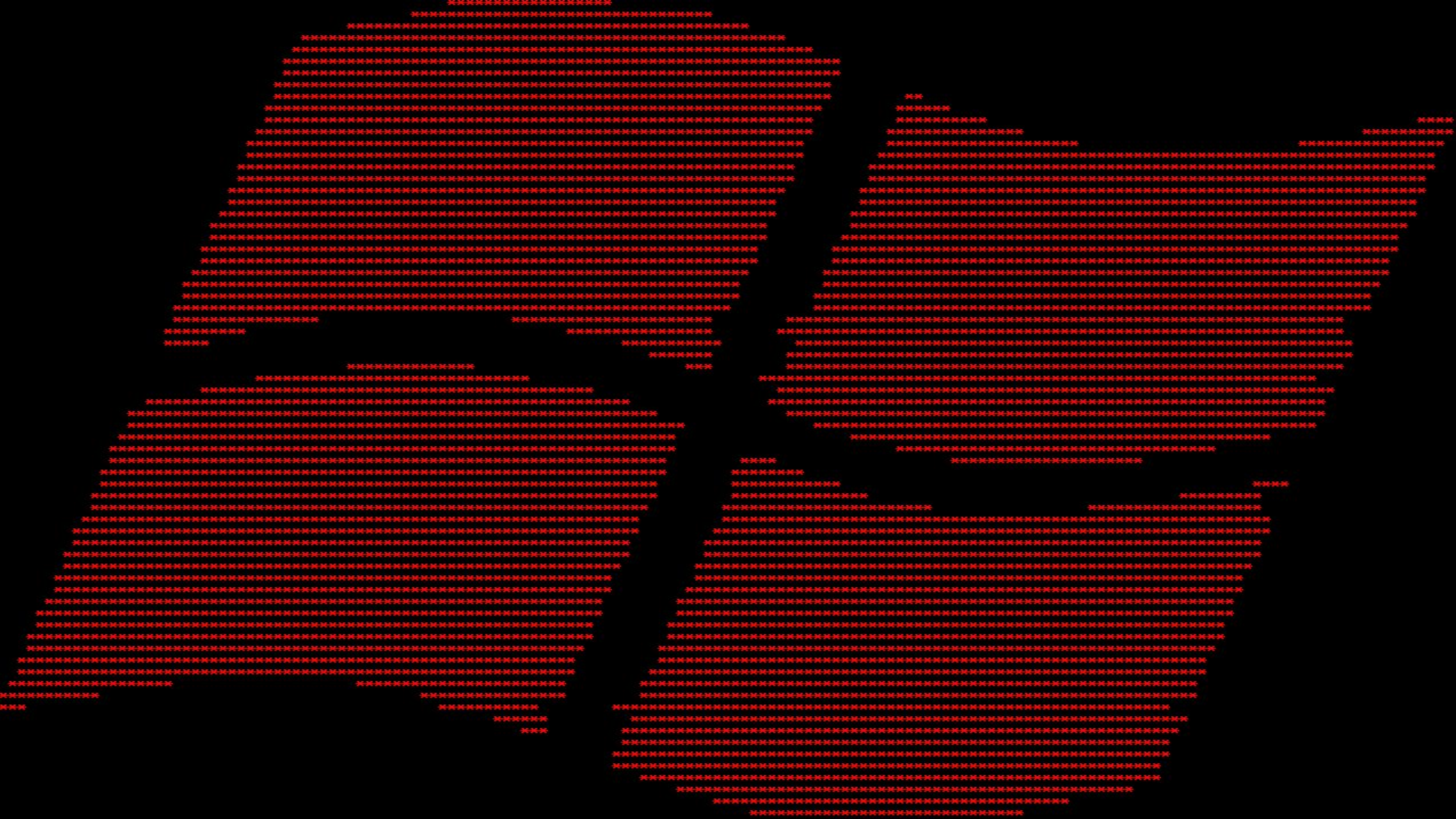
BATCH

Igor Cardozo Martins

https://github.com/Gowq/dosMania

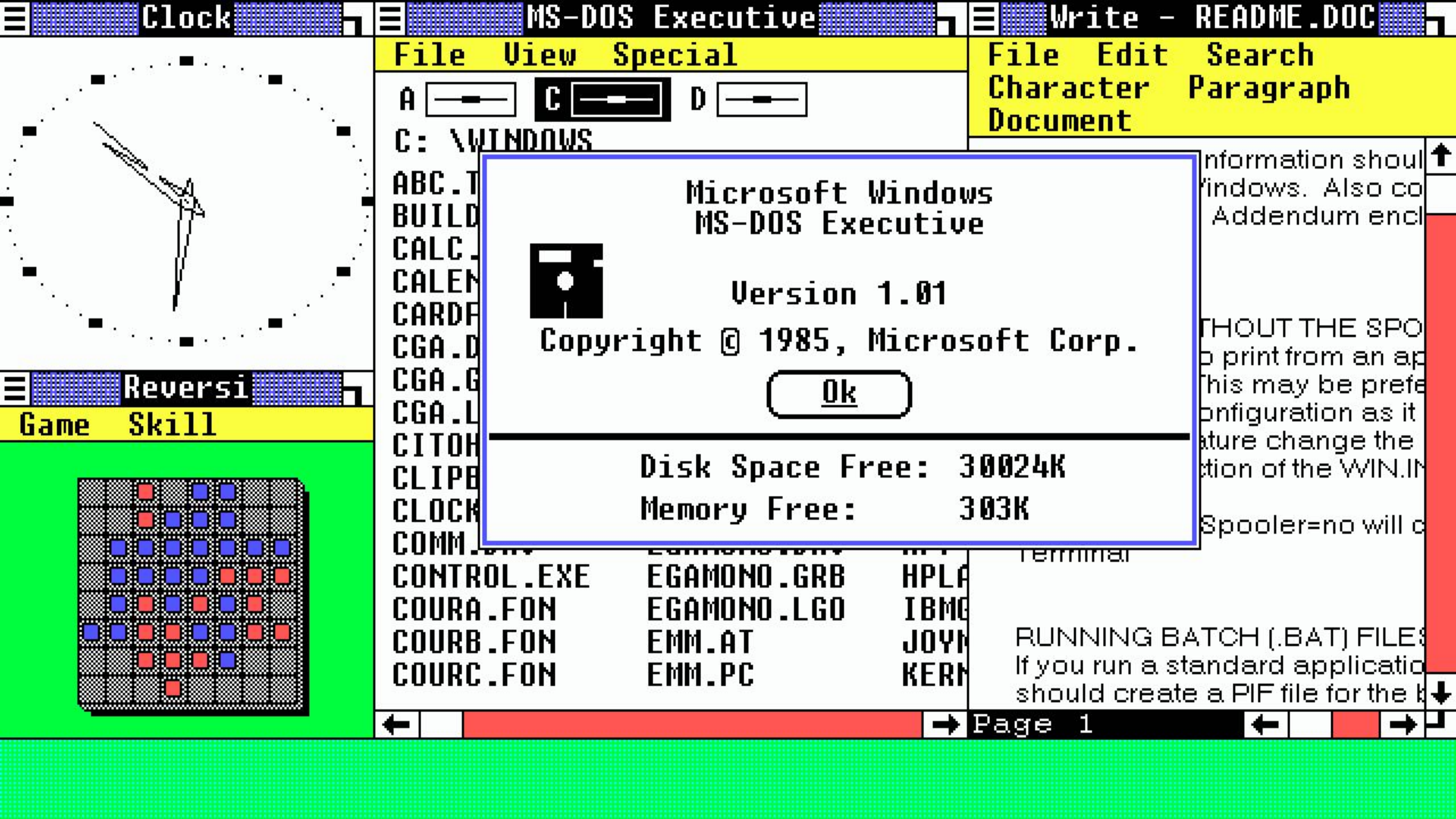


SISTEMAS DA MICROSOFT

MS-DOS 1.X -> MS-DOS 6.X

COM DEPENDÊNCIA AO MS-DOS

- WINDOWS 1.X
- WINDOWS 2.X
- WINDOWS 3.X
- WINDOWS 95
- WINDOWS 98
- WINDOWS ME



C: \WINDOWS

```
ABC.T
BUILD
CALC.
CALEN
CARDF
CGA.D
CGA.G
CGA.L
CITOH
CLIPB
CLOCK
COMM.DRV
CONTROL.EXE    EGAMONO.GRB    HPLA
COURA.FON      EGAMONO.LGO    IBMG
COURB.FON      EMM.AT         JOYM
COURC.FON      EMM.PC         KERN
```

Microsoft Windows
MS-DOS Executive

Version 1.01

Copyright © 1985, Microsoft Corp.

