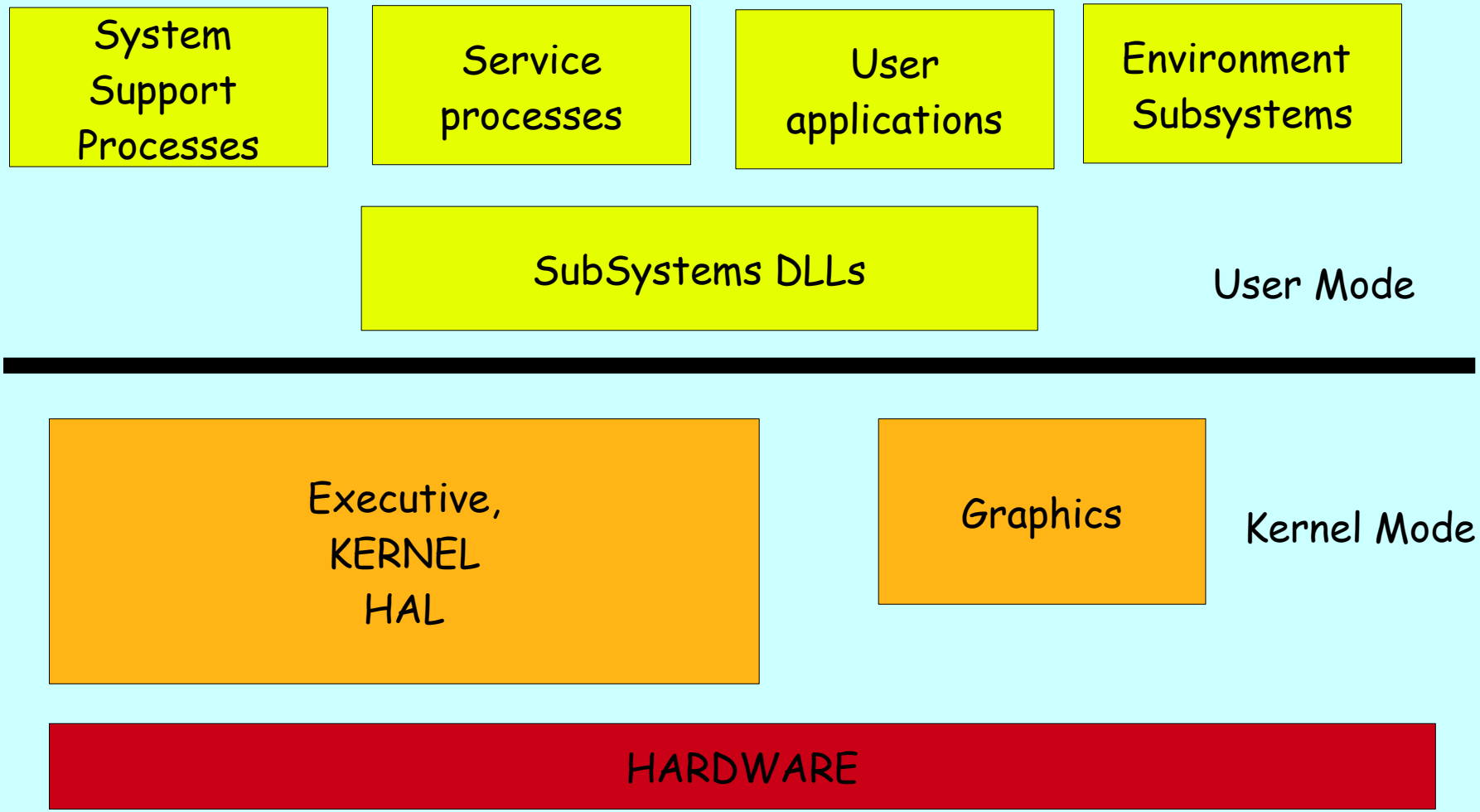
75-08 Sistemas Operativos
Lic. Ing. Osvaldo Clúa
2010

