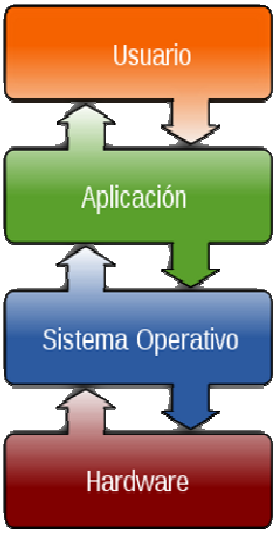
Sistemas Operativos, Bases de Datos, Redes

Sistemas de computación

- Componentes:
  - **Hardware**: unidad central de proceso (CPU), memoria, dispositivos de entrada/salida
  - **Sistema operativo**
  - **Programas de aplicación**: compiladores, aplicaciones de oficina, sistemas de bases de datos, aplicaciones internet, juegos
  - **Usuarios**: personas, maquinas, otros dispositivos



Sistemas operativos

- Un sistema operativo es un programa que actúa como intermediario entre el usuario y el hardware de la computadora, con el propósito de crear un entorno en que el usuario pueda ejecutar programas de forma **cómoda** y **eficiente**.
- El sistema operativo debe garantizar el funcionamiento correcto del sistema de la computadora.
- Ofrece ciertos servicios a los programas y a los usuarios de esos programas, con el fin de facilitar las tareas.
- Los servicios específicos ofrecidos difieren según el sistema operativo. (pero, hay un conjunto en común para todos)

Ejemplos

Sistema operativo= núcleo o kernel

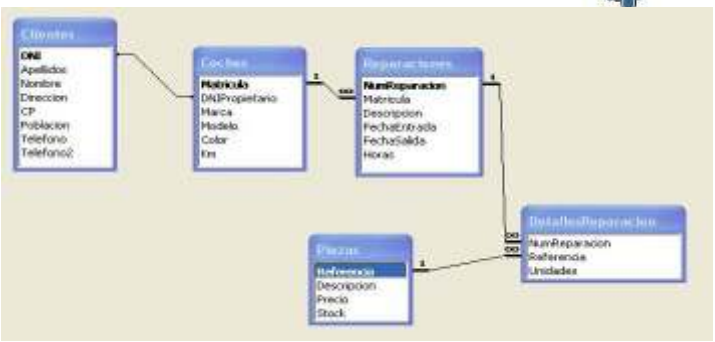
Bases de datos

- Una **Base de Datos** es un conjunto de datos organizados y relacionados que se encuentran agrupados ó estructurados para permitir un acceso directo a través de programas o lenguajes de consulta.
- Gráficamente similar a un *almacén* de datos, grandes volúmenes de información organizada según sus relaciones.
- Cada base de datos se compone de una o más tablas que guarda un conjunto de datos. Cada tabla tiene una o más columnas y filas. Las columnas guardan una parte de la información sobre cada elemento que queramos guardar en la tabla, cada fila de la tabla conforma un registro.

Modelos de bases de datos

- Bases de datos jerárquicas
- Base de datos en red
- Bases de datos transaccionales
- Bases de datos relacionales
- Bases de datos multidimensionales
- Bases de datos orientadas a objetos
- Bases de datos documentales
- Bases de datos deductivas

- Las BD utilizan lenguajes de consulta y gestión.



Redes de datos

- Durante las dos primeras décadas de existencia, los sistemas de computadoras estaban altamente centralizados y por lo general una sola máquina satisfacía las necesidades de una organización
- En las décadas de los 70 y 80 se produjo la integración entre el mundo de las comunicaciones y el campo de las computadoras, desencadenando un gran cambio tecnológico. (*no olvidar aparición de las PC)*

Resultado: conjunto de computadoras interconectadas para realizar tareas.

El inicio…Años 60

- 1960 ARPA (Agencia de Investigación de Proyectos Avanzados – DoD USA)
- 1964: ideas clave
  - red descentralizada con múltiples caminos entre dos puntos.
  - La división de mensajes completos en fragmentos que seguirían caminos distintos. La red estaría capacitada para responder ante sus propios fallos.
- Octubre de 1969:

  Primer mensaje de Internet: "login" . La **l** y la **o** llegan a destino pero en la **g** el sistema colapsa

Actualidad

- **2.405.518.376** usuarios de internet (Junio 2012) (http://www.internetworldstats.com/)
- **631.521.198** sites (http://news.netcraft.com/)
- 10^{18} bytes capacidad de almacenamiento (Exabyte)
- Velocidad de transmisión en Gb
- Dispositivos ultralivianos
- A partir del año 99 boom comercial de Internet

