Interrupciones del BIOS

- BIOS (basic input/output System): es el firmware básico instalado en la placa base.
- Proporciona rutinas básicas de acceso al hardware
- Pueden dividirse en 5 grupos:
  - Interrupciones asociadas a la CPU (INT 0 a INT 7)
  - Interrupciones asociadas al controlador de interrupciones 8259 (INT 8 a INT 0Fh)
  - Servicios del BIOS (INT 10h a INT 1Ah e INT 40h)
  - Rutinas de usuario (INT 1Bh e INT 1Ch)
  - Punteros a tablas de datos (INT 1Dh a INT 1Fh e INT 41h)

Asociadas a la CPU

INT 0: División por cero
- Generada por la CPU cuando el cociente de una división (DIV o IDIV) es demasiado grande para ser almacenado en AL o AX
- Imprime en consola "Divide overflow" y retorna al DOS

INT 1: Ejecución paso a paso
- Se activa cuando la bandera de trampa (TF) vale 1 y la CPU ha ejecutado cualquier instrucción
- El DOS inicializa el vector de interrupción con una dirección que contiene la instrucción IRET
- Los programas de depuración DEBUG, SYMDEB, TD,... cambian el vector a una rutina de servicio que permite la ejecución paso a paso de los programas

INT 2: No enmascarable
- Se activa con flanco ascendente en el pin NMI de la CPU. El pin está conectado al detector de paridad de la RAM
- Imprime en la consola "Parity check 1" y detiene la CPU

INT 3: Punto de ruptura (break point)
- Se activa cuando se ejecuta una instrucción con código CCh
- Se usa en programas de depuración: permite la ejecución de un programa hasta que se encuentra con esa instrucción
- El DOS inicializa el vector de interrupción con una dirección que contiene la instrucción IRET

Int 4: Desbordamiento (overflow)
- Se activa mediante la instrucción INTO
- Genera una INT 4 si bandera O=1
- El DOS inicializa el vector de interrupción con una dirección que contiene la instrucción IRET

INT 5: Imprimir pantalla
- Esta interrupción imprime el texto que se está mostrando en pantalla
- Puede activarse con la tecla Impr-Pant

INT 6, 7 (No utilizadas)

Interrupciones asociadas al controlador de interrupciones
Las interrupciones 8 a 15 (0Fh) están asociadas al controlador de interrupciones hardware (8259A) y se activan cada vez que se produce un flanco en sus entradas IRQ0 a IRQ7

INT 8 Temporizador
- El temporizador del sistema (8253) activa esta interrupción 18'2 veces por segundo (cada 55ms)
- La rutina de servicio incrementa en uno el contador de 32 bits situado en las siguientes direcciones de la BIOS (y lo pone a 0 cada 24 horas)
  0040h:006Ch (palabra baja)
  0040h:006Eh (palabra alta)
- La rutina de servicio también activa una INT 1Ch

INT 9: Teclado
- se activa cada vez que se pulsa o libera una tecla
- La rutina de servicio guarda el código de la tecla en el buffer de teclado

INT 0Ah (No utilizable)
INT 0Bh: Puerto serie 1
INT 0Ch Puerto serie 2
INT 0Dh Disco duro (XT) o puerto paralelo 2 (AT)
INT 0Eh Disquete
INT 0Fh Puerto paralelo 1

Interrupciones servicios del BIOS

INT 10h: Entrada/salida de video
Lo Diversas funciones relacionadas con la salida de video según AH

INT 11h Chequeo del equipo físico
La Retorna en AX una descripción del hardware instalado

INT 12h: Tamaño de memoria
La Retorna en AX el número de bloques de 1KB de la RAM instalada

INT 13h: Acceso a disco
Lo Diversas funciones relacionadas con acceso a disco según el valor de AH

INT 14h Acceso a puerto serie RS-232

INT 15h Acceso a cassette

INT 16h Entrada/Salida de teclado
Lo Diversas funciones relacionadas con el teclado según el valor de AH

