Sistemas Informáticos II

Tema 4: Aspectos operacionales de los Sistemas Distribuidos: Seguridad

Antonio E. Martínez
Daniel Hernández Lobato (daniel.hernandez@uam.es)
Alvaro Ortigosa (alvaro.ortigosa@uam.es)
Manuel Sánchez-Montañés (manuel.smontanes@uam.es)

Contenido

- Introducción.
- Técnicas criptográficas básicas de protección de la información.
  - Cifrado.
  - Resúmenes.
  - Firma digital.
  - Criptoanálisis.
- Sistemas de gestión de la seguridad en la información.
- Sistemas de seguridad de red.
  - Autenticación.
  - Protocolos.
  - Cortafuegos.
  - Sistemas de detección de intrusiones.
- Seguridad en los equipos HW y SW. *Common Criteria.*
- Bibliografía especial del tema.

Introducción

- Las amenazas en el *mundo digital* son una imagen de las amenazas en el *mundo real*. Los delincuentes roban donde está el dinero, sea en los bancos o en la red.
- Sin embargo, el *ciberespacio* introduce tres nuevas características a estas amenazas que, combinadas, las hacen aún más peligrosas:
  - Automatización.
    - Ataques de bajo beneficio individual pueden hacerse rentables.
    - Es fácil recoger o sustraer información de diversas fuentes y explotarla para abusar de ella.
  - Acción a distancia. Facilita el ataque y dificulta la persecución del criminal.
  - Propagación y reutilización de las técnicas. Basta con un experto para generar una herramienta que puede ser utilizada por cualquier delincuente en cualquier parte del mundo.
- El delincuente es el primero que se aprovecha de las tecnologías

Los ataques en el mundo digital

- Ataques que buscan obtener un beneficio. Ataques criminales.
  - Fraude.
  - Timos.
  - Ataques destructivos.
  - Robo de propiedad intelectual.
  - Usurpación de la identidad.
  - Usurpación de marca.
- Ataques que buscan obtener publicidad. Pueden ser o no delito, dependiendo del hecho.
  - Intrusiones, *spoofing*, virus, gusanos…
  - Denegación de servicio.
- Violaciones de privacidad. Pueden ser o no delito, dependiendo del país.
  - Ataques dirigidos.
  - Recolección de datos *(data harvesting)*.
  - Vigilancia.
  - Bases de datos personales.
  - Análisis de tráfico (aunque no se revele el contenido).
  - Vigilancia electrónica masiva (ECHELON)
- Ataques legales. Uso del sistema legal y sus debilidades, reales o posibles.

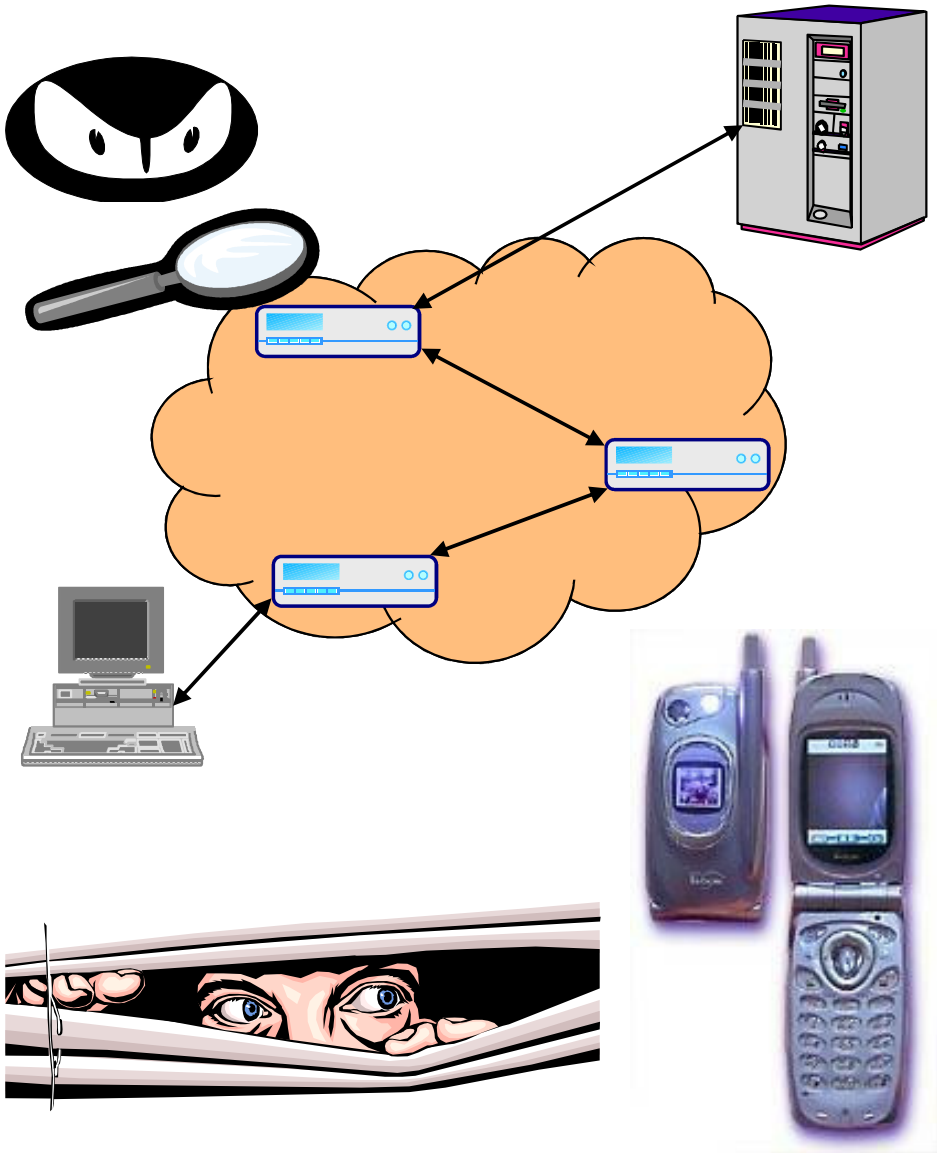
Los adversarios en el mundo digital

- Son también similares a los del *mundo real*. Es importante conocer sus características para evaluar el nivel de amenaza que representan.
  - Pueden perseguir distintos objetivos: beneficio, información, publicidad, diversión…
  - Pueden tener diferentes niveles de acceso a los sistemas.
  - Pueden asumir diferentes niveles de riesgo.
  - Pueden tener distintos niveles de conocimiento y experiencia.
  - Pueden tener distintos niveles de recursos.
- Tipos concretos:
  - *Hackers* maliciosos *(Crackers)*
  - *Pseudo-hackers (lamers, script kiddies).*
  - Criminales solitarios.
  - Personal interno (empleados, subcontratados…) maliciosos.
  - Espías industriales.
  - Crimen organizado.
  - Terroristas.
  - Atacantes *legales:* Prensa, policía, agencias de inteligencia nacionales.
  - *Infowarriors*.

Necesario cambio cultural: El atacante informático no es un genio, es un criminal.

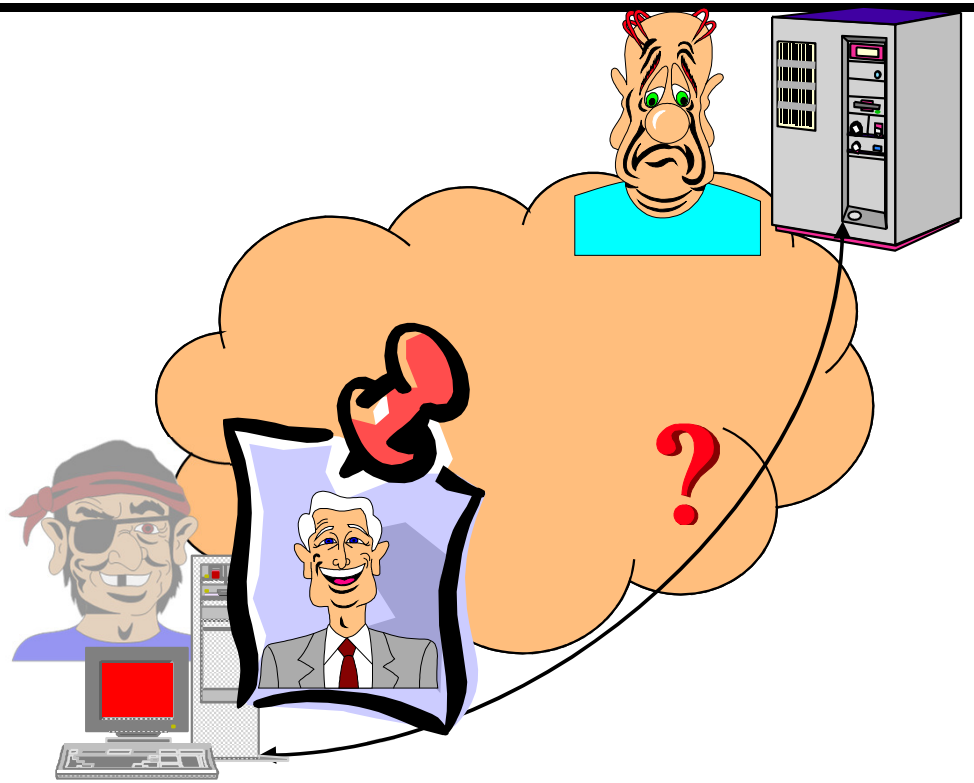
Los métodos básicos de ataque

- Vigilancia *(sniffing)*
  - Es un ataque pasivo. El atacante no afecta a los recursos del sistema.
  - A través de la línea de comunicaciones o por otros métodos.
  - Base para realizar ataques posteriores de otro tipo.
  - Puede obtener directamente información.
  - Puede realizar análisis de tráfico o correlacionar información adquirida para obtener información adicional



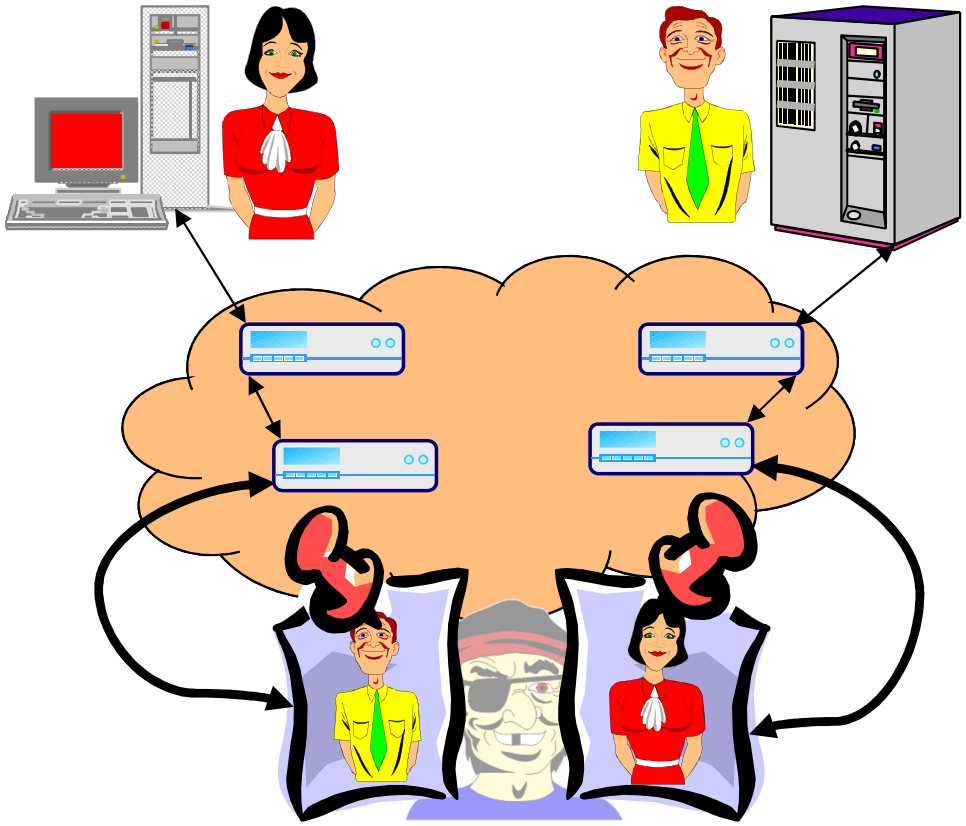
Los métodos básicos de ataque

- Suplantación *(spoofing)*
  - Es un ataque activo.
  - Una de las entidades que interactúan finge ser quien no es.
    - Suplantación de *cliente.*
    - Suplantación de *servidor.*
  - A través de red o por otros métodos.



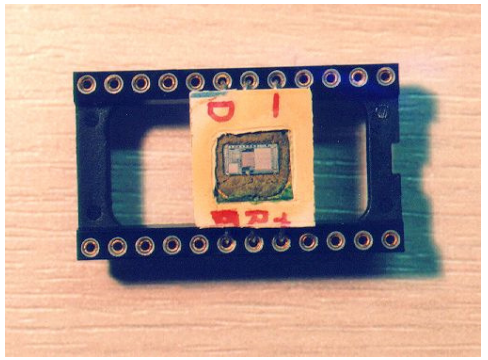
Los métodos básicos de ataque

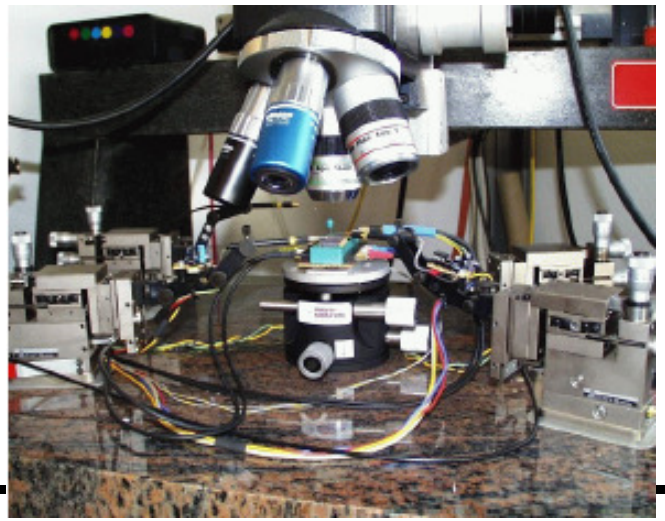
- *Man-in-the-middle*.
  - Suplantación doble.
    - El atacante finge ser el recíproco para cada uno de los extremos de una comunicación.
  - Realizada en el transcurso de una comunicación establecida. *(connection hijacking)*.



Los métodos básicos de ataque

- Defectos en los componentes
  - Defectos de hardware.
    - Forzado *(tampering).*
    - Canal adyacente *(EMR, timing attacks…).*
  - Defectos en el software *(bugs)*.
    - Fallos que permiten conseguir accesos privilegiados.
    - Fallos que vuelven inoperativo el sistema.
    - *Buffer Overflow*.
    - Comportamiento en altas cargas de trabajo.
  - *Malware: Trampillas (trap doors), puertas traseras (back doors),* caballos de Troya…





Los métodos básicos de ataque

- El factor humano. Ataques que aprovechan la intervención humana en todos los sistemas.
  - Dificultad de reacción ante situaciones poco frecuentes.
  - Ignorar falsas alarmas que se disparan frecuentemente.
  - Relajación en el seguimiento de las normas de seguridad por la molestia o carga añadida de trabajo que suponen.
  - Intervención humana maliciosa, frecuentemente desde *dentro*.
  - *Ingeniería social*. Persuadir a otros de que hagan lo que se les pide (normalmente como ayuda), aunque salte normas.
    - Revelación de procedimientos, métodos de acceso, contraseñas…
    - Propagación de virus, cartas encadenadas…

Las necesidades básicas de seguridad en las TIC

Establecidas en el estándar ISO 10181.

