IDT y Syscalls en JOS

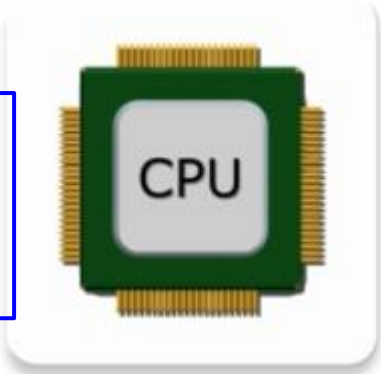
Sistemas Operativos - FIUBA

Interrupciones en x86

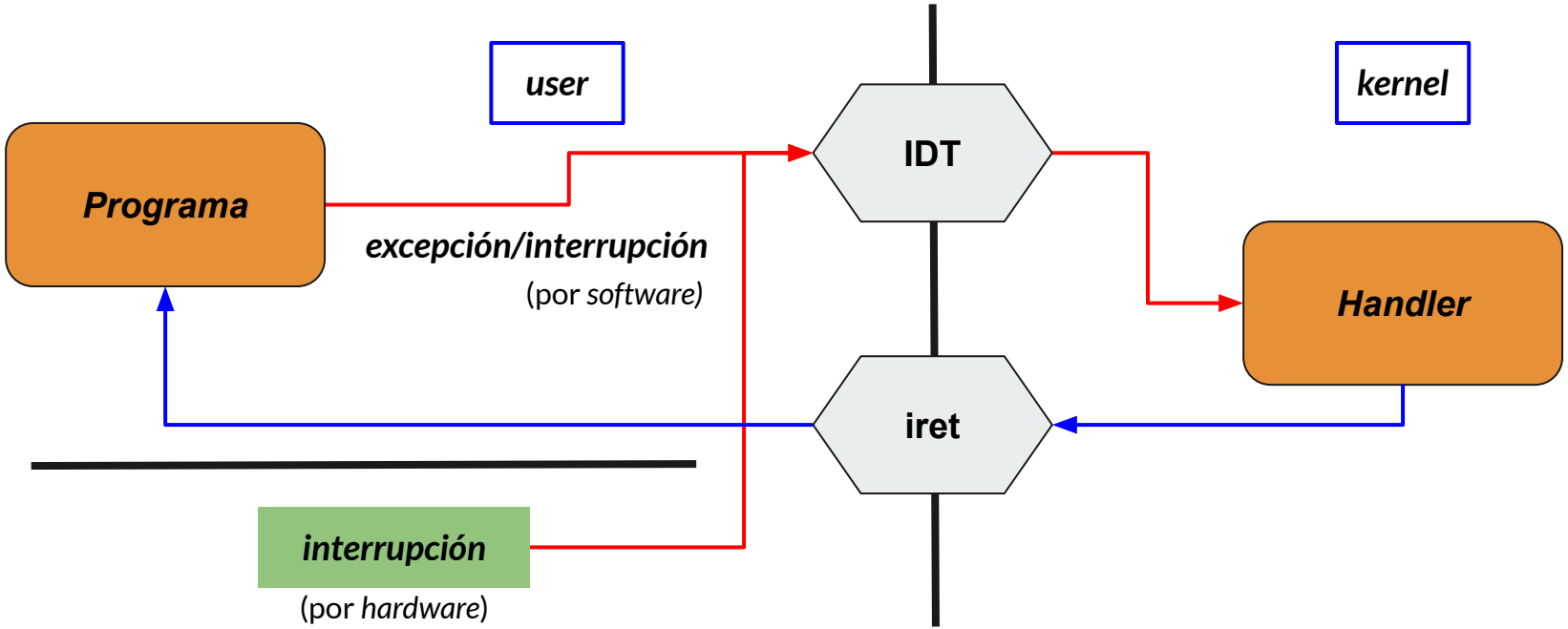
Interrupciones y Excepciones

Interrupciones → Son generadas debido a señales externas de dispositivos de hardware, o ejecutadas por software

