Sistemas Operacionais

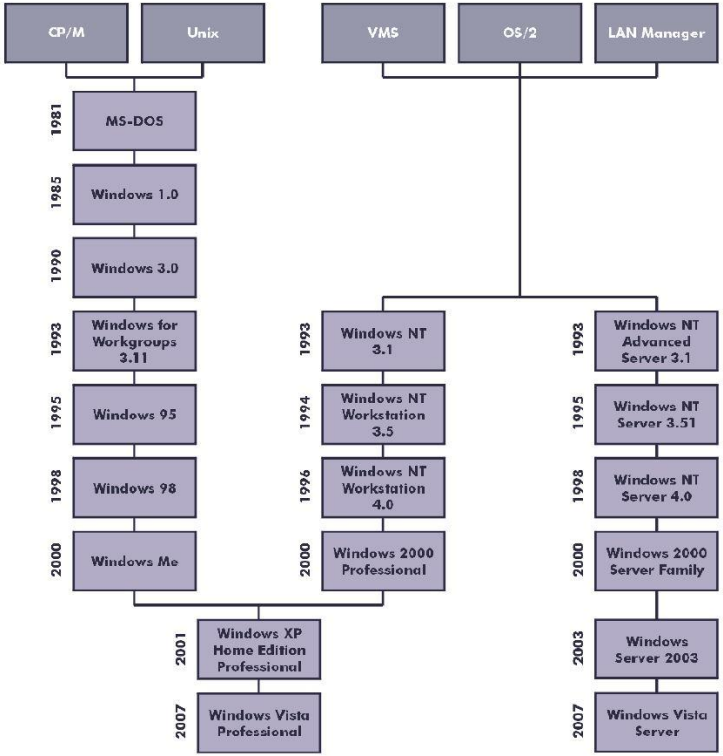
Estudo de Caso: Windows

Heli Henriques
Instituto Federal de Sergipe - IFS

História do Windows

Ano	MS-DOS	Windows baseado no MS-DOS	Windows baseado em NT	Windows moderno	Observações
1981	1.0				Distribuição inicial para IBM PC
1983	2.0				Suporte para PC/XT
1984	3.0				Suporte para PC/AT
1990		3.0			Dez milhões de cópias em 2 anos
1991	5.0				Incluído gerenciamento de memória
1992		3.1			Funcionava somente em 286 ou superior
1993			NT 3.1		
1995	7.0	95			MS-DOS embutido no Win 95
1996			NT 4.0		
1998		98			
2000	8.0	Me	2000		Win Me era inferior ao Win 98
2001			XP		Substituiu o Win 98
2006			Vista		Vista não conseguiu suplantar o XP
2009			7		Melhoria significativa sobre o Vista
2012				8	Primeira versão moderna
2013				8.1	Microsoft passou para lançamentos rápidos
2015				10	

História do Windows



MS-DOS

- Década de 1980
- Sistema criado pela IBM
- Microsoft Disk Operating System (MS-DOS)
- Características:
  - Sistema de 16 bits
  - Monousuário
  - Linha de Comando (Command Line Interface)
  - Computador Pessoal 8088 - 8 KB de Memória
  - Em 1986 – Intel 286 – 36 KB

MS-DOS-Based Windows

- Primeira Interface Gráfica (Windows 1.0 e 2.0)
- Base: MS-DOS
- Em 1990 - Windows 3.0: Ambiente Gráfico – Intel 386
- Em 1995 - Windows 95: SO mais completo (memória virtual, gerenciamento de processos e multiprogramação)
- Programação 32 bits
- Windows 98 e Windows ME

NT-Based Windows

- New Tecnology (NT)
- Não baseado no MS-DOS
- Em 1993 - Windows NT 3.1
  - demandava muita memória, poucas aplicações 32 bits e incompatibilidade com 16 bits
- Em 1996 – Windows NT 4.0
  - poder, confiabilidade e segurança
  - forte em servidores de rede
  - compatibilidade com Windows 95 (API Win32)
- Funciona em diferentes processadores (MIPS e PowerPC)

NT-Based Windows

- Em 2000 – Windows 2000
  - Suportava apenas processadores x86

- Características:
  - plug-and-play (Placas PCI)
  - Serviço de diretório de redes

