad específica de que los expertos en seguridad puedan observar en secreto la actividad de los intrusos.
- Es un servidor que presenta ciertas vulnerabilidades para “tentar” a intrusos.
- Mientras los intrusos vulneran el Server, los auditores documentan las nuevas técnicas y con ello se verifica los servidores reales en producción.
- www.project.honeynet.org.

Estadísticas de la amenaza

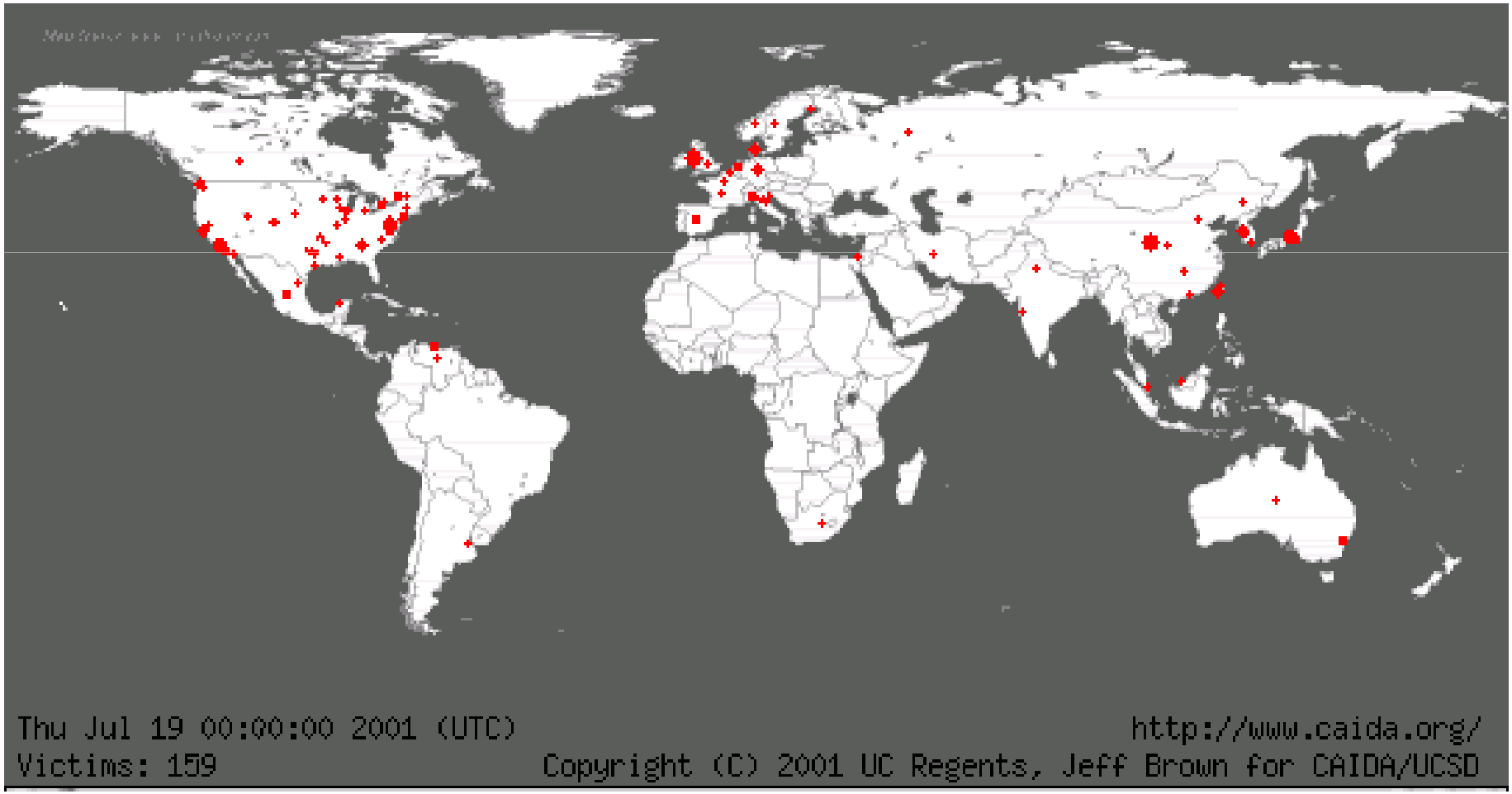
- Honeynet Project (project.honeynet.org)
  - Grupo de investigación dedicado a aprender las herramientas, tácticas y motivaciones de la comunidad de hackers y a compartir las lecciones aprendidas
  - Enfoque en dos áreas:
    - Medir la agresividad de la comunidad de hackers
    - Evaluar el concepto de Alerta y Predicción Temprana

Estadísticas de la amenaza

- Honeynet Project
  - Analizando el pasado ...
    - Los resultados asustan (1 servidor comprometido a los 15 minutos de estar en la Internet)
    - La comunidad de hackers es MUY agresiva
    - No se hicieron intentos de anunciar los “éxitos”
  - Prediciendo el futuro
    - Análisis estadístico de meses de actividad

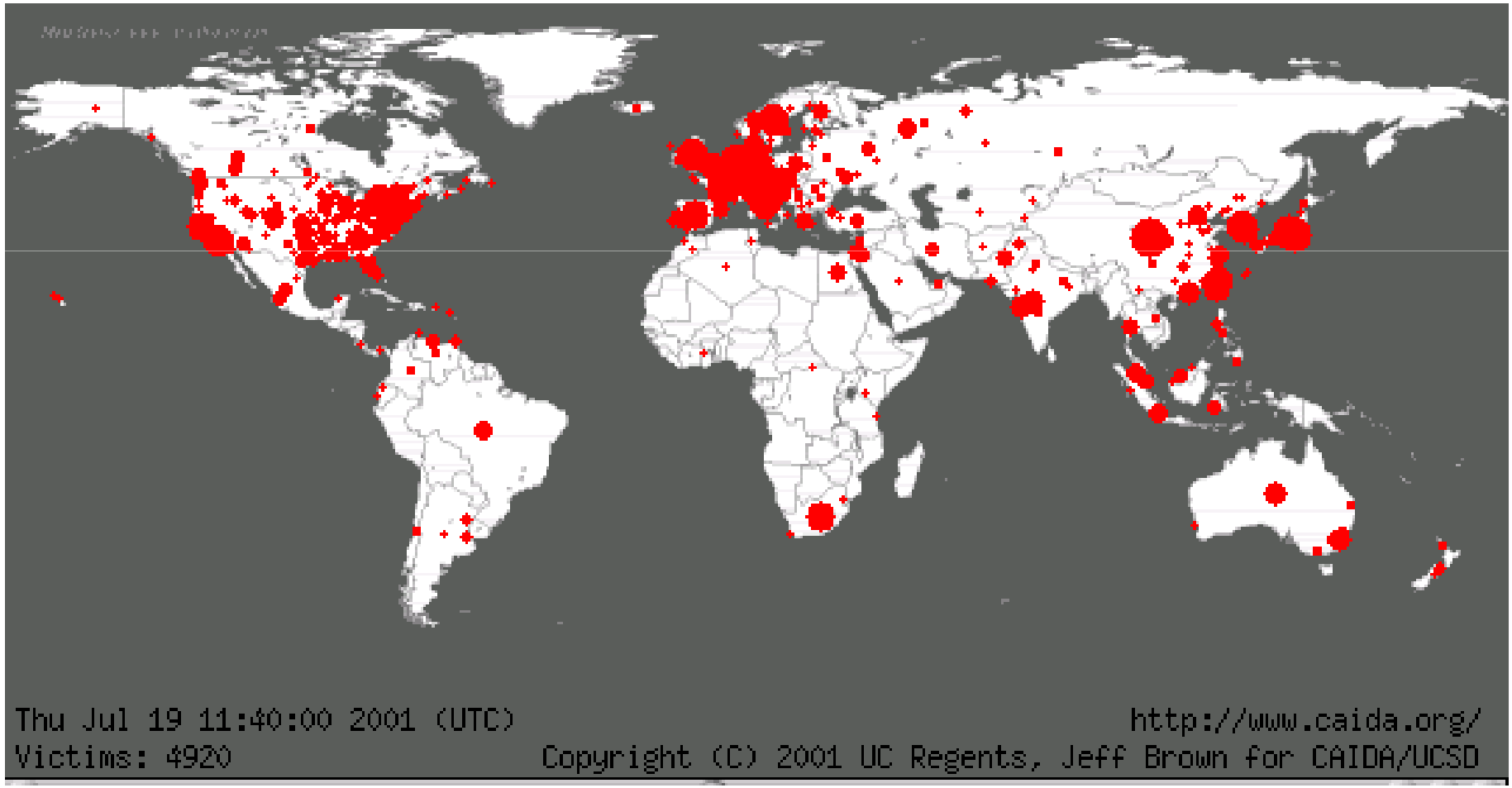
Propagación del Code Red

19 de Julio, Media Noche - 159 Hosts Infectados



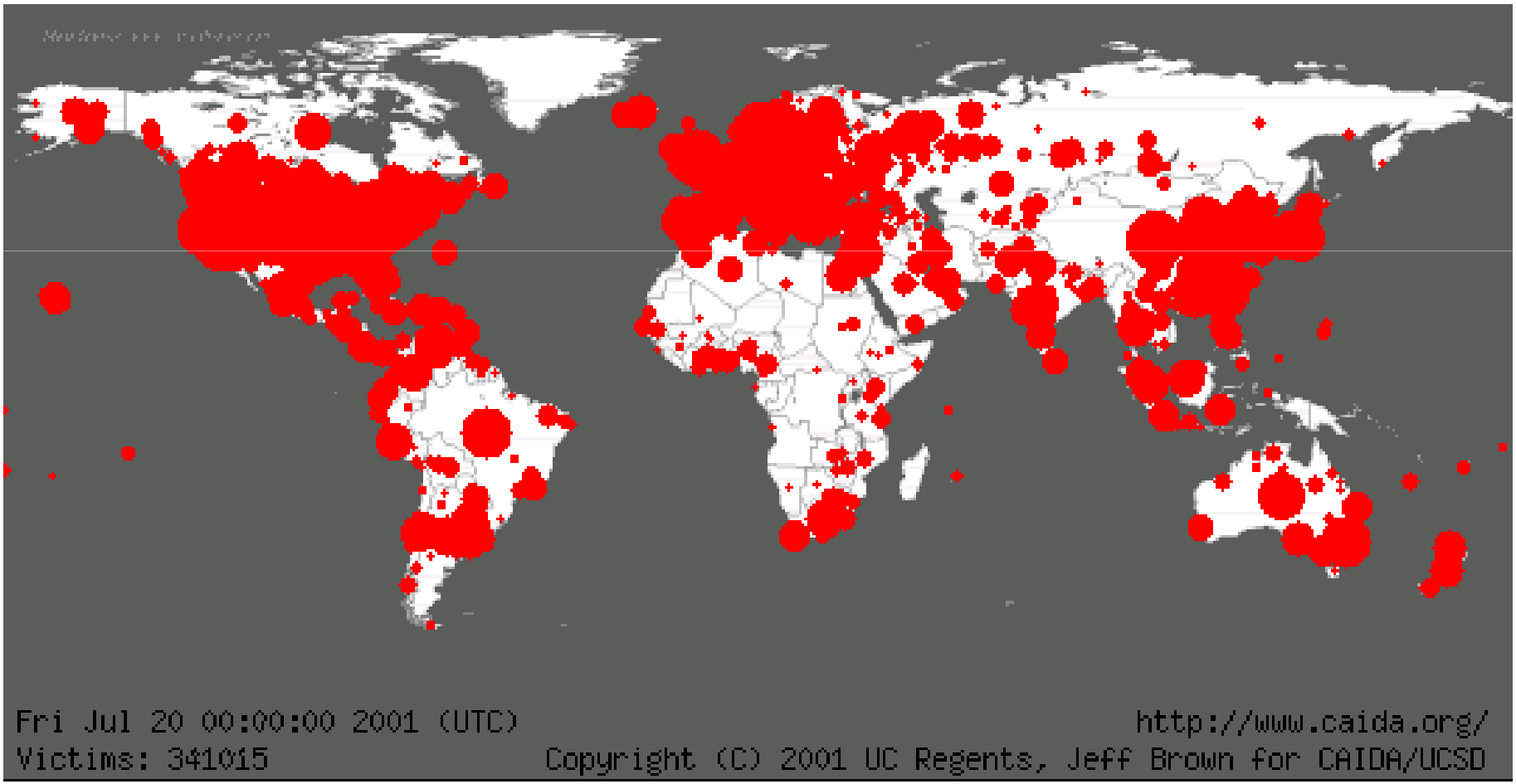
Propagación del Code Red

19 de Julio, 11:40 am - 4,920 Hosts Infectados



Propagación del Code Red

20 de Julio, Media Noche - 341,015 Hosts Infectados



Ejemplos de signos de ataque

- El sistema se para
- Discrepancias en la información sobre las cuentas (p. ej. /usr/admin/lastlog disminuye a veces)
- Intentos de escritura en los ficheros del sistema
- Algunos ficheros desaparecen
- Denegación de servicio (el sistema pasa a monousuario, y ni siquiera el administrador puede entrar)
- Las prestaciones del sistema son inexplicablemente bajas
- Sondas sospechosas (logins incorrectos repetidos desde otro nodo).

Ejemplos de signos de ataque

- Logins desde lugares o a horas no habituales
- Ficheros con nombres sospechosos (“...”, “.. ”, “.xx”, “.mail”, etc.)
- Cambios en los ficheros de claves, listas de grupos, etc.
- Cambios en ficheros de configuración del sistema, en bibliotecas, en ejecutables, etc.
- Cambios en los datos: páginas WWW, servidores FTP, applets, plugIns, etc.
- Herramientas dejadas atrás por el atacante: Caballos de Troya, Sniffers, etc.
- Procesos periódicos (at, cron) o transferencias periódicas (ftp, mail) no justificables
- Interfaces de red en modo promiscuo

Ejemplos de agujeros en la seguridad

- Claves fáciles de adivinar, o claves por defecto
- Cuentas inactivas o no usadas, cuentas innecesarias, cuentas de grupo
- Servicios no seguros mal configurados (tftp, sendmail, ftp)
- Servicios no seguros e inútiles (finger, rusers, rsh)
- Ficheros de configuración de la red o del acceso no seguros (“entradas +” en configuración NIS)
- Consolas inseguras
- Protección de acceso y propiedad de ficheros sensibles mal configurada.
- Versiones no actualizadas del sistema operativo.
- Conexiones telefónicas inseguras
- Política de copias de seguridad inexistente o mal diseñada.