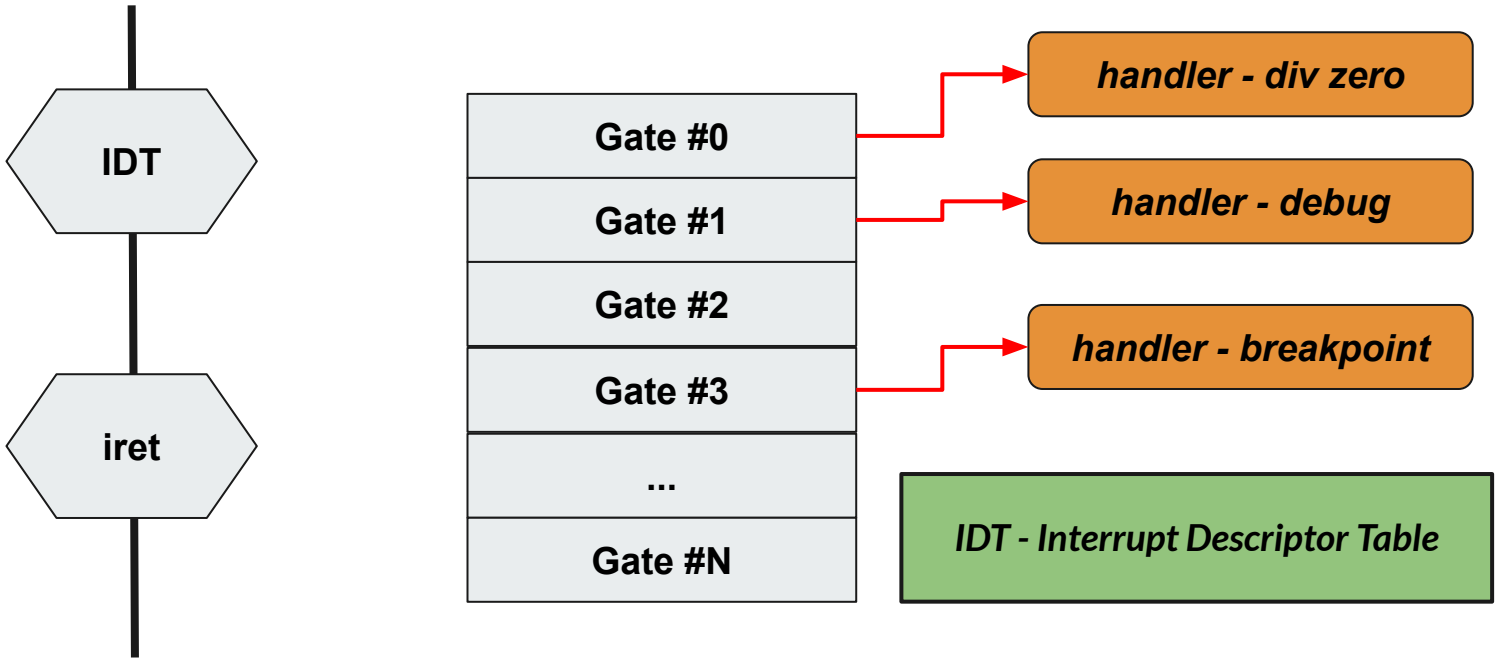
Excepciones → Ocurren cuando el CPU detecta un error en la ejecución de una instrucción



