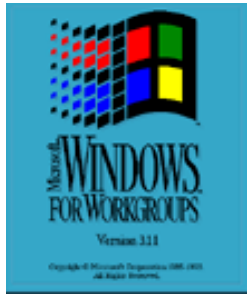









# Sistema Operativo Windows

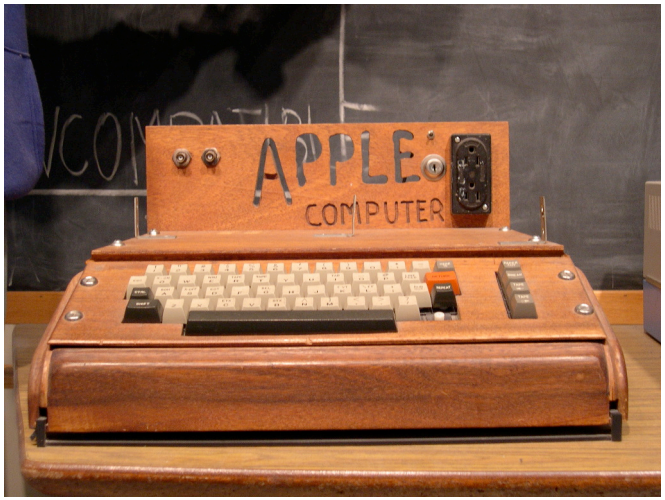
MSc. Ivan A. Escobar

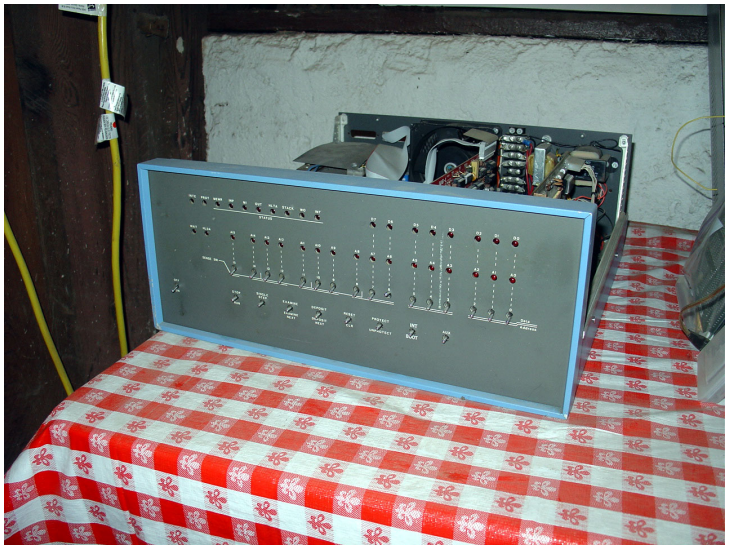
iescobar@itesm.mx





# Un poco de historia…



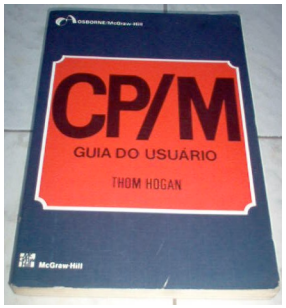





www.fortunecity.com/marina/reach/435/micro.htm

# Los personajes

Gary A. Kildall



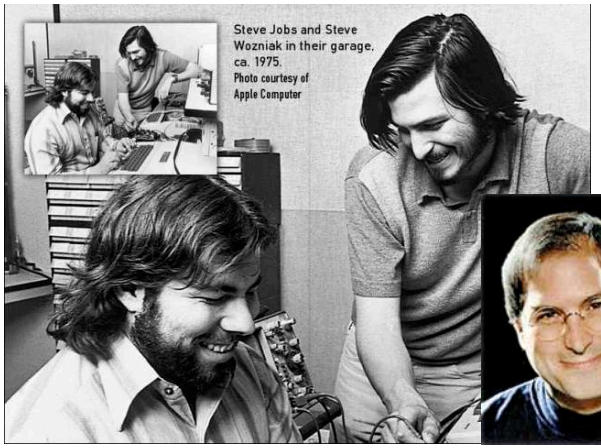

Ed Roberts with the Altair 8800

Rod Canion, Jim Harris and Bill Murto

Paul Allen y Bill Gates

Bill Gates y Paul Allen

Tim Patterson




Steve Wosniak y Steve Jobs

William C. "Bill" Lowe

# Versiones

- Windows 1
- Windows 2
- Windows/386
- Windows 3.0
- Windows 3.1
- Windows 3.11
- Windows for Workgroups 3.1
- Windows 95
- Win32s
- Windows 98
- Windows NT 3.1
- Windows NT 3.5
- Windows NT 4
- Windows 2000
- Windows CE
- Windows XP
- Windows 2003 Server

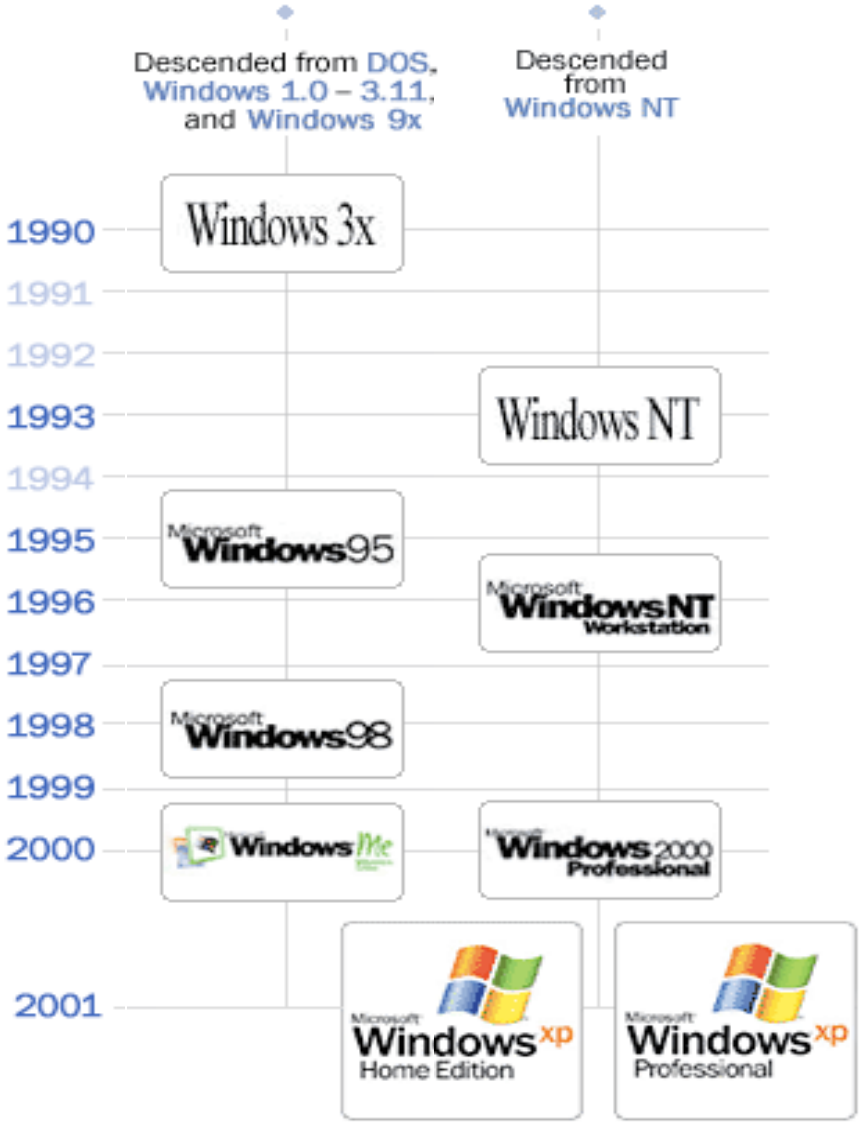
# Características versiones (1)

| Win 1 | Win 2/286 | Win /386 | Win 3.0 | Win 3.1 | Win 3.11 workgroups |
|---|---|---|---|---|---|
| 20 ago 85 | otoño 1987 | finales 1987 | 30 may 1990 | abr 1992 | 3.1 oct 92<br>3.11 nov 93 |
| DOS en desarollo | DOS en desarollo | múltiples máquinas virtuales DOS | direccionar más alla de 640 Kb | OLE<br>Object Linking Embedding | soporte red |
| interfaz gráfica | interfaz gráfica | | se agrega admon. programas y archivos | DDE Dynamic Data Exchange | incorpora el modelo cliente/ servidor |
| no ventanas traslapadas | ventanas traslapadas | | | | |

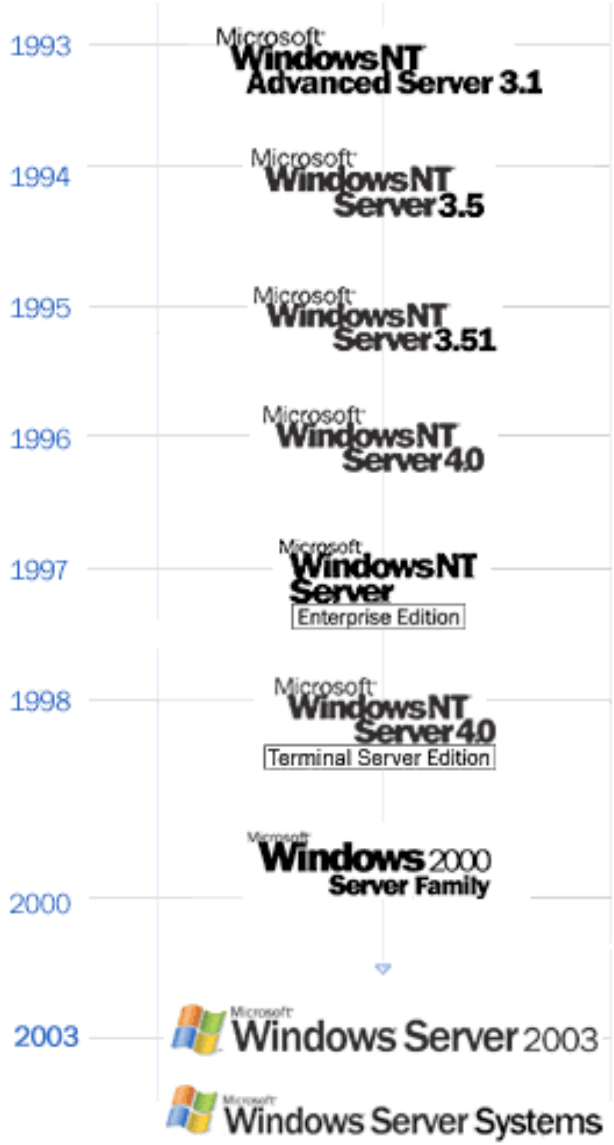
# Características versiones (2)

| Win 95 | Win 98 | Win 32S | Win NT 3.1 | Win NT 3.5 | Win NT 4.0 |
|---|---|---|---|---|---|
| 4 ago 95 | junio 1998<br>SE: may 1999 | feb 1996 | julio 1993 | sep 1994 | ago 1996 |
| Deja de ser solo un interfaz | soporte FAT 32 | conjunto librerisa para win 3.1 | New Technology<br>Sist. Archivos: FAT, NTFS y HPFS | versión servidor y estación de trabajo | denominada CAIRO |
| MS DOS 7.0 es una aplicación | Soporte drivers USB y DVD | posible correr programas NT en 3.1 | direccionamiento 4G en RAM | | |
| stack TCP/ IP integrado al núcleo | Internet Explores 5.0 y Net Meeting 3.0 | | versión servidor y estación trabajo | | |

# Historia: Desktops



# Historia: Servers




TEC
DE MONTERREY
Campus Estado de México


microsoft

# Historia

# Historia

- NT: New Technology ?
  - David Cutler Vax/VMS
    - 1988 bye DEC, hello MS
    - Se integran 20 Ingenieros de VMS al proyecto OS/2 NT.
    - MS rompe relación con IBM
  - “Similaridades” entre NT y VMS
    - Trato entre MS y DEC

# Historia

- En agosto de 1988 Bill Gates contrató a Cutler
  - Contratación de 20 empleados de Digital para trabajar con el.
- OS/2 NT
  - Microsoft rompe relaciones con IBM y el éxito de Windows 3.0 => **Windows NT**

# Historia

- Cambio su API oficial (16 bits) a una API de 32 bits.
  - Compatibilidad con Windows 3.X, DOS, OS/2 y POSIX
- En 1993 lanzamiento público de Windows NT
- Exceso de similaridades entre VMS y WNT

# El Trato

- A cambio de no demandar, DEC recibió:
  - Entrenamiento especializado para sus ingenieros.
  - Mercadotecnia para presenter a NT y VMS como 2 tiers en arquitectura c/s de 3.
  - Soporte de NT para Alfa.
  - Entre 65 y 100 Millones de Dls.
  - DEC ya es Compaq...
    - y ahora HP

# NT y UNIX

- Sabías que:
  - En 1980's los *NIX mas importantes:
    - UNIX system III (Bell)
    - UNIX BSD (UC Berkeley)
    - XENIX (MS)
    - XENIX se vendió a SCO en 1995.

# Arquitectura Windows NT

- Objetivos iniciales:
  - 32 bits (POSIX, OS/2).
  - Networking nativo (win 3.1, 3.11, DOS)
  - Seguridad integrada al kernel.
  - Multitasking preemptive-scheduling.
  - Direccionamientos de memoria protegida, de 32 bits a la UNIX.

# Windows NT

- S.O. de 32 bits, basado en microkernel, multitasking preemtive scheduling
- Modos de ejecución privilegiado y no privilegiado
- Compatible con S.O. DOS, Windows 3.1, OS/2 y POSIX

# SO de 32 bits

- La memoria es direccionada utilizando direcciones de 32 bits lo que resulta en un espacio máximo de direcciones físicas de 4Gb (2 a 3Gb para programas de aplicación)

# Basado en microkernel

- El programa que sirve como core central se diseña para ser lo mas pequeño y eficiente posible.
- Sólo las funciones fundamentales e importantes se llevan a cabo por este kernel.

# NT: Microkernel modificado

- Punto medio entre sistema microkernel y monolítico
- Los ambientes (personalidades) del SO se ejecutan en modo usuario
  - DOS, Win16, Win32, OS/2 y Posix
- Los subsistemas básicos se ejecutan en modo kernel
  - Process Manager, Virtual Memory Manager

# Multitasking preemptive

- Multitasking preemptive. El scheduler del SO es responsable de decidir que proceso correrá en un periodo de tiempo y cuando un proceso debe detenerse para dejar que otro corra.
- Multitasking cooperative. Un proceso en ejecución tiene el control completo del sistema hasta que voluntariamente lo deja.

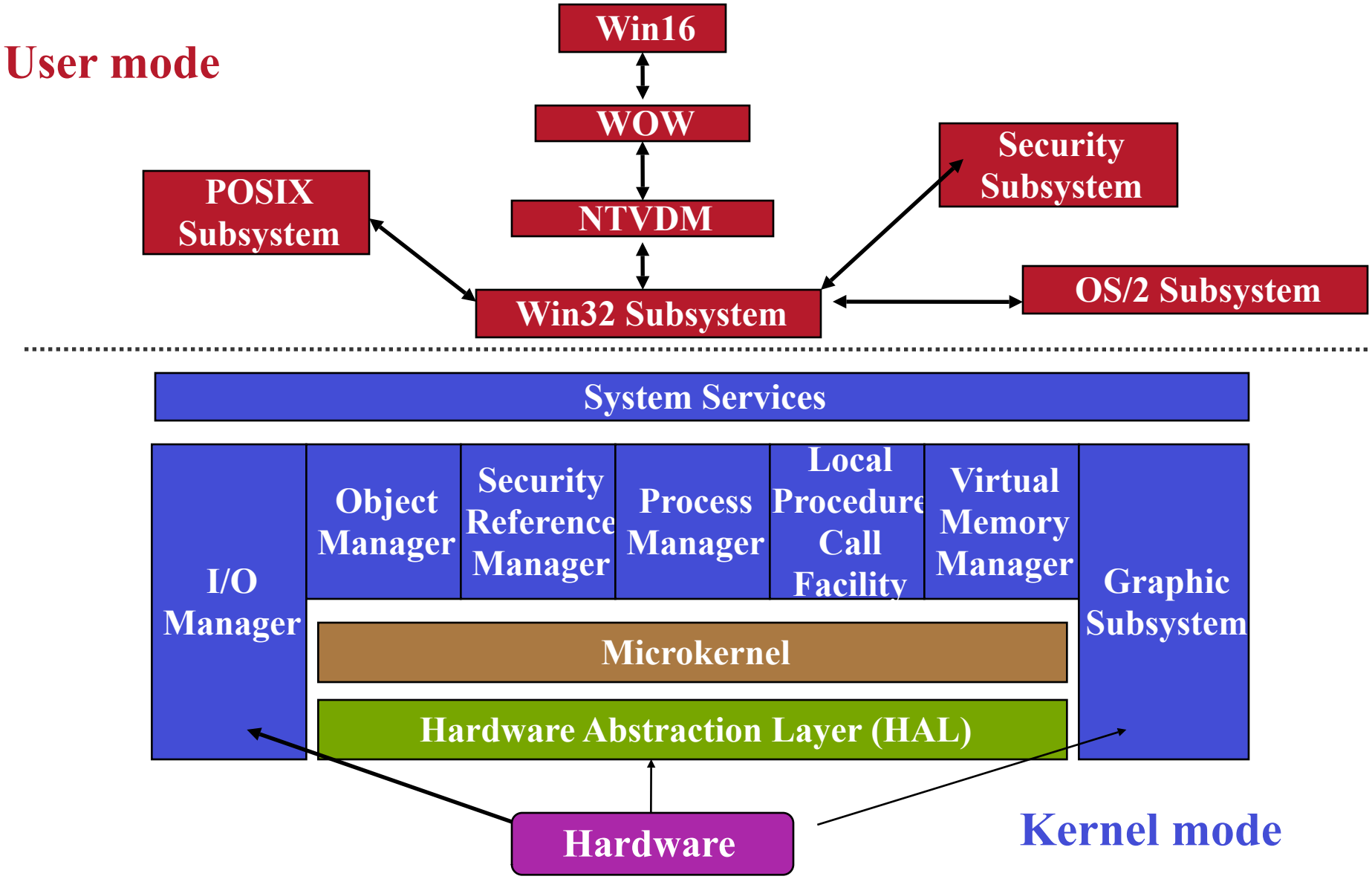
# Modos de ejecución

- Modo usuario.
  - Modo no privilegiado
  - Acceso a los recursos del sistema haciendo peticiones al SO.
  - No tiene acceso a hardware
  - No tiene acceso a memoria protegida directamente

# Modos de ejecución

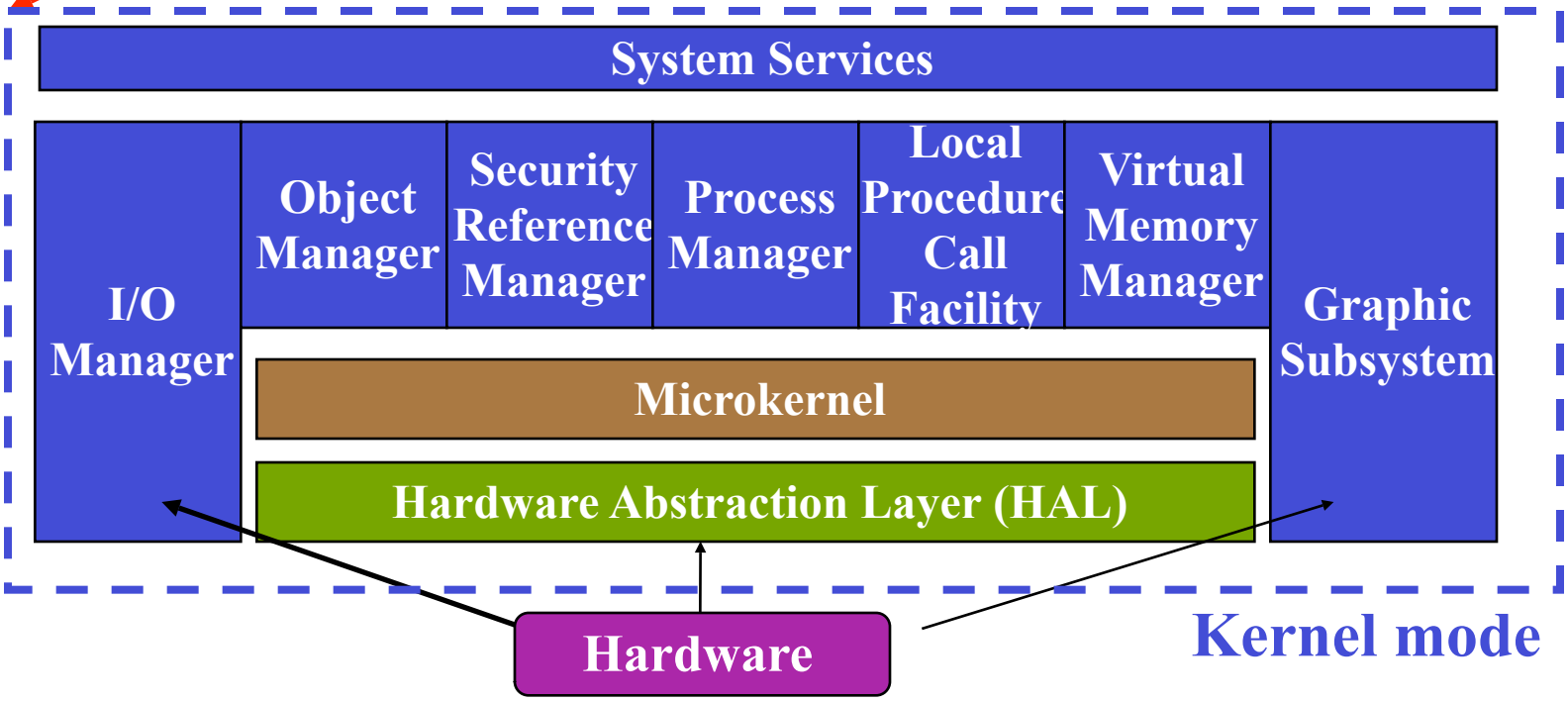
- Modo kernel.
  - Modo privilegiado
  - Acceso completo a todos los recursos del sistema
  - Acceso a toda la memoria

# Arquitectura de Windows NT



# Arquitectura de Windows NT: the executive

**Corazón del sistema operativo Windows NT**
**"Excecutive Services", "NT Excecutive"**
**Kernel del Sistema operativo**

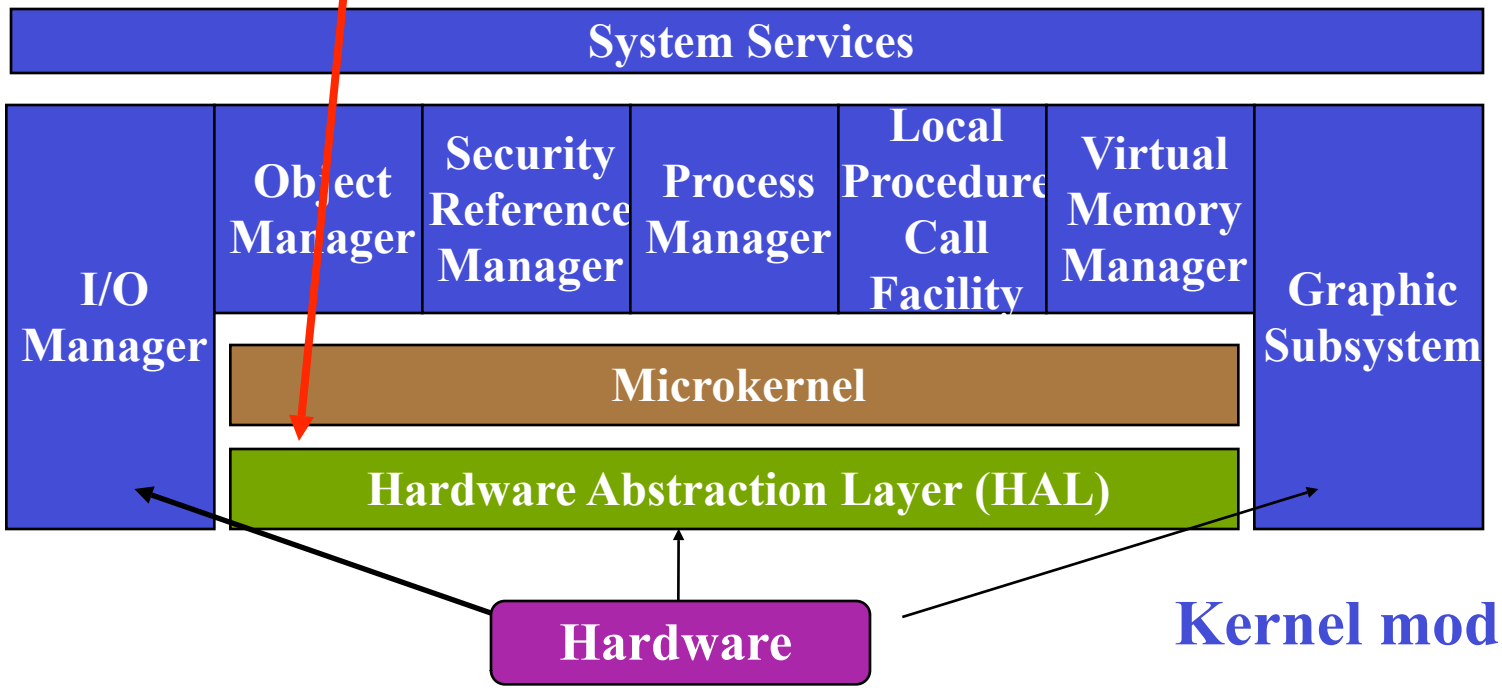


# The Executive

- Los subsistemas ejecutivos se encargan de las tareas clásicas del SO.
- Todos los subsistemas forman parte de un mismo proceso: el executive.
- Ntoskrnl.exe contiene todo.
- Bueno casi… win32k.sys

# Arquitectura de Windows NT: HAL

**Se llevan a cabo la mayoría de las interacciones con el hardware de la computadora**

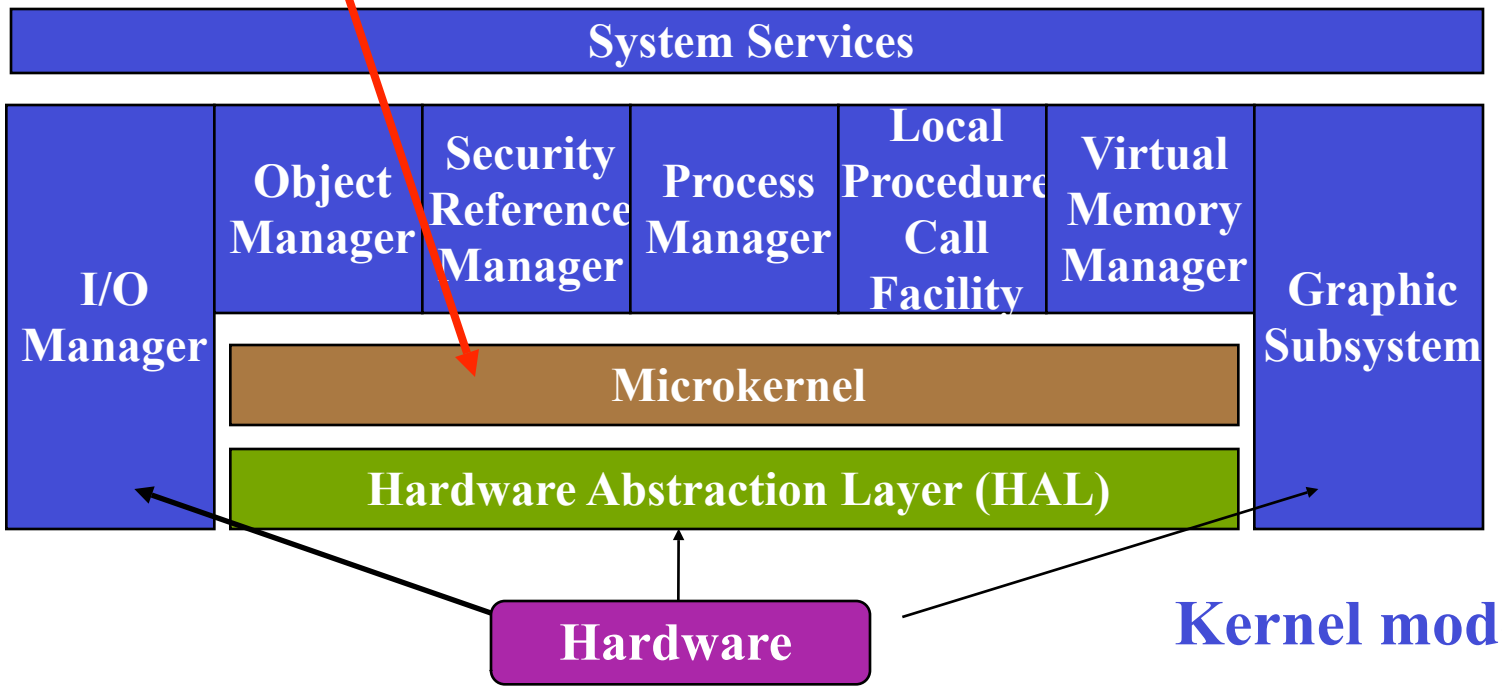


# El HAL

- Interfaz de NT con el procesador (en crudo).
- Uni, Multi, y debug (para desarrolladores).
- Esconde detalles entre procesadores, motherboards y otros.
- Abstrae el HW para que trabaje con NT.