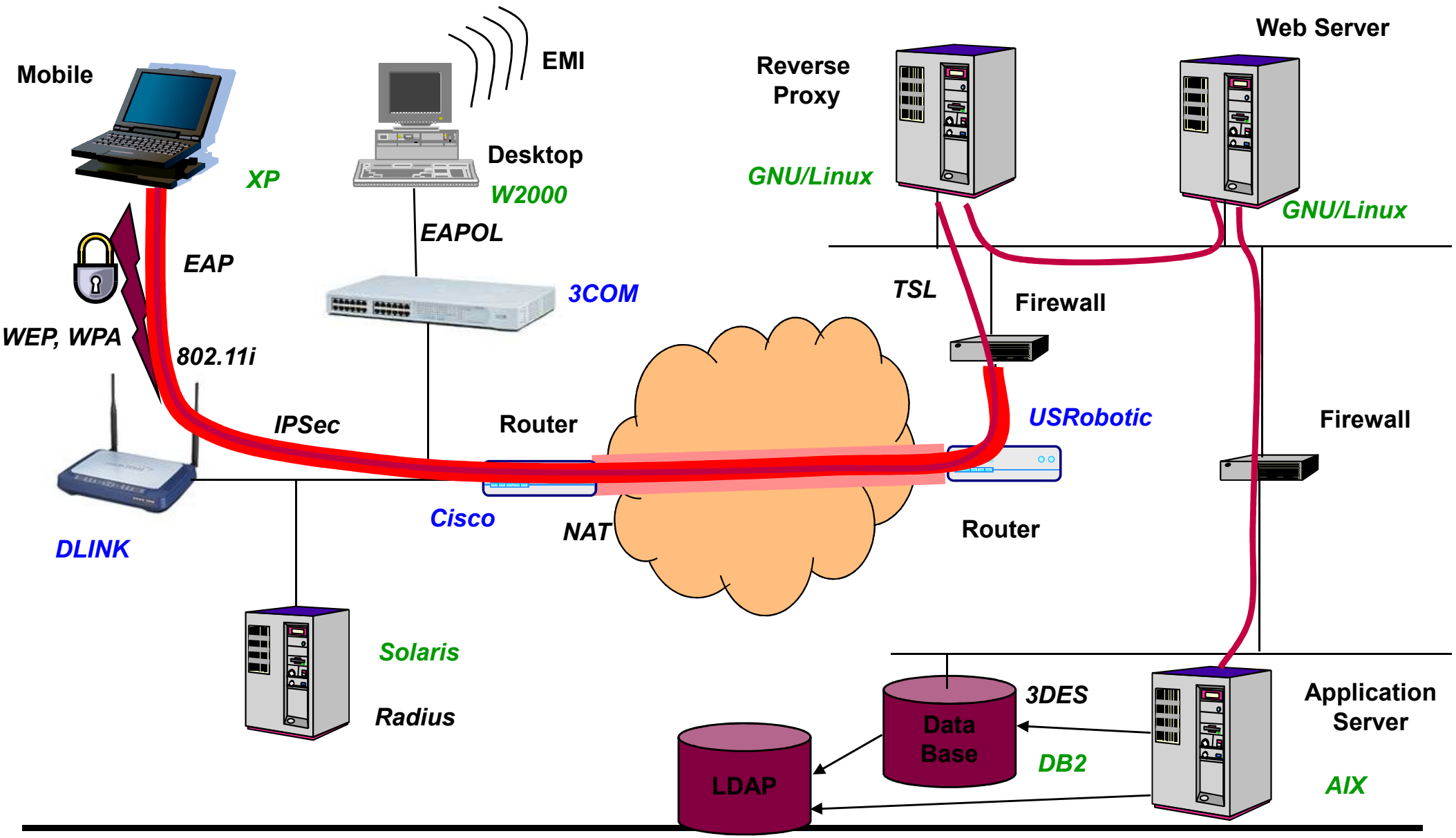
- Autenticación.
  - Corroboración de que un extremo de la comunicación es quien dice ser.
- Control de acceso.
  - Prevención de uso no autorizado de un recurso.
- No repudio.
  - Imposibilidad por parte de un extremo de una comunicación de negar que ha participado en ella.
- Confidencialidad.
  - La información no se hace disponible a entes no autorizados.
- Integridad.
  - La información no se altera ni destruye de forma no autorizada.
- Auditoría de seguridad y alertas.
  - Revisiones de los registros de actividad del sistema para comprobar que se cumple una determinada política de seguridad.

La seguridad es un problema de sistemas, no de componentes

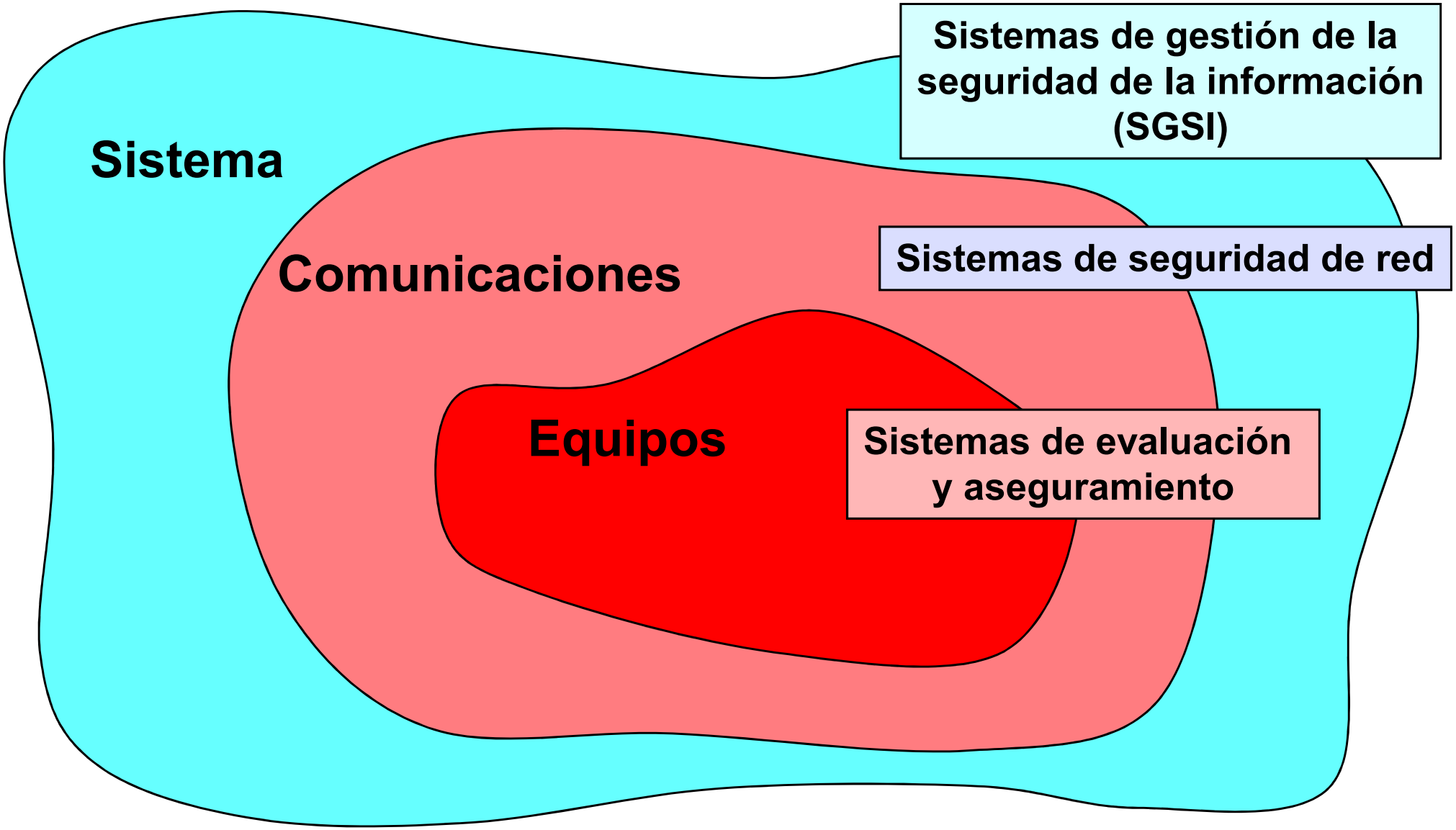
- Para garantizar la seguridad de un sistema no basta con garantizar la seguridad de sus componentes básicos. Hay que garantizar la del conjunto.
- El *todo* es más que la suma de las *partes*:
  - Los sistemas son complejos. La complejidad aumenta la probabilidad de fallo, y el fallo, el problema de seguridad.
  - Los sistemas interaccionan entre sí. A mayor interacción, mayor complejidad. Es difícil prever todas las posibles interacciones.
  - Los sistemas tienen propiedades emergentes. Su implantación y uso puede producir la aparición de elementos no considerados en su diseño.
- La seguridad de los sistemas requiere:
  - Prevención: Aplicación de la teoría de la seguridad para lograr un efecto.
  - Detección: Alertas que permitan la detección precoz de problemas.
  - Reacción: Capacidad para tomar medidas que permitan cancelar el ataque.

La seguridad es una cadena: es tan fuerte como su eslabón más débil.
La seguridad es un proceso, no un producto. **Bruce Schneier.**

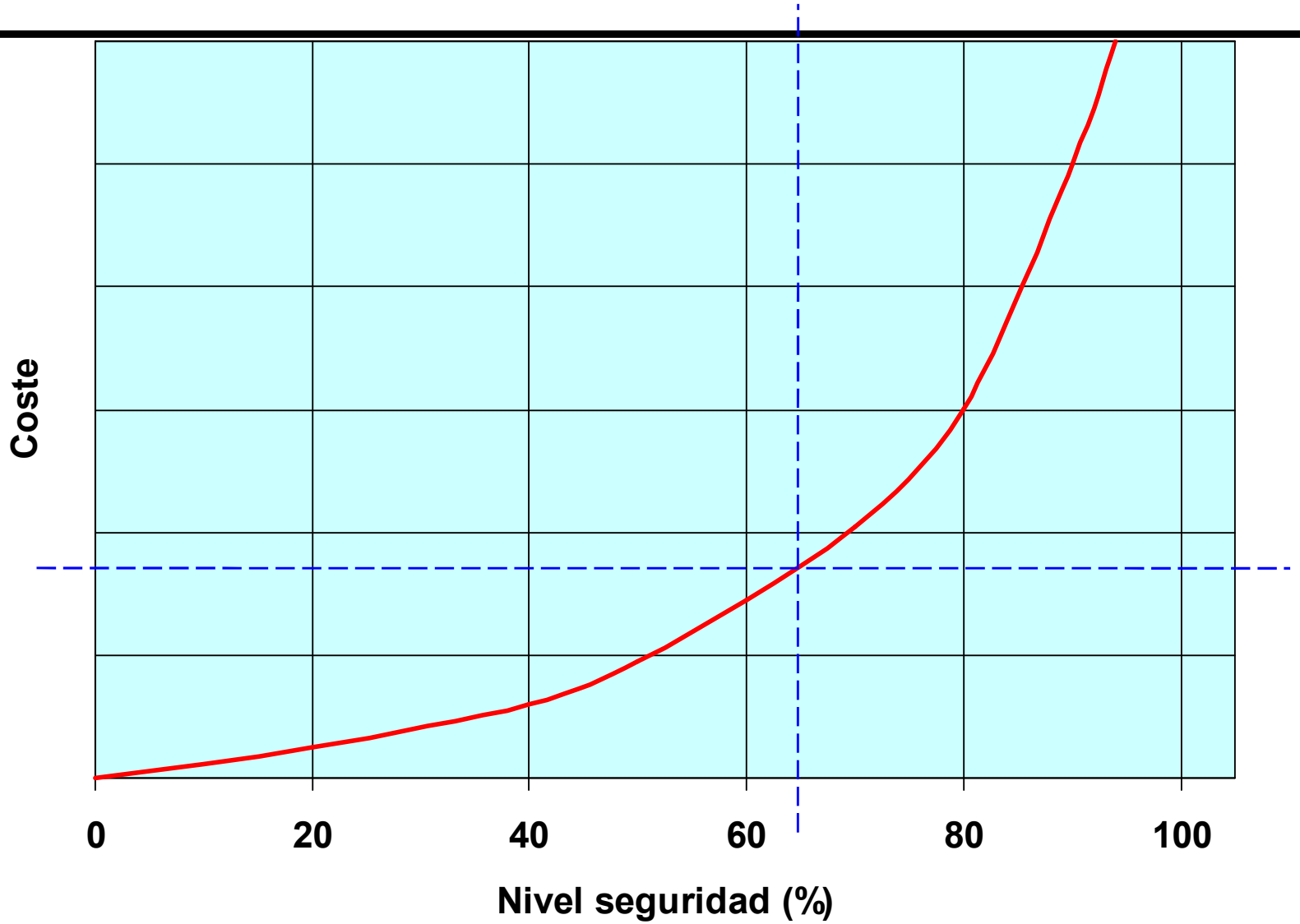
La seguridad es un problema de sistemas, no de componentes



Los niveles de aplicación de la seguridad



El coste de la seguridad



El 100% de seguridad no es posible.

Ningún sistema de seguridad en la información puede hacerlo todo.

Directrices de la OCDE para regular la seguridad de los sistemas y redes de información

Declaración de principios de la OCDE sobre la seguridad en las TIC.

Se basa en nueve principios complementarios, que deben verse en conjunto:

1. Concienciación. Los participantes deberán ser conscientes de la necesidad de contar con sistemas y redes de información seguros, y tener conocimiento de los medios para ampliar la seguridad.
2. Responsabilidad. Todos los participantes son responsables de la seguridad de los sistemas y redes de información.
3. Respuesta. Los participantes deben actuar de manera adecuada y conjunta para prevenir, detectar y responder a incidentes que afecten la seguridad.
4. Ética. Los participantes deben respetar los intereses legítimos de terceros.
5. Democracia. La seguridad de los sistemas y redes de información debe ser compatible con los valores esenciales de una sociedad democrática.
6. Evaluación de riesgos. Los participantes deben llevar a cabo evaluaciones de riesgo.
7. Diseño y realización de la seguridad. Los participantes deben incorporar la seguridad como un elemento esencial de los sistemas y redes de información.
8. Gestión de la seguridad. Los participantes deben adoptar una visión integral de la administración de la seguridad.
9. Reevaluación. Los participantes deben revisar y reevaluar la seguridad de sus sistemas y redes de información, y realizar las modificaciones pertinentes sobre sus políticas, prácticas, medidas y procedimientos de seguridad.

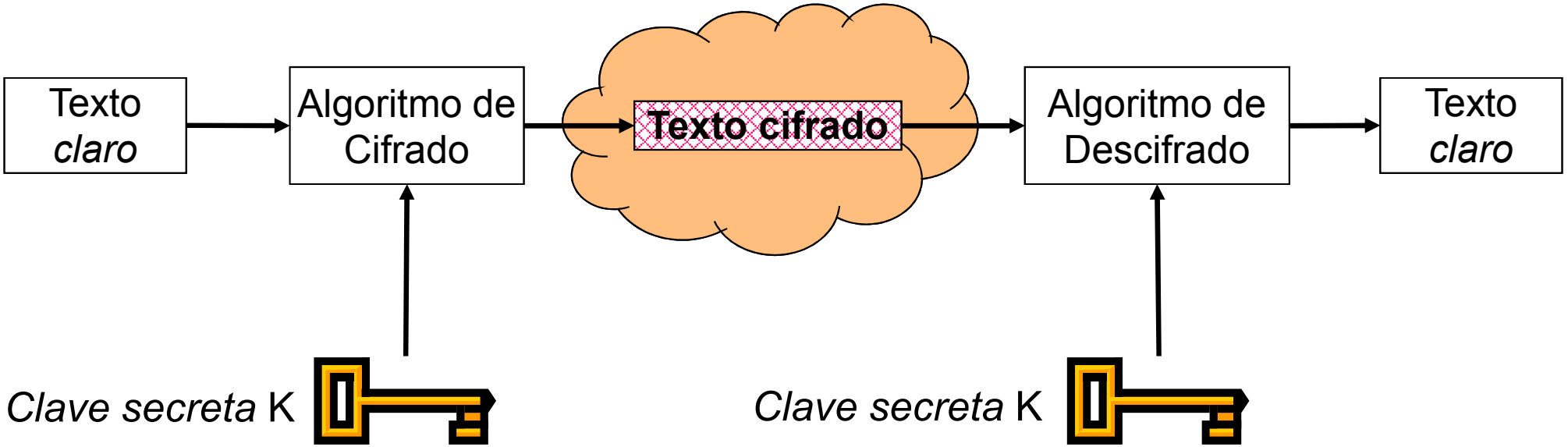
Técnicas criptográficas básicas de protección de la información. Criptografía

- Conjunto de técnicas y aplicaciones que permiten realizar dos procesos:
  - Cifrado: Transformación de un mensaje entendible (texto claro, texto plano, *plaintext)*, en un mensaje que no puede ser reconocido (texto cifrado, *ciphertext)*.
  - Descifrado: Obtener a partir del texto cifrado el mensaje original.
- Cifrado y descifrado se realizan aplicando un algoritmo a sus datos de entrada.
- Aplicación de un algoritmo a los datos transmitidos basada en una clave.
- **La seguridad debe depender del secreto de la clave, no del secreto del algoritmo.**(1)
- Clasificación:
  - Clave secreta / clave pública.
  - Cifrado de bloques / cifrado de flujo de datos *(data stream).*

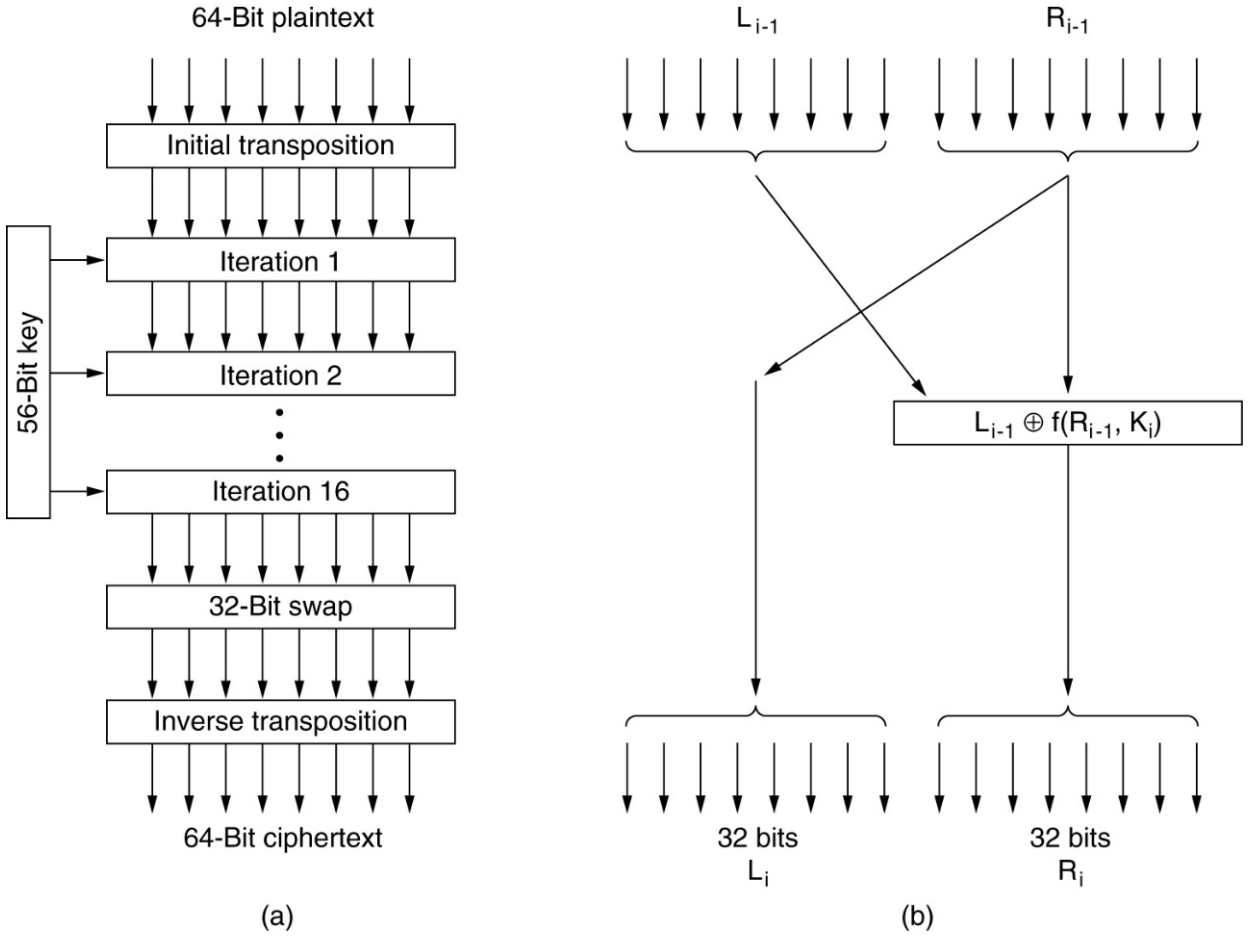
(1) Auguste Kerckhoff. 1883.

