

Seguridad Informática.

3º - Grado en Ingeniería Informática
José Manuel Sáiz Diez – jmsaiz@ubu.es



Formato del Documento.

1. Teoría de Seguridad.

1. Introducción a la información (3).
2. Planes de Seguridad (23).
3. Seguridad física (41).
4. Principios de Seguridad (46).
5. Introducción a la criptografía (69).
6. Certificados y autoridades de certificación (96).

Nota: Nos centramos en la información pero se hará extensible a todos los posibles campos.



1. Introducción a la información.

■ Índice.

- ¿Qué es la información.
- La información en la empresa.
- Importancia de la información.
- Vulnerabilidad de la información.
- Disminuir las vulnerabilidades.
- Acciones contra los datos.
- Protección de los datos.
- Hackers y crackers.
- ¿Dónde está el enemigo?.
- ¿El enemigo está en casa?.
- Delitos informáticos.
- Algunos delitos informáticos.
- Algunas medidas básicas de prevención contra los virus.
- ¿Qué hacer en caso de estar infectado?.



¿Qué es la información?.



■ El concepto en ingeniería:

- Estudio de las estadísticas y características del lenguaje que nos permitirá su análisis desde un punto de vista matemático, científico y técnico.

■ El concepto en la empresa:

- Conjunto de datos propios que se gestionan y mensajes que se intercambian personas y/o máquinas dentro de una organización.



La información en la empresa.

Se entenderá como:

Todo el conjunto de datos.

Todos los mensajes intercambiados.

Todo el historial de clientes y proveedores.

Todo el historial de productos, ... etc.

En definitiva, el *know-how* de la organización.

Si esta información se pierde o deteriora, le será muy difícil a la empresa recuperarse y seguir siendo competitiva ⇒ políticas de seguridad.



Importancia de la información.

El éxito de una empresa dependerá de la calidad de la información que genera y gestiona.

Diremos entonces que una empresa tiene una información de **calidad** si ésta presenta, entre otras características: **confidencialidad, integridad y disponibilidad**.

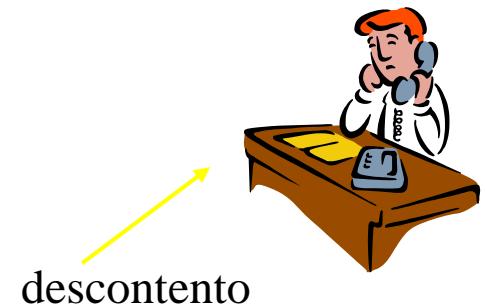
La implantación de unas medidas de seguridad informática en la empresa comienza a tener un peso específico en este sector sólo a finales de la década de los 80.



Vulnerabilidad de la información.

La información (datos) se verá afectada por muchos factores, incidiendo básicamente en los aspectos de confidencialidad, integridad y disponibilidad de la misma.

Desde el punto de vista de la empresa, uno de los problemas más importantes puede ser el que está relacionado con el delito o crimen informático, por factores externos e internos.



descontento

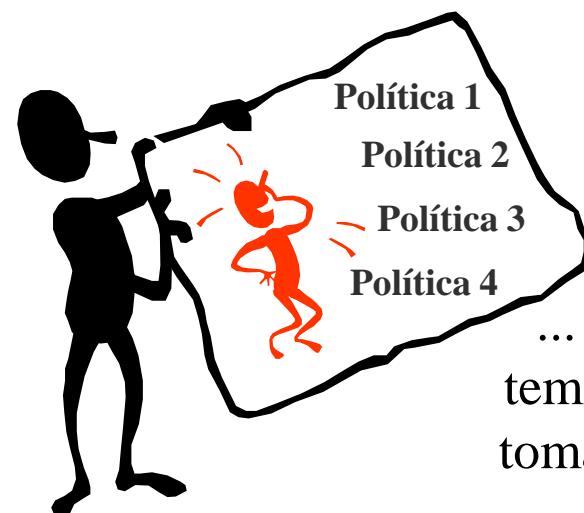


Disminuir las vulnerabilidades.

Esto se verá agravado por otros temas, entre ellos los aspectos legales y las características de los nuevos entornos de trabajo de la empresa del siglo XXI.

Solución ?

La solución es sencilla: aplicar técnicas y políticas de seguridad...



... sólo ahora el tema comienza a tomarse en serio.



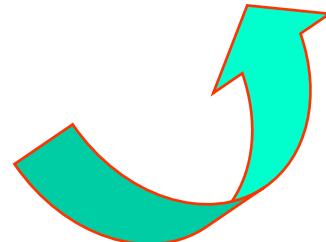
Acciones contra los datos.

■ Una persona no autorizada podría:

- Clasificar y desclasificar los datos.
- Filtrar información.
- Alterar la información.
- Borrar la información.
- Usurpar datos.
- Hojear información clasificada.
- Deducir datos confidenciales.



**Deberemos
proteger
nuestros datos**



Protección de los datos.

- La medida más eficiente para la protección de los datos es determinar una buena política de copias de seguridad o backups:
 - Copia de seguridad completa
 - ✗ Todos los datos (la primera vez).
 - Copias de seguridad incrementales
 - ✗ Sólo se copian los ficheros creados o modificados desde el último backup.
 - Elaboración de un plan de backup en función del volumen de información generada
 - ✗ Tipo de copias, ciclo de esta operación, etiquetado correcto.
 - ✗ Diarias, semanales, mensuales: creación de tablas.



Hackers y Crackers.

Algunas definiciones

Hacker:

Definición inicial de los ingenieros del MIT que hacían alardes de sus conocimientos en informática.

Pirata Informático.

Cracker:

Persona que intenta de forma ilegal romper la seguridad de un sistema por diversión o interés.

No existe uniformidad de criterios...



¿Dónde está el enemigo?

Las empresas relacionadas con las Nuevas Tecnologías de la Información NTIs hacen uso de varias técnicas y herramientas de redes para el **intercambio de datos**:

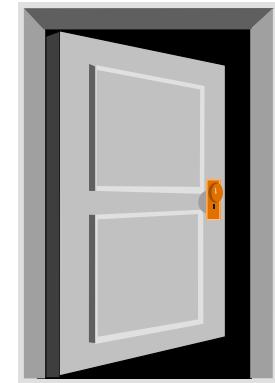
- Transferencia de ficheros (ftp)
- Transferencia de datos e información a través de Internet (http)
- Conexiones remotas a máquinas y servidores (telnet)

Todo esto presentará graves riesgos de ataques de hackers y otros delincuentes informáticos, **pero ...**

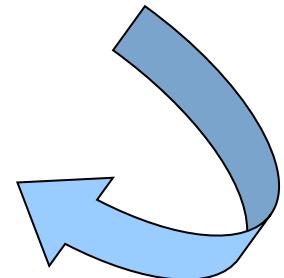


¿El enemigo está en casa?

Por muy organizados que puedan estar estos grupos de vándalos, hay que ponerse en el lugar que nos corresponde y no caer en la paranoia. Y además debemos pensar que el peor enemigo bien puede estar dentro de casa...



La solución sigue siendo la misma: la puesta en marcha de una adecuada **política de seguridad** en la empresa.



Delitos informáticos.

Son acciones que vulneran la confidencialidad, integridad y disponibilidad de la información.

Ataques a un sistema informático:

- | | | |
|----------------|---------------------|---------------|
| 👉 Fraude | 👉 Malversación | 👉 Robo |
| 👉 Sabotaje | 👉 Espionaje | 👉 Chantaje |
| 👉 Revelación | 👉 Mascarada | 👉 Virus |
| 👉 Gusanos | 👉 Caballos de Troya | |
| 👉 Phishing | 👉 Spyware | 👉 Bluejacking |
| 👉 Hijacking... | etc. | |



Algunos delitos informáticos.

Fraude

Acto deliberado de manipulación de datos perjudicando a una persona física o jurídica que sufre de esta forma una pérdida económica. El autor del delito logra de esta forma un beneficio normalmente económico.

Sabotaje

Acción con la que se desea perjudicar a una empresa entorpeciendo deliberadamente su marcha, averiando sus equipos, herramientas, programas, etc. El autor no logra normalmente con ello beneficios económicos pero pone en jaque mate a la organización.



Algunos delitos informáticos (2).

Chantaje

Acción que consiste en exigir una cantidad de dinero a cambio de no dar a conocer información privilegiada o confidencial y que puede afectar gravemente a la empresa, por lo general a su imagen corporativa.

Mascarada – Enmascaramiento – Suplantación – Spoofing

Utilización de una clave por una persona no autorizada y que accede al sistema suplantando una identidad. De esta forma el intruso se hace dueño de la información, documentación y datos de otros usuarios con los que puede, por ejemplo, chantajear a la organización.



Algunos delitos informáticos (3).

Virus

Código diseñado para introducirse en un programa, modificar o destruir datos. Se copia automáticamente a otros programas para seguir su ciclo de vida. Es común que se expanda a través de plantillas, las macros de aplicaciones y archivos ejecutables.

Gusanos

Virus que se activa y transmite a través de la red. Tiene como finalidad su multiplicación hasta agotar el espacio en disco o RAM. Suele ser uno de los ataques más dañinos porque normalmente produce un colapso en la red (p.e. el gusano de Internet de Robert Morris Jr.).



Algunos delitos informáticos (4).

Caballos de Troya

Virus que entra al ordenador y posteriormente actúa de forma similar a este hecho de la mitología griega. Así, parece ser una cosa o programa inofensivo cuando en realidad está haciendo otra y expandiéndose. Ejemplo: el huevo de Pascua de Windows 95.

Software Espía - Spyware

Aplicaciones que **recopilan información**, a veces con fines publicitarios.



Algunos delitos informáticos (5).

Phishing

Una estafa que utiliza mecanismos electrónicos, como puede ser un mensaje de correo electrónico o una página web, para **convencer al usuario que revele información sensible (información confidencial)**, que va desde datos personales y privados hasta las credenciales de acceso a servicios.

Bluejacking

Enviar **mensajes no deseados** entre dispositivos Bluetooth.



Algunos delitos informáticos (6).

Hijacking

Un término general que incluye toda técnica para **apoderarse de algo** como sesiones, etc...

Y hay muchos más delitos. Incluso aparecerán nuevos delitos y ataques a los sistemas informáticos y redes que a fecha de hoy no sabemos cómo serán ni qué vulnerabilidad atacarán... Este enfrentamiento entre el “bien” y el “mal” es inevitable en un sistema abierto ... y las comunicaciones hoy son así.



Algunas medidas básicas de prevención contra los virus.

Proteger los disquetes/Pendrive con la pestaña.

Es una protección tipo hardware elemental.

Escanear de vez en cuando el disco duro (por ejemplo una vez al día) y siempre los disquetes y otro tipo de elementos extraíbles.

Usar software con licencia.

Controlar el acceso de extraños al disco duro.

Instalar un antivirus.

Dejarlo en modo residente y actualizar la versión al menos una vez al mes a través de Internet.

Ser cuidadoso con todo aquello que resulte sospechoso (correos, etc.).



¿Qué hacer en caso de estar infectado?.

- Detener las conexiones remotas.
- No mover el ratón ni activar el teclado.
- Apagar el sistema.
- Arrancar con un disquete de arranque o emergencia limpio y ejecutar un programa antivirus.
- Hacer copia de seguridad de ficheros del sistema.
- Formatear el disco duro a bajo nivel si no queda otra solución ☹.
- Instalar nuevamente el sistema operativo y restaurar las copias de seguridad.



2. Planes de Seguridad.

■ Índice.

- Seguridad Lógica-Física.
- Análisis de riesgos.
- Efectividad del coste.
- Políticas de seguridad.
 - ✗ Políticas administrativas.
 - ✗ Políticas de control de acceso.
 - ✗ Políticas de control de flujo.
- Vandalismo informático y su prevención.
- ¿Y si se produce una catástrofe?.
- Importancia de contar con un plan.
 - ✗ Pérdidas por no contar con un plan.
 - ✗ Tiempo de recuperación ante desastres.
- Plan de continuidad.
 - ✗ Ejemplo parcial.
- Planes de contingencia.
 - ✗ Implantación de medidas del Plan de Contingencia (Subplanes).



Seguridad Lógica-Física.

Los datos deben protegerse aplicando:

- Seguridad Lógica
 - Uso de herramientas de protección de la información en el mismo medio en el que se genera o transmite.
- Seguridad Física
 - Procedimientos de protección física del sistema (incendios, agua, terremotos, etc.).
- Medidas de prevención de riesgos tanto físicos como lógicos.



Ref.: <http://www-5.ibm.com/es/press/informes/bcrs.html>
Fuente: IBM



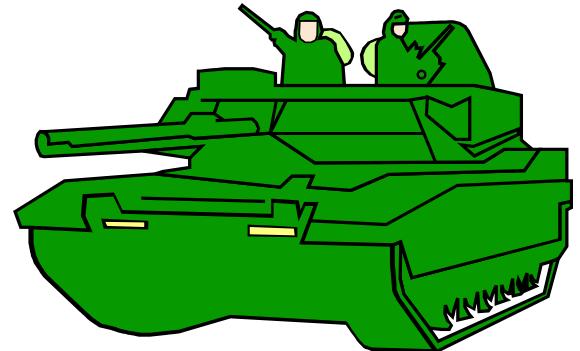
Análisis de riesgos.

- Proceso de identificación y evaluación del riesgo a sufrir un ataque y perder datos, tiempo y horas de trabajo, comparándolo con el costo de la prevención de esta pérdida.
- Su análisis no sólo lleva a establecer un nivel adecuado de seguridad: permite conocer mejor el sistema que vamos a proteger.