# Arquitectura de Windows NT: micronúcleo

**Corazón del kernel. Supervisa el trabajo de todos los otros módulos y maneja las comunicaciones entre ellos y el HAL**

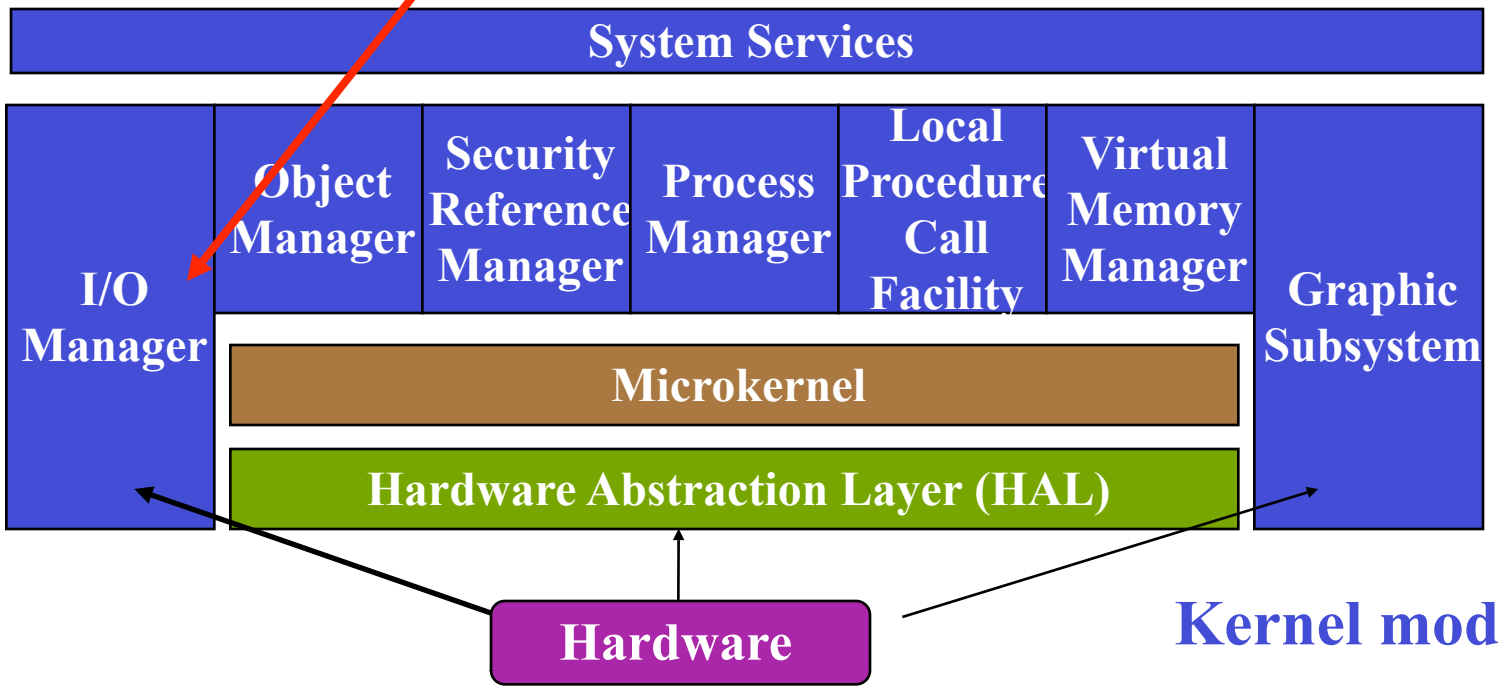


# El micro núcleo

- Servicios:
  - Scheduler
  - Administra que el Executive haga uso del HW.
  - Software Interrupt Handlers.
  - Exporta primitivas de sincronización.
- Usa:
  - HAL.
- NT es portable entre procesadores.
  - El código especifico se encuentra en el Kernel y HAL.

# Arquitectura de Windows NT: I/O Manager

**Controla la mayoría de entradas y salidas en el Sistema**

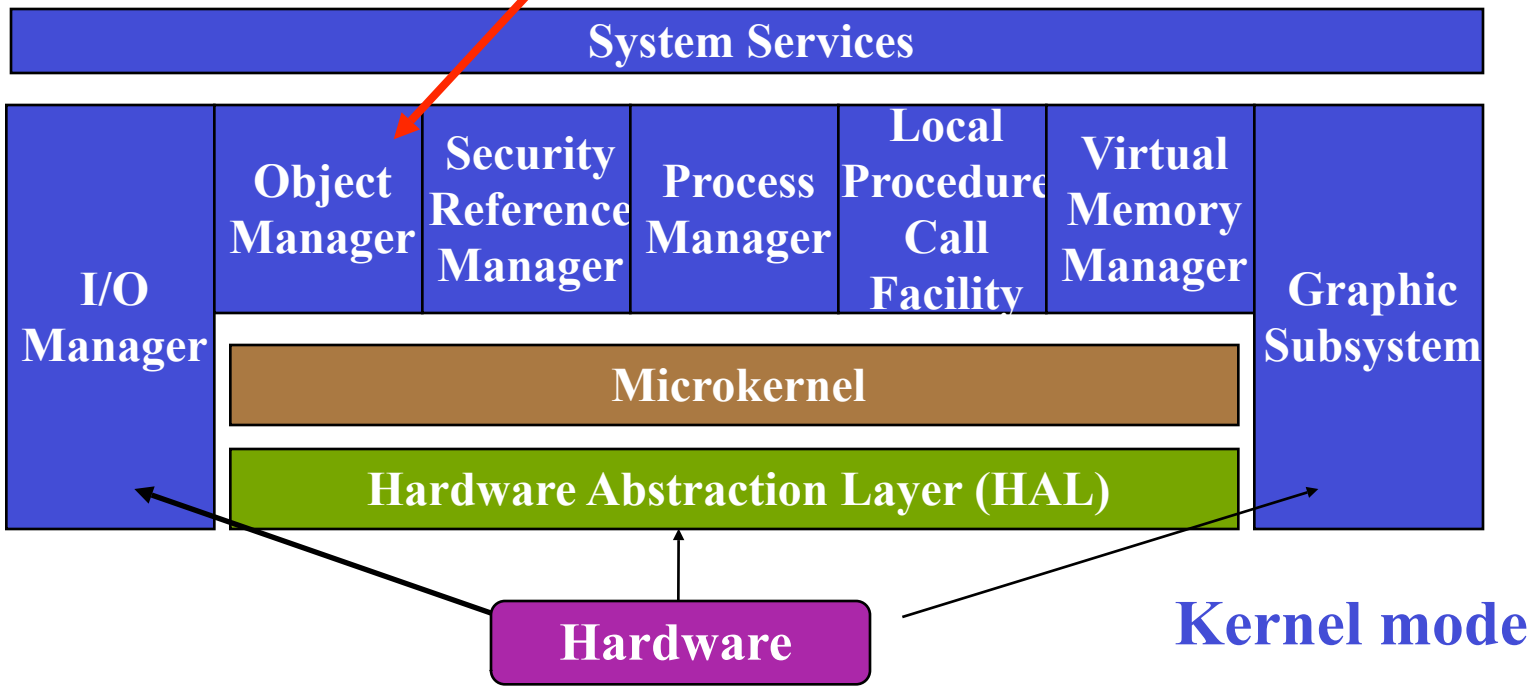


# I/O Manager

- Integración de dispositivos (drivers) con el resto de NT.
- I/O Basado en paquetes y asíncrono.
- 64 bit offsets para operaciones de archivos I/O
  - procesos limitados a un espacio de 2G
- Drivers en capas
    - NTFS
    - Fault Tolerant Disk
    - HD Driver

# Arquitectura de Windows NT: Object Manager

**Crear, modificar y eliminar objetos usados por todos los sistemas que conforman el "execuive" de Windows. Proporciona información sobre el estado de los objetos a todo el Sistema Operativo.**

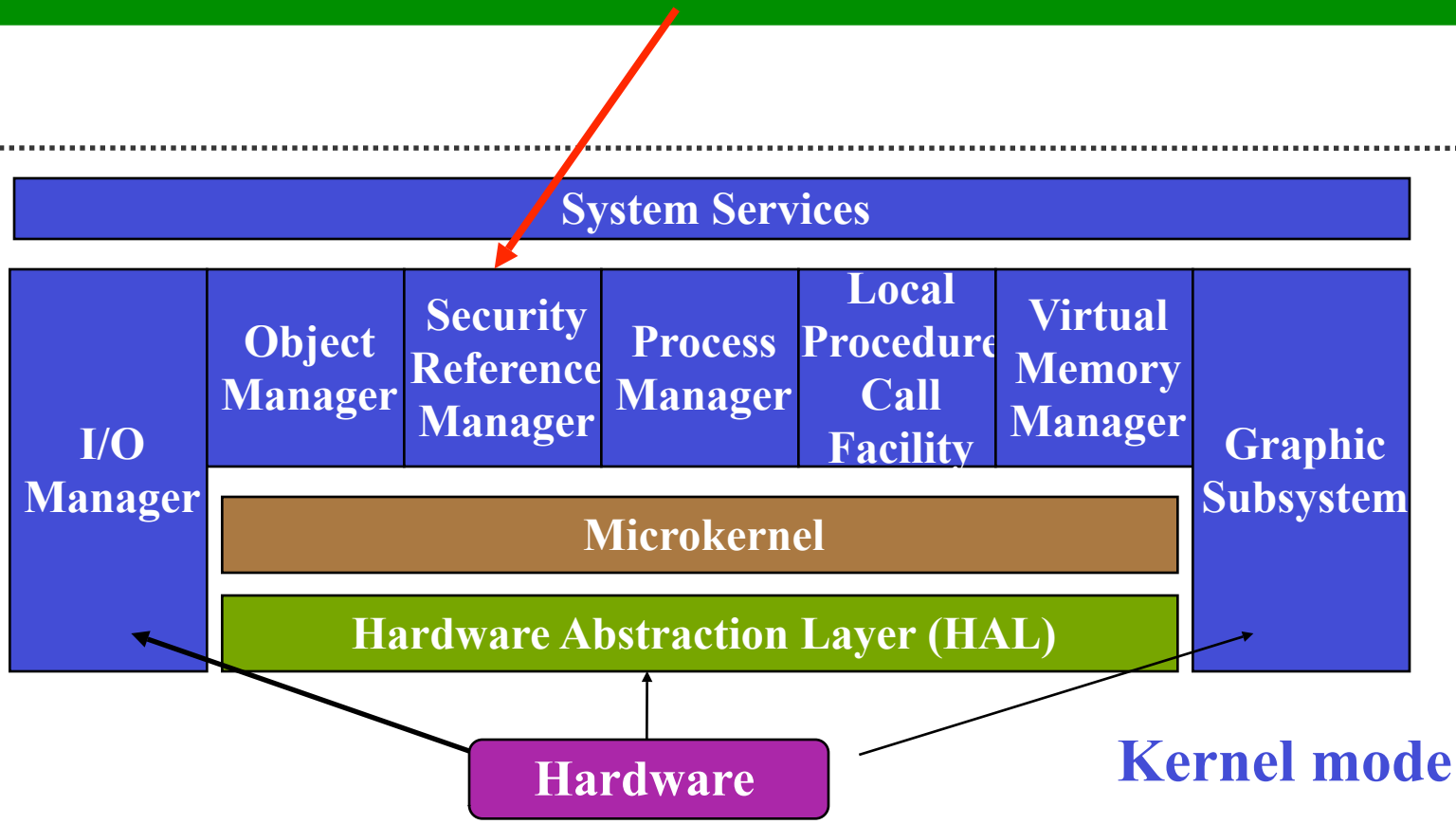


# Object Manager

- Administración y seguimiento de recursos del SO (objetos).
  - Identificación.
  - Número de referencias.
  - Regresa los infames handles.
- Casi todo el API nativo invoca recursos, por lo tanto requiere de los servicios del Object Manager.

# Arquitectura de Windows NT

**Es el lecho de toda la seguridad dentro del sistema WINDOWS y es el responsable de hacer cumplir todas las políticas de seguridad en la computadora local.**

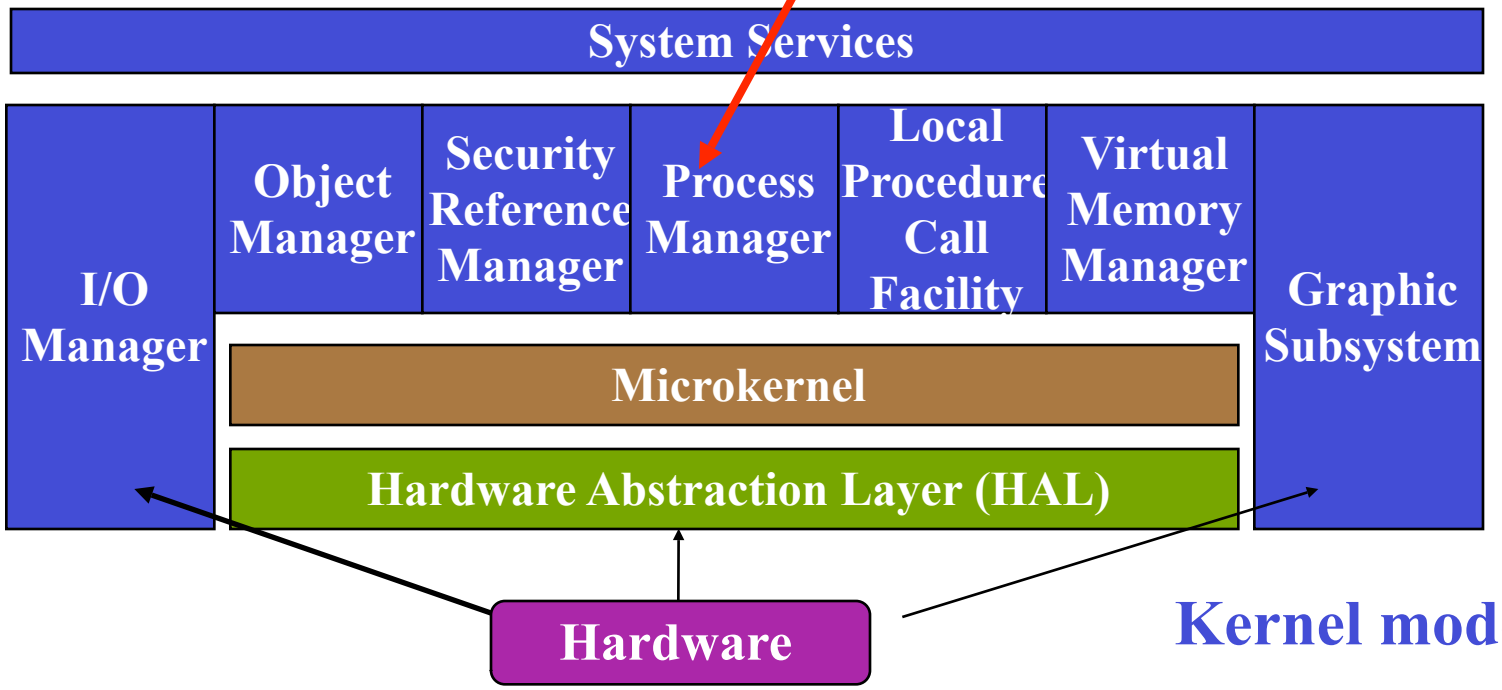


# Security Reference Monitor

- Socio del Object Manager.
- Permite o niega accesos a recursos.
- Basado en SID's y DACL's.
- Se permite impersonar.
- Implementa SACL's.
- Muchos elementos de auditoría.

# Arquitectura de Windows NT

**Crea y maneja procesos de sistema sin embargo la planificación de procesos se lleva a cabo por el microkernel**

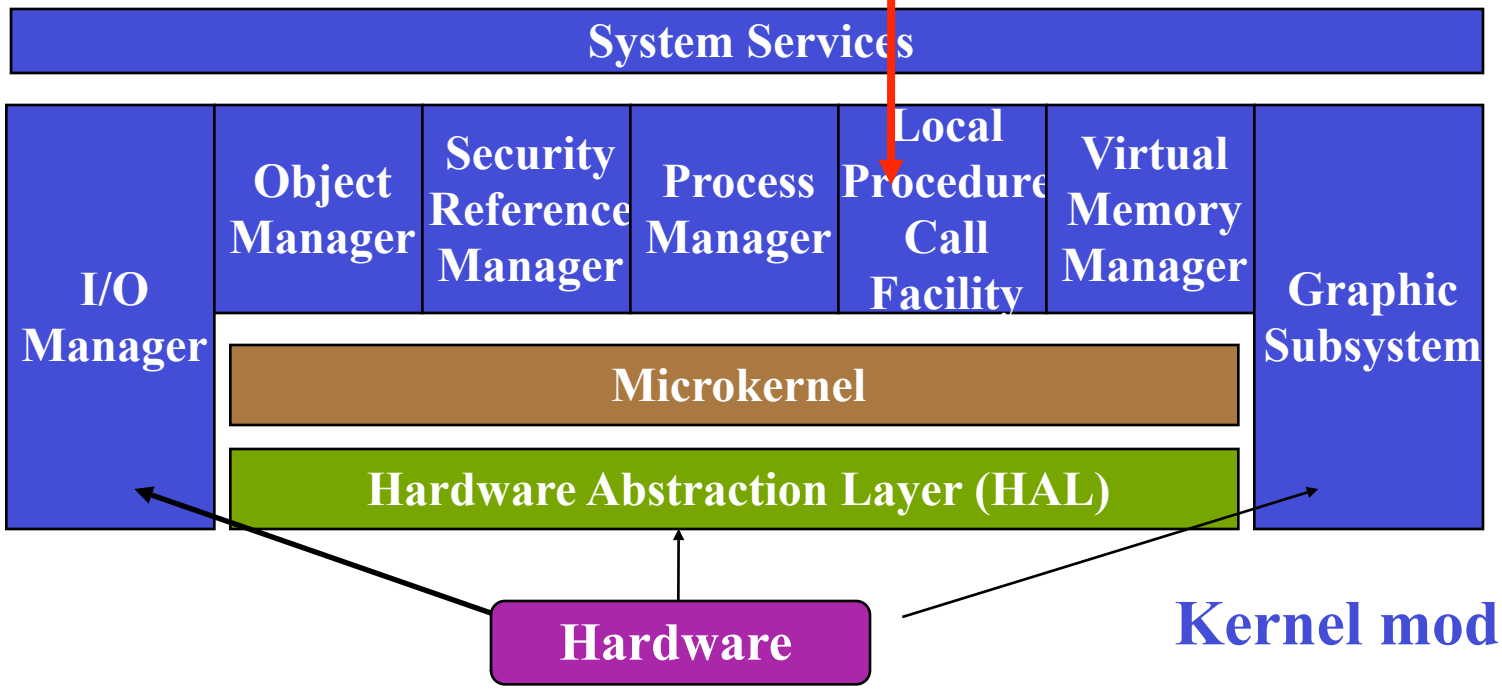


# Process Manager

- Exporta la Interfaz de procesos hacia otros subsistemas y aplicaciones en modo usuario.
- Crea, elimina, modifica prioridades, etc.

# Arquitectura de Windows NT

**Responsable de la comunicación entre distintos procesos (Interprocess communication)**

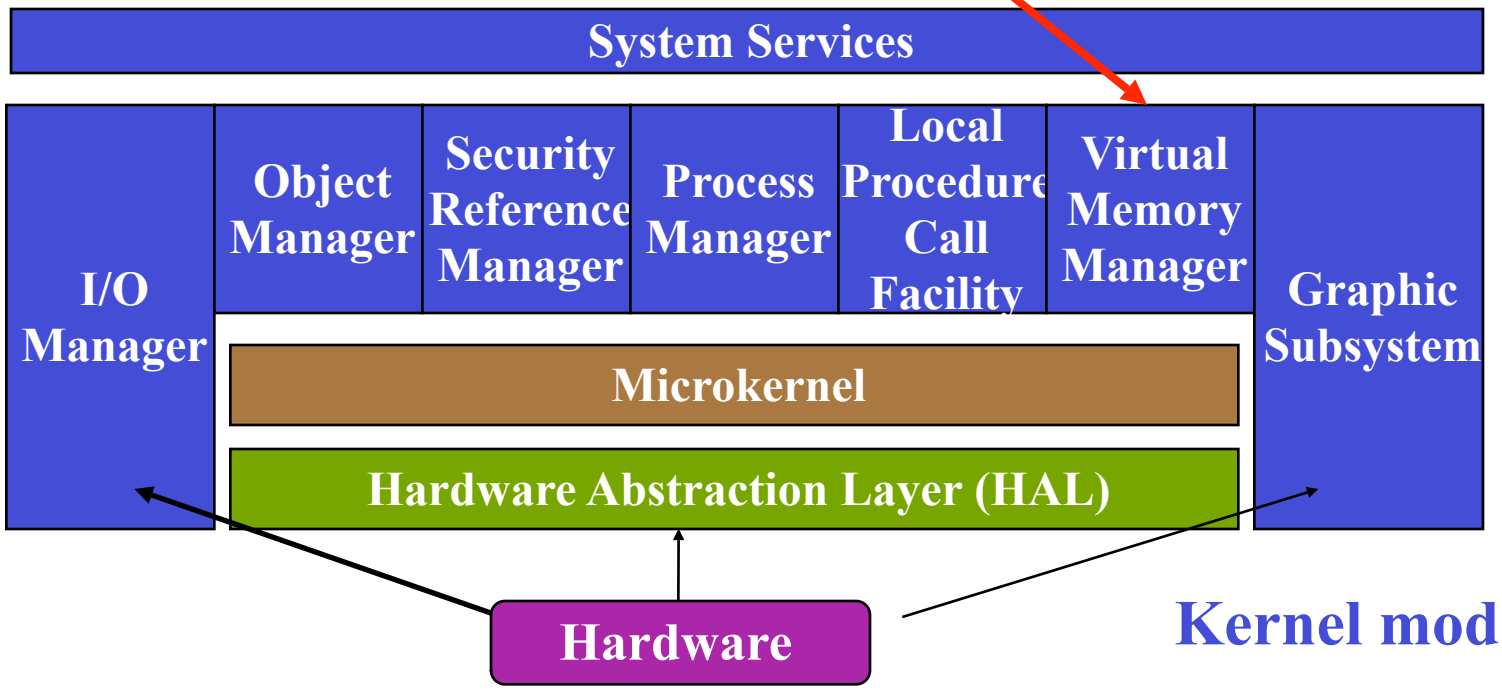


# LPC Facility

- Optimiza la comunicación entre aplicaciones y personalidades.
- Connection Port/Comm. Port
- IPC a través de memoria compartida.

# Arquitectura de Windows NT

**Maneja la asignación y uso de la memoria del sistema**

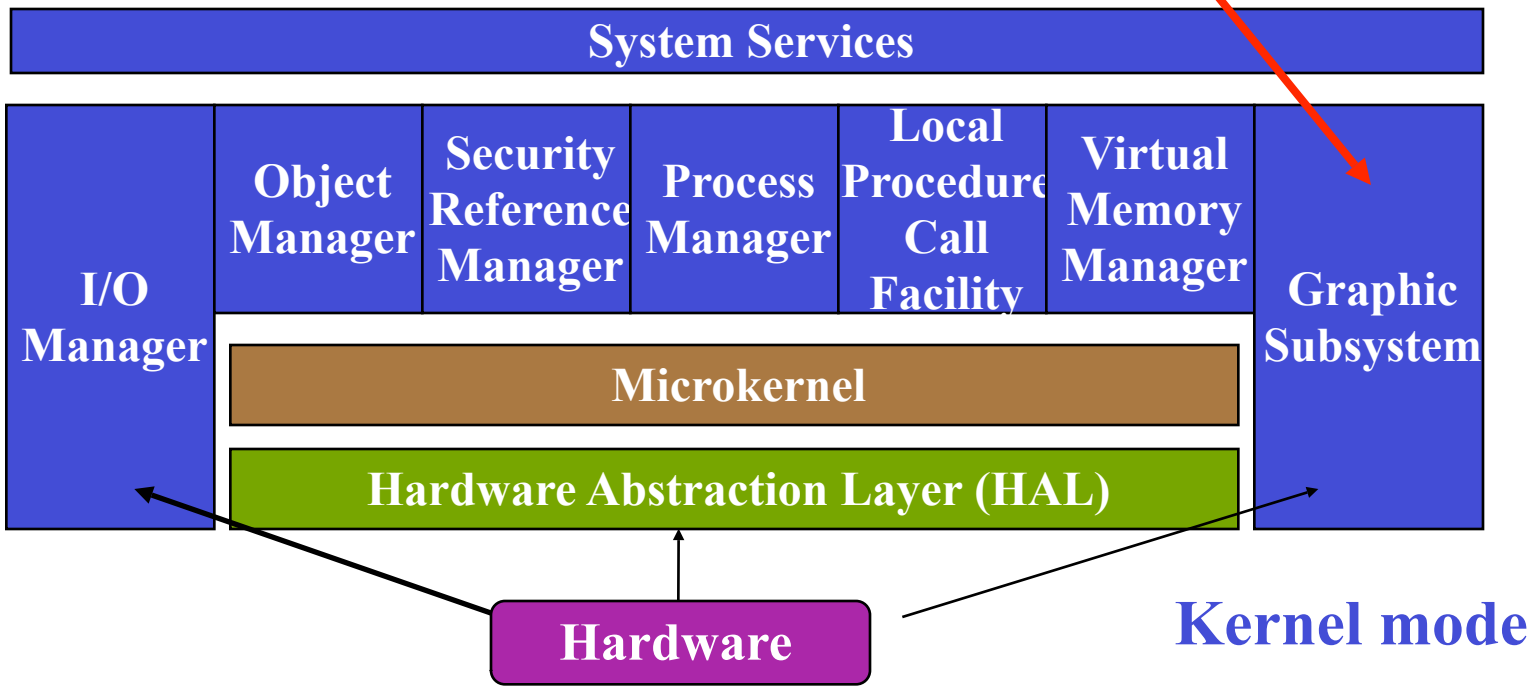


# Virtual Memory Manager

- Crea y administra mapas de direcciones para procesos.
- Controla la asignación física de la memoria.
- Implementa paginación por demanda.
- File memory mapping, memory sharing, copy-on-write protection.