Ok

Disk Space Free: 30024K
Memory Free: 303K

nformation shoul
Windows. Also co
Addendum encl

THOUT THE SPO
o print from an ap
This may be prefe
onfiguration as it
ature change the
tion of the WIN.IN
Spooler=no will c
Terminal

RUNNING BATCH (.BAT) FILES
If you run a standard applicatio
should create a PIF file for the b

LINHAS DE COMANDO (CLI x GUI)

-> GERENCIAMENTO DE GRANDES VOLUMES.

-> NEM TODAS FERRAMENTAS DE INFOSEC POSSUEM INTERFACE GRÁFICA (ex. t50 do Nelson Brito).

-> HÁ AMBIENTES QUE ESSA FORMA DE ACESSO É EXCLUSIVA.

-> AUDITORIA/RASTREIO POSSÍVEIS E RELATIVAMENTE FÁCEIS.

-> CRIAÇÃO DE ROTINAS.

BATCH - ROTINAS EM ARQUIVOS DE LOTE

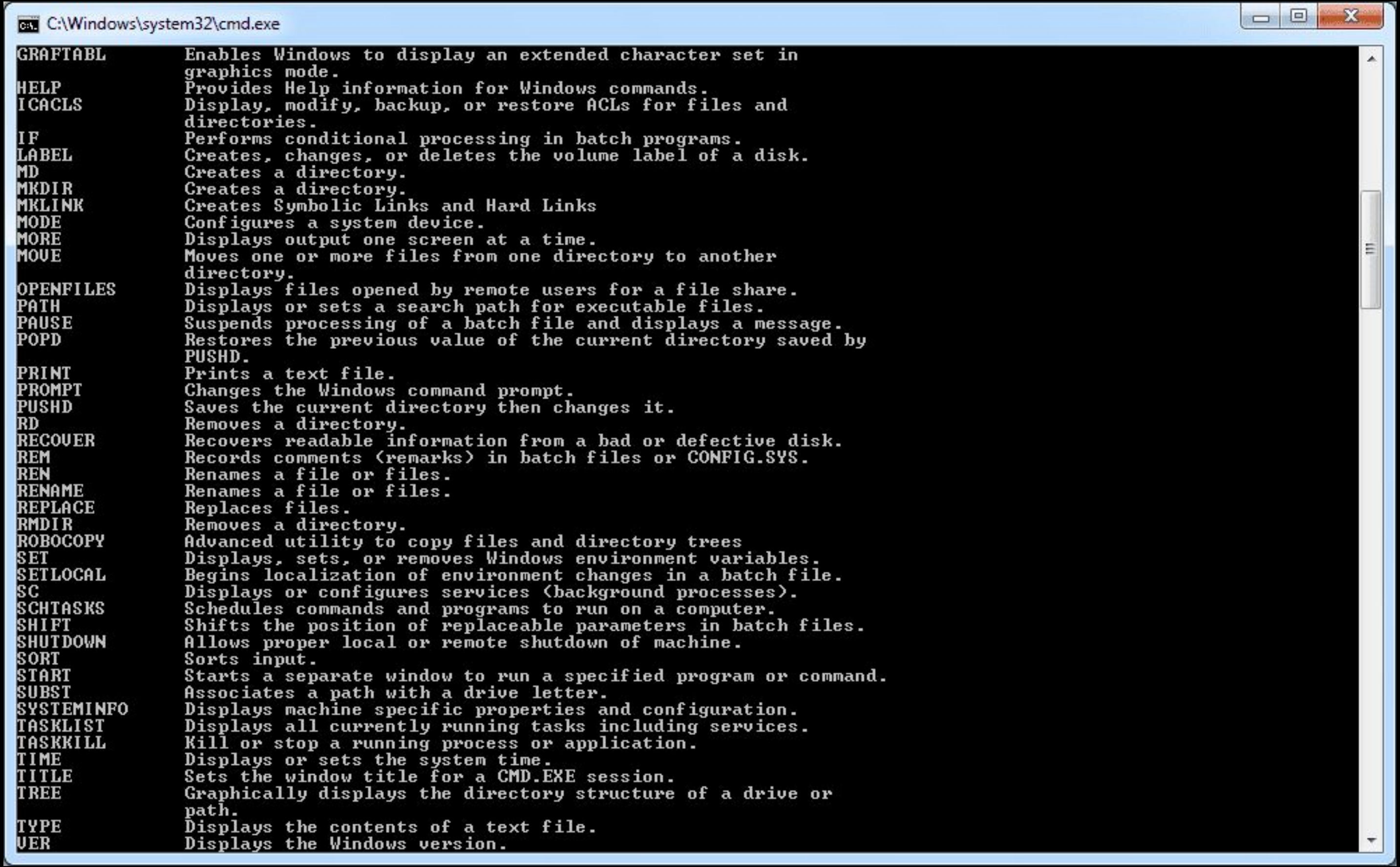
Def. Instruções de rotina interpretadas sequencialmente.