INT 17h: Entrada/Salida de impresora

INT 18h: Ejecución del BASIC

INT 19h: Inicio del sistema
Lo lee el sector 1 de la pista 0 del disco de arranque y ejecuta el programa de arranque del DOS

INT 1Ah: Hora del día
Lo Acceso al contador de 32 bits del temporizador (INT 8)

INT 1Bh: Ruptura desde teclado
- Lo Es activa la rutina de servicio de la INT 9 cuando detecta Ctrl+C
- Lo El BIOS inicializa el vector de interrupción con una dirección que contiene la instrucción IRET
- El DOS cambia el vector de interrupción a una rutina que activa bandera interna y llama a INT 23h

INT 1Ch: Tic del temporizador
- Lo Es activa la rutina de servicio de la INT 8
- Lo El BIOS inicializa el vector de interrupción con una dirección que contiene instrucción IRET

Punteros a tablas de datos

Son interrupciones 1Dh a 1Fh y 41h son en realidad direcciones de tablas de parámetros usadas por los servicios de vídeo y disco del BIOS

INT 1Dh: Parámetros de vídeo

INT 1Eh: Parámetros de disquete

INT 1Fh: Tabla de caracteres gráficos

INT 41h: Parámetros de disco duro

INT 20h: Finaliza programa

La acaba ejecución de programa retornando al intérprete de comandos, se recomienda usar con AH=4Ch (Finaliza programa, cerrando ficheros y liberando memoria)

INT 21h: Despachador del DOS

La ejecuta los distintos servicios del DOS según AH

INT 22h Dirección de terminación

La Dirección de la rutina que se ejecuta cuando finaliza el programa

INT 23h Rutina de servicio de Ctrl-C

La llamada por el DOS cuando detecta CTRL-C

INT 24h Manejador de errores críticos

La Invocada por DOS cuando se produce un error crítico en acceso a un dispositivo hardware

INT 27h: Finaliza programa dejando residente

acaba ejecución de un programa .COM dejándolo residente en memoria

Para dejar residente un .EXE se emplea int 21h con AH=31h

```
MOV AX, 4C00h
int 21h
```

Ejecución de programas desde el DOS

- Los programas en código máquina están almacenados en ficheros ejecutables de disco
- Cuando se ejecuta un programa, el intérprete de comandos carga el contenido de su fichero ejecutable en una zona libre que reserva en RAM
- Como parte de la carga se añade una zona de 256 bytes que contiene datos relacionados con el programa (Prefijo de Segmento de Programa, PSP)
- Los ficheros ejecutables pueden estar en formato .EXE o .COM, teniendo su ejecución un comportamiento ligeramente distinto
- Cuando acaba un programa, se devuelve el control al intérprete del DOS y la memoria que ocupaba se deja libre salvo que se deje residente

PSP → Prefijo de segmento de programa

- Zona de datos de 256 bytes que encabeza los programas .EXE o .COM una vez están cargados en RAM para su ejecución
  - Generada por el DOS mediante el intérprete de comandos (COMMAND.COM)
  - Campos más destacados del PSP
    - Offsets 0 y 1 (2 bytes)
      - Instrucción INT 20h
      - Permite acabar el programa saltando al offset 0
    - Offsets 0Ah a 0Dh (4 bytes)
      - Vector original de la rutina de servicio de la INT 22h (dirección de terminación de programa)
      - Cuando acaba el programa se copia a la tabla de vectores de interrupción y se salta a esa dirección
    - Offsets 0Eh a 11h (4 bytes)
      - Vector original de la rutina de servicio de la INT 23h
      - El programa puede cambiar la rutina de esa interrupción para capturar Ctrl+C
      - Cuando acaba el programa se repone la rutina original copiando su dirección desde este campo a la tabla de vectores de interrupción
    - Offsets 12h a 15h (4 bytes)
      - Vector original de la rutina de servicio INT 24h
      - El programa puede cambiar la rutina de la interrupción para capturar errores críticos
      - Cuando acaba el programa se repone la rutina original copiando su dirección desde este campo a la tabla de vectores de interrupción