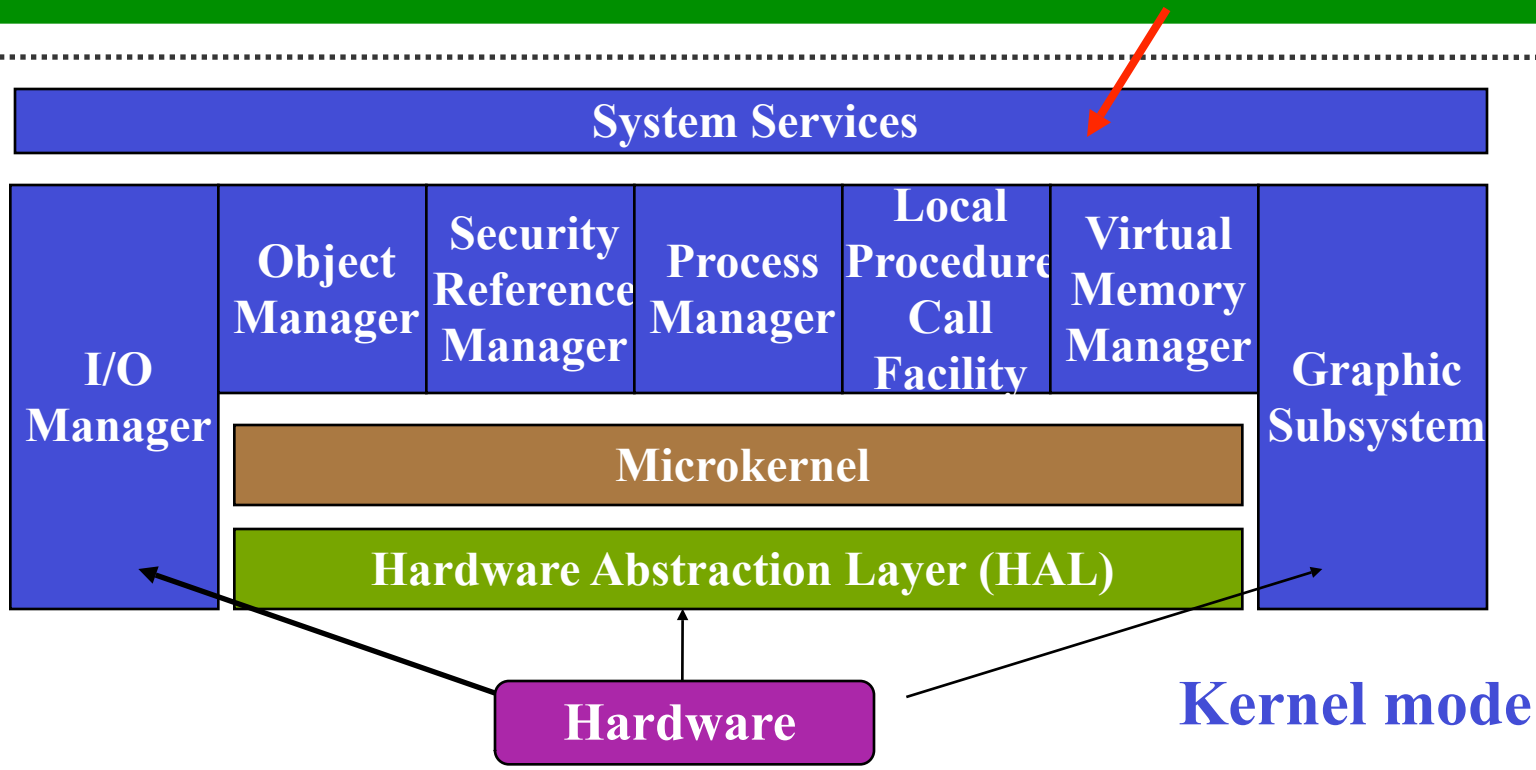
# Arquitectura de Windows NT

**Provee los servicios requeridos para poder llevar a cabo la interfaz con despliegues gráficos. Este componente se convirtió en parte del kernel con la versión 4 antes era parte del subsistema Win32**



# Arquitectura de Windows NT

**Todos los componentes mencionados proveen Servicios de sistema, es decir, operaciones a nivel sistema y funciones disponibles para procesos ordinarios para llevar a cabo tareas comunes.**

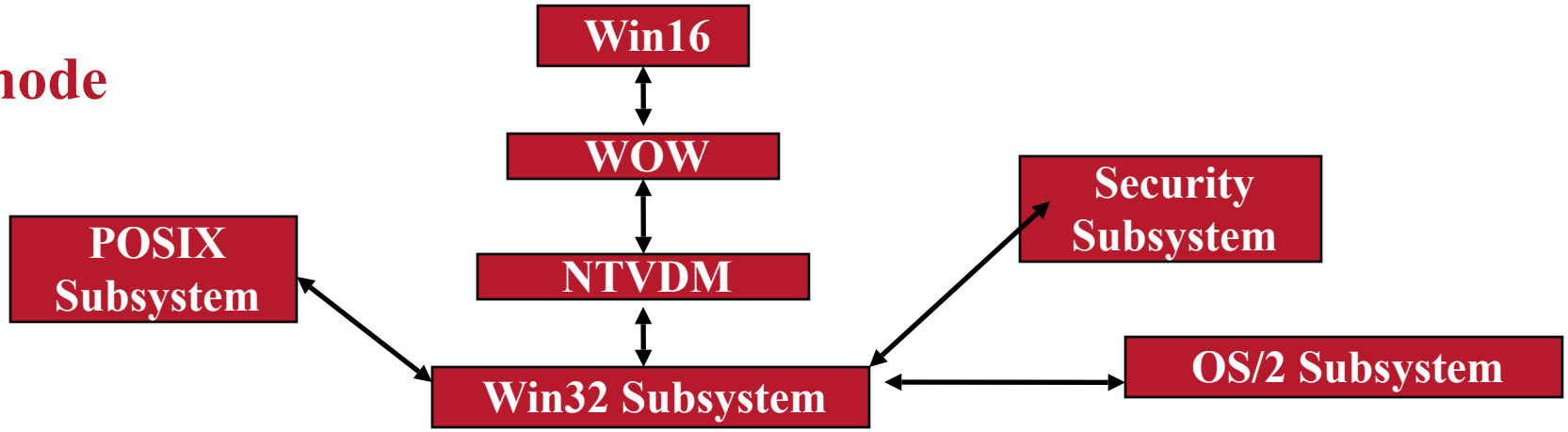


# System Services

- Exportan el API Nativo fuera del modo kernel.
- Una aplicación puede hacer uso del API nativo sin pasar por la “personalidad” del SO.
- El hacer el bypass de la personalidad, no logra elevar privilegios.

# Arquitectura de Windows NT: personalidades

**User mode**




**Todos los componentes de esta parte se ejecutan en modo usuario, estos pueden acceder a recursos del sistema y a la memoria sólo por medio de un conjunto limitado de interfaces no privilegiadas que son proveídas como servicios del sistema**

# Personalidades (1)

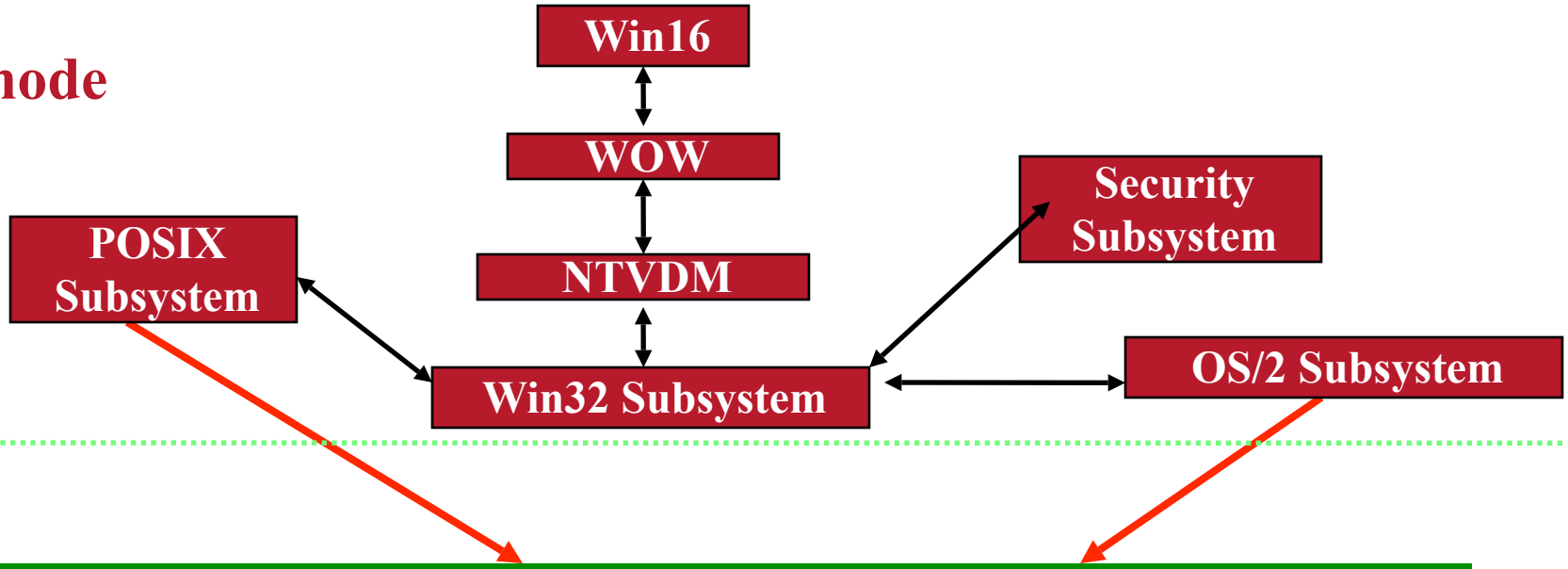
- Se implementan como C/S
  - Linking estático hacia DLL's cliente, que se encargan de exportar el API.
  - Ej:
    - Una aplicación win32 es un cliente del servidor de la personalidad de win32, por lo que se liga con las DLL's cliente que incluyen entre otras a:
      - » kernel32.dll
      - » gdi32.dll
      - » user32.dll

# Personalidades (2)

- Provee procesos con la API estandar.
- Todos los programas de aplicación interactuan con este componente del S.O.
- Los programas nativos Windows NT Win32 se comunican directamente con el Subsistema Win32

# Arquitectura de Windows NT

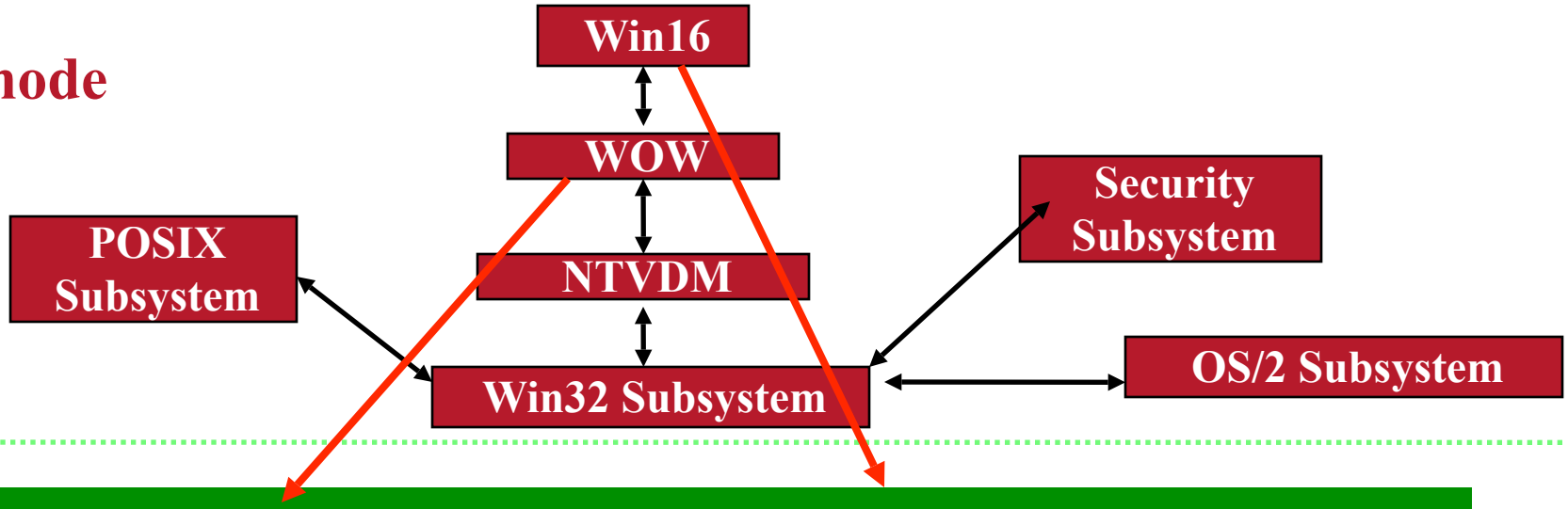
**User mode**




**La compatibilidad con programas diseñados para otros ambientes se lleva a cabo por medio de una serie de subsistemas API secundarios.**

# Arquitectura de Windows NT

User mode




**Aplicaciones DOS y Win16 son manejadas por una serie de subsistemas.**
**El NTVDM (NT Virtual DOS Machine) provee ambiente compatible con DOS para programas DOS.**
**Las aplicaciones Windows de 16 bits estas llamadas se convierten a llamadas Windows de 32 bits en un subsistema llamado Windows on Win32 (WOW) estas aplicaiones también requieren el NTVDM**

# El Registro de NT

configurando el sistema

# El Registro de NT

- En NT la información de configuración del sistema y de las aplicaciones se guarda en el registro.
- El registro de NT es una base de datos jerárquica, organizada en forma de árbol.
  - cada llave contiene subllaves o un valor
- El registro se divide en cinco llaves principales
- Para acceder al registro existen programas
  - regedit.exe y regedt32.exe

# Principales claves (hives)

- HKEY_LOCAL_MACHINE
  - esta clave almacena toda la configuración del sistema
  - es independiente de quien se encuentre en el sistema
- HKEY_USERS
  - información de la base de datos de usuarios y grupos.
- HKEY_CURRENT_USER
  - contiene una copia de la clave que representa al usuario que ha iniciado sesión interactiva
  - si un usuario diferente se conecta en la misma máquina, la información en este hive cambiara de acuerdo al usuario que se encuentra en la computadora

# Principales claves (hives)

- HKEY_CLASSES_ROOT
  - núcleo de la interfaz del usuario
  - todos los tipos de archivos que las aplicaciones son capaces de manejar
  - shortcut
- HKEY_CURRENT_CONFIG
  - configuración actual de algunos servicios y dispositivos
  - información acerca de la configuración actual del hardware

# Ubicaciones hives

| | |
|---|---|
| HKEY_CLASSES_ROOT | Realmente es un enlace a esta otra clave: HKEY_LOCAL_MACHINE\SOFTWARE\Classes. |
| HKEY_CURRENT_USER | Realmente es un enlace a la subclave del usuario en curso dentro de la clave: HKEY_USERS. |
| HKEY_LOCAL_MACHINE\SYSTEM | X:\Windows\System32\Config\System |
| HKEY_LOCAL_MACHINE\SAM | X:\Windows\System32\Config\Sam |
| HKEY_LOCAL_MACHINE\SECURITY | X:\Windows\System32\Config\Security |
| HKEY_LOCAL_MACHINE\SOFTWARE | X:\Windows\System32\Config\Software |
| HKEY_LOCAL_MACHINE\HARDWARE | No se almacena en disco, se crea y elimina de la memoria en cada inicio de Windows. |
| HKEY_USERS\ | X:\Documents and Settings\Usuario\Ntuser.dat |
| HKEY_USERS_Classes | X:\Documents and Settings\Usuario\Configuración local\Application Data\Microsoft\Windows\Usrclass.dat |
| HKEY_USERS\.DEFAULT | X:\Windows\System32\Config\Default |

# Principales tipos valores llaves

- Palabra (REG_DWORD)
  - almacena un dato numérico, con 4 bytes
- Binario (REG_BINARY).
  - almacena un grupo de datos binario.
- Cadena (REG_SZ)
  - almacena una cadena de caracteres.
- Cadena expandida (REG_EXPAND_SZ)
  - almacena una cadena de caracteres de tamaño variable.
- Cadena múltiple (REG_MULTI_SZ)
  - almacena un conjunto de cadenas de caracteres.

# Almacenamiento de las claves

- Las claves principales suelen estar representadas por archivos.
- Las principales son:
  - SAM:  contiene la base de datos del dominio o del ordenador, dependiendo de si es un NT configurado como controlador de dominio, servidor o estación de trabajo.
  - Software: contiene la sublcave software de la clave HKEY_LOCAL_MACHINE
  - Security: contiene la subclave security de la clave HKEY_LOCAL_MACHINE
  - System: contienen HKEY_LOCAL_MACHINE, salvo las subclaves que se guardan en su propio archivo.

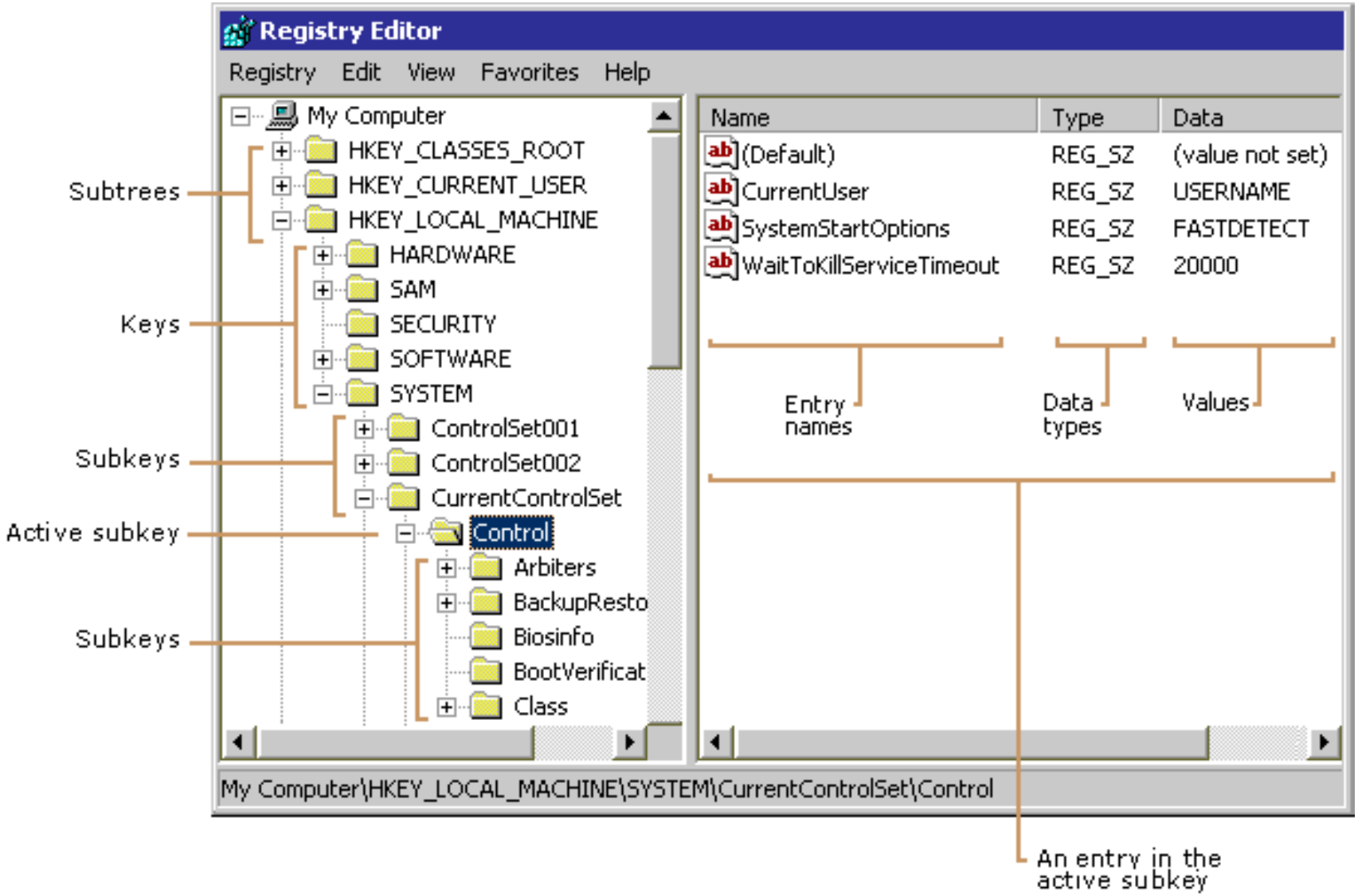
# Claves y archivos relacionados

| Clave | Nombre del archivo |
|---|---|
| HKEY_LOCAL_MACHINE\SAM | Sam, Sam.log, Sam.sav |
| HKEY_LOCAL_MACHINE\Security | Security, Security.log, Security.sav |
| HKEY_LOCAL_MACHINE\Software | Software, Software.log, Software.sav |
| HKEY_LOCAL_MACHINE\System | System, System.log, System.sav |
| HKEY_CURRENT_CONFIG | System, System.log, System.sav |

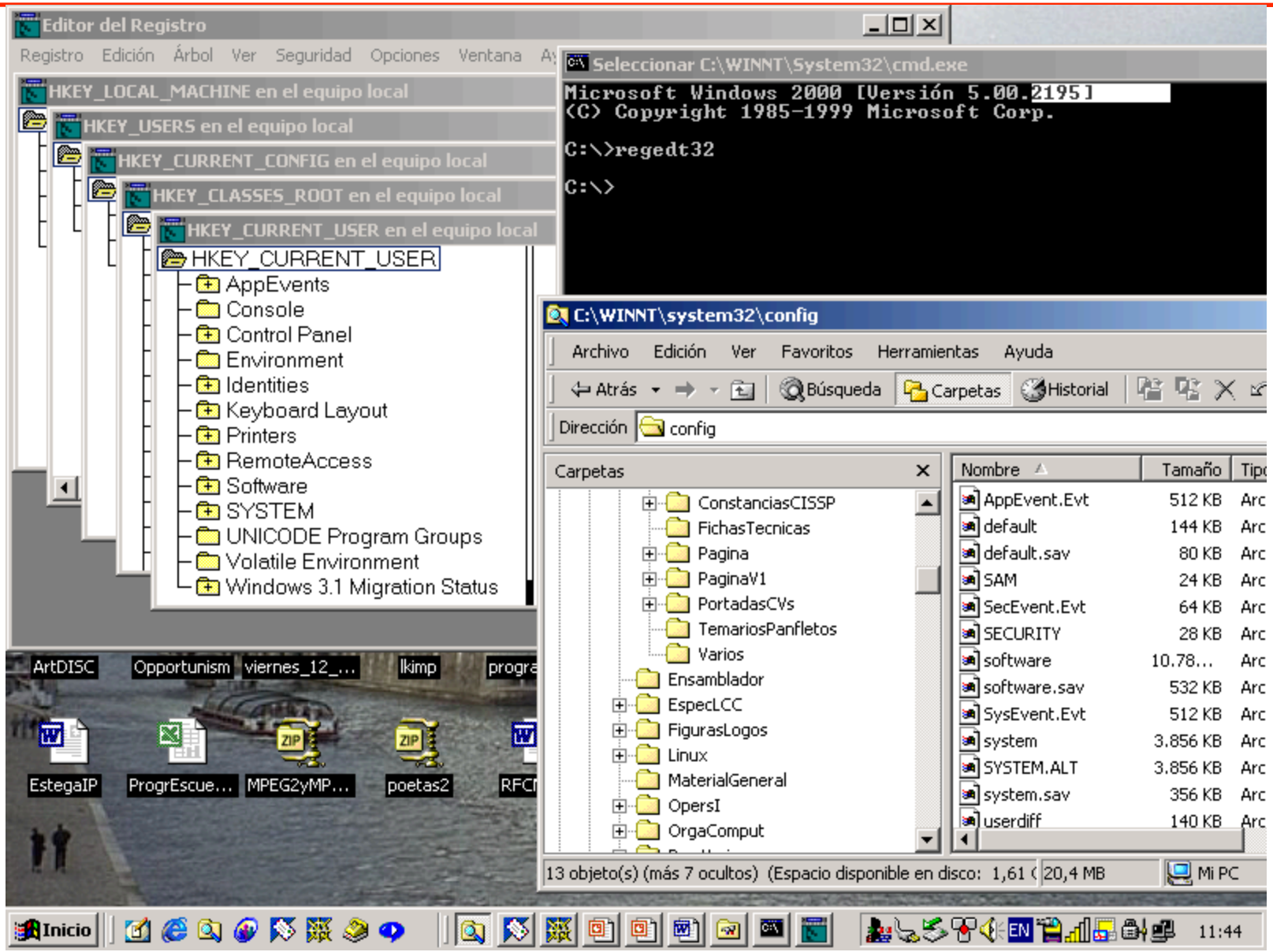
# Claves y archivos relacionados

| **Clave** | **Nombre del archivo** |
|---|---|
| HKEY_USERS\.DEFAULT | Default, Default.log, Default.sav |
| Archivos no asociados a ninguna clave | Userdiff, Userdiff.log |
| HKEY_CURRENT_USER | Ntuser.dar, Ntuser.dat.log |

# Elementos del registro

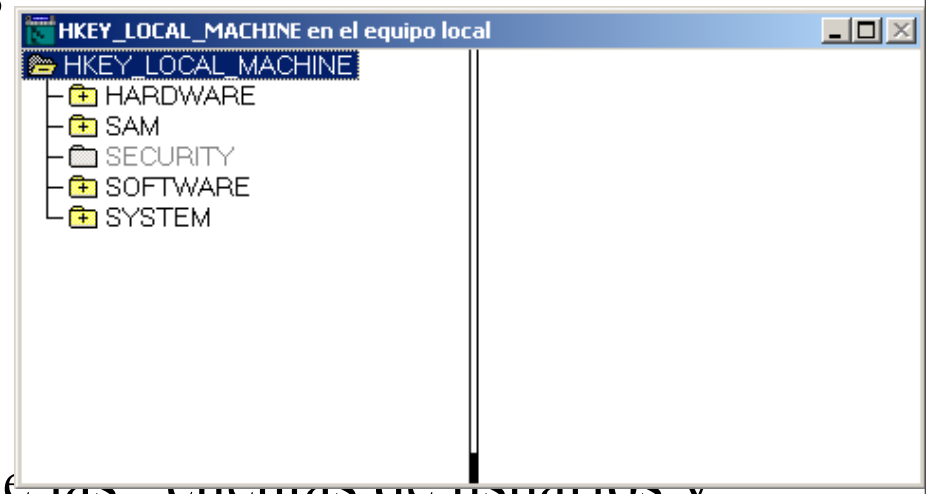


# Registros, editor y archivos



# La clave HKEY_LOCAL_MACHINE

- Contiene las subclaves que almacenan información sobre la propia máquina, es decir, el hardware que está instalado, los controladores asociados, …
- Se divide en cinco subclaves
- HARDWARE
  - configuración arranque de la máquina y el arranque del sistema
- SAM
  - contiene información acerca de las cuentas de usuarios y grupos en la base de datos SAM (Security Account Manager) de la computadora



# Subclaves
# HKEY_LOCAL_MACHINE

- SECURITY
  - incluye los derechos de los usuarios en la máquina, política de seguridad en cuento a claves de acceso e información sobre los miembros de grupos locales
- SOFTWARE
  - contiene información sobre la configuración del software instalado en la máquina
- SYSTEM
  - contiene datos sobre los controladores y los dispositivos instalados, los perfiles de hardware, el estado del registro, información acerca de los discos duros e información sobre la configuración de la PC

# HKEY_USERS

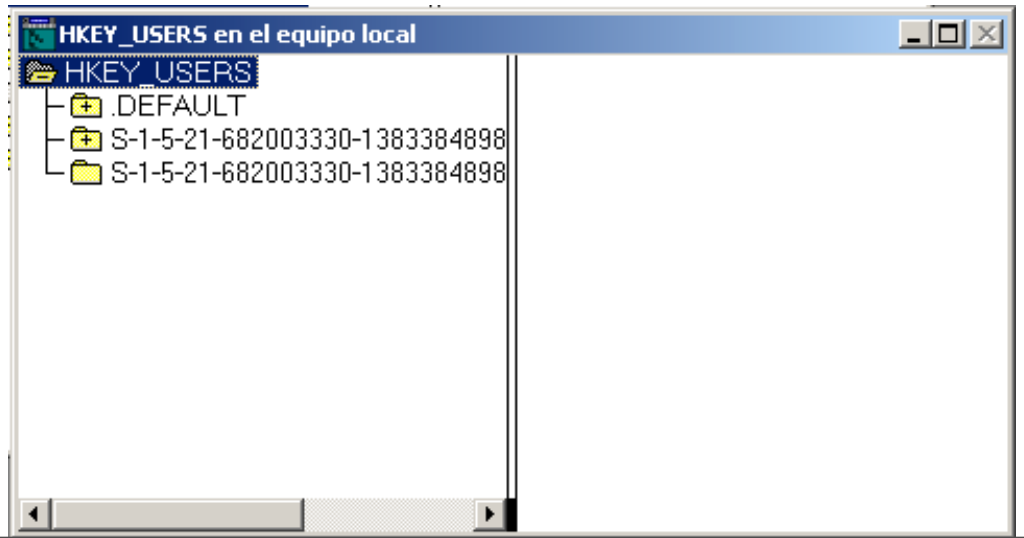
- Almacena información acerca de cada una de las cuentas locales al equipo.
- Habrá una entrada por cada uno de los usuarios definidos y una más denominada DEFAULT, que contiene la configuración predeterminada que se utiliza cuando se crea un usuario nuevo
- En cada una de las subclaves asociadas al usuario guarda también la configuración del escritorio.

