

# Sistema Operativo Windows

Roberto Gómez Cárdenas

rogomez@itesm.mx

Lámina 1

<http://www.aci.com.pl/mwchary/guidebook/interfaces/windows/win31/win31>

Roberto Gómez C.

# Un poco de historia...

[13]

Lámina 2

[www.fortunecity.com/marina/reach/435/micro.htm](http://www.fortunecity.com/marina/reach/435/micro.htm)

Roberto Gómez C.



## Los personajes



---



Gary A. Kildall



CP/M  
GUÍA DO USUÁRIO



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 Jobs and Steve Wozniak in their garage, ca. 1975. Photo courtesy of Apple Computer.




William C. "Bill" Lowe




Steve Jobs y Steve Jobs

Lámina 3 Roberto Gómez C.



## 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

Lámina 4 Roberto Gómez C.



<div>  <div>Características versiones (1)</div>  </div>					
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 3.11 nov 93
DOS en desarrollo	DOS en desarrollo	múltiples máquinas virtuales DOS	direccionar más alla de 640 Kb	OLE 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				

Lámina 5 Roberto Gómez C.



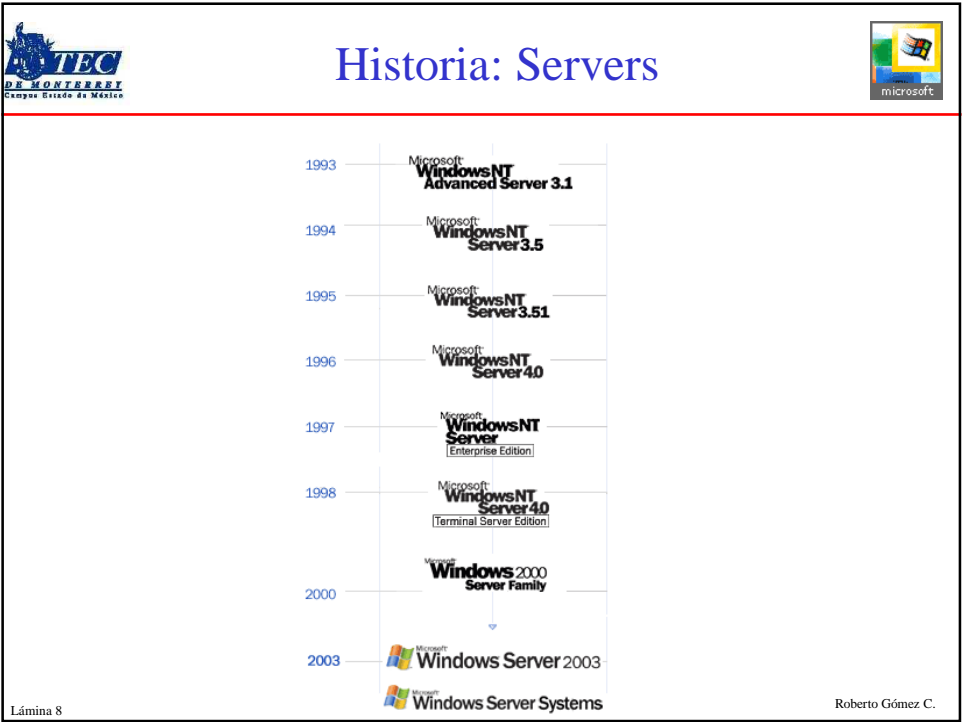
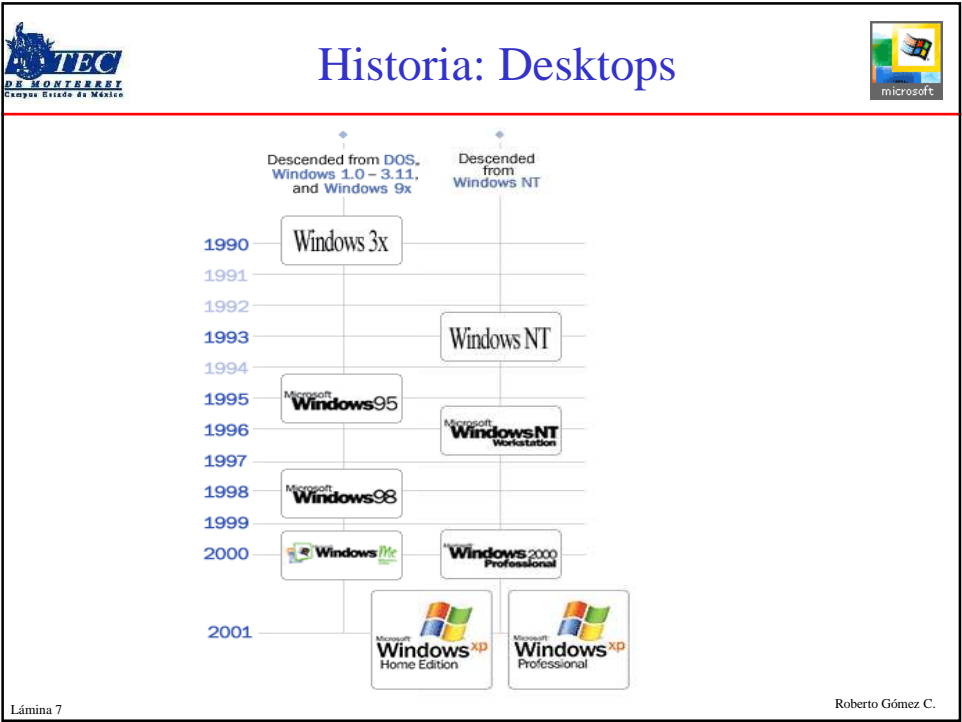


<div>  <div>Características versiones (2)</div>  </div>					
Win 95	Win 98	Win 32S	Win NT 3.1	Win NT 3.5	Win NT 4.0
4 ago 95	junio 1998 SE: may 1999	feb 1996	julio 1993	sep 1994	ago 1996
Deja de ser solo un interfaz	soporte FAT 32	conjunto librería para win 3.1	New Technology Sist. Archivos: FAT, NTFS 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 o 4G en RAM		
stack TCP/IP integrado al núcleo	Internet Explores 5.0 y Net Meeting 3.0		versión servidor y estación trabajo		

Lámina 6 Roberto Gómez C.







## 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

Lámina 9

Roberto Gómez C.




## 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**

Lámina 10

Roberto Gómez C.




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 similitudes entre VMS y WNT

Lámina 11

Roberto Gómez C.





El Trato



- A cambio de no demandar, DEC recibió:
  - Entrenamiento especializado para sus ingenieros.
  - Mercadotecnia para presentar 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

Lámina 12



Roberto Gómez C.



## 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.



Lámina 13 Roberto Gómez C.



## 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.



Lámina 14 Roberto Gómez C.



## Windows NT

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

Lámina 15 Roberto Gómez C.




## 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)

Lámina 16 Roberto Gómez C.






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.