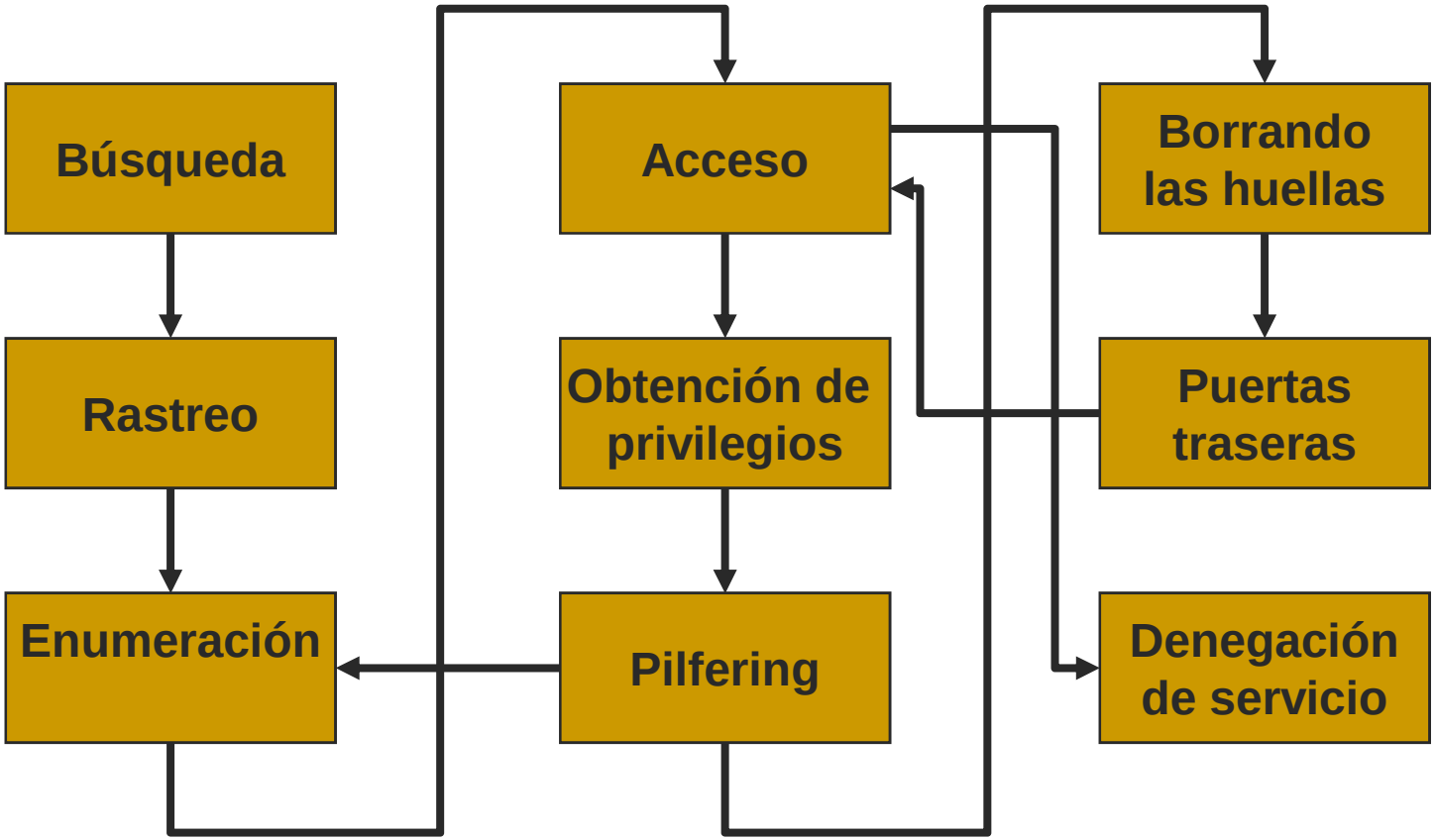
Contramedidas

- Identificación y Autenticación (I&A). Procedimiento por el que se reconocen y verifican identidades válidas de usuarios y procesos. Tres tipos:
  - Estática (username/password)
  - Robusta (claves de un solo uso, firmas electrónicas)
  - Continua (firmas electrónicas aplicadas a todo el contenido de la sesión)
- Control de la adquisición y actualización del software. Previene contra los virus, caballos de Troya, el software interactivo (Java, ActiveX), y el robo de licencias
- Cifrado. Proporciona confidencialidad, autenticidad e integridad
- Actuaciones en el nivel de arquitectura: Redes virtuales privadas, Sistemas de acceso remoto, acceso a bases de datos, etc.

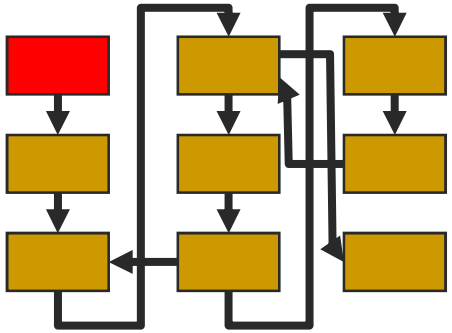
Contramedidas

- Gestión de incidentes. Detección de ataques, históricos, control de integridad, etc.
- Acciones administrativas. Identificación de responsables de seguridad, política de sanciones, políticas de privacidad, definición de buenas prácticas de uso, etc.
- Formación. Información a los usuarios de las amenazas y cómo prevenirlas, políticas de la empresa frente a fallos de seguridad, etc.

Anatomía de un ataque

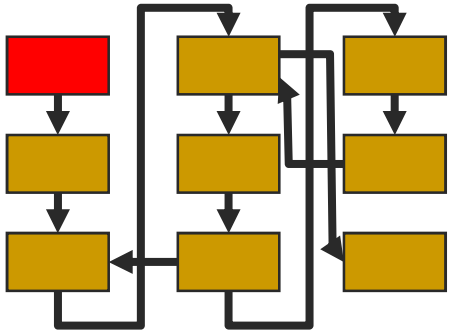


Anatomía de un ataque. Búsqueda



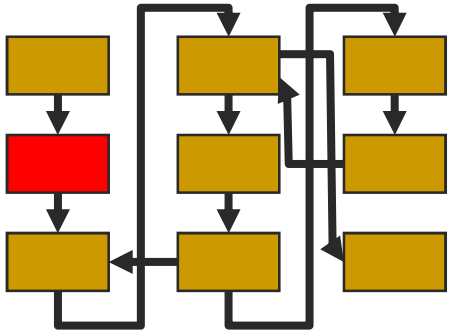
- Objetivo
  - Recogida de información, ingeniería social, selección de rangos de direcciones y espacios de nombres
- Técnicas
  - Búsquedas en información pública (Altavista con directivas link: o host:)
  - Interfaz web a whois
  - ARIN whois
  - DNS zone transfer (nslookup)
  - Reconocimiento de redes (traceroute)
  - Sondeo SMTP

Anatomía de un ataque. Búsqueda



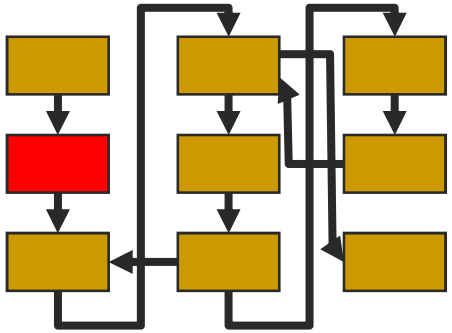
- Contramedidas
  - Control del contenido de la información pública
  - Precaución con la información de registro
  - Seguridad en DNS (p. ej. no permitir las transferencias de zona)
  - Instalación de sistemas de detección de intrusiones (NIDS)

Anatomía de un ataque. Rastreo (*scanning, barrido*)



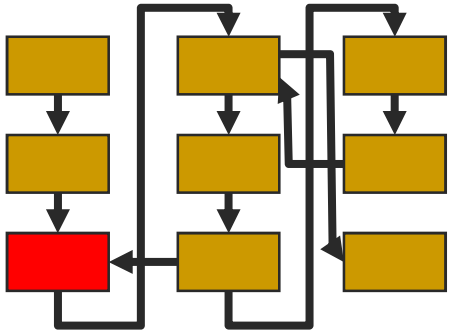
- Objetivo
  - Identificación de equipos y servicios.
  - Selección de los puntos de entrada más prometedores
- Técnicas
  - Ping sweep (fping, nmap)
  - Consultas ICMP (icmpquery)
  - TCP/UDP port scan (Strobe, udp-scan, netcat, nmap, SuperScan, WinScan, etc.)
  - Detección del sistema operativo (nmap, queso)
  - Herramientas de descubrimiento automático (Chaos)

Anatomía de un ataque. Rastreo



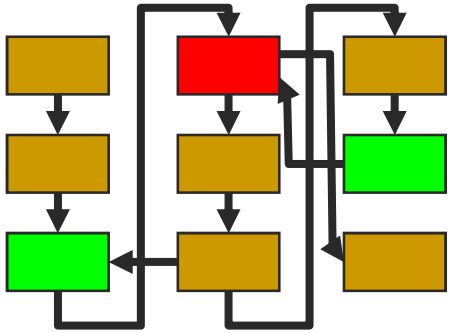
- Contramedidas
  - Herramientas de detección de ping (Scanlogd, Courtney, Ippl, Protolog)
  - Configuración adecuada de los routers de frontera (access lists)
  - Cortafuegos personales, herramientas de detección de rastreo (BlackICE, ZoneAlarm)
  - Desconectar servicios inútiles o peligrosos

Anatomía de un ataque. Enumeración



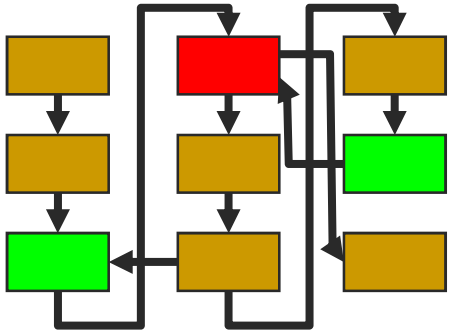
- Objetivo
  - Descubrir cuentas de usuario válidas y recursos compartidos mal protegidos
- Técnicas
  - Listados de cuentas (finger)
  - Listados de ficheros compartidos (showmount, enumeración NetBIOS)
  - Identificación de aplicaciones (banners, rpcinfo, rpcdump, etc.)
  - NT Resource Kit
- Contramedidas
  - Las del rastreo
  - Control del Software
  - Formación de los usuarios

Anatomía de un ataque. Acceso



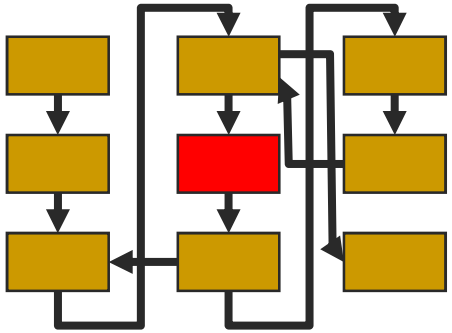
- Objetivo
  - Ya disponemos de información suficiente para intentar un acceso *documentado* al sistema
- Técnicas
  - Robo de passwords (eavesdroping) y crackeado de passwords (Crack, John the Ripper)
  - Forzado de recursos compartidos
  - Obtención del fichero de passwords
  - Troyanos y puertas traseras (BackOrifice, NetBus, SubSeven)
  - Ingeniería social

Anatomía de un ataque. Acceso



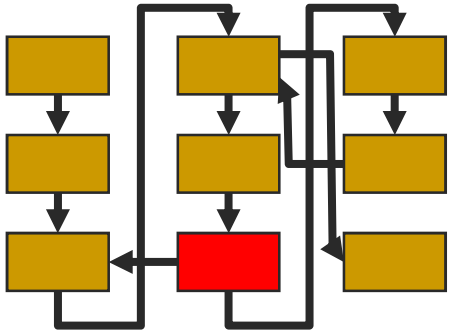
- Contramedidas
  - Control de las actualizaciones del software
  - Control en la instalación o ejecución de aplicaciones
  - Cortafuegos personales, detección de intrusiones
  - Educación de los usuarios (selección de buenas passwords)
  - Auditoría e históricos

Anatomía de un ataque. Obtención de privilegios



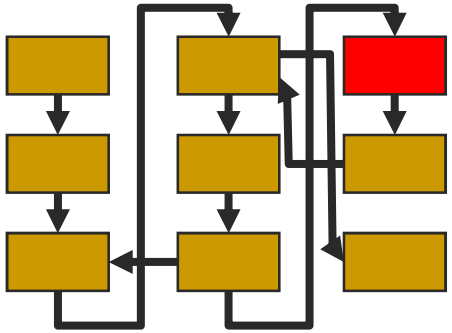
- Objetivo
  - Obtener permisos de administrador a partir de los permisos de usuario
- Técnicas
  - Vulnerabilidades conocidas
  - Desbordamiento de buffers, errores en el formato de cadenas, ataques de validación de entradas
  - Capturadores de teclado
  - Las del acceso
- Contramedidas
  - Las del acceso

Anatomía de un ataque. Pilfering



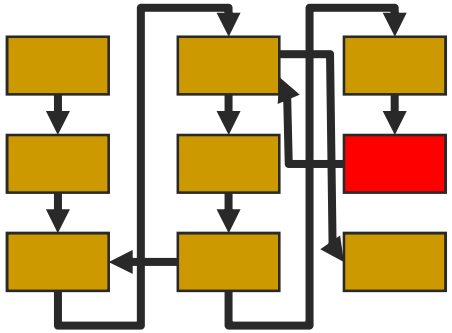
- Objetivo
  - Nueva búsqueda de información para atacar a otros sistemas de confianza
- Técnicas
  - Evaluación del nivel de confianza (rhosts, secretos LSA)
  - Búsqueda de passwords en claro (bases de datos, servicios Web)
- Contramedidas
  - Las del acceso
  - Herramientas de monitorización de red
  - Actuaciones en el nivel de arquitectura