Efectividad del coste.

- El control ha de tener menos coste que el valor de las pérdidas debido al impacto del riesgo temido si éste se produce.
- Ley básica: el coste del control ha de ser menor que el activo que protege.



Políticas de seguridad.

Políticas administrativas

Procedimientos administrativos.

Políticas de control de acceso

Privilegios de acceso del usuario o programa.

Políticas de flujo de información

Normas bajo las cuales se comunican los sujetos dentro del sistema.



Políticas administrativas.

Políticas administrativas

Se establecen en la organización aquellos procedimientos de carácter administrativo.

Por ejemplo en el desarrollo de programas: modularidad en aplicaciones, revisión sistemática, etc.



Políticas de Control de Acceso.

Políticas de control de acceso

Política de menor privilegio

Acceso estricto a objetos determinados

Política de compartición

Acceso de máximo privilegio

Granularidad

Número de objetos accesibles (gruesa y fina)



Políticas de control de flujo.

Políticas de control de flujo

La información a la que se accede se envía por

¿Canales lícitos o canales ocultos?

¿Qué es lo que hay que potenciar?

¿La confidencialidad?

¿La integridad?

¿La disponibilidad?

⇒ Diferencias según organización

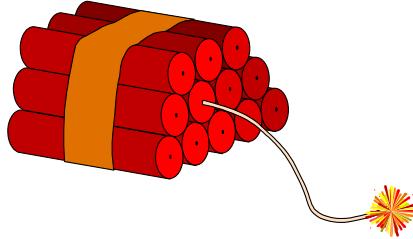


Vandalismo informático y su prevención.

■ Actuaciones intencionadas

- Terrorismo
- Sabotaje
- Robo

- Virus
- Programas malignos



■ Medidas de prevención

- ◆ Entradas fortificadas
- ◆ Guardia Jurado
- ◆ Patrullas
- ◆ Circuito cerrado TV
- ◆ Control de accesos
- ◆ Protección de software y hardware con un antivirus.



¿Y si se produce una catástrofe?.

■ Dependencias críticas:

- Las empresas dependen hoy en día de los equipos informáticos y de los datos que hay allí almacenados.
- Dependen también cada vez más de las comunicaciones a través de redes de datos.

Si falla el sistema informático y no puede recuperarse, la empresa puede desaparecer.



Importancia de contar con un plan.

- Además de seguridad, la empresa gana en conocimiento real de sus fortalezas y debilidades.
- Si no lo hace se expone a sufrir una pérdida irreparable mucho más costosa que la implantación de este plan.



Pérdidas por no contar con un plan.

- Pérdida de clientes
- Pérdida de imagen
- Pérdida de ingresos por beneficios
- Pérdida de ingresos por ventas y cobros
- Pérdida de ingresos por producción
- Pérdida de competitividad
- Pérdida de credibilidad en el sector



Tiempo de recuperación ante desastres.

■ Período máximo de paro de una empresa sin poner en peligro su supervivencia:

- Sector Seguros: 5,6 días
- Sector Fabricación: 4,9 días
- Sector Industrial: 4,8 días
- Sector Distribución: 3,3 días
- Sector Financiero: 2,0 días

Ref. *Estudio de la Universidad de Minnesota*

¿Y en la enseñanza?... ¿Y en la administración?.....



Plan de continuidad (*Business Continuity Plan - BCP*).

- **Marco conceptual, que integra el alcance y objetivos de los siguientes enfoques:**
 - Plan de Recuperación de Desastres - Disaster Recovery Planning (DRP): El DRP se enfoca en la recuperación de los servicios de TI y los recursos, dado un evento que ocasionara una interrupción de grandes proporciones en su funcionamiento.
 - Plan de Contingencia - Contingency Planning (CP): El CP se enfoca en la recuperación de los servicios y recursos de TI después de un desastre de dimensiones mayores o de una interrupción menor. Especifica los protocolos y procedimientos para la recuperación tanto en áreas de la empresa como las ajenas.
 - Plan de Reanudación de Negocios - Business Resumption Planning (BRP): El BRP se centraliza en la reanudación de los procesos de negocios afectados por un fallo en las aplicaciones de TI. Se enfoca en la utilización de procedimientos relacionados con el área de trabajo.
 - Plan de Continuidad de las Operaciones - Continuity of Operations Planning (COOP): El COOP busca la recuperación de las funciones estratégicas de una organización que son desempeñadas en sus instalaciones corporativas.
 - Plan de Respuesta ante Emergencias - Emergency Response Planning (ERP): Su objetivo es el de salvaguardar, a los empleados, público, ambiente y a los activos de la empresa. Se busca llover la situación de crisis de manera inmediata a un estado de control.



Ejemplo parcial de Plan de Continuidad (Business Continuity Plan - BCP).

■ ...

■ **Instalaciones alternativas**

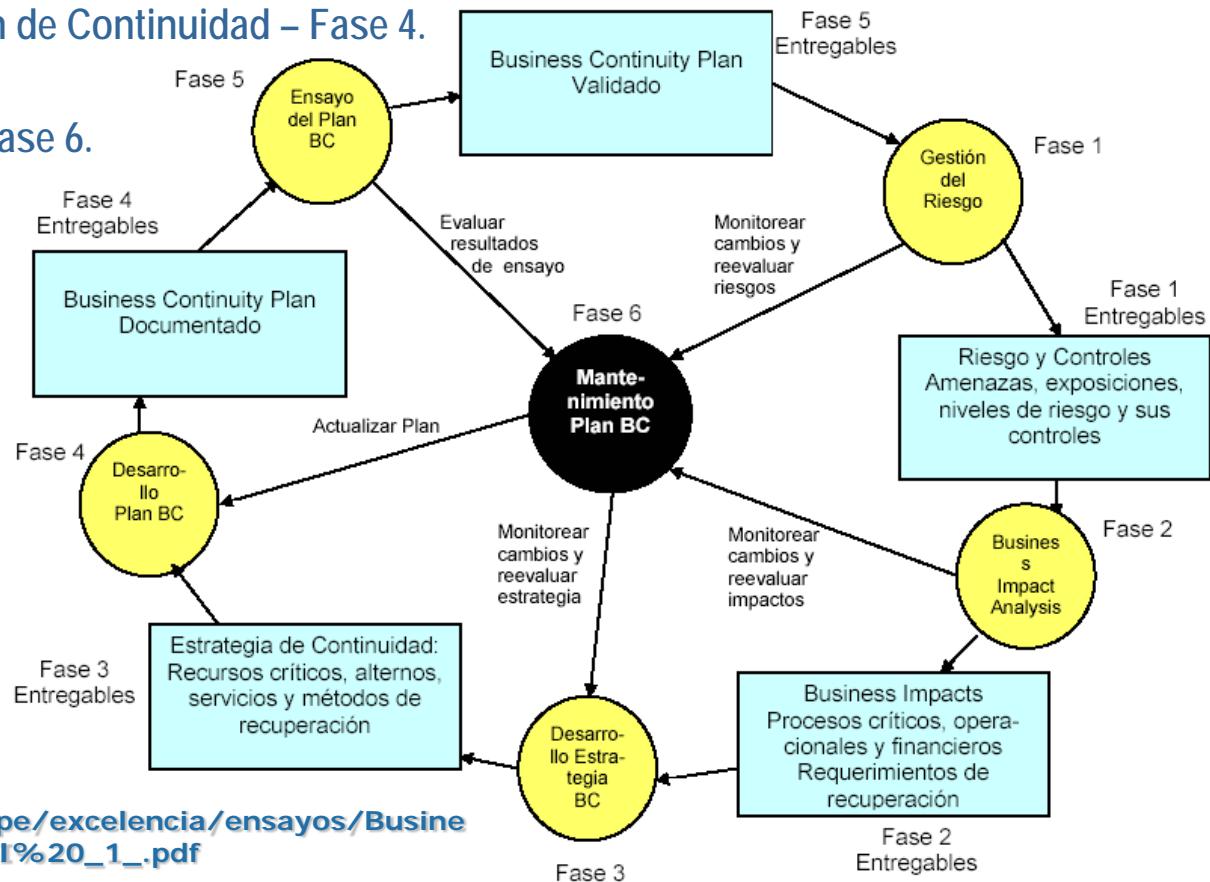
- Oficina de servicios propia
- Acuerdo con empresa vendedora hardware
- Acuerdo recíproco entre dos o más empresas
- Arranque en frío; sala vacía propia
- Arranque en caliente: centro equipado
- Sistema Up Start: caravana, unidad móvil
- Sistema Hot Start: centro gemelo



Implantación de medidas del Plan de Continuidad.

■ Previo al Plan de Continuidad:

- Análisis de riesgos, debilidades e impacto – Fases 1 y 2.
- Desarrollo de estrategias (requerimientos y opciones) – Fase 3.
- Desarrollo del Plan de Continuidad – Fase 4.
- Ensayos – Fase 5.
- Mantenimiento – Fase 6.



Ref.:

http://www.centrum.pucp.edu.pe/excelencia/ensayos/Business%20Continuity%20Plan%20III%20_1_.pdf

Planes de contingencia.

¿Qué es un Plan de Contingencia?

- Recursos, Personas, Responsabilidades, Protocolos o Procedimientos.

¿Por qué es necesario implementarlo?

¿Qué gana la empresa con este plan?

Y si no lo tiene ¿a qué se expone?



Implantación de medidas del Plan de Contingencia (Subplanes).

- **El plan de respaldo.** Contempla las contramedidas preventivas antes de que se materialice una amenaza. Su finalidad es evitar dicha materialización.
 - Previo al Plan de Continuidad:
 - ✗ Asignación de responsabilidades.
 - ✗ Análisis de riesgos, debilidades e impacto.
 - ✗ Desarrollo de estrategias (requerimientos y opciones).
 - ✗ Discusión de procedimientos.
 - Mantenimiento: Revisión periódica de Protocolos y Procedimientos.
- **El plan de emergencia.** Contempla las contramedidas necesarias durante la materialización de una amenaza, o inmediatamente después. Su finalidad es paliar los efectos adversos de la amenaza.
 - Vidas, heridos, activos, evacuación personal
 - Inventariar recursos siniestrados
 - Evaluar el coste de la inactividad
- **El plan de recuperación.** Contempla las medidas necesarias después de materializada y controlada la amenaza. Su finalidad es restaurar el estado de las cosas tal y como se encontraban antes de la materialización de la amenaza.



3. Seguridad Física.

■ Índice.

- Seguridad Física en entornos de PCs.
- Desastres naturales y su prevención.
- Amenazas del agua y su prevención.
- Amenazas del fuego y su prevención.



Seguridad Física en entornos de PCs.

- Anclajes a mesas de trabajo.
- Cerraduras.
- Tarjetas con alarma.
- Bloqueo de disquetera.
- Protectores de teclado.
- Tarjeta de control de acceso al hardware.

- Etiquetas con adhesivos especiales.

- Suministro ininterrumpido de corriente.
- Toma de tierra.
- Eliminación de la estática... etc.

Temas a tener
en cuenta en un
entorno PC



Desastres naturales y su prevención.

■ Desastres naturales

- Huracán
- Tormenta
- Inundación
- Tornado
- Vendaval, etc

✗ Destruyen nuestro sistema

■ Medidas prevención

- ◆ Emplazamientos adecuados
- ◆ Protección fachadas, ventanas, puertas



Amenazas del agua y su prevención.

- Inundaciones por causas propias de la empresa
- Inundaciones por causas ajenas
- Pequeños incidentes personales (botella de agua, taza con café)

■ **Medidas prevención**

- ◆ Revisar conductos de agua
- ◆ Localizar la sala con los equipos más caros en un sitio libre de estos problemas
- ◆ Instalar sistemas de drenaje emergencias



Amenazas del fuego y su prevención.

- Debido a una mala instalación eléctrica
- Debido a descuidos (fumar en la sala de ordenadores)
- Papeleras mal ubicadas (se tira un cigarrillo no apagado)
- Problemas de humo

■ Medidas prevención

- ◆ Detector humo y calor
- ◆ Materiales ignífugos
- ◆ Almacén de papel separado de máquinas
- ◆ Estado del falso suelo
- ◆ Extintores revisados
- ◆ Es la amenaza más temida por su rápido poder destructor.



4. Principios de Seguridad.

■ Índice.

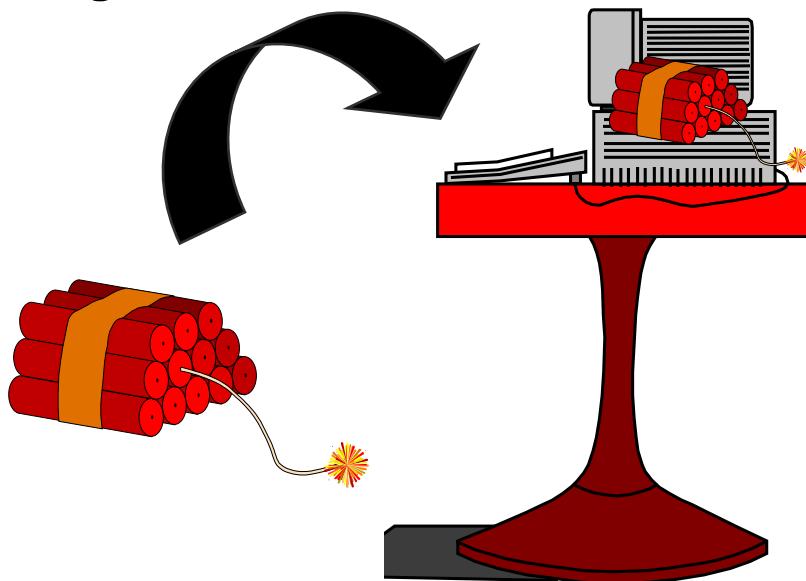
- ¿Conectado o desconectado?.
- Conciencia de las debilidades.
- Las dos últimas décadas.
- ¿Qué hay de nuevo en los 00's?.
- ¿Cifrar o encriptar?.
- Interés en el delito informático.
- Seguridad física/lógica.