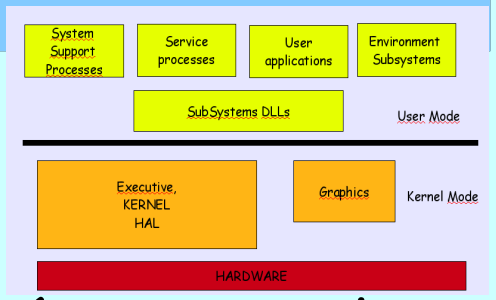
Facultad de Ingeniería
Universidad de Buenos Aires

Mecanismos básicos en Windows (XP, 7)

Arquitectura Simplificada

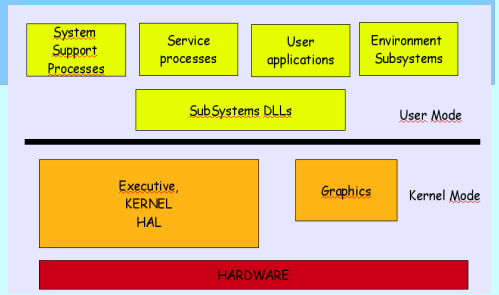


User Mode Processes



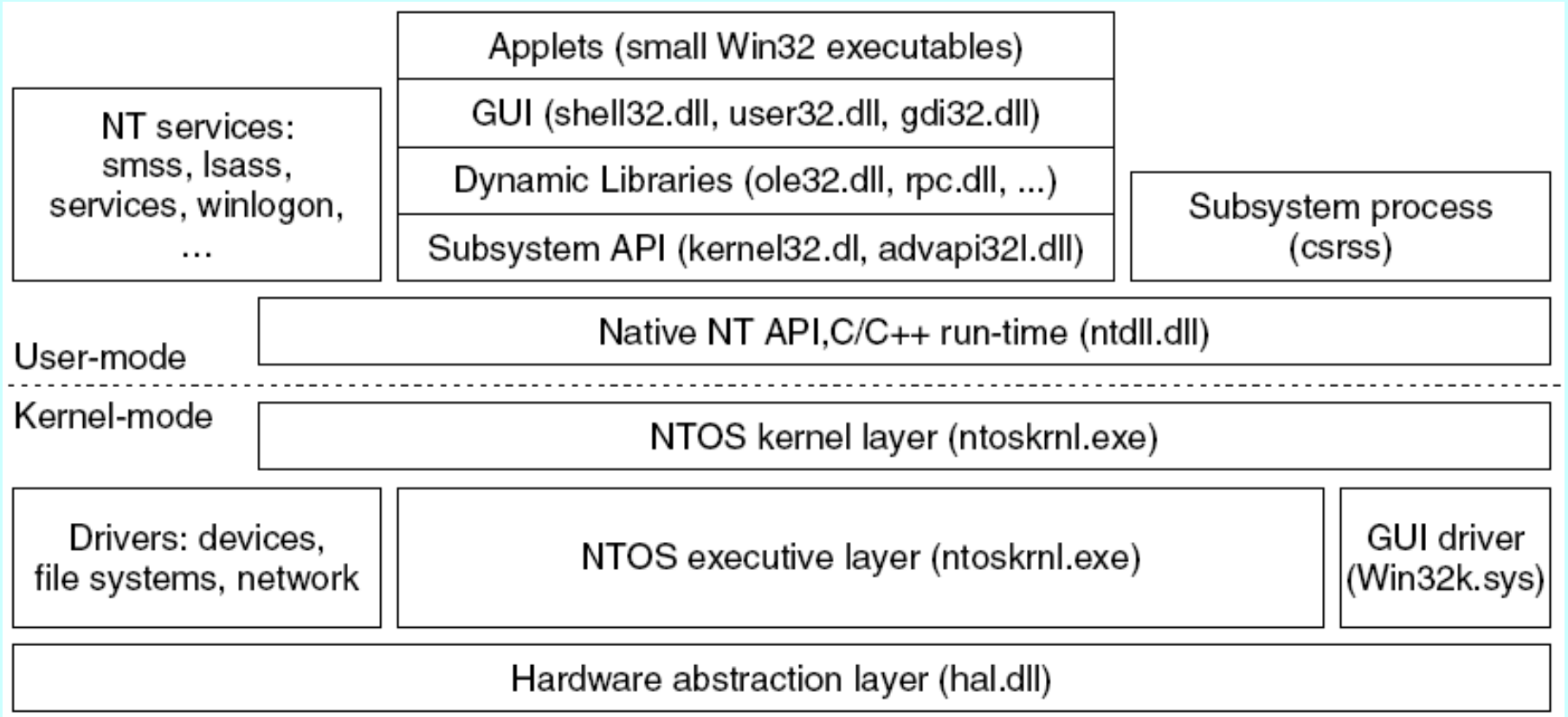
- System Service Processes.
  - Servicios generales no-windows (no iniciados por el Service Control Manager)
    - Logon, Session Manager ...
- Service processes
  - Son servicios windows, independientes del subsistema
    - Task Scheduler, SQL Server ...