- Offsets 2Ch y 2Dh (2 bytes)
  Número de segmento físico que contiene una copia de las variables de entorno del DOS
  Permite al programa acceder a esas variables
- Offset 80h (1 byte)
  Tamaño en bytes de los parámetros del programa en línea de comandos
- Offset 81h a FFh (127 bytes)
  - Códigos ASCII de los parámetros del programa en línea de comandos. Acaba con código 13 (retorno de carro)
  - Permite al programa acceder a los parámetros indicados por línea de comandos

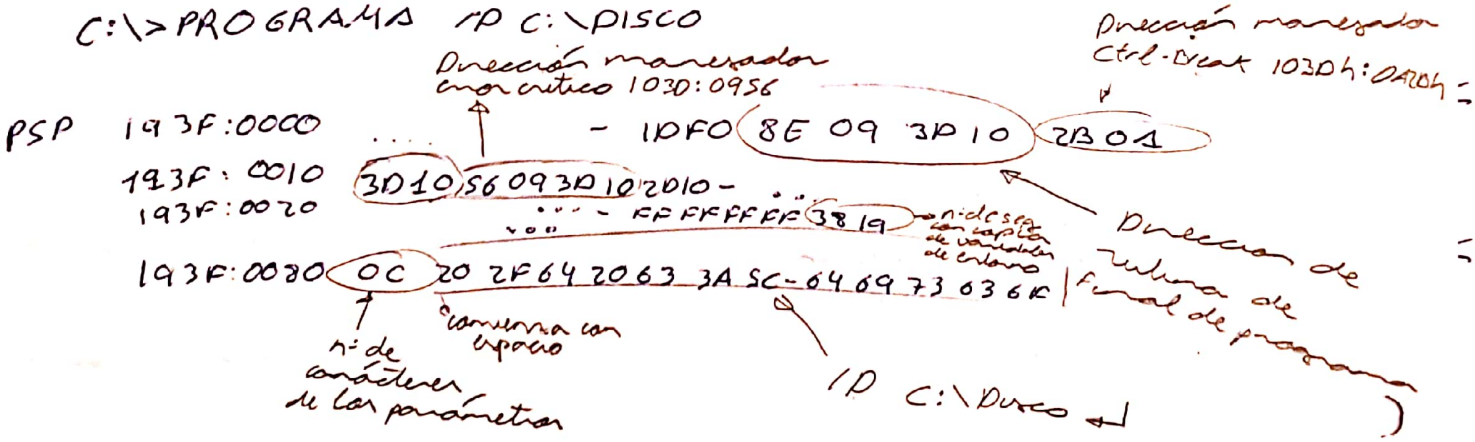
Ejemplo

- Dadas las siguientes variables de entorno (comando SET de DOS),

```
COMSPEC=C:\DOS60\COMMAND.COM
PROMPT=$P$G
TEMP=C:\TEMP
PATH=C:\TO;C:\TASM
```

- Si se ejecuta el programa con parámetros /D y C:\DISCO

```
C:\>PROGRAMA /D C:\DISCO
```



Tres tipos de ficheros ejecutables en DOS:

- BAT
  - Secuencias de comandos del DOS (no código máquina)
- .EXE
  - Programas en código máquina
  - Generados por un montador (linker) a partir de uno o varios ficheros de código objeto generados por un compilador o ensamblador
- .COM
  - son programas en código máquina
  - El programa ocupa un único segmento físico de 64 KB con código, datos y pila
  - su primera instrucción ejecutable está en la dirección 256 (100h) respecto al origen del segmento. Se debe usar la directiva ORG 256 antes de la 1ª instr. ensamblador
  - se crean a partir de un .EXE con el comando EXE2BIN o con la opción /6 del montador