# Subclaves HKEY_USERS

- AppEvents
  - almacena directorios donde estan los archivos de sonido asociados a diferentes eventos del sistema
- Console
  - define características de la consola, tamaño ventana, etc
- ControlPanel
  - guarda información de la configuración de pantalla
- Enviroment
  - almacena todas las variables de entorno definidas y sus valores
  - una vez hechas las modificaciones, no tendrán efecto hasta que se vuelva a ejecutar de nuevo la aplicación que accede a dichos valores

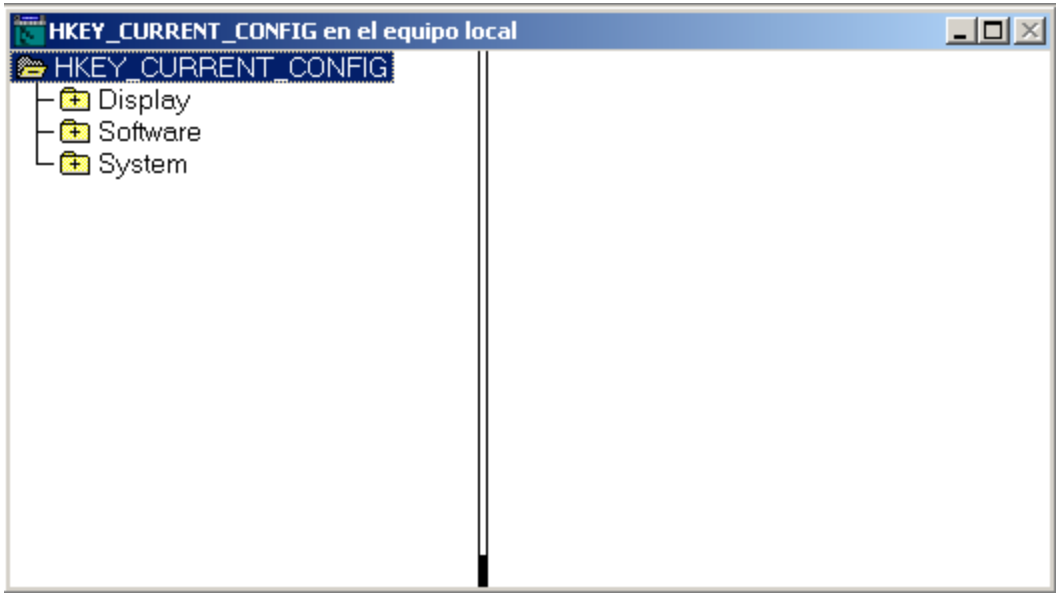
# Subclaves HKEY_USERS

- Keyboard Layout
  - incluye la información sobre el tipo de teclado que se está utilizando
  - estos valores pueden ser modificados directamente desde el Panel de Control, hay un icono dedicado a esto
- Software
  - guarda las propiedades del software instalado para un usuario concreto



# HKEY_CURRENT_CONFIG

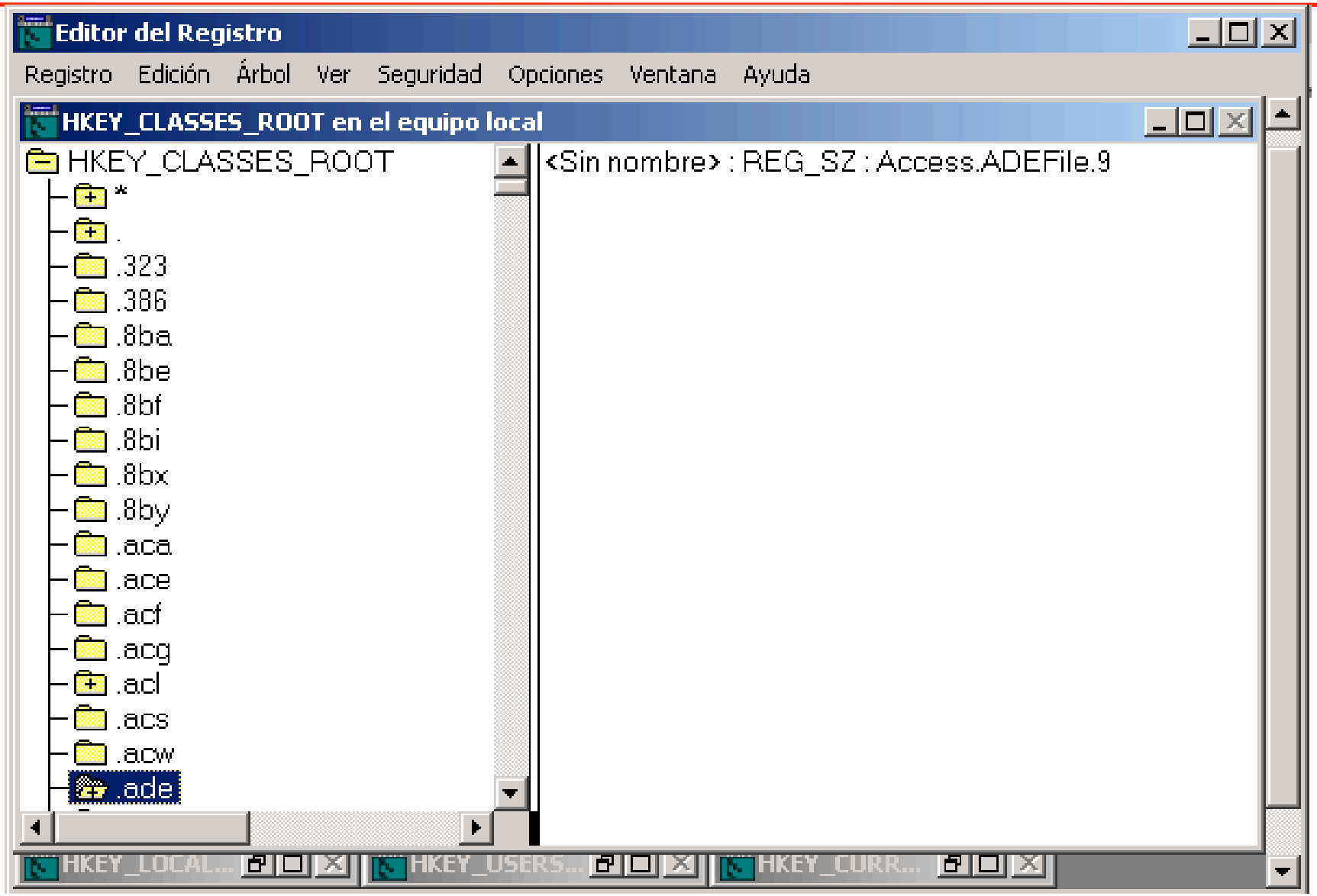
- Contiene datos que definen la configuración actual del hardware del equipo.
- Es un alias de la clave
  - HKEY_LOCAL_MACHINES\System\CurrentControlSet\Hardware\Profiles\Current



# HKEY_CLASSES_ROOT

- Contiene información asociada a los datos asociados a las extensiones de los archivos
- Se utiliza para ejecutar operaciones
  - abrir la aplicación adecuada cuando se abre un archivo desde el Explorador de Windows NT y para la vinculación e incrustación de objetos OLE
- Dichos datos deben ser modificados desde el File Manager y no desde aquí.
- También guarda información de los objetos COM

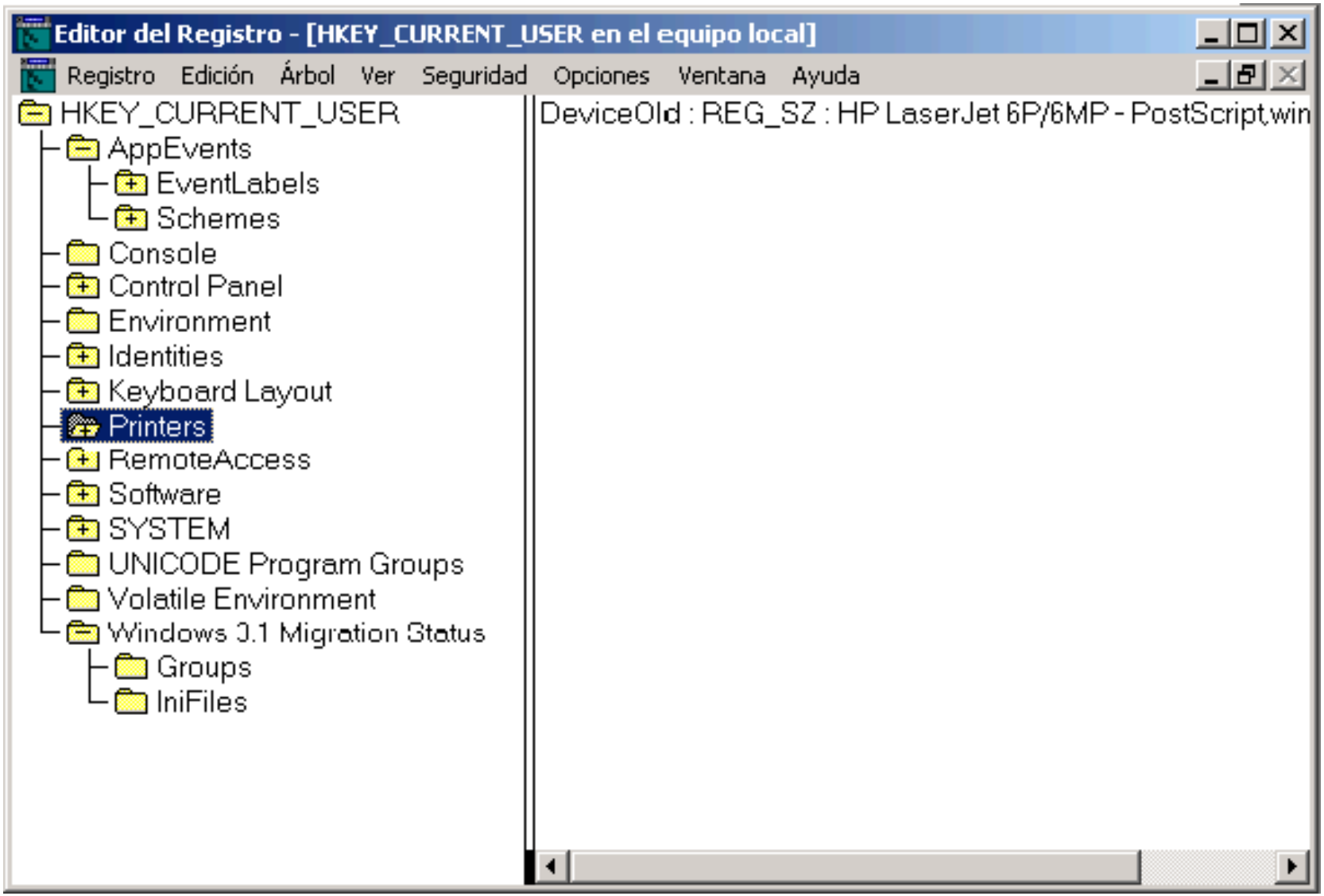
# Ejemplo HKEY_CLASSES_ROOT



# HKEY_CURRENT_USER

- Es la raíz de la información de configuración del usuario que esta conectado actualmente.
- Aquí se almacenan datos tales como las carpetas de usuario, los colores de la pantalla y la configuración del Panel de control.
- Esta información se conoce como Perfil de usuario
- Esta clave guarda una copia de los datos alamacenados en la clave HKEY_USERS para el usuario que haya iniciado la sesión.

# Ejemplo HKEY_CURRENT_USER



# Ejemplo uso: borrando historial navegación internet explorer

- Subarbol: HKEY_CURRENT_USER
- Llave: Software
- Subllave: Microsoft
- Subllave: Internet Explorer
- Subllave: Typed URLs
- ¿Para otro navegador?

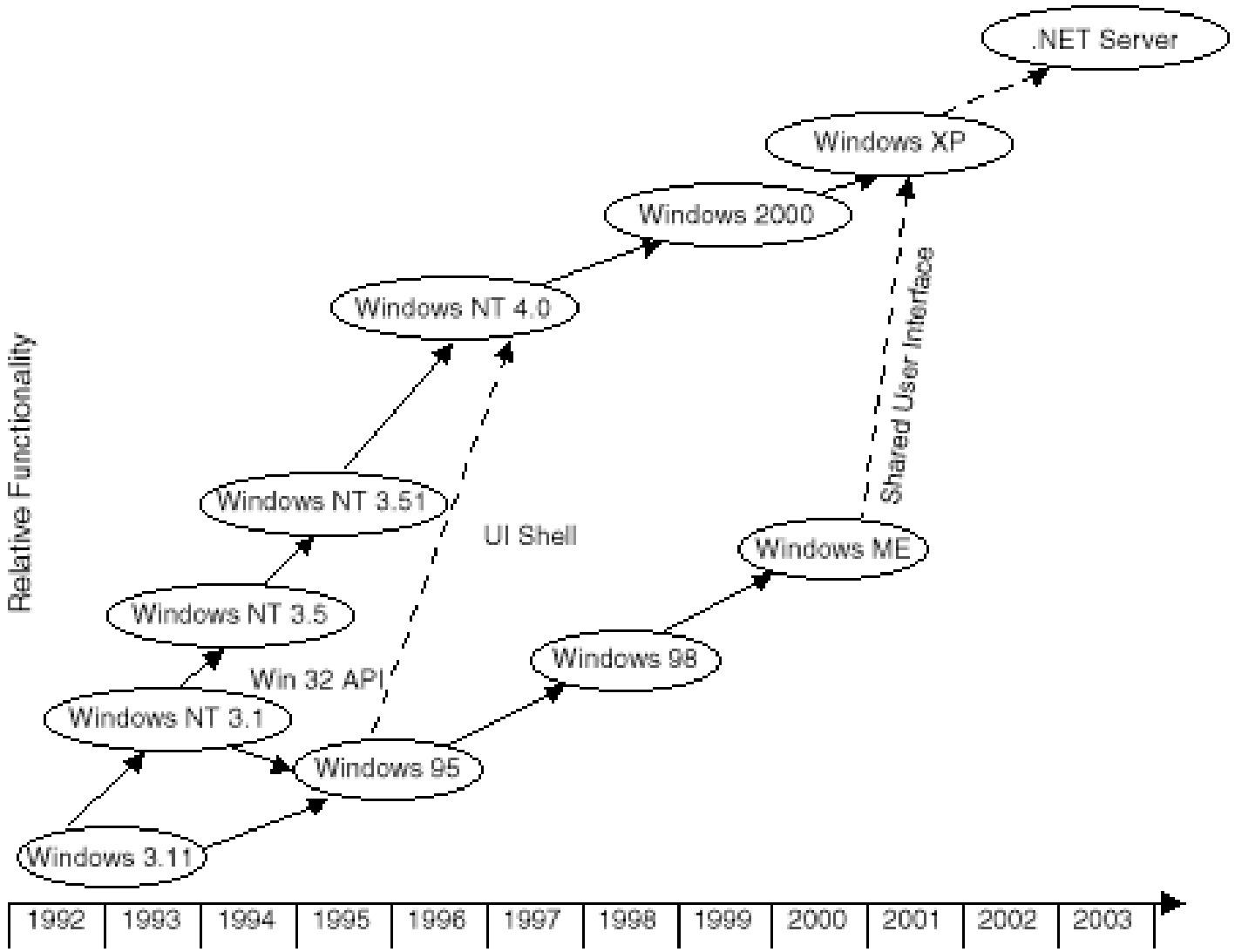
# Modificando llaves

- Seleecionar HKEY_CLASSES_ROOT
- Seleccionar Exportar archivo del Registro".
- Asignar cualquier nombre
  - asegúrarse de que termina en ".reg".
- Abrirlo con wordpad
- Modificar lo que se desee
- Importar usando la versión importar del regedit.
  - solo se puede hacer si el archivo termina en .reg

# Autenticación y control de acceso

participantes

# Recordando: evolución Windows



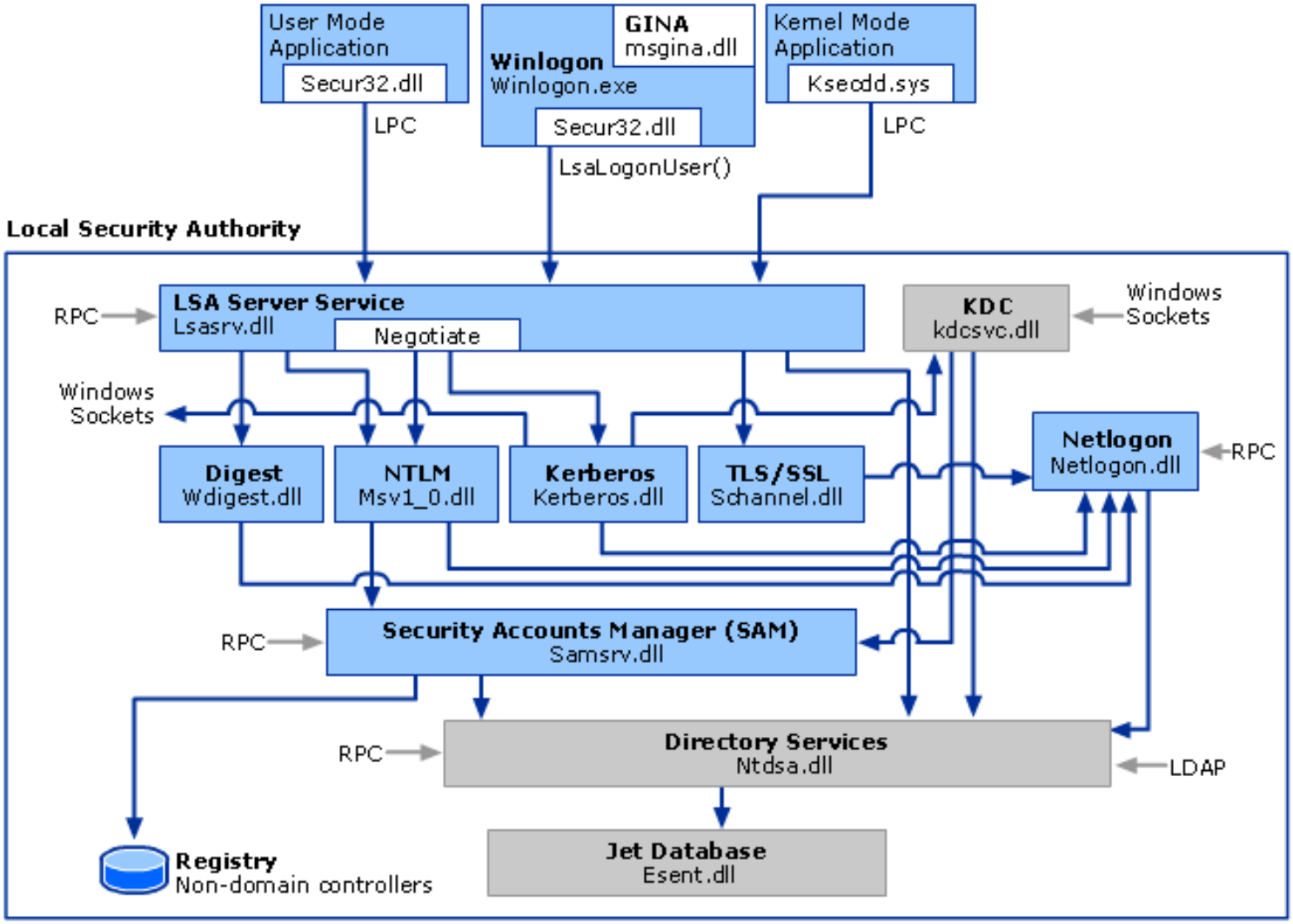
# Autenticación y control de acceso

- Todo a cargo de cuatro componentes:
  - Local Security Authority (Autoridad de seguridad local)
  - SAM: Security Account Manager (Administrador de seguridad de cuentas)
  - SRM: Security Reference Monitor (Monitor de referencia de seguridad)
  - UI: User Interface (Interfaz de usuario)

# El LSA

- Servidor de Autenticación de seguridad local
- Encargado de las directivas de seguridad
- Establece que cuentas pueden iniciar una sesión, las directivas que se han diseñado en cuanto a las contraseñas y los privilegio de acceso a los distintos recursos
- Información es recogida en la base de datos de directivas

# Arquitectura del LSA



# El SAM

- Administrador de cuentas de seguridad
- Son las subrutinas encargadas de manejar la base de datos SAM, que guarda las distintas cuentas de usuario y contraseñas definidas.

# El SRM

- Monitor de Referencia de Seguridad
- Es el único que se ejecuta en el modo núcleo y es el responsable de controlar el acceso a los objetos por parte de usuarios y aplicaciones.

# Responsabilidad controlador

- Centrada en seguridad
- Autenticacion
  - login/password
  - base datos SAM
- Control de acceso
  - Identificadores de seguridad (SID)
    - S-1-5-21-1638239387-7675610646-9254035128-545
  - Listas de control de acceso (ACL)
    - constituidas por una o más entradas de control de acceso (ACE - Access Control Entries), cada una de las cuales contienen un SID y derechos de acceso asociados a este.

# El SID

S-1-5-21-1638239387-7675610646-9254035128-545

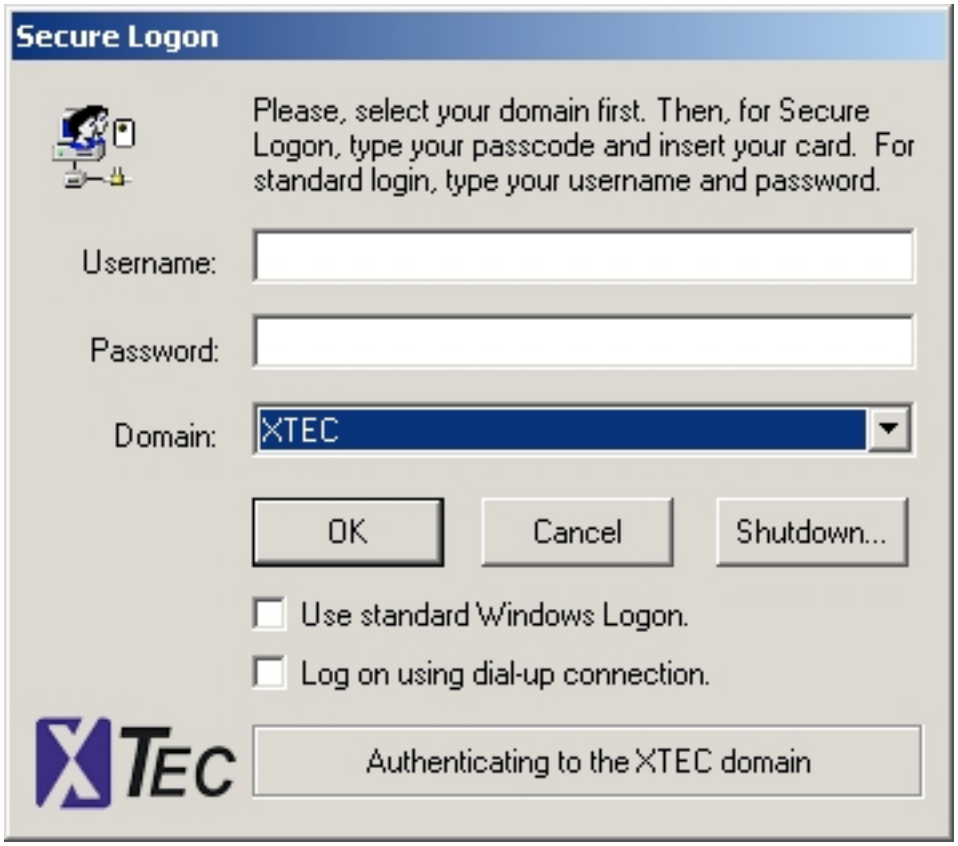
identificador relativo (RID)

SID: S-1-0
Name: Null Authority
Description: An identifier authority.

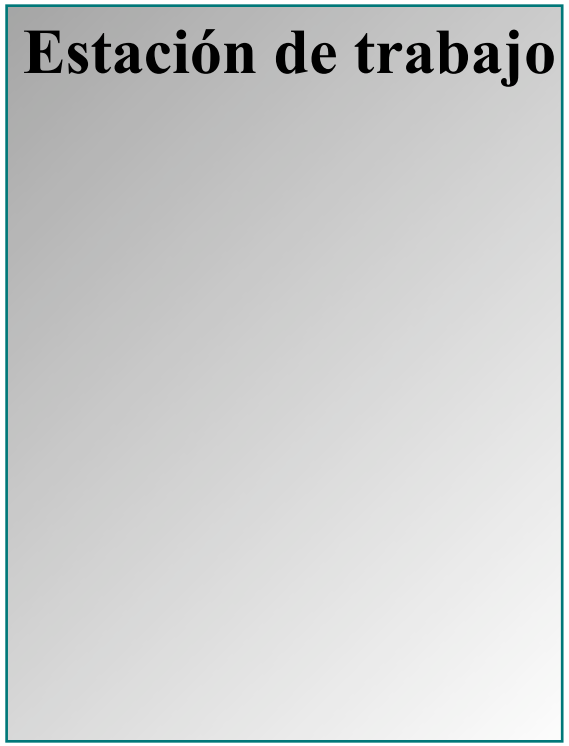
SID: S-1-0-0
Name: Nobody
Description: No security principal.

SID: S-1-1
Name: World Authority
Description: An identifier authority.