Lámina 17

Roberto Gómez C.





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

Lámina 18



Roberto Gómez C.



## 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.



Lámina 19 Roberto Gómez C.



## 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

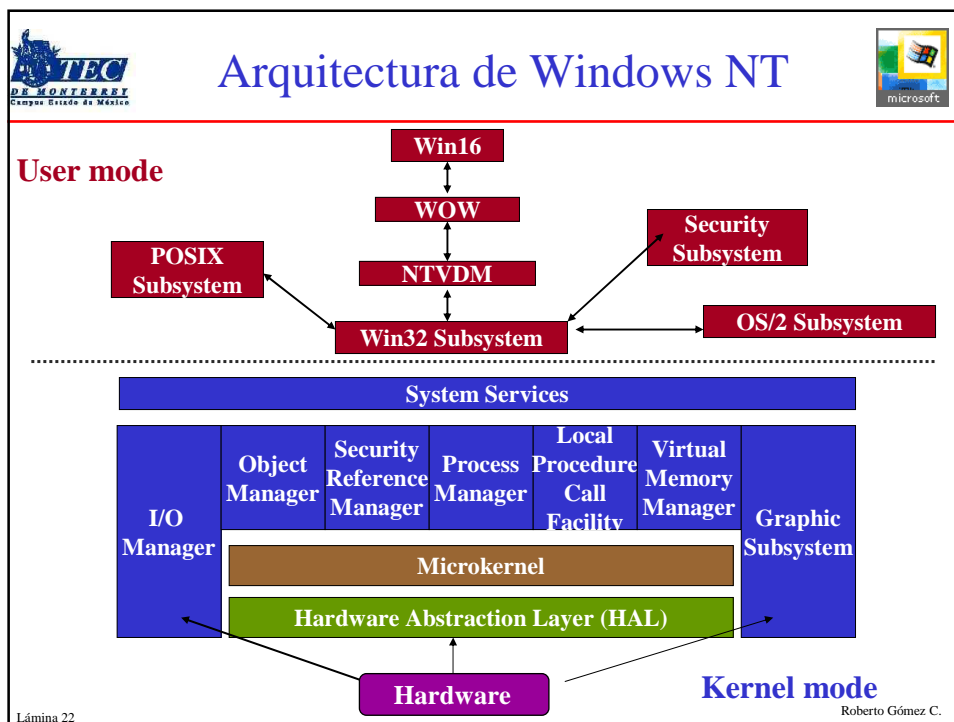
Lámina 20 Roberto Gómez C.

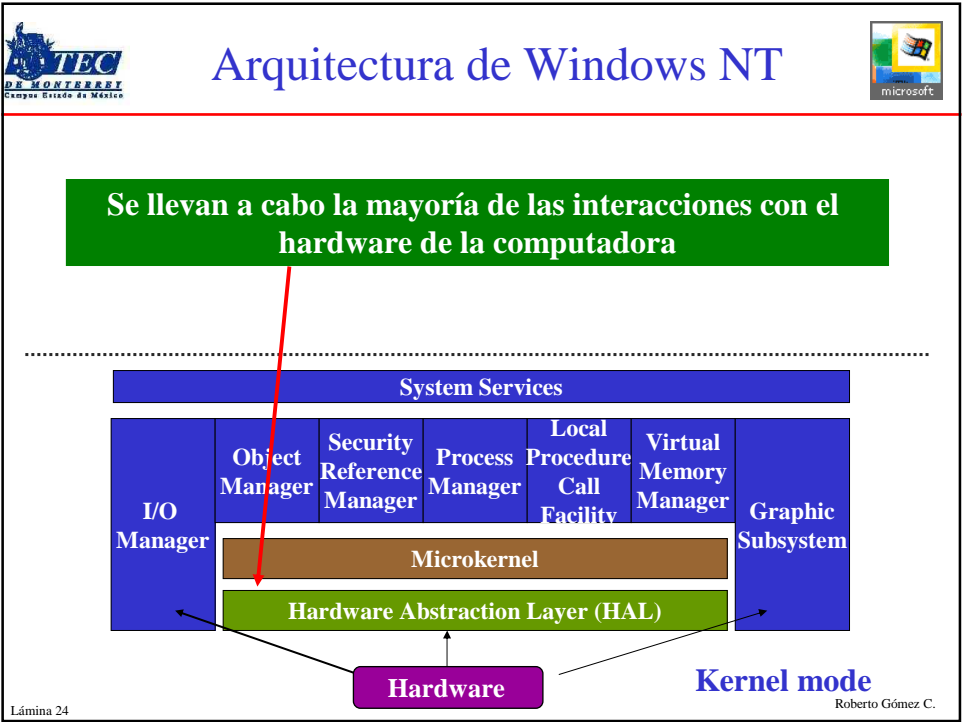
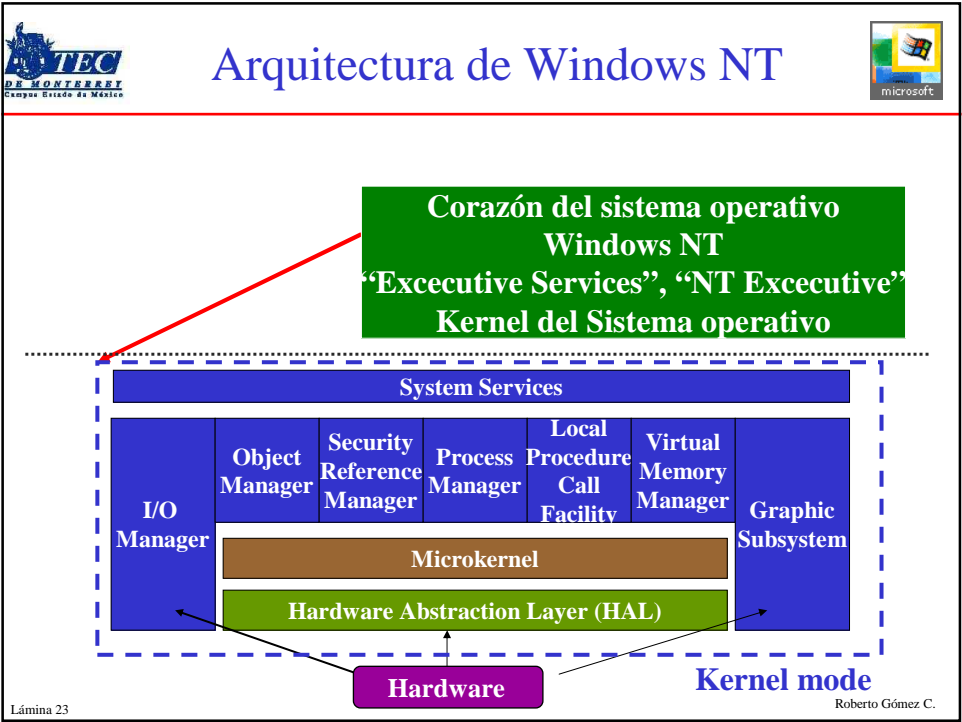