-> Command.com (Windows 95, 98 e ME) extensão .bat

-> Cmd.exe (Windows NT) extensão .bat e .cmd

-> 4DOS/4OS2 E 4NT (Instalável) extensão .btm

COMANDO HELP



```
GRAFTABL        Enables Windows to display an extended character set in
                graphics mode.
HELP            Provides Help information for Windows commands.
ICACLS          Display, modify, backup, or restore ACLs for files and
                directories.
IF              Performs conditional processing in batch programs.
LABEL           Creates, changes, or deletes the volume label of a disk.
MD              Creates a directory.
MKDIR           Creates a directory.
MKLINK          Creates Symbolic Links and Hard Links
MODE            Configures a system device.
MORE            Displays output one screen at a time.
MOVE            Moves one or more files from one directory to another
                directory.
OPENFILES       Displays files opened by remote users for a file share.
PATH            Displays or sets a search path for executable files.
PAUSE           Suspends processing of a batch file and displays a message.
POPD            Restores the previous value of the current directory saved by
                PUSHD.
PRINT           Prints a text file.
PROMPT          Changes the Windows command prompt.
PUSHD           Saves the current directory then changes it.
RD              Removes a directory.
RECOVER         Recovers readable information from a bad or defective disk.
REM             Records comments (remarks) in batch files or CONFIG.SYS.
REN             Renames a file or files.
RENAME          Renames a file or files.
REPLACE         Replaces files.
RMDIR           Removes a directory.
ROBOCOPY        Advanced utility to copy files and directory trees
SET             Displays, sets, or removes Windows environment variables.
SETLOCAL        Begins localization of environment changes in a batch file.
SC              Displays or configures services (background processes).
SCHTASKS        Schedules commands and programs to run on a computer.
SHIFT           Shifts the position of replaceable parameters in batch files.
SHUTDOWN        Allows proper local or remote shutdown of machine.
SORT            Sorts input.
START           Starts a separate window to run a specified program or command.
SUBST           Associates a path with a drive letter.
SYSTEMINFO      Displays machine specific properties and configuration.
TASKLIST        Displays all currently running tasks including services.
TASKKILL        Kill or stop a running process or application.
TIME            Displays or sets the system time.
TITLE           Sets the window title for a CMD.EXE session.
TREE            Graphically displays the directory structure of a drive or
                path.
TYPE            Displays the contents of a text file.
VER             Displays the Windows version.
```

COMANDO HELP PELAS VERSÕES

2000 -> XP Remove <KEYB>

XP -> Vista Adiciona <BCDEDIT, DISKPART, DRIVERQUERY, FSUTIL, GPRESULT, ICACLS, ICACLS, ICACLS, ROBOCOPY, SC, SCHTASKS, SHUTDOWN, SYSTEMINFO, TASKLIST, TASKLIST, WMIC>

