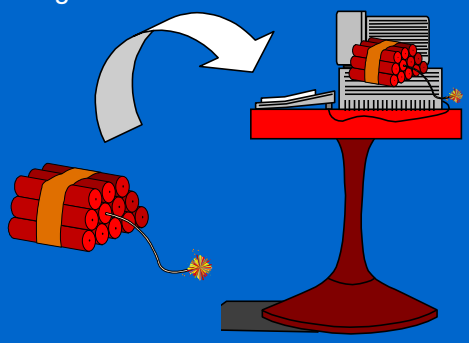
¿Conectado o desconectado?

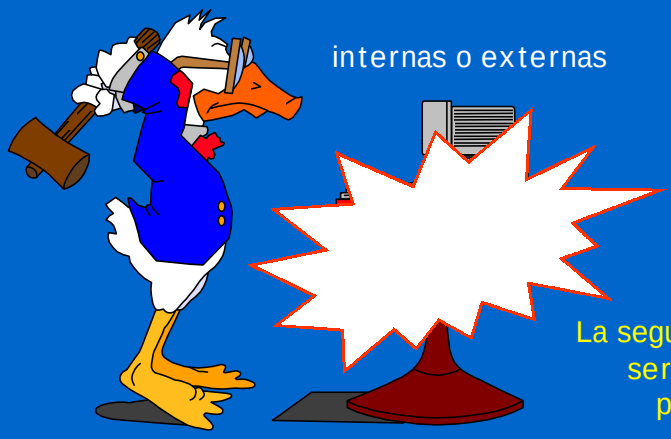
No podemos aceptar esa afirmación popular que dice que el computador más seguro ...

... 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

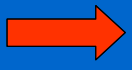
La seguridad informática será un motivo de preocupación.

... 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

Una definición de criptografía

Criptografía:

Rama de las Matemáticas -y en la actualidad de la Informática- que hace uso de métodos matemáticos con el objeto principal de cifrar un mensaje o archivo por medio de un algoritmo y una o más claves, dando lugar a distintos criptosistemas que permiten asegurar, al menos, dos aspectos básicos de la seguridad como son la confidencialidad y la integridad de la información.

He aquí una definición menos afortunada de criptografía por parte de la Real Academia de la Lengua Española...

¿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, 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 no esté recogida en la última edición del diccionario de la RAE (octubre de 2001).

Interés en el delito informático

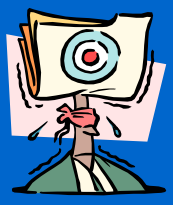
- El delito informático parece ser un “buen negocio”:
  - **Objeto Pequeño**: la información está almacenada en “contenedores pequeños”: no es necesario un camión para robar el banco, joyas, dinero, ...
  - **Contacto Físico**: no existe contacto físico en la mayoría de los casos. Se asegura el anonimato 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, ...).
- Unica 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. Este tema será tratado en el capítulo 3.
  - **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.

1er 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.

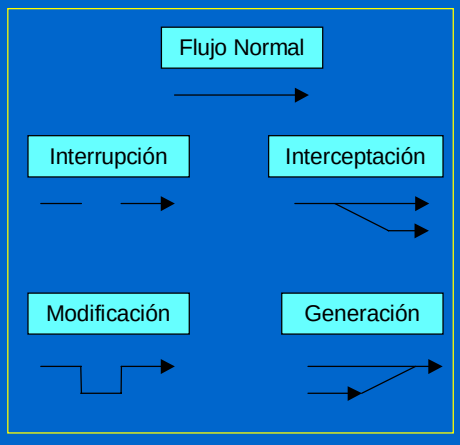
Debilidades del sistema informático (2)

- **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.

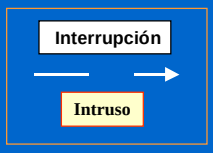
- Es muy difícil diseñar un plan que contemple de forma eficiente todos estos aspectos.
- Debido al Principio de Acceso más Fácil, no se deberá descuidar ninguno de los cinco elementos susceptibles de ataque del sistema informático.

Amenazas del sistema

- Las amenazas afectan principalmente al Hardware, al Software y a los Datos. Estas se deben a fenómenos de:
  - **Interrupción**
  - **Interceptación**
  - **Modificación**
  - **Generación**



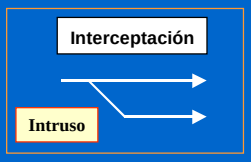
Amenazas de interrupción



- 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.

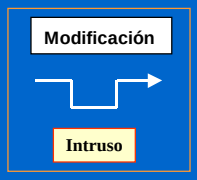
Amenazas de interceptación



- Acceso a la información por parte de personas no autorizadas. Uso de privilegios no adquiridos.
- Detección difícil, no deja huellas.

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

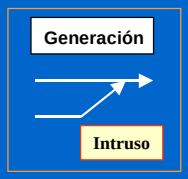
Amenazas de modificación



- 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.

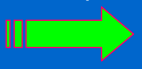
El triángulo de debilidades

Interrupción (pérdida)	**Interceptación** (acceso)	**Modificación** (cambio)	**Generación** (alteración)

Los datos serán la parte más vulnerable del sistema.

