Mini Intro a Sistemas Operativos

Sistemas Operativos

Objetivos

- Proveer recursos a las apps
- Administrar recursos

Problemas

- Memoria insuficiente
- Fragmentación de memoria
- Seguridad

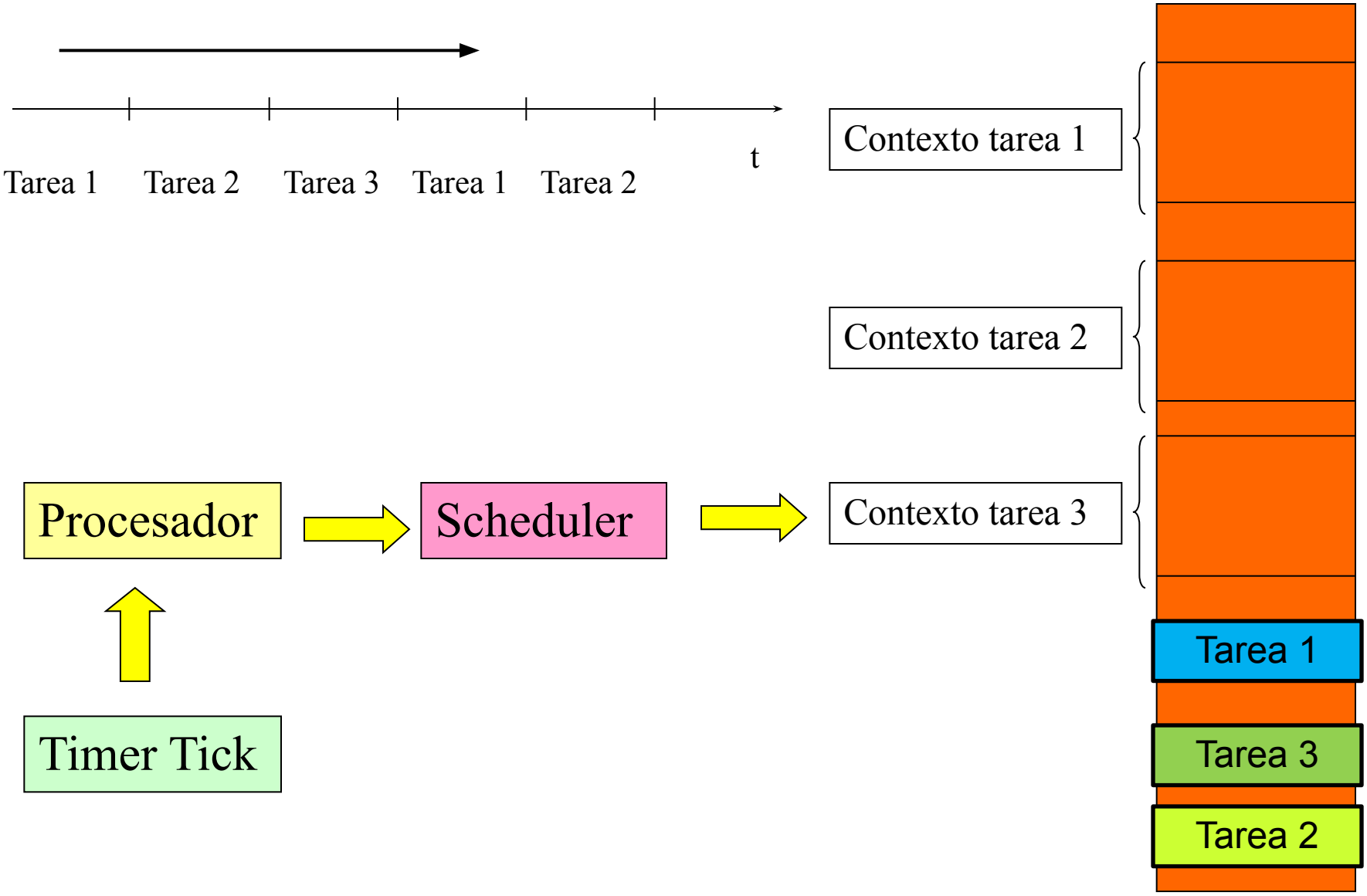
Veamos qué nos puede proveer el procesador sobre esto....

¿Cómo?

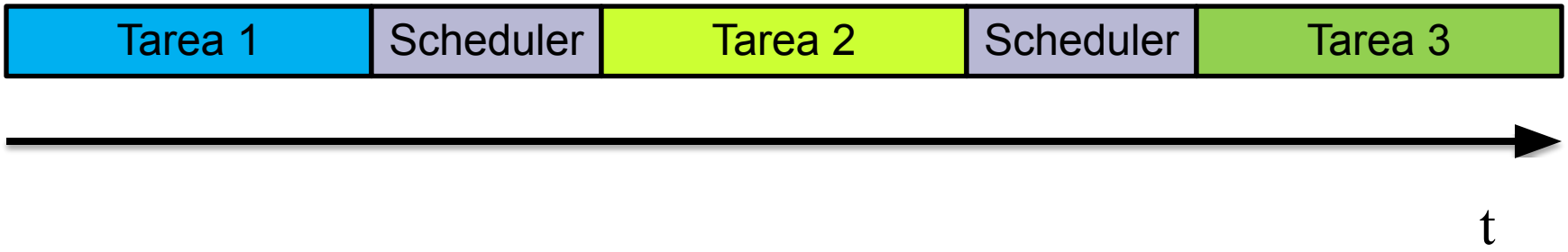
- Abstracción (mostrar un ambiente no físico)
- Interposición (interceptar acciones)