- Ejecución de programas .COM:
  - CS, DS, ES y SS apuntan al PSP
  - IP se inicializa a 256 (posición siguiente al PSP)
  - SP se inicializa con OFFFEh
  - AL se indica si es correcta la unidad de disco del primer fichero (0 si es correcta)
  - AH indica si es correcta la unidad de disco del segundo fichero (0 si es correcta)
  - Al acabar el programa se devuelve el control al sistema operativo (intérprete de comandos) y se libera la zona de memoria donde se cargó el programa

- Ejecución de programas .EXE
  - CS y SS inicializados por el DOS
  - DS y ES apuntan al PSP
  - IP inicializado con dirección indicada en cabecera EXE
  - SP inicializado con el valor más alto de la pila
  - AL indica si es correcta la unidad de disco del 1º fichero y AH del segundo fichero
  - Al acabar el programa se devuelve el control al sistema operativo (intérprete de comandos) y se libera la zona de memoria donde se cargó el programa

- Programas residentes
  - Programas .COM o .EXE que terminan su ejecución dejando sin liberar parte de la memoria que ocupan
  - Su posición en memoria suele almacenarse en forma de vector de interrupción
  - Pueden ser llamados desde otros programas en ejecución o desde rutinas de servicio de interrupción

- Programas residentes .COM (instalación)
  - Finalizan con INT 27h
  - DX debe contener el offset de la posición siguiente a la última que se quiere dejar residente.
  - Cuidado de dar partes
    - [para información (código, variables, ...) que queda residente
    - [el código que instala lo justo que se deja residente

Ejemplo de instalación de una rutina de servicio de la interrupción 40h

```
codigo segment
    ASSUME cs:codigo
    ORG 256
inicio: jmp instalador
; Variables globales
tabla DB "abcdf"
flags DW 0
; Rutina de servicio a la int
rsi PROC FAR
    ; salva registros modificados
      push...
    ; instrucciones de la rutina
    ...
    ; recupera registros modificados
      pop...
      iRET
rsi ENDP
...
instalador PROC
    mov ax, 0
    mov es, ax
    mov ax, offset rsi
    mov bx, cs
    cli
    mov es:[40h*4], ax
    mov es:[40h*4+2], bx
    sti
    mov dx, offset instalador
    int 27h, acaba dejando residente.
             PSP, variables y rutina rsi
instalador ENDP
Codigo ends
END Inicio
```

Programas residentes .COM (desinstalación)

- Ha de ejecutarse un programa o rutina (desinstalador) que libere la memoria que deja residente
- Se libera un segmento físico de memoria mediante INT 21h con AH=49h y ES=número de segmento
- Se deben liberar dos segmentos físicos:
  - segmento de código del programa residente (donde guardarse el viejo vector de interrupción)
  - segmento de variables de entorno (offset 2Ch del PSP)
- Antes de liberar un programa es conveniente comprobar que está instalado
  - Vector de interrupción != 0
  - Primeros bytes de la rutina de servicio son los del programa que se desea instalar (firma digital del programa)
  - Ejemplo de desinstalación de la rutina de int 40h

```
desinstalar_40h PROC
    push ax bx cx dx es
    mov cx, 0
    mov ds, cx ; segmento de vect de int
    mov es, ds:[40h*4+2] ; lee segmento rsi
    mov bx, es:[2Ch] ; lee segmento de entorno del PSP de rsi
    mov ah, 49h
    int 21h          ; libera segmento de RSI (es)
    mov es, bx
    int 21h          ; libera segmento de variable de entorno de RSI (bx, es)
    cli
    mov ds:[40h*4], cx ; Pone a 0 el vector de interrupción (cx=0)
    mov ds:[40h*4+2], cx
    sti
    pop es dx cx bx ax
    ret
desinstalar_40h ENDP
```