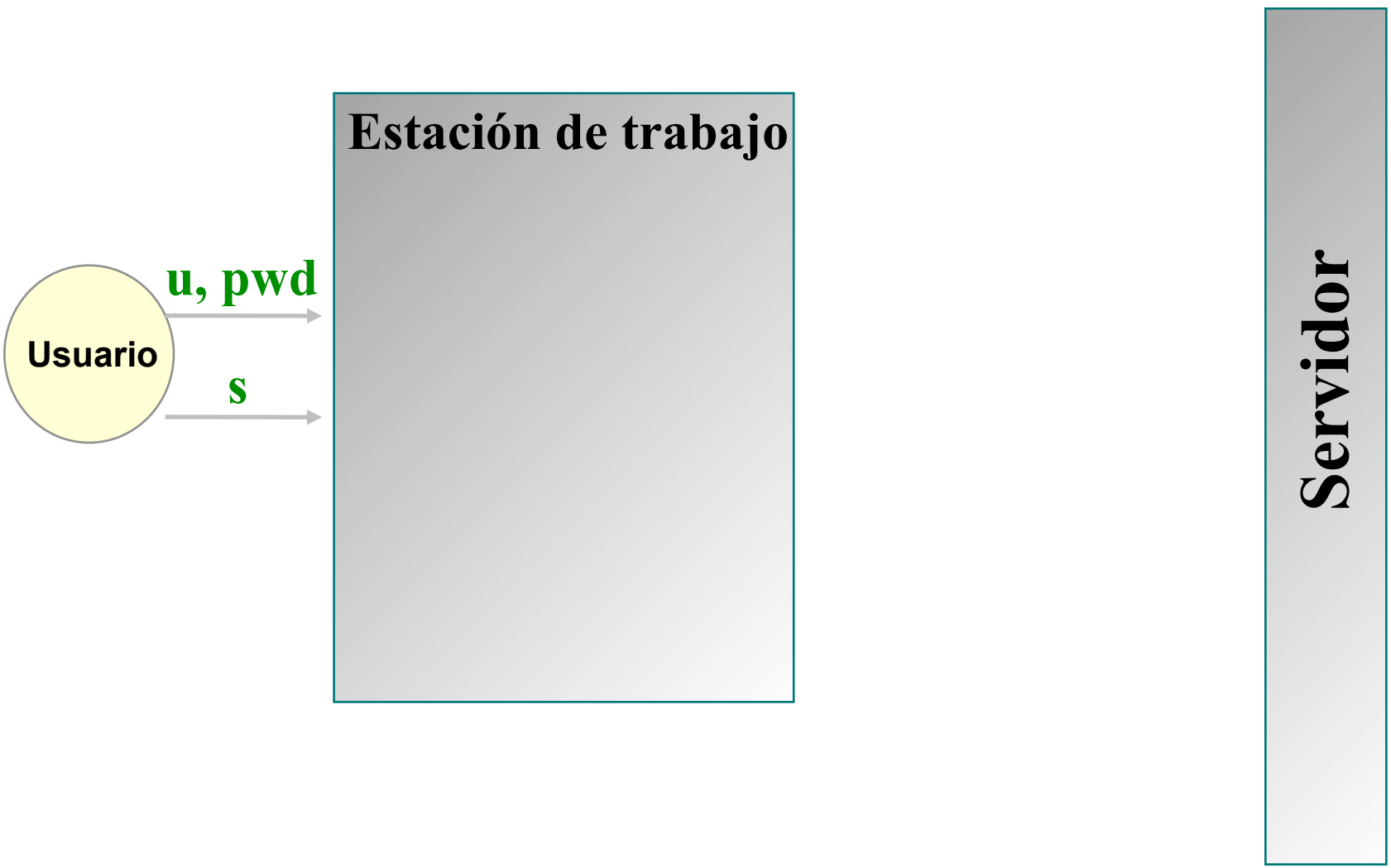
# Autenticación



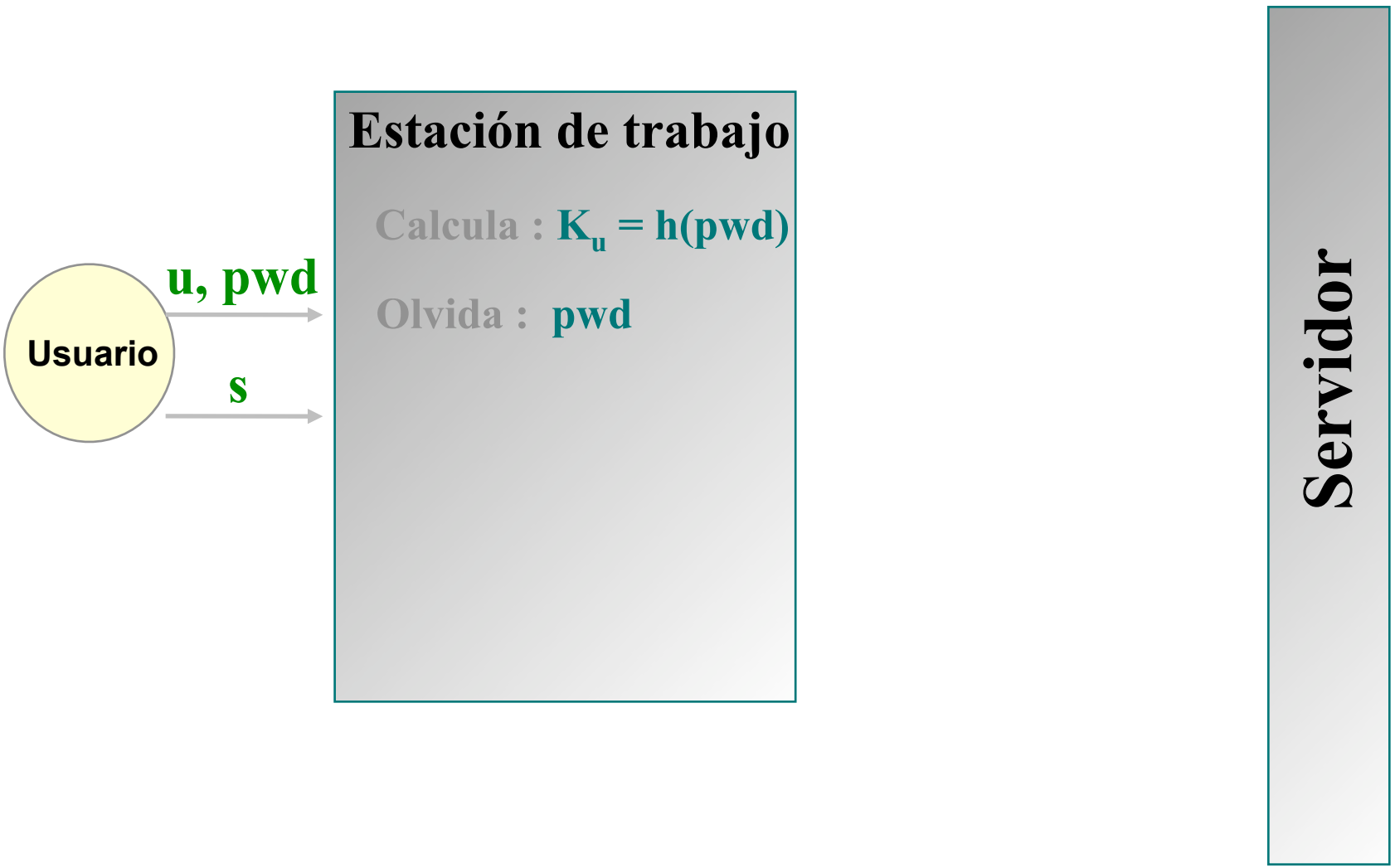
# Autenticación en Windows NT/2000

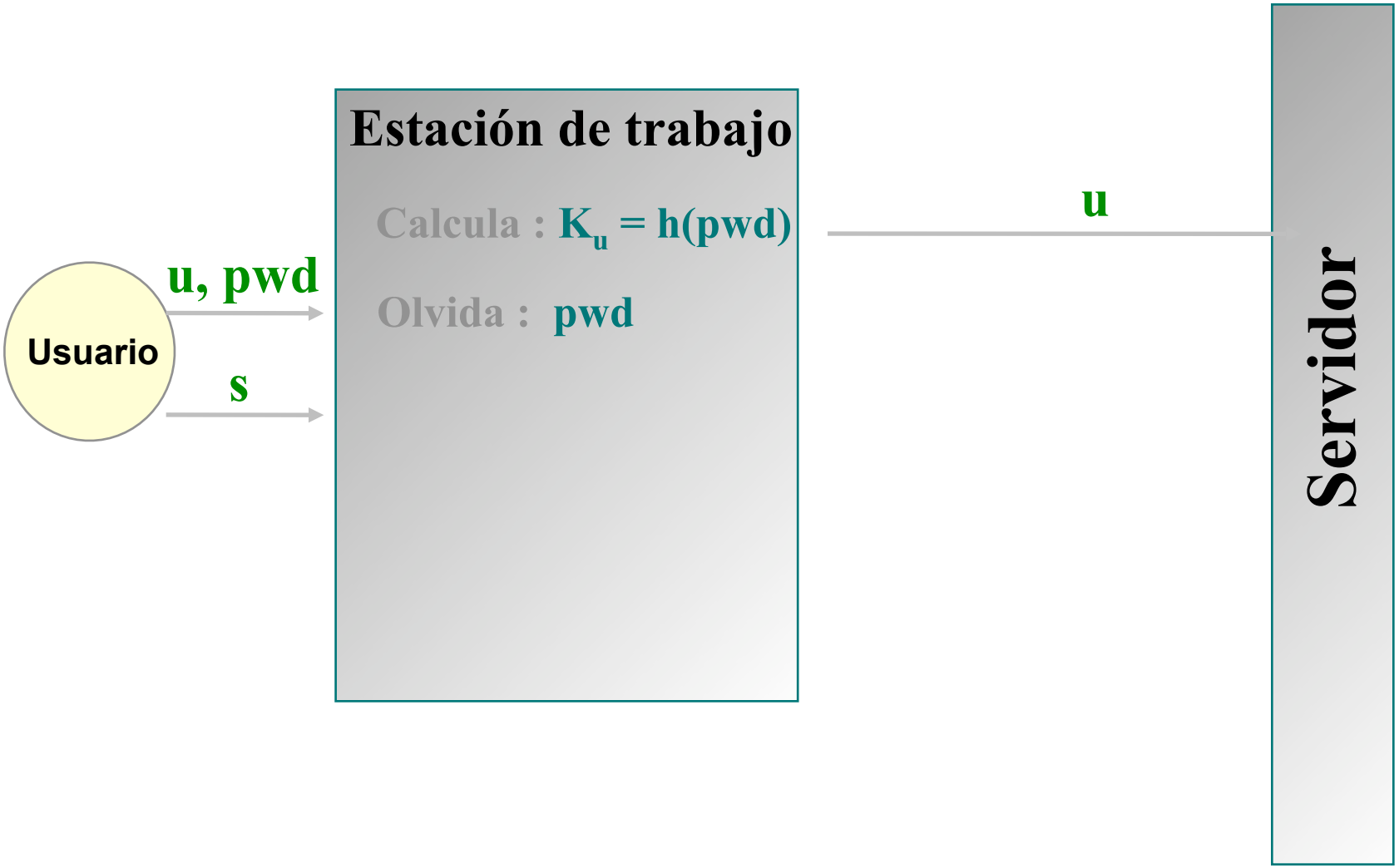

# Autenticación en Windows NT/2000



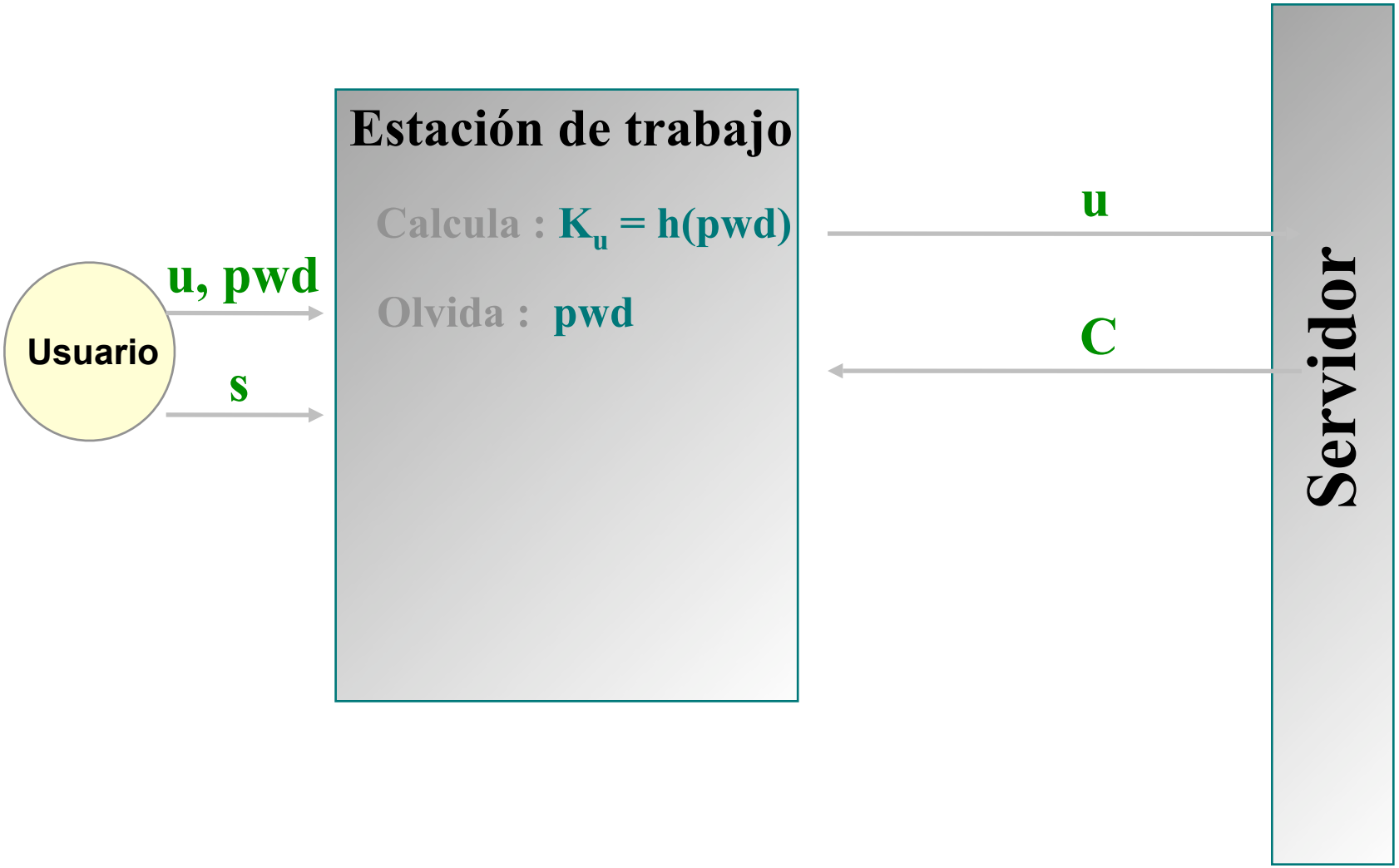
# Autenticación en Windows NT/2000



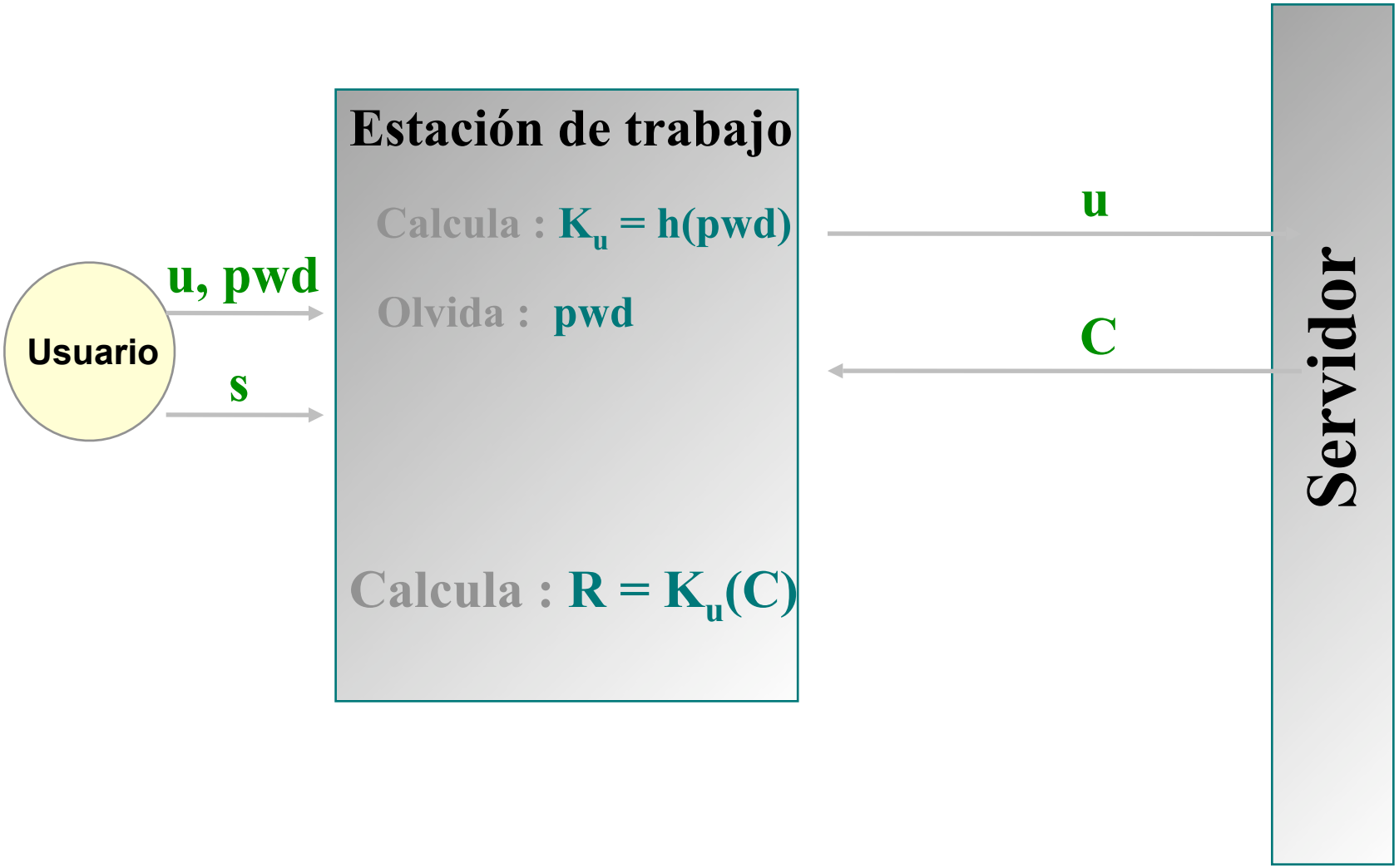
# Autenticación en Windows NT/2000



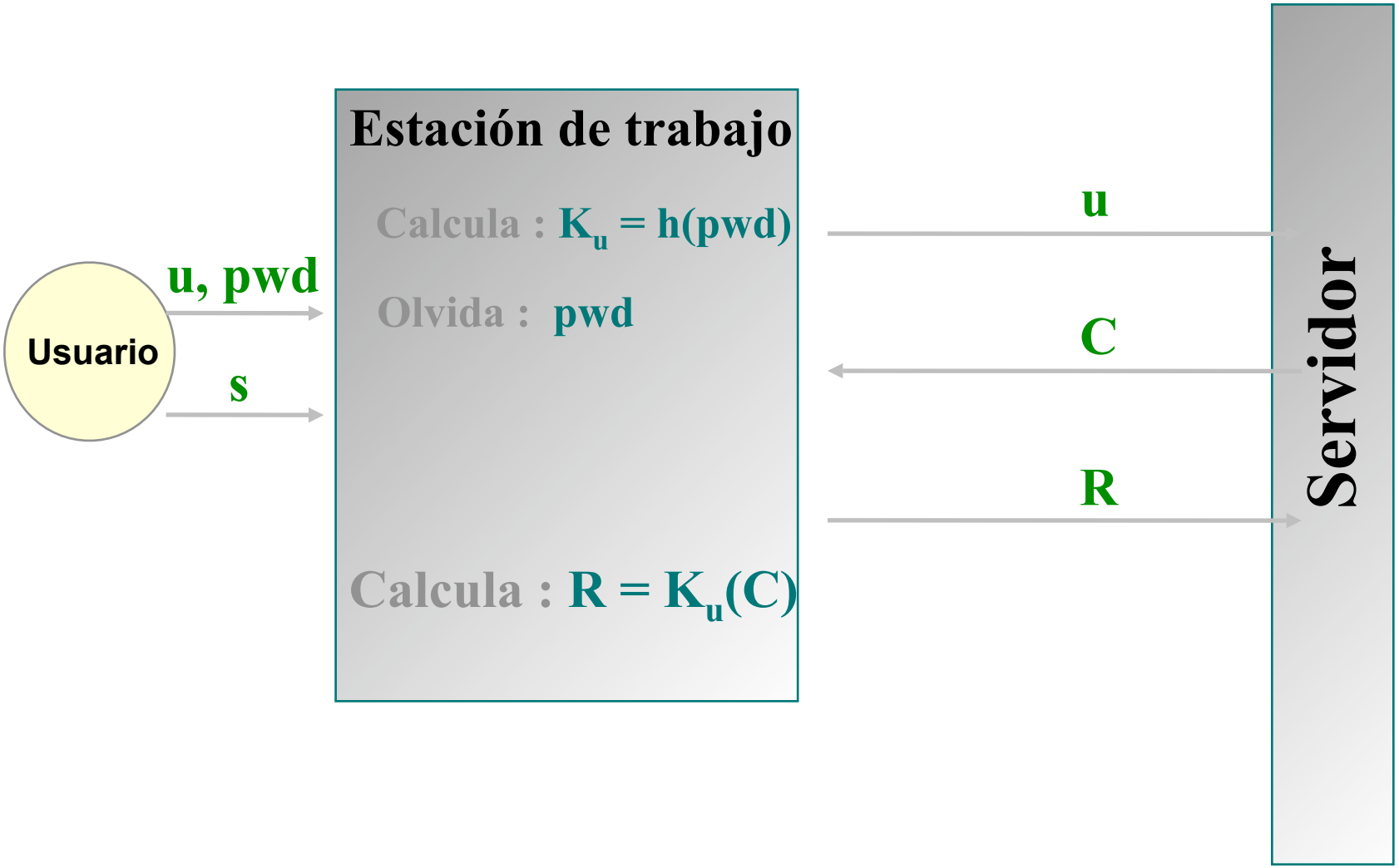
# Autenticación en Windows NT/2000



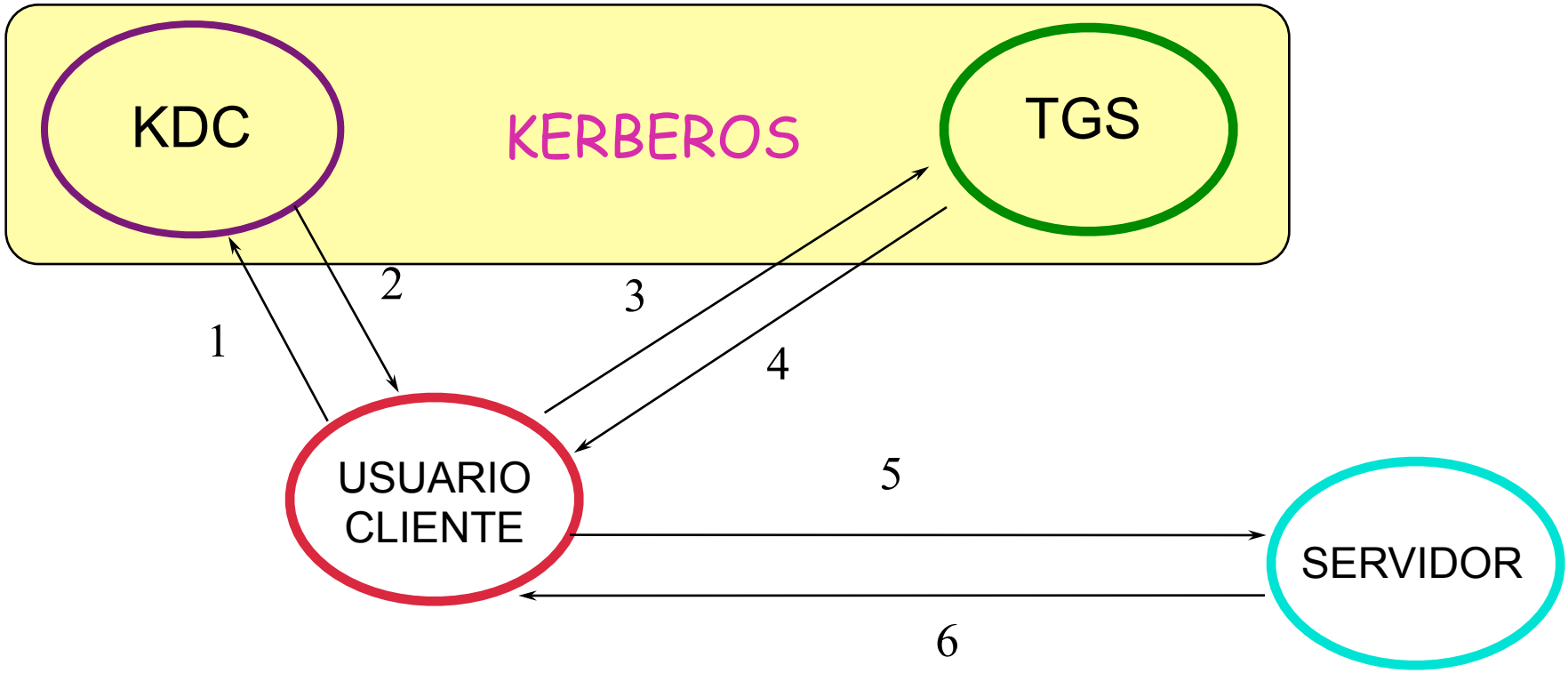
# Autenticación en Windows NT/2000



# Autenticación en Windows NT/2000



# El protocolo Kerberos




1) SOLICITUD DE TICKET PARA TGS
2) TICKET PARA EL TGS
3) SOLICITUD DE TICKET PARA SERVIDOR
4) TICKET PARA SERVIDOR
5) SOLICITUD DE SERVICIO
6) AUTENTIFICACION DEL SERVIDOR

# Windows para grupos de trabajo y dominos

# Definiciones

- Grupos:
  - Agrupamiento lógico de computadoras que comparten recursos
  - Mantenimiento local de la seguridad en cada nodo de forma individual.
  - En un grupo podemos encontrar: Win95, Win98 o NT Wkst
- Dominios:
  - Agrupación lógica de computadoras, que comparten recursos, con una política de seguridad centralizada.
  - Un dominio puede administrarse de forma centralizada.
  - En un dominio tenemos al menos un NT Server (PDC) y posiblemente otro (BDC). El resto: Win95, 98 o NT Wkst
- Criterios de selección:
  - redes pequeñas (de 2 a 20): modelo de grupos
  - en redes grandes: modelo de dominio

# Sistema de recursos de red

- En una red Microsoft se pueden compartir varios tipos de recursos.
- El nombre de los recursos sigue el siguiente convenio:

  \\servidor\recurso

- Dos tipos de navegación en una red SMB
  - Navegar por una lista de ordenadores y sus recursos compartidos
  - Navegar por los recursos compartidos de un determinado ordenador

# NetBios

- Network Basic Input/Output System
- Diseñado por IBM en 1984
- Es una interfaz que abstrae el acceso a la red
  - igual que BIOS abstrae el acceso al hardware de los PCs
- Sirve para establecer
  - nombres lógicos en la red
  - sesiones entre los nombres (nodos) de la red
- NetBios aparece antes que IP!
- El servicio soporta transferencia de datos
  - Para sesiones NetBIOS y SMB

# Características NetBios

- Es una API
  - herramienta que permite a las aplicaciones contar con un medio para direccionar un host por su nombre
- Aplicaciones esperan un hostname
  - no saben que hacer con una direccion MAC
- Como interfaz con ambiente TCP/IP, el API usa una herramientas especial llamada NETBT
  - NETBios sobre TCP/IP

# NetBEUI

- NetBIOS Extended User Interface
- Introducido por IBM en 1985
- Es un protocolo de red simple y eficiente para comunicar hasta 254 máquinas
- Es el protocolo por defecto en Windows 95
- Limitaciones
  - Utiliza el nombre de la máquina como dirección
  - No soporta encaminamiento
- Como actualmente TCP/IP es el estándar de facto, las nuevas versiones de Windows soportan NetBIOS sobre TCP/IP
  - NBT resuelve la conversión de nombres a números de IP

# SMB

- SMB (Server Message Block)
  - Protocolo de comunicación: Windows, OS/2
- Fue introducido en MS-DOS para proporcionar servicios de compartición de recursos entre nodos de red.
- Es un protocolo petición-respuesta
- El puerto por defecto es 139

# WINS

- Windows Internet Name Service 
- Es la realización del servidor de nombres de NetBIOS (NBNS) producida por Microsoft.
- Es plano
  - Solo se puede usar un nombre para una cosa: máquina o grupo
- Es dinámico
  - Una máquina se registra su nombre, dirección y grupo
  - Periódicamente se tiene que refrescar el registro
  - Si no se utiliza dominio o grupo, la máquina se puede registrar en cualquier servidor y servir cualquier servicio.
- Puede haber varios servidores
  - Hay un mecanismo para comunicar información entre ellos
  - El resultado es una base de datos global sincronizada

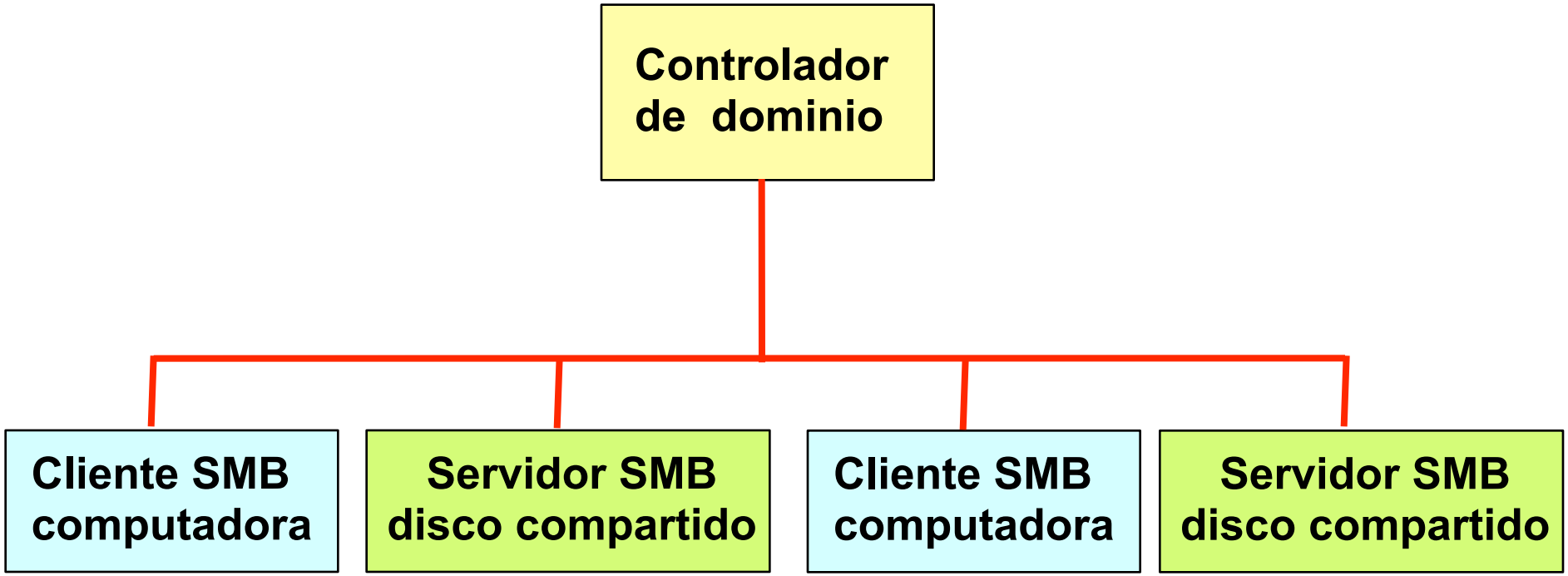
# Dominios NT

- Introducción de la presencia de un administrador
- Compuesto por un manejador primario (PDC) y estaciones que actuan como clientes
- El PDC almacena la base de datos de usuarios y de computadoras del dominio

# Elementos de un dominio

- PDC (Controlador principal de dominio)
- BDC (Controladores de reserva del dominio)
- Estaciones de trabajo
- Servidores NT

# Un simple dominio windows



# El PDC

- Controlador principal de dominio
- Obligatorio
- Mantiene la base de datos del dominio
- Debe ser un NT Server configurado como controlador principal del dominio

# El BDC

- Controladores de reserva del dominio
- Puede haber varios en el dominio
- Ayudan al PDC en caso de sobrecarga o mal funcionamiento
- Recomendable tener al menos un BDC en el dominio

# Estaciones de trabajo

- Son los clientes del dominio
- Pueden ser de diferentes tipos: Windows, OS/2, etc

# Los controladores del domino

- Todo dominio tiene una base de datos de usuarios.
- La copia original de esta base de datos reside en el PCD.
- En esta base de datos quedan registradas todas las características de los usuarios, sus cuentas, y de las computadoras que forman parte del dominio.