Modo Protegido

Modo protegido-Conmutación de tareas



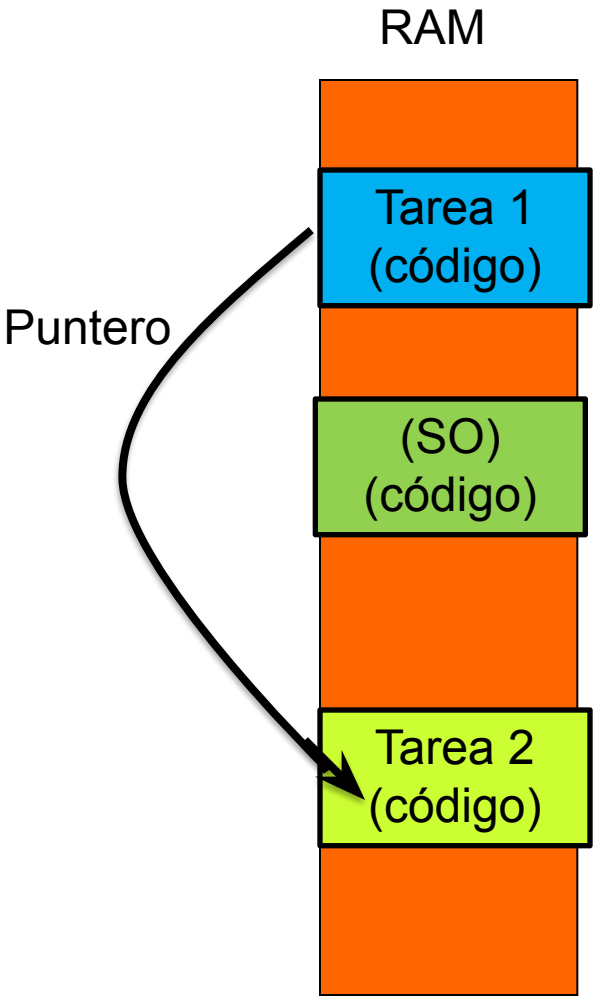
Modo protegido-Conmutación de tareas



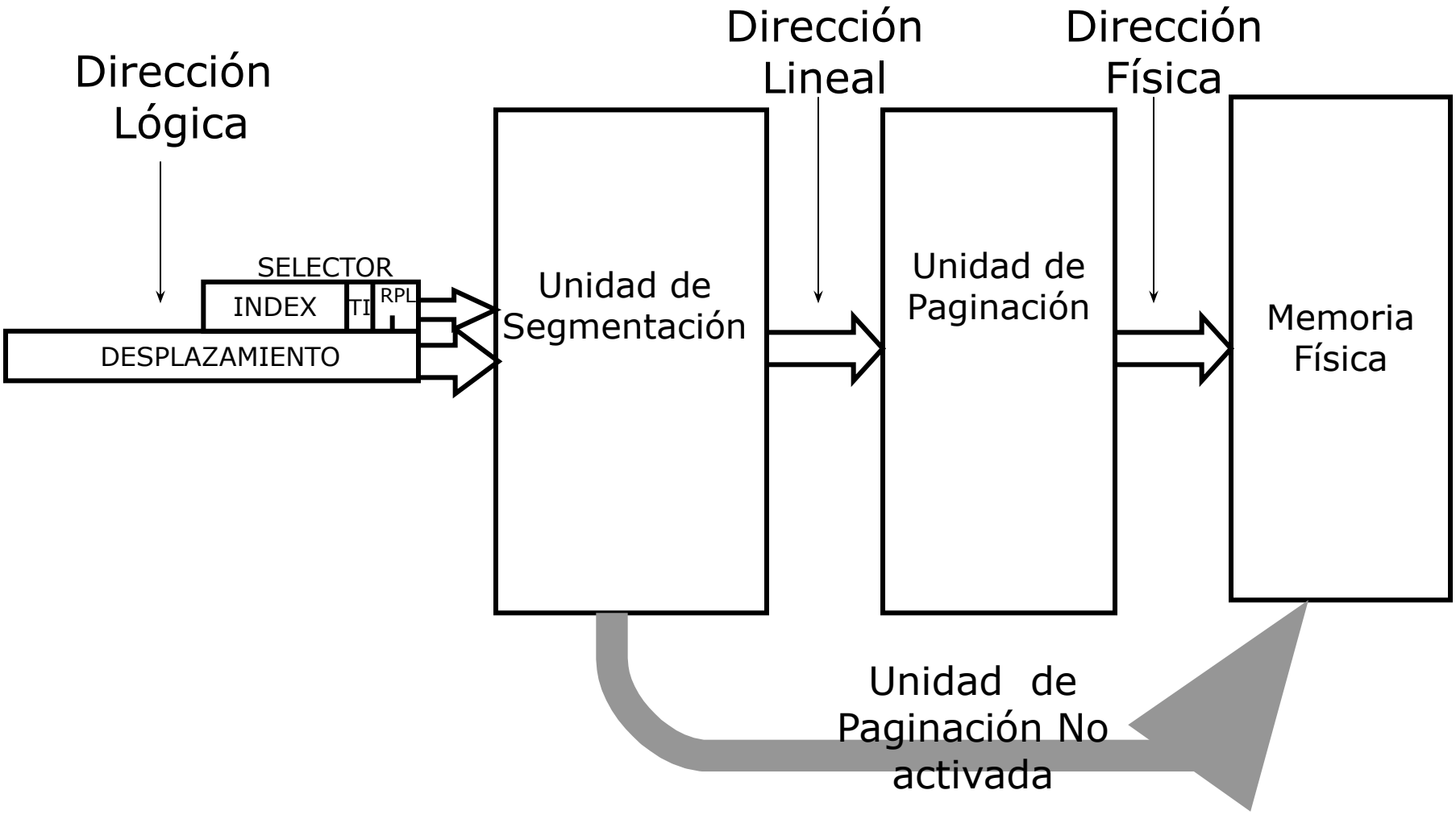
¿El SO es una tarea ?

Modo protegido- Protección de tareas

¿Cómo puede evitar el SO este acceso?



Modo protegido-MMU



Modo protegido-MMU

-La unidad de segmentación NO se puede deshabilitar.

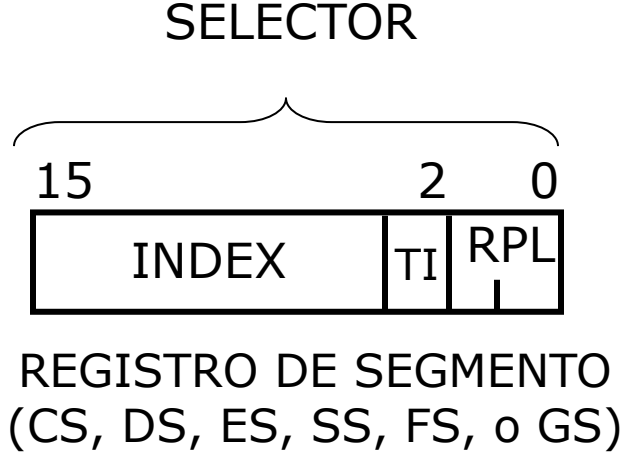
-La unidad de paginación SI se puede deshabilitar.

Debido a esta limitación de los procesadores Intel, algunos sistemas operativos eligen utilizar la memoria en modo "flat" (se verá luego) para no utilizar las reglas de segmentación pero si las de paginación.