Componentes User Mode

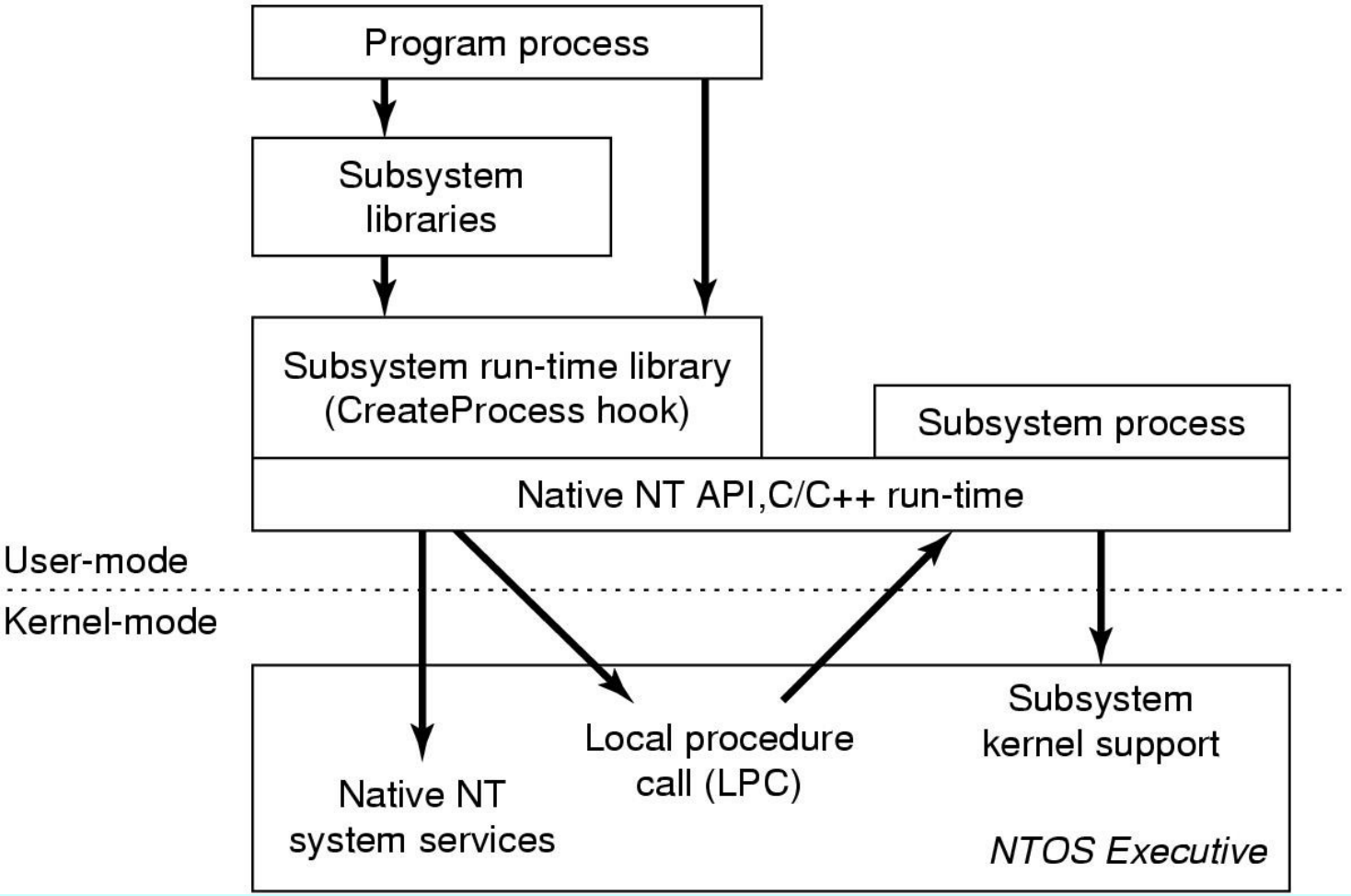


- User Applications.
  - Corresponden a Win 16, Win 32, Win 64, DOS ...
- Environment Subsystem
  - Personalidad presentada al programador.
- Las aplicaciones no usan los servicios del Sistema Operativo directamente ...
  - ... usan las DLL's del subsistema ..
    - ... que puede (o no) comunicarse con el Environment Subsystem

Capas de Programación en Win



Llamado al sistema en Win



Archivos del sistema

Core OS components:

NTOSKRNL.EXE		Executive and kernel
NTKNNLPA.EXE	(32 bits)	PAE para sistemas de 32 bits
HAL.DLL		Hardware abstraction layer