# Los controladores del domino

- Además del PCD, puede haber dentro de un dominio varios BCD.
- En estos controladores se mantiene una copia de la base de datos de usuarios del dominio.
- Si el controlador del dominio está muy cargado o simplemente está inactivo,
  - cualquier controlador del dominio puede validar el inicio de sesión en el dominio.

# Usuarios y grupos

- Todo usuario tienen un nombre de usuario y una contraseña.
- Los grupos son colecciones de usuarios
- Los usuarios y grupos tienen asignados derechos y permisos

# Las cuentas

- Las cuentas de usuarios contienen información acerca de usuarios
  - Nombre completo
  - Nombre usuarios
  - Contraseña
  - Directorio hogasr
  - Información de cuando y en que horario el usuario puede usar una sesion
  - Parámetros personales del escritorio

# Tipos de cuentas

- Cuentas locales
  - cuentas que solo tienen permiso de acceso local
- Cuentas globales
  - cuentas disponibles en todo el dominio

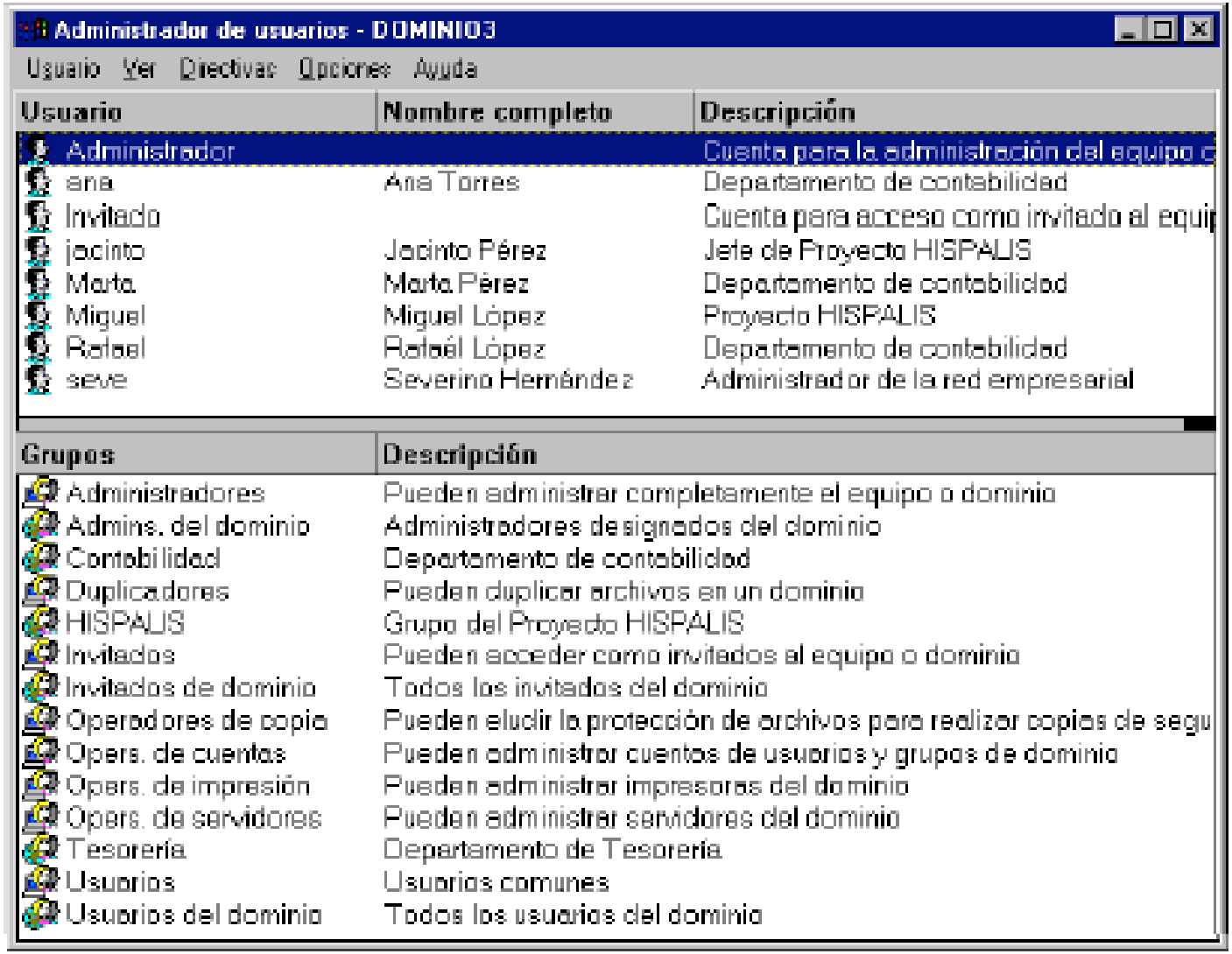
# Cuentas especiales

- Administrador
  - cuenta de mayor nivel
- Guest
  - permite acceso restringido a un sistema para la gente que no tiene una cuenta
  - por omisión esta deshabilitada
- System
  - cuenta especial usada por el sisytema para ejecutar programas, utilidades y controladores

# El administrador de usuarios

- En NT hay dos tipos de usuarios, aquellos que pertenecen a una máquina que corre NT Workstation o Server y aquellos que pertenecen a un dominio NT. Para cada uno de estos tipos de usuarios existe una herramienta de administración: el administrador de usuarios incluido en NT Workstation y el administrador de usuarios para dominios incluido en NT Server. El funcionamiento de ambos es muy similar, pero el administrador de usuarios para dominios dispone de más opciones.

# El administrador de usuarios



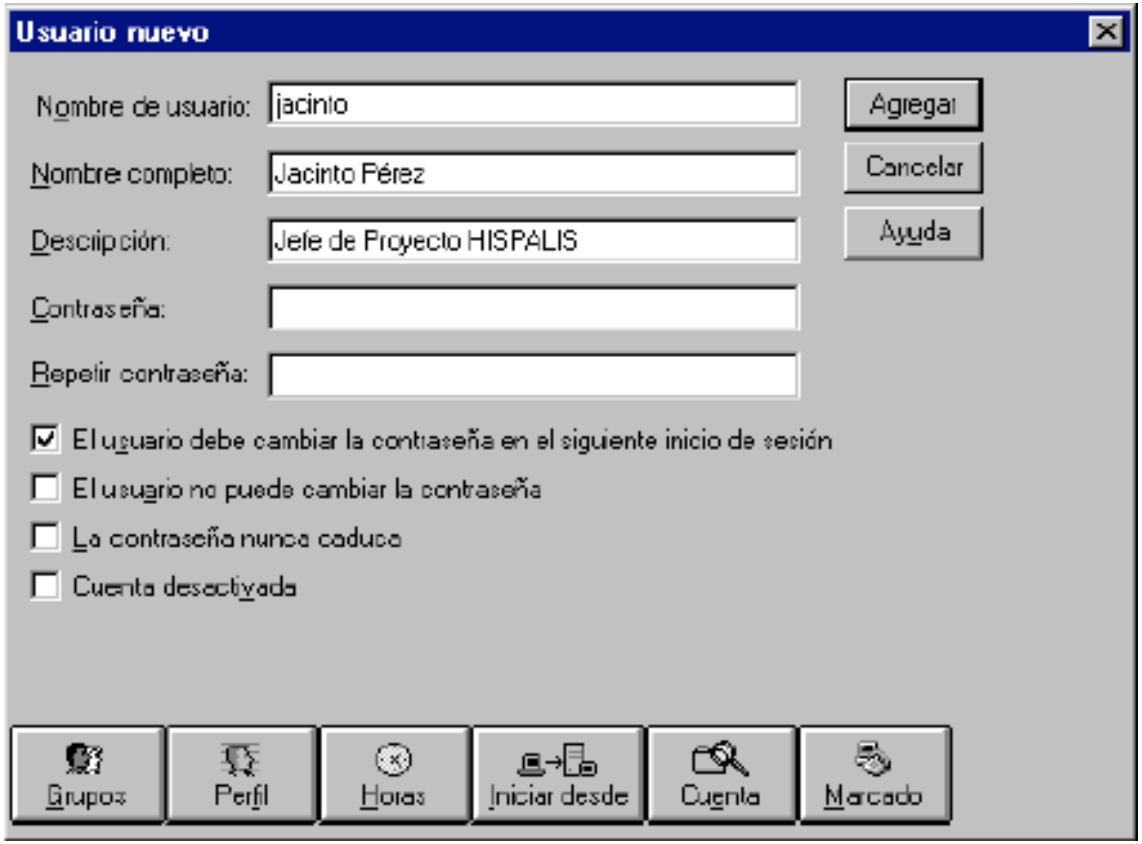
# El administrador de usuarios

- Tareas que se pueden realizar con el administrador de usuarios:
  - Añadir, modificar y eliminar usuarios del dominio.
  - Añadir, modificar y eliminar grupos locales y globales del dominio.
  - Fijar el plan de cuentas y contraseñas en el dominio.
  - Fijar la política de derechos de usuario en el dominio.
  - Establecer el sistema de auditoria en el dominio.
  - Establecer relaciones de confianza entre dominios.

# El administrador de usuarios

## Creación y modificación de usuarios

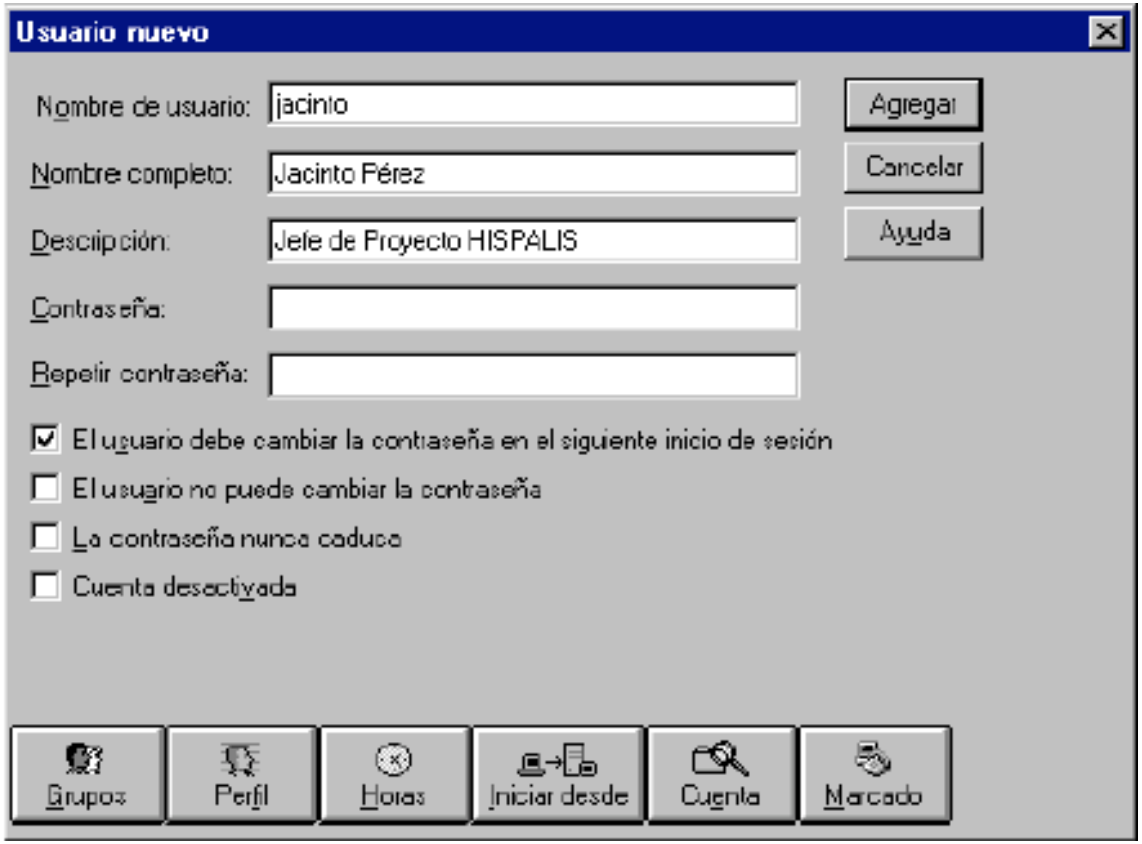
- Usuarios\Nuevo



# El administrador de usuarios

## Creación y modificación de usuarios

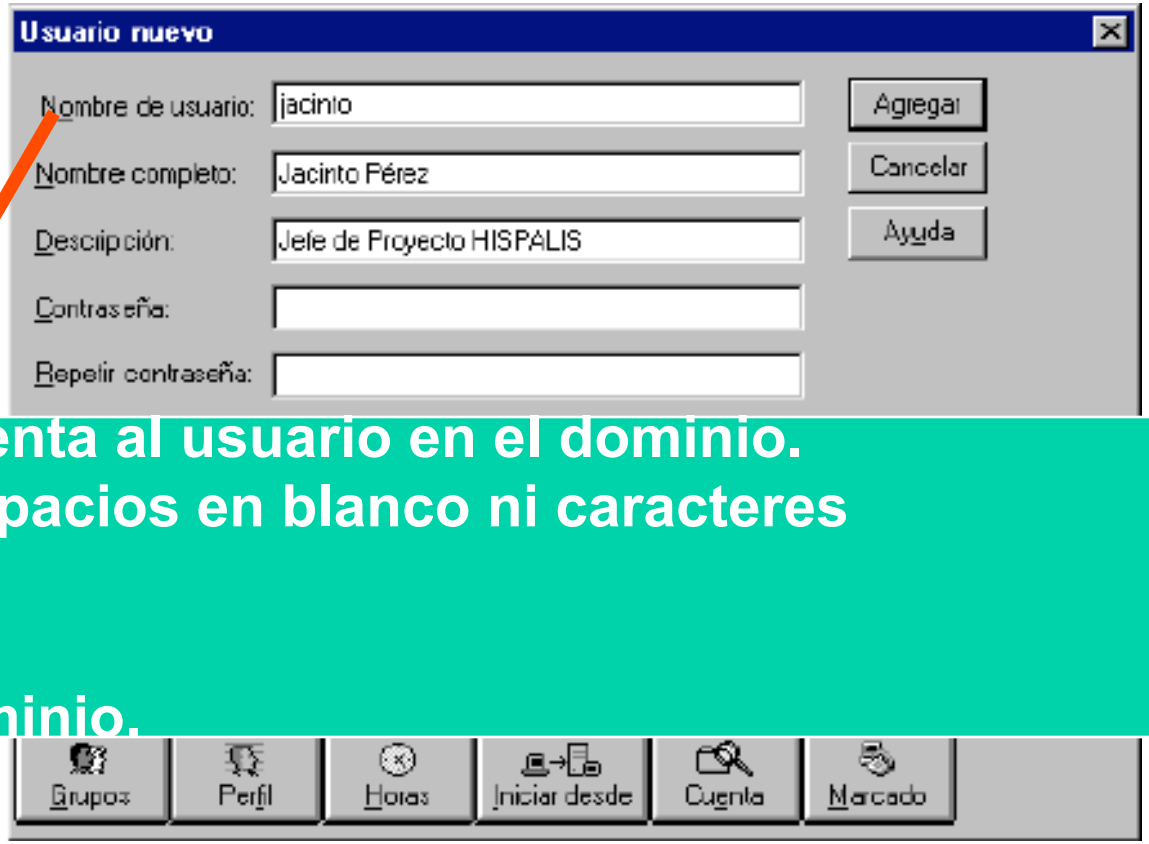
- Usuarios\Nuevo



# El administrador de usuarios

## Creación y modificación de usuarios

– Usuarios\Nuevo

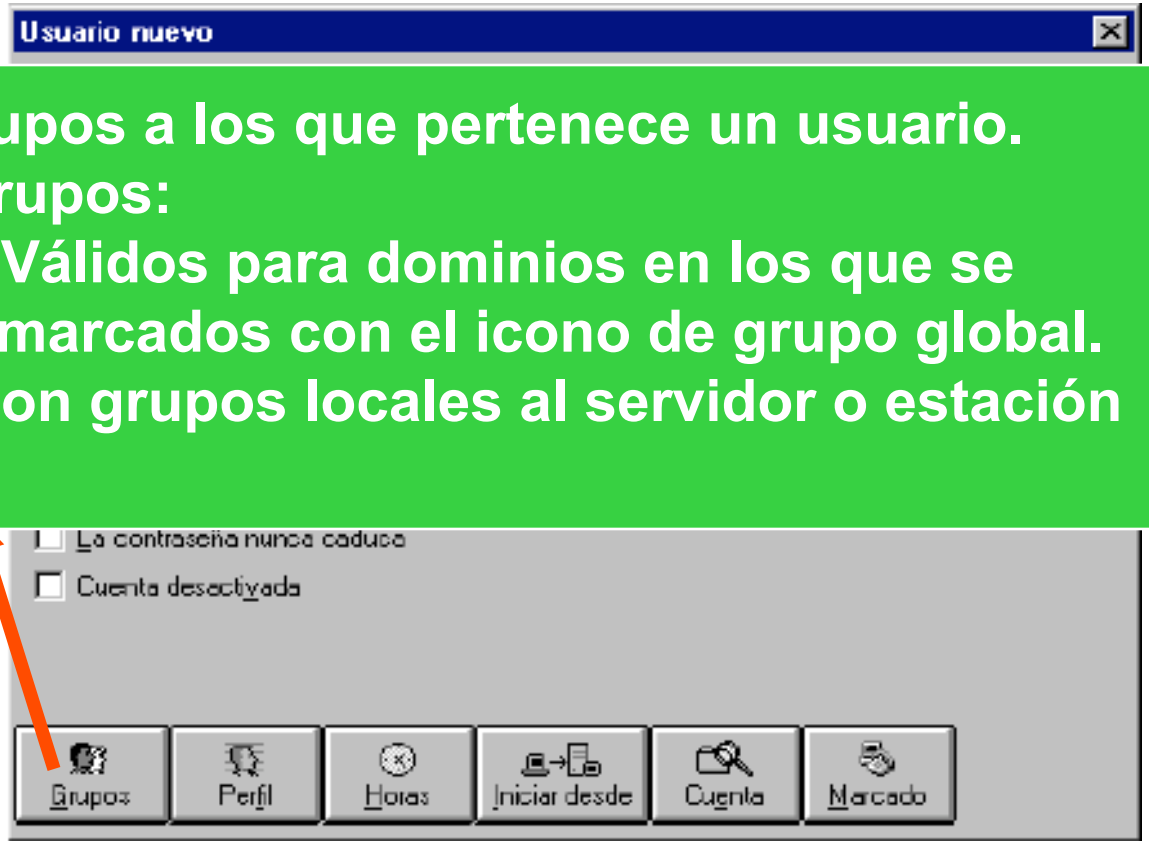



- Identificador que representa al usuario en el dominio.
- Palabra completa, sin espacios en blanco ni caracteres especiales
- Hasta 14 caracteres
- Debe ser único en el dominio.

# El administrador de usuarios

## Creación y modificación de usuarios

– Usuarios\Nuevo




**Permite establecer los grupos a los que pertenece un usuario.**
**En NT hay dos tipos de grupos:**

- **Grupos globales. Válidos para dominios en los que se confían. Aparecen marcados con el icono de grupo global.**
- **Grupos locales. Son grupos locales al servidor o estación de trabajo.**

# El administrador de usuarios

## Creación y modificación de usuarios

**Permite controlar las características del entorno de un usuario.**

**Perfíl. Nombre del fichero que representa el perfil del usuario para NT.**

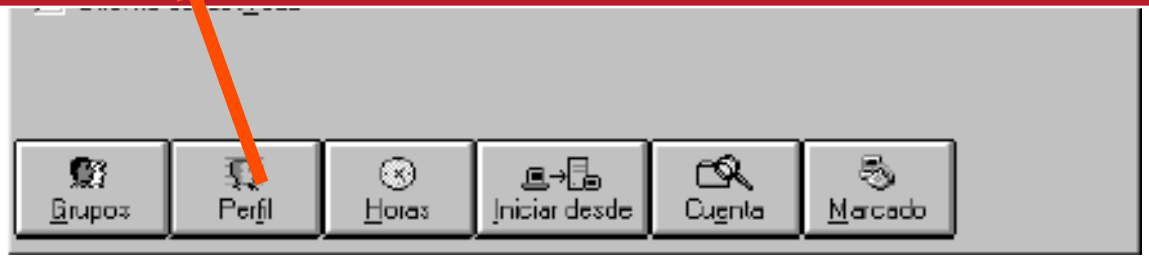
**\\servidor\recurso\directorio\fichero.bat.**

**Archivo de inicio. Asigna un archivo que se ejecutará al iniciar la sesión de red en el dominio.**

**Directorio de trabajo. Admite dos modalidades de uso.**

**Ruta de acceso local. Utilizar una ruta local al ordenador en que se inicia la sesión.**

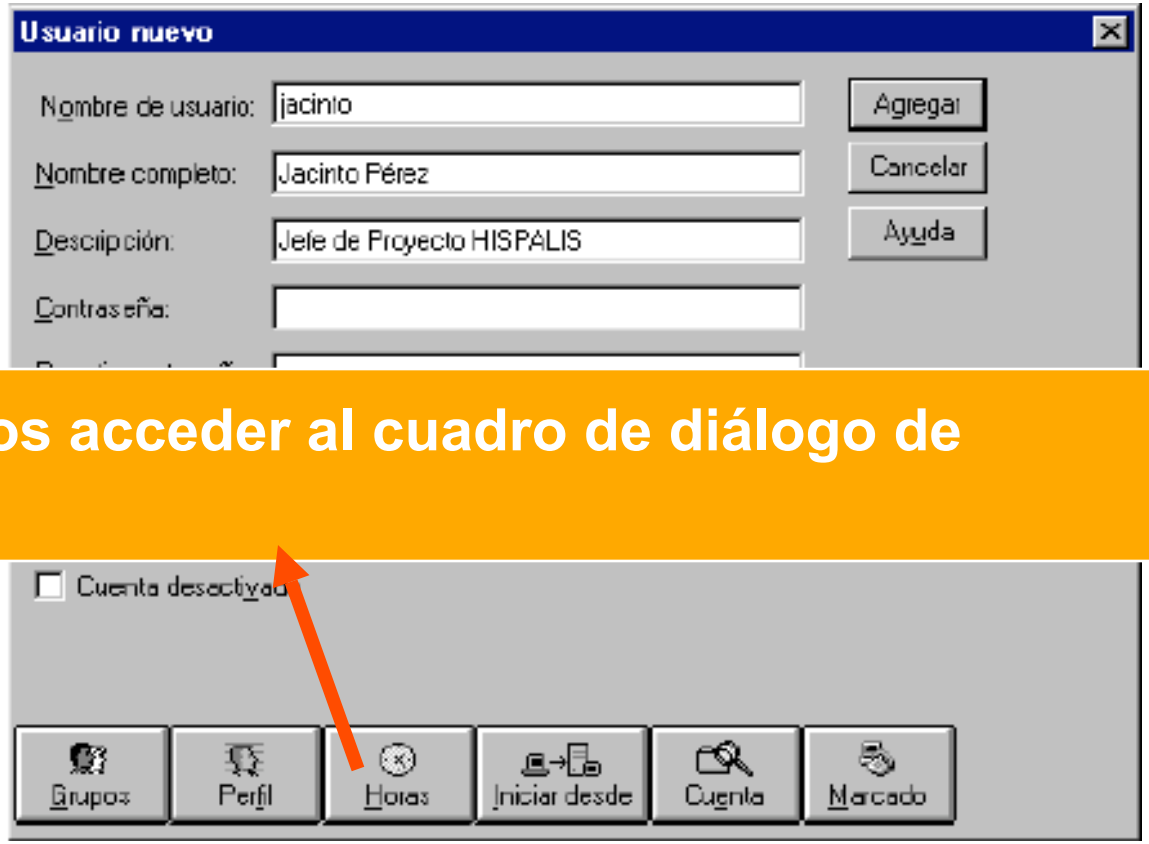
**Conectar una letra de unidad a una unidad de red del tipo \\servidor\recurso.**