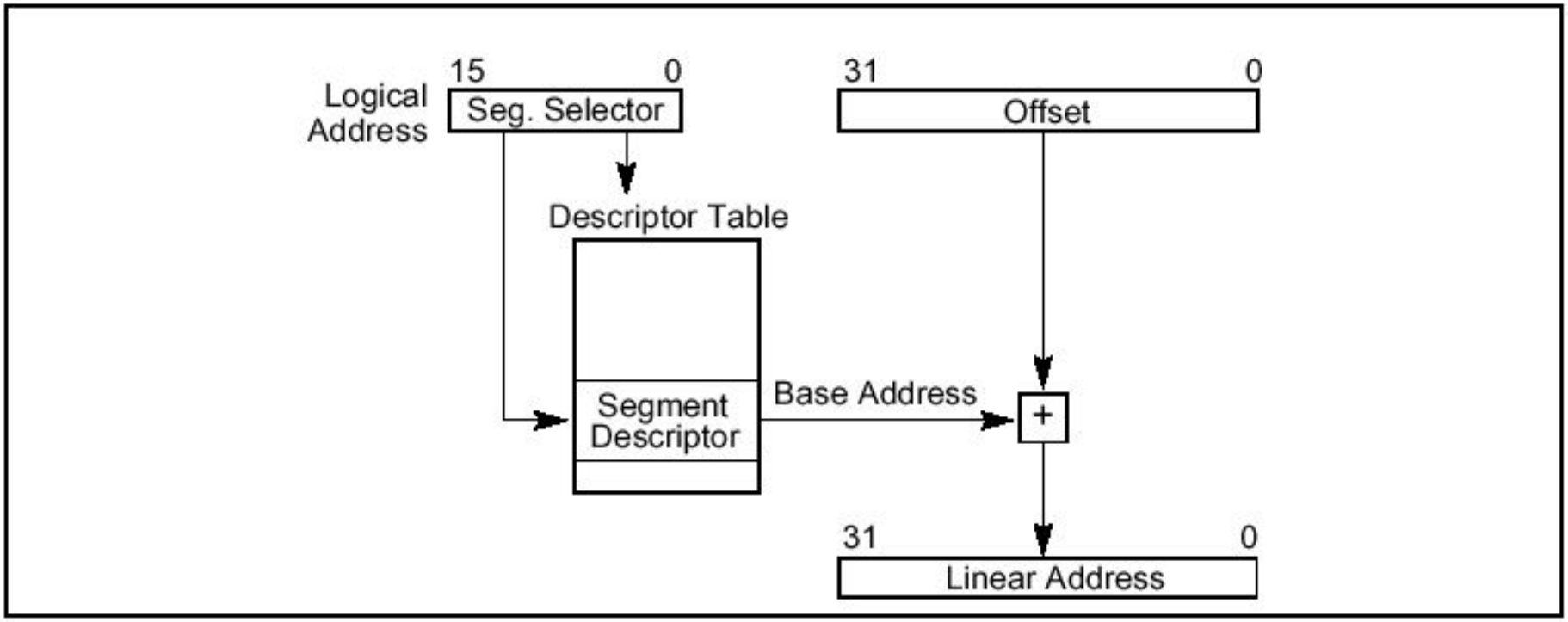
Dirección lógica

Ejemplo: DS = 20h y Offset = 1000h

Mov DS:[1000h], EAX



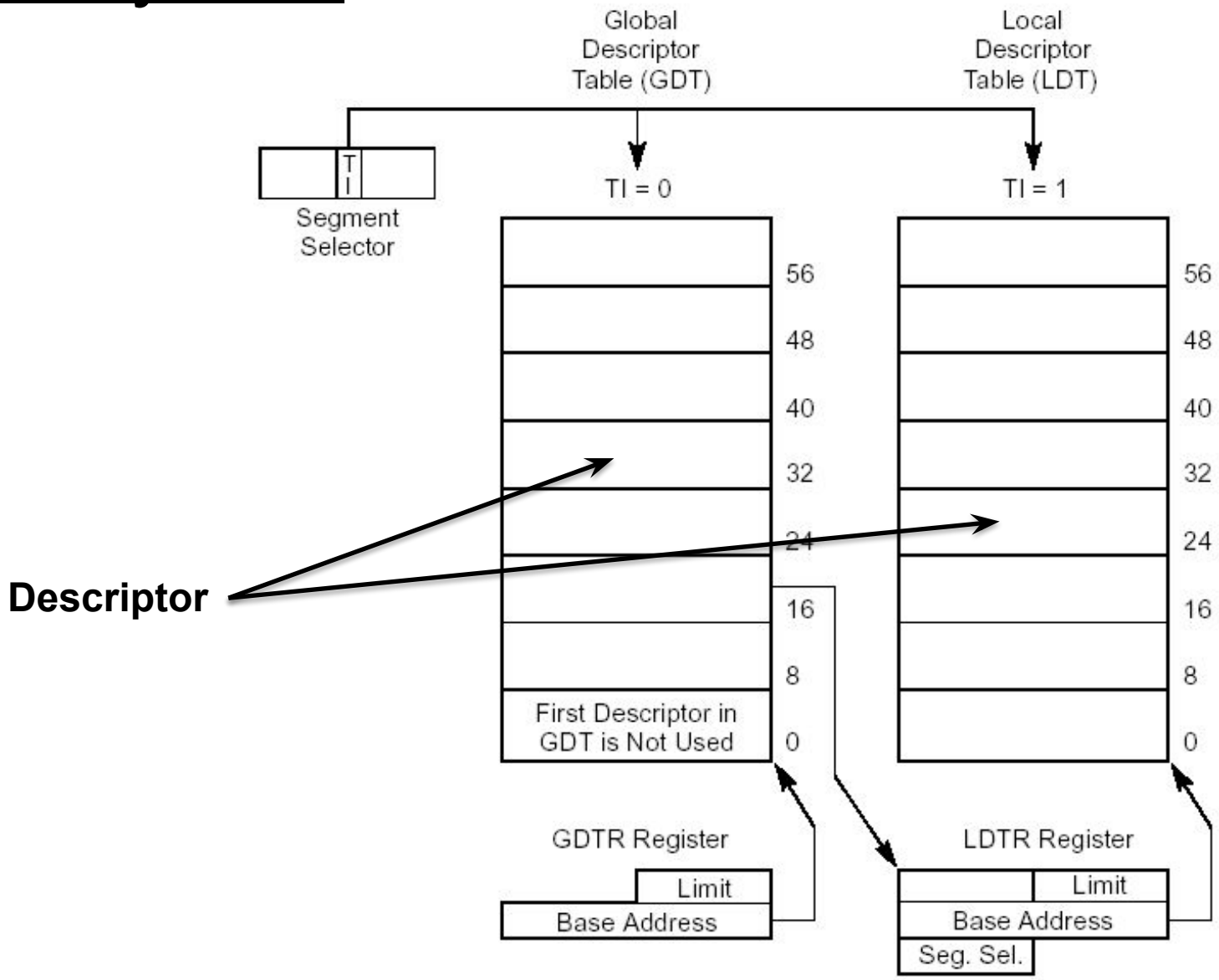
Dirección lógica a lineal



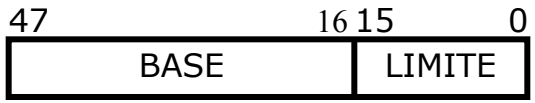
Ejemplo: DS = 20h y Offset = 1000h

Mov DS:[1000h], EAX

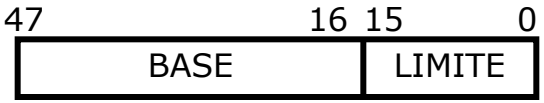
GDT y LDT


Global
Descriptor
Table (GDT)
Local
Descriptor
Table (LDT)
TI
Segment
Selector
TI = 0
TI = 1
56
48
40
32
24
16
8
0
First Descriptor in
GDT is Not Used
Descriptor
GDTR Register
Limit
Base Address
LDTR Register
Limit
Base Address
Seg. Sel.