- 1^{er} principio de la seguridad informática.
 - Debilidades del sistema informático.
 - Amenazas del sistema.
 - Amenazas de interrupción.
 - Amenazas de intercepción.
 - Amenazas de modificación.
 - Amenazas de generación.
 - El triángulo de debilidades.
 - Ataques característicos.
- 2º principio de la seguridad informática.
- 3^{er} principio de la seguridad informática.
- Elementos de seguridad informática.
- Datos seguros.



¿Conectado o desconectado?.

No podemos aceptar esa afirmación popular que dice que el computador más seguro ...



... es aquel que está apagado y, por tanto, desconectado de la red.

A pesar de todas las amenazas del entorno que, como veremos, serán muchas y variadas.



¿Conciencia de las debilidades?.



internas o externas



La seguridad informática
será un motivo de
preocupación.

... y las empresas, organismos y particulares comienzan a tener verdadera conciencia de su importancia.



Las dos últimas décadas.

- A partir de los años 80, el uso del ordenador personal comienza a ser común. Asoma ya la preocupación por la integridad de los datos.
- En la década de los años 90, proliferan los ataques a sistemas informáticos, aparecen los virus y se toma conciencia del peligro que nos acecha como usuarios de PCs y equipos conectados a Internet.
- Las amenazas se generalizan a finales de los 90.
- Se toma en serio la seguridad: década de los 00s



¿Qué hay de nuevo en los 00s?.

- Principalmente por el uso de Internet, el tema de la protección de la información se transforma en una necesidad y con ello se populariza la terminología técnica asociada a la criptología:

- ◆ Cifrado, descifrado, criptoanálisis, firma digital.
- ◆ Autoridades de Certificación, comercio electrónico.

- Ya no sólo se transmiten estas enseñanzas en las universidades. El usuario final desea saber, por ejemplo, qué significa firmar un e-mail.
- Productos futuros:  Seguridad añadida



¿Cifrar o encriptar?. ☠

Cifra o cifrado:

Técnica que, en general, protege o autentica a un documento o usuario al aplicar un algoritmo criptográfico. Sin conocer una clave específica, no será posible descifrarlo o recuperarlo.

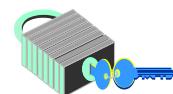
En algunos países por influencia del inglés se usará la palabra *encriptar*. Si bien esta palabra no existe en la 23^a edición del diccionario de la RAE, podría ser el acto de “meter a alguien dentro de una cripta”, ☺ †... algo bastante distinto a lo que deseamos expresar.

Ejemplos como éstos encontraremos muchísimos. Sin ir más lejos, aceptamos la palabra “privacidad” e incluso está escrita en Leyes, aunque sólo ha sido recogida en las últimas ediciones del diccionario de la RAE (posterior a octubre de 2001 – 22^a edición).



Interés en el delito informático.

- El delito informático parece ser un “buen negocio”:
 - Objeto Pequeño: la información está almacenada en “contenedores pequeños”: no es necesario un camión para robar el banco, joyas, dinero, ...
 - Contacto Físico: no existe contacto físico en la mayoría de los casos. Se asegura el anonimato y la integridad física del delincuente.
 - Alto Valor: el objeto codiciado tiene un alto valor. El contenido (los datos) vale mucho más que el soporte que los almacena (disquete, disco compacto, ...).
- Única solución: el uso de técnicas criptográficas.



Seguridad Física v/s Seguridad Lógica.

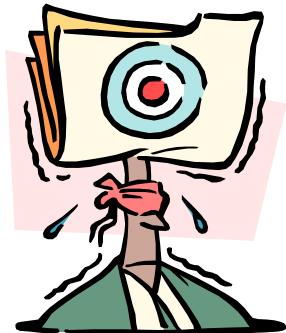
- El estudio de la seguridad informática puede plantearse desde dos enfoques:
 - Seguridad Física: Protección del sistema ante las amenazas físicas, planes de contingencia, control de acceso físico, políticas de backups, etc.
 - Seguridad Lógica: Protección de la información en su propio medio mediante el enmascaramiento de la misma usando técnicas de criptografía. Este enfoque propio de las Aplicaciones Criptográficas será tratado a lo largo de todo el curso.



1^{er} principio de la seguridad informática.

“El intruso al sistema utilizará cualquier artilugio que haga más fácil su acceso y posterior ataque”.

- Existirá una diversidad de frentes desde los que puede producirse un ataque. Esto dificulta el análisis de riesgos porque el delincuente aplica la filosofía del punto más débil de este principio.



PREGUNTA:

¿Cuáles son los puntos débiles de un sistema informático?



Debilidades del sistema informático (1).

HARDWARE - SOFTWARE - DATOS
MEMORIA - USUARIOS

Los tres primeros puntos conforman el llamado Triángulo de Debilidades del Sistema:

- Hardware: Errores intermitentes, conexión suelta, desconexión de tarjetas, etc.
- Software: Sustracción de programas, modificación, ejecución errónea, defectos en llamadas al sistema, etc.
- Datos: Alteración de contenidos, introducción de datos falsos, manipulación fraudulenta de datos, etc.

- Memoria: Introducción de virus, mal uso de la gestión de memoria, bloqueo del sistema, etc.
- Usuarios: Suplantación de identidad, acceso no autorizado, visualización de datos confidenciales, etc.



Debilidades del sistema informático (2).

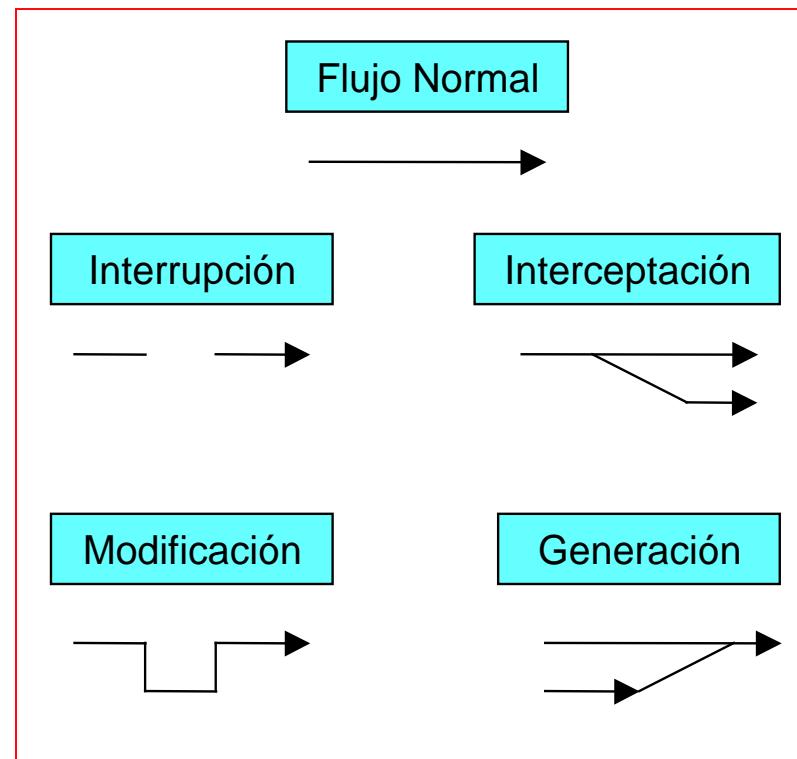
- Es muy difícil diseñar un plan que contemple de forma eficiente todos estos aspectos.
- Debido al Principio de Acceso más Fácil, no se deberá descuidar ninguno de los cinco elementos susceptibles de ataque del sistema informático.



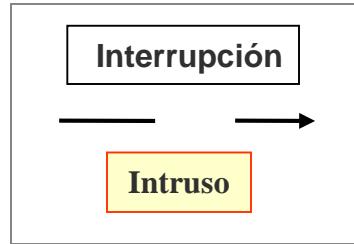
Amenazas del sistema.

■ Las amenazas se deben a fenómenos de:

- ◆ Interrupción
- ◆ Interceptación
- ◆ Modificación
- ◆ Generación



Amenazas de interrupción.



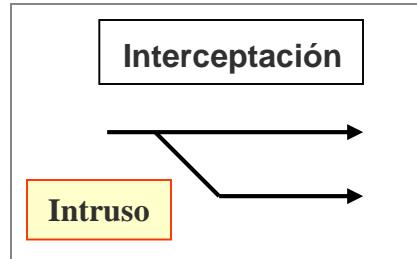
- Se daña, pierde o deja de funcionar un punto del sistema.
- Detección inmediata.

Ejemplos:

- Destrucción del hardware.
- Borrado de programas, datos.
- Fallos en el sistema operativo.



Amenazas de interceptación.

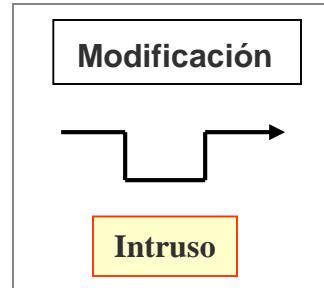


- Personas no autorizadas acceden a la información. Por tanto hacen uso de privilegios adquiridos irregularmente.
- Detección difícil, no deja huellas.

Ejemplos: Copias ilícitas de programas.
Escucha en línea de datos.



Amenazas de modificación.

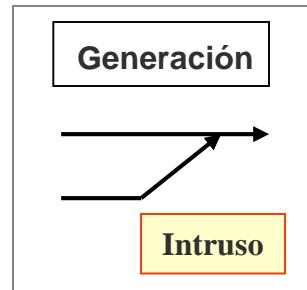


- Acceso no autorizado que cambia el entorno para su beneficio.
- Detección difícil según circunstancias.

Ejemplos: Modificación de bases de datos.
Modificación de elementos del HW.



Amenazas de generación.



- Creación de nuevos objetos dentro del sistema.
- Detección difícil. Delitos de falsificación.

Ejemplos: Añadir transacciones en red.
Añadir registros en base de datos.



El triángulo de debilidades.

Interrupción
(pérdida)

Interceptación
(acceso)

Modificación
(cambio)

Generación
(creación)

Los datos serán la
parte más vulnerable
del sistema.

DATOS

HD

SW

Interrupción (denegar servicio)
Interceptación (robo)

Modificación (falsificación)
Interrupción (borrado)
Interceptación (copia)

Ejemplos de ataques



Ataques característicos.

■ Hardware:

- Agua, fuego, electricidad, polvo, cigarrillos, comida.

■ Software:

- Borrados accidentales, intencionados, fallos de líneas de programa, bombas lógicas, robo, copias ilegales.

■ Datos:

- Los mismos puntos débiles que el software.
- Dos problemas: no tienen valor intrínseco pero sí su interpretación y algunos son de carácter público.



2º principio de la seguridad informática.

"Los datos deben protegerse sólo hasta que pierdan su valor".

- Se habla, por tanto, de la caducidad del sistema de protección: tiempo en el que debe mantenerse la confidencialidad o secreto del dato.
- Esto nos llevará a considerar la fortaleza del sistema de cifra.



PREGUNTA:

¿Cuánto tiempo deberá protegerse un dato?



3^{er} principio de la seguridad informática.

"Las medidas de control se implementan para ser utilizadas de forma efectiva. Deben ser eficientes, fáciles de usar y apropiadas al medio".

- Y de acuerdo a este principio
 - que funcionen en el momento oportuno.
 - que lo hagan optimizando los recursos del sistema.
 - que pasen desapercibidas para el usuario.
- Ningún sistema de control resulta efectivo hasta que es utilizado al surgir la necesidad de aplicarlo.



Elementos de la seguridad informática (1).

■ Confidencialidad

- Los componentes del sistema son accesibles sólo por los usuarios autorizados.

■ Integridad

- Los componentes del sistema sólo pueden ser creados y modificados por los usuarios autorizados.

■ Disponibilidad

- Los usuarios deben tener disponibles todos los componentes del sistema cuando así lo deseen.



Elementos de la seguridad informática (2).