# El administrador de usuarios

## Creación y modificación de usuarios

- Usuarios\Nuevo

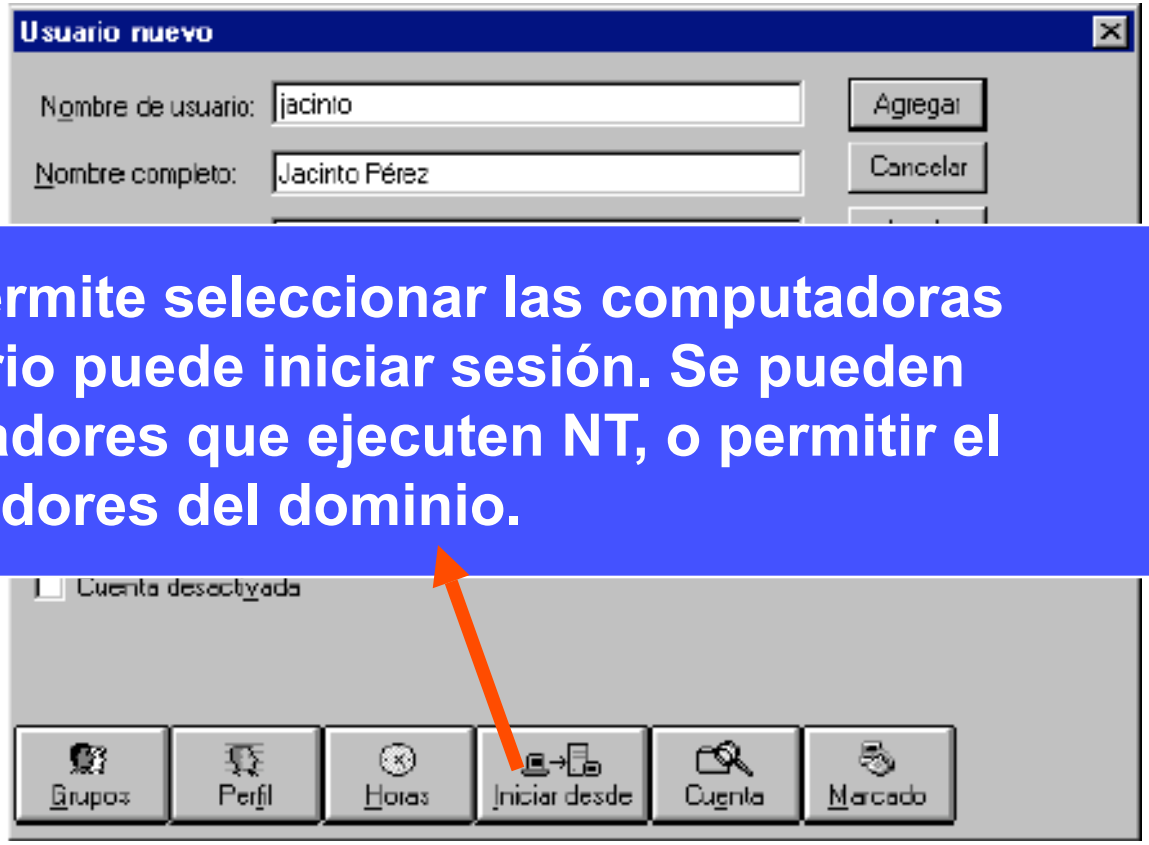



**En el botón Horas podemos acceder al cuadro de diálogo de Horas de inicio de sesión.**

# El administrador de usuarios

## Creación y modificación de usuarios

- Usuarios\Nuevo

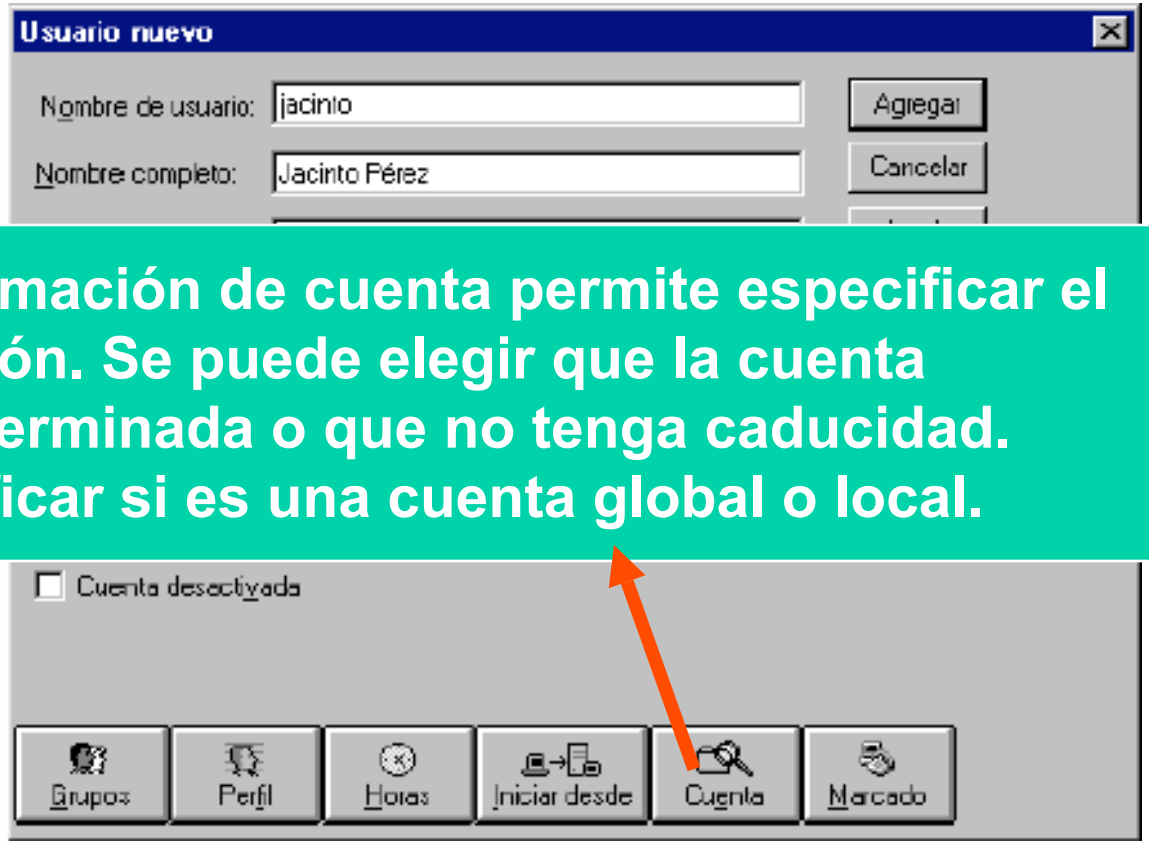



**Este cuadro de diálogo permite seleccionar las computadoras desde las cuales un usuario puede iniciar sesión. Se pueden especificar hasta 8 ordenadores que ejecuten NT, o permitir el inicio en todos los ordenadores del dominio.**

# El administrador de usuarios

## Creación y modificación de usuarios

- Usuarios\Nuevo

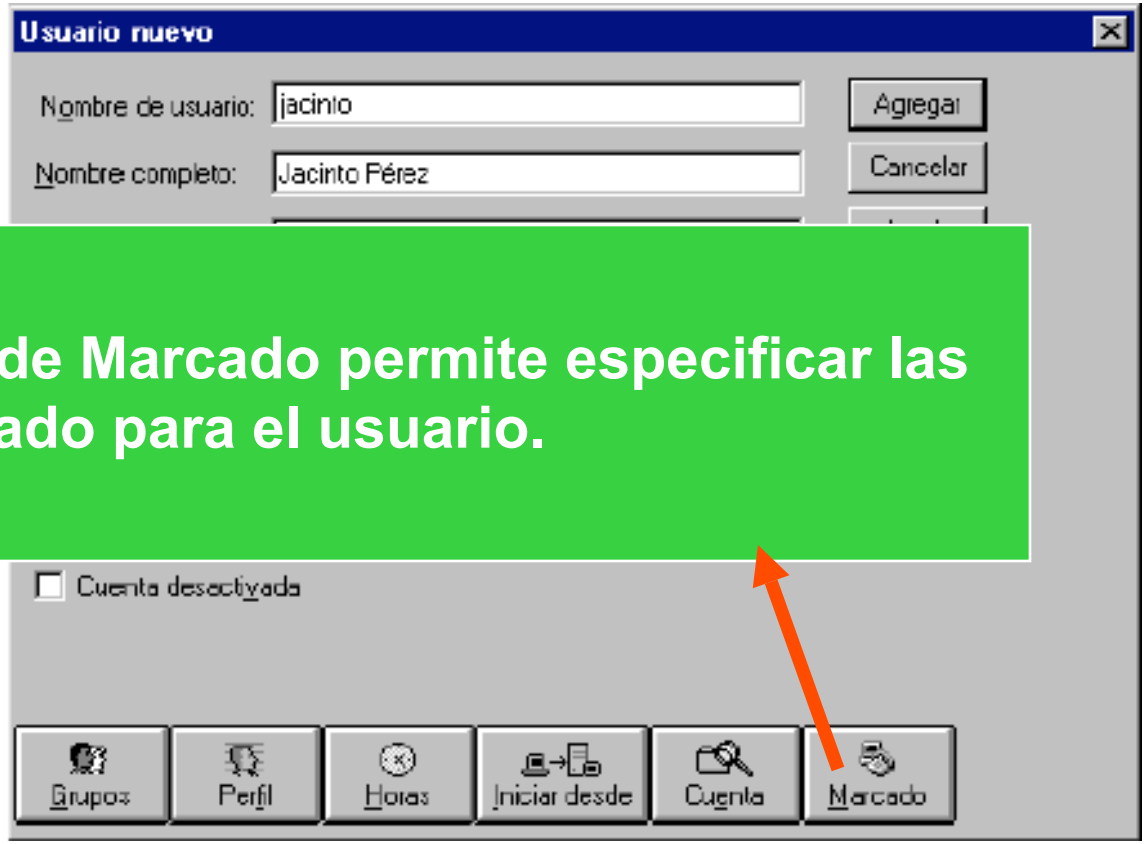



**El cuadro de diálogo Información de cuenta permite especificar el tipo de cuenta y su duración. Se puede elegir que la cuenta caduque en una fecha determinada o que no tenga caducidad. También se puede especificar si es una cuenta global o local.**

# El administrador de usuarios

## Creación y modificación de usuarios

- Usuarios\Nuevo




**El cuadro de diálogo de Marcado permite especificar las propiedades de marcado para el usuario.**

# El administrador de usuarios

## Modificar un usuario.

- Usuario\Propiedades
  - Se acceden a los mismos cuadros de diálogo empleados al crearlo salvo que ahora aparece una casilla para cuentas bloqueadas. Si el bloqueo de cuentas está activado en el dominio y el usuario ha fallado el número de veces limitado para ese dominio, esta casilla aparece activada. Al desactivarla, la cuenta del usuario es desbloqueada.

# El administrador de usuarios

## Creación de Grupos.

- Usuario\Propiedades
  - El Administrador de usuarios NT WS o Server configurado como servidor permite:
    - Crear usuarios locales: sólo tienen validez en el propio ordenador.

# El administrador de usuarios

## Creación de Grupos.

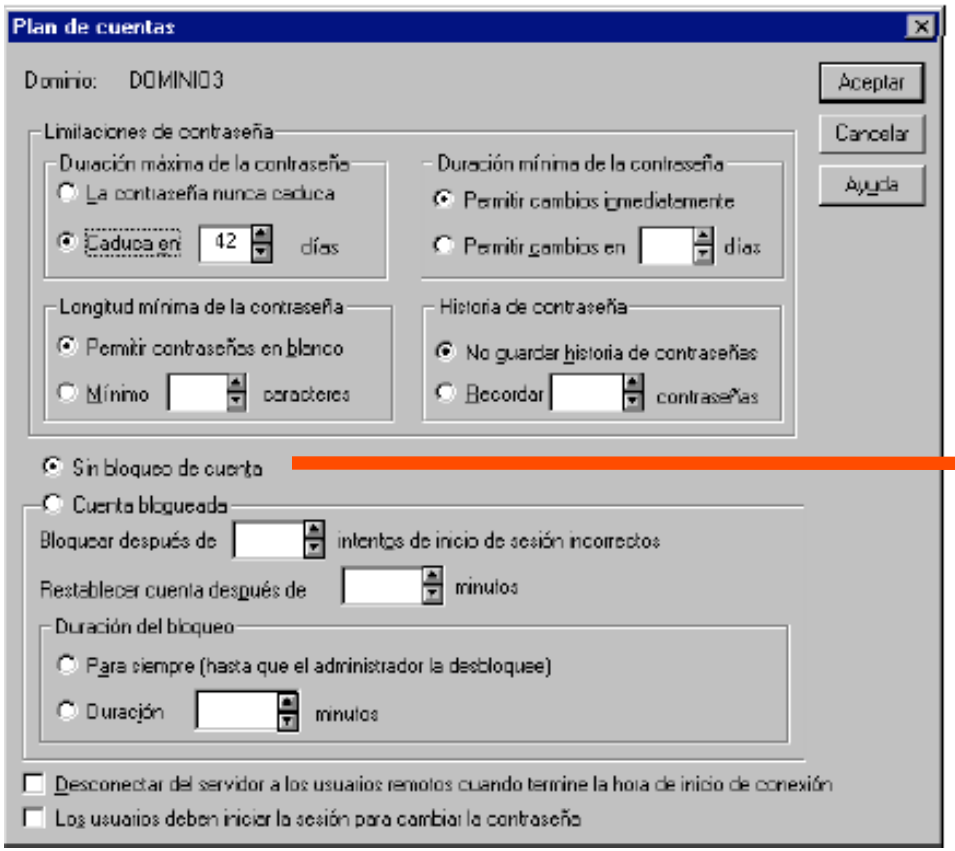
- Usuario\Propiedades
  - El administrador de usuarios para dominios permite crear:
    - Grupos globales. Tienen como miembros a los usuarios del dominio y se pueden utilizar tanto en los servidores del dominio como en las estaciones de trabajo del dominio. También se pueden usar en otros dominios en los que se confía.
    - Grupos locales. Pueden obtener permisos en los servidores del dominio propio. Pueden ser miembros de los grupos locales los miembros del dominio, los grupos globales del dominio y los grupos globales de otros dominios en los que se confía.

# Administración del plan de seguridad.

- **En NT se pueden fijar una serie de directivas comunes para todo el dominio.**
  - **Plan de cuentas para el dominio, que fija propiedades de las cuentas tales como la política de contraseñas.**
  - **Plan de derechos de usuarios, que permite asignar determinados permisos genéricos a usuarios o grupos del dominio.**
  - **Plan de auditoria, que permite activar los elementos del sistema de auditoria en el dominio.**

# Administración del plan de seguridad.
## Administración del plan de cuentas.

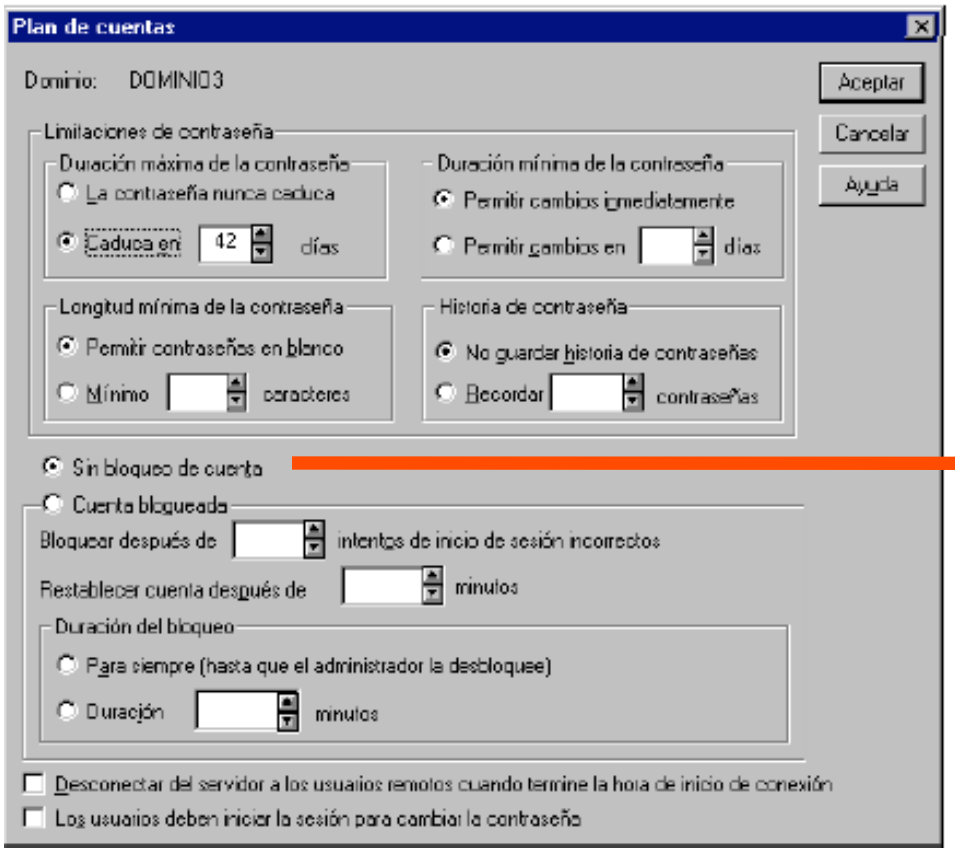
- Directivas\Cuentas




El sistema de bloqueo. Reacciona frente a los intentos fallidos de iniciar sesión en el dominio. Una vez bloqueada la cuenta se puede elegir entre desbloqueo automático o manual, con intervención del administrador del dominio.

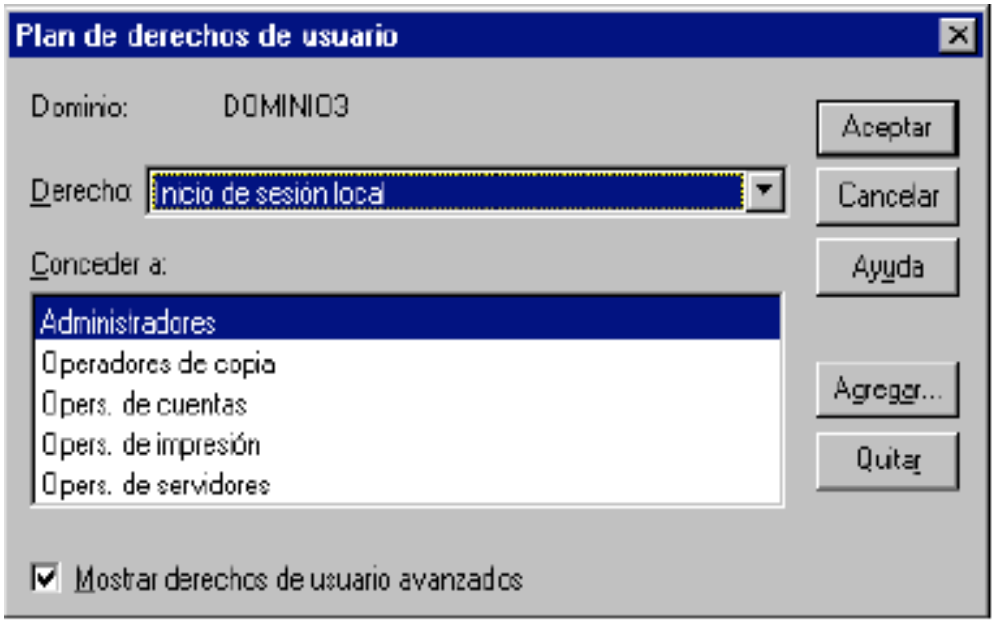
# Administración del plan de seguridad.
## Administración del plan de cuentas.

- Directivas\Cuentas




El sistema de bloqueo. Reacciona frente a los intentos fallidos de iniciar sesión en el dominio. Una vez bloqueada la cuenta se puede elegir entre desbloqueo automático o manual, con intervención del administrador del dominio.

- Directivas\Derechos de usuarios



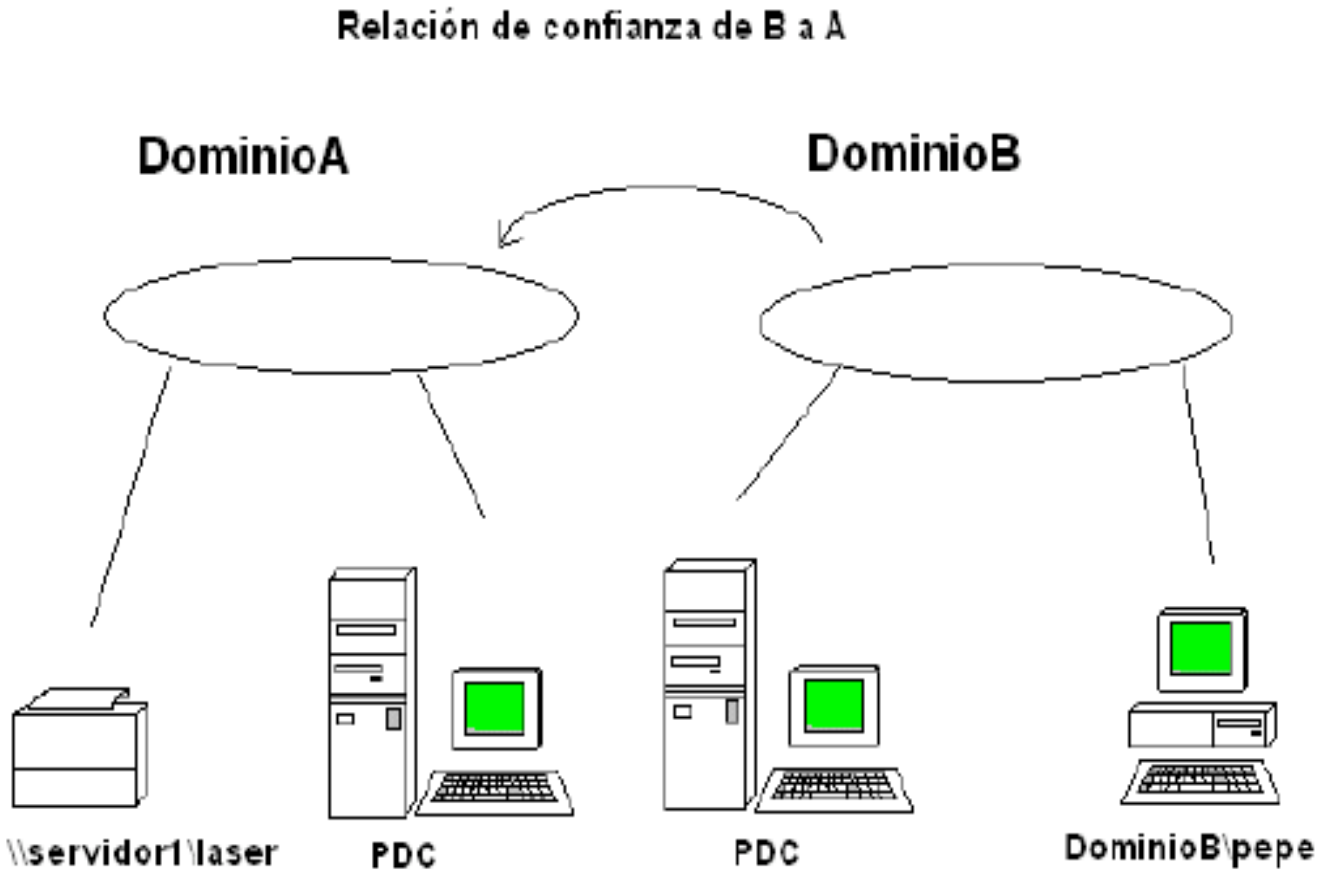

**Los derechos de usuarios son una serie de permisos que no se aplican sobre un objeto concreto, como un archivo, impresora o directorio, sino que se aplican al sistema completo. Se pueden asignar a cada tipo de derecho de usuario los usuarios o grupos de usuarios a los que se necesite otorgar ese derecho.**

# Relaciones de confianza entre dominios y múltiples dominios

- El sistema de dominios de NT tiene actualmente un grave inconveniente: no existe una jerarquía de dominios.
- Organización compleja -> Sistema de múltiples dominios.
  - Se puede establecer unas relaciones entre ellos de manera que los usuarios, recursos y equipos sean reconocidos en diferentes dominios.
  - Establecer relaciones de confianza entre dominios permite que los miembros de un dominio puedan reconocer las cuentas de usuario de otros dominios.

# Relaciones de confianza entre dominios y múltiples dominios

## Creación de una relación de confianza entre dos dominios

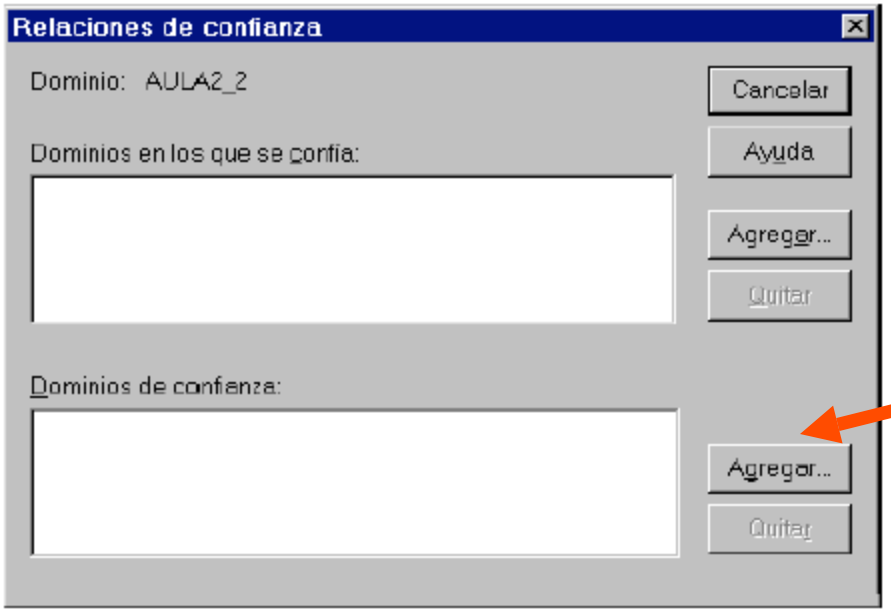



**NT para delegar la autentificación es la relación de confianza entre dominios.**

- La relación de confianza entre dos dominios permite a los servidores de un dominio consultar la base de datos de usuarios y equipos de otro dominio para autentificar a un usuario de ese dominio.
- Las relaciones de confianza son unidireccionales, es decir, puede existir una relación de confianza de A a B y otra de B a A.

- Escenario:
  - DominioB\pepe debe imprimir en el servidor de impresión de DominioA,
- Requisito
  - la base de datos de usuarios de DominioB debe ser accesible para los miembros del DominioA.
  - Por ello debemos configurar los dos dominios:

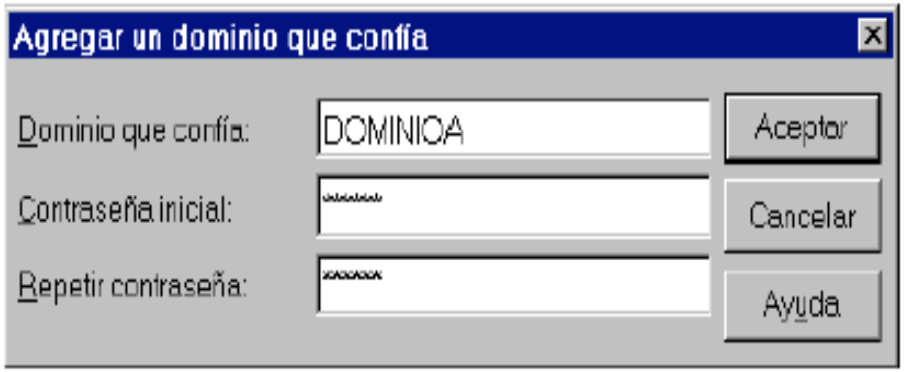
- DominioB. Abrimos el Administrador de usuarios para Dominios y seleccionamos el menú Directivas\Relaciones de confianza. Aparece un cuadro de diálogo con las relaciones de confianza establecidas actualmente.




**Ahora pulsamos el botón Agregar de la sección Dominios de confianza. Aparece el cuadro de diálogo Agregar dominio que confía.**

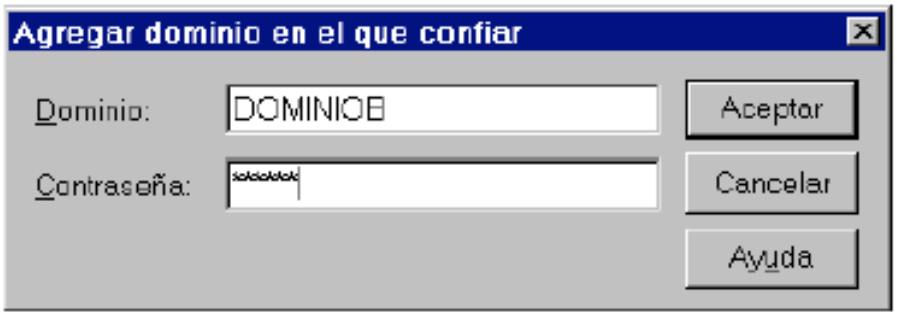
- DominioB. Abrimos el Administrador de usuarios para Dominios y seleccionamos el menú Directivas\Relaciones de confianza. Aparece un cuadro de diálogo con las relaciones de confianza establecidas actualmente.