Registros

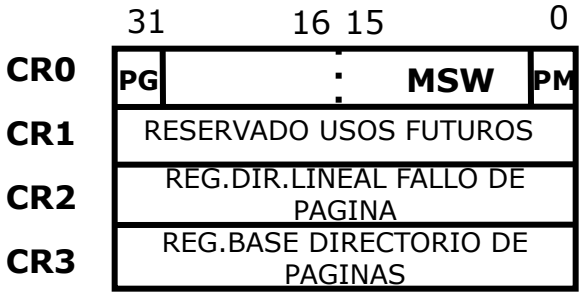


GDTR

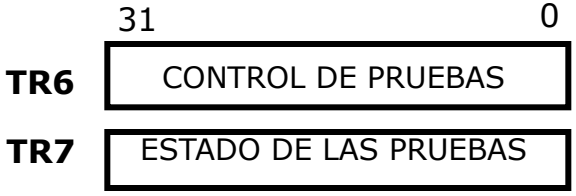


IDTR

REGISTROS DE DEBUGGING



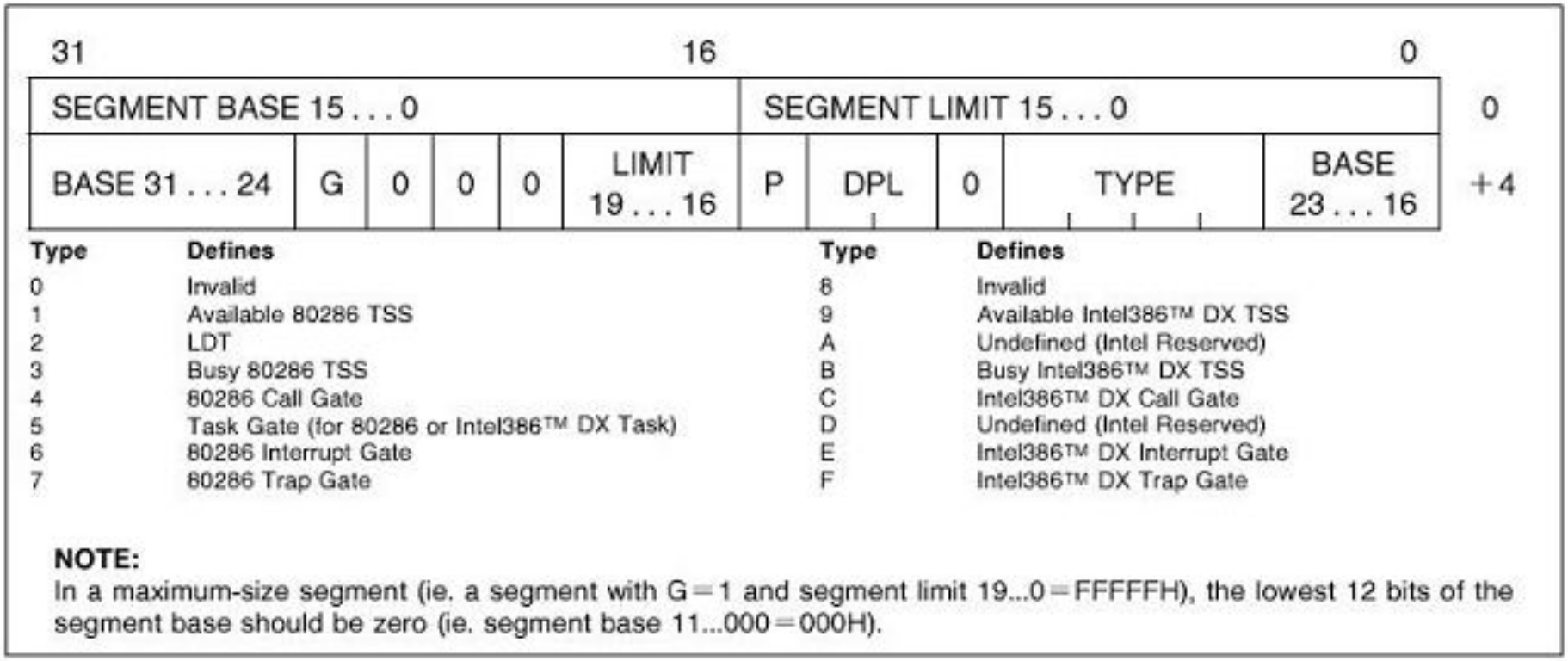
REGISTROS DE CONTROL



REGISTROS DE PRUEBA DE LA TLB

Descriptores

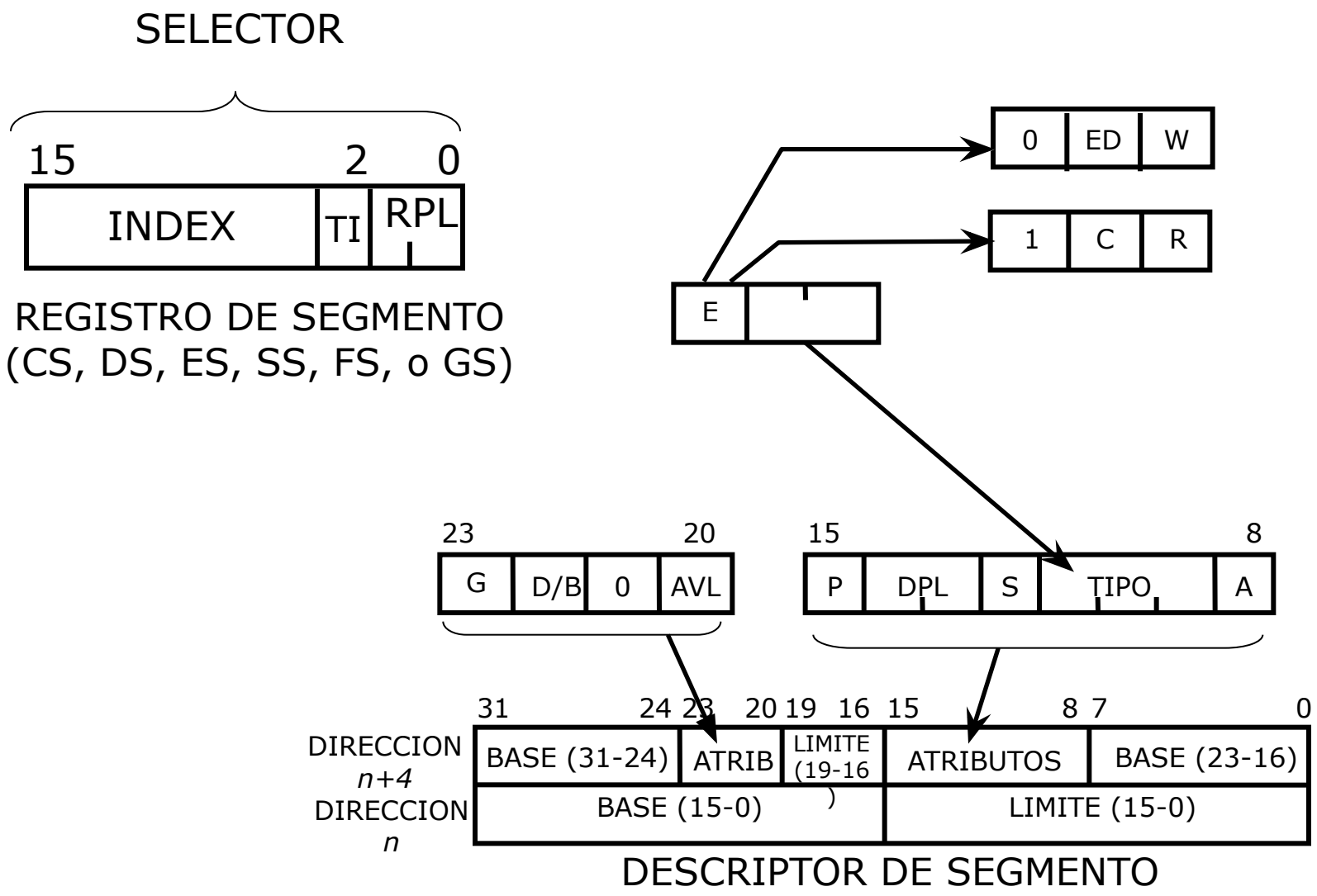
Veamos la estructura genérica de los descriptores de sistemas