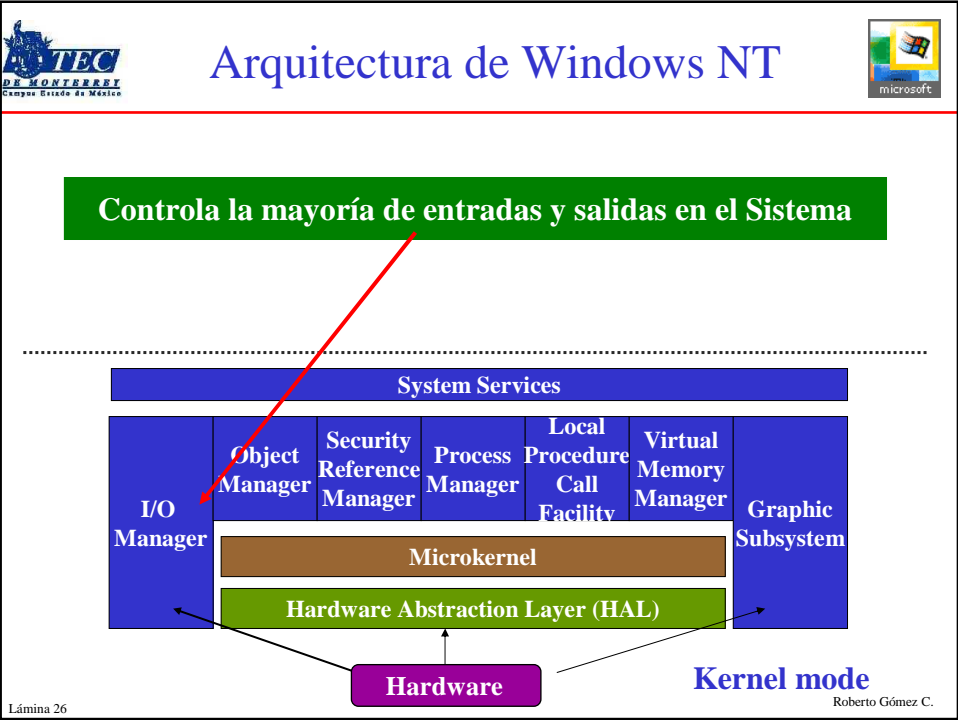
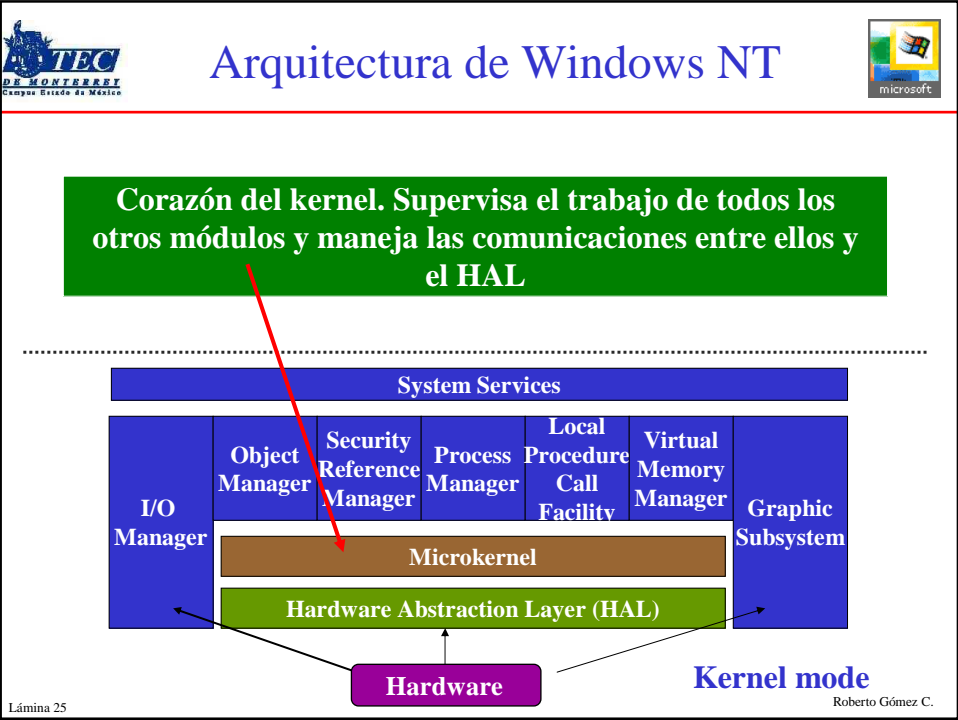
## Modos de ejecución