Anatomía de un ataque. Borrando las huellas



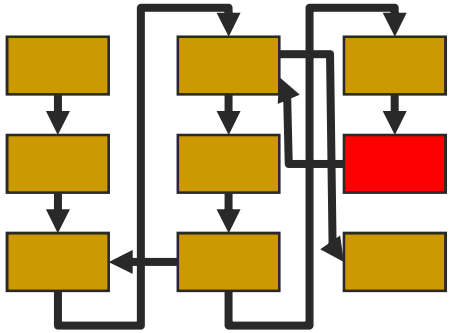
- Objetivo:
  - Una vez que se tiene el control total del sistema, ocultar el hecho al administrador legitimo del sistema
- Técnicas
  - Limpieza de logs
  - Ocultación de herramientas
  - Troyanos y puertas traseras
- Contramedidas
  - Gestión de históricos y monitorización, a nivel de red y a nivel de host.
  - Control del SW instalado

Anatomía de un ataque. Creación de puertas traseras



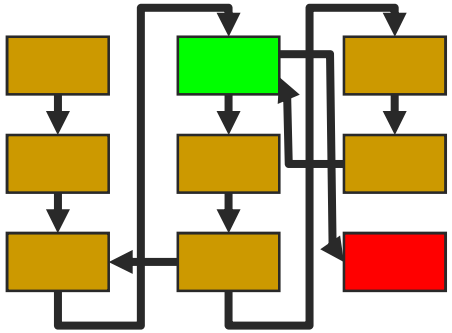
- Objetivo
  - Permiten a un intruso volver a entrar en un sistema sin ser detectado, de la manera más rápida y con el menor impacto posible
- Técnicas
  - Cuentas de usuario ficticias, robadas o inactivas
  - Trabajos batch
  - Ficheros de arranque infectados, librerías o núcleos modificados
  - Servicios de control remoto y caballos de Troya (Back Orifice)
  - Servicios de red inseguros (sendmail, rhosts, login, telnetd, cronjob)
  - Ocultación del tráfico de red y ocultación de procesos

Anatomía de un ataque. Creación de puertas traseras



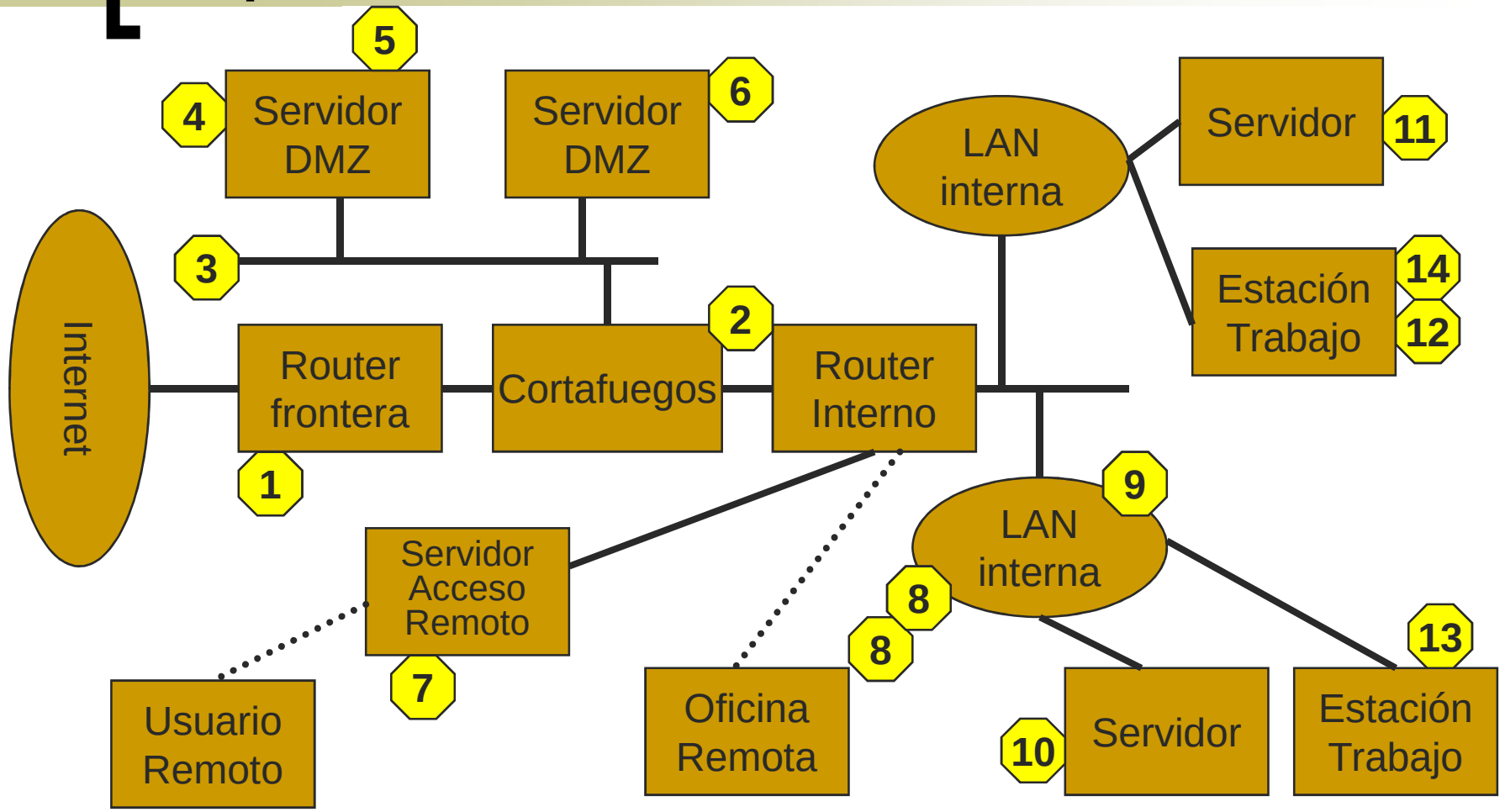
- Contramedidas
  - Básicamente, las del acceso (control riguroso del SW ejecutado, monitorización de los accesos, sobre todo a determinados puertos, cortafuegos personales, etc.)
  - Búsqueda de ficheros sospechosos (nombres por defecto de las puertas traseras).

Anatomía de un ataque. Denegación de servicio

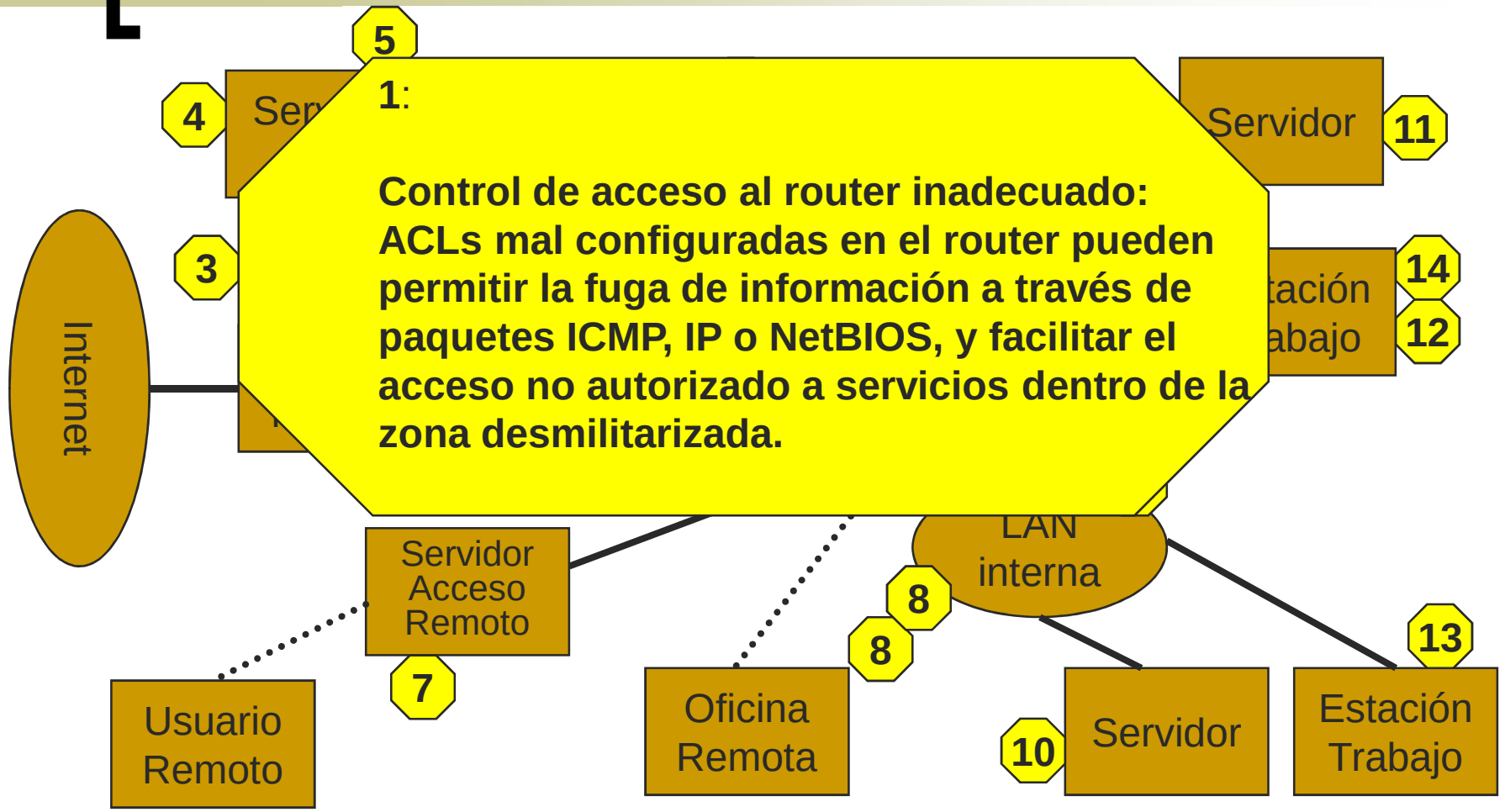


- Objetivo
  - Si no se consigue el acceso, el atacante puede intentar deshabilitar el objetivo
- Técnicas
  - Inundación de SYNs
  - Técnicas ICMP
  - Opciones TCP fuera de banda (OOB)
  - SYN Requests con fuente/destino idénticos
- Contramedidas
  - Configuración cuidadosa de los cortafuegos y routers.