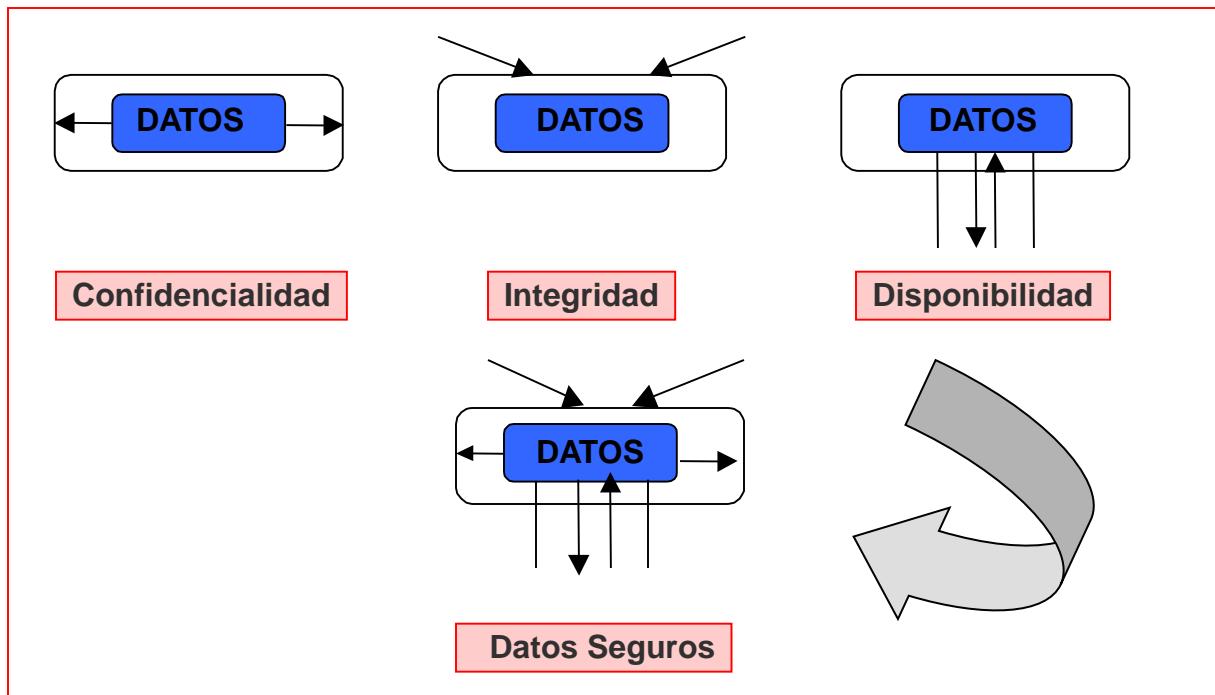
■ No Repudio

- Este término se ha introducido en los últimos años como una característica más de los elementos que conforman la seguridad en un sistema informático.
- Está asociado a la aceptación de un protocolo de comunicación entre emisor y receptor (cliente y servidor) normalmente a través del intercambio de sendos certificados digitales.
- Se habla entonces de **No Repudio de Origen** y **No Repudio de Destino**, forzando a que se cumplan todas las operaciones por ambas partes en una comunicación.



Datos seguros.

Si se cumplen estos principios, diremos en general que los datos están protegidos y seguros.



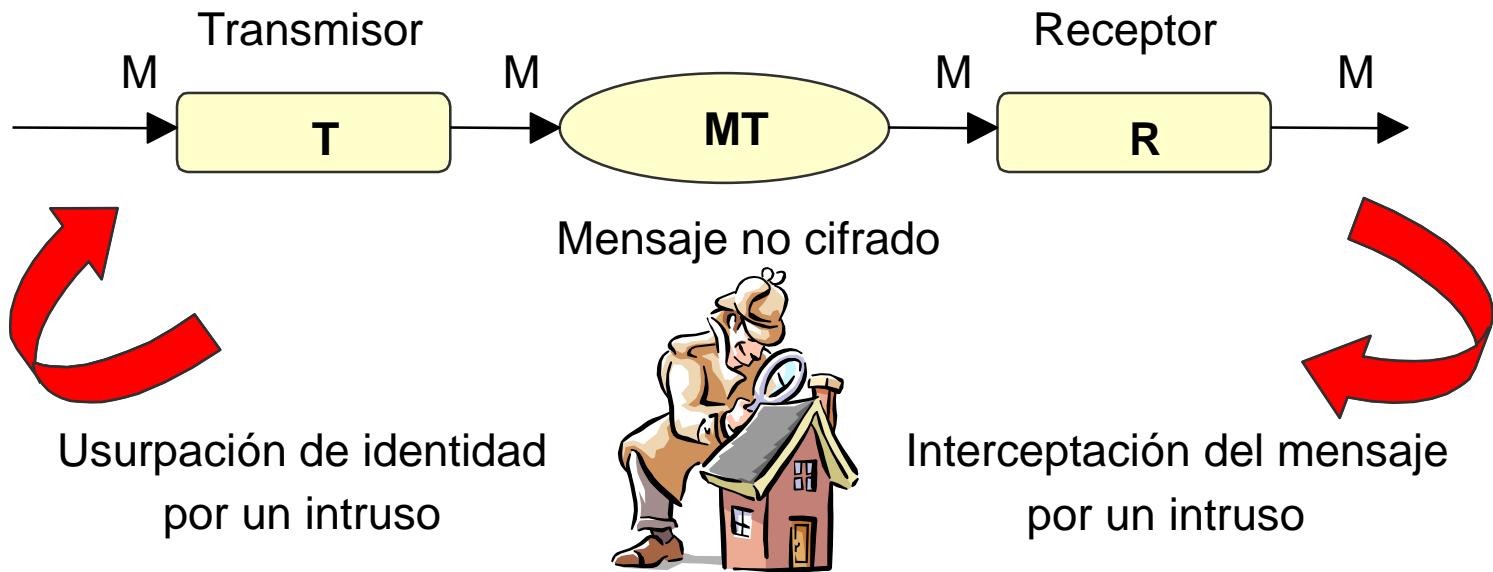
5. Introducción a la Criptografía.

■ Índice.

- Inseguridades en la transmisión de datos.
- Sistema de cifrado.
- Esquema de un criptosistema.
- Requisitos de un criptosistema.
- Recomendaciones de Bacon.
- Recomendaciones de Kerckhoffs.
- Fortaleza: Tipos de ataques.
- Clasificación de los criptosistemas.
- Tipos de criptosistemas.
- Cifrado en bloque y en flujo.
- Comparativa: cifrado en bloque/flujo.
- Criptosistemas Simétricos y Asimétricos.
- Confidencialidad e Integridad.
- Criptosistema de clave secreta o simétricos.
- Criptosistema con clave secreta.
- Resumen para sistema de clave secreta.
- Criptosistema con clave pública o asimétricos.
- Resumen para sistema con clave pública.
- Tipos de Cifra con Sistemas Asimétricos.
- ¿Clave pública o clave secreta?.
- La solución híbrida.
- ¿Qué usar, Simétricos o Asimétricos?.
- Sistema Híbrido de Cifra y Firma.



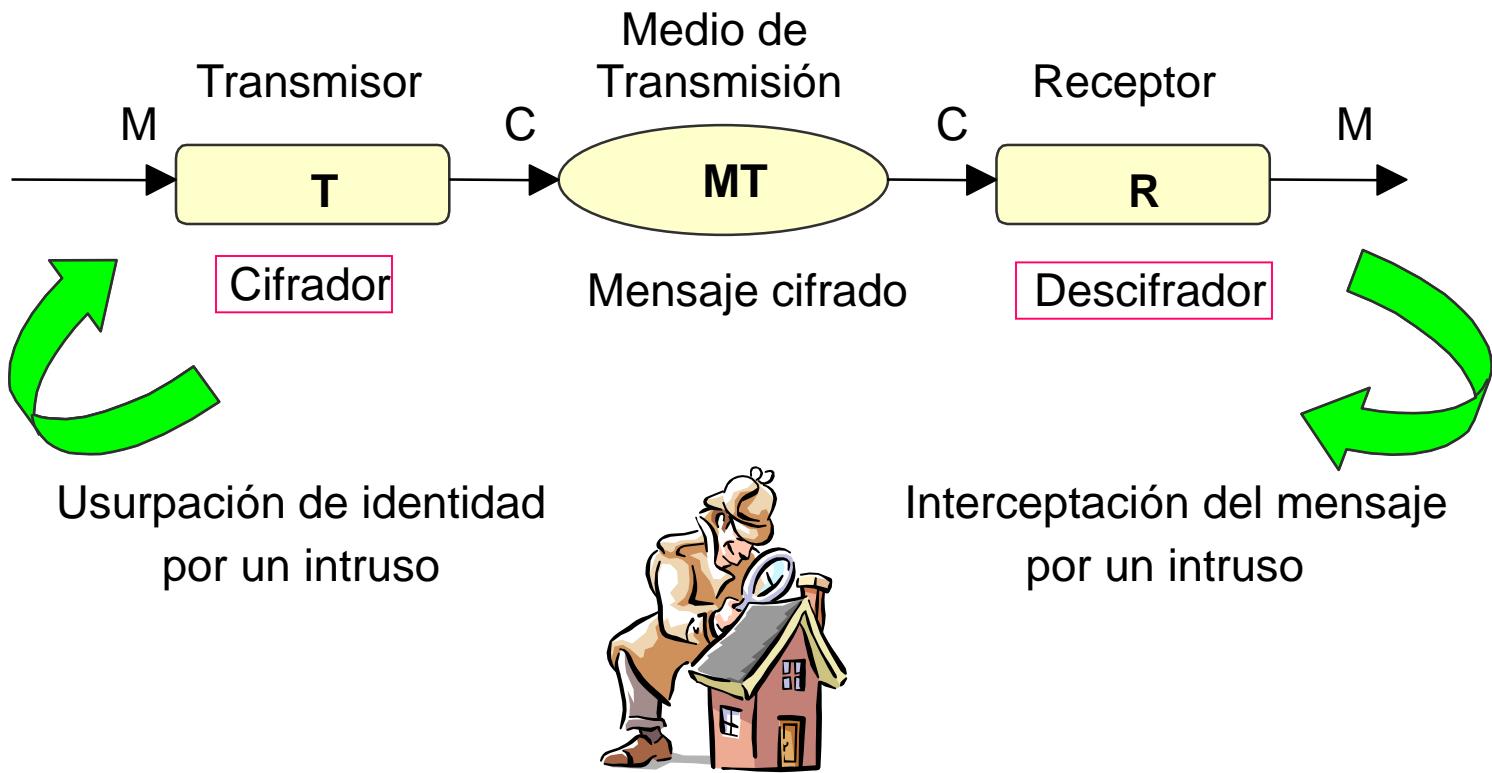
Inseguridades en la transmisión de datos.



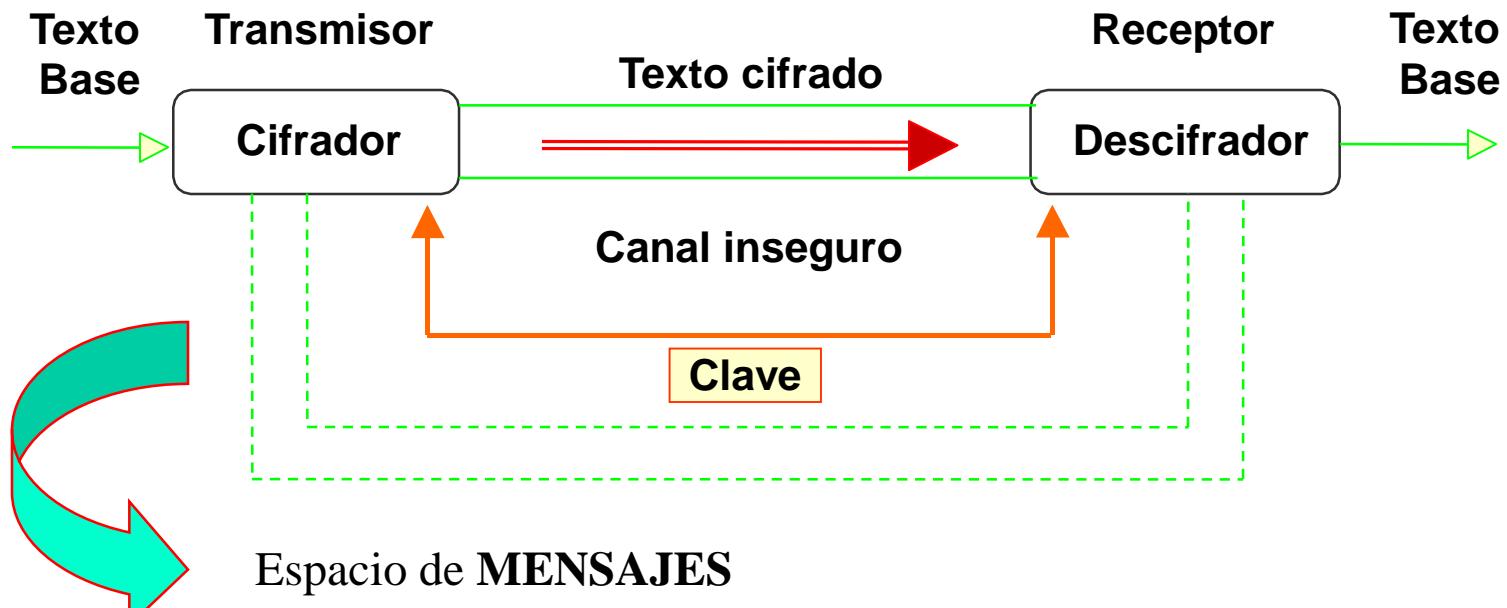
Sea cual sea el medio de transmisión (enlace, red telefónica, red de datos, disco magnético, disco óptico, etc.), éste es, por definición, **INSEGURO**.



Sistema de cifrado.



Esquema de un criptosistema.



Espacio de **MENSAJES**

Espacio de **TEXTOS CIFRADOS**

Espacio de **CLAVES**

Transformaciones de **CIFRADO** y **DESCIFRADO**



Requisitos de un criptosistema.

- Algoritmo de cifrado/descifrado rápido y fiable.
- Posibilidad de transmitir ficheros por una línea de datos, almacenarlos o transferirlos.
- No debe existir retardo debido al cifrado o descifrado.
- La seguridad del sistema deberá residir solamente en el secreto de una clave y no de las funciones de cifra.
- La fortaleza del sistema se entenderá como la imposibilidad computacional de romper la cifra o encontrar la clave secreta.



Recomendaciones de Bacon.

■ Filósofo y estadista inglés del siglo XVI

- Dado un texto en claro M y un algoritmo de cifra E_k , el cálculo de $E_k(M)$ y su inversa, $D_k(E_k(M))$, debe ser *sencillo*.
- Será *imposible* encontrar el texto en claro M a partir del criptograma C si se desconoce la función de descifrado D_k .
- El criptograma deberá contener caracteres distribuidos para que su *apariencia* sea inocente y no dé pistas a un intruso.