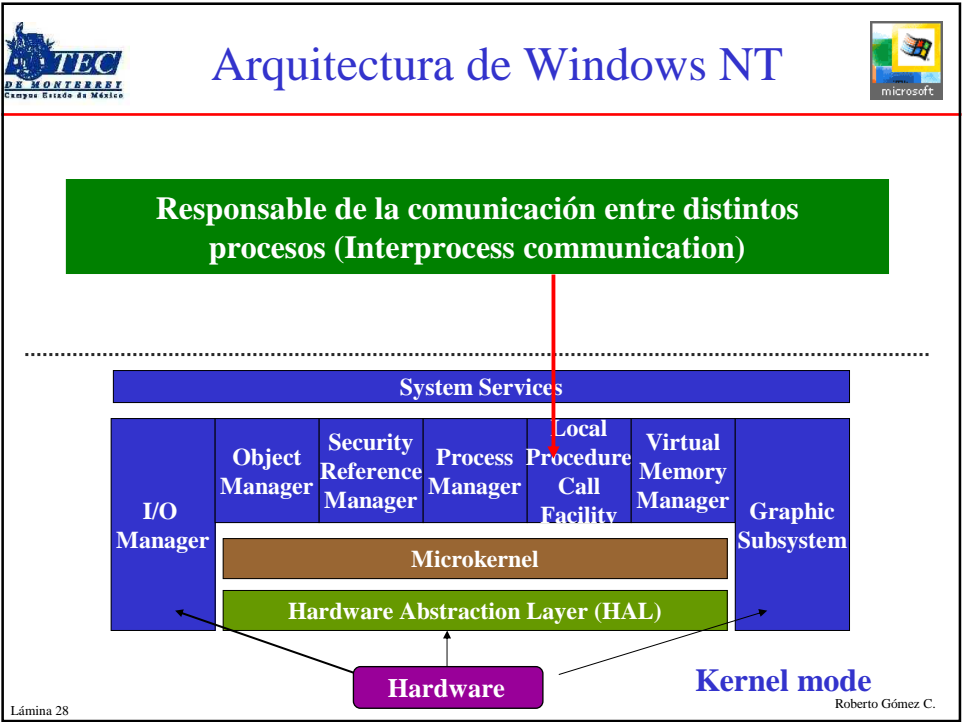
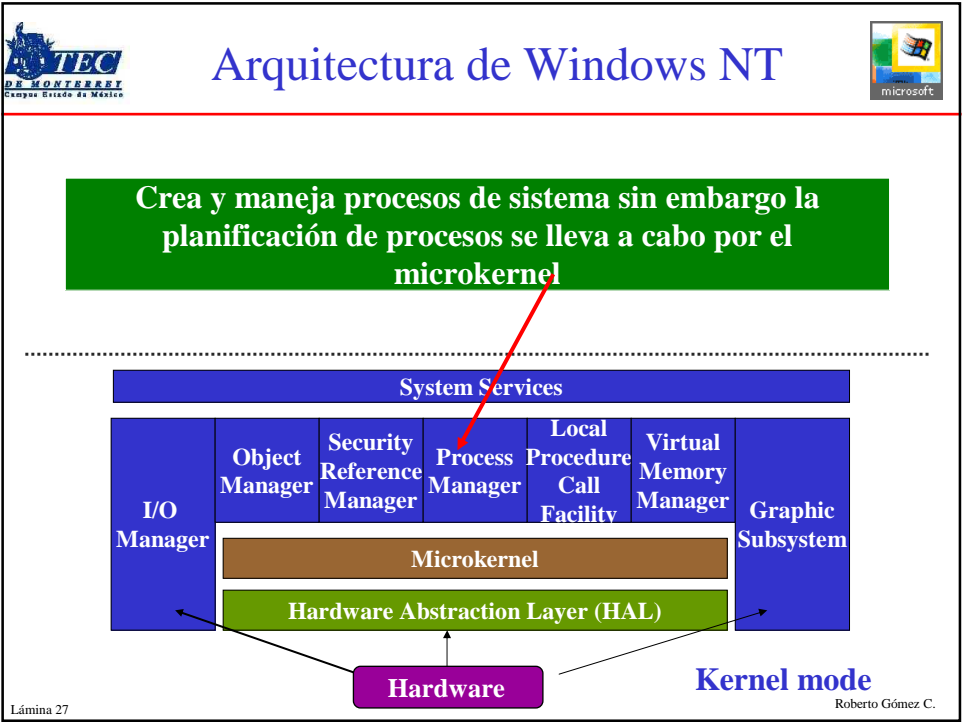
- Modo kernel.
  - Modo privilegiado
  - Acceso completo a todos los recursos del sistema
  - Acceso a toda la memoria

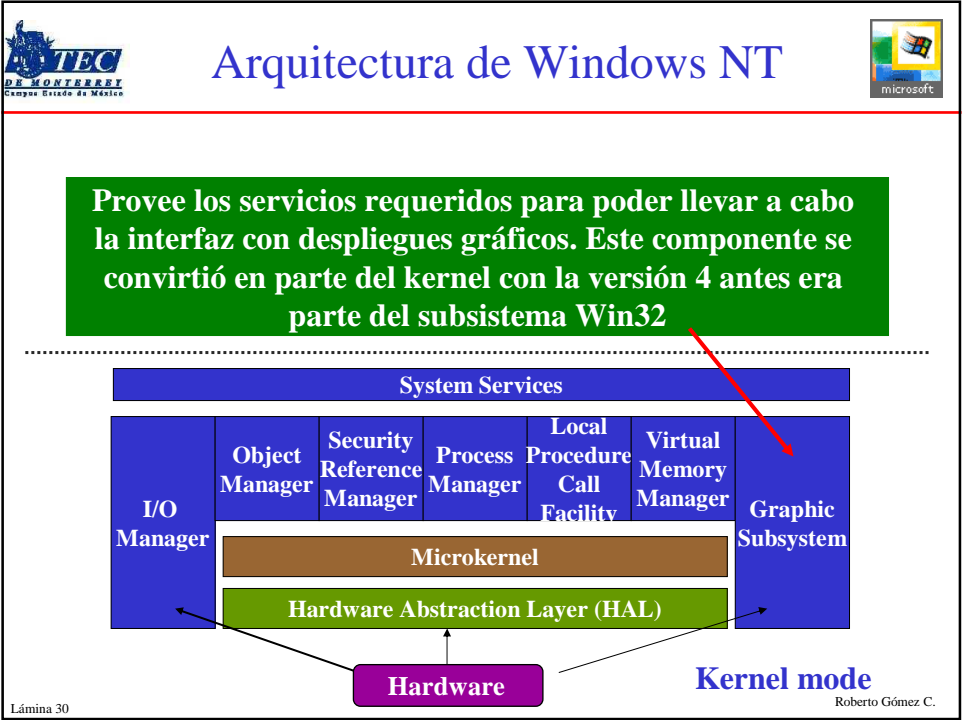
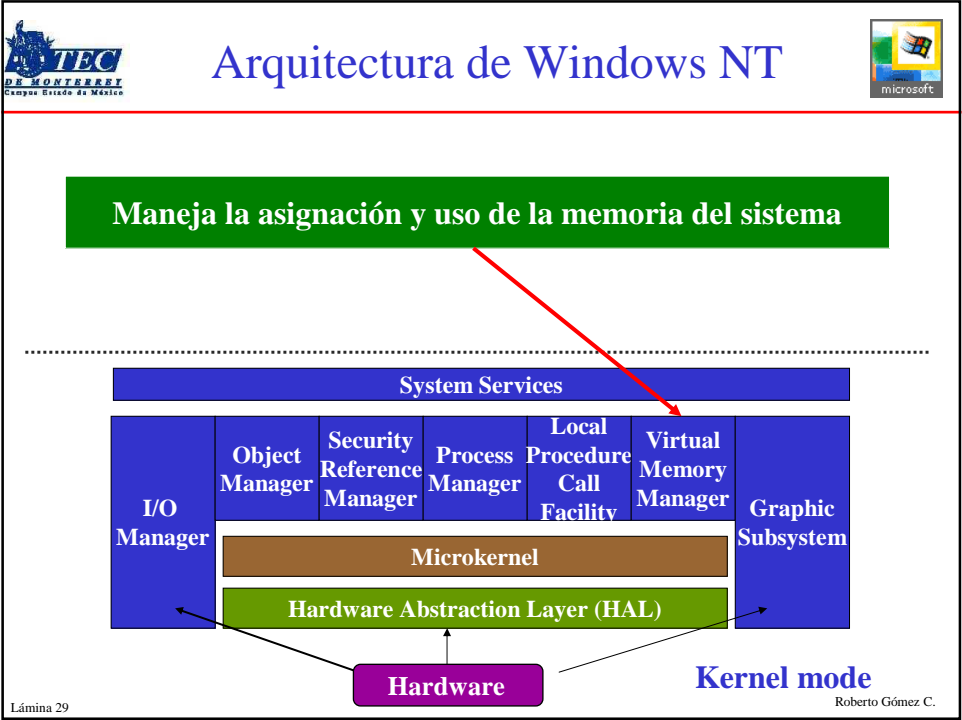
Lámina 21 Roberto Gómez C.