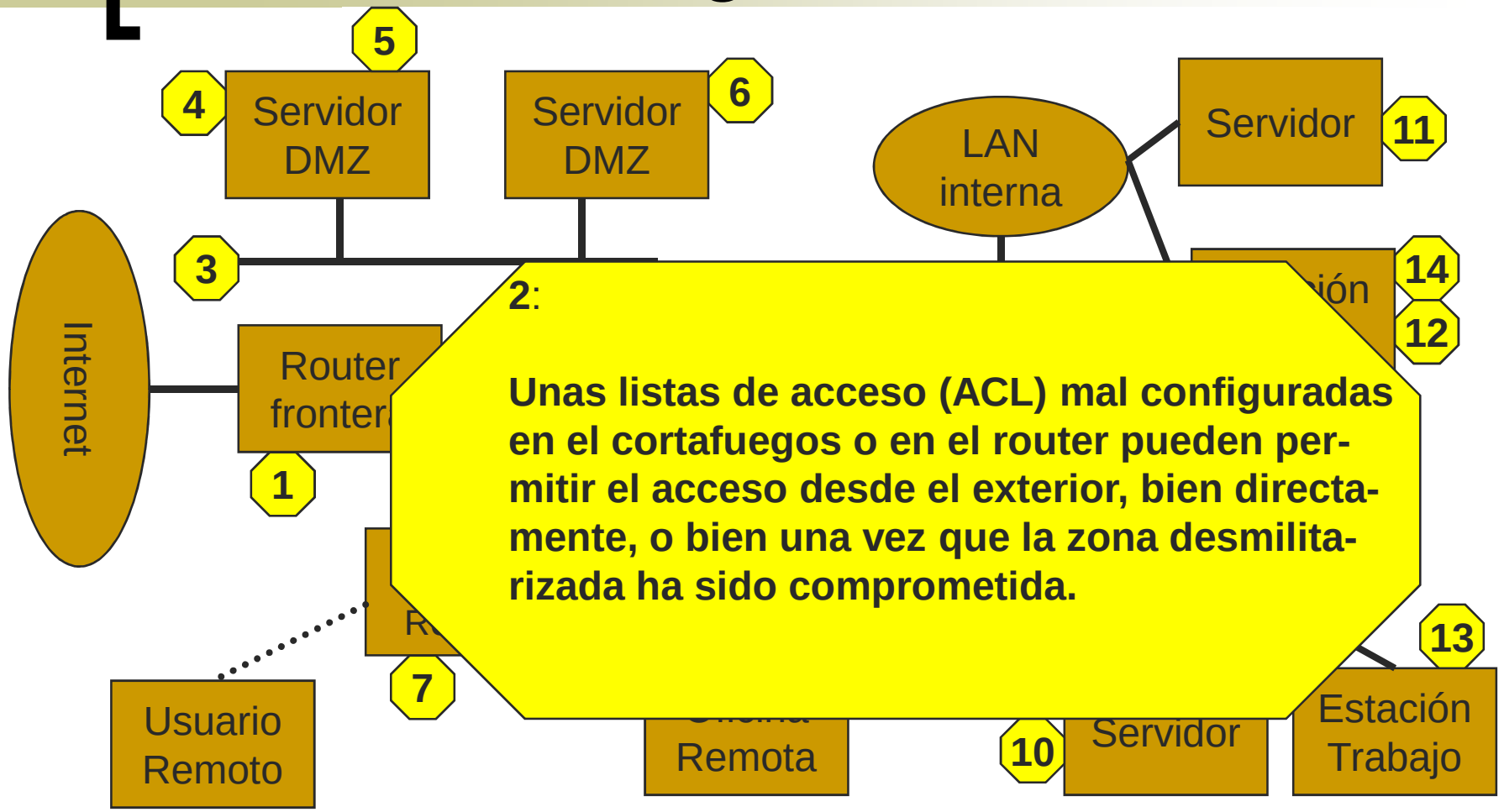
Las 14 vulnerabilidades más importantes



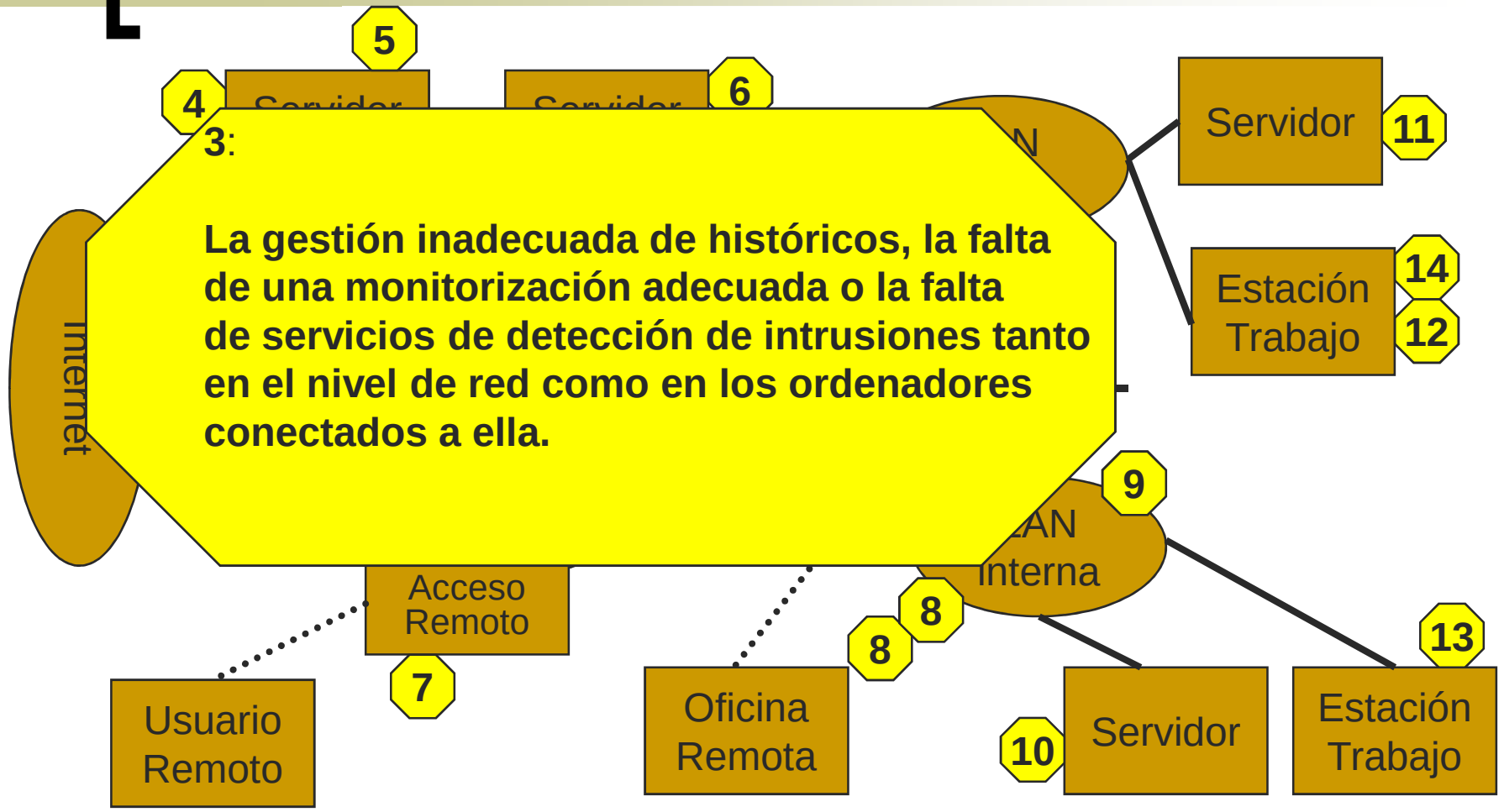
En el router frontera.



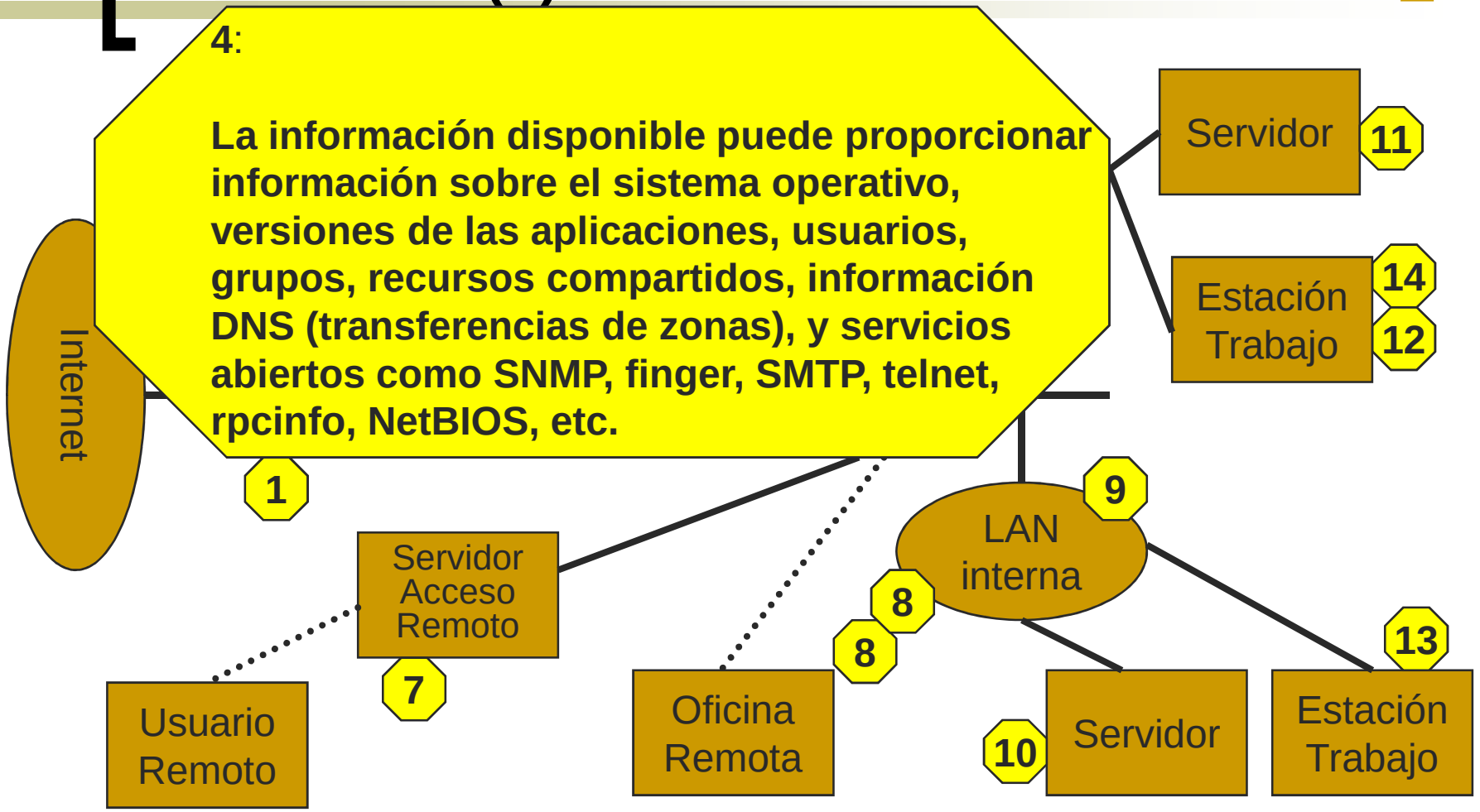
En el cortafuegos



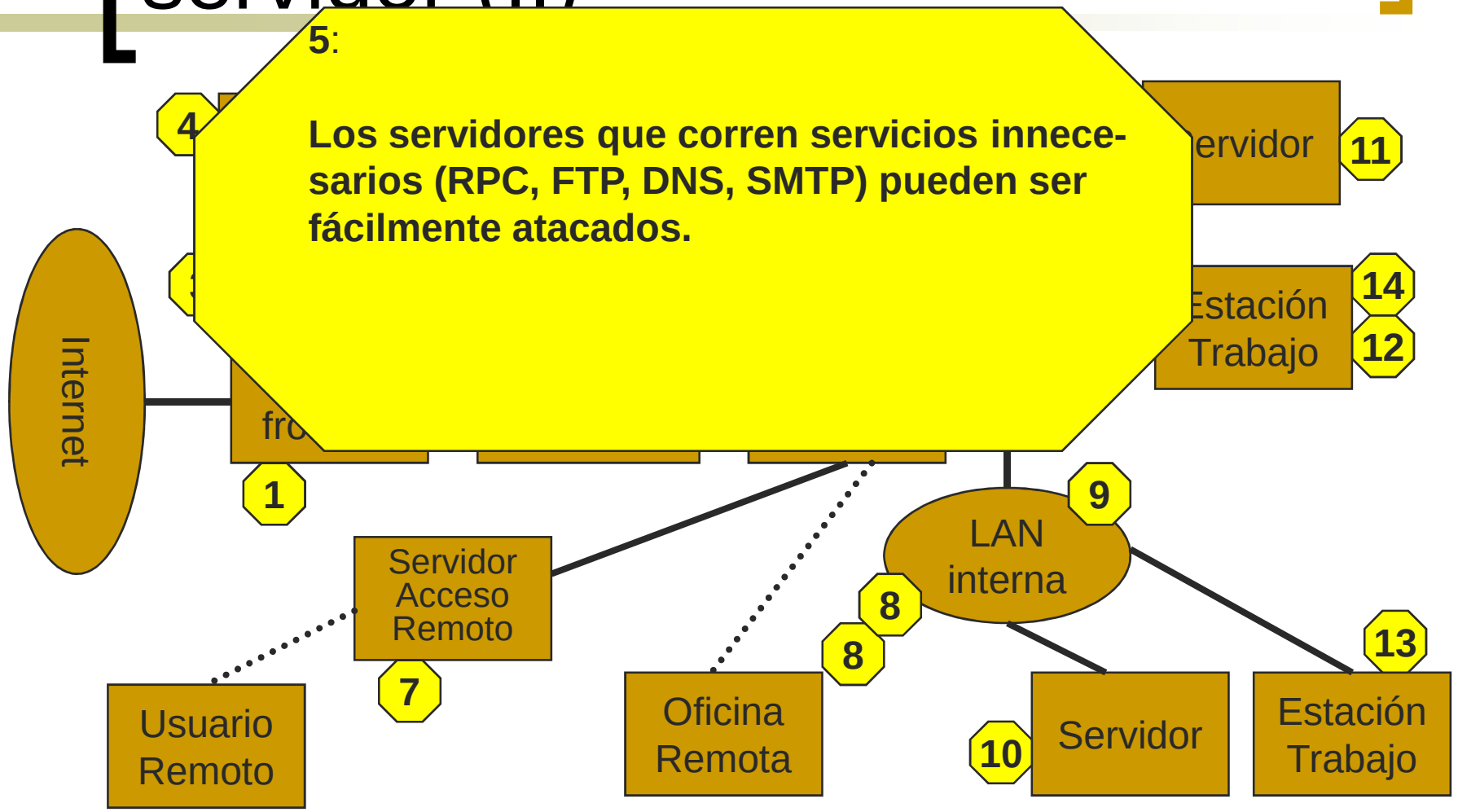
En la zona desmilitarizada



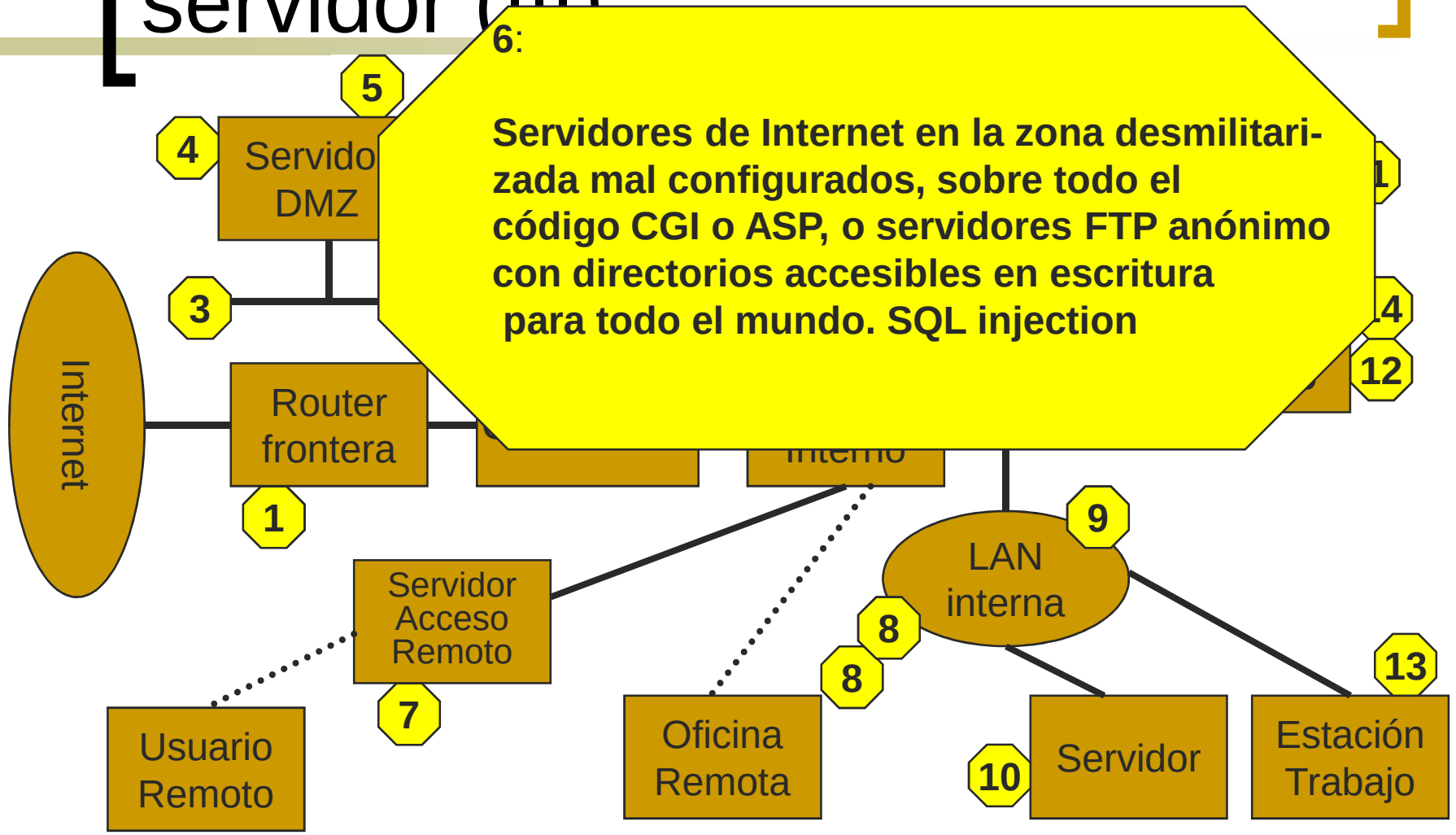
En la zona desmilitarizada: el servidor (I)