Type	Defines	Type	Defines
0	Invalid	8	Invalid
1	Available 80286 TSS	9	Available Intel386™ DX TSS
2	LDT	A	Undefined (Intel Reserved)
3	Busy 80286 TSS	B	Busy Intel386™ DX TSS
4	80286 Call Gate	C	Intel386™ DX Call Gate
5	Task Gate (for 80286 or Intel386™ DX Task)	D	Undefined (Intel Reserved)
6	80286 Interrupt Gate	E	Intel386™ DX Interrupt Gate
7	80286 Trap Gate	F	Intel386™ DX Trap Gate

NOTE:
In a maximum-size segment (ie. a segment with G = 1 and segment limit 19...0 = FFFFFH), the lowest 12 bits of the segment base should be zero (ie. segment base 11...000 = 000H).

Descriptores de segmento



Atributos

- **P** (Bit de presencia)
  - Si P=1 el segmento esta cargado en la memoria física.
  - Si P=0 es segmento esta ausente.

- **DPL** (Nivel de privilegio)
  - Indica el nivel de privilegio del segmento
  - 0 = máximo privilegio, 3=minimo privilegio

- **S** (tipo de segmento)
  - Si S=1 se trata de un segmento normal (código datos o pila)
  - Si S=0 se trata de un segmento de sistema (puerta de llamada, TSS, etc).

Atributos

- **Tipo**: Es un campo de tres bits.
  - En el caso de un segmento normal
    - Si E: Ejecutable es 1, se trata de un segmento ejecutable
    - El siguiente bit (C: Ajustable o comforming) define si el segmento al ser accedido cambia su nivel de privilegio al nivel de privilegio de segmento que lo llamo (C=1)
    - El ultimo bit (R: Leíble) define si el segmento de código puede ser leído (R=1).
  - Si el bit E es 0 se trata de un segmento de datos
    - El segundo bit (ED: Expansión decreciente) define si se trata de un segmento de datos normal cuando ED=0, o de un segmento de pila cuando ED=1.
    - El tercer bit (W: Escribible) define si el segmento se puede escribir cuando W=1 o si es de solo lectura cuando W=0.

Dirección Lineal

Ejemplo: DS = 20h y Offset = 1000h

Mov DS:[1000h], EAX

DS= 0020h = 0000 0000 0010 0000 b

- Accede al Descriptor nro 4 de la GDT.
- Obtiene dirección base.
- (ej) Dirección base= 5600 0000h
- Luego suma offset de 1000 h
- Dirección lineal 5600 1000h

Descriptores

Cuando el bit S=0 se lo denomina “descriptor de sistema”.

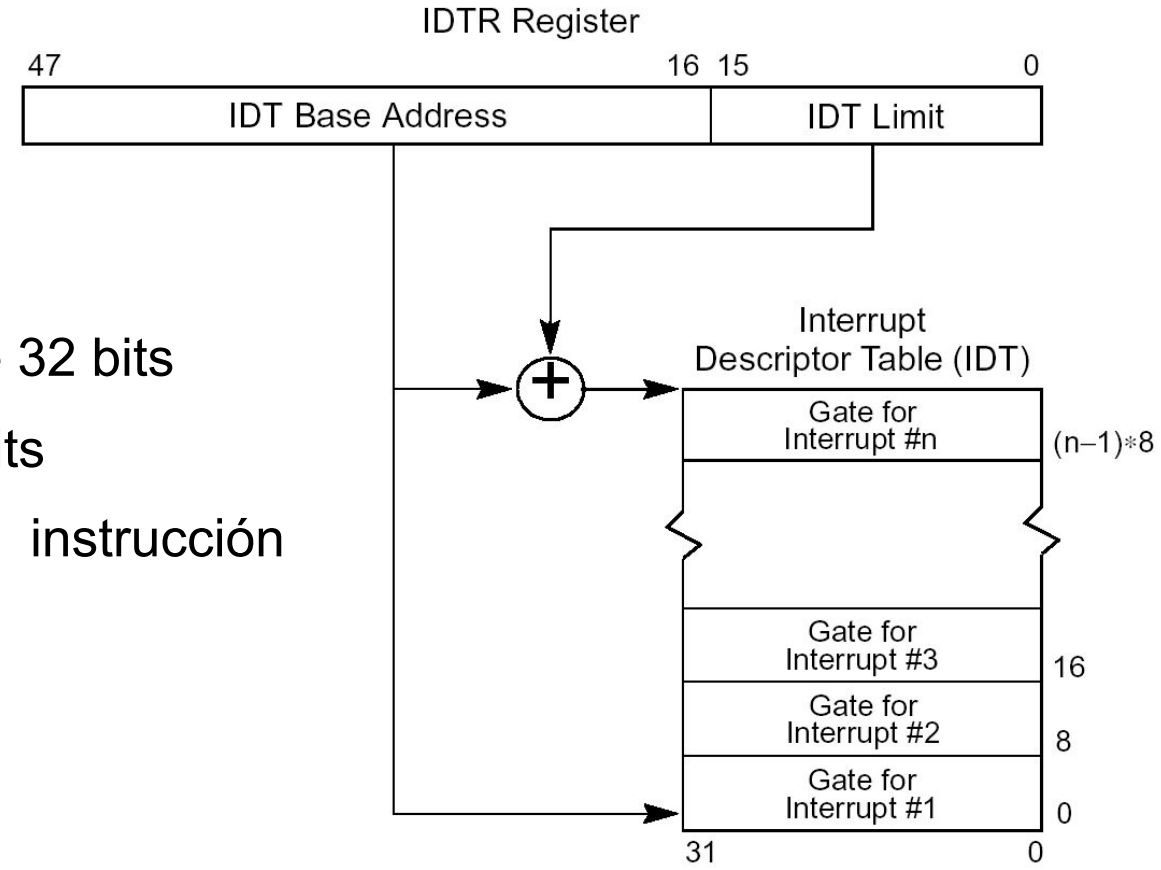
Existen diferentes tipos, los mas usuales son:

- Trap Gate (Puerta de excepción)
- Interrupt Gate (Puerta de interrupción)
- Task Gate