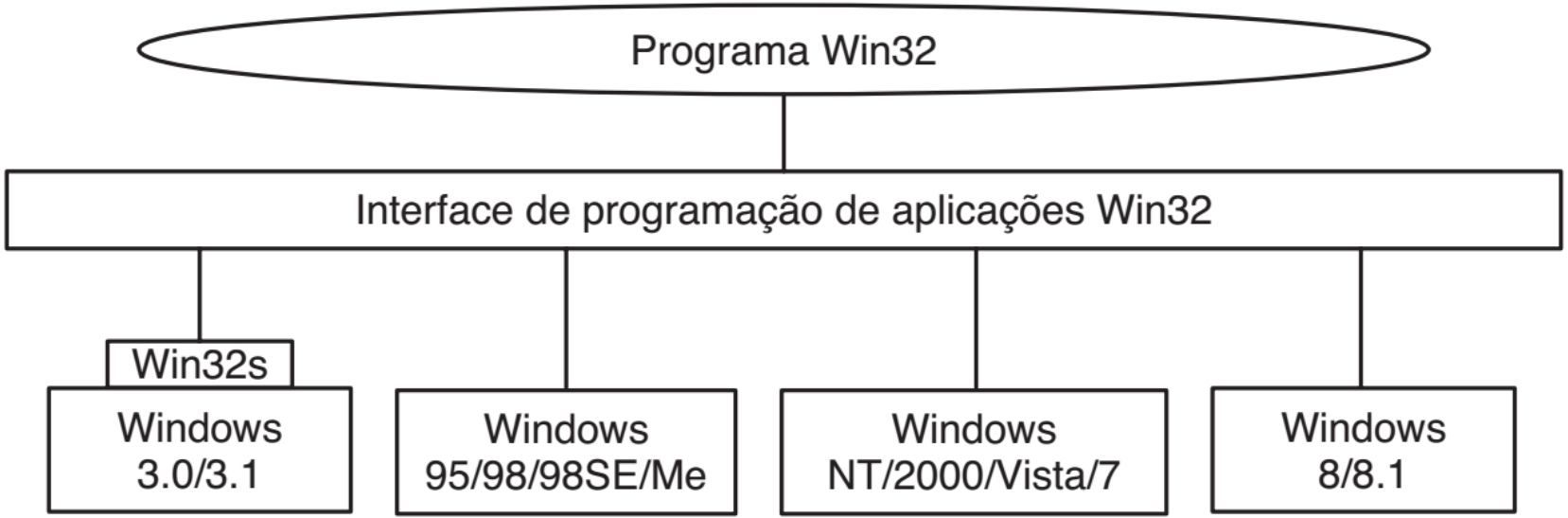
- Em 2001 – Windows XP

- Característica:
  - Interface Gráfica mais agradável

- Windows 2003
  - versão para Servidores de Rede

Windows baseados no NT

- A API (Application Programming Interface) Win32 permite que os programas sejam executados em quase todas as versões do Windows.



NT-Based Windows

- Em 2006 – Windows Vista
  - inovação na interface gráfica
  - novas características de segurança
  - confiabilidade