Recomendaciones de Kerckhoffs.

■ Profesor holandés en París del siglo XIX

- K₁: El sistema debe ser en la *práctica imposible* de criptoanalizar.
- K₂: Las limitaciones del sistema no deben plantear *dificultades* a sus usuarios.
- K₃: Método de elección de claves *fácil* de recordar.
- K₄: Transmisión del texto cifrado por *telégrafo*.
- K₅: El criptógrafo debe ser *portable*.
- K₆: No debe existir una larga lista de *reglas* de uso.



Fortaleza: tipos de ataques.

Conociendo el algoritmo de cifra, el criptoanalista intentará romper la cifra:

1. Contando únicamente con el criptograma.
2. Contando con texto en claro conocido.
3. Eligiendo un texto en claro.
4. A partir de texto cifrado elegido.

ATAQUE POR FUERZA BRUTA



5. Buscando combinaciones de claves.

Mayor trabajo



Clasificación de los criptosistemas.

- Sistemas de cifra: clásicos v/s modernos

- Clasificación histórica y cultural.

- Sistemas de cifra: en bloque v/s en flujo

- Clasificación de acuerdo a cómo se produce la cifra.



- Sistemas de clave: secreta v/s pública

- Clasificación de acuerdo a la cifra, usando una única clave secreta o bien sistemas con dos claves, una de ellas pública y la otra privada.



Tipos de criptosistemas.

Clasificación de los criptosistemas

Según el tratamiento del mensaje se dividen en:

Cifrado en bloque (DES, IDEA, RSA: 64 - 128 bits)

Cifrado en flujo (A5) cifrado bit a bit

Según el tipo de claves se dividen en:



Cifrado con clave secreta

Cifrado con clave pública

Sistemas simétricos

Sistemas asimétricos



Cifrado en bloque y en flujo.

■ CIFRADO EN BLOQUE:

- El mismo algoritmo de cifra se aplica a un bloque de información (grupo de caracteres, número de bytes, etc.) repetidas veces, usando la misma clave.

■ CIFRADO EN FLUJO:

- El algoritmo de cifra se aplica a un elemento de información (carácter, bit) mediante un flujo de clave en teoría aleatoria y mayor que el mensaje.



Comparativa cifrado en bloque v/s flujo.

CIFRADO EN BLOQUE

Ventajas:

- * Alta difusión de los elementos en el criptograma.
- * Inmune: imposible introducir bloques extraños sin detectarlo.

Desventajas:

- * Baja velocidad de cifrado al tener que leer el bloque.
- * Propenso a errores de cifra. Un error se propagará a todo el bloque.

CIFRADO EN FLUJO

Ventajas:

- * Alta velocidad de cifra al no tener en cuenta otros elementos.
- * Resistente a errores. Cifra independiente de cada elemento.

Desventajas:

- * Baja difusión de elementos en el criptograma.
- * Vulnerable. Pueden alterarse los elementos por separado.



Criptosistemas simétricos y asimétricos.

Criptosistemas simétricos:

Existirá una única clave (secreta) que deben compartir emisor y receptor. Se cifra y se descifra con la misma clave por lo que la seguridad reside en mantener dicha clave en secreto.

Criptosistemas asimétricos:

Cada usuario crea un par de claves, una privada y otra pública, inversas dentro de un cuerpo finito. Lo que se cifra en emisión con una clave, se descifra en recepción con la clave inversa. La seguridad del sistema reside en la dificultad computacional de descubrir la clave privada a partir de la pública. Para ello usan funciones matemáticas de un solo sentido con trampa.



Confidencialidad e integridad (1).

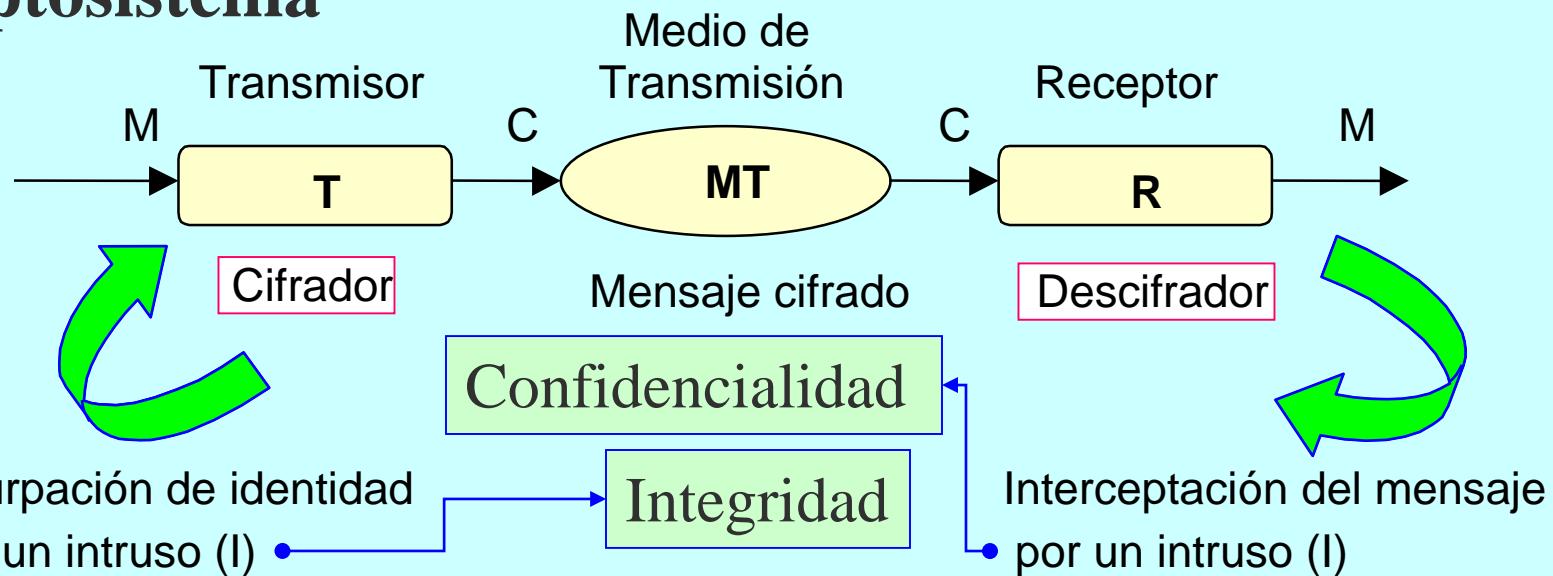
- Vamos a ver cómo se obtienen en cada uno de estos sistemas de cifra (cifrado con clave secreta **y** cifrado con clave pública) los dos aspectos más relevantes de la seguridad informática:

**La confidencialidad
y la integridad**



Confidencialidad e integridad (2).

Criptosistema

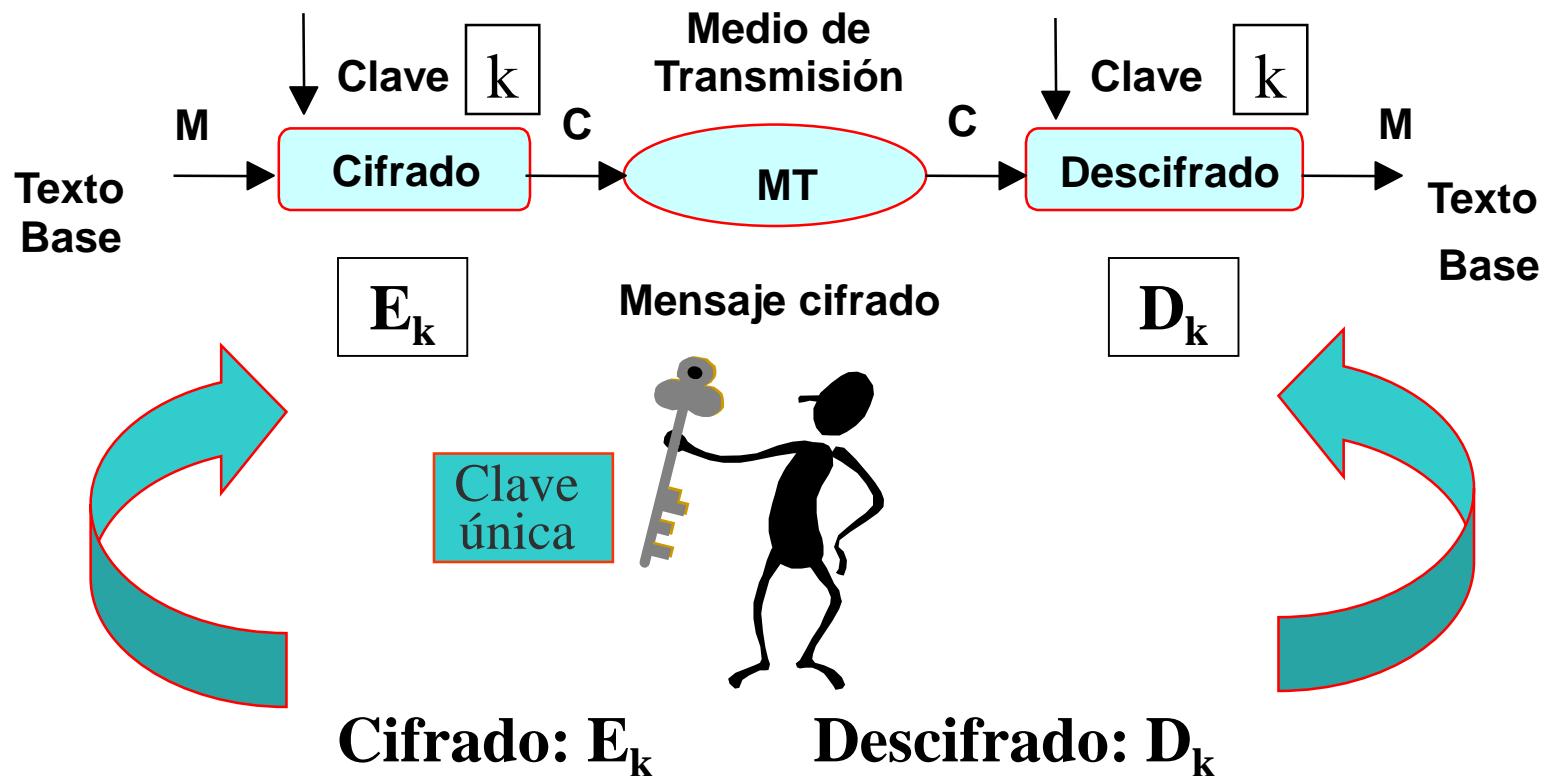


Estos dos principios de la seguridad informática, el de la confidencialidad y la integridad, (además de la disponibilidad y el no repudio) serán muy importantes en un sistema de intercambio de información segura a través de Internet.

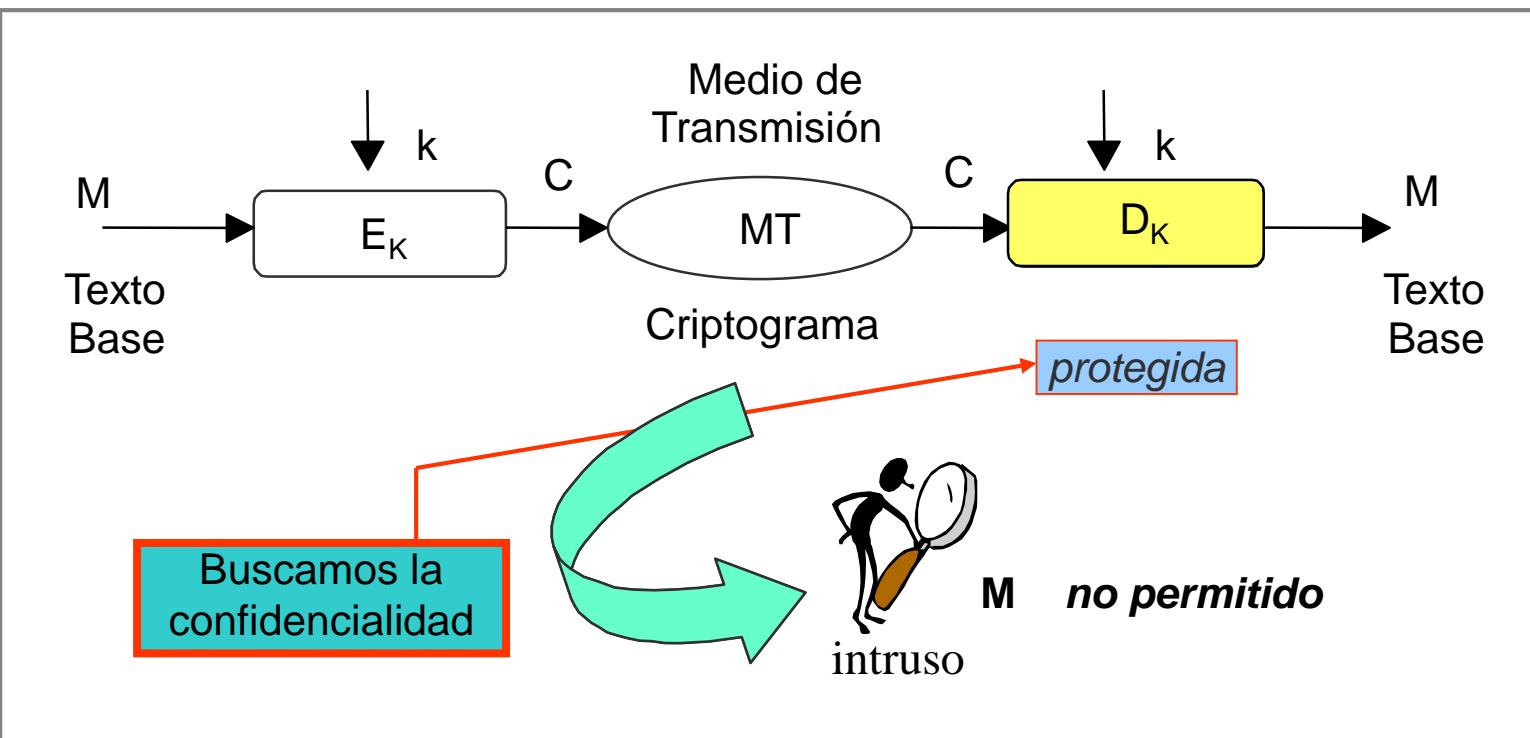


Criptosistemas de clave secreta o simétricos.