Carga de IDT

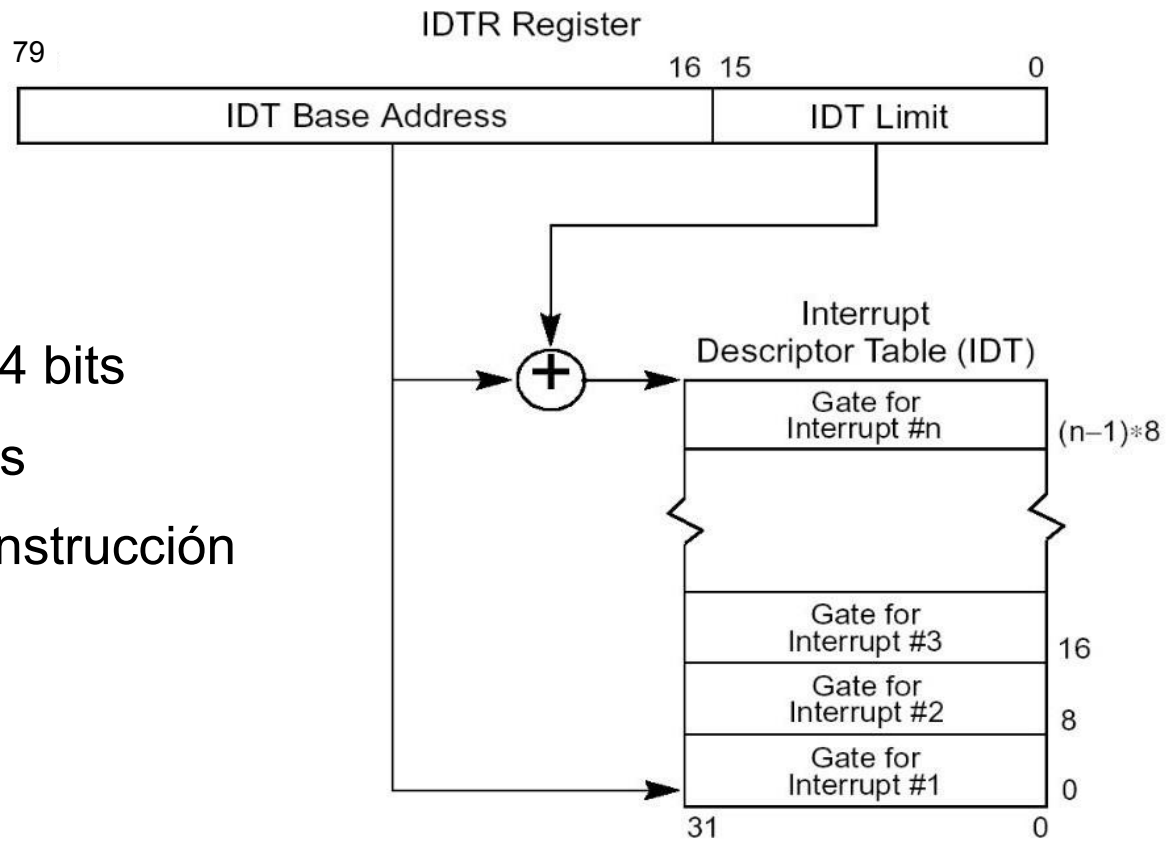
Interrupciones en Modo protegido (32 bits)

- IDT Base Address de 32 bits
- Descriptores de 64 bits
- IDTR se carga con la instrucción LIDT

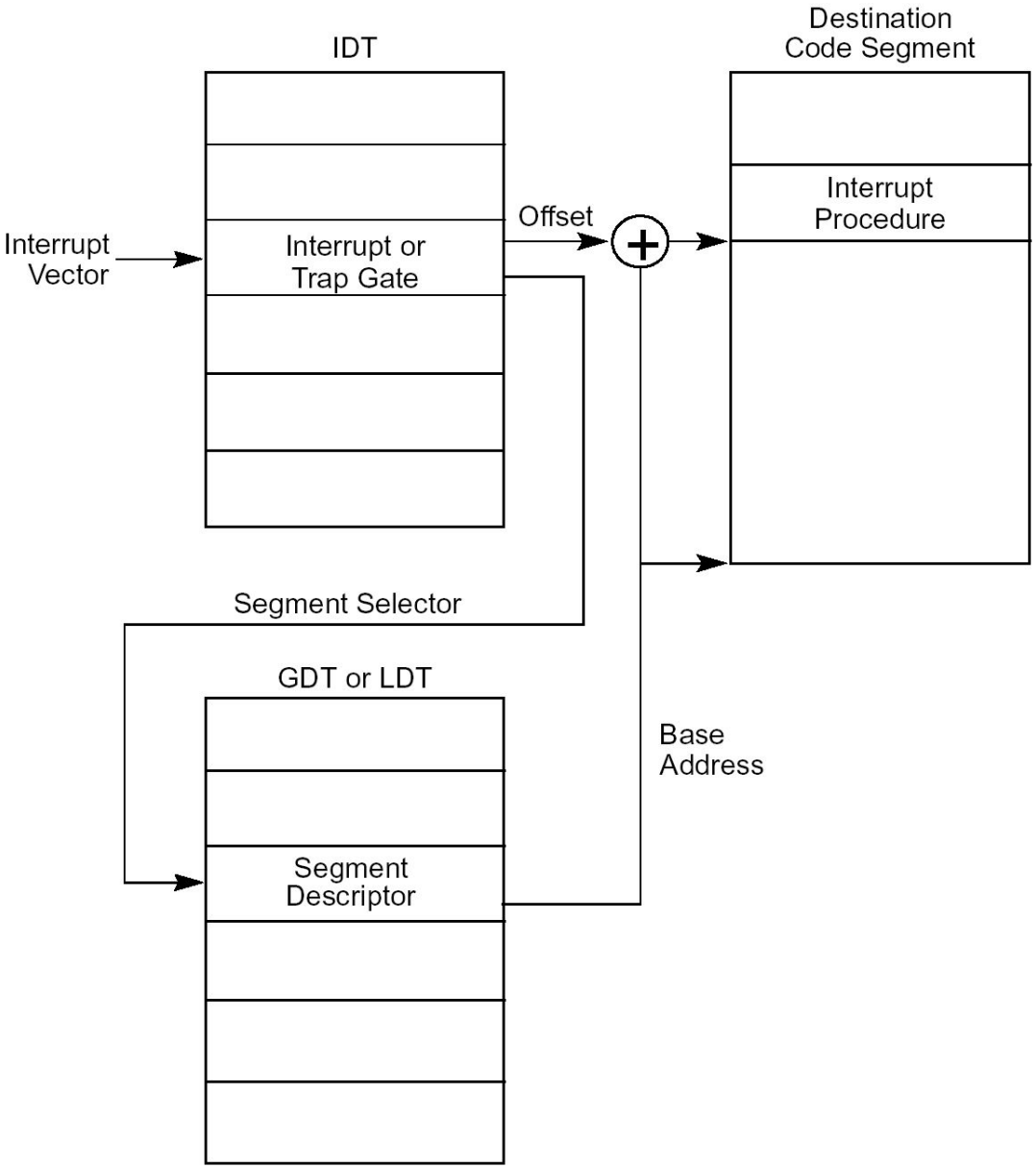


Interrupciones en Modo protegido (64 bits)

- IDT Base Address de 64 bits
- Descriptores de 128 bits
- IDTR se carga con la instrucción LIDT



Interrupciones en Modo protegido



Interrupciones en PRE_TPE

El código necesario para cargar su propia interrupción sólo debería involucrar:

1. Definir la rutina de atención de interrupción
2. Cargar la interrupción dentro de *load_idt* invocando a *setup_IDT_entry* pasandole el número de la interrupción y el puntero a la rutina de atención de interrupción
3. Si la interrupción es de hardware, dicha rutina debe enviar el EOI y deben habilitar el IRQ con la máscara correspondiente

Pueden hallar información más detallada en http://wiki.osdev.org/Interrupt_Descriptor_Table

Interrupciones en Modo protegido

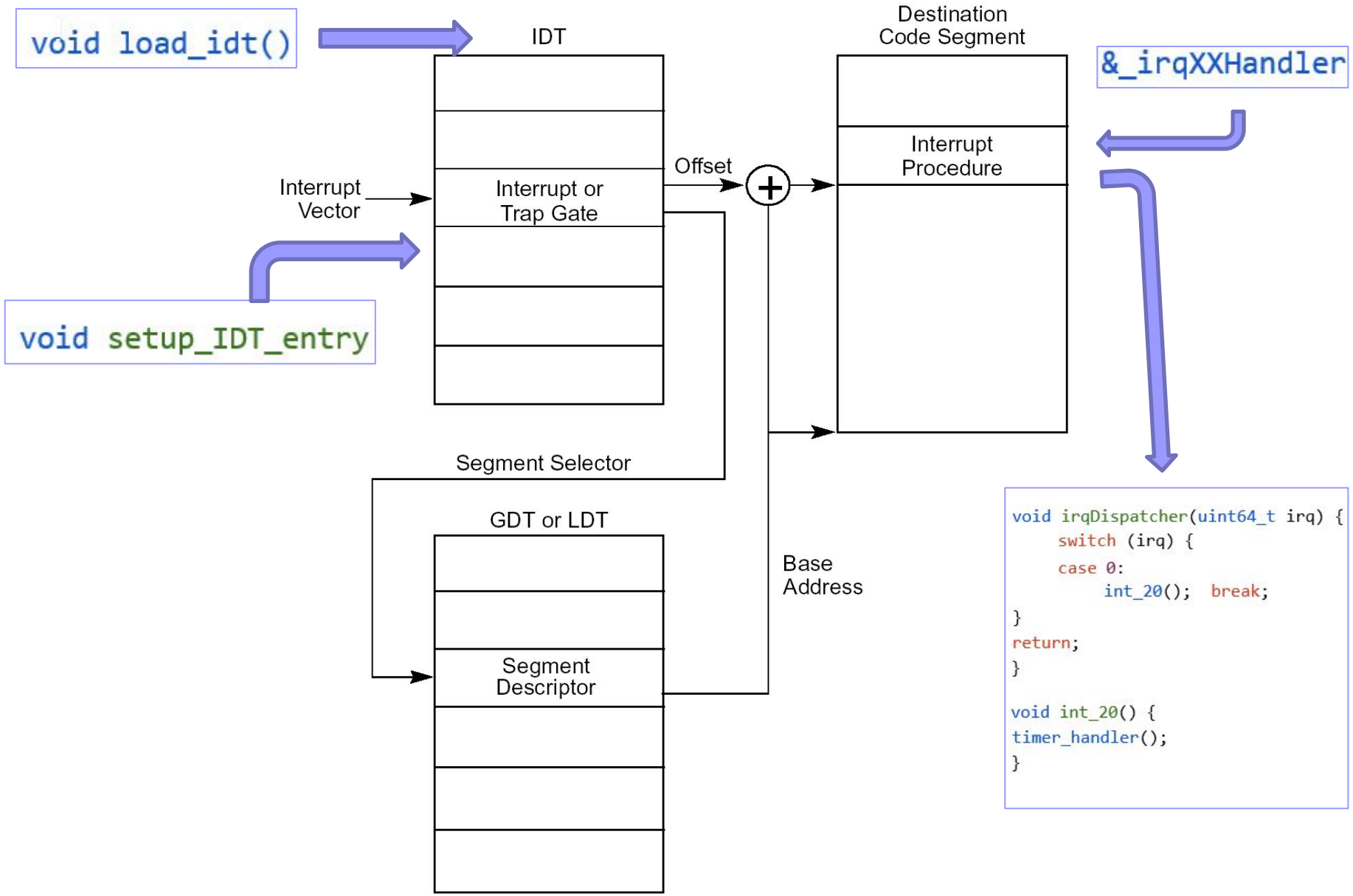
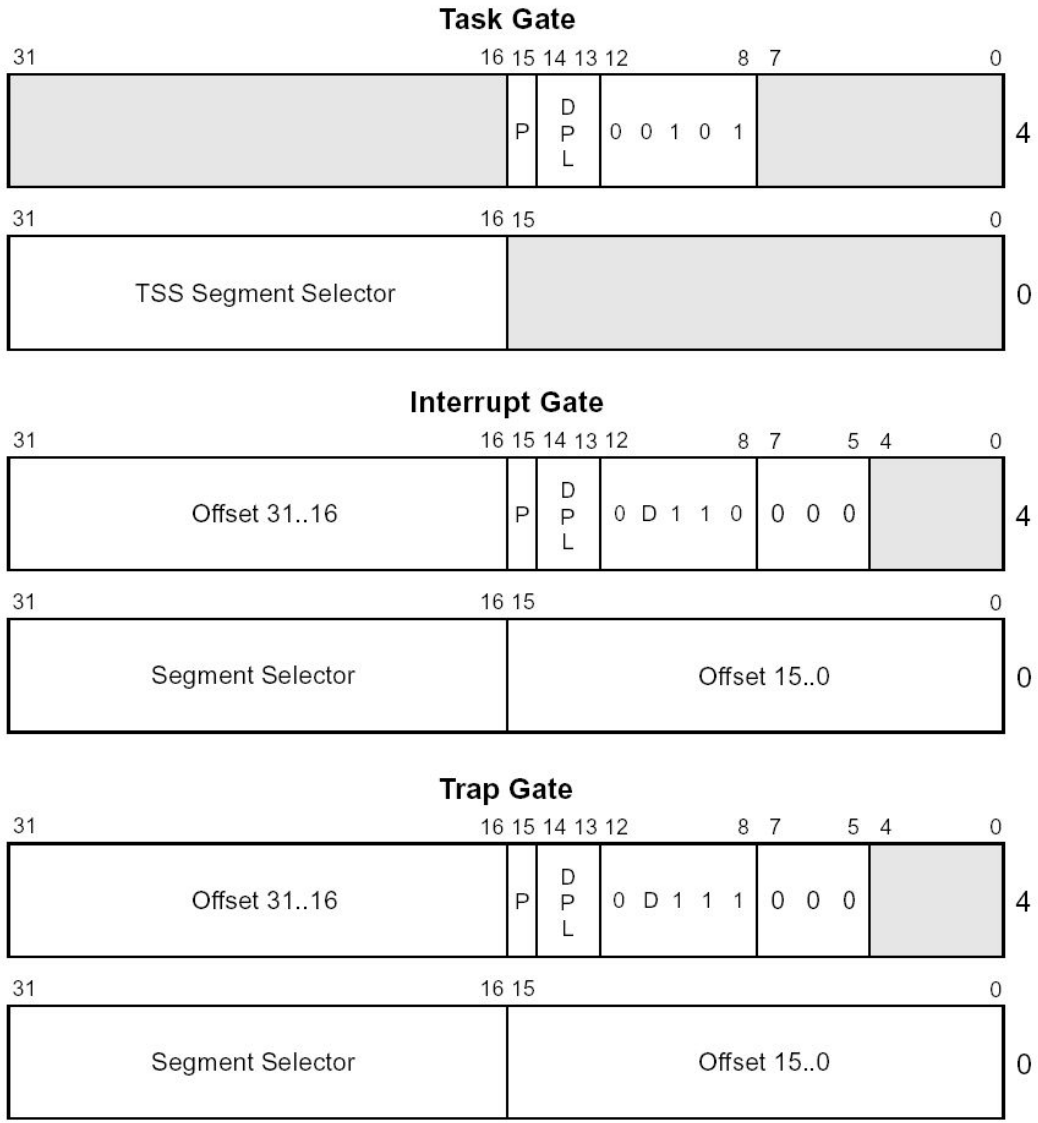