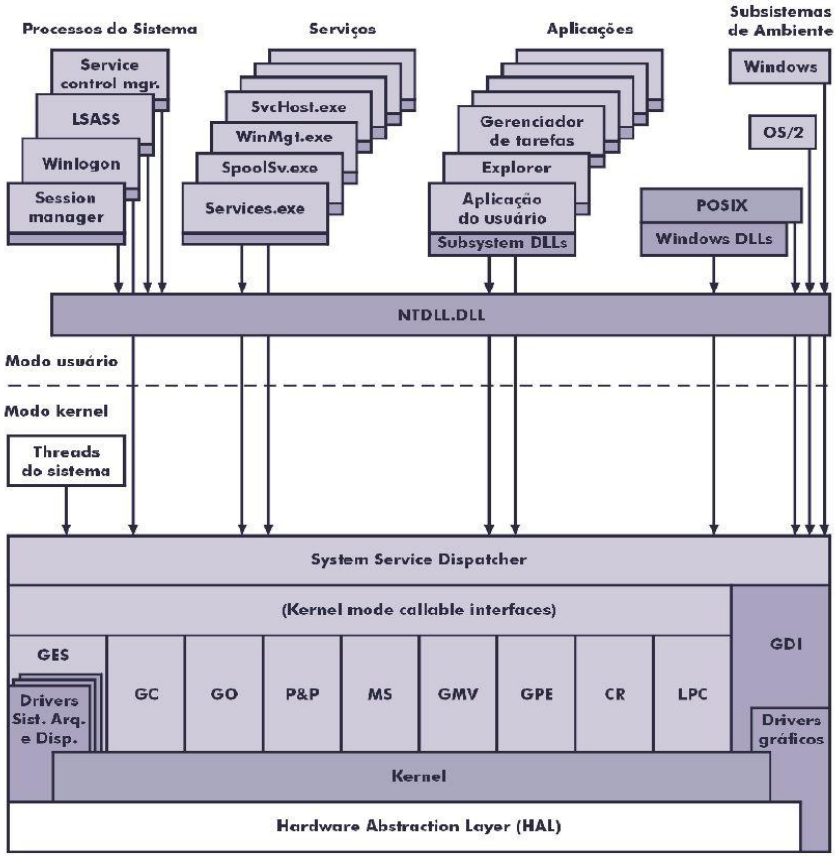
- Versão Servidor: Windows 2008 Server

- Em 2009 – Windows 7

Windows Moderno

- Em 2012 – Windows 8 / 8.1
- Em 2015 – Windows 10

Estrutura do Windows



Estrutura do Windows Moderno

- Abaixo das camadas de applets e da GUI estão as interfaces de programação sobre as quais as aplicações são construídas.

- As camadas são formadas por bibliotecas de código (**DLLs – Dynamic Library Links**), com as quais os programas se conectam dinamicamente para acessar os recursos do sistema operacional.

- O Windows também inclui um conjunto de interfaces de programação que são implementadas como serviços que funcionam como processos separados.

- As aplicações se comunicam com serviços no modo usuário por meio de chamadas de procedimento remoto (**Remote-Procedure-Calls — RPCs**).