Mecanismo de cifrado con un Modelo Simétrico:



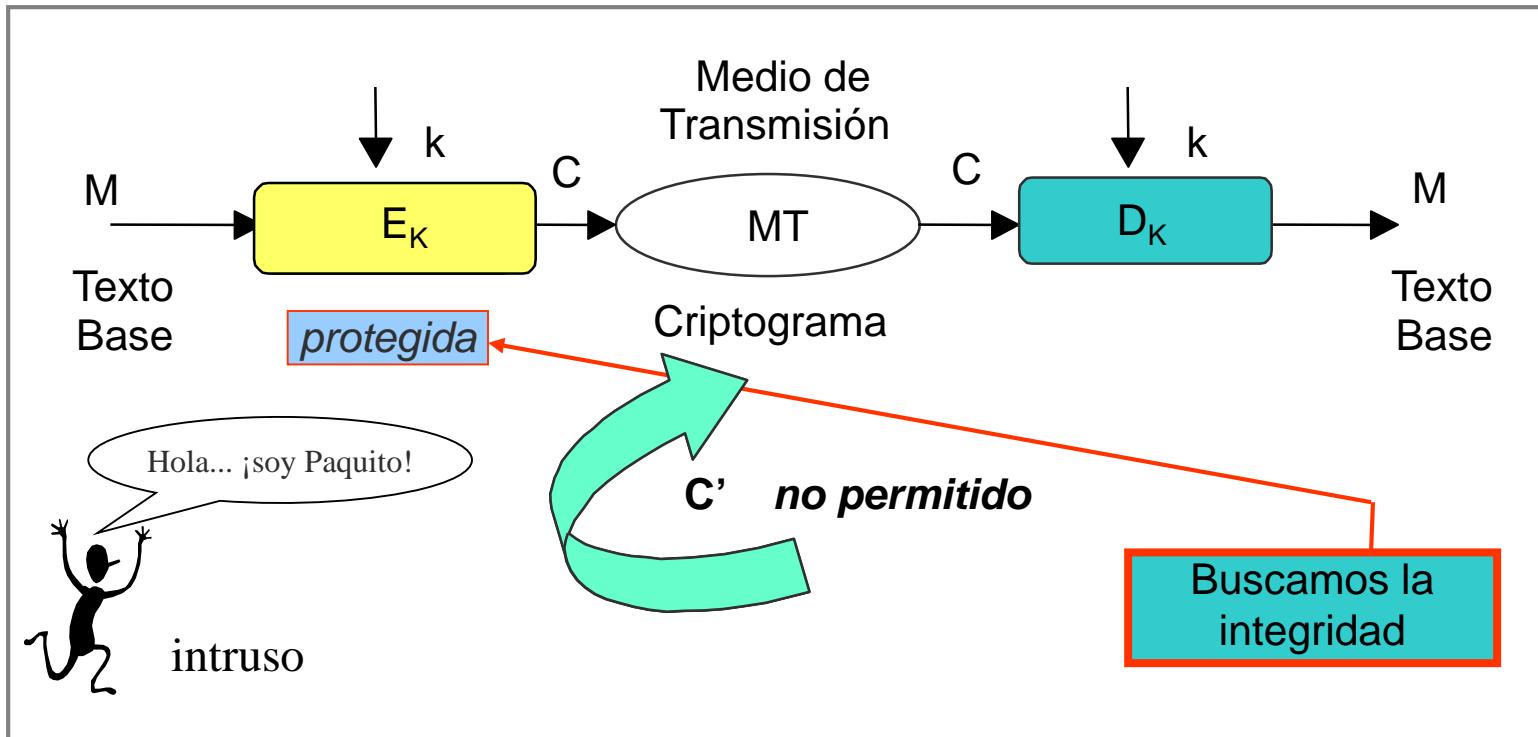
Criptosistema con clave secreta (1).



El criptoanalista no podrá descifrar el criptograma **C** o cualquier otro texto cifrado bajo la transformación E_K .



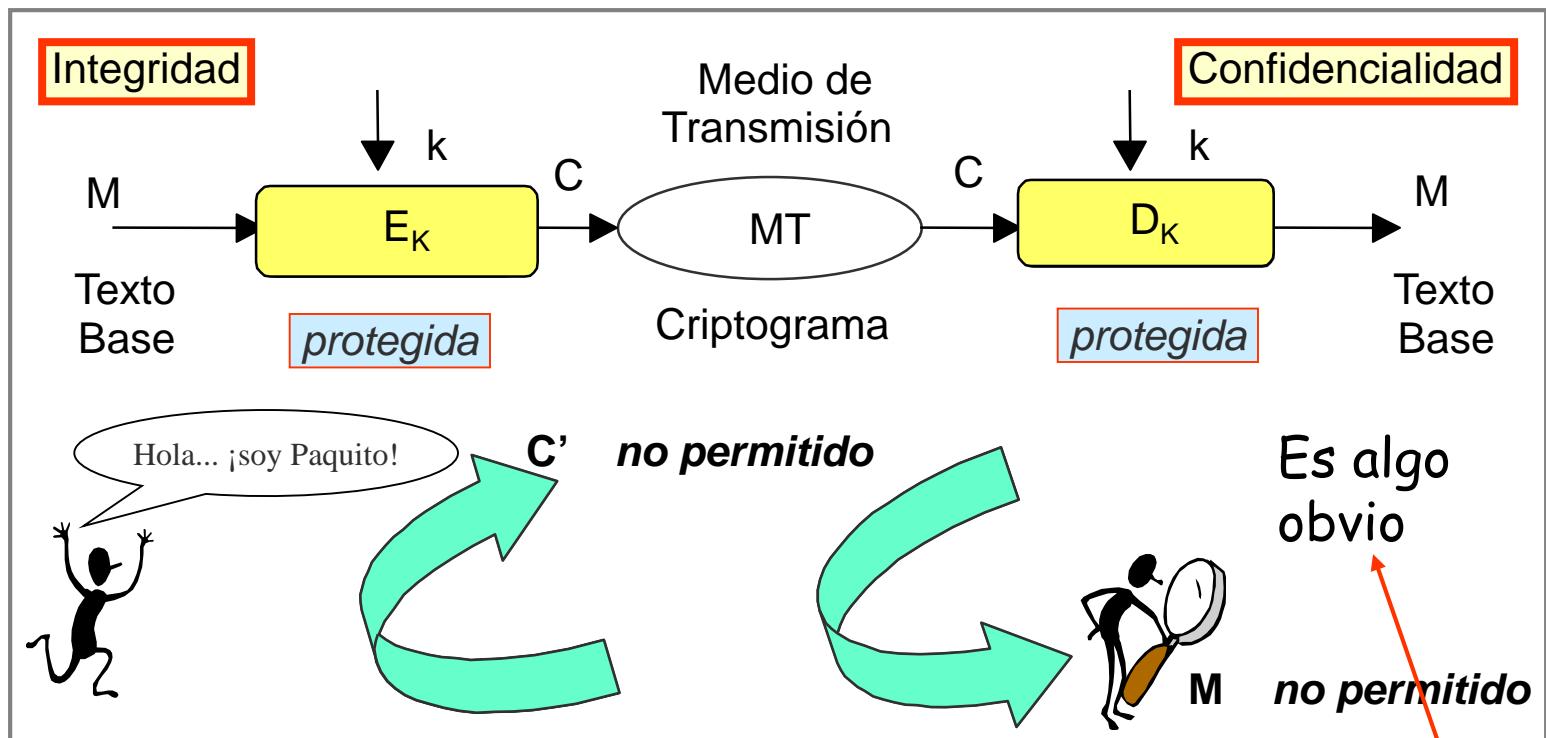
Criptosistema con clave secreta (2).



El criptoanalista no podrá cifrar un texto en claro M' y enviarlo al destinatario como $C' = E_K(M')$.



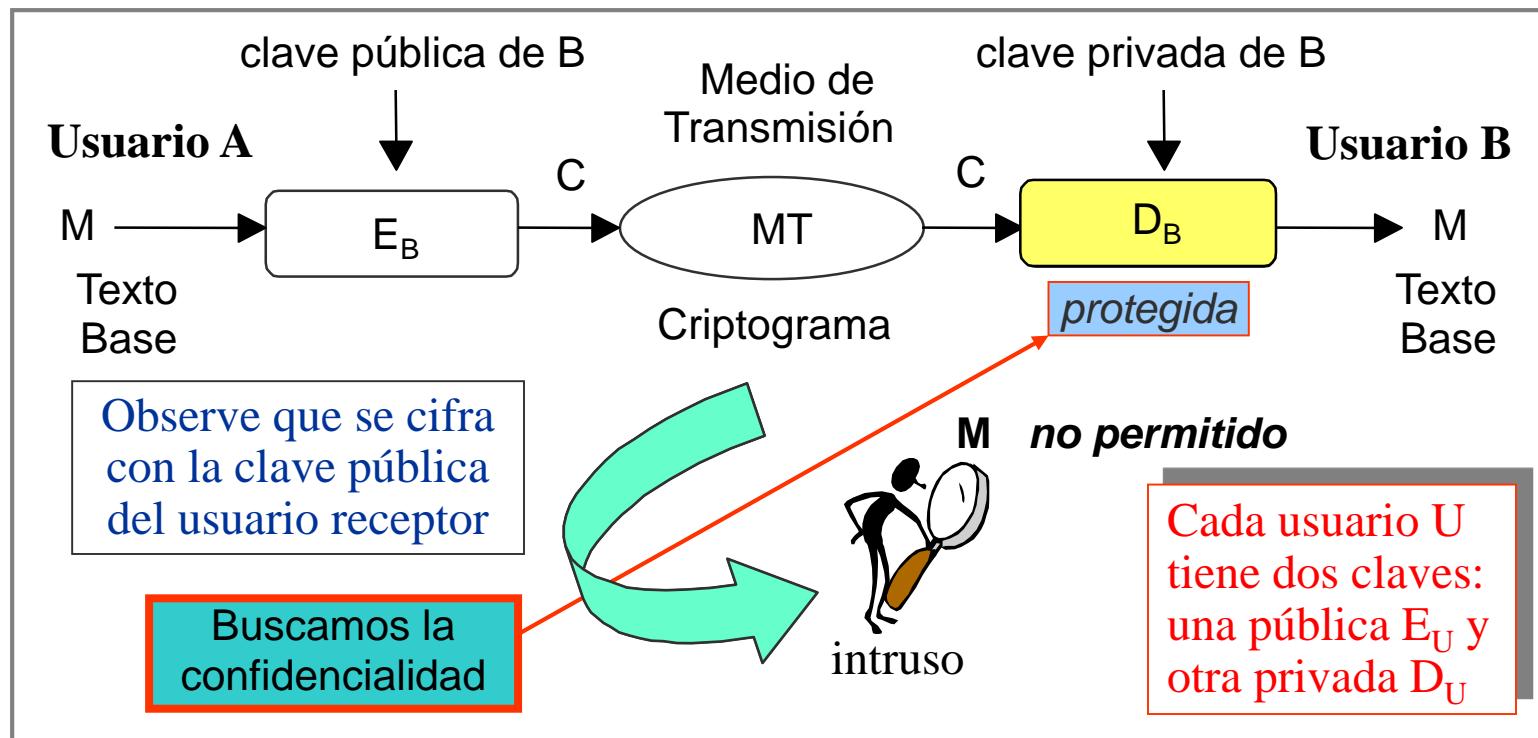
Resumen para sistema de clave secreta.



La confidencialidad y la integridad se lograrán simultáneamente si se protege la clave secreta.



Criptosistema con clave pública o asimétricos (1).