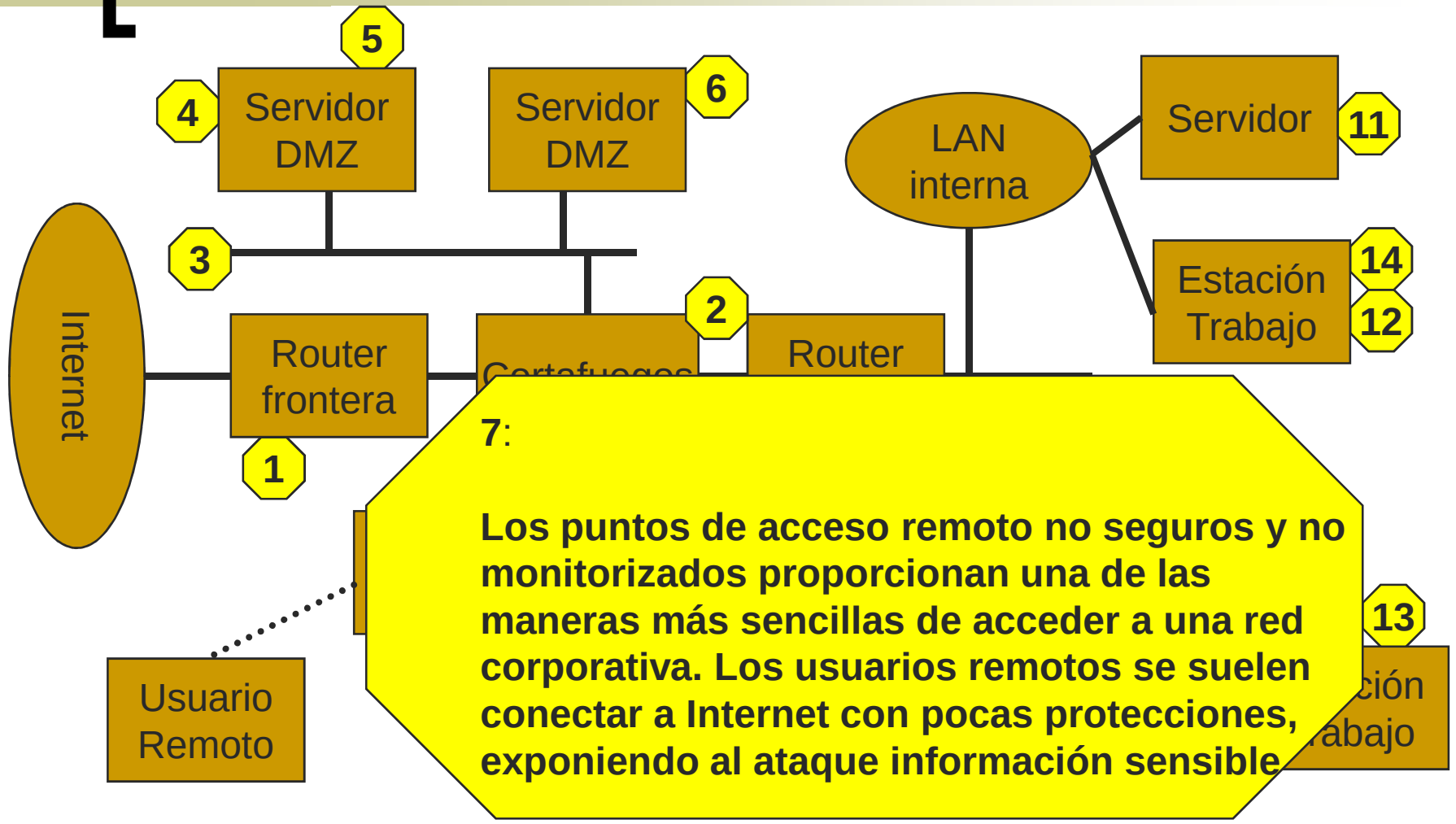
En la zona desmilitarizada: el servidor (II)



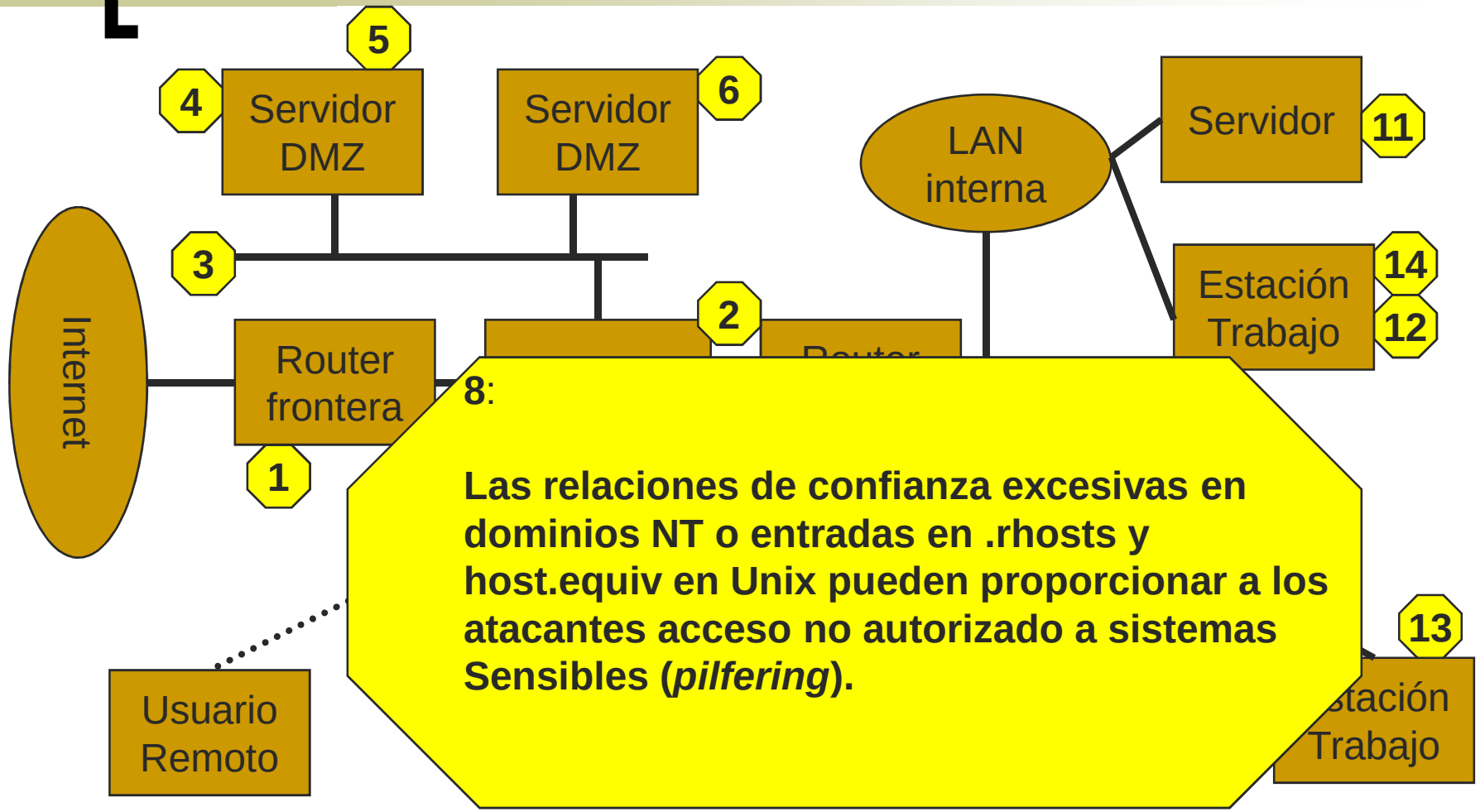
En la zona desmilitarizada: el servidor (III)