NTDLL.DLL		Internal support functions and system service dispatch stubs to executive functions

Core system processes:

SMSS.EXE	Session manager process
WINLOGON.EXE	Logon process
SERVICES.EXE	Service controller process
LSASS.EXE	Local Security Authority Subsystem

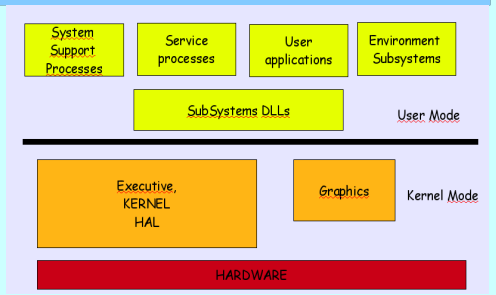
Windowing subsystem:

CSRSS.EXE	Windows subsystem process
WIN32K.SYS	USER and GDI kernel-mode components
KERNEL32/USER32/GDI32.DLL	Windows subsystem DLLs
ADVAPI32.DLL (Win 7)	

“Kernel”

- En Windows puede referirse a:
  - Todo el código que se ejecuta en “Kernel mode”
  - *ntoskrnl.exe* (archivo con kernel+executive)
  - Kernel layer en *notskrnl.exe*
  - User mode Win32 library *kernel32.dll*