DominioB confia en DominioA




**Escribimos el nombre de dominio que va a consultar nuestra base de datos, es decir DominioA, y una contraseña para que pueda consultar la base de datos de usuarios.**

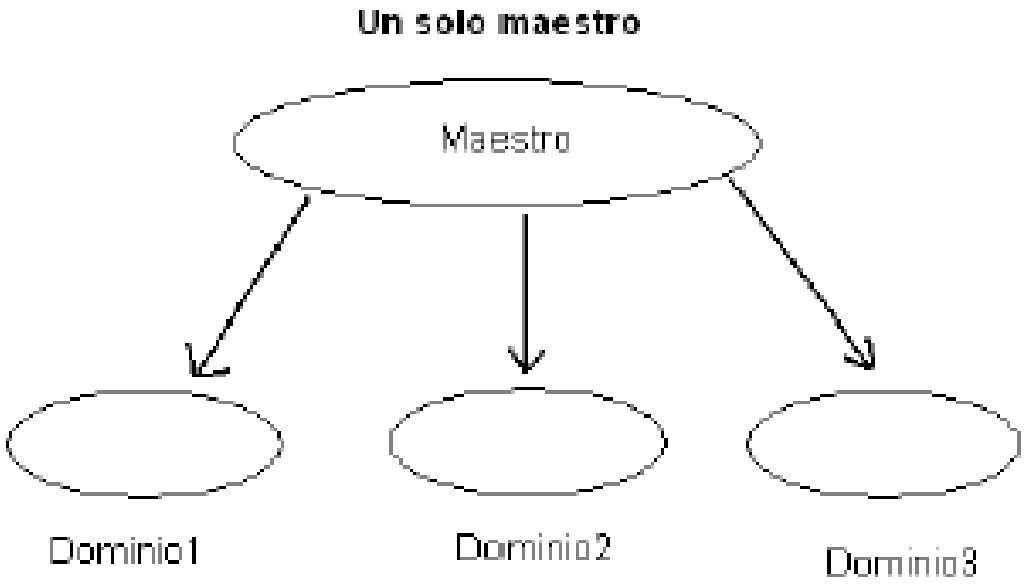
- DominioA. Abrimos el Administrador de usuarios para dominios y seleccionamos Directivas\Relaciones de confianza. En el cuadro de diálogo de Relaciones de confianza. Pulsamos el botón Agregar de la sección Dominios en los que se confía. Aparece el cuadro de diálogo Agregar dominio en el que confiar.




**Introducimos el DominioB y la contraseña que se ha creado en el DominioB. Si todo funciona correctamente un mensaje en pantalla nos informará de que la relación de confianza se ha establecido.**

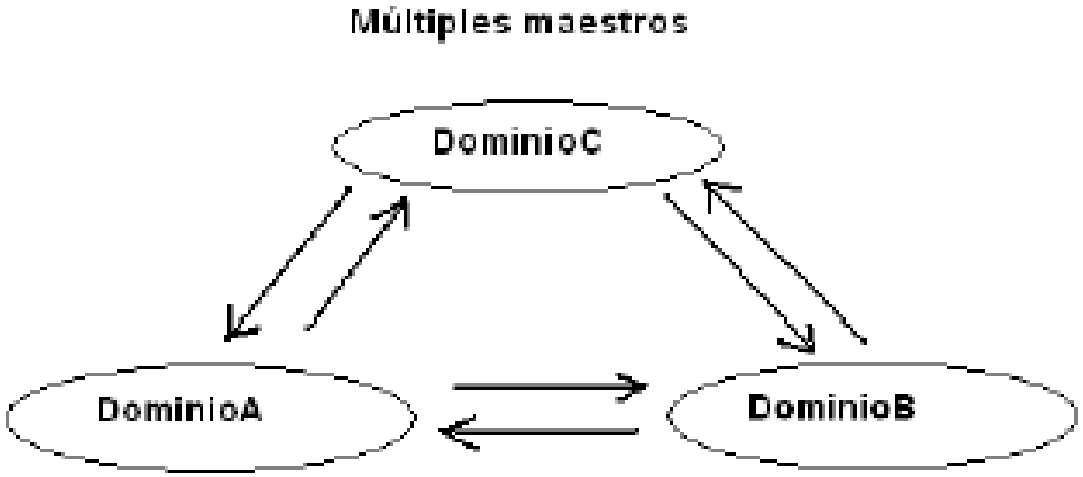
# Relaciones de confianza

- Mediante las relaciones de confianza se pueden establecer configuraciones para múltiples dominios:
  - **Configuración con un solo maestro**. En esta configuración los dominios subordinados pueden consultar la base de datos de usuarios del maestro, pero no al revés.



# Relaciones de confianza

- Mediante las relaciones de confianza se pueden establecer configuraciones para múltiples dominios:
  - **Configuración múltlipes maestro.** En esta configuración se establecen ambas relaciones de confianza entre todos los dominios. De esta manera las cuentas de cada dominio serían válidas en los demás.



# El modelo de seguridad

# Asegurando objetos Windows

- Objetos
  - memoria usuario y memoria nucleo
- Corazon modelo seguridad
  - Descriptores seguridad SD
  - Listas Control Acceso  ACL
- Todos los objetos son asegurables
  - archivos, unidades, conductos, procesos, hilos, temporizadores, impresorrar
  - cuentan con un SD adjunto

# Porciones seguridad del SD

- SID del objeto prioritario
- SID del grupo propietario principal
- La DACL
- La SACL

# Los SID

- Internamente W2K representa cada cuenta, grupo, maquina y dominio con un SID
- SID es independiente del numero de cuenta
- SID estructura numerica longitud variable, compuesta por
  - Nivel revision SID de 8 bits
  - Cuenta 8 bits subautoridades presentes
  - 48 bits hasta tres SID autoridad identificador
  - identificadores relativos RID

# ACL

# Tipos ACE

| Tipo | Hace a la ACL de tipo |
|---|---|
| ACCESS_ALLOWED_ACE | DACL |
| ACCESS_DENIED_ACE | DACL |
| ACCESS_ALARM_ACE* | SACL |
| ACCESS_AUDIT_ACE | SACL |

* no soportado en Windows 2000

# NTFS

El sistema de archivos de Windows NT

# NTFS

- Sistema de archivos estándar de Windows NT y de sus descendientes
  - 2000, 2003 y XP
- Versiones 9x (MS-DOS, W95, W98 y WME) no pueden leer este sistema de archivos de manera predeterminada
  - existen utilidades para salvar esta carencia.
- Tres versiones de NTFS:
  - v1.2 en NT 3.51 y NT 4 (v4.0)
  - v3.0 en Windows 2000 (v5.0)
  - v3.1 en Windows XP y Windows 2003 Server (v5.1)

# Mejoras con respecto a FAT

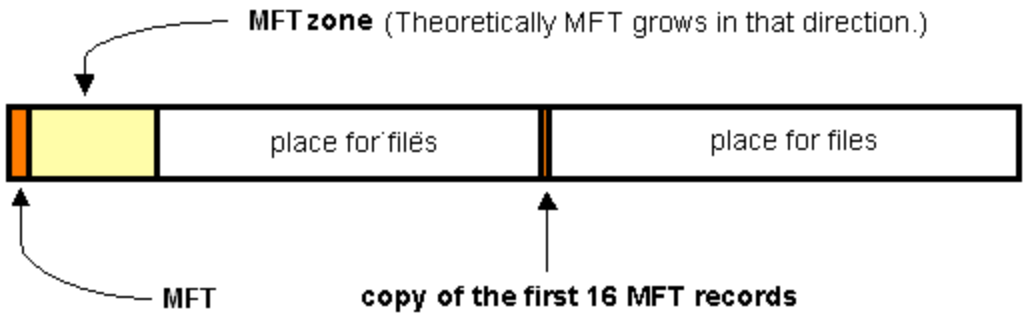
- Compatibilidad mejorada con metadatos
- Uso de estructura de datos avanzadas (árboles-B) para optimizar el rendimiento, estabilidad, y el aprovechamiento del espacio en disco,
- Listas de control de acceso
- Registro de transacciones (journaling).
- Seguridad a nivel de archivo y carpeta

# Tamaño partición y cluster

| Rango tamaño partición (GiB) | Número de sectores por cluster por default | Tamaño por default del cluster |
|---|---|---|
| <= 0.5 | 1 | 0.5 |
| >0.5 a 1.0 | 2 | 1 |
| >1.0 a 2.0 | 4 | 2 |
| >2.0 a 4.0 | 8 | 4 |
| > 4.0 a 8.0 | 16 | 8 |
| > 8.0 a 16.0 | 32 | 16 |
| > 16.0 a 32.0 | 64 | 32 |
| > 32.0 | 128 | 64 |

# Estructura de una partición

- Espacio dividido en clusters
- Disco NTFS esta simbolicamente dividido en dos partes
  - Primera parte (12%) asignado al área MFT
    - Master File Table
    - no es posible grabar información en este espacio
  - Segunda parte (88%) espacio para archivos
    - todo tipo de información, inclusive info de MFT



# Meta-archivos

| Archivo | Función |
|---|---|
| $MFT | el MFT en sí |
| $MFTmirr | copia de los primeros 16 registros del MFT |
| $LogFile | archivo de soporte de bitácoras |
| $Volume | información del volumen, nombre, versión sistema archivos, etc |
| $AttrDef | lista de los atributos estandar de los archivos |
| $. | directorio raíz |
| $Bitmap | bitmap de espacio libre |
| $Boot | sector de booteo (partición booteable) |
| $Quota | archivo donde los derechos de los usuarios sobre el uso del espacio en disco se almacenan (empieza a funcionar en la v5) |
| $Upcase | tabla de correspondencia entre las letras minúsculas y mayúsculas |

# Windows 2000

Lo nuevo, lo malo y lo feo…

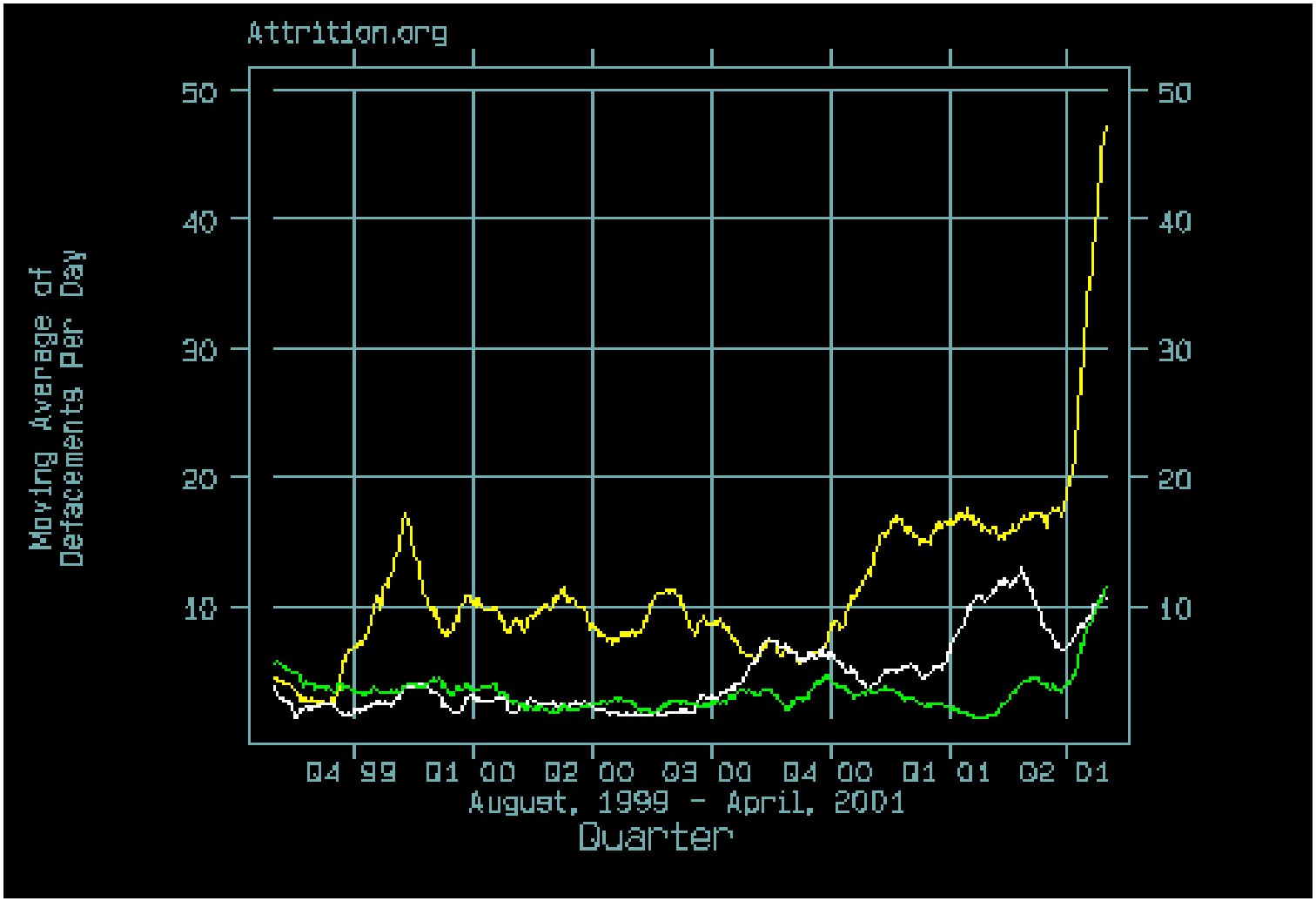
# Windows 2000
# Alias NT 5.0

- La familia 2K y Me son el siguiente paso de la estrategia de MS para terminar la migración de 16/32 bits a familias nativas de 32 bits.
  - 9* eran parches para terminar de pasar a 32 bits.
  - NT 4.0 fue convirtiéndose en un sistema más confiable, pero no es muy amigable.
    - No USB
    - No Plug and Play
    - Dificil de configurar.

# Windows 2000

- Conserva gran parte de la arquitectura de NT 4.0
- Agrega muchos elementos nuevos de seguridad.
- Pero…

# Estadística de Ataques a Websites
# Ago 1999 – Abr 2001




NT:

Yellow

Linux:

White

Others:

Green

# Windows 2000

- La llegada ha sido dolorosa.
- Demasiados Service packs y hot fixes liberados.
- Recuerden: W2K es la pieza de software más compleja liberada en toda la historia del SW comercial.
  - BUGS!!!
  - Problemas de diseño
  - Problemas de implementación

# Windows 2000: Novedades de Seguridad

- Active Directory y Autenticación
- Kerberos V5.0
- PKI
- Encrypting File System (EFS).
- IPSec

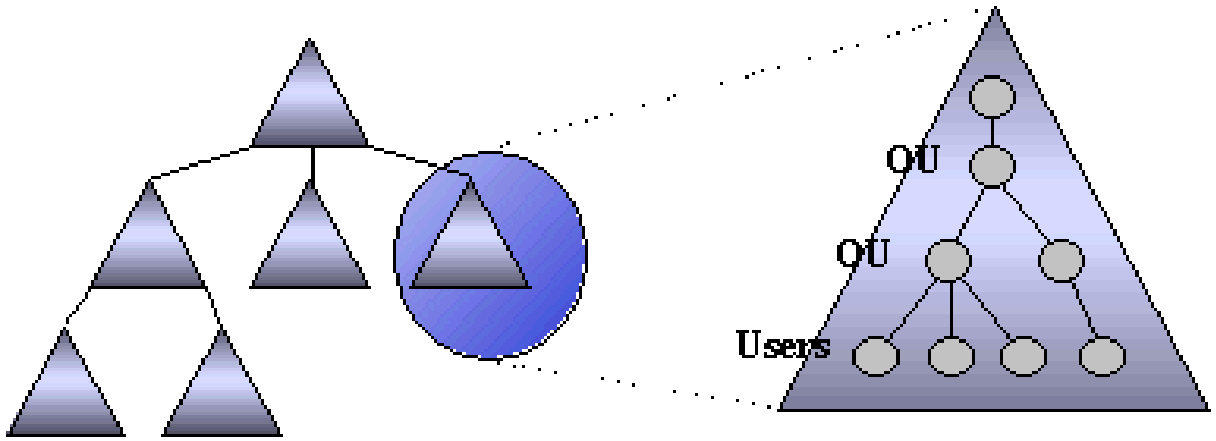
# WIN2K
# Control de Acceso

- En la instalación de facto, los controles son más astringentes.
- El grupo everyone ya no es forzoso como contenedor.
- Los usuarios pertenecen solo a grupos donde el administrador tiene control sobre sus permisos, con grano mas fino.

# Seguridad Distribuida: Active Directory

## Domain Hierarchy: *Domain Tree*

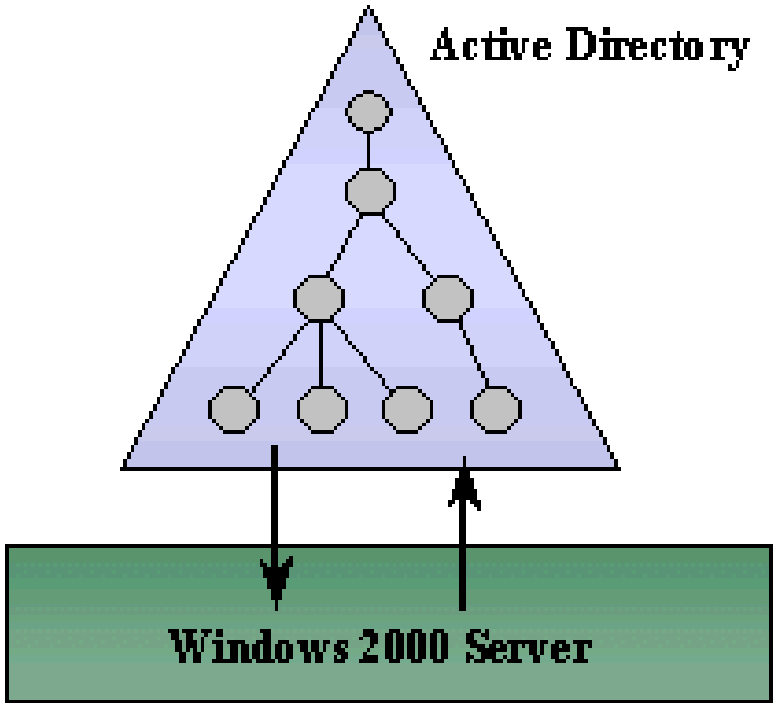
- Organizational Unit (OU) hierarchy within a Domain
  - Users, Groups, Machines, Printers, etc.



# Seguridad Distribuida: Active Directory

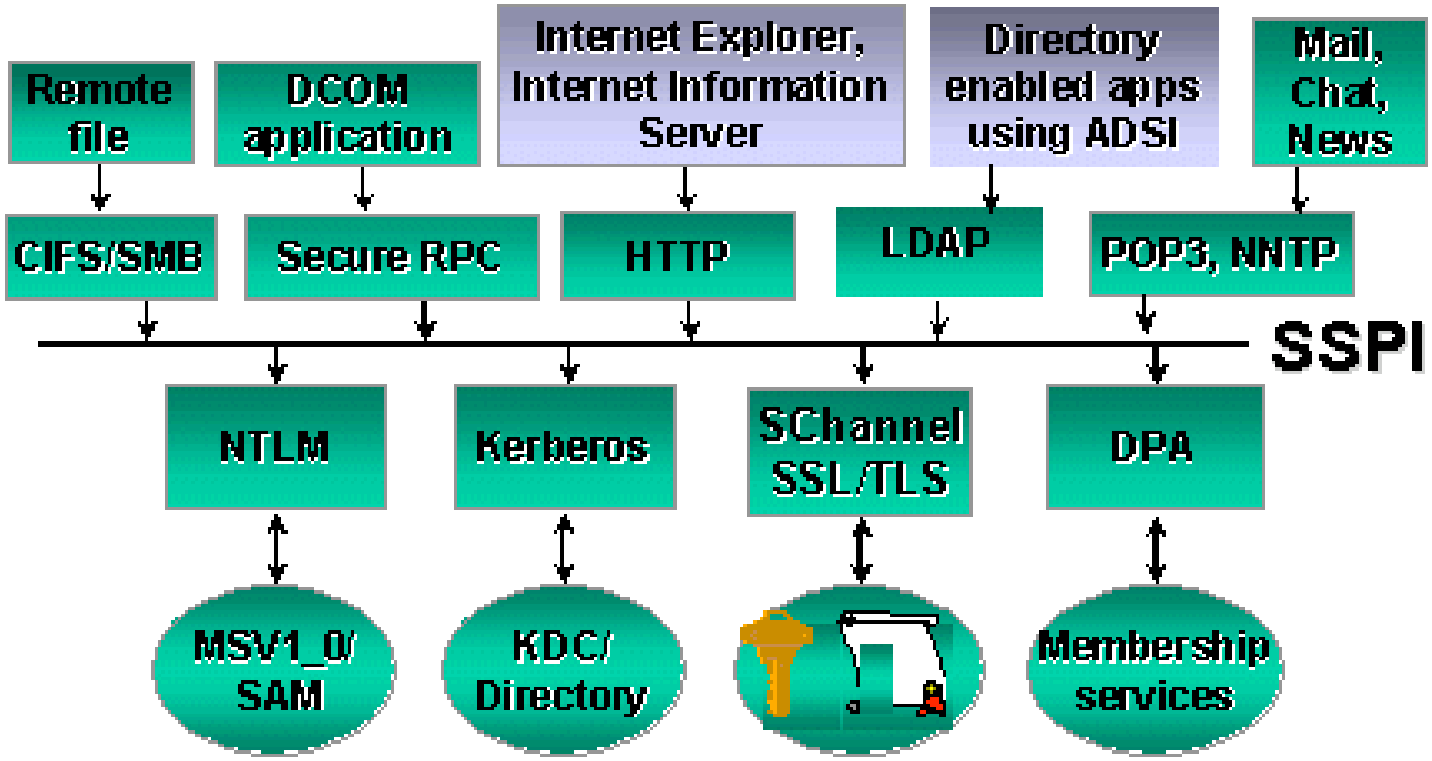
## Directory and Security Services

- Active Directory
  - Stores security policy and account information
- Operating system
  - Implements security model on all objects
  - Trusts information stored securely in the directory

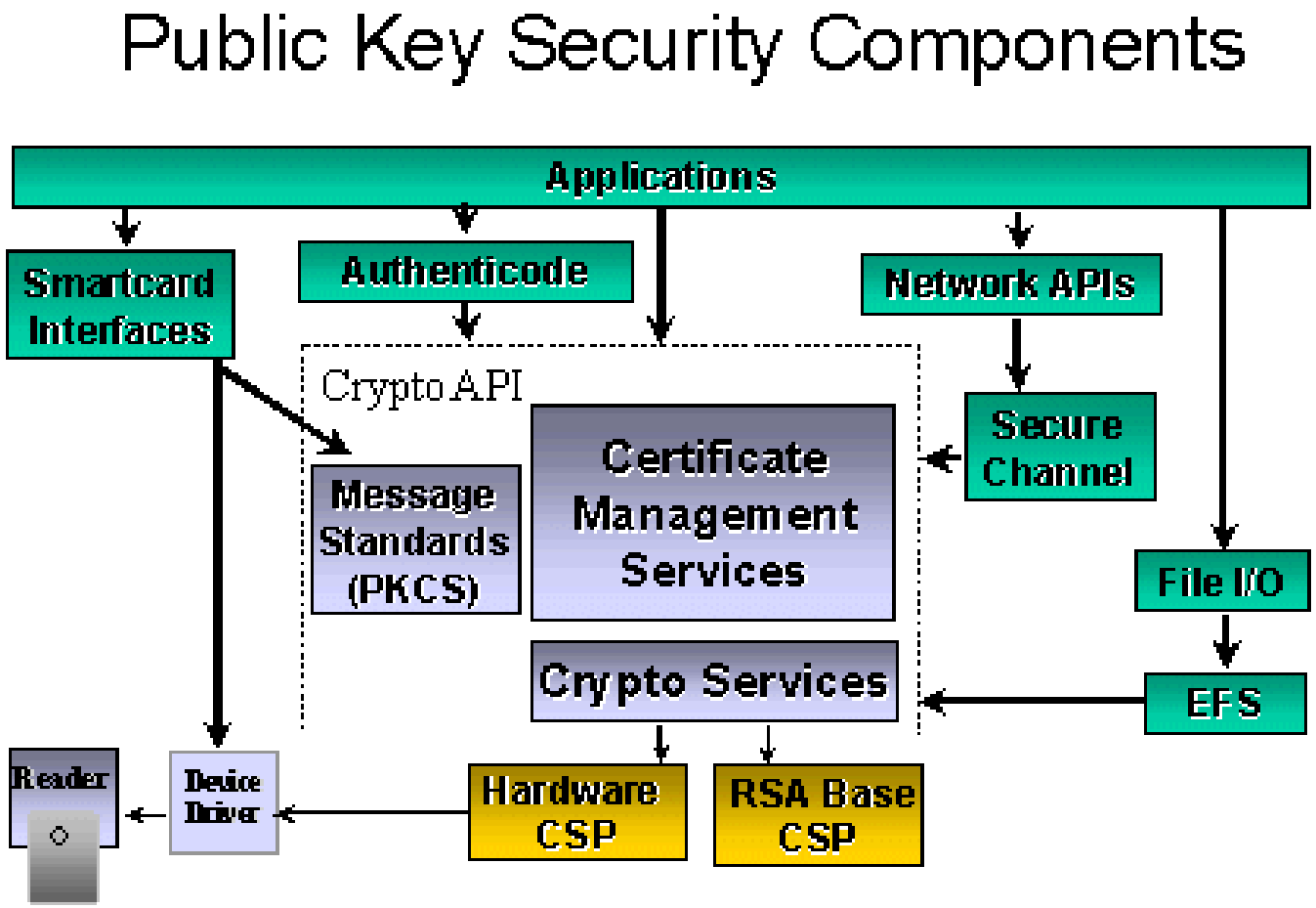


# Seguridad Distribuida: Active Directory

## Architecture For Multiple Authentication Services



# Seguridad Distribuida: Active Directory



# Windows XP

- NT 5.1?
- Más campanas y lucesitas
  - Nueva interfaz (GUI)
  - IE 6
  - Nuevas tecnologías de MS (DirectX, Media player, etc.
- Multimedia
- Mejoras de seguridad
  - Deja vu?
- Mejoras en la estabilidad del sistema
- Boot más rápido.

# Windows XP

- Mejoras de Seguridad
  - EFS (uso)
  - Internet Firewall Connection
  - SmartCards, Biométricos y Wireless
    - SP2
  - Raw Sockets
    - Admin por default en instalación
  - .NET
    - CLR

# Comentarios Windows XP

- Buena actualización
- Persisten problemas
  - Instalación de facto insegura
  - Tecnologías de MS inseguras
  - VIRUS
- Altas expectativas del SP2, sobre todo en la parte de seguridad

# Windows 2003 Server

- Windows Server 2003 Web Edition
- Windows Server 2003 Standard Edition
- Windows Server 2003 Enterprise Edition
- Windows Server 2003 Datacenter Edition
- Referencia
  - http://www.microsoft.com/windowsserver2003/evaluation/features/compareeditions.mspx

# Familia de Servidores

# Familia de Servidores

- Windows Server 2003, Standard Edition
  - para las necesidades diarias de empresas de cualquier tamaño, ofrece una solución para compartir archivos e impresoras, garantizar la seguridad de la conexión a Internet, posibilitar un desarrollo centralizado de aplicaciones de escritorio y una colaboración fructífera entre empleados, socios y clientes

- Windows Server 2003, Enterprise Edition
  - para empresas de tamaño medio o grande, permite disponer de infraestructura comercial, aplicaciones de unidad de negocio y transacciones de comercio electrónico

# Familia de Servidores

# Familia de Servidores

- Windows Server 2003, Web Edition
  - para servicios y  hospedaje Web, ofrece una plataforma para desarrollar e implementar rápidamente servicios y aplicaciones Web tres capas.
  - IIS6.0, ASP.Net, XML
- Windows Server 2003, Datacenter Edition
  - para aplicaciones empresariales y críticas que requieran procesos de transacciones de gran volumen, y niveles altos de escalabilidad y disponibilidad

# Clientes Windows

- Cliente ideal → XP Professional
  - Características de instalación automática y configuración controldada por Windows Server 2003
  - Documentos, parámetros personales de usuarios pueden almacenarse o replicarse en servidores
    - **acceso**: desde cualauier máquina de red
    - **disponibilidad**: aún fuera de línea
    - **Mejor protección**: Todos los archivos residen en el servidor

- *Un **cliente** es una computadora que tiene acceso a los recursos de otra*

# Windows 2003 Server

- Iniciativa $SD^3+C$
  - Secure by design
    - Secure Architecture
    - Security features
    - Reducción de vulnerabilidades existentes y nuevas en el código antes del embarque del producto
  - Secure by default
    - Minimizar la superficie de contacto a ataques
  - Secure in deployment and Communications
    - Protección, detección y defensa de sistemas
    - Recuperación de sistemas atacados
    - Administración y coordinación de las tareas anteriores
    - Diseminación veloz de parches

# Mejoras de Seguridad

- Forest trust
- Administrador de credenciales
- Limitación en la impersonación
- Protocol Transition (Kerberos)
- .Net Passport integrado a Active Directory
- RBAC
- Control de acceso basado en URL
- Cuarentena