Resumen Libro 2 — H1.

Redes

- Arquitectura de comunicaciones → Software que da soporte a un grupo de computadores en red. Brinda soporte a las aplicaciones.
  - La mas utilizada es un conjunto de protocolos TCP/IP
- Sistemas Operativos de red → Red de maquinas, estaciones de trabajo de un solo usuario y una o mas maquinas servidoras.
  - Brindan servicios de red o aplicaciones.
  - El sistema operativo de red es añadido al SO Local que permite conectarse a los servidores.
- Sistemas Operativos Distribuidos → Sistema Operativo compartido por red de computadores.
  - Les provee acceso a recursos de diversas maquinas
  - Puede depender de una arquitectura de comunicaciones

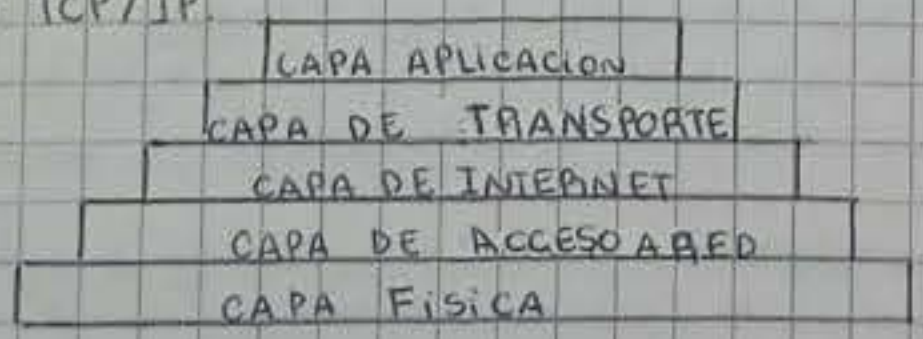
LA NECESIDAD DE UNA ARQ. DE PROTOCOLOS.

- Protocolo → se utiliza para comunicar entidades de diferentes sistemas
  - Conjunto de reglas que gobiernan el intercambio de datos entre dos entidades.
  - Elementos → Sintaxis → Formato de datos y niveles de señales
    - Semantica → Info de control para realizar coordinacion y gestion de errores.
    - Temporizacion → Ajustes de velocidades y secuenciamiento.
- Arquitectura de protocolos → descomposicion de una tarea en subtareas, las cuales se pueden implementar de forma individual

LA ARQUITECTURA DE PROTOCOLOS TCP/IP.

- Protocolos llevados a cabo en la red de intercambio de paquetes.
- Utilizados como estandares de internet.

- CAPAS TCP/IP.



- Capa Fisica → Cubre la interfaz fisica entre un dispositivo de transmicion de datos y un medio de transmicion o red.
- Capa de acceso a red → Se preocupa del intercambio de datos entre un sistema final y la red a la que esta unido.
- Protocolo de Internet → se utiliza como funcion de encaminamiento entre redes.
  - un encaminador se encarga de conectar dos redes.

- Capa de Transporte → Asegura que los datos lleguen a la aplicacion destino y que los reciban en el orden que fueran enviados.

- Capa de aplicacion → Contiene la logica necesaria para soportar las aplicaciones de usuario.

TCP → Protocolo de la capa de transporte, proporciona una conexion fiable para transmitir datos entre aplicaciones.
→ Una conexion es simplemente una asociacion logica temporal entre dos entidades de diferentes sistemas.

Sockets → Permite la comunicación entre un proceso cliente y un proceso servidor y puede ser orientado a conexion o no orientado a conexion.
→ Puede ser considerado como un punto final en la comunicacion.
→ Cada vez que entran en comunicacion los sockets → los computadores pueden intercambiar informacion.
→ Se utiliza para definir una interfaz de programacion de aplicaciones.

¿Que es la computacion Cliente / servidor?.

- Entorno entre clientes y servidores
- Las maquinas cliente → son estaciones de trabajo que proporcionan una interfaz de facil manejo para el usuario final

- Terminologia:

- Interfaz de programacion de aplicacion → Conjunto de funciones y programas que permiten a los clientes y servidores intercomunicarse.

- Cliente → Un elemento de la red que solicita informacion, normalmente un PC o estacion de trabajo. Puede interrogar a una base de datos o solicitar info de un servidor.