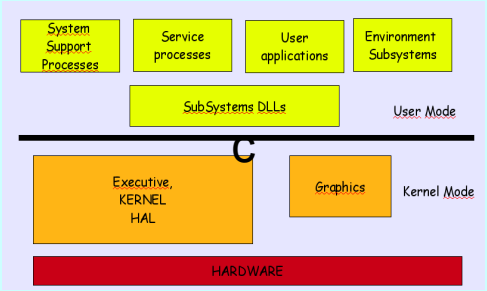
Componentes Kernel Mode



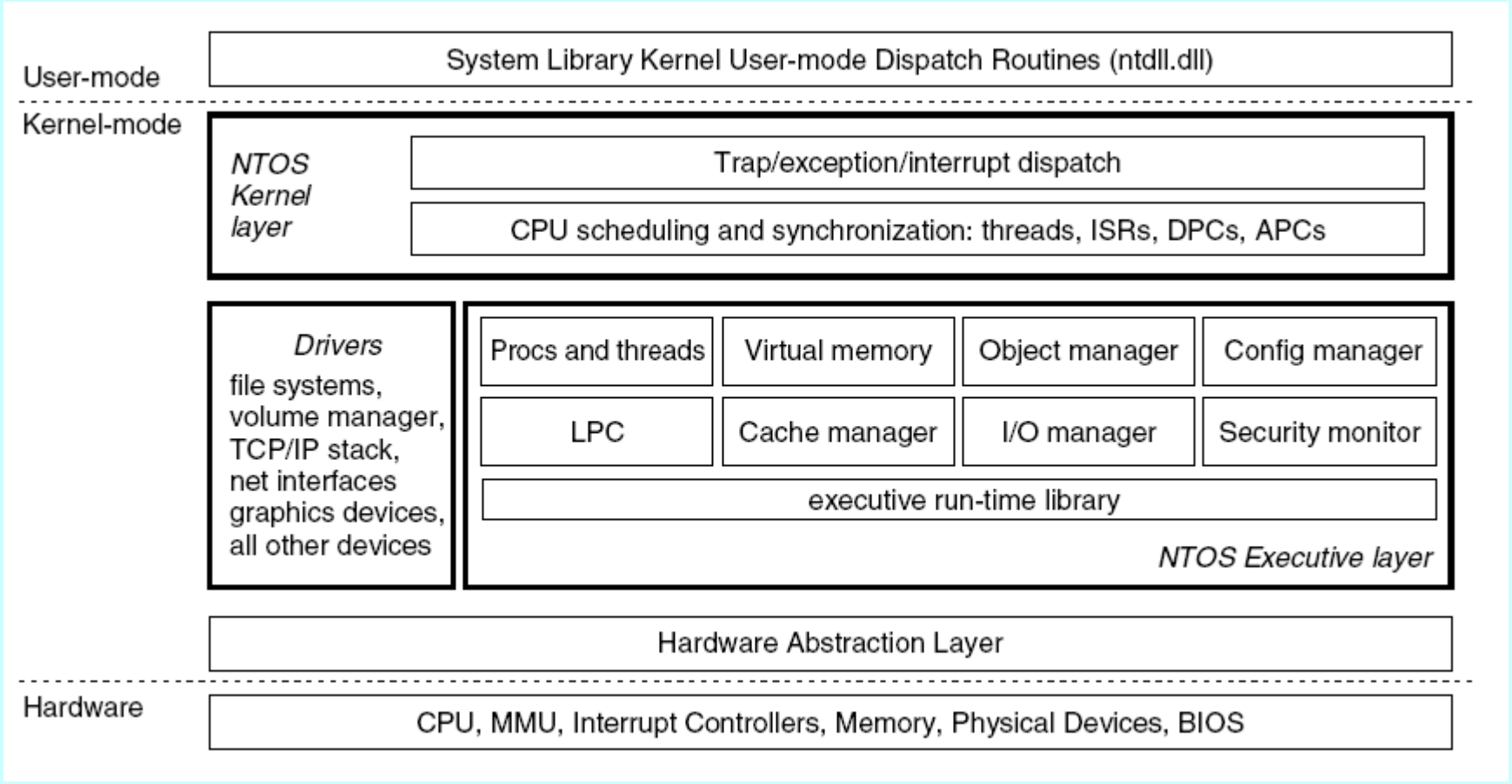
- Executive
  - Con las funciones básicas
    - Red, seguridad, administración de memoria, administración de procesos, Intercomunicación de procesos, administración de I/O, Hyper-V.
- Kernel
  - Funciones de bajo nivel
    - Despacho de interrupciones, planificación de threads y administración de objetos (del SO)