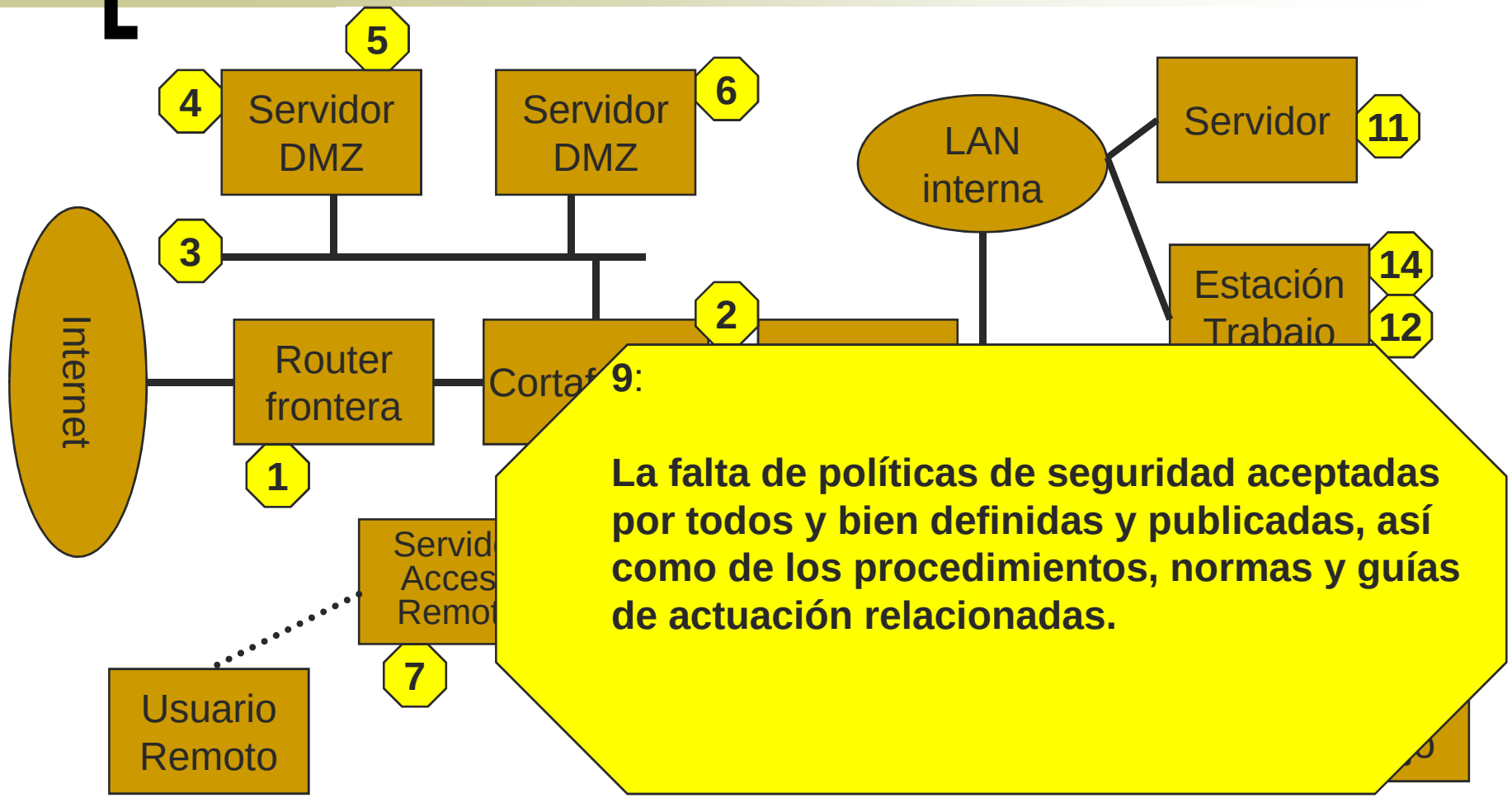
En el servidor de acceso remoto



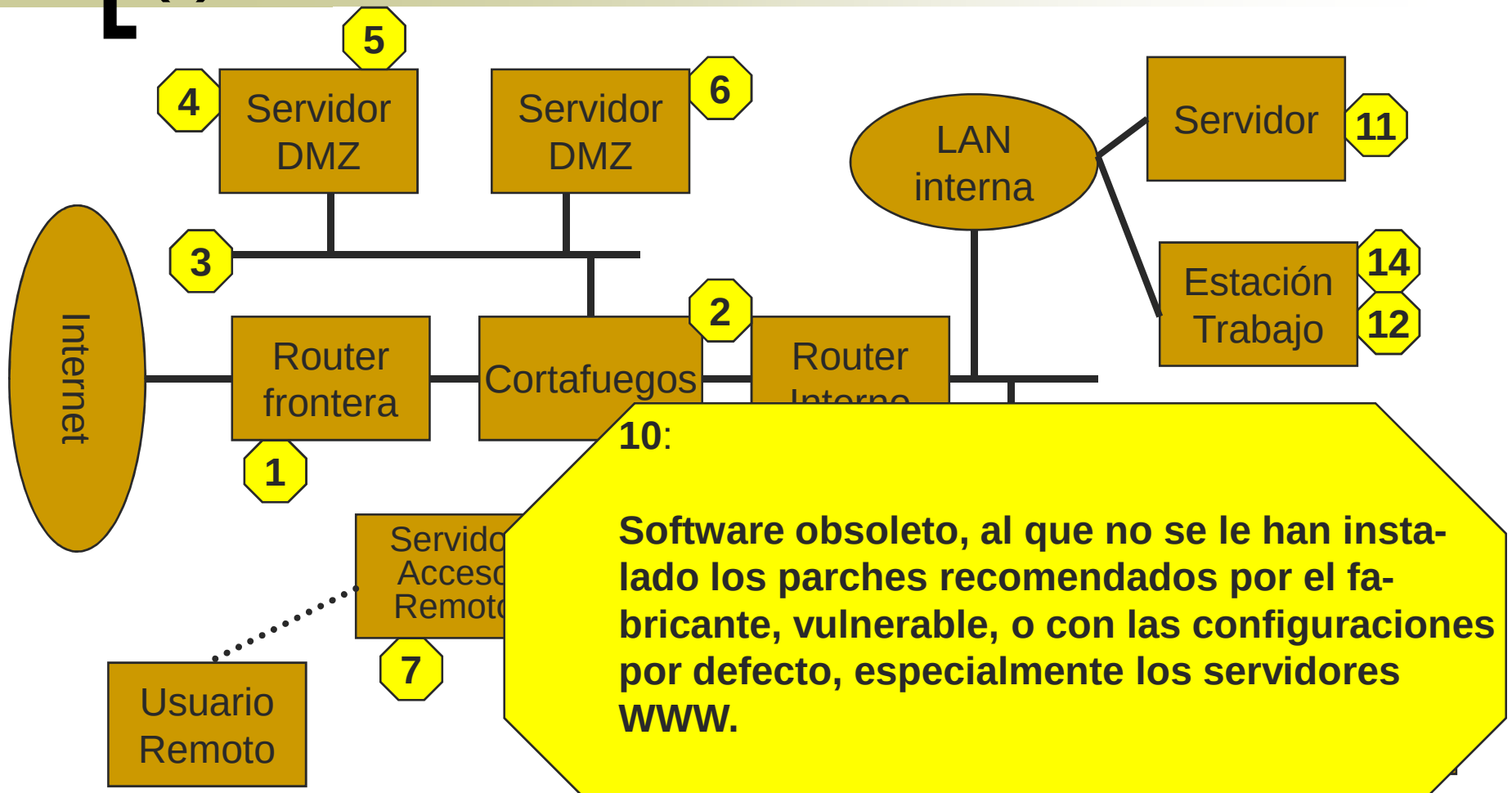
En una oficina remota o en la LAN interna



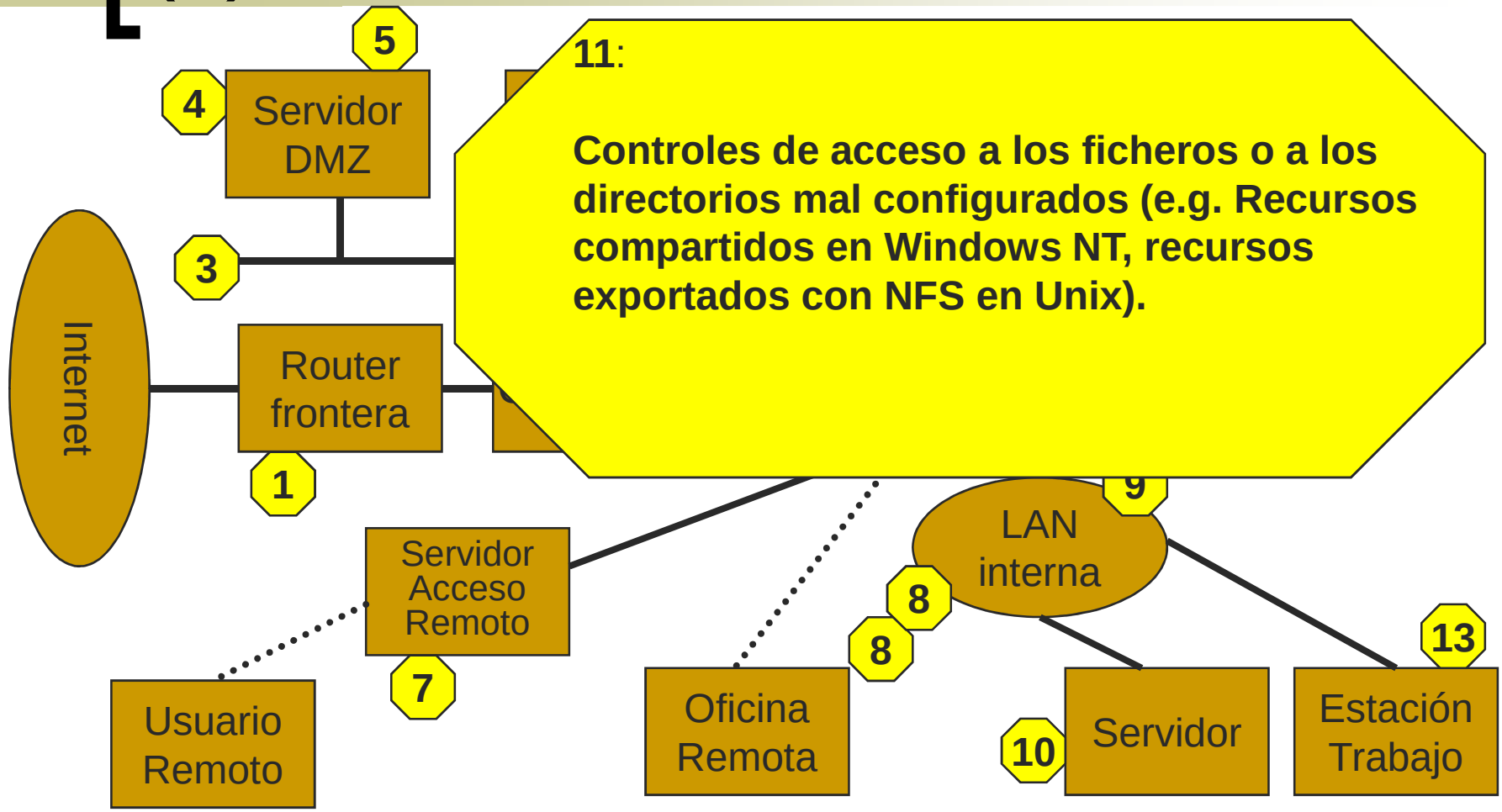
En la LAN interna



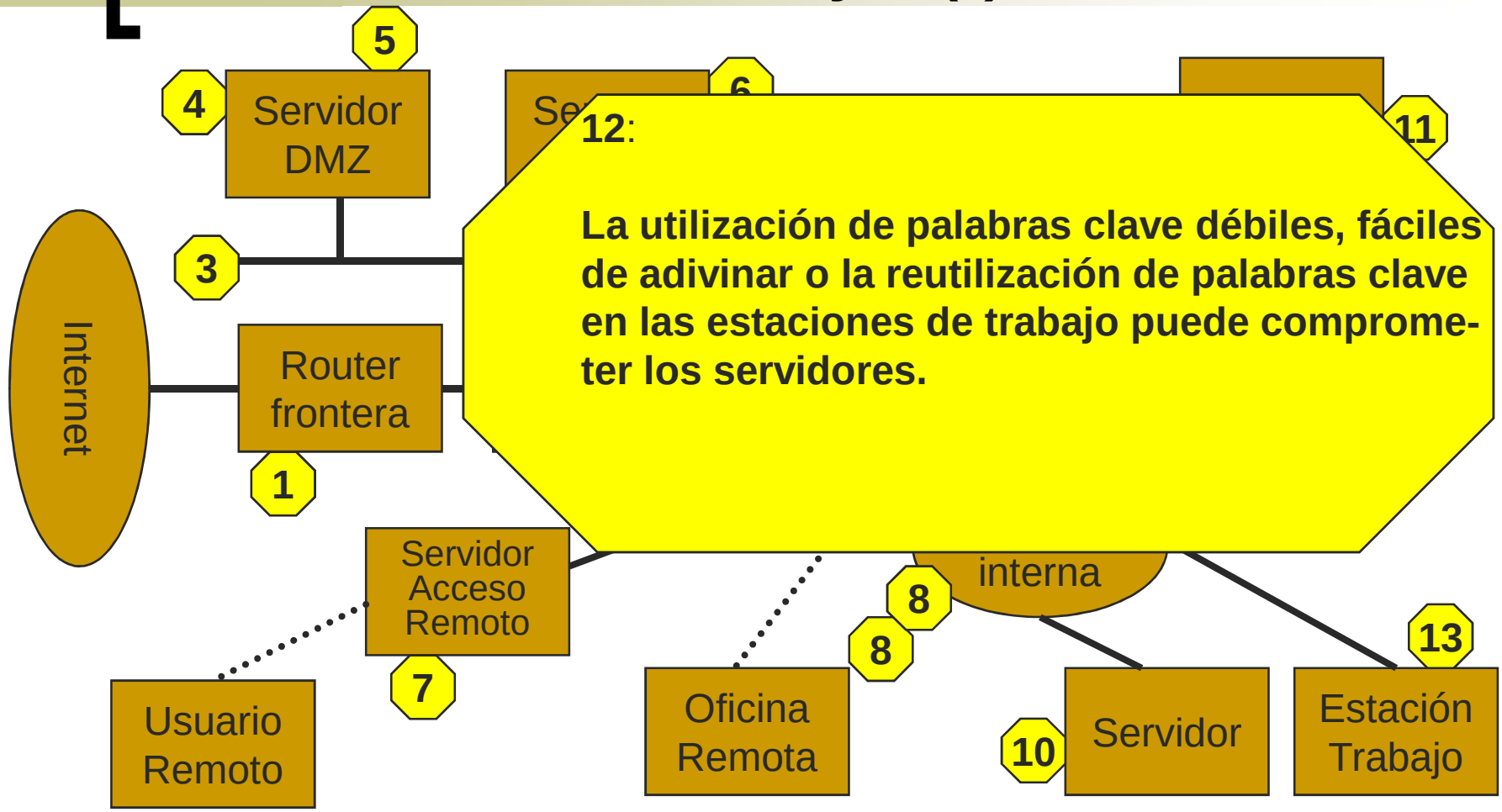
En la LAN interna: un servidor (I)



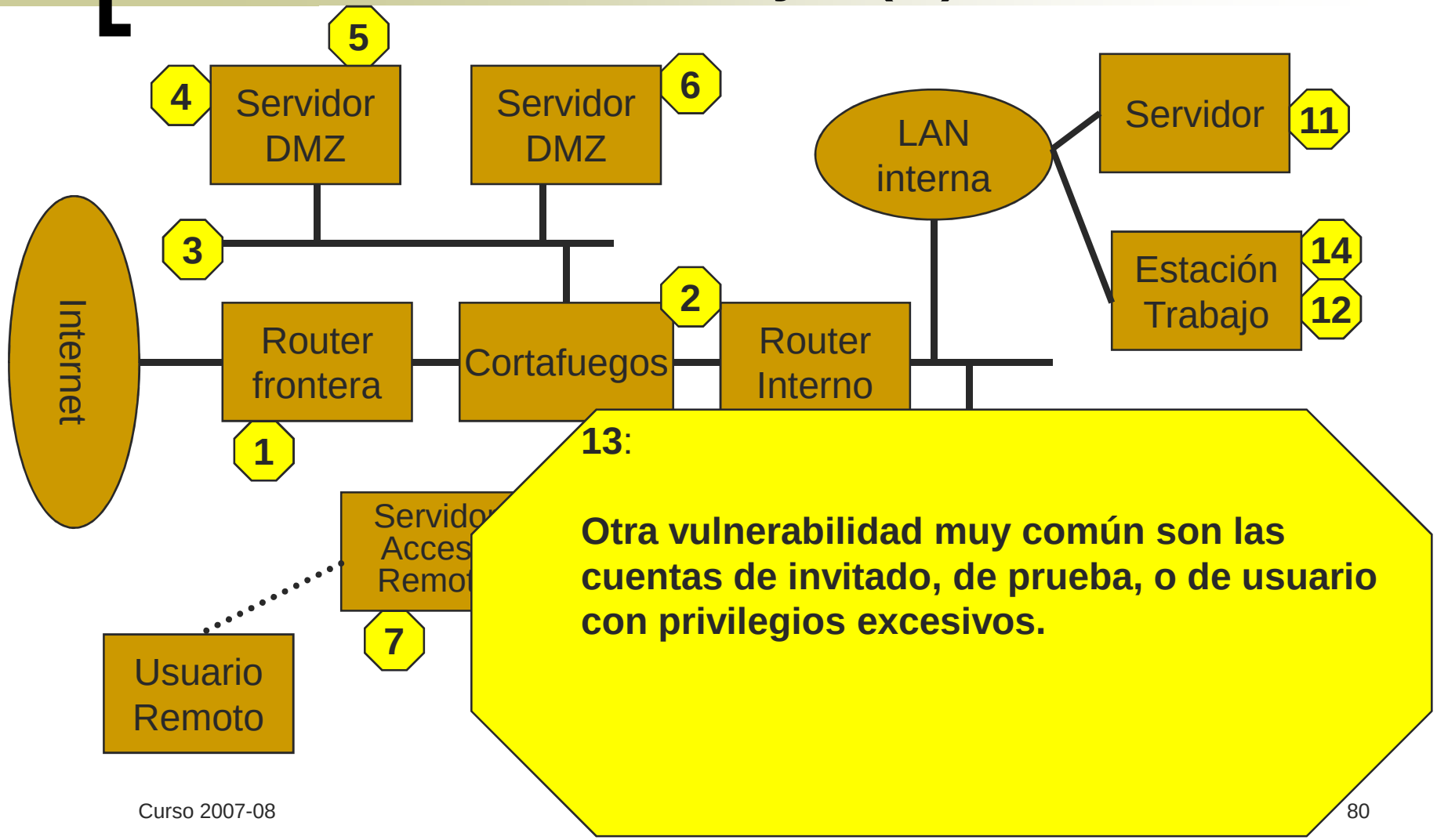
En la LAN interna: un servidor (II)