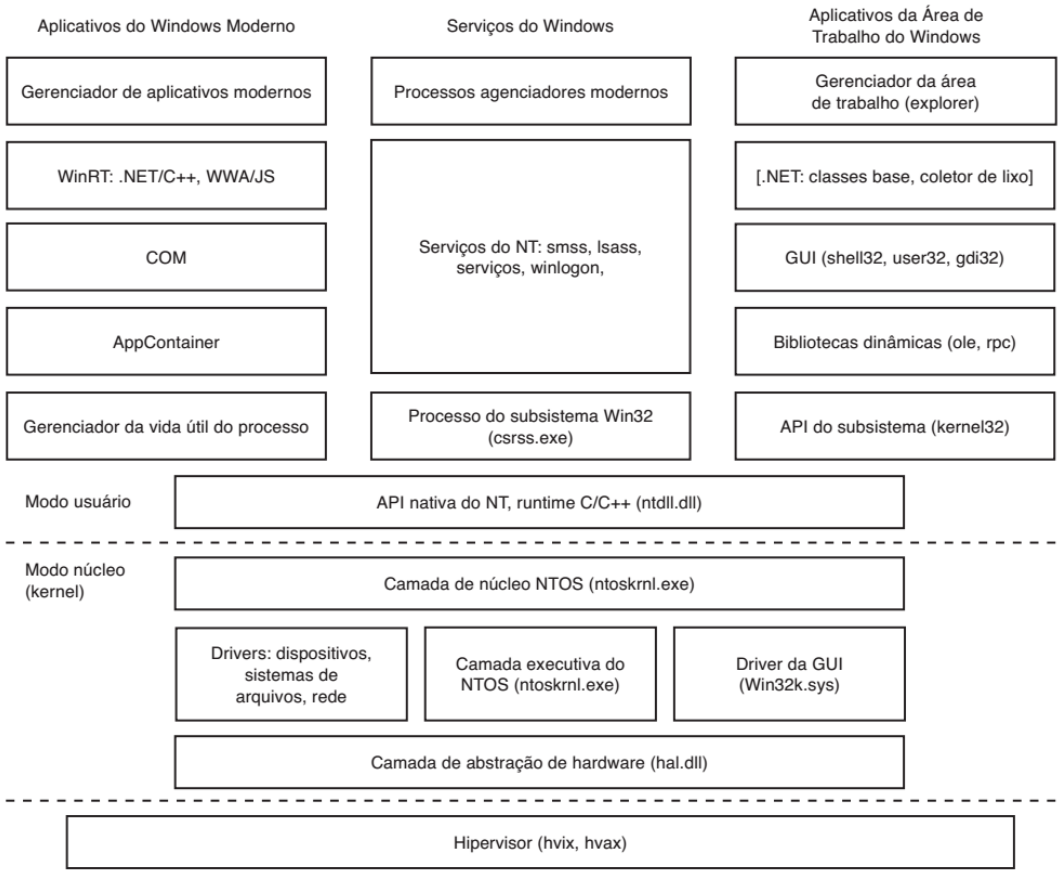
Estrutura do Windows Moderno

- O núcleo do Sistema Operacional NT é o programa de modo núcleo **NTOS** (*ntoskrnl.exe*).

- Todas as interfaces de modo usuário são implementadas utilizando subsistemas.
  - Executam em camadas acima do NTOS.

- Win32 – todas as aplicações são escritas no topo desse subsistema.

Estrutura do Windows Moderno



Estrutura do Windows Moderno

- WinRT API – um único SO executar em diversos dispositivos (desktop, celulares, tablet).

- Win32 foi mantida.

- Sistema Operacional decide o tempo de vida do processo:
  - troca de aplicação (troca de contexto)
  - gerencia capacidade de hardware (podendo terminar o processo)
  - tarefas em segundo plano (background)

- Objetivo: economizar energia e otimizar o aplicativo em dispositivos portáteis.

Estrutura do Windows Moderno

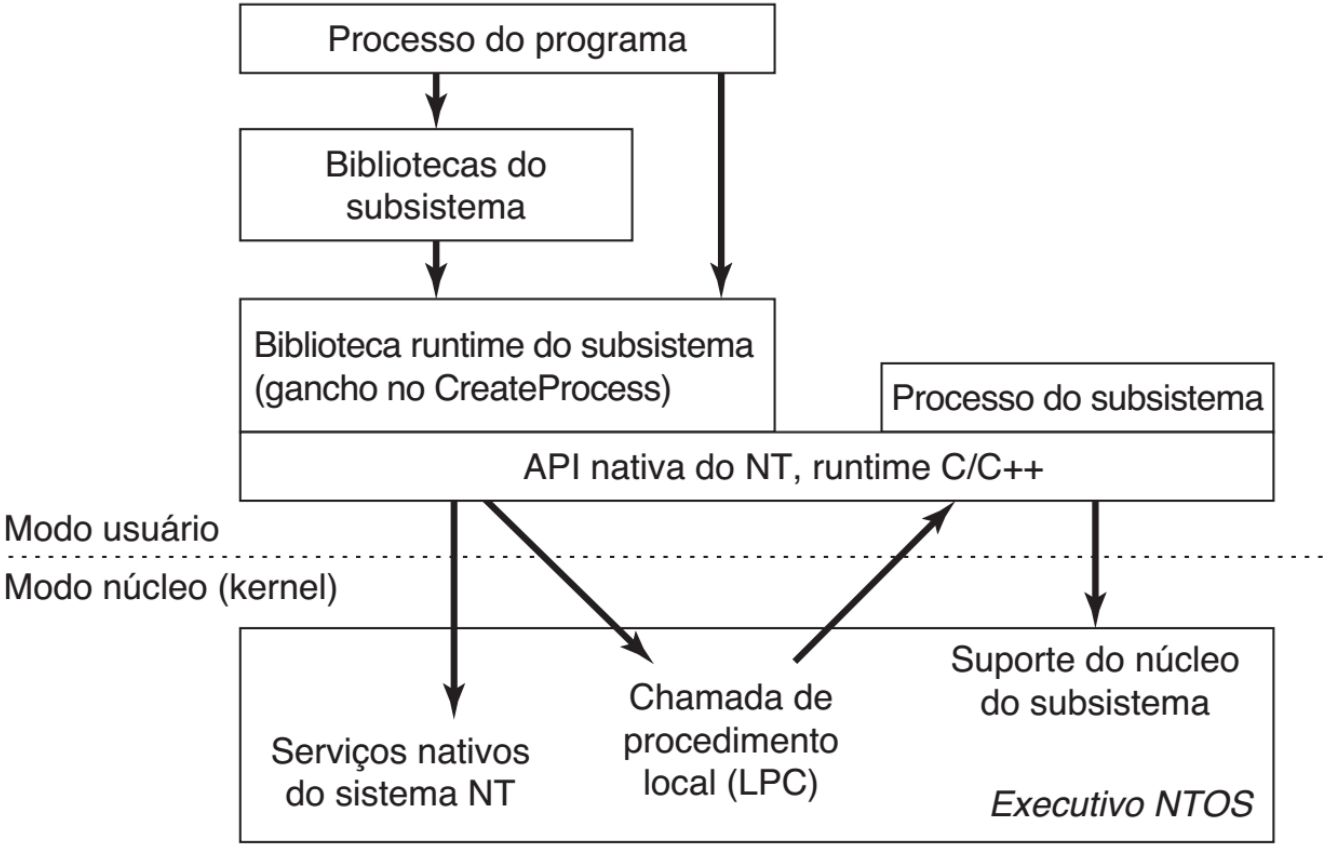
- Uma aplicação é executada em uma sandbox, chamada AppContainer.