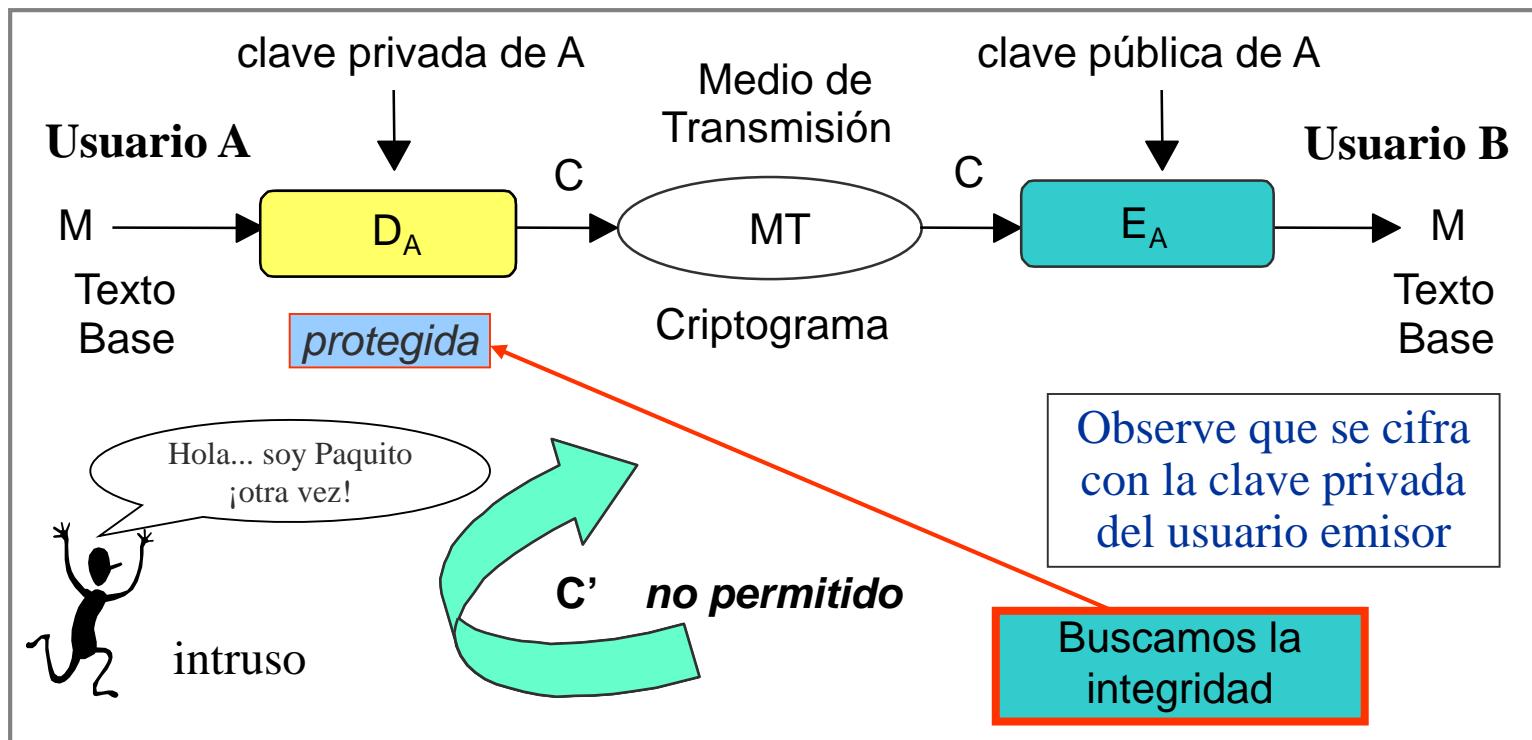
$$C = E_B(M)$$

$$M = D_B(C) = D_B(E_B(M))$$

D_B y E_B son números inversos dentro de un cuerpo



Criptosistema con clave pública o asimétricos (2).



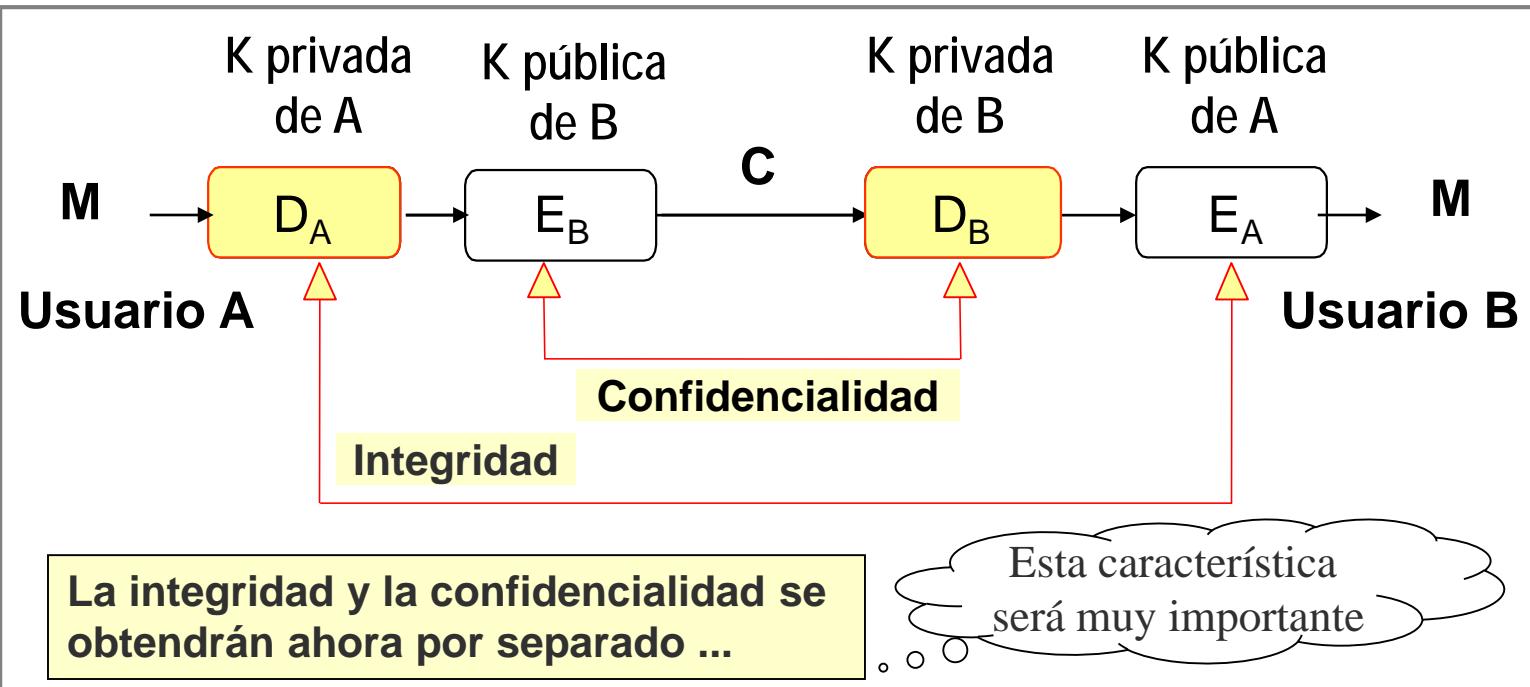
$$C = D_A(M)$$

E_A y D_A son inversos en un cuerpo

$$M = E_A(C) = E_A(D_A(M))$$



Resumen para sistema con clave pública.

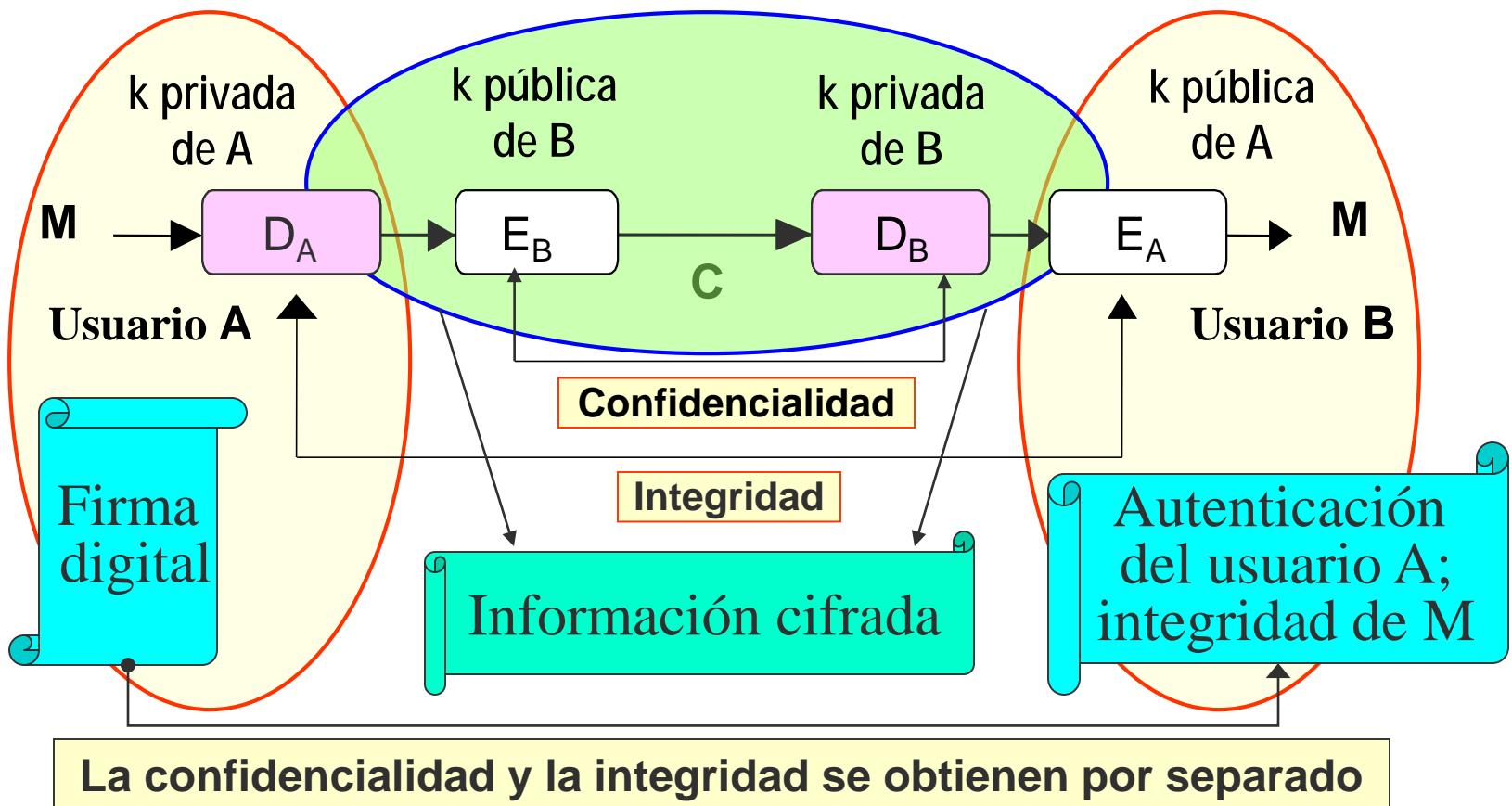


$$C = E_B(D_A(M)) \quad \text{Cifrado del “mensaje” y firma digital}$$
$$M = E_A(D_B(C)) \quad \text{Descifrado y comprobación de firma}$$



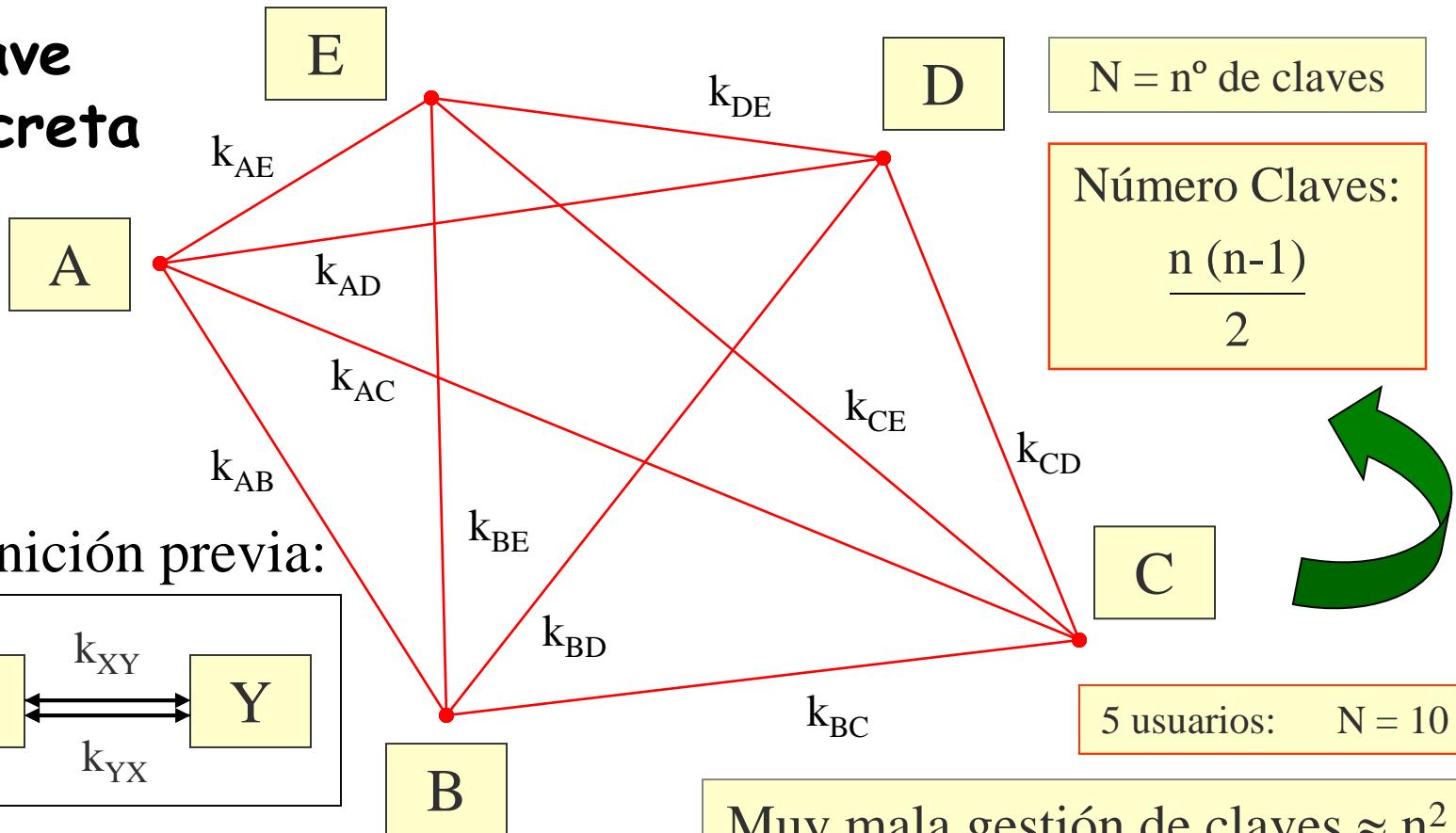
Tipos de cifra con sistemas asimétricos.