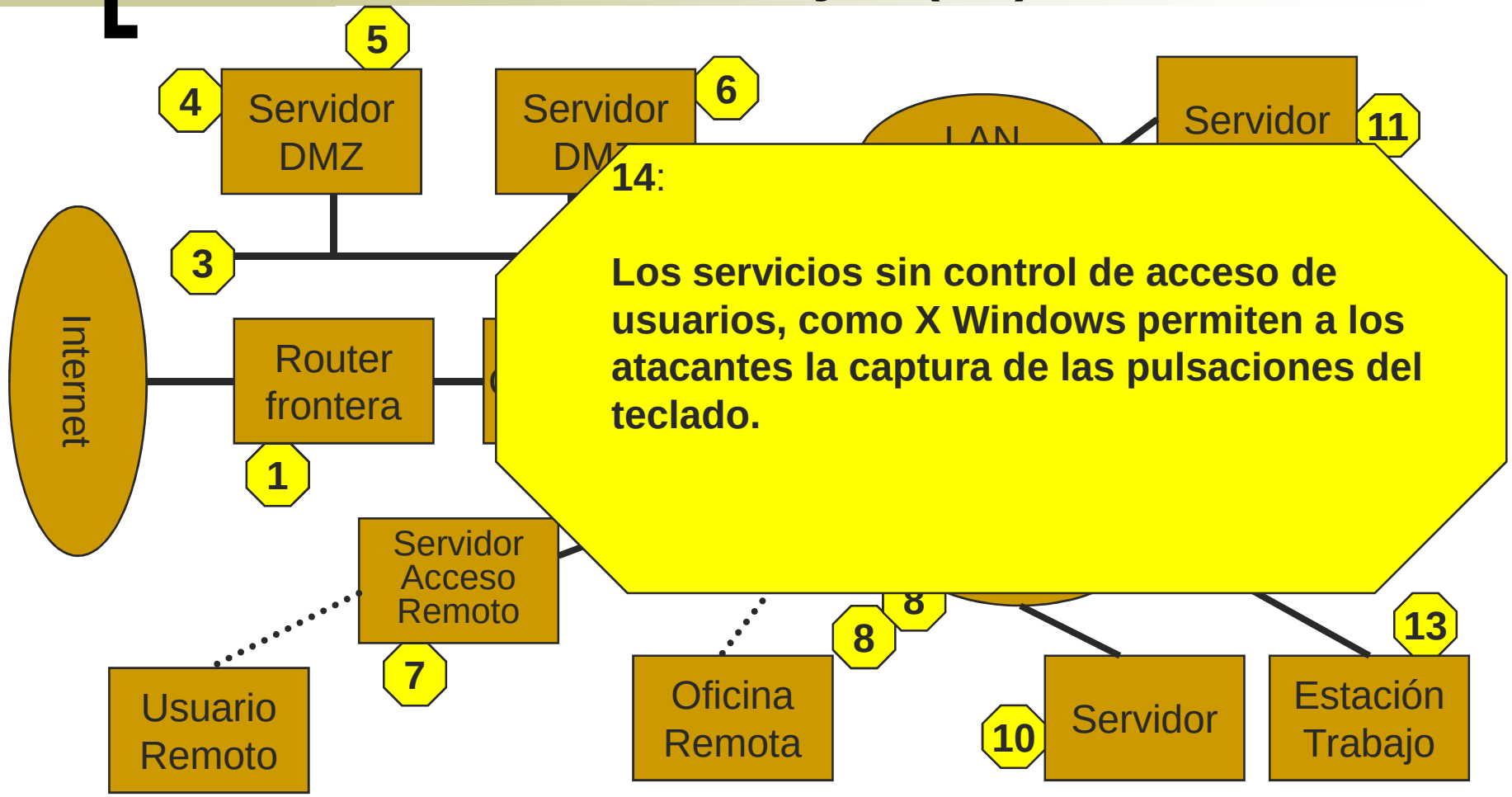
En la LAN interna: una estación de trabajo (I)



En la LAN interna: una estación de trabajo (II)



En la LAN interna: una estación de trabajo (III)



Política de Seguridad

- **Objetivo**
  - Definir cómo se va a proteger una organización ante los ataques. Tiene dos partes:
    - **Política general**: define el enfoque general:
      - Análisis de vulnerabilidad
      - Identificación de las amenazas
    - **Reglas específicas**: definen las características y acciones concretas, para cada servicio o sistema, orientadas a cumplir los objetivos de la política general

Política de Seguridad

- **Hitos de una buena política de seguridad.**
  - Para cada aspecto de la política:
    - Autoridad ¿Quién es el responsable?
    - Ámbito ¿A quién afecta?
    - Caducidad ¿Cuándo termina?
    - Especificidad ¿Qué se requiere?
    - Claridad ¿Es entendible por todos?

Política de Seguridad

- **Características de una buena política de seguridad (RFC 2196)**
  - Se tiene que poder poner en práctica mediante **procedimientos concretos** de administración de sistemas, mediante la publicación de guías sobre el uso aceptable de los recursos informáticos, o mediante otros métodos prácticos apropiados.
    - No debe ser una entelequia.
    - Debe ser **implementable**
  - Se debe obligar su cumplimiento mediante **herramientas de seguridad**, donde sea posible, y mediante **sanciones**, donde la prevención no sea posible técnicamente.
    - No debe tener agujeros, y si los tiene hay que poder detectarlos
  - Debe definir claramente las **áreas de responsabilidad** de los usuarios, los administradores y la dirección.
    - Tiene que haber **un responsable** para toda situación posible

Política de Seguridad

- **Componentes de una buena política de seguridad (RFC 2196)**
  - **Guía de compra de hardware y software**, donde se especifique las funciones relacionadas con la seguridad requeridas o deseadas.
  - Una **política de privacidad** que asegure un nivel mínimo de privacidad en cuanto a acceso a correo electrónico, ficheros de usuario, ficheros de traza, etc.
  - Una **política de acceso** que defina los niveles de seguridad, los derechos y privilegios, características de las conexiones a las redes internas y externas, mensajes de aviso y notificación, etc.
  - Una **política de responsabilidad** que defina las responsabilidades de los usuarios, y del personal técnico y de gestión. Debe definir los procedimientos de auditoría y de gestión de incidentes (a quién avisar, cuándo y cómo, etc.)
  - Una **política de autenticación** que establezca un esquema de claves o palabras de paso (*passwords*), que especifique modelos para la autenticación remota o el uso de dispositivos de autenticación.

Política de Seguridad

- **Componentes de una buena política de seguridad (RFC 2196), cont.**
  - Una **declaración de disponibilidad**, que aclare las expectativas de los usuarios en cuanto a la disponibilidad de los recursos. Debe definir temas como la redundancia, la recuperación ante intrusiones, información de contacto para comunicar fallos en los sistemas y/o en la red, etc.
  - Una **política de mantenimiento** que describa cómo se lleva a cabo el mantenimiento interno y externo, si se permite mantenimiento remoto y/o mantenimiento por contratas externas, etc.
  - Una **política de comunicación de violaciones** que defina qué tipos de amenazas, y cómo y a quién se deben comunicar.
  - **Información de apoyo** que indique a los usuarios, personal técnico y administración cómo actuar ante cualquier eventualidad, cómo discutir con elementos externos los incidentes de seguridad, qué tipo de información se considera confidencial o interna, referencias a otros procedimientos de seguridad, referencias a legislación de la compañía y externa, etc.

Aspectos legales

- Leyes españolas
  - Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal
  - Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y Comercio Electrónico
  - Real Decreto-Ley 14/1999, de 17 de septiembre, de Firma Electrónica
- Normas Internacionales
  - Norma ISO 17799 Information technology -- Code of practice for information security management (actualizada por la ISO 27001)
    - Política de seguridad, asignación de responsabilidades, educación y capacitación en seguridad, comunicación de incidencias, aspectos de la gestión de continuidad de negocio, protección de datos de carácter personal y de la intimidad, salvaguarda de los registros de una organización, derechos de propiedad intelectual

Seguridad en Internet

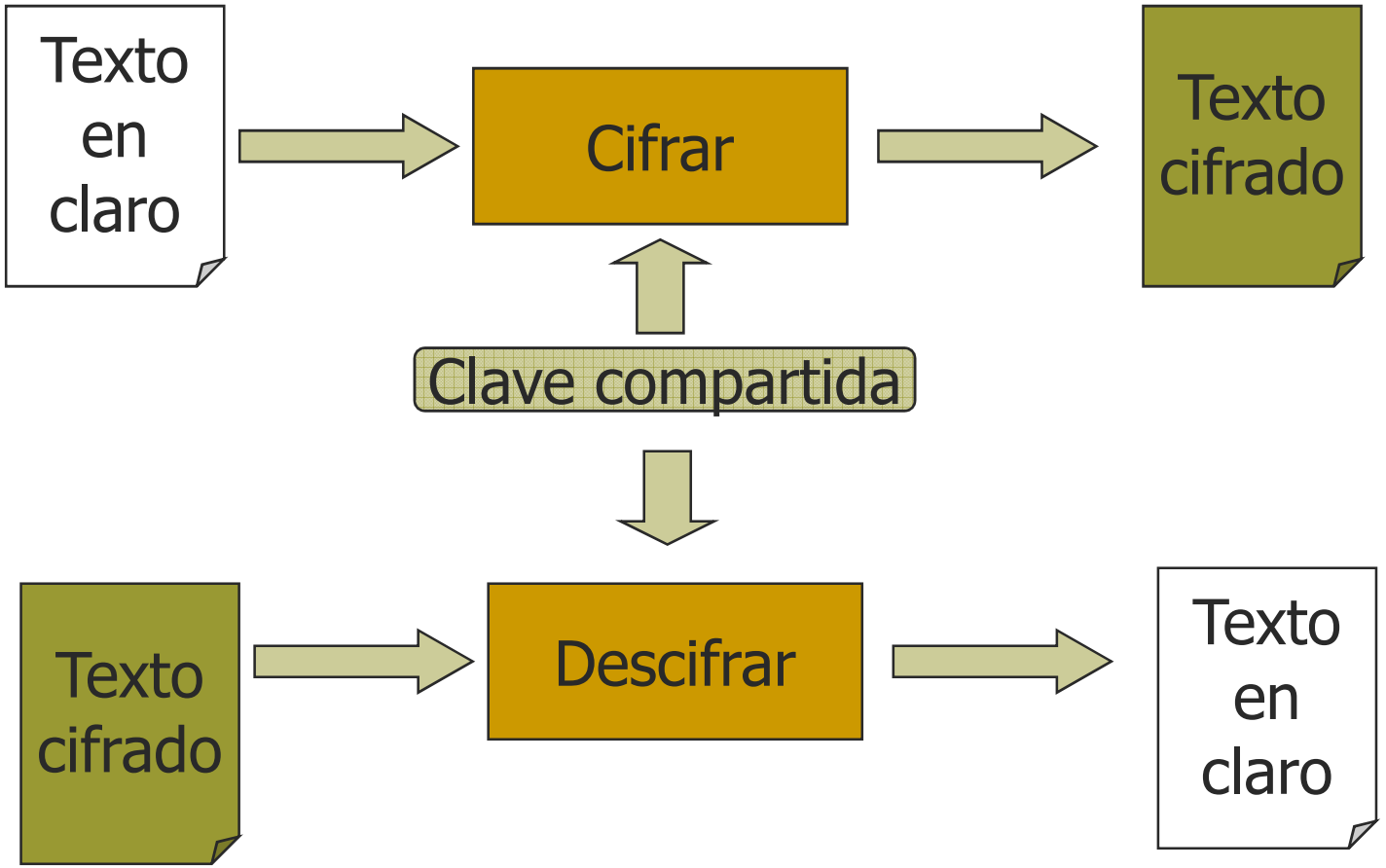
2. Introducción a la criptografía

Principios de criptografía

- Criptografía simétrica o de clave secreta (SKC)
- Criptografía asimétrica o de clave publica (PKC)
- Funciones de hash

Si mucha gente muy inteligente no ha conseguido resolver un problema todavía, muy probablemente ese problema no se resolverá en un futuro próximo

Criptografía de clave secreta



Criptografía de clave secreta

- Aplicaciones
  - Transmisión segura en canales no seguros
  - Almacenamiento seguro en medios no seguros
  - Autentificación
    - Autentificación fuerte basada en desafíos
    - Control de integridad (MIC, MAC)

Criptografía de clave secreta

- Cifrado simétrico
  - Cifrar(Texto, Clave) = Texto cifrado
  - Descifrar(Texto cifrado, Clave) = Texto
  - Usualmente, claves de 40 a 128 bits
  - Se basa en permutaciones y traducciones basadas en tablas (*table lookup*)
- Hashing (Message Integrity Check)
  - MIC = Cifrar(Hash(Texto), Clave)