Tabla de excepciones

Vector No.	Mnemonic	Description	Type	Error Code	Source
0	#DE	Divide Error	Fault	No	DIV and IDIV instructions.
1	#DB	Debug	Fault/ Trap	No	Any code or data reference or the INT 1 instruction.
2	—	NMI Interrupt	Interrupt	No	Nonmaskable external interrupt.
3	#BP	Breakpoint	Trap	No	INT 3 instruction.
4	#OF	Overflow	Trap	No	INTO instruction.
5	#BR	BOUND Range Exceeded	Fault	No	BOUND instruction.
6	#UD	Invalid Opcode (Undefined Opcode)	Fault	No	UD2 instruction or reserved opcode.[1]
7	#NM	Device Not Available (No Math Coprocessor)	Fault	No	Floating-point or WAIT/FWAIT instruction.
8	#DF	Double Fault	Abort	Yes (Zero)	Any instruction that can generate an exception, an NMI, or an INTR.
9		Coprocessor Segment Overrun (reserved)	Fault	No	Floating-point instruction.[2]
10	#TS	Invalid TSS	Fault	Yes	Task switch or TSS access.
11	#NP	Segment Not Present	Fault	Yes	Loading segment registers or accessing system segments.
12	#SS	Stack-Segment Fault	Fault	Yes	Stack operations and SS register loads.
13	#GP	General Protection	Fault	Yes	Any memory reference and other protection checks.
14	#PF	Page Fault	Fault	Yes	Any memory reference.
15	—	(Intel reserved. Do not use.)		No	
16	#MF	x87 FPU Floating-Point Error (Math Fault)	Fault	No	x87 FPU floating-point or WAIT/FWAIT instruction.
17	#AC	Alignment Check	Fault	Yes (Zero)	Any data reference in memory.[3]
18	#MC	Machine Check	Abort	No	Error codes (if any) and source are model dependent.[4]
19	#XF	SIMD Floating-Point Exception	Fault	No	SSE and SSE2 floating-point instructions[5]
20-31	—	Intel reserved. Do not use.			
32-255	—	User Defined (Non-reserved) Interrupts	Interrupt		External interrupt or INT *n* instruction.

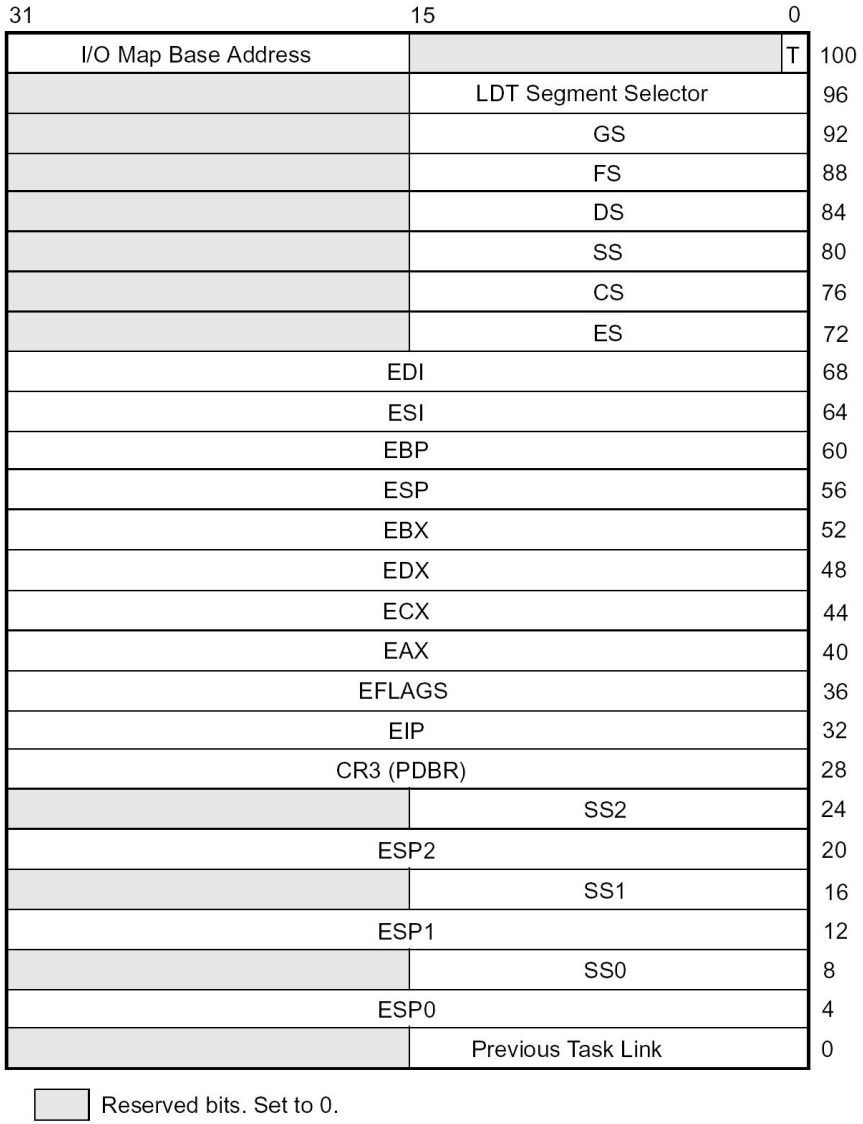
Tipos de descriptores en la IDT



Manejo de tareas

El procesador de Intel, nos da una herramienta para guardar el contexto de ejecución. Se lo denomina TSS (Task State Segment).

Tiene un tamaño mínimo de 100 bytes



Privilegios de E/S

El procesador provee 2 mecanismos:

- Campo de 2 bits IOPL en los EFLAGS. Que especifica el mínimo nivel de privilegio que se debe tener para poder usar instrucciones de Entrada/Salida.

- Mapa de bits de E/S en el TSS.

Las instrucciones “sensibles” son:

- **IN (Input)**
- **OUT (Output)**
- **INS (Input String)**
- **OUTS (Output String)**
- **Cli (Clear Interrupt)**
- **Sti (Set Interrupt)**

Para ejecutarlas el nivel de privilegio debe ser igual o menor que IOPL.