Mecanismo de cifrado con un Modelo Asimétrico:



¿Clave pública o clave secreta?

**Clave
secreta**

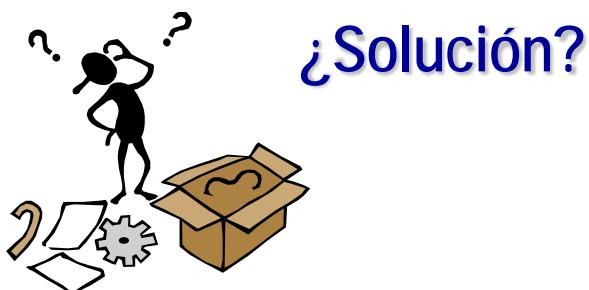


La solución híbrida.

¿Es entonces la clave pública la solución?

NO

- Tendrá como inconveniente principal (debido a las funciones de cifra empleadas) una tasa o velocidad de cifra mucha más baja que la de los criptosistemas de clave secreta.



¿Solución?



Sistemas de
cifra híbridos



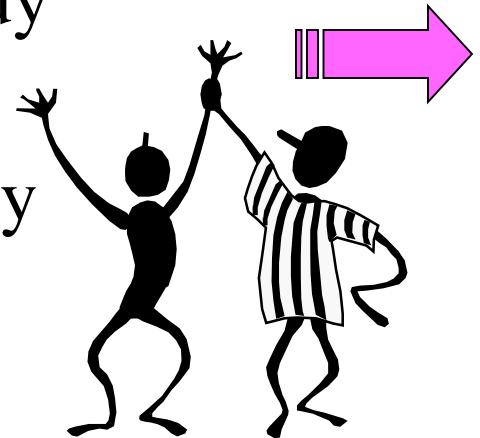
¿Qué usar, simétricos o asimétricos?.

Los sistemas de clave pública son muy lentos pero tienen firma digital.

Los sistemas de clave secreta son muy rápidos pero no tienen firma digital.



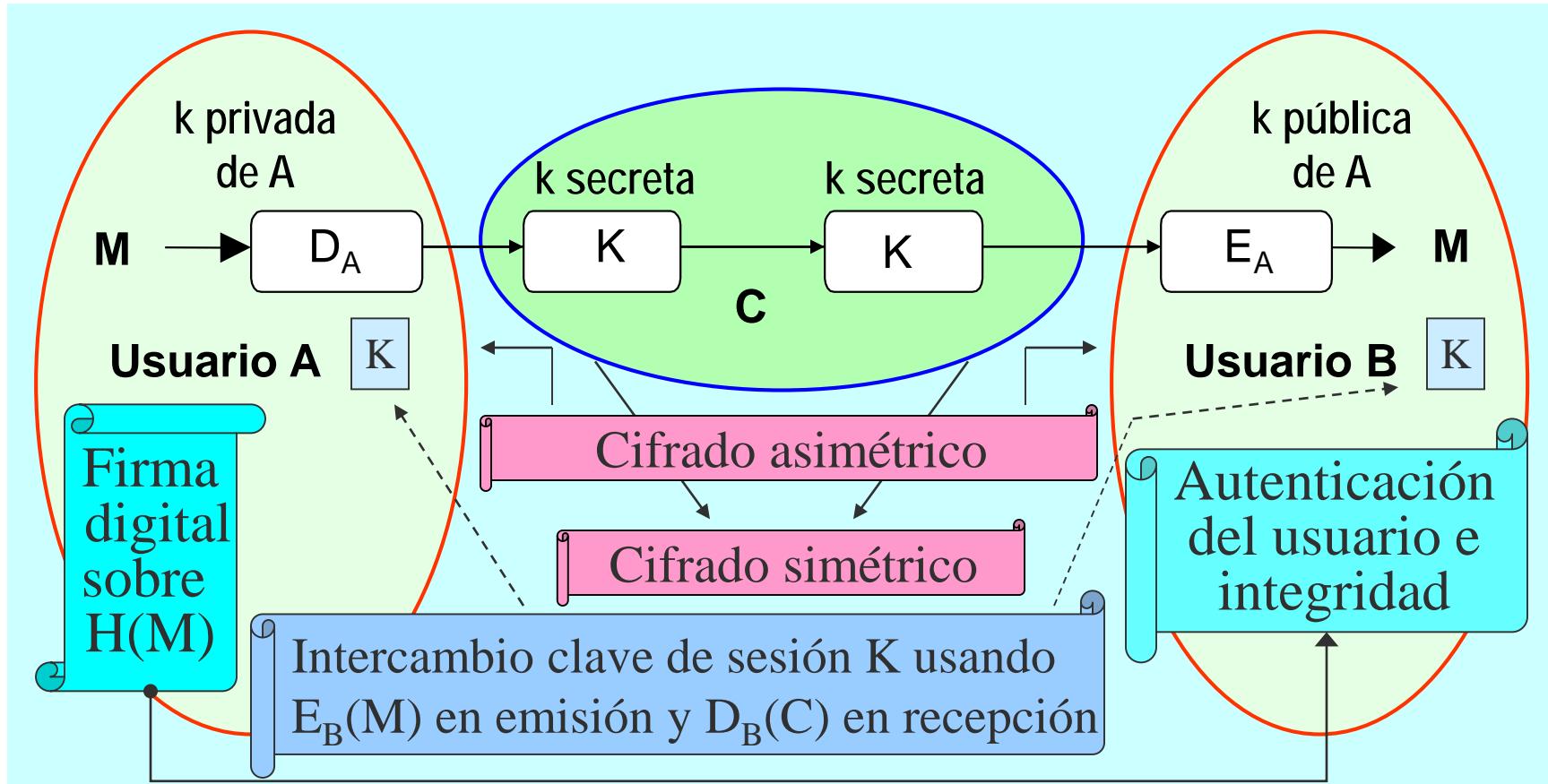
¿Qué hacer?



Cifrado de la información:
Sistemas de clave secreta
Firma e intercambio de clave de sesión:
Sistemas de clave pública



Sistema híbrido de cifra y firma.



6. Certificados y Autoridades de Certificación.

■ Índice.

- ¿Qué son los certificados digitales?.
- Certificados digitales X.509.
- Formato del certificado digital.
- Campos del certificado digital X.509.
- Autoridades de certificación.
- Elementos de un AC.
- Algunas características de diseño de la AC.
- Funcionamiento de la AC.



¿Qué son los certificados digitales?.

Un certificado digital es un documento que contiene diversos datos, entre ellos el nombre de un usuario y su clave pública, y que es firmado por una Autoridad de Certificación (AC).

Como emisor y receptor confiarán en esa AC, el usuario que tenga un certificado expedido por ella se autenticará ante el otro, en tanto que su clave pública está firmada por dicha autoridad.



Certificados digitales X.509.

X.509 está basado en criptografía asimétrica y firma digital. En X.509 se define un framework (una capa de abstracción) para suministrar servicios de autenticación a los usuarios del directorio X.500. La autenticación se realiza mediante el uso de certificados.

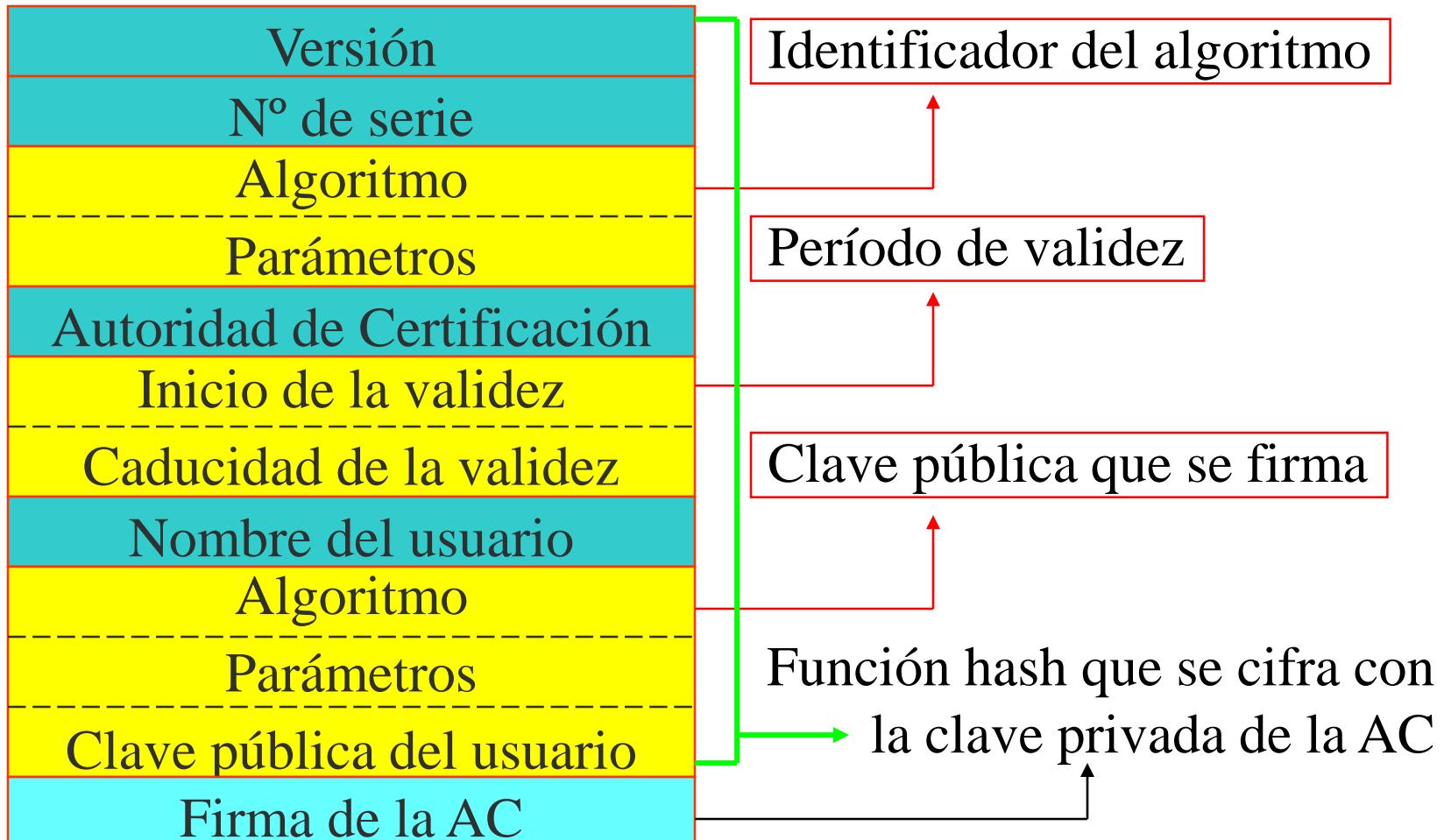
Un certificado contiene: el nombre de la CA, el nombre del usuario, la clave pública del usuario y cualquier otra información como puede ser un *timestamp*.

El certificado se cifra con la clave privada de la CA.

Todos los usuarios poseen la clave pública del CA.



Formato del certificado digital X.509.



Campos del certificado digital X.509.

- V: Versión del certificado (actualmente V3).
- SN: Número de serie.
- AI: identificador del algoritmo de firma que sirve para identificar el algoritmo usado para firmar el paquete X.509.
- CA: Autoridad certificadora.
- T_A : Periodo de validez.
- A: Propietario de la clave pública que se está firmando.
- P: Clave pública más identificador de algoritmo utilizado y más parámetros si son necesarios.
- Y{I}:Firma digital de Y por I usando la clave privada de la unidad certificadora.

CA<<A>> = CA { V, SN, AI, CA, T_A , A, AP }

Y<<X>> es el certificado del usuario X expedido por la autoridad certificadora Y.



Autoridades de certificación.

Autoridad de Certificación es un ente u organismo que, de acuerdo con unas políticas y algoritmos, certificará -por ejemplo- claves públicas de usuarios o servidores.

El usuario A enviará al usuario B su certificado (la clave pública firmada por AC) y éste comprobará con esa autoridad su autenticidad. Lo mismo en sentido contrario.



Elementos de un AC.

El sistema de autenticación debe tener:

- Una política de certificación
- Un certificado de la CA
- Los certificados de los usuarios (X.509)
- Los protocolos de autenticación, gestión y obtención de certificados:
 - Se obtienen de bases de datos (directorio X.500)
 - O bien directamente del usuario en tiempo de conexión (WWW con SSL)



Algunas características de diseño de la AC.

- Deberá definirse una política de certificación
 - Ámbito de actuación y estructura
 - Relaciones con otras ACs
- Deberá definirse el procedimiento de certificación para la emisión de certificados:
 - Verificación on-line
 - Verificación presencial
- Deberá generarse una Lista de Certificados Revocados



Funcionamiento de la AC.

■ Puesta en marcha de la AC:

- Generará su par de claves
- Protegerá la clave privada con una *passphrase*
- Generará el certificado de la propia AC

■ Distribución del certificado de la AC:

- A través del Directorio X.500
- Por medio de páginas Web

■ Podrá certificar a servidores y a clientes