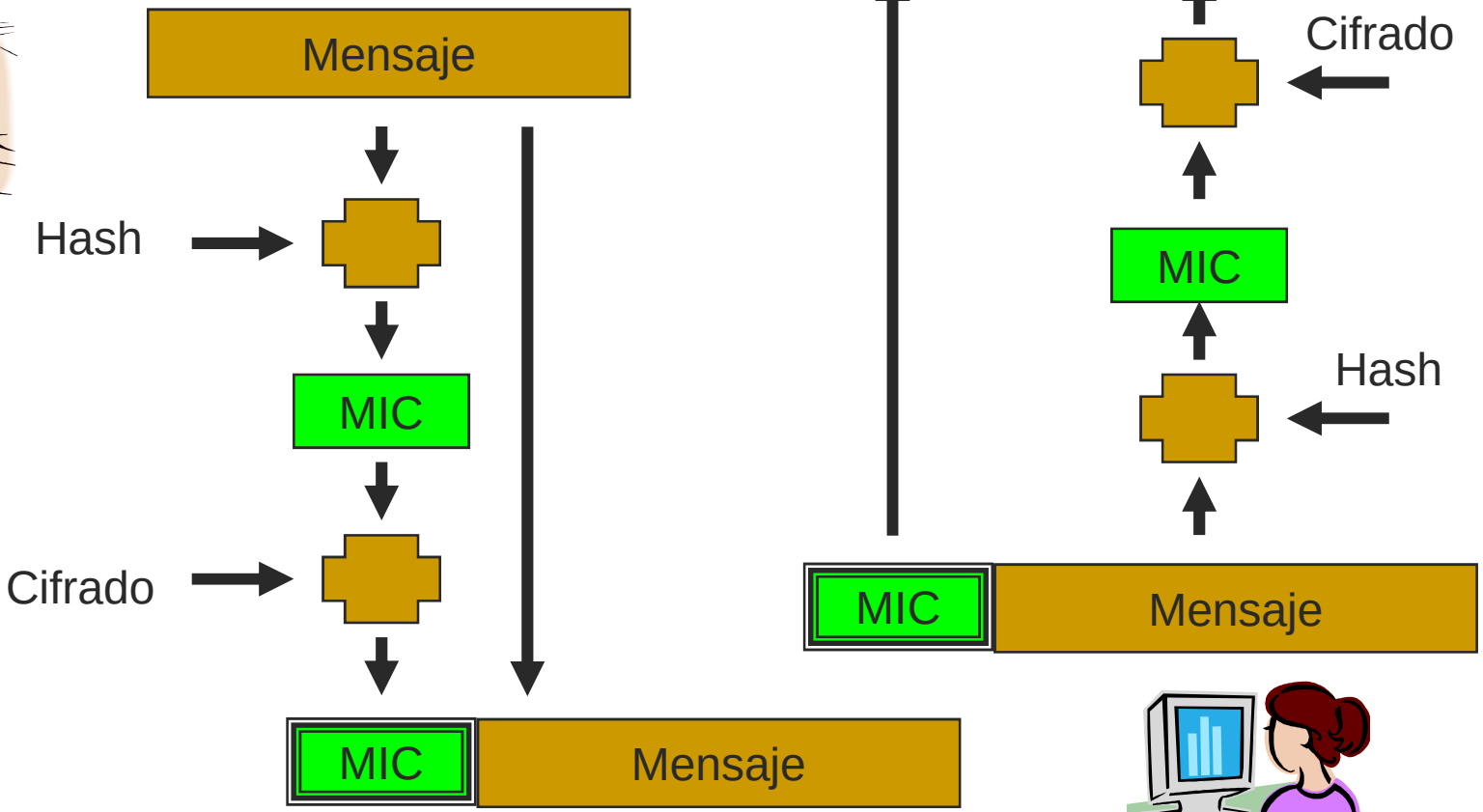
Criptografía de clave secreta

- Estándares de SKC
  - **DES**: Data Encryption Standard.
    - Claves de 64 (56) bits para cifrar bloques de 64 bits.
  - **IDEA**: International Data Encryption Algorithm
    - Claves de 128 bits para cifrar bloques de 64 bits.
  - **AES**: Advanced Encryption Standard
    - Claves de tamaño variable (128..256) y bloques de tamaño variable (128..256).

Funciones de hash

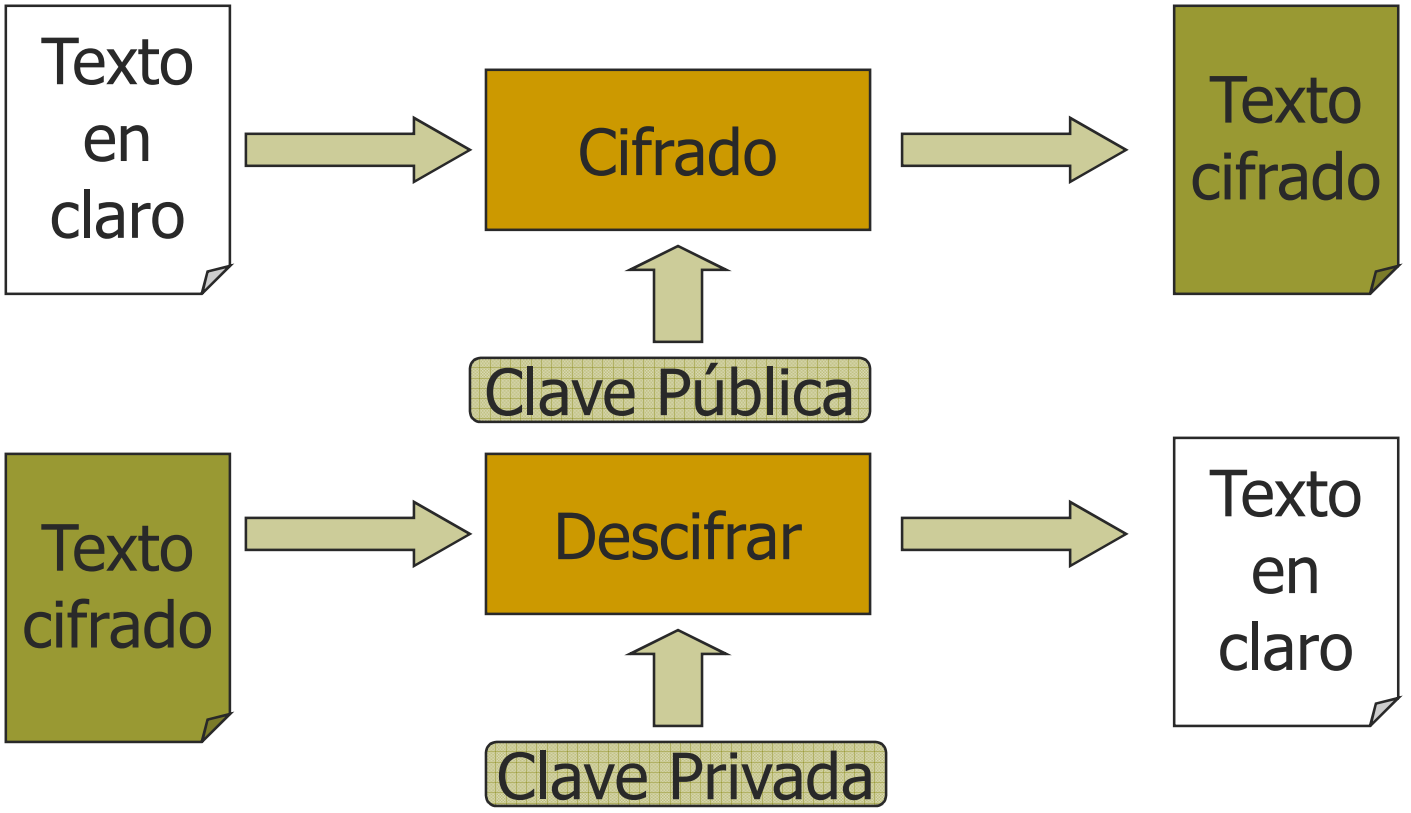
- Son funciones muchos a uno (*many to one*)
- Se utilizan para control de integridad y en firmas electrónicas
- Ejemplos
  - Checksums, cyclic-redundancy check, message digests
- Propiedades
  - Dado un MIC *y* , no es computacionalmente factible elaborar un mensaje *x* tal que *Hash(x) = y*.
  - No es computacionalmente factible encontrar dos mensajes cualesquiera *x* e *y* tales que *Hash(x) = Hash(y)*
- Algoritmos: MD2, MD4, MD5, SHA-1

Funciones de hash



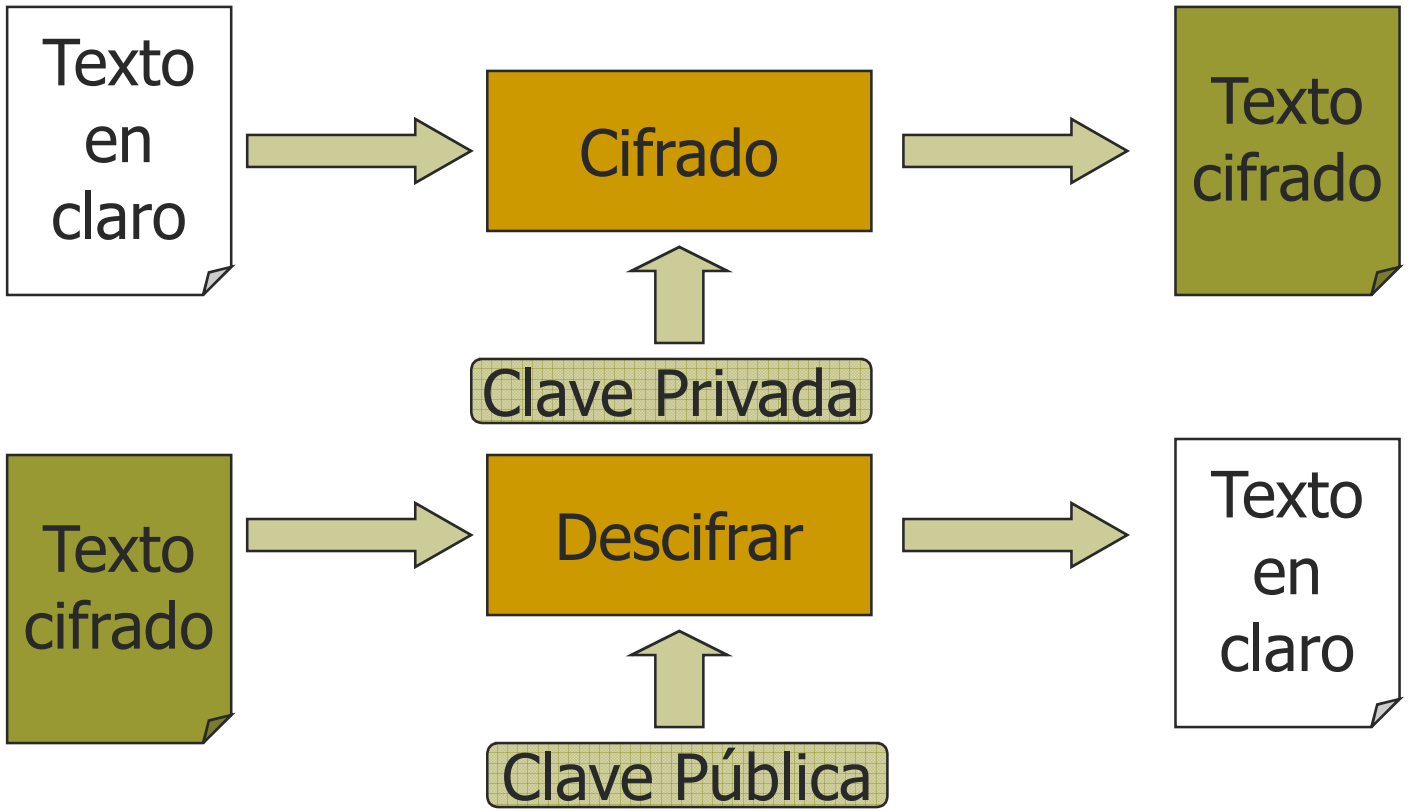
Criptografía de clave pública

- Propiedad I



Criptografía de clave pública

- Propiedad II



Criptografía de clave pública

- Funcionamiento de la PKC
  - Propiedad general I:
    - Cifrar(Texto, CPublica) = Texto cifrado
    - Descifrar(Texto cifrado, CPrivada) = Texto
  - Propiedad general II:
    - Cifrar(Texto, CPrivada) = Texto cifrado
    - Descifrar(Texto cifrado, CPública) = Texto
  - Se basan en la complejidad computacional de determinadas operaciones matemáticas (factorización, extracción del logaritmos, curvas elípticas, etc.)

Criptografía de clave pública

- Algunos estándares de PKC
  - **RSA** (Rivest, Shamir and Adleman)
    - Claves de tamaño variable. La más común es 1024 bits
    - Bloques de tamaño variable, menores que el tamaño de la clave
    - Basado en el problema de factorización de números grandes.
  - **Diffie-Hellman**
    - No soporta cifrado ni firmas digitales. Se utiliza para acordar claves de sesión (generar un secreto compartido).
    - Basado en el cálculo de logaritmos discretos.
  - **Criptografía de curva elíptica**

Criptografía de clave pública

- Funcionamiento de la PKC
  - Consecuencia de la propiedad I
    - Privacidad: Cifrado con la clave pública del receptor, quien puede descifrar el mensaje con su clave privada.
    - Integridad: Generación de un código MIC a partir del mensaje, que se envía cifrado junto al mensaje
  - Consecuencia de la propiedad II
    - Autentificación: Cifrado de un extracto del mensaje con la clave privada del remitente (firma digital). El receptor puede comprobar la identidad del remitente descifrando el (extracto del) mensaje con la clave pública de éste

Firmas digitales

Manolo

Mensaje

Hash

MIC

Cifrado con clave privada de Manolo

Firma

Mensaje

MIC ? = MIC

Descifrar con clave Pública de Manolo

Firma

MIC

Hash

Firma

Mensaje

María

Certificados Digitales

- Nacen con dos objetivos:
  - Resolver el problema de la administración de claves públicas.
  - Evitar que la identidad de su dueño pueda ser falsificada.
- La idea es que una tercera persona intervenga en la administración de las claves públicas.

Certificados Digitales

- Las tres partes más importantes de un certificado digital son:
  - Una clave pública
  - La identidad del implicado: nombre y datos generales.
  - La firma privada de una tercera entidad llamada “autoridad certificadora” que todos reconocen como tal y que valida la asociación clave pública/identidad.

Certificados Digitales

- ¿Quién da validez a los certificados?
  - Autoridades de certificación (notarios electrónicos)
  - Los certificados emitidos por éstas entidades están firmados con sus claves privadas
  - Se crea una cadena de entidades certificadoras, desde una entidad raíz hasta el certificado final

Criptografía de clave pública

- Entidades certificadoras raíz
  - Fábrica Nacional de Moneda y Timbre: www.fnmt.es
  - VeriSign: www.verisign.com
  - EUnet International: www.eunet.com
  - Microsoft: www.microsoft.com
  - Agencia de Certificación Electrónica: www.ace.es
  - Global Trust Authority: www.gta.multicert.org
  - ...