Cifrado simétrico o de clave secreta

- Emplean la misma clave para el proceso de cifrado y descifrado.
- Características:
  - El algoritmo empleado debe ser robusto.
  - El número posible de claves a usar debe ser muy grande.
  - El método para establecer la clave secreta debe ser seguro.
- Algoritmos más empleados: DES, Triple DES, AES.

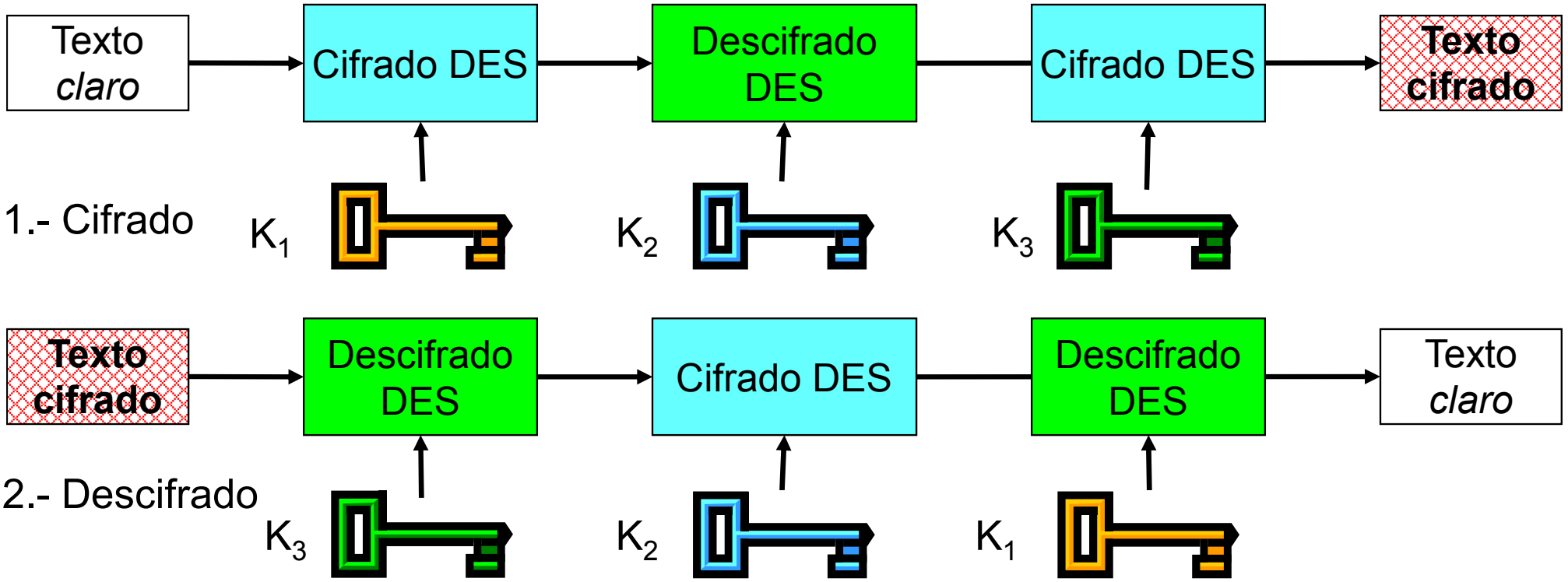


Funcionamiento básico algoritmo DES



Fuente: Tanenbaum, A., *Computer Networks*, Prentice-Hall, 2002. 4ª ed.

Triple DES



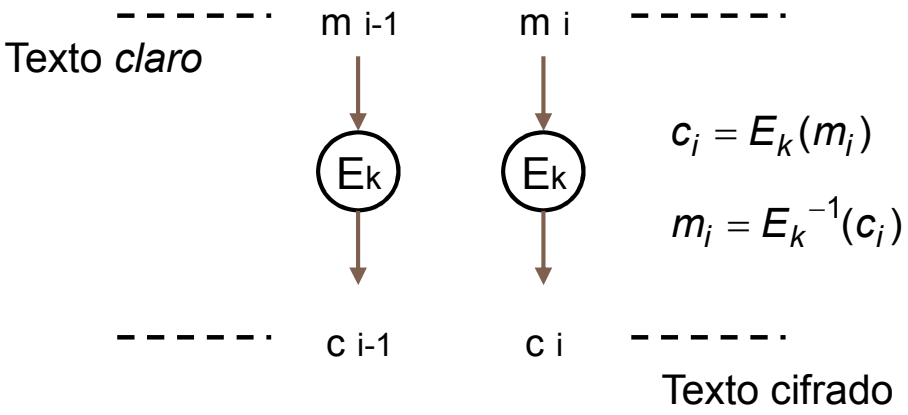
- Si las tres claves son distintas, 3DES. Clave de 168 bits.
- Si K1 = K3, 2DES. Clave de 112 bits.
- Si K1 = K2 = K3 es un DES estándar

Características de los algoritmos simétricos más empleados

Algoritmo	Autor	Longitud clave (bits)	Tamaño del bloque (bits)	Comentarios
Blowfish	Bruce Schneier	1-448	64	Lento y anticuado
DES	IBM	56	64	Débil para su uso actual
IDEA	Massey y Xuejia	128	64	Bueno, pero patentado
RC2	Ronald Rivest	0-1024	64	Algunas claves son *débiles*. Patentado.
RC4	Ronald Rivest	8-2048	Flujo	Versión de flujo de RC2
RC5	Ronald Rivest	0-2040	32, 64, 128	Bueno, patentado.
Rijndael	Daemen y Rijmen	128-256	128	Mejor elección. Elegido para el AES.
Serpent	Anderson, Biham, Knudsen	128-256	128	Muy fuerte. Segundo clasificado en AES.
Triple DES	IBM	112-168	64	Segunda mejor elección
Twofish	Bruce Schneier	128, 192, 256	128	Muy fuerte. Tercer clasificado AES.

Modos de funcionamiento cifradores de bloques (I)

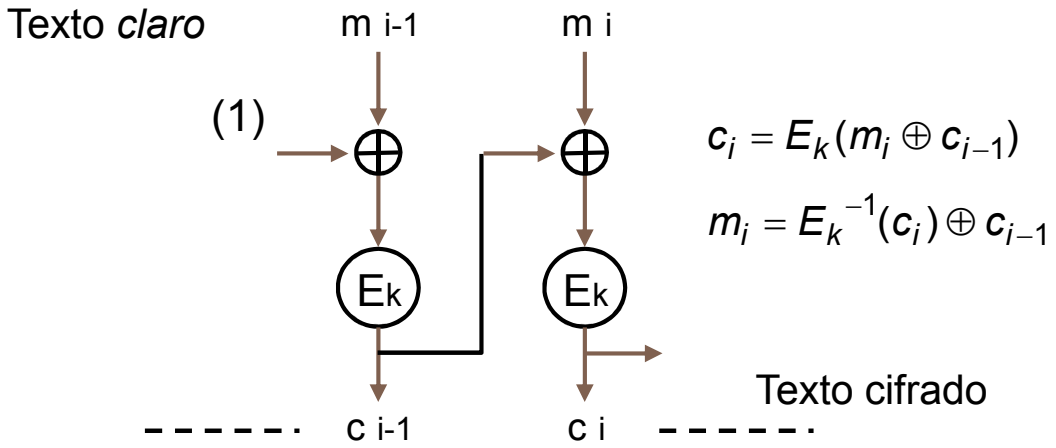
Electronic Code Block, ECB



$c_i = E_k(m_i)$

$m_i = E_k^{-1}(c_i)$

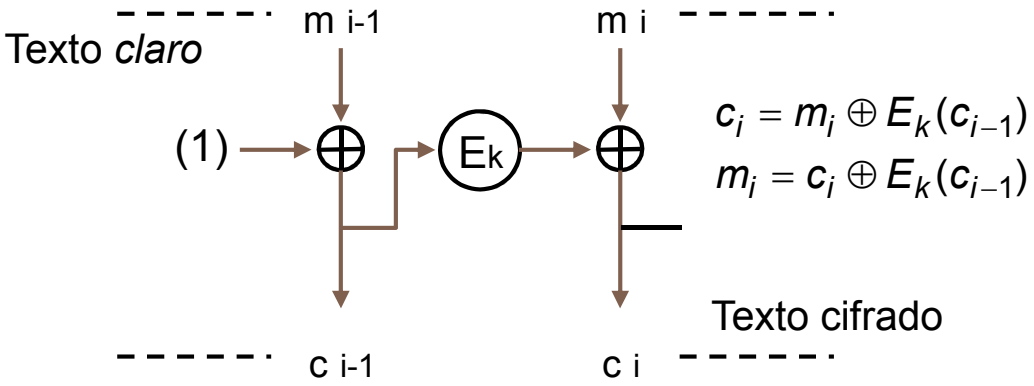
Cipher Block Chaining, CBC



$c_i = E_k(m_i \oplus c_{i-1})$

$m_i = E_k^{-1}(c_i) \oplus c_{i-1}$

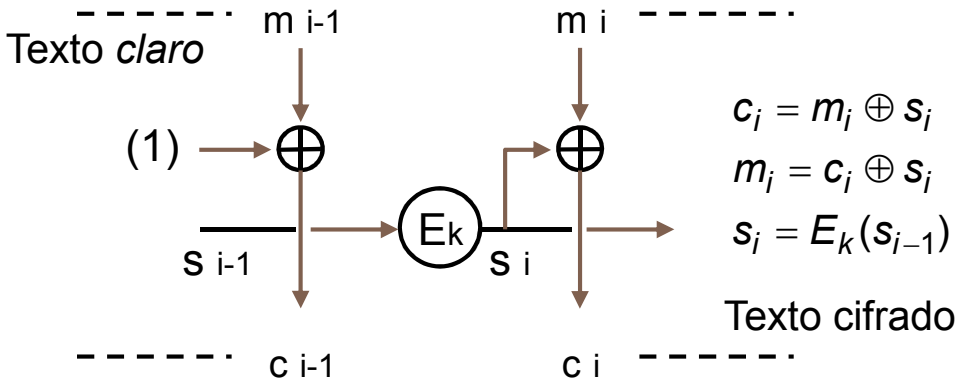
Cipher Feedback Block, CFB



$c_i = m_i \oplus E_k(c_{i-1})$

$m_i = c_i \oplus E_k(c_{i-1})$

Output Feedback Block, OFB



$c_i = m_i \oplus s_i$

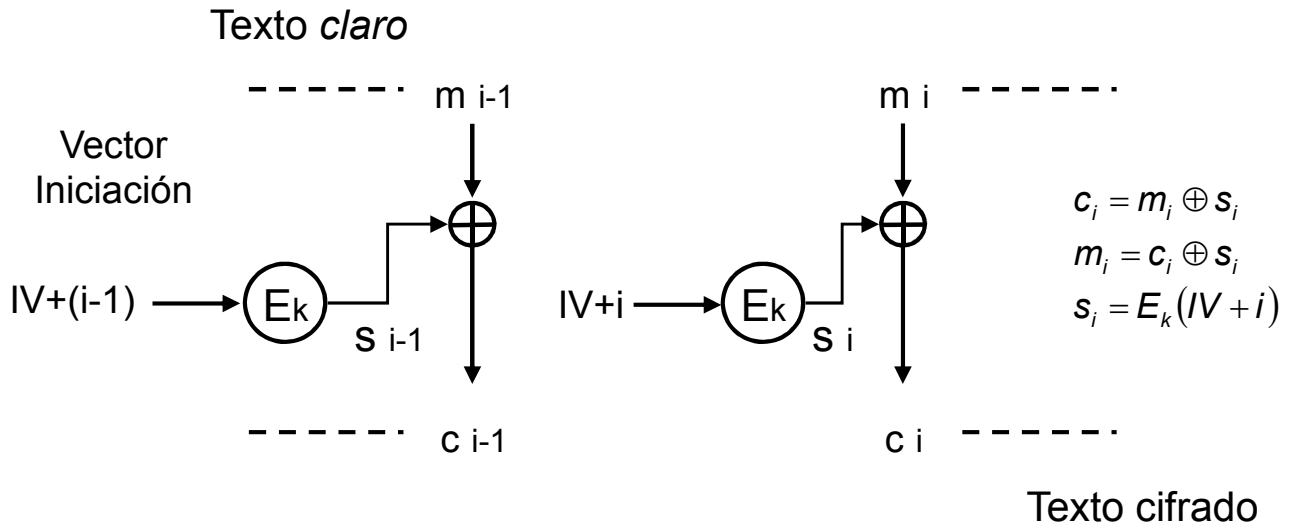
$m_i = c_i \oplus s_i$

$s_i = E_k(s_{i-1})$

(1) El primer bloque (*Initialization Vector*, IV) se genera de forma aleatoria y se transmite con el texto

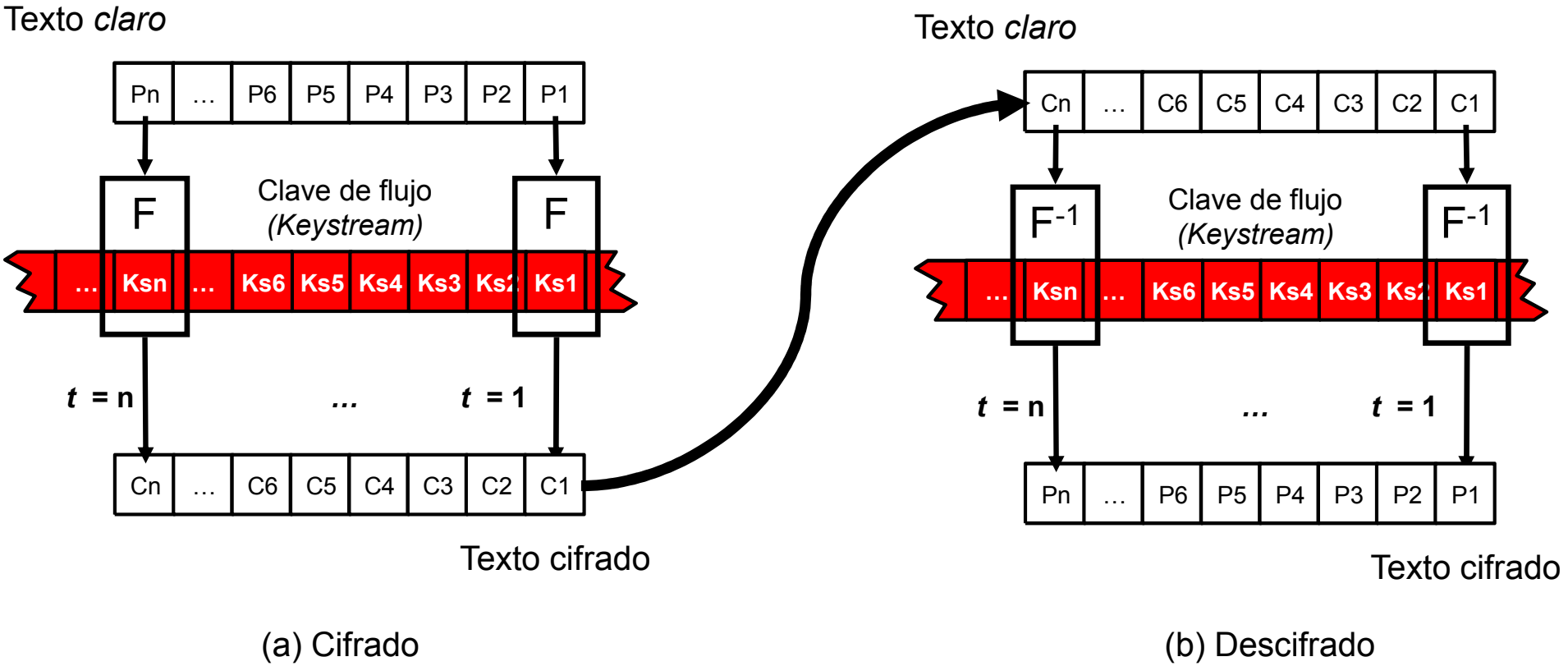
Modos de funcionamiento cifradores de bloques (II)

- Modo contador
  - Permite acceso aleatorio a los datos cifrados
  - El cifrado se aplica a un vector de iniciación que es incrementado para cada bloque de texto claro.
  - Es necesario utilizar un vector de iniciación distinto en cada cifrado para evitar ataques de reutilización de claves.