Vista -> 7 Nenhuma

7 -> 8.1 Nenhuma

8.1 -> 10 Remove <DISKCOMP, DISKCOPY>

PRINCIPAIS COMANDOS

Input/Output - <echo>, <set /a> e <set /p>

Controle de fluxo - <if>, <for>, <goto> e <call>

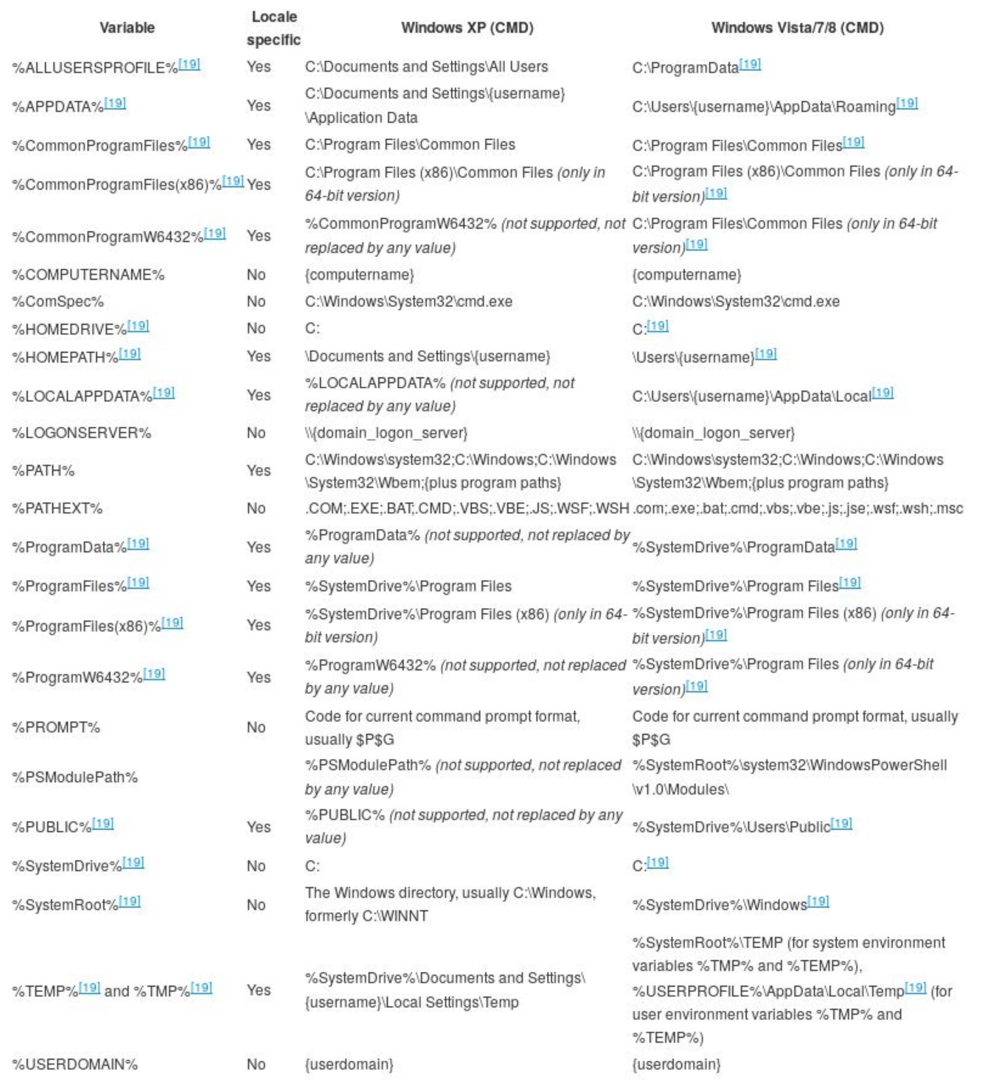
Manipulação de diretórios - <attrib>, <cd>, <move>,<copy>, <del> e <rmdir>

Manipulação de processos - <tasklist> e <taskkill>

Conexão - <netstat>, <ping> e <tracert>

VARIÁVEIS DE AMBIENTE

<%userprofile%>	-> %SystemDrive%\Users\{username}
<%windir%>	-> %SystemDrive%\Users\{username}
<%appdata%>	-> C:\Users\{username}\AppData\Roaming
<%user%>	-> {username}
<%temp%>	-> %USERPROFILE%\AppData\Local\Temp
<%0%> (...)	-> Pseudo variável