Componentes Kernel Mode

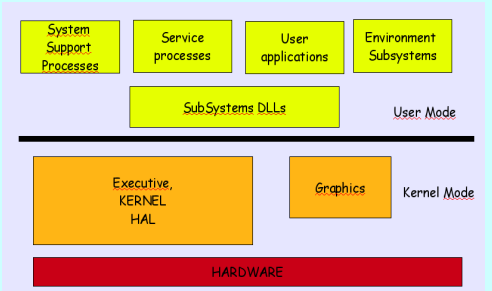
- Drivers
  - Manejo de la I/O de bajo nivel.
- HAL (Hardware Abstraction Layer)
  - Aisla al kernel de las diferencias de hard.
- Gráficos
  - Implementa las funciones USER y GDI para el manejo de ventanas y gráficos.



Detalle del Kernel



SubSistemas



- La idea era presentar distintas personalidades al programador.
  - OS/2 para migrar programas --- discontinuado.
  - POSIX para correr aplicaciones UNIX --- instalación opcional y funcionalidad limitada.
  - WINDOWS para presentar una interface WIN32.
    - Necesaria para poder correr el Sistema Operativo.

Windows SubSystem

- CSRSS.exe
  - Maneja la consola, crea procesos y threads.
- WIN32K.sys
  - Administra ventanas y gráficos (GDI).
- SubSystem DLL
  - Traduce las APIs documentadas en llamadas a las funciones no-documentadas al sistema.

NTOSKRNL

- Contiene al Executive y al Kernel
  - Además incluye entry points para rutinas de Hal.Dll
- Cuatro variantes:
  - NTOSKRNL.EXE Uniprocessor
  - NTKRNLMP.EXE Multiprocessor
  - NTKRNLPA.EXE Uniprocessor w/extended addressing support (Page Address Extention)
  - NTKRPAMP.EXE Multiprocessor w/extended addressing support

Executive

- "Upper layer" de NTOSKRNL.EXE
- Provee "generic operating system functions" ("services")
  - Process Manager
  - Object Manager
  - Cache Manager
  - LPC (local procedure call) Facility
  - Configuration Manager (Registry)
  - Memory Manager
  - Security Reference Monitor (Common Criteria)
  - I/O Manager
  - Power Manager
  - Plug-and-Play Manager
- Código C , corre en modo privilegiado (ring 0), con interfaces no documentadas

Kernel

- "Lower Layer" de NTOSKRNL.EXE
  - Implementa dos mecanismos de comunicación
    - DPC (Deferred Procedure Call)
      - Difiere la ejecución de una rutina de atención de interrupciones (ISR, *Interrupt Service Routine*) hasta que terminen las rutinas de mayor prioridad.
    - APC (Asynchronous Procedure Call)
      - Difiere la ejecución de rutinas en el ambiente de un thread hasta su planificación (ej: retorno de interrupción)
      - Parecido a las *signal* de UNIX.

Local Procedure Call (LPC)

- Interface "no documentada" para comunicarse con los Environment Subsystems y los System Support Processes.
  - Es una cola de mensajes. Tiene un mecanismo especial para mensajes cortos.
  - La usan las subsystem dll para implementar sus funciones.
  - En Vista se extiende a ALPC (Advanced LPC).

Procesos del Sistema

- Idle Process (un thread por CPU que corre en el tiempo ocioso).
- lsass.exe (local security administration services).
- Logon (winlogon.exe).
- Session Manager (smss.exe).
- Service Control Manager (SCM)
- System Process (contiene threads que corren en modo kernel, agrupados por svchost.exe).
- Windows Subsystem (csrss.exe).

Servicios

- Creados y administrados por el SCM (Service Control Manager Services.exe)
  - El SCM es un LPC server.
  - Parecidos a los daemons de UNIX.
  - En general no interactúan con el Desktop ni con el usuario.
- Los servicios pueden tener tres nombres:
  - Registry, Service tool, Process name.