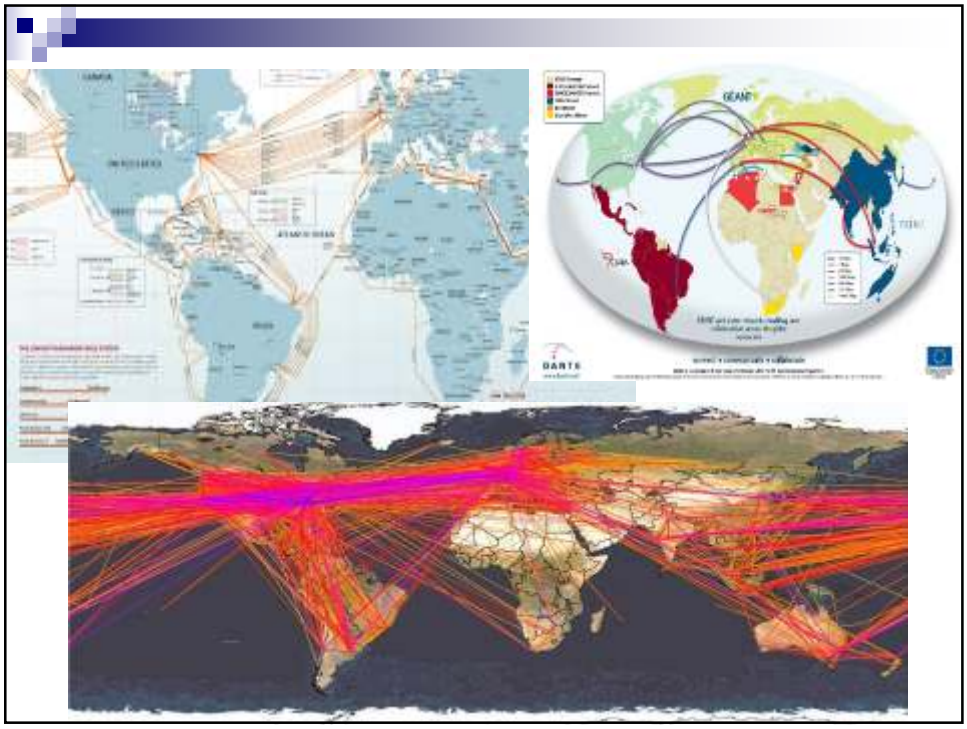
Qué es una red?

- **Red de computadoras**: colección de dispositivos autónomos interconectados, es decir, capaces de intercambiar información (Texto – Sonido - Imagen fija - Imagen en movimiento)

Elementos
- **Emisor**
- **Receptor**
- **Canal de transmisión**
- **Datos (señales)**

Inter-Net: interconexión de redes

Medios de trasmisión



WWW (World Wide Web)

- Es un sistema que asocia documentos hipermediales almacenados en equipos de computación interconectados a través de la red Internet.
- El conjunto de los servidores Web de Internet forman parte del World Wide Web, aunque no hay una administración central ni una coordinación de servidores.
- Cada servidor se identifica por una dirección **IP**, mientras que cada recurso o documento en un servidor Web está designado por una dirección **URL**.

Ejemplos
IP: 200.3.115.8
URL: www.fcad.uner.edu.ar

Un mundo de protocolos

- **Protocolo**: conjunto de reglas y requisitos que permite organizar la comunicación entre partes. Comunicación dentro de la PC, comunicación entre sistemas, entre computadoras, etc.
- Ejemplo protocolos de red:
  - IP: Protocolo Internet
  - FTP: protocolo transferencia de archivos entre equipos
  - SMTP: protocolo de correo electrónico Administración de sistemas HTTP: Protocolo transferencia de hipertexto (www)
  - H323: conjunto de protocolos para videoconferencias.
  - VoIP: protocolos para transmitir voz sobre internet
  - TCP: protocolo para transportar datos sobre internet.

Aplicaciones

- Browsers: Firefox, Chrome, IE, Opera
- Buscadores: Google, Bing, Yahoo, Lycos, DuckDuckGo
- Metabuscadores: Carrot, MetaCrawler
- Videos: YouTube
- Información social: Facebook, Twitter
- Sistemas de etiquetados: RSS
- Correo internet (webmail): Hotmail, Gmail
- Voz: Skype, Hangouts
- Etc…etc…etc..

Seguridad informática

- Siempre hay que tener en cuenta que la seguridad comienza y termina con **personas**
- No existe un sistema 100% seguro.
- La implementación de un sistema de seguridad incrementa la complejidad en la operatoria de la organización, tanto técnica como administrativa.(disminución de la funcionalidad)
- Algunas organizaciones gubernamentales y no gubernamentales internacionales han desarrollado documentos, directrices y recomendaciones que orientan en el uso adecuado de las nuevas tecnologías para obtener el mayor provecho y evitar el uso indebido de la mismas, lo cual puede ocasionar serios problemas en los bienes y servicios de las empresas en el mundo.
- En este sentido, las Políticas de Seguridad Informática (PSI), surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos. Estos permiten a la compañía desarrollarse y mantenerse en su sector de negocios.

Seguridad informática

- **Seguridad Física** consiste en la "*aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial*". Controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo.
- Las principales amenazas que se prevén en la seguridad física son:
  - Desastres naturales, incendios accidentales tormentas e inundaciones.
  - Amenazas ocasionadas por el hombre.
  - Disturbios, sabotajes internos y externos deliberados.
- Ejemplo: Control de Acceso
  - El control de acceso no sólo requiere la capacidad de identificación, sino también asociarla a la apertura o cerramiento de puertas, permitir o negar acceso basado en restricciones de tiempo, área o sector dentro de una empresa o institución.