- Sandbox - é uma técnica de segurança para isolar o código menos confiável de modo que ele não possa mexer livremente no sistema ou nos dados do usuário.

- O AppContainer do Windows trata cada aplicação como um usuário distinto e usa as facilidades de segurança do Windows para evitar que a aplicação acesse recursos aleatórios do sistema.

- Quando uma aplicação precisa de acesso a um recurso do sistema, faz uma chamada APIs WinRT que se comunicam como processos agenciadores (broker), que possuem acesso a mais partes do sistema, como os arquivos de um usuário.

Estrutura do Windows Moderno



Estrutura do Windows Moderno

Componentes:

- processo do subsistema - serviço
- conjunto de bibliotecas - implementa as funções de alto nível do sistema operacional. Contém rotinas de comunicação entre processos, através das de Chamada de Procedimento Local (**LPC - Local Procedure Call**).
- ganchos no CreateProcess – detecta o subsistema necessário para o processo e o processo do subsistema se responsabiliza por carregar o processo.
- suporte no núcleo

Estrutura do Windows Moderno

- suporte no núcleo – oferece diversas facilidades de uso geral:
  - gerenciamento de endereços virtuais
  - threads
  - manipuladores (handles) e exceções

Estrutura do Windows Moderno

- API nativa de aplicações NT
  - executadas em modo núcleo
  - Utilização do Win32

Categoria de objeto	Exemplos
Sincronização	Semáforos, mutexes, eventos, portas de IPC, filas de conclusão de E/S
E/S	Arquivos, dispositivos, drivers, temporizadores
Programa	Tarefas, processos, threads, seções, tokens
GUI do Win32	Área de trabalho, retorno (callback) de aplicações

Estrutura do Windows Moderno

- API do Win32
  - Relação da Win32 com as chamadas nativas da API do NT:

Chamada do Win32	Chamada API nativa do NT
CreateProcess	NtCreateProcess
CreateThread	NtCreateThread
SuspendThread	NtSuspendThread
CreateSemaphore	NtCreateSemaphore
ReadFile	NtReadFile
DeleteFile	NtSetInformationFile
CreateFileMapping	NtCreateSection
VirtualAlloc	NtAllocateVirtualMemory
MapViewOfFile	NtMapViewOfSection
DuplicateHandle	NtDuplicateObject
CloseHandle	NtClose

Estrutura do Windows Moderno

- WOW (Windows-on-Windows)
  - WOW32 é usado em sistemas de 32 bits x86 para executar aplicações de 16 bits do Windows 3.x mapeando as chamadas de sistema e os parâmetros entre os ambientes.
  - WOW64 permite às aplicações do Windows de 32 bits serem executadas em sistemas x64.

Estrutura do Windows Moderno

- Registro do Windows
  - tipo especial de sistema de arquivos
  - organizado em volumes (*hives*)
  - Cada *hive* mantido em um arquivo separado (diretório C:\Windows\system32\config\ do volume de inicialização)