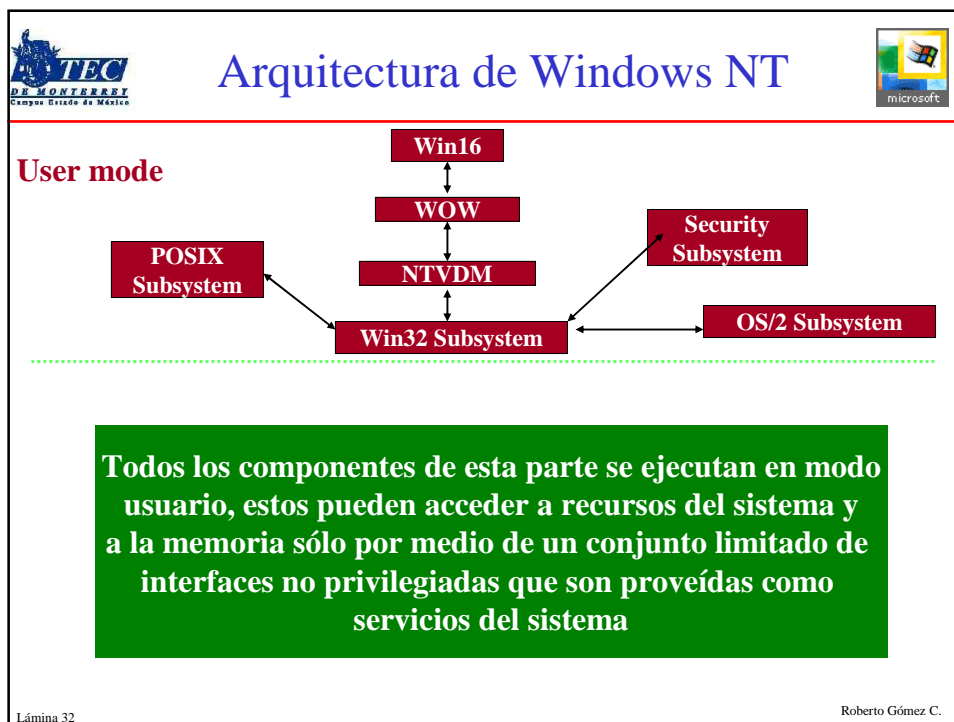
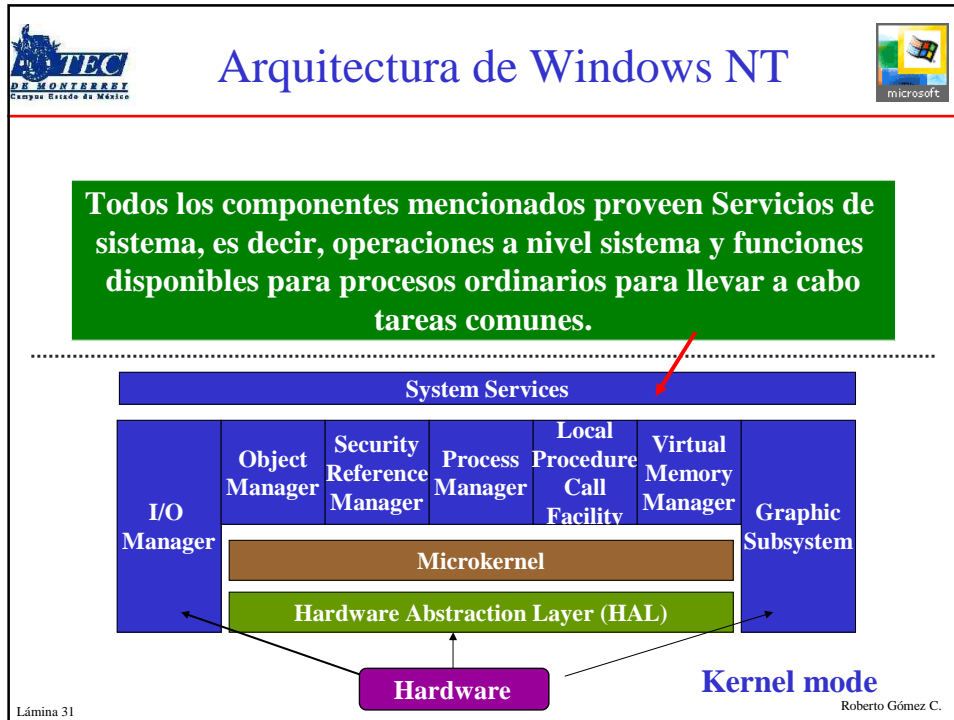




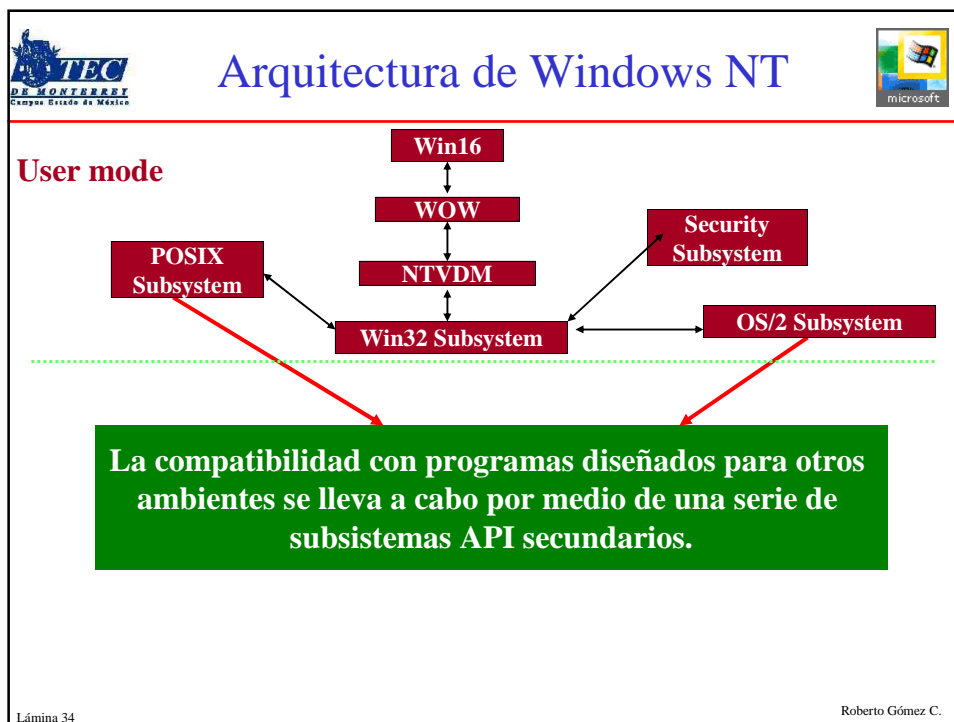
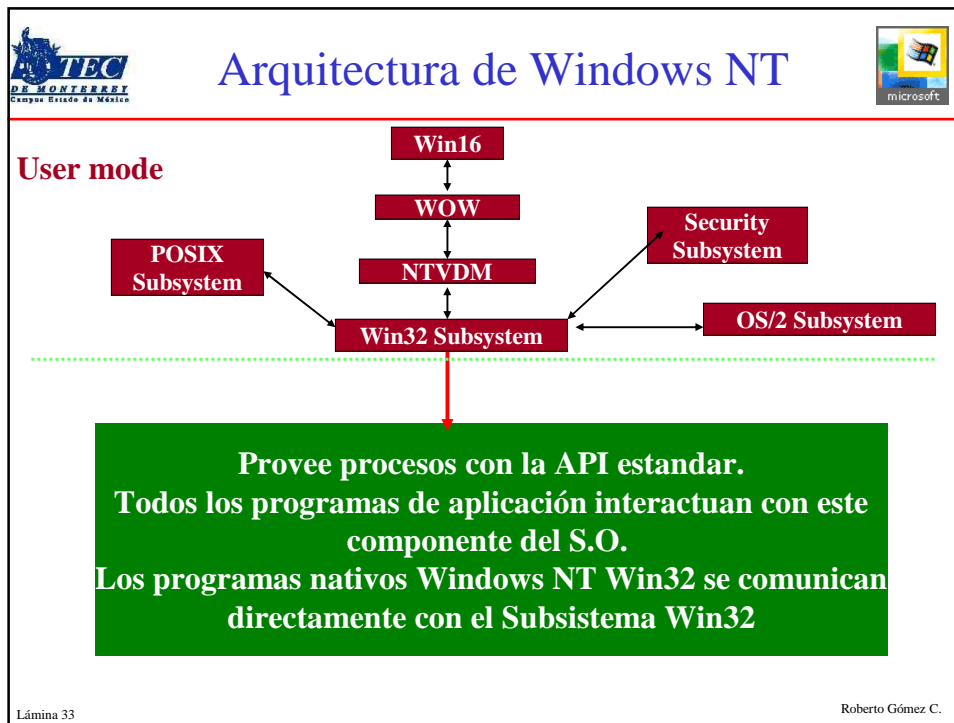