Seguridad informática

- **Seguridad Lógica** "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."
- Algunos objetivos :
  - Restringir el acceso a los programas y archivos.
  - Asegurar que los operadores no puedan modificar los programas ni los archivos que no correspondan.
  - Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.
  - Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
  - Que la información recibida sea la misma que ha sido transmitida.
- **Ejemplo: Controles de Acceso**

  Estos controles pueden implementarse en el Sistema Operativo, sobre los sistemas de aplicación, en bases de datos, en un paquete específico de seguridad...

- **Seguridad en redes** es mantener bajo protección los recursos y la información con que se cuenta en la red, a través de procedimientos basados en una política de seguridad tales que permitan el control de lo actuado.
  - Seguridad en los equipos
  - Seguridad en los enlaces de comunicación
  - Seguridad en las aplicaciones

- **Garantizar**:
  - **Confidencialidad:** la información en un computador o que circula por la red es accesible solo a los entes autorizados
  - **Integridad:** los recursos del computador o la información circulante son modificados (escribir, cambiar datos o estado, suprimir, crear) solo por entes autorizados
  - **Disponibilidad:** los recursos del computador están disponibles a los entes autorizados

Ejemplo ataques activos: Código malicioso

Se define como todo programa o fragmento del mismo que genera algún tipo de problema en el sistema en el cual se ejecuta, interfiriendo de esta forma con el normal funcionamiento del mismo. Existen diferentes tipos de código malicioso:

- **Bombas lógicas**: Se encuentran diseñados para activarse ante la ocurrencia de un evento definido en su lógica.
- **Troyanos:** Suele propagarse como parte de programas de uso común y se activan cuando los mismos se ejecutan.
- **Gusanos**: Tienen el poder de autoduplicarse causando efectos diversos.
- **Virus**: distribuidos a través de adjuntos de correo electrónico.

Delitos informáticos

- Se define como toda acción u omisión culpable realizada por un ser humano, que cause un perjuicio a personas sin que necesariamente se beneficie el autor o que, por el contrario, produzca un beneficio ilícito a su autor aunque no perjudique de forma directa o indirecta a la víctima, que se realiza en el entorno informático y está sancionado con una pena

Marco legal vigente

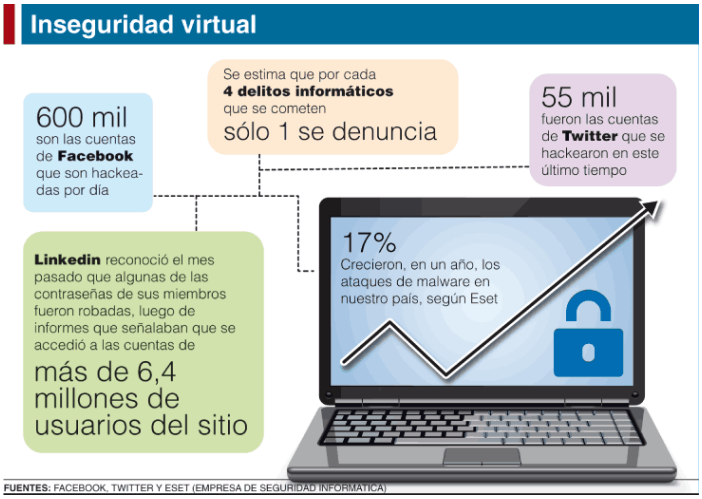
- Ley 24.766 de Confidencialidad (30/12/96)
- Ley 24.769 Penal Tributaria (15/01/97)
- Ley 25.036 Propiedad Intelectual (15/11/98)
- Ley 25.236 Habeas Data (02/11/00)
- Ley 25.506 Firma Digital (14/12/01)
- Ley 25.520 Inteligencia Nacional (06/12/01)
- Ley 25.873 Nacional de Telecomunicaciones (09/02/04)
- Ley 25.891 Servicio de Comunicaciones Móviles (25/05/04)
- Ley 26.388- Código Penal (Junio de 2008)

Internet y Ética- RFC 1087

- Determina: que es inmoral e inaceptable cualquier actividad que a propósito trate de:
  - Obtener acceso no autorizado a recursos de internet
  - Alterar el destino/uso de la red
  - Generar mal uso de los recursos como consecuencia de esas acciones
  - Destruir/atentar contra la integridad de la información
  - Poner en peligro la privacidad de los usuarios

Contempla todos los usuarios y usos:
Académicos, investigación, usuario hogareño

Un problema que crece



Robo de identidad – Robo de datos

Contenidos curriculares de:

- Arquitectura de Computadoras, Sistemas Operativos, Bases de datos, Comunicaciones y Redes, Seguridad y Control de Sistemas, Ética y Deontología Profesional.
- Seguridad: contenido transversal en la mayoría de las asignaturas del Plan de Estudios