Variable	Locale specific	Windows XP (CMD)	Windows Vista/7/8 (CMD)
%ALLUSERSPROFILE%[19]	Yes	C:\Documents and Settings\All Users	C:\ProgramData[19]
%APPDATA%[19]	Yes	C:\Documents and Settings\{username}\Application Data	C:\Users\{username}\AppData\Roaming[19]
%CommonProgramFiles%[19]	Yes	C:\Program Files\Common Files	C:\Program Files\Common Files[19]
%CommonProgramFiles(x86)%[19]	Yes	C:\Program Files (x86)\Common Files *(only in 64-bit version)*	C:\Program Files (x86)\Common Files *(only in 64-bit version)*[19]
%CommonProgramW6432%[19]	Yes	%CommonProgramW6432% *(not supported, not replaced by any value)*	C:\Program Files\Common Files *(only in 64-bit version)*[19]
%COMPUTERNAME%	No	{computername}	{computername}
%ComSpec%	No	C:\Windows\System32\cmd.exe	C:\Windows\System32\cmd.exe
%HOMEDRIVE%[19]	No	C:	C:[19]
%HOMEPATH%[19]	Yes	\Documents and Settings\{username}	\Users\{username}[19]
%LOCALAPPDATA%[19]	Yes	%LOCALAPPDATA% *(not supported, not replaced by any value)*	C:\Users\{username}\AppData\Local[19]
%LOGONSERVER%	No	\\{domain_logon_server}	\\{domain_logon_server}
%PATH%	Yes	C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;{plus program paths}	C:\Windows\system32;C:\Windows;C:\Windows\System32\Wbem;{plus program paths}
%PATHEXT%	No	.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.WSF;.WSH	.com;.exe;.bat;.cmd;.vbs;.vbe;.js;.jse;.wsf;.wsh;.msc
%ProgramData%[19]	Yes	%ProgramData% *(not supported, not replaced by any value)*	%SystemDrive%\ProgramData[19]
%ProgramFiles%[19]	Yes	%SystemDrive%\Program Files	%SystemDrive%\Program Files[19]
%ProgramFiles(x86)%[19]	Yes	%SystemDrive%\Program Files (x86) *(only in 64-bit version)*	%SystemDrive%\Program Files (x86) *(only in 64-bit version)*[19]
%ProgramW6432%[19]	Yes	%ProgramW6432% *(not supported, not replaced by any value)*	%SystemDrive%\Program Files *(only in 64-bit version)*[19]
%PROMPT%	No	Code for current command prompt format, usually PG	Code for current command prompt format, usually PG
%PSModulePath%		%PSModulePath% *(not supported, not replaced by any value)*	%SystemRoot%\system32\WindowsPowerShell\v1.0\Modules\
%PUBLIC%[19]	Yes	%PUBLIC% *(not supported, not replaced by any value)*	%SystemDrive%\Users\Public[19]
%SystemDrive%[19]	No	C:	C:[19]
%SystemRoot%[19]	No	The Windows directory, usually C:\Windows, formerly C:\WINNT	%SystemDrive%\Windows[19]
%TEMP%[19] and %TMP%[19]	Yes	%SystemDrive%\Documents and Settings\{username}\Local Settings\Temp	%SystemRoot%\TEMP (for system environment variables %TMP% and %TEMP%), %USERPROFILE%\AppData\Local\Temp[19] (for user environment variables %TMP% and %TEMP%)
%USERDOMAIN%	No	{userdomain}	{userdomain}

HELLO WORLD

```
@echo off

echo Hello World

pause>nul
```

ALGUMAS ROTINAS ÚTEIS (*ou não*)

-> CALCULADORA

-> VELOCÍMETRO

-> ROTINAS DE BACKUP

-> JOGOS

VÍRUS e MALWARES

Forkbomb - ‘repetidor.bat’

Worm - ‘replicante.bat’ e ‘iloveyou.vbs’

Vírus - ‘deletador.bat’

‘Cavalo de Troia’ - SFX winrar

PROBLEMAS CONHECIDOS

-> Expansão atrasada

-> Caracteres de escape

-> Sleep ou delay

-> Textos concatenados

-> Aspas e espaços nas strings

-> ‘Caracteres especiais’

Alternativas ao DOS

-> VBS

-> Powershell