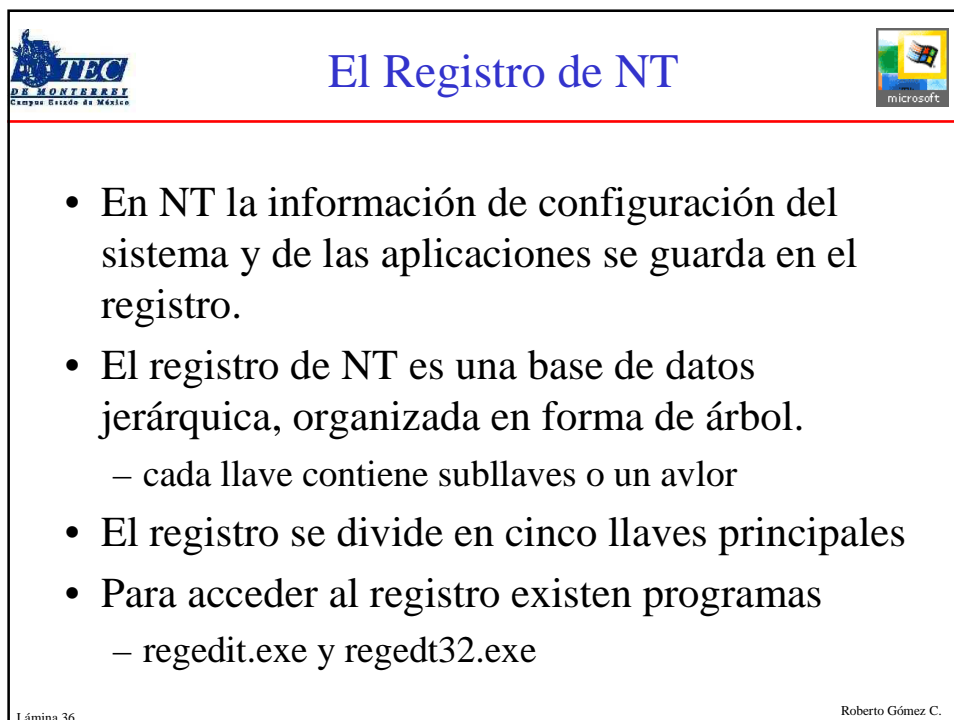
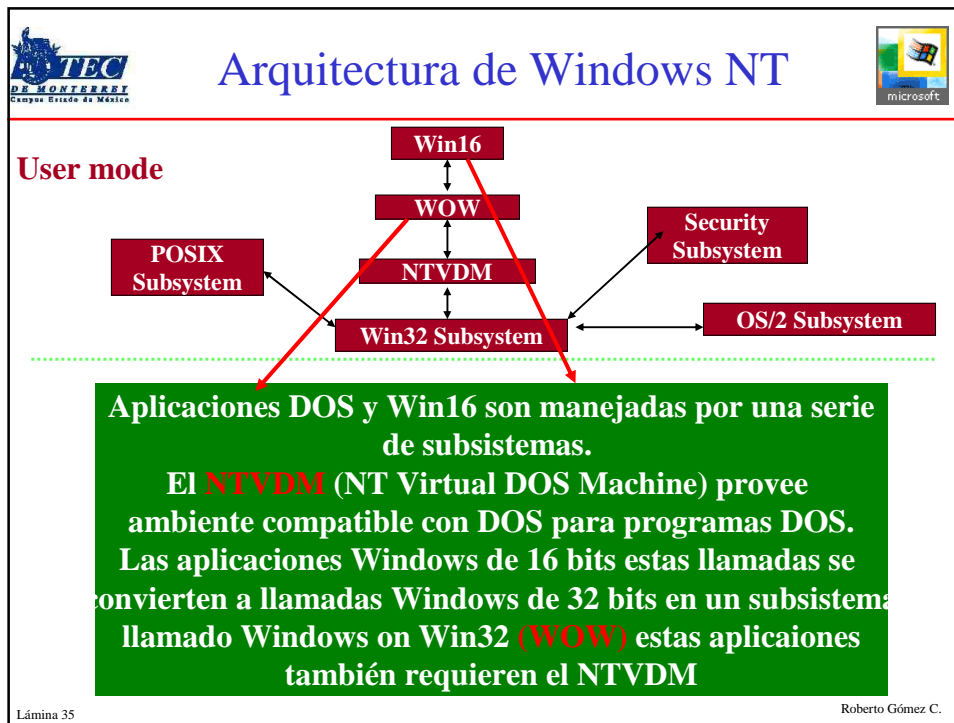

















Principales claves (hives)




- **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

Lámina 37

Roberto Gómez C.




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

Lámina 38

Roberto Gómez C.




## 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

Lámina 39
Roberto Gómez C.




## 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.

Lámina 40
Roberto Gómez C.