Cifradores de flujo de datos

- Generan un byte a la salida por cada byte de entrada.
- Texto cifrado generado a partir del texto claro combinándolo con una clave de flujo *(keystream).* Habitualmente se hace un XOR de ambos.
- Imprescindible evitar la reutilización de la clave de flujo.
  - *One time pads* o generada pseudoaleatoriamente.



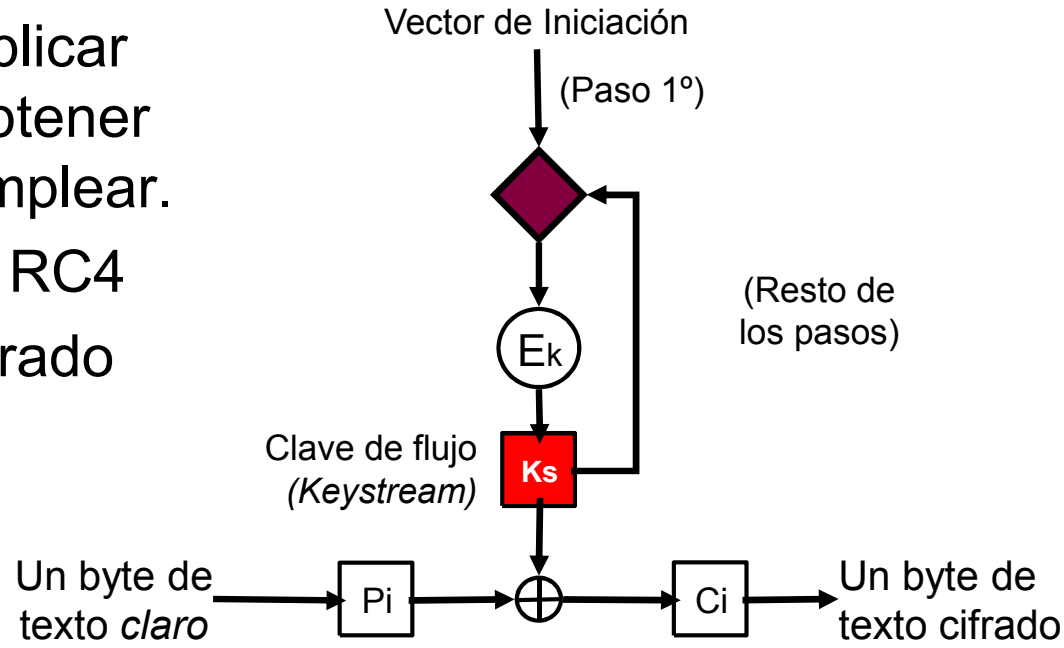
Generación de las claves de flujo

Mediante un algoritmo de cifrado

- La clave de flujo se obtiene cifrando con una determinada clave secreta un vector de iniciación.
- Cada unidad de datos del texto claro (habitualmente un byte) se combina con una unidad de datos de la clave de flujo, produciendo una unidad del texto cifrado.
- A continuación, se vuelve a aplicar el algoritmo de cifrado para obtener la siguiente clave de flujo a emplear.

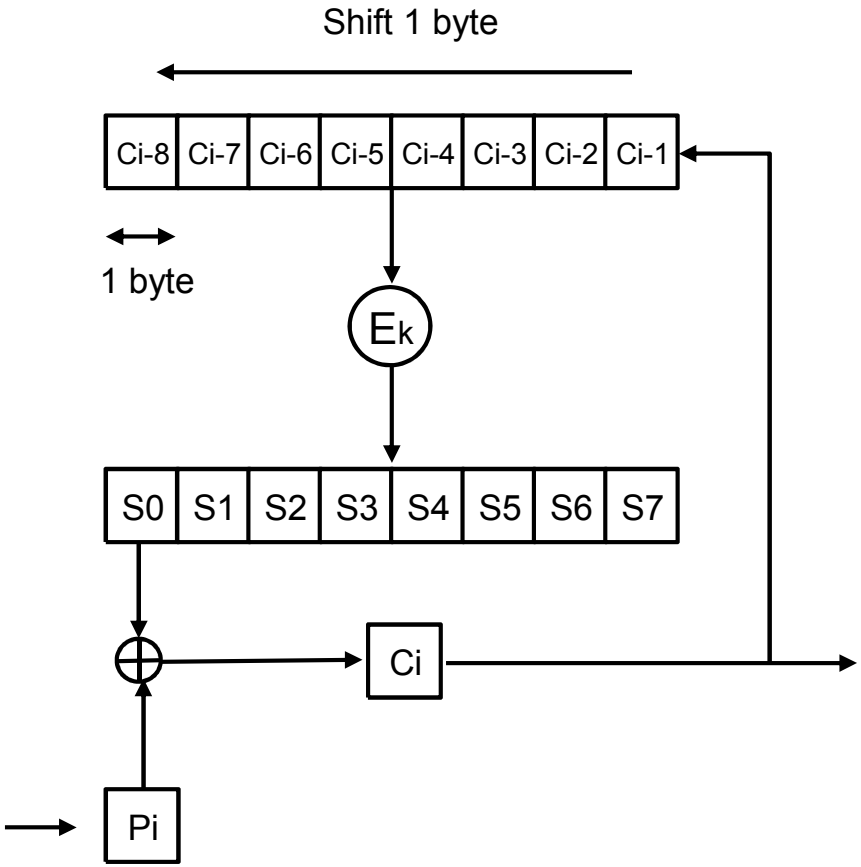
De este modo funciona el algoritmo RC4

- Emplea como algoritmo de cifrado el RC2.

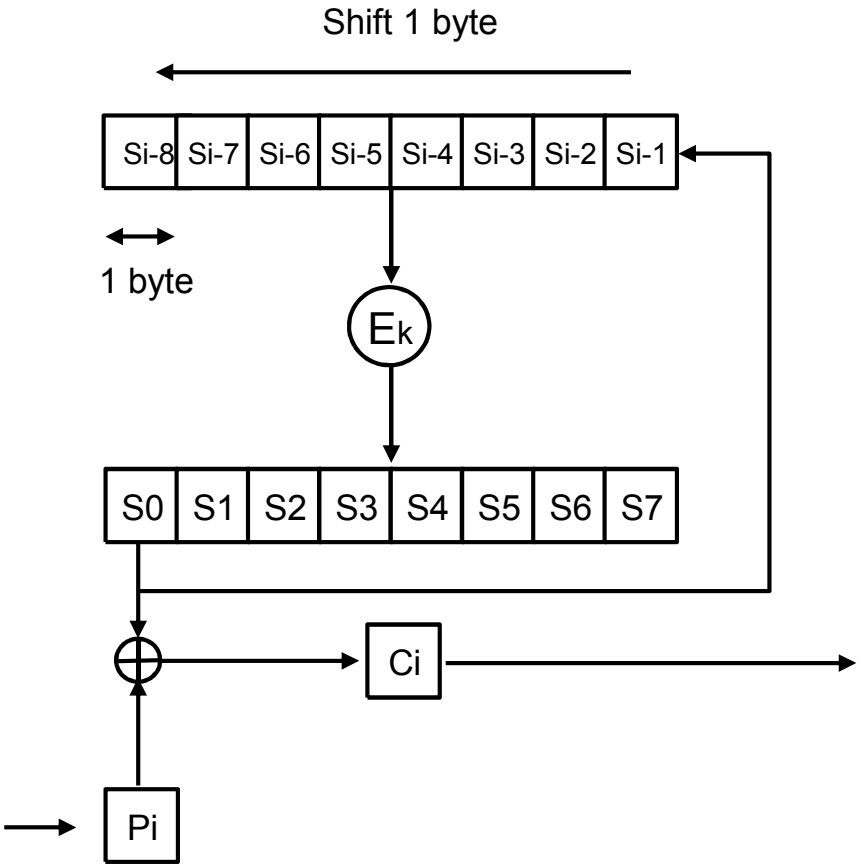


Cifrado modo *stream* con cifradores de bloques

Usando *Cipher Feedback Block, CFB*

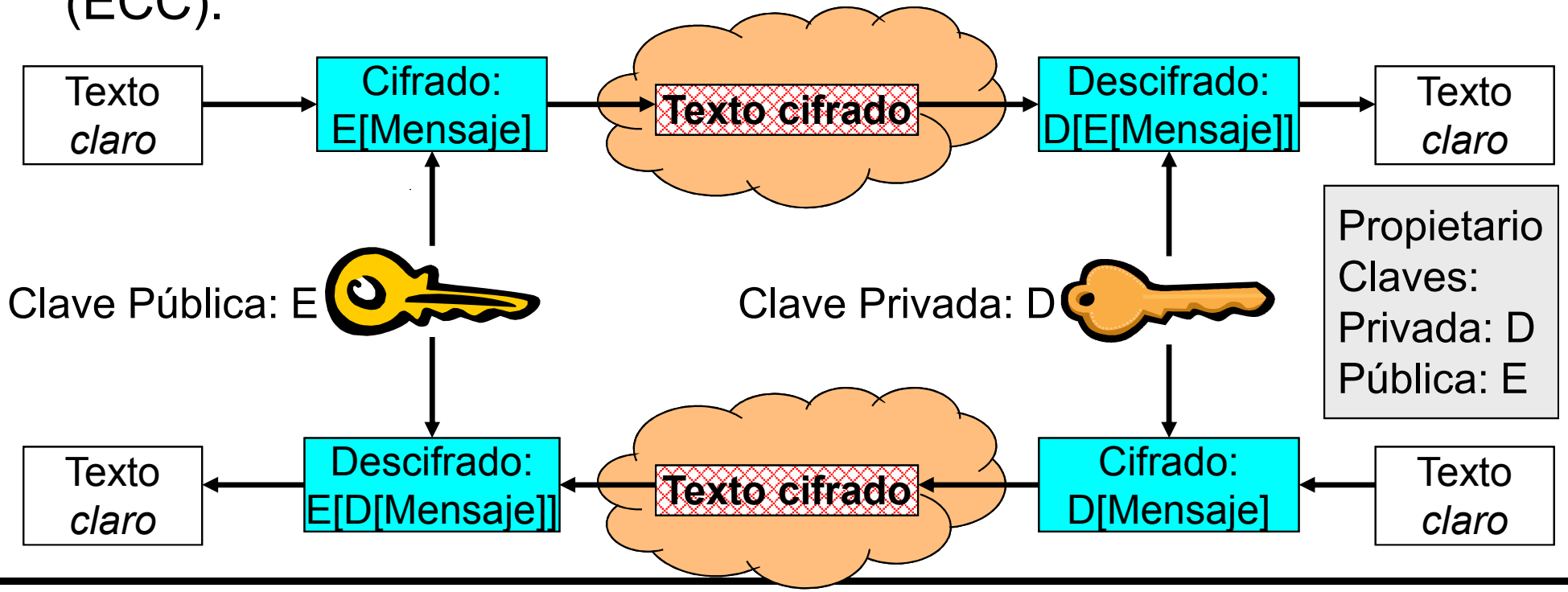


Usando *Output Feedback Block, OFB*



Cifrado asimétrico o de clave pública - privada

- Dos claves. El propietario publica una de ellas, y mantiene en secreto la otra.
- Lo que se cifre con una de ellas sólo se puede descifrar con la otra, y viceversa.
- Algoritmos más empleados: RSA, ElGamal, Curvas Elípticas (ECC).



Características del cifrado asimétrico

- El cifrado asimétrico no es intrínsecamente más seguro que el cifrado simétrico.
- El coste computacional para realizar el cifrado asimétrico es muy superior al del cifrado simétrico.
- Por las razones anteriores, el cifrado asimétrico no ha desplazado al cifrado simétrico ni se prevé que pueda desplazarlo a corto plazo. Cada uno conserva un ámbito de aplicación concreta.
- Estándares de implementación de los sistemas de cifrado asimétricos basada en los *Public Key Infrastructure Standards* (PKCS), de RSA. http://www.rsasecurity.com/rsalabs/pkcs/.

El algoritmo de cifrado RSA

- Se genera una cantidad, denominada módulo, como

$$n = p \cdot q$$

  donde p y q son dos números primos muy grandes y no muy próximos.
- El cifrado se realiza como:

$$C = P^{e} \bmod n$$

- Y el descifrado:

$$P = C^{d} \bmod n$$

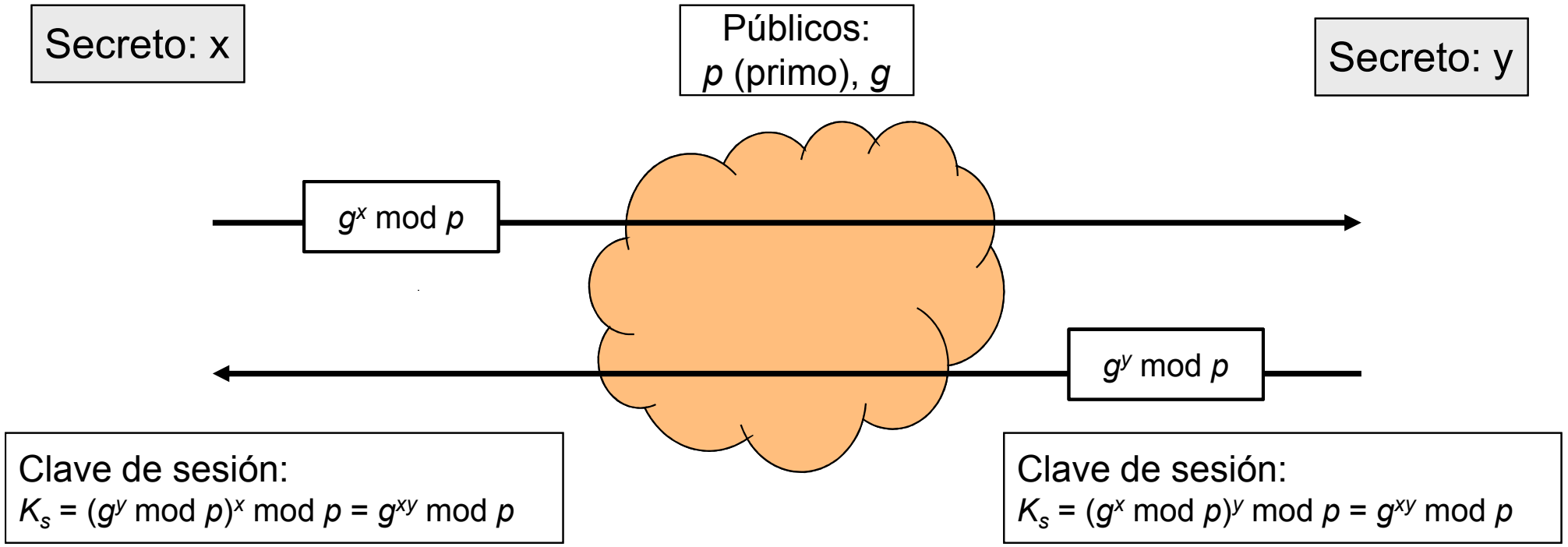
  donde se debe verificar que:

$$(e \cdot d) \bmod ((p-1) \cdot (q-1)) = 1$$

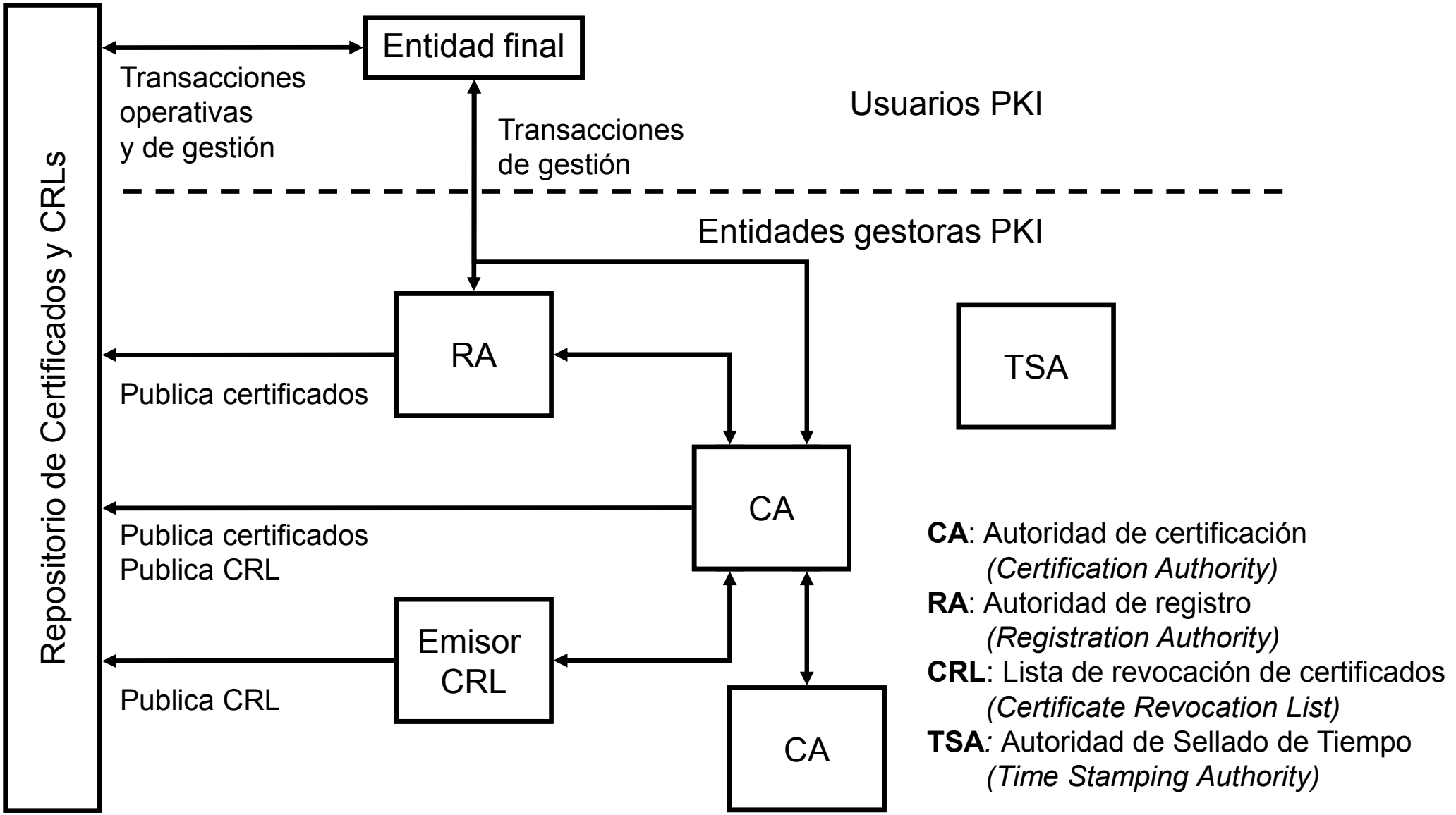
Establecimiento de claves de cifrado

- En algoritmos simétricos, imprescindible mantener el secreto de la clave.
  - Transporte de claves: Se genera en un extremo y la comunica al otro.
    - Transporte mediante algoritmos de cifrado asimétricos.
  - Acuerdo de claves: Ambas partes aportan información para generarla.
    - Métodos de Diffie-Hellman y Menezes-Qu-Vanstone.
- En algoritmos asimétricos, imprescindible asegurar la asociación entre una clave pública y la entidad propietaria.
  - Garantizada por un tercero de confianza *(Trusted Third Party, TTP)* a través de un **certificado digital**.
    - Formando una *Public Key Infrastructure, PKI*.
  - El formato más empleado es el X.509 versión 3.
  - Contiene, entre otros campos, la clave pública, identidad origen, usos, intervalo temporal de validez y firma digital del TTP.
  - Los TTP emiten *listas de revocación* de certificados emitidos.