- Middleware → un conjunto de controladores, API y software adicional que mejoran la conectividad entre una aplicacion cliente y un servidor.

- Base de datos relacional → Una base de datos en la que el acceso a la informacion esta restringido por la seleccion de filas que satisfacen todos los criterios de busqueda.

- Servidor → Un computador, normalmente una estacion de trabajo de gran potencia, un microcomputador, o un mainframe, que almacena la informacion para los clientes de la red.

- Lenguaje estructurado de consultas → Lenguaje desarrollado por IBM, y estandarizado por ANSI que permite acceder, crear, actualizar e interrogar base de datos relacionales.

- Características.

- Es imperativo que los usuarios tengan aplicaciones de facil manejo en sus sistemas. Gran control del usuario sobre su computadora.

- Apesar de apps dispersas, se hace un esfuerzo para centralizar las bases de datos corporativas y muchas funciones de utilidad y de gestion de redes.

- Existe un compromiso entre organizaciones y vendedores de mantener un sistema abierto y modular

- La red tiene una prioridad muy alta en la organizacion y funcionamiento de los sistemas de información.

Middleware.

- Conjunto de Interfaces de programacion y protocolos estandares entre aplicaciones y el software de comunicaciones y el sistema operativo

Estacion del cliente

Servicios de Presentacion
Logica de aplicación
Middleware
Software de comunicación
Sist. Operativo cliente
Plataforma de Hardware

Servidor

Middleware	
sw. de comunicaciones	servicios de app
Sist. Operativo servidor	
Plataforma Hardware.	

Paso de mensaje distribuido.

- Fiable → Garantiza la entrega si es posible.
  - No es necesario informar al proceso que el envio fue exitoso.
  - Informa solo en caso de error.

- No fiable → Envia mensaje a la red, pero no informa ni exito ni Fracaso.

- No bloqueante. → No se suspende a un proceso como resultado de realizar un Send o Receive

- bloqueante → No devuelve el control al proceso emisor hasta que el mensaje ha sido transmitido o hasta que el mensaje ha sido enviado y se ha recibido el acuse de recibo.

Llamadas a procedimientos
- Sincrono → Requiere que el proceso llamante espere hasta que el proceso llamado devuelva el valor.
- Asincrono → No bloquean al llamante, las respuestas se pueden recibir como y cuando sean requeridas, permitiendo de esta forma al cliente ejecutar en paralelo con el servidor.

- **Clusters** → Son sistemas que proporcionan un alto rendimiento y alto disponibilidad
  - → Grupo de computadoras completas e interconectadas, que trabajan en conjunto como un recurso de computacion unificado.
  - → Caracteristicas
    - → Escalabilidad absoluta
    - → Escalabilidad incremental
    - → Alta disponibilidad
    - → Relacion precio/prestaciones.
  - → Servicios o Funciones
    - → Unico punto de entrada
    - → Unica jerarquia de ficheros
    - → Unico punto de control
    - → Unica red virtual.
    - → Unico espacio de memoria.
    - → Unico sistema de control de trabajos
    - → Unica interfaz de usuario.
    - → Unico espacio de E/s
    - → Unico espacio de procesos.
    - → Puntos de control.
    - → Migracion de procesos.

Seguridad.

- **Requisitos basicos**
  - **Confidencialidad** → La informacion debe poder leerse solo por aquellas partes autorizadas.
  - **Integridad** → La informacion debe poder ser modificada por aquellas partes autorizadas.
  - **Disponibilidad** → Los componentes del sistema deben poder estar disponibles para las partes autorizadas.
  - **Autenticación** → El sistema informatico debe poder ser capaz de verificar la identidad del usuario.

- **Tipos de peligros**
  - **Interrupcion** → Ataque centrado a la disponibilidad
  - **Intercepcion** → Ataque centrado a la confidencialidad.
  - **Modificacion** → Ataque centrado a la integridad
  - **Fabricacion** → Ataque centrado a la autenticacion.

- Componentes de un sist. Informatico.
  - Categorias
    - Hardware → Daño a los equipos, o robo de los mismos
      - Principal peligro → Disponibilidad.
    - Software → Borrado de programas y denegacion de acceso a usuarios.
      - Copia no autorizada de software.
      - Modificacion de un programa con fin malintencionado.