## 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 subclave 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.

Lámina 41
Roberto Gómez C.




## 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

Lámina 42
Roberto Gómez C.




## 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

Lámina 43

Roberto Gómez C.



## Registros, editor y archivos



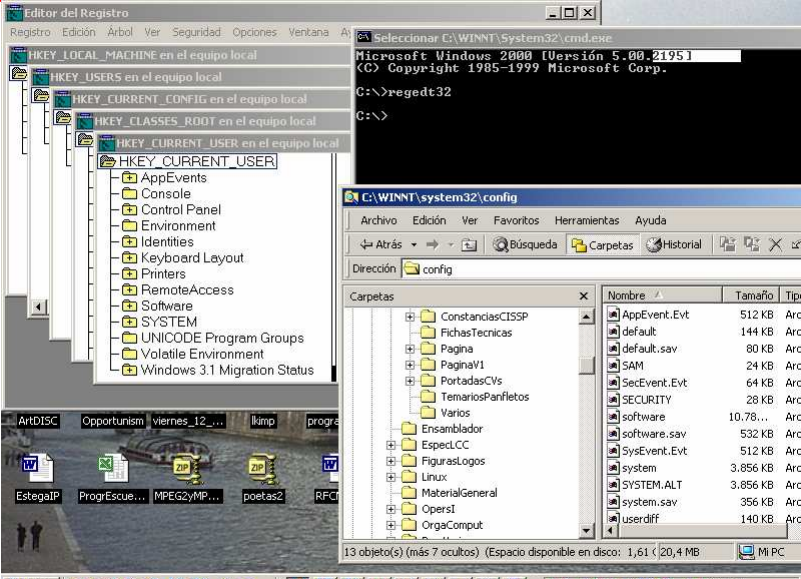




Lámina 44

Gómez C.



## 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

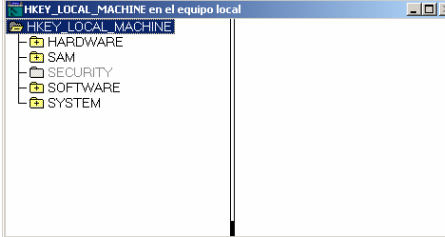




Lámina 45 Roberto Gómez C.





## Subclaves HKEY\_LOCAL\_MACHINE



- **SECURITY**
  - incluye los derechos de los usuarios en la máquina, política de seguridad en cuanto 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



Lámina 46 Roberto Gómez C.



## 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.

Lámina 47 Roberto Gómez C.




## 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

Lámina 48 Roberto Gómez C.





## 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

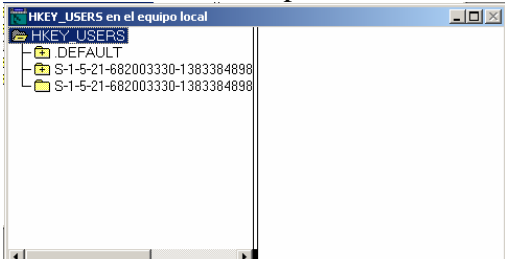




Lámina 49 Roberto Gómez C.



## 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






Lámina 50 Roberto Gómez C.




## 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

Lámina 51 Roberto Gómez C.



## Ejemplo HKEY\_CLASSES\_ROOT



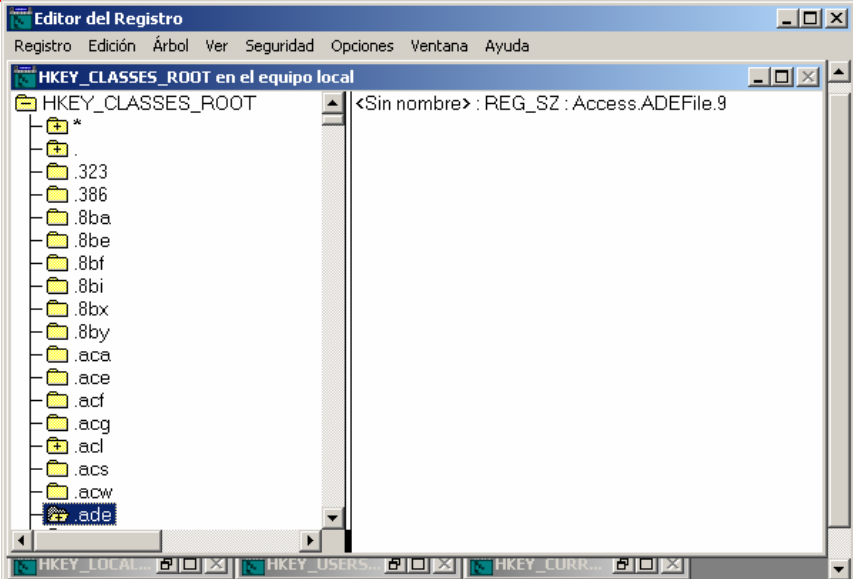






Lámina 52 Roberto Gómez C.



## 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 almacenados en la clave HKEY\_USERS para el usuario que haya iniciado la sesión.

Lámina 53 Roberto Gómez C.



## Ejemplo HKEY\_CURRENT\_USER

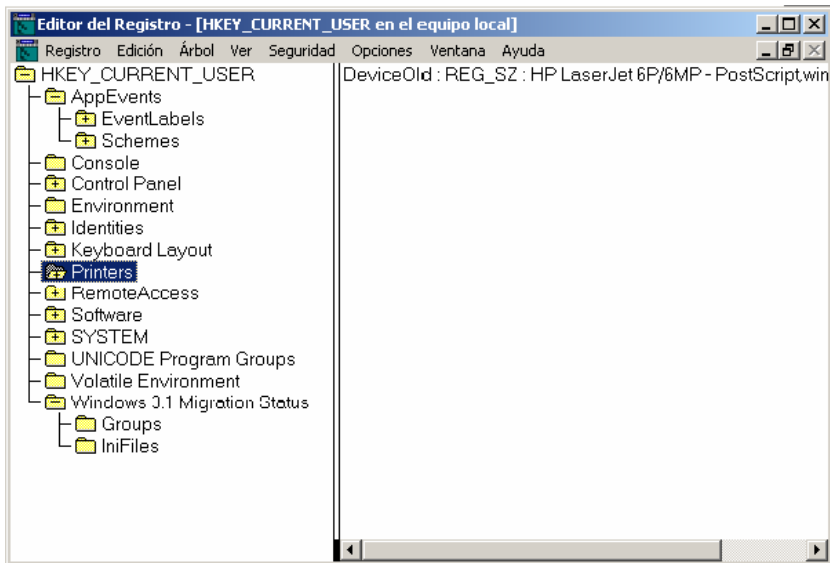






Lámina 54 Roberto Gómez C.



## Dominios NT

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



Lámina 55 Roberto Gómez C.



## Elementos de un dominio

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



Lámina 56 Roberto Gómez C.



## 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



Lámina 57 Roberto Gómez C.



## 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

Lámina 58 Roberto Gómez C.