Intercambio de claves por el método de Diffie-Hellman



Estructura de un sistema PKI



Criptoanálisis

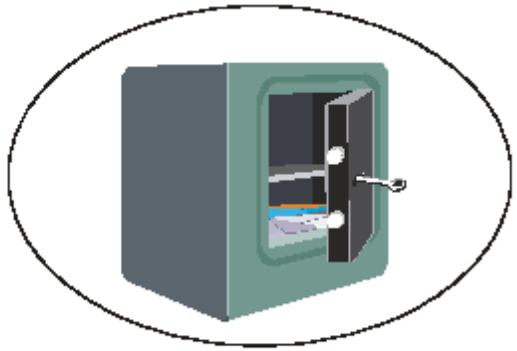
- Técnica por la que se intenta descubrir un texto claro a partir de un texto cifrado.
- Un esquema de cifrado es *computacionalmente seguro* si:
  - El coste de romper el cifrado excede el valor de la información cifrada.
  - El tiempo necesario para romper el cifrado excede el tiempo de vida útil de la información protegida.
- *Fuerza bruta*: búsqueda exhaustiva de claves.
  - Evitado utilizando claves de longitud suficiente.
- Criptoanálisis diferencial: diferencias entre cifrados conocidos permiten intuir la clave.
- Reutilización de clave: permite eliminar la clave conociendo dos textos cifrados con la misma.
- Adivinación de texto claro: intuir el texto y cifrarlo con la clave pública para saber si se está en lo cierto.
- *Ataques de cumpleaños*: Obtener un texto claro que produzca el mismo valor de resumen que un texto dado.

Sistemas de Gestión de la Seguridad de la Información SGSI

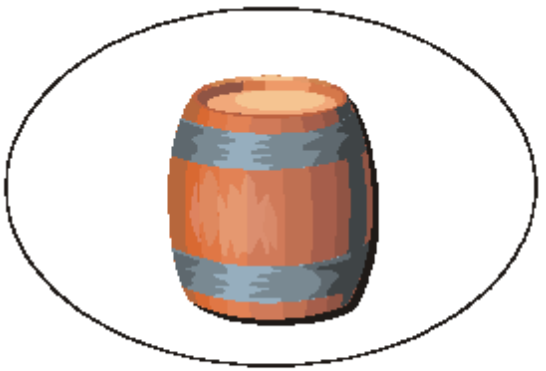
- La seguridad es un proceso, no un producto.
- Como todo proceso, es conveniente su desarrollo de acuerdo con un mecanismo basado en:
  - Planificación: establecer las bases de su ejecución.
  - Ejecución: implementarlo y operarlo correctamente.
  - Comprobación: monitorización y revisión del proceso.
  - Acciones posteriores: mantenimiento y mejora.

- Esta metodología de gestión de procesos se conoce con el nombre *Plan-Do-Check-Act (PDCA).*
- Mediante la implantación de un Sistema de Gestión se garantiza que se realizan los controles adecuados para garantizar la calidad de la ejecución del proceso (ISO 9001).
- En el caso de la seguridad, el sistema recibe el nombre de Sistema de Gestión de la Seguridad de la Información, SGSI *(Information Security Management System, ISMS).*
- El estándar ISO 27001 establece el modelo de referencia para los SGSI.

Necesidad de estándares en los procesos de seguridad



Entonces me dices que puedo estar tranquilo, que ya tienes claro lo que quiero para mis datos



Cuenta con ello, mi compañía tiene el sistema perfecto y seguro para cubrir tus expectativas

Sistemas de seguridad de red

- Las redes de comunicaciones, por su propia naturaleza, son uno de los puntos de un sistema distribuido donde se concentra un mayor número de riesgos.
- TCP/IP, estándar *de facto* en las comunicaciones actuales, no está diseñado para reforzar la seguridad.
  - Situación original Internet:
    - Entorno limitado a Universidades.
    - Confianza general en los usuarios que acceden a los servidores.
    - Todo permitido.
  - Situación actual:
    - Entorno abierto a todas las empresas y usuarios.
    - Circula información con valor comercial.
    - Necesidad de establecer mecanismos de seguridad.
- Controlar la seguridad en tres áreas principales:
  - Reforzar los sistemas de autenticación de usuarios en la red.
  - Proteger la confidencialidad y la integridad de la información que circula por la red mediante protocolos seguros.
  - Establecer mecanismos de defensa perimetral: Cortafuegos *(Firewalls)*.
  - Mantener una vigilancia continua mediante un sistema de detección de intrusiones.

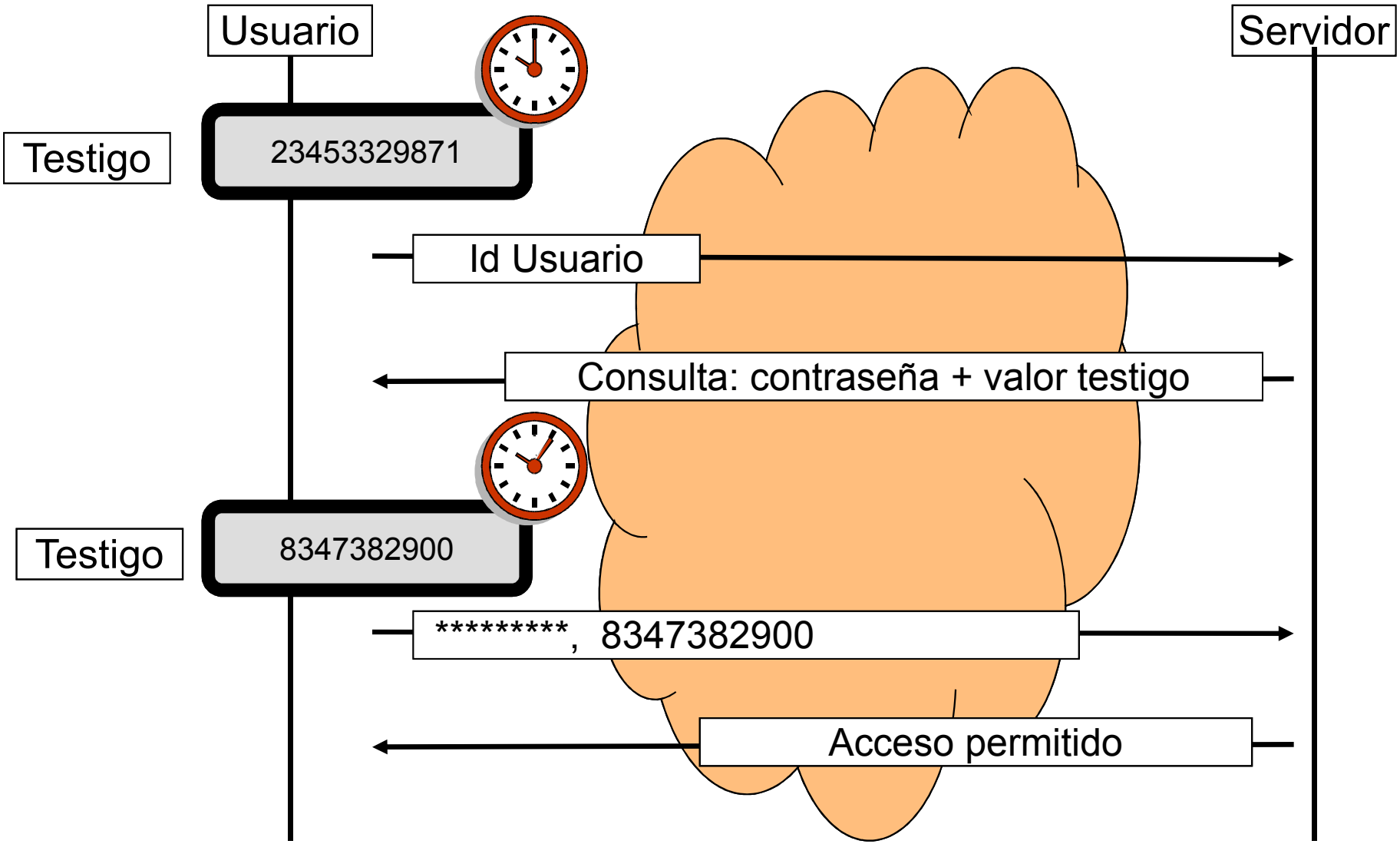
Autenticación

- Paso previo para garantizar la seguridad de cualquier comunicación: identificar las entidades entre las cuales se establece.
- Los mecanismos de autenticación emplean tres técnicas distintas, por separado o conjuntamente:
  - Verificar algo que el usuario *sabe*: contraseña, respuesta a un desafío.
  - Verificar algo que el usuario *tiene*: testigos, certificados digitales.
  - Verificar algo que el usuario *es*: rasgos biométricos.
- Se distinguen dos tipos de mecanismos de autenticación:
  - Autenticación sencilla o simple: verificación de contraseña almacenada.
  - Autenticación fuerte o robusta: impiden la suplantación de la identidad.

Mecanismos de autenticación más frecuentes

- Autenticación simple. Envío de:
  - Usuario y contraseña en *claro*.
  - Usuario, número aleatorio, y testigo generado mediante un resumen de la contraseña y número aleatorio. No se puede repetir dos veces el mismo número.
- Autenticación fuerte.
  - Desafío-respuesta: Tarjetas de coordenadas, S-Key.
  - Autenticación por dos factores: algo que el usuario sabe y algo que tiene.
  - Autenticación mediante sistemas de cifrado simétricos:
    - Needham-Schroeder.
    - Otway-Rees.
    - Kerberos.
  - Autenticación mediante sistemas de cifrado asimétricos:
    - Unidireccional, Bidireccional y Tridireccional.
  - Autenticación biométrica.

Autenticación por dos factores mediante testigo



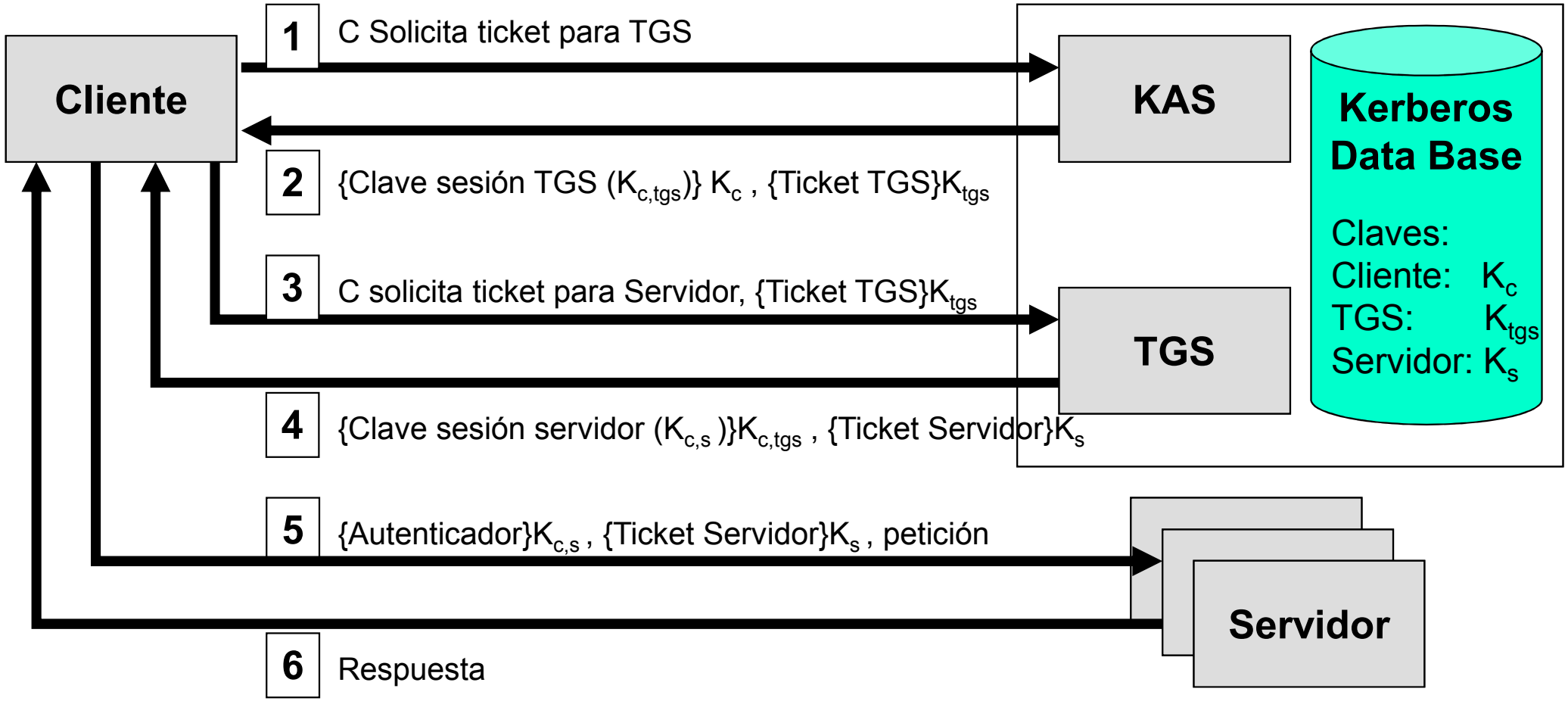
Kerberos

- Sistema de autenticación y autorización en red basado en cifrado simétrico.
- Proporciona autenticación mutua entre usuarios y servidores.
- Proporciona esquemas de autorización que pueden ser implementados por cada servidor de modo independiente del esquema de autenticación.
- Permite la implementación de un sistema de contabilidad integrado, seguro y fiable.
- Asume lo siguiente:
  - Entorno de clientes y servidores con un nivel de seguridad física. No adecuado en redes abiertas.
  - Relojes de clientes y servidores sincronizados.
- Se compone de los siguientes elementos centrales:
  - *Kerberos Ticket Granting Server, TGS*: Emite tickets para que un cliente acredite su identidad ante cualquier servidor de la red.
  - *Kerberos Authentication Server, KAS*: Emite tickets para que un cliente acredite su identidad ante el *TGS*.
  - *Kerberos Database*: Base de datos que contiene las contraseñas de todos los clientes y servidores de la red.
    - Mantenimiento realizado por el *Kerberos Data Base Manager, KDBM*.
    - Accesos a ella realizados a través del *Kerberos Key Distribution Server, KKDS*.