Tipos de ataques

- Pasivos → Son el espionaje o la monitorizacion de mensajes.
  - Analisis de trafico.
- Activos → Enmascaramiento → Ocurre cuando un elemento intenta hacerse pasar por otro diferente, dejandolo tener beneficios extra.
  - Reenvio → Implica la captura pasiva de una unidad de datos y su posterior retransmision para producir un efecto no autorizado.
  - Modificacion de mensajes → una parte del mensaje ha sido alterado o han sido borrados o reordenados para producir un efecto no autorizado.
  - Denegacion de servicio → previene o imposibilitar el uso normal o la gestion de las instalaciones de comunicaciones
    - Ej: Un elemento suprime todos los mensajes a un objetivo especifico.

- Protección → Recursos a proteger → Procesador
  - Memoria
  - Dispositivos E/s
  - Programas
  - Datos
  - Niveles de protección → Sin proteccion
    - Aislamiento → cada proceso trabaja por su propia cuenta sin compartir o comunicarse con otro proceso.
    - Compartición completa o sin compartición → define si el objeto es publico o privado.
    - Compartido via limitaciones de acceso → El so verifica si el que quiere acceder esta autorizado.
    - Acceso via capacidades dinamicas → creacion dinamica de derechos de acceso a los objetos.
    - Uso limitado de un objeto → Limita no solo el uso sino el acceso a un objeto.

Software Malicioso

- Puerta Secreta → Posee un acceso sin utilizar los procedimientos de acceso de seguridad estandar
- Bomba Logica → Es un codigo insertado dentro de un programa, que se ejecutara bajo ciertas condiciones.
- Troyano → Es un programa o mandato que contiene un codigo oculto; que al invocarse, realiza una funcion malisiosa.
- Gusano → utilizan la red para expandirse de un sistema a otro.
- Zombie → Toma el control de otro equipo mediante internet y lo utiliza para lanzar ataques.

- Tipos de virus →
  - Virus parasito
  - Virus residente en memoria
  - Virus en el sector de arranque
  - Virus Oculto
  - Virus polimorfico.

Sistemas distribuidos

- Redes de Area Local (LAN) → Permiten la conexion de varios equipos en un mismo espacio fisico.
- Redes de Area Amplia (WAN) → Permiten que millones de maquinas en toda la tierra con gran velocidad.
- Sistemas distribuidos → Sistema de computo compuesto por un gran número de CPU conectados mediante una red de alta velocidad.
  Es una coleccion de computadoras independientes que aparecen ante los usuarios del sistema como una unica computadora.
  - Aspectos - El hardware → Las maquinas son autonomas
    - El software → Los usuarios piensan que es una unica computadora.

- Ventajas con respecto a los sistemas Centralizados.
  - Permite trabajar a muchos usuarios de manera conjunta.
  - Distribucion de applicaciones de manera inherente. → Hacer que el sistema se vea como una sola computadora para las aplicaciones.
  - Descentralizacion.
  - Trabajos y juegos cooperativos apoyados por computadora → Conexiones a otro nivel y desde multiples localizaciones.
  - mayor confiabilidad → Distribuir carga de trabajo en varios equipos.
  - Crecimiento por incrementos → añadir procesadores para un desarrollo gradual.

- Ventajas con respecto de las Pc independientes.
  - Conexion entre maquinas y datos compartidos.
  - Perifericos compartidos
  - mayor flexibilidad potencial

- Desventajas de los sistemas distribuidos
  - Perdida de mensajes → implica la utilizacion de un software especial.
    - dependencia de la red.
  - Software distribuido especifico.
  - Seguridad en el acceso de la informacion compartida.

Diferencias entre tipos de sistemas.

Elemento.	So de red	So Distr..	So de Mul.
¿Se ve como un uniprocesador virtual?	No	Si.	Si.
Todos tienen que ejecutar el mismo SO?	No	Si	Si
Cuantas copias del sistema operativo existen?	N	N	1.
Como se logra la comunicación?	Archivos compartidos	Mensajes	Memoria compartida
¿Se requiere un acuerdo en los protocolos de la red?	Si	Si	No
Existe una cola de Ejecucion?	NO	No	Si
Existe una semantica bien definida para los archivos compartidos?	No	Si	Si

Aspectos del diseño.