## Estaciones de trabajo

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

Lámina 59

Roberto Gómez C.





## 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`

Lámina 60

Roberto Gómez C.





## Los controladores del dominio

- 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.

Lámina 61

Roberto Gómez C.





## Los controladores del dominio

- 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.

Lámina 62

Roberto Gómez C.





## 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

Lámina 63

Roberto Gómez C.





## Las cuentas

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

Lámina 64

Roberto Gómez C.







## Tipos de cuentas

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

Lámina 65

Roberto Gómez C.





## 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 sistema para ejecutar programas, utilidades y controladores

Lámina 66

Roberto Gómez C.



## 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.

**Un solo maestro**

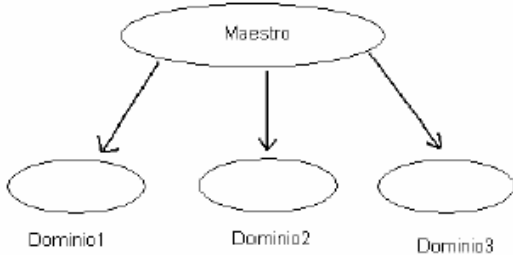




Lámina 67 Roberto Gómez C.



## Relaciones de confianza

- Mediante las relaciones de confianza se pueden establecer configuraciones para múltiples dominios:
  - Configuración múltiples 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.

**Múltiples maestros**

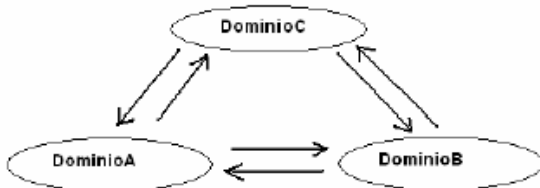




Lámina 68 Roberto Gómez C.





## Windows 2000

Lo nuevo, lo malo y lo feo...

Lámina 69

Roberto Gómez C.




## 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
    - Difícil de configurar.


Lámina 70

Roberto Gómez C.



TEC  
DE MONTERREY  
Campus Estado de México

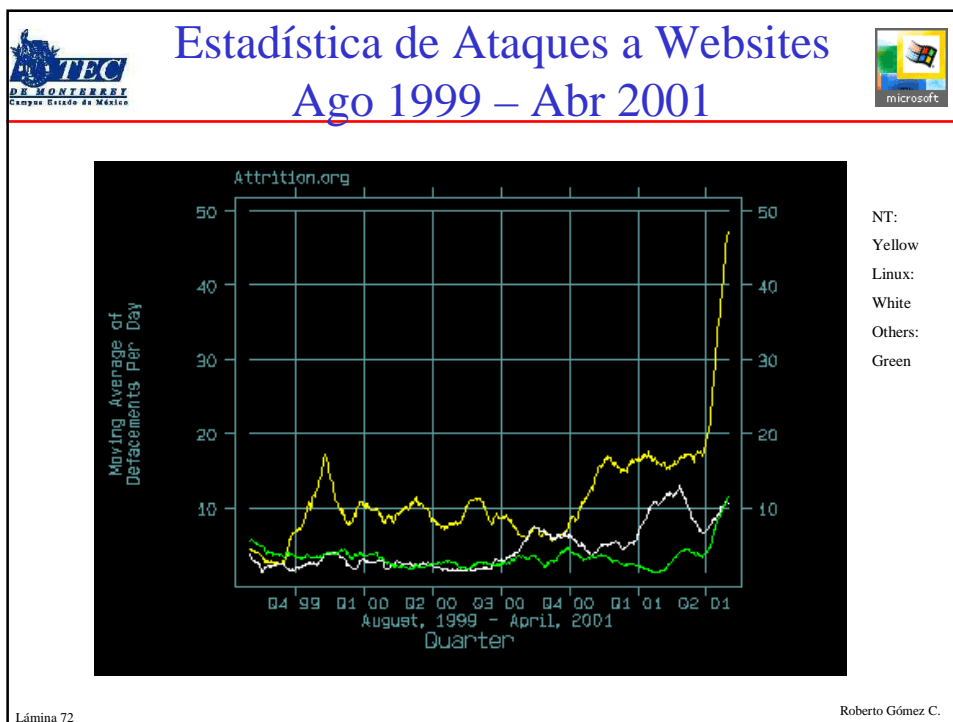
## Windows 2000





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

Lámina 71

Roberto Gómez C.







## 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


Lámina 73 Roberto Gómez C.




## Windows 2000: Novedades de Seguridad

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

Lámina 74 Roberto Gómez C.



## Seguridad Distribuida: Active Directory



---

### Domain Hierarchy: *Domain Tree*

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

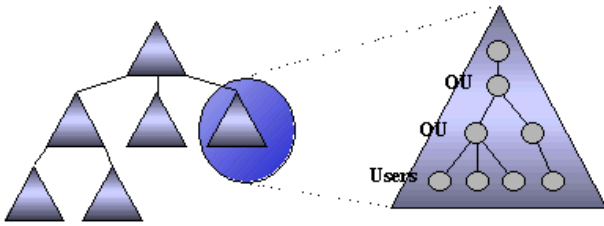




Lámina 75
Roberto Gómez C.



## Seguridad Distribuida: Active Directory



---

### Public Key Security Components

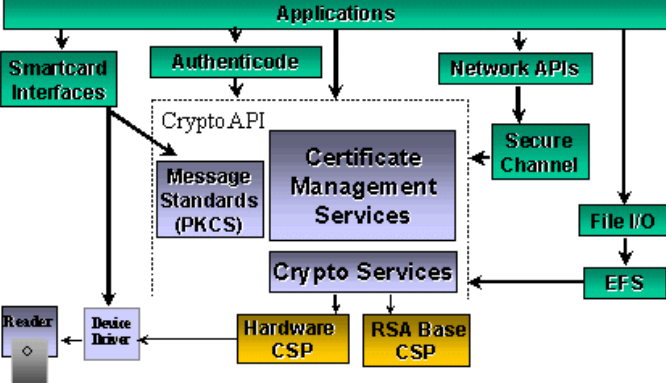




Lámina 76
Roberto Gómez C.




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.

Lámina 77

Roberto Gómez C.





Windows XP



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

Lámina 78



Roberto Gómez C.



## 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

Lámina 79 Roberto Gómez C.





## 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>

Lámina 80 Roberto Gómez C.







## 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



Lámina 81 Roberto Gómez C.



## 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



Lámina 82 Roberto Gómez C.



## Cientes Windows

- Cliente ideal → **XP Professional**
  - Características de instalación automática y configuración controlada por Windows Server 2003
  - Documentos, parámetros personales de usuarios pueden almacenarse o replicarse en servidores
    - **acceso**: desde cualquier 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*



Lámina 83 Roberto Gómez C.



## Windows 2003 Server

- Iniciativa SD<sup>3</sup>+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

Lámina 84 Roberto Gómez C.



## 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

Lámina 85

Roberto Gómez C.