Interrupciones y Excepciones



Interrupciones y Excepciones



IDT - Interrupt Descriptor Table

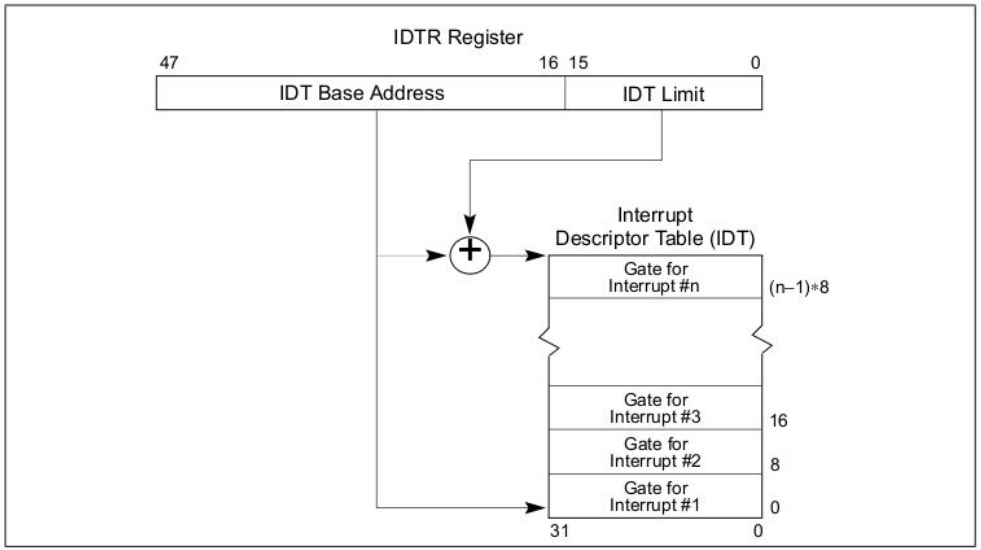


Figure 6-1. Relationship of the IDTR and IDT

Fuente: Intel Vol 3A - C-6.10

IDT - Interrupt Descriptors

Interrupt Gates

istrap = 0

Trap Gates (alias: Exceptions)

istrap = 1

Muy IMPORTANTE!!

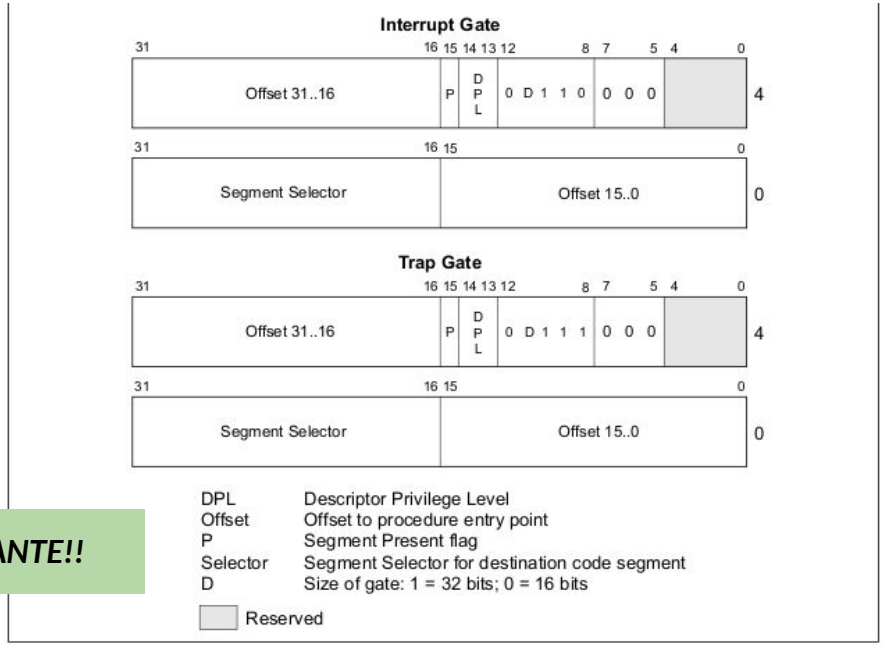


Figure 6-2. IDT Gate Descriptors

Fuente: Intel Vol 3A - C-6.11

IDT - Interrupt Call Flow

- Se produce un cambio de **stack.** ¿A cuál? Y ¿de dónde se obtiene?
- Se hace un *push* en el stack de:
  - SS
  - ESP
  - EFLAGS
  - CS
  - EIP
- Si la excepción generó un **código de error** se realiza un *push* adicional, ¿por qué?