Estrutura do Windows Moderno

- Registro do Windows

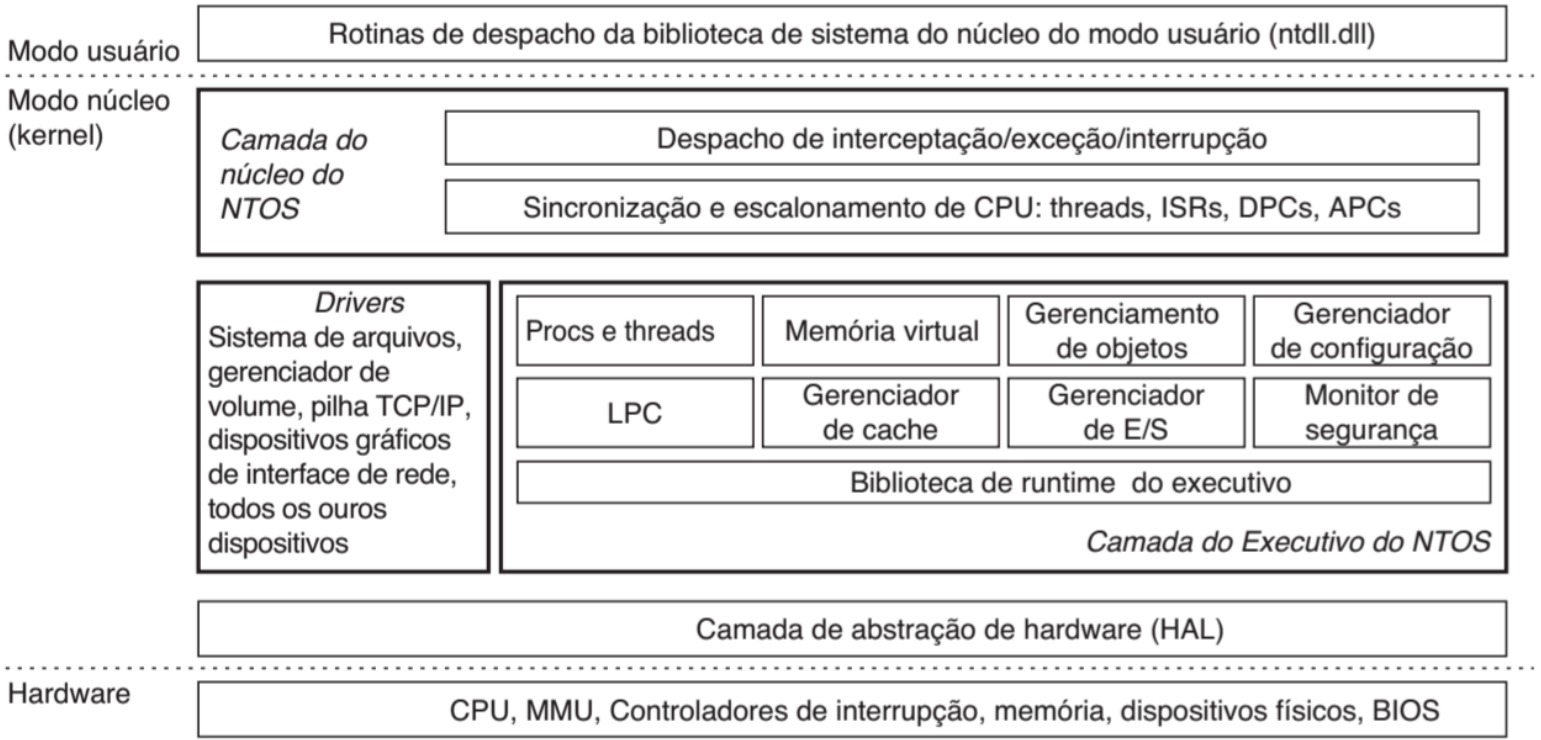
Arquivo colmeia	Nome montado	Utilização
SYSTEM	HKLM\SYSTEM	Informações de configuração do sistema operacional, usadas pelo núcleo
HARDWARE	HKLM\HARDWARE	Colmeia em memória, que grava hardwares detectados
BCD	HKLM\BCD*	Base de dados de configurações de inicialização
SAM	HKLM\SAM	Informações de contas de usuários locais
SECURITY	HKLM\SECURITY	Informações de contas do lsass e outras informações de segurança
DEFAULT	HKEY_USERS\.DEFAULT	Colmeia-padrão para novos usuários
NTUSER.DAT	HKEY_USERS \<user id>	Colmeia específica de usuários, mantida no diretório pessoal
SOFTWARE	HKLM\SOFTWARE	Classes de aplicações registradas pelo COM
COMPONENTS	HKLM\COMPONENTS	Manifestos e dependências para os componentes do sistema