- Transparencia → Ocultar distribucion a los usuarios
  - Diseño de una interfaz de llamadas al sistema de modo que no sea visible la existencia de varios procesadores.
  - Tipos → localizacion → los usuarios no pueden indicar la localizacion de los recursos.
    - Migracion → Los recursos se pueden mover sin cambiar el nombre.
    - Replica → Los usuarios no pueden indicar el numero de copias existentes
    - Concurrencia → Varios usuarios pueden compartir recursos de manera automatica.
    - Paralelismo → Las actividades pueden ocurrir en paralelo sin el conocimiento de los usuarios.

- Flexibilidad → La mejor Forma de evitar errores es estar abierto a opciones
  - Tipos de nucleo → monolitico → SO centralizado basico actual, aumentado con capacidades de red y la integracion de servicios remotos.
    - La mayoria de las llamadas al sistema se realizan mediante señalamientos al nucleo.
  - Microncleo. → servicios → Un mecanismo de comunicacion entre procesos
    - Cierta adm. de memoria
    - Una cantidad limitada de planificacion y administracion de procesos de bajo nivel
    - Entrada/salida de bajo nivel.
  - Capacidad de añadir, eliminar y modificar servicios.

- Confiabilidad → Si una maquina falla, otra ocupe su lugar y realice el trabajo.
  - Una cierta cantidad de servidores funcionan para ejecutar el sistema.
  - Disponibilidad → Fraccion de tiempo en que se puede utilizar el sistema.
    - Se puede mejorar mediante un diseño que no exija el funcionamiento simultaneo de un numero sustancial de componentes criticos.
    - Redundancia.
  - Los archivos y recursos deben ser protegidos contra el uso no autorizado.
  - Tolerancia a fallas.
  - Ocultar Fallas a los usuarios.

- Desempeño → Tiempo de respuesta.
  - Numero de trabajos por hora
  - Cantidad consumida de capacidad de red.
  - problema → Retraso en envio de mensajes.
  - Estrategias → Ejecutar varias cosas en paralelo → Paralelismo de grano fino
    - Paralelismo de grano grueso

- Escalabilidad → Componentes centralizados → Un solo servidor de correo para todos los usuarios.
  - Tablas centralizadas → Un directorio telefonico en linea
  - Algoritmos centralizados → Realizacion de un ruteo con base en la Información completa.
  - Diferencia respecto a sistemas centralizados
    - Ninguna maquina tiene la info completa acerca del estado del sistema
    - Las maquinas toman decisiones sólo con base en info local.
    - La falla de una maquina no arruina el algoritmo.
    - No existe una hipotesis implicita de la existencia de un reloj global.

- Proteccion
  - Proteccion de la memoria
  - Control de acceso orientado a usuario → Identificacion Usuario/password.
    → Arquitectura Single sign on
  - Control de acceso orientado a datos → Permisos especificos para determinados usuarios.
    → Matriz de acceso.
      - Sujeto
      - Objeto
      - Derecho de acceso.
    → Lista de control de acceso
    → Tickets de capacidades.

- Intrusos
  - Enmascarado → Un individuo que no está autorizado a utilizar un ordenado y que penetra en los controles de acceso del sistema para aprovecharse de una cuenta de usuario.
  - Trasgresor → Usuario legitimo que accede a datos, programas o recursos para los cuales dicho acceso no está autorizado, o si esta autorizado usa los recursos de forma maliciosa.
  - Usuario Clandestino → Un usuario que sobrepasa el control de supervision del sistema y usa dicho control para evadir la auditoria y el control de acceso o para suprimir la recogida de registros de acceso.

- Tecnicas de intrusión
  - Formas de proteccion de fichero de contraseña → Cifrado Unidireccional
    → Control acceso.
  - Estrategias de seleccion de contraseñas → Educacion de los usuarios
    → Contraseñas generadas por ordenador
    → Verificacion reactiva
    → Verificacion proactiva.

- Deteccion de Intrusos
  - Bitacoras (registros de sucesos y logs)
  - Deteccion de anomalias → por umbral
    → Basado en el perfil.
  - Prevención.