DATOS

Ejemplos de ataques



HD

SW

Interrupción (denegar servicio)
Interceptación (robo)

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

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 la fortaleza del sistema de cifra.

PREGUNTA:
¿Cuánto tiempo deberá protegerse un dato?

3er 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".
  - 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.

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 pasada.

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.

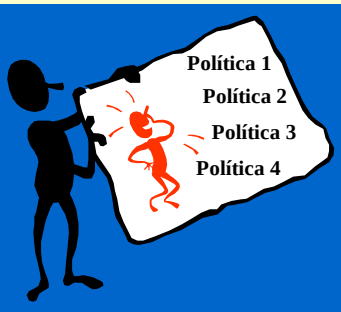
- Desde el punto de vista de la empresa, uno de los problema más importantes puede ser el que está relacionado con el delito o crimen informático, por factores externos e internos.

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...



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 crakers

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 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.

Algunos delitos informáticos (1)

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
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.

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.

Transmisión de un virus

- Se transmisten sólo mediante la ejecución de un programa. *Esto es muy importante recordarlo*.
- El correo electrónico por definición no puede contener virus al ser sólo texto. No obstante, sí puede contener archivos añadidos que se ejecuten en el cliente de correo del usuario y éstos pueden tener incluido un virus. ¡***Ahí está el peligro***!
- El entorno web es mucho más peligroso. Un hiperenlace puede lanzar un programa en Java u otro que se ejecute en el disco duro del cliente.

Tipos de ataque de un virus

- Aquellos que infectan a programas .EXE, .COM y .SYS por ejemplo.
  - Residen en memoria al ejecutarse el huésped y de ahí se propagan a otros archivos.
- Aquellos que infectan el sistema y el sector de arranque y tablas de entrada (áreas determinadas del disco).
  - Se instalan directamente allí y por lo tanto residen en memoria.

Algunas medidas básicas de prevención

- Proteger los disquetes con la pestaña.
  - Es una protección tipo hardware elemental.
- Escanear de vez en cuando el disco duro (por ejemplo una vez al mes) y siempre los disquetes.
- 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.

¿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.

Fin del Tema 2

Seguridad 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.

Seguridad Física en entornos de PCs

Temas a tener en cuenta en un entorno PC

- Anclajes a mesas de trabajo.
- Cerraduras.
- Tarjetas con alarma.
- Etiquetas con adhesivos especiales.
- Bloqueo de disquetera.
- Protectores de teclado.
- Tarjeta de control de acceso al hardware.
- Suministro ininterrumpido de corriente.
- Toma de tierra.
- Eliminación de la estática... etc.

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.

Información del análisis de riesgos (1)

- Información que se obtiene en un análisis de riesgos:
  - Determinación precisa de los recursos sensibles de la organización.
  - Identificación de las amenazas del sistema.
  - Identificación de las vulnerabilidades específicas del sistema.
  - Identificación de posibles pérdidas.

Información del análisis de riesgos (2)

- Información que se obtiene en un análisis de riesgos (continuación):
  - Identificación de la probabilidad de ocurrencia de una pérdida.
  - Derivación de contramedidas efectivas.
  - Identificación de herramientas de seguridad.
  - Implementación de un sistema de seguridad eficiente en costes y tiempo.

Efectividad del coste

- El control ha de tener menos coste que el valor de las pérdidas debido al impacto de ésta si se produce el riesgo temido.
- Ley básica: el costo 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 la cuales se comunican los sujetos dentro del sistema.

Políticas administrativas

- Políticas administrativas
  - Se establecen aquellos procedimientos de carácter administrativo en la organización como por ejemplo en el desarrollo de programas: modularidad en aplicaciones, revisión sistemática, etc.

Planes de contingencia

- ¿Qué es un Plan de Contingencia?
- ¿Por qué es necesario implementarlo?
- ¿Qué gana la empresa con este plan?
- Y si no lo tiene ¿a qué se expone?

Lo veremos a continuación

Definición de plan de contingencia

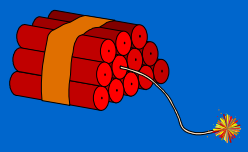
- Un Plan de Contingencia consiste en un análisis pormenorizado de las áreas que componen nuestra organización que nos servirá para establecer una política de recuperación ante un desastre.
  - Es un conjunto de datos de la empresa que se plasma en un documento con ese fin.

Desastres naturales y su prevención

- Desastres naturales
  - Huracán
  - Tormenta
  - Inundación
  - Tornado
  - Vendaval, etc
    - Destruyen nuestro sistema
- Medidas prevención
  - Emplazamientos adecuados
  - Protección fachadas, ventanas, puertas

Vandalismo informático y su prevención

- Terrorismo
- Sabotaje
- Robo



- Virus
- Programas malignos

- Medidas de prevención
  - Fortificación entradas
  - Guardia Jurado
  - Patrullas
  - Circuito cerrado TV
  - Control de accesos
  - Protección de software y hardware con un antivirus.

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 del 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.