Estrutura do Windows Moderno

- Registro do Windows
  - regedit – programa com insterface gráfica para explorar o registro
  - procmon (Process Monitor) - ferramentas da Microsoft disponibilizada em www.microsoft.com/technet/sysinternals
  - http://live.sysinternals.com/
  - PowerShell - linguagem de scripts da Microsoft

Estrutura do Sistema Operacional

- Modo Kernel (Núcleo)



Estrutura do Windows Moderno

- Modo Kernel (Núcleo)
  - Camada Central - NTOS
    - Executivo - implementa a maioria dos serviços
    - Núcleo - implementa os mecanismos de interrupção e interceptação usados na transição do modo usuário para o modo núcleo

Estrutura do Windows Moderno

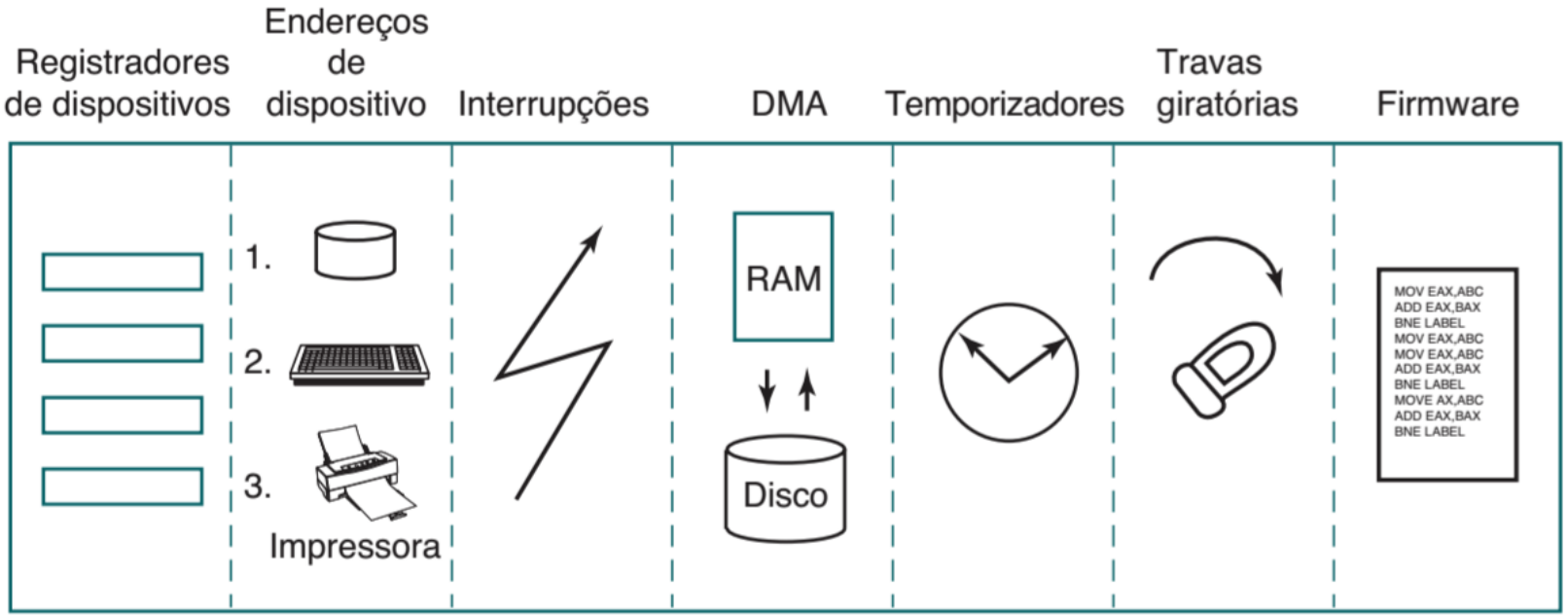
- Camada do Núcleo
  - Gerenciamento da CPU
    - Gerenciamento de Threads

Estrutura do Windows Moderno

- Camada do Executivo
  - Gerenciador de Objetos
  - Gerenciador de E/S
  - Gerenciador de Processos
  - Gerenciador de Memória
  - Gerenciador de Cache

Estrutura do Sistema Operacional

- Camada de Abstração de Hardware (HAL – Hardware Abstraction Layer)



Estrutura do Sistema Operacional

- Drivers de Dispositivos
    - são bibliotecas de ligação de dinâmicas (DLL)