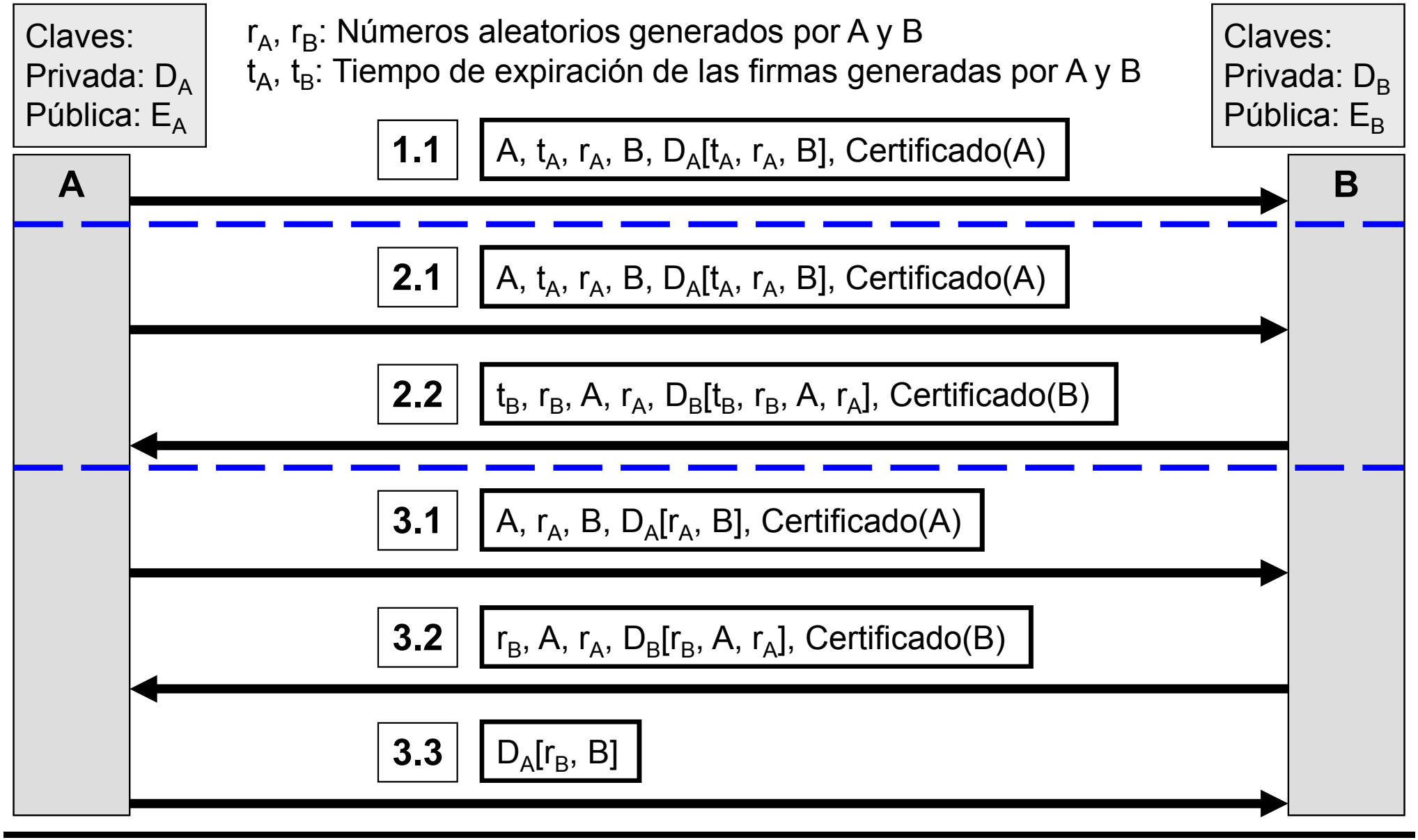
Tickets

- Elemento básico de autenticación en Kerberos.
- Permite autenticar a un cliente ante un determinado servidor.
- Emitido y garantizado por un tercer servidor en quien ambos confían.
- Contiene:
  - Identidad del cliente que solicita la conexión.
  - Identidad del servidor para el que está destinado.
  - Una clave de sesión para comunicar entre cliente y servidor.
  - Una numeración de secuencia que permita identificarlo.
  - Un *timestamp*, que permita verificar si su validez ha expirado o no.
- El ticket se cifra con una clave secreta del servidor destino, produciéndose un **ticket sellado**.
  - El cliente recibe el ticket, pero no es capaz de leer ni modificar su contenido.
  - El cliente enviará este ticket al servidor destino para que extraiga de él la información del cliente, y verifique su autenticidad.

Autenticación mediante Kerberos



Autenticación mediante cifrado asimétrico



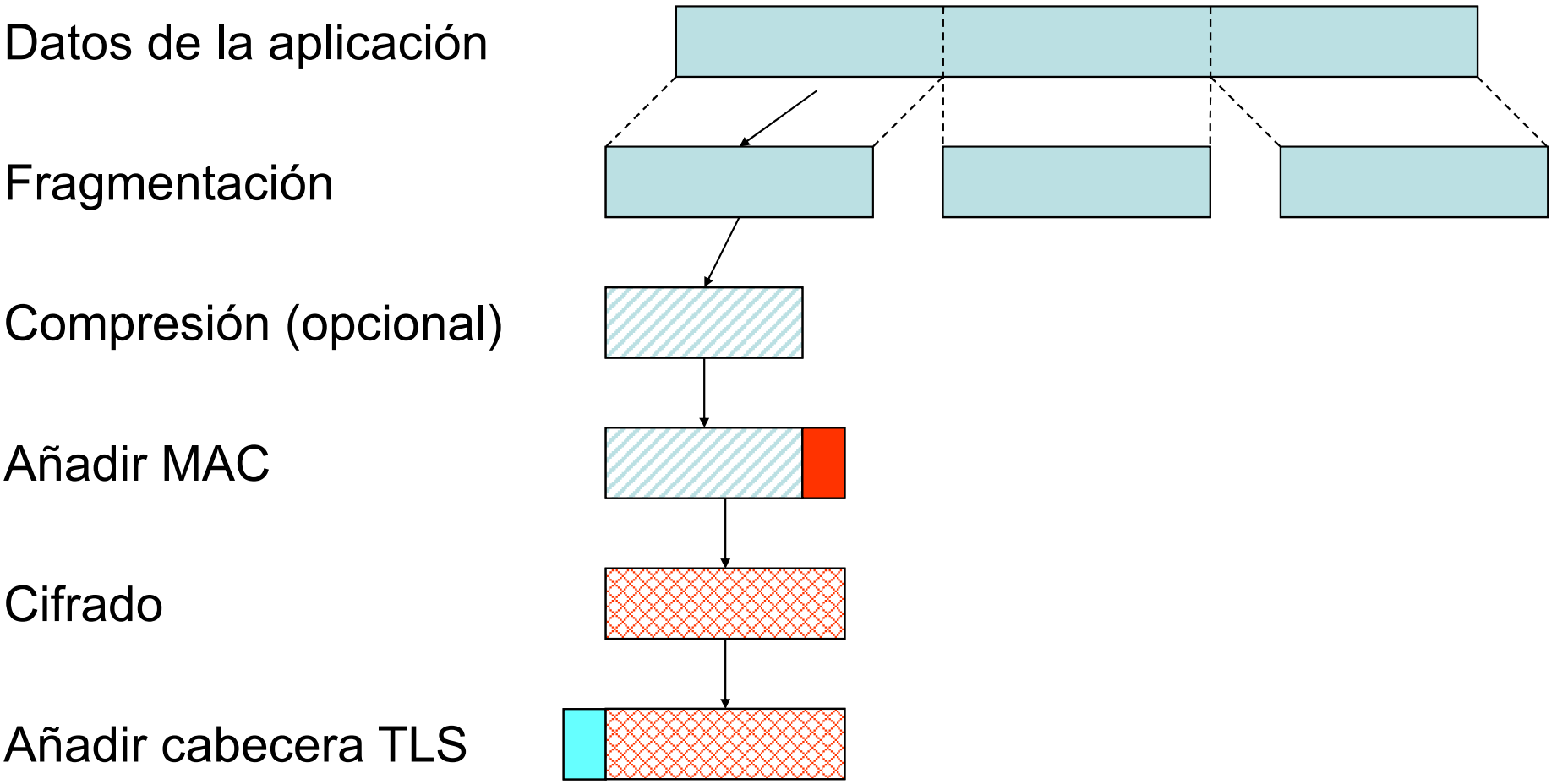
Seguridad en los protocolos de comunicaciones

- Los protocolos básicos de Internet, tanto de transporte como de aplicación, no están pensados para reforzar la seguridad ni en sus niveles más básicos: confidencialidad, integridad, autenticación.
- Se han definido protocolos sobre TCP/IP para cubrir esta carencia de seguridad. Algunos de los más utilizados son:
  - *Transport Layer Security, TLS.*
  - *Secure Shell, SSH.*
  - *IPSec*

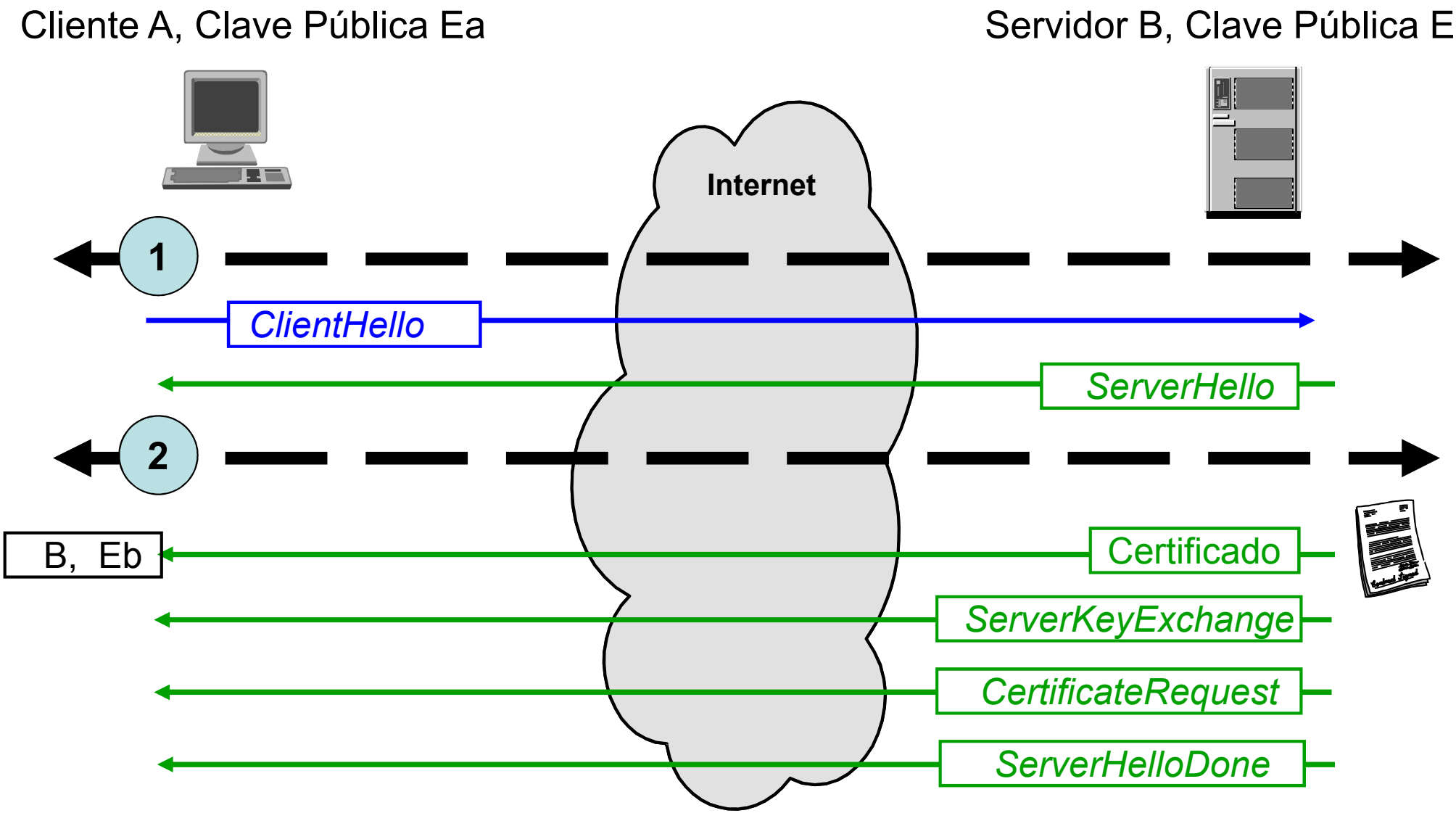
Transport Layer Security, TLS

- Estandarización por parte de la IETF del protocol *Secure Sockets* Layer, propiedad de *Netscape*.
- Protocolo de transporte.
  - Inicialmente utilizado para transportar HTTP.
  - Puede ser utilizado por cualquier protocolo de nivel superior.
- Proporciona
  - Autenticación de participantes mediante mecanismos de cifrado asimétricos.
  - Cifrado de las comunicaciones para garantizar confidencialidad e integridad.
- Se descompone en dos niveles:
  - *SSL Record Protocol*: Empleado para encapsular protocolos de nivel superior.
  - *SSL Handshake Protocol*: Negociación de las características del cifrado entre cliente y servidor. Requiere envío de certificados.

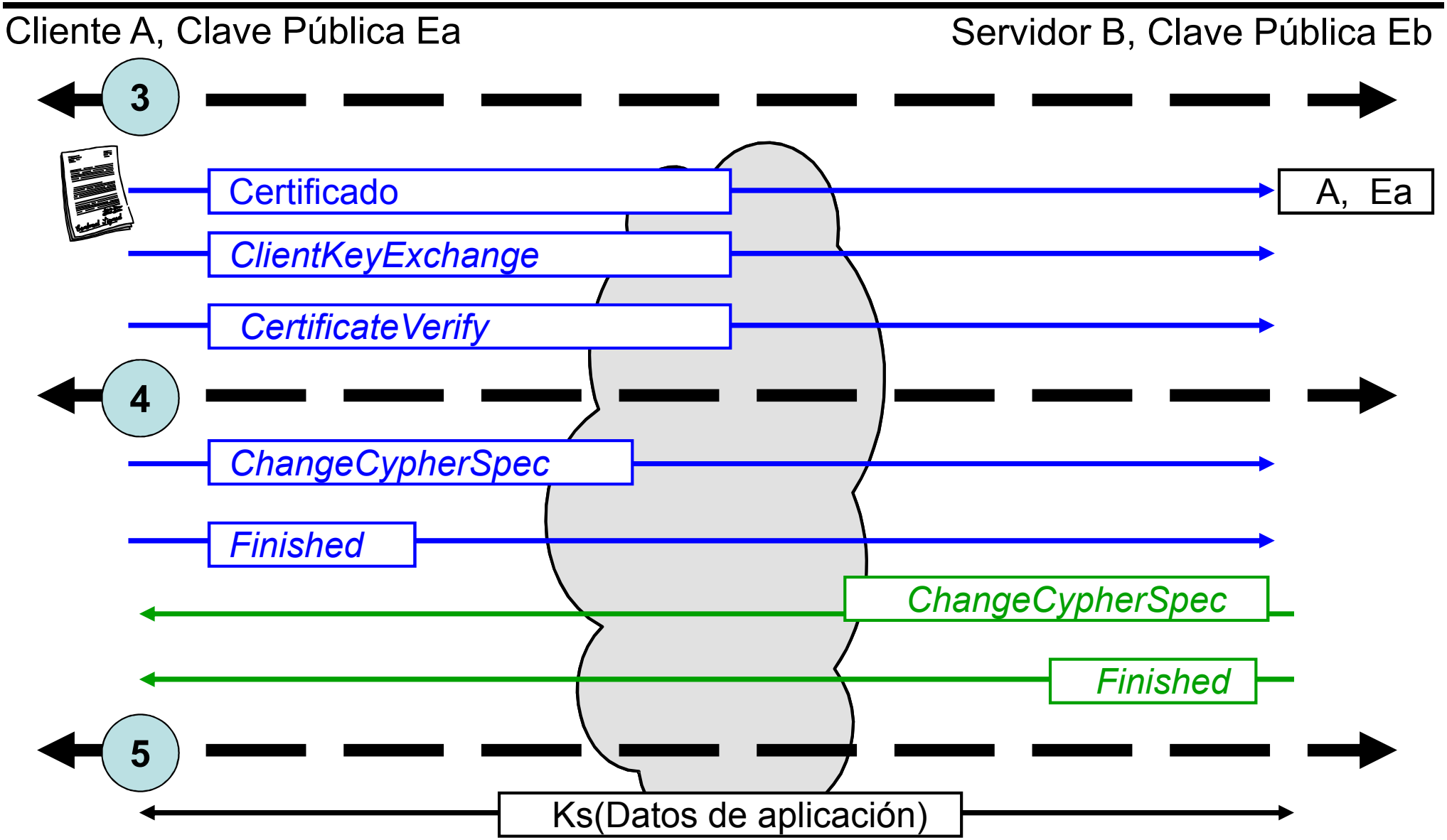
TLS Record Protocol



TLS Handshake Protocol (I)

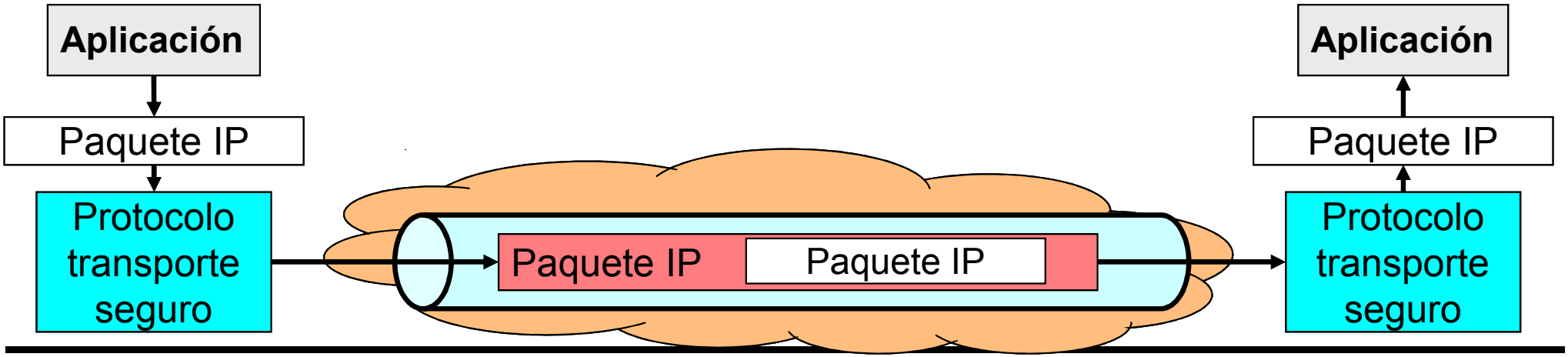


TLS Handshake Protocol (II)



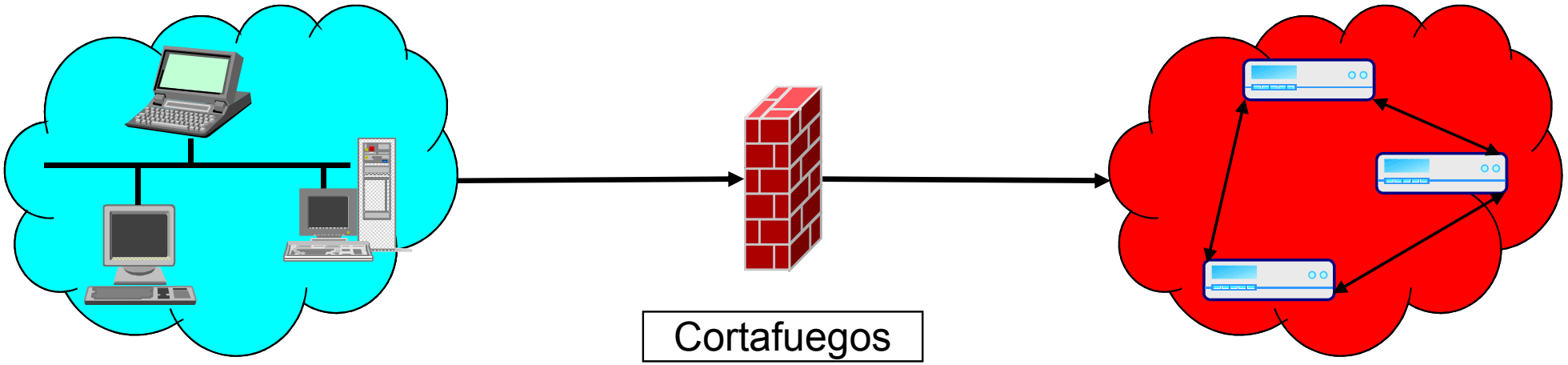
Protocolos seguros: SSH

- *Secure Shell*: Desarrollado para sustituir los programas de acceso remoto nativos de Unix rsh, rcp, rlogin. Actualmente en la versión 2 incluye:
  - Protocolo de transporte SSH. Proporciona autenticación del servidor, confidencialidad e integridad.
  - Protocolo de autenticación del usuario que está en el ordenador cliente, mediante contraseñas o por intercambios basados en cifrado asimétrico.
  - Protocolo de conexión. Permite ejecutar diversas aplicaciones sobre el transporte SSH.
- Permite realizar túneles seguros entre ordenadores para transportar cualquier otro protocolo.



Cortafuegos *(Firewalls)*

- Conjunto de elementos y funciones que se utilizan para garantizar la seguridad en la conexión entre una red controlada por una entidad o usuario, que denominaremos **red segura**, y una red externa no controlada, que denominaremos **red insegura**.
- Controla todas las conexiones externas y el tráfico.
- Hace cumplir la política de seguridad en la conexión.
- Rechaza los ataques y violaciones de la política de seguridad e informa de ellos.

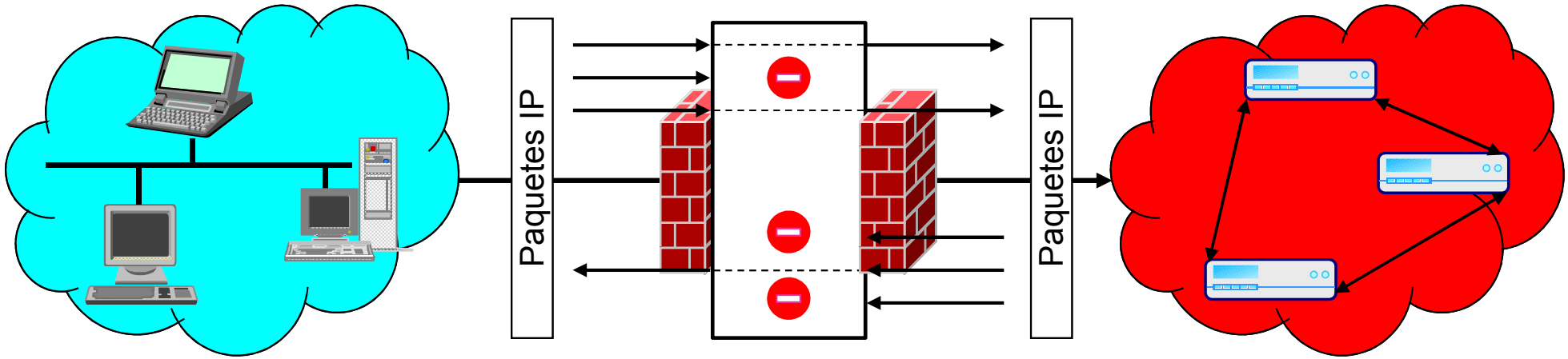


Funciones de un Cortafuegos

- Filtrado de paquetes.
- *Proxy* de aplicación.
- *Proxy* de circuito.
- *Proxy* inverso.
- Traducción de direcciones (NAT).
- Redes virtuales privadas.

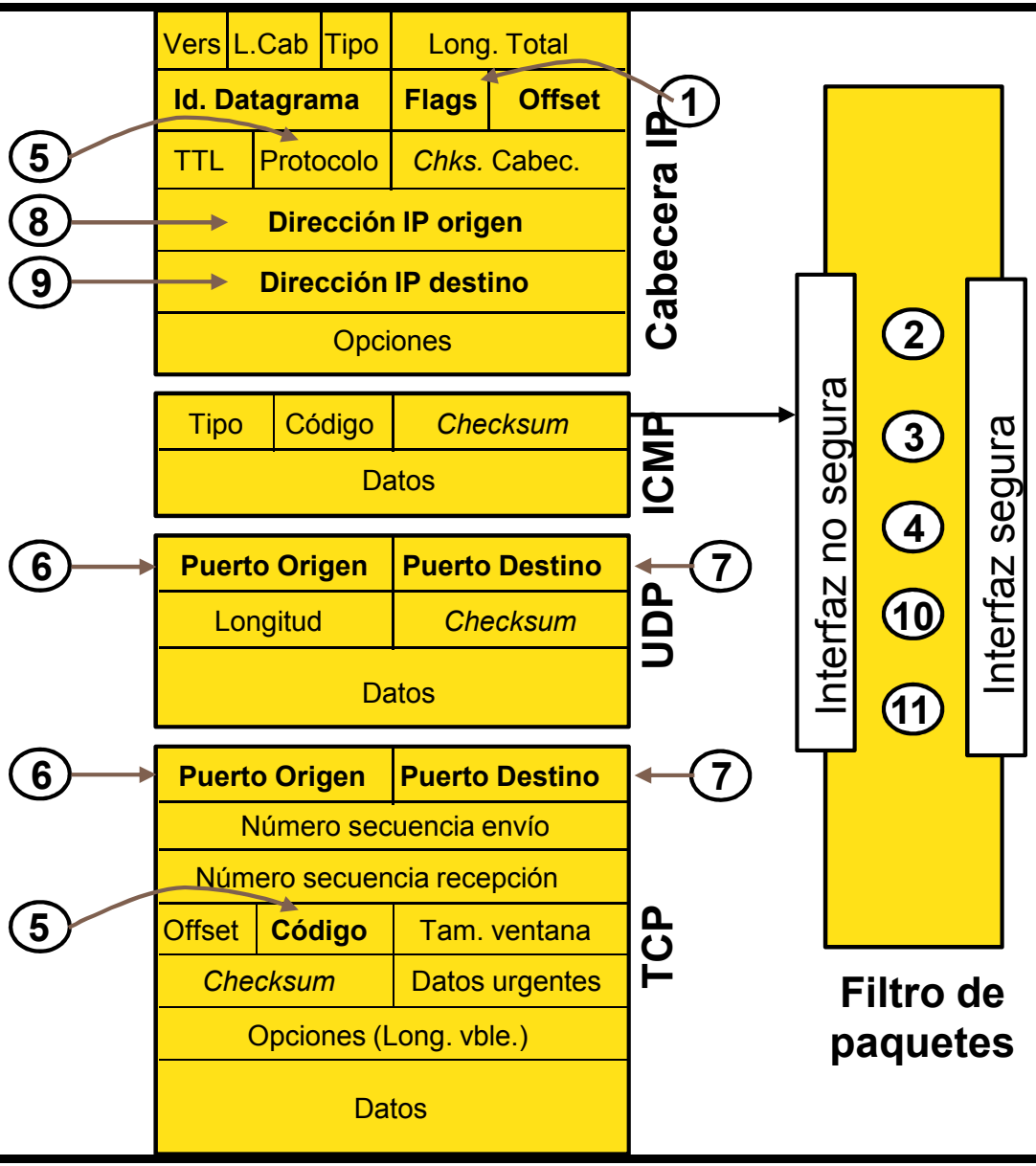
Filtrado de paquetes

- Desactiva el envío de paquetes basado en distintos criterios.
- Características:
  - Acceso transparente, sin interrupciones.
  - Usa y revela las direcciones IP internas.
  - Validación basada en direcciones IP.



Criterios de filtrado

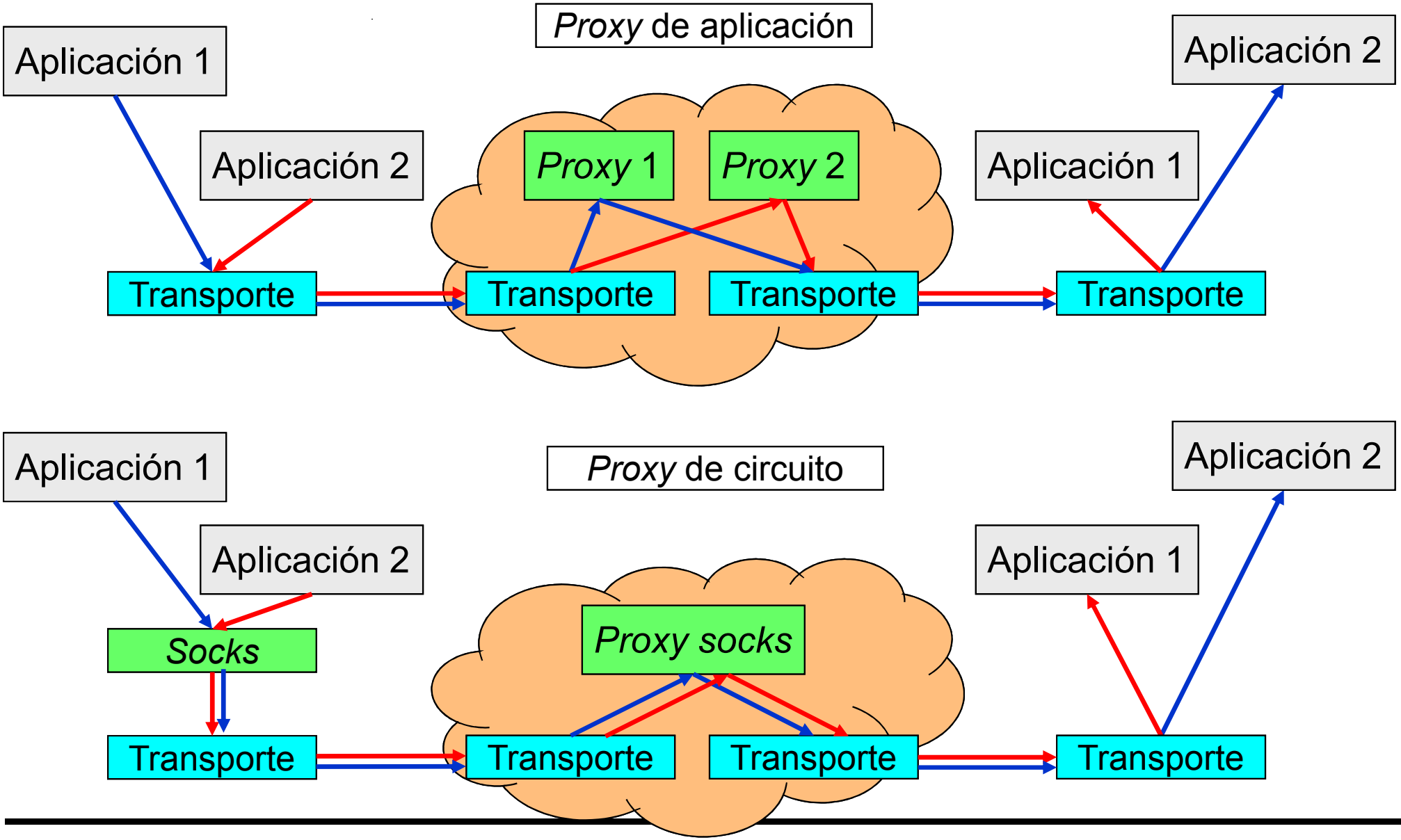
1. Fragmento (comprobar offset).
2. Dirección (entrante, saliente).
3. Local / encaminado.
4. Interfaz (segura / no segura / nombre)
5. Protocolo(TCP, UDP, ICMP, TCP/ACK)
6. Puerto origen.
7. Puerto destino.
8. Dirección origen.
9. Dirección destino.
10. Política de túnel / clave válida.
11. Hora del día, día de la semana, mes.



Pasarelas *(Proxy)*

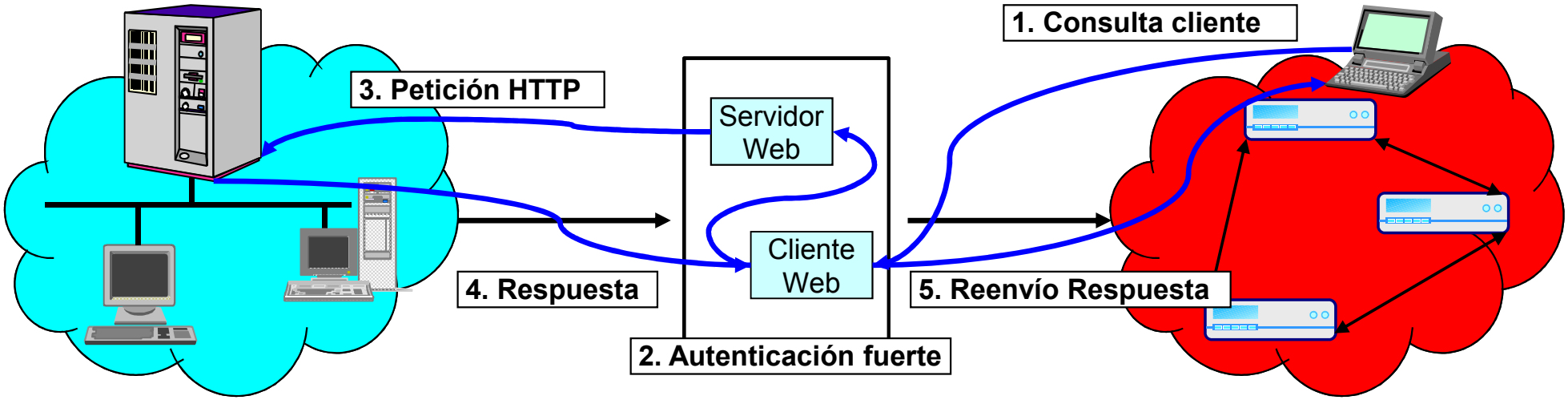
- Servidor interpuesto entre la red segura y la red externa.
- Todo usuario que quiere conectarse a la red externa debe en primer lugar
  - Establecer una conexión con el proxy.
  - Evalúa las peticiones del cliente interno y decide si debe enviarlas o no al exterior.
  - Si las pasa, es el proxy quien habla con el servidor real en lugar del cliente, y devuelve a éste las contestaciones conforme las vaya recibiendo.
- No es transparente al usuario.
- Oculta las direcciones IP internas al exterior.
- Dos tipos de *proxies*:
  - *Proxy* de aplicación.
  - *Proxy* de circuito *(socks)*.

Proxy de aplicación y *Proxy* de circuito *(socks)*



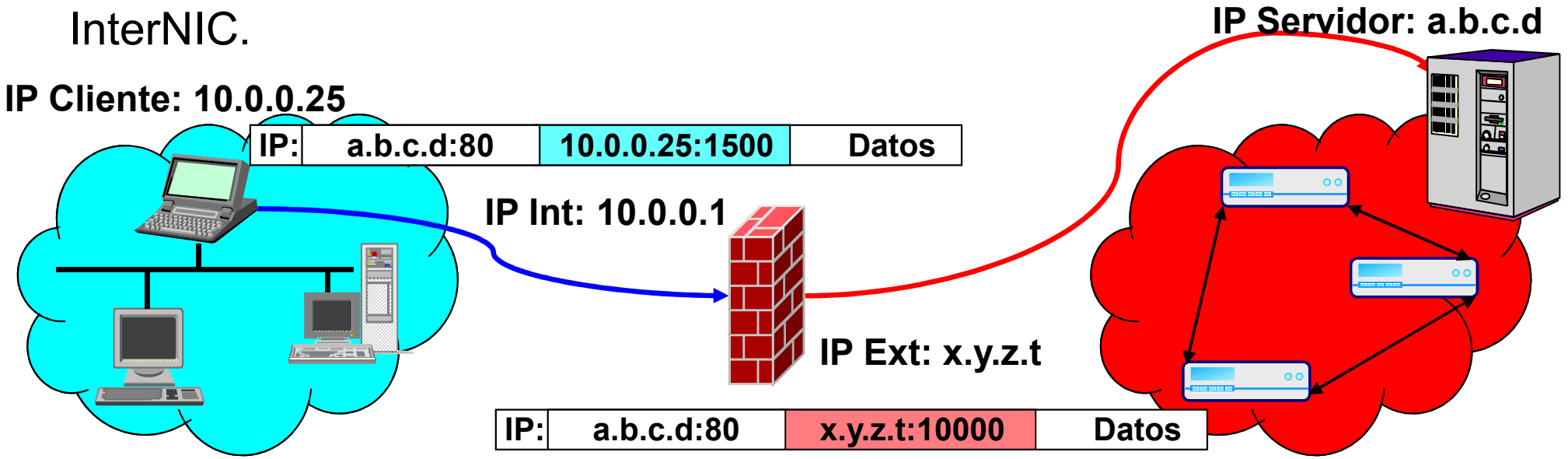
Proxy inverso: Control tráfico entrada

- Pasarela cuyo objetivo es facilitar la conexión desde estaciones de trabajo externas a servidores internos
- Las contraseñas de conexión viajan por la red no segura. Hay que implementar un sistema de autenticación fuerte:



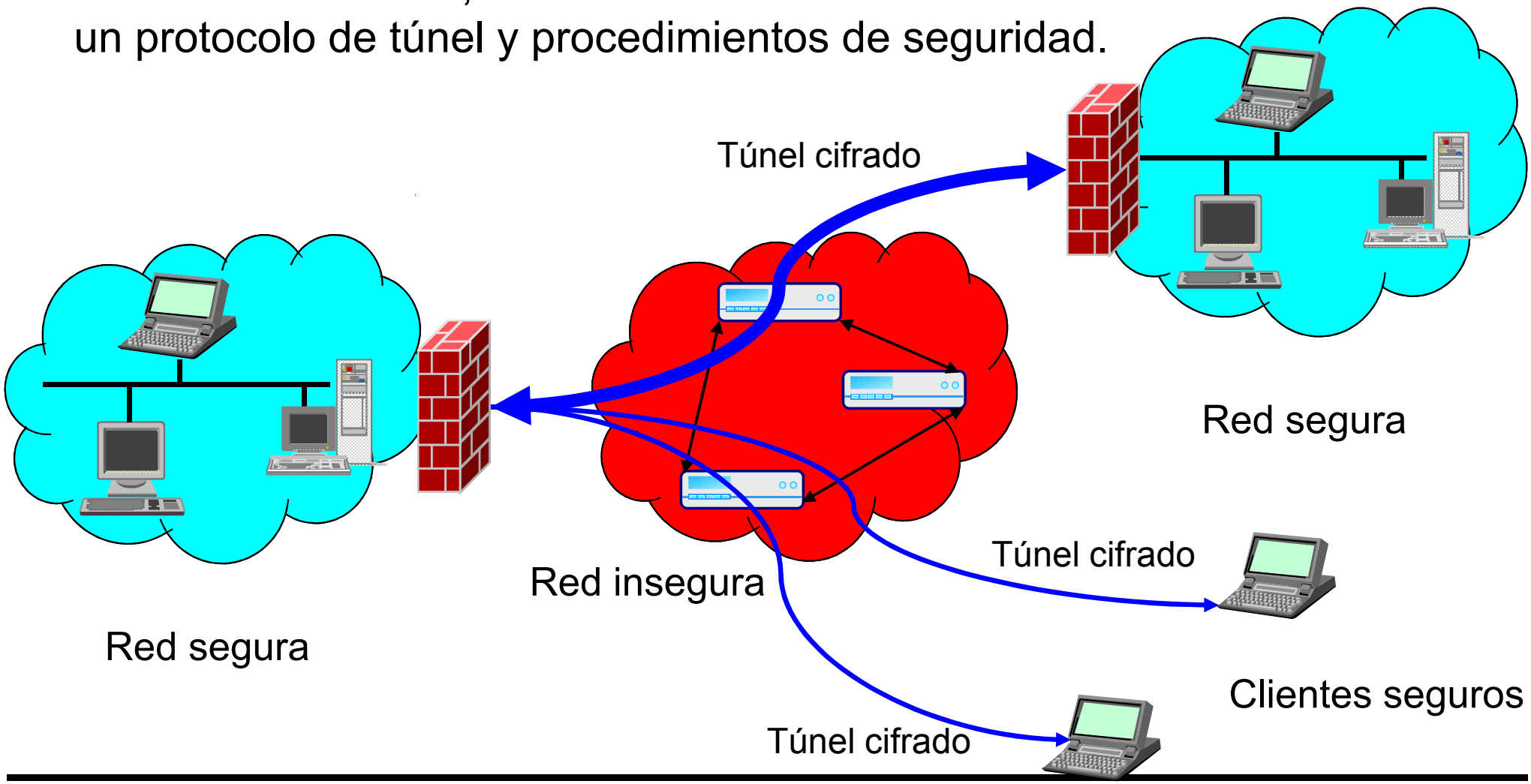
Network Address Translation, NAT

- Traduce direcciones IP internas a direcciones externas.
- Muchos ordenadores de la red interna pueden compartir una única dirección externa.
  - Asignación IPCliente:PuertoCliente -> IPNAT:PuertoNat.
- Las direcciones internas no se revelan a la Internet.
- Permite acceso de LANs a Internet sin tener direcciones registradas InterNIC.

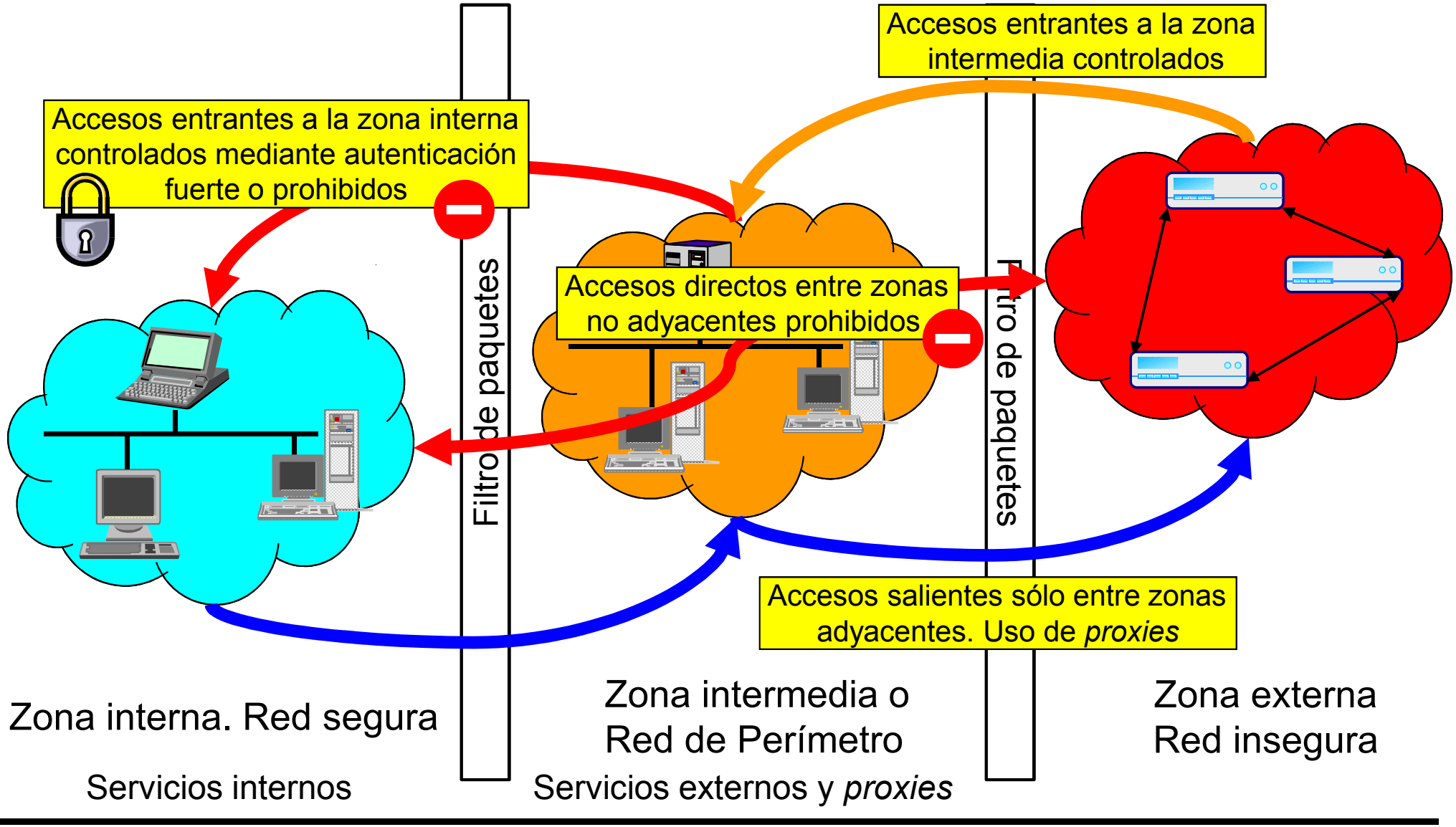


Redes Virtuales Privadas

- Red privada de datos que hace uso de una infraestructura pública de telecomunicaciones, manteniendo la confidencialidad mediante el uso de un protocolo de túnel y procedimientos de seguridad.



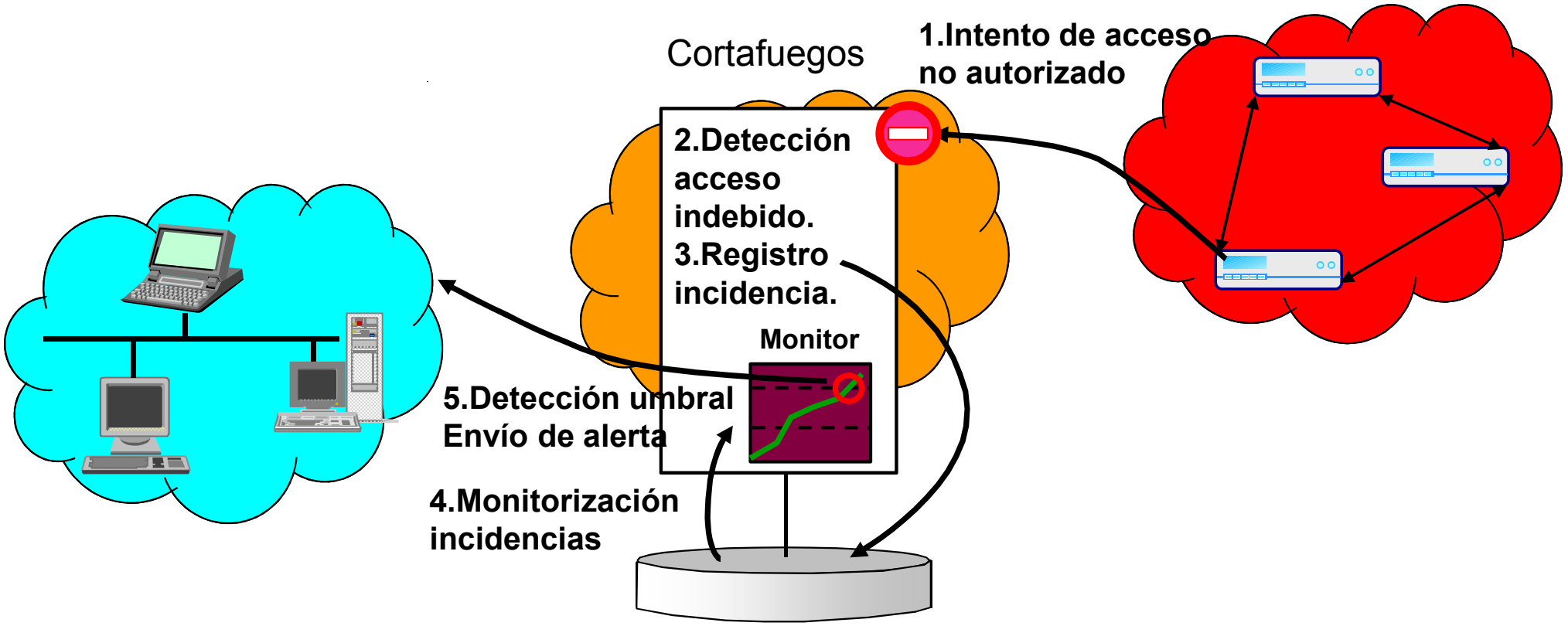
Arquitectura de seguridad perimetral en redes



Sistemas de detección de intrusiones
(Intrusion Detection Systems, IDS)

- Es imposible predecir y contener todas las posibles vulnerabilidades.
  - Es imprescindible implantar herramientas que intenten detectar cualquier intento, satisfactorio o fallido, de un incidente de seguridad.
- Las herramientas de detección deben ir acompañadas siempre de reacciones ante los incidentes que se detecten, automáticos o manuales.
  - Procedimientos con pruebas periódicas y entrenamiento de operadores.
- Estos sistemas no son totalmente fiables. Su fiabilidad se mide por:
  - El ratio de incidentes no descubiertos (falsos negativos).
  - El ratio de incidentes falsos detectados (falsos positivos).
- Técnicas empleadas:
  - Análisis de los registros de actividad.
  - Análisis del tráfico entrante.
  - Control de la integridad del sistema.
  - Antivirus.
  - “Tarros de miel” *(honeypots)* y alarmas antirrobo *(burglar alamrs)*.
  - Auditorías internas de seguridad.
  - Análisis forense.

Análisis de registros de actividad



Auditorías de seguridad (I)

- Auditoría de seguridad: Rastreo periódico del cortafuegos y de otros servidores críticos.
  - En la evaluación inicial del sistema de protección instalado.
  - Periódicamente, para comprobar su correcto mantenimiento.
- El auditor se convierte en un presunto intruso y trata de realizar ataques conocidos al sistema *(hacking ético)* con dos tipos de herramientas:
  - Rastreadores internos: realizan las comprobaciones desde dentro de los sistemas expuestos.
    - Permisos incorrectos de los archivos.
    - Existencia de usuarios sin contraseña.
    - Análisis de debilidades de las contraseñas.
    - Falta de aplicación del nivel correcto de parches.
    - Utilización de servicios vulnerables.
    - ...

Auditorías de seguridad (II)

- Rastreadores de red: realizan las comprobaciones desde accesos externos al sistema.
  - Existencia de servicios inseguros: *rlogin, rsh, tftp*...
  - Existencia de servicios de información que proporcionen datos del sistema: *finger, snmp*…
  - Respuestas a sondas ICMP.
  - Intentos de acceso a servicios estándar (como ftp, telnet...) utilizando usuarios y contraseñas de configuración habitual (por ejemplo, contraseña igual al nombre de usuario).
  - Vulnerabilidades de los servicios descubiertos:
    - Problemas de desbordamiento de buffer.
    - Posibilidad de realizar ataque de denegación de servicio.
    - ...

Análisis forense

- Análisis forense: procedimientos, técnicas y herramientas con el objetivo de investigar un presunto delito informático o incumplimiento normativo dentro de la compañía.
- Búsqueda de evidencias digitales.
  - Admisibles, auténticas, completas, confiables y creíbles.
  - Capturar imágenes del sistema.
  - Evitar la manipulación y alteración de los datos originales.
    - No ejecutar programas en el ordenador afectado.
  - Registrar todas las actuaciones del análisis forense.
  - Actuar siempre con conocimiento técnico.
  - Cumplir las normativas de seguridad de la organización y legales.
  - Actuar con celeridad.
  - Priorizar el análisis de los datos volátiles frente a los estáticos.
  - Documentar exhaustivamente para el testimonio.
  - Asegurar que las acciones son reproducibles.

Seguridad de los equipos HW y SW

- El último nivel de seguridad debe basarse en los elementos de proceso.
- Los sistemas expuestos deben someterse a un proceso de fortalecimiento en la seguridad para convertirse en servidor “bastión”.
  - Empleo de sistemas de seguridad certificada. Criterios Comunes.
  - Sencillez. Principio *KISS: Keep It Simple, Stupid!*
    - Configuración correcta del servidor y aplicaciones que ejecuta.
      - Política por defecto: todo prohibido. Permisos explícitos.
    - Eliminar todos los programas no imprescindibles
      - No sólo parar servicios: desinstalar los ejecutables.
  - Actualizar los sistemas a los últimos niveles de modificaciones disponibles.
  - Utilizar programas altamente estables y probados.
  - Realizar un plan adecuado de copias de respaldo.
  - Registro completo de actividad

Bibliografía especial del tema

- CARRACEDO, J., *Seguridad en redes telemáticas*, McGraw-Hill, 2004
- CHAPMAN, D. Brent and ZWICKY, Elizabeth D., *Building Internet Firewalls*, Sebastapol (CA), O'Reilly, 2000. 2ª ed.
- CHESWICK, William R. and BELLOVIN, Steven M., *Firewalls and Internet Security: Repelling the Wily Hacker*, Reading (MA), Addison-Wesley, 1994.
- GARFINKEL, S. and SPAFFORD, G., *Practical Unix and Internet Security*, Sebastapol (CA), O'Reilly, 1996. 2ª ed.
- MENEZES, A. J., VAN OORSCHOT, P. C. y VANSTONE, S. A., *Handbook of Applied Cryptography*, CRC Press, octubre 1996. URL: http://osi.ugm.ac.id/download/docs/
  kriptogafi-www.cacr.math.uwaterloo.ca/
- National Institute of Standards and Technology (NIST), *An Introduction to Computer Security: The NIST Handbook*, Special Publication 800-12, October 1995. http://csrc.nist.gov/publications/nistpubs/800-12/.

Bibliografía especial del tema

- OCDE, *Recomendación relativa a las directrices para la seguridad de sistemas y redes de información*, www.csi.map.es/csi/pdf/OCDE_directrices_esp.PDF.
- RSA Labs, *Frequently Asked Questions About Today's Cryptography*, Version 4.1, 2000.
  URL: http://www.rsasecurity.com/rsalabs/faq/index.html.
- SCHNEIER, B., *Secrets & Lies. Digital Security in a Networked World*, Wiley, 2000.
- SCHNEIER, B., *Applied Cryptography. Protocols, Algorithms and Source Code in C*, Wiley, 1996. 2ª ed.
- STALLINGS, W., *Fundamentos de seguridad en redes. Aplicaciones y Estándares*, Prentice-Hall, 2003. 2ª ed.
- TANENBAUM, A., *Computer Networks*, Prentice-Hall, 1996. 3ª ed.
- TANENBAUM, A., *Computer Networks*, Prentice-Hall, 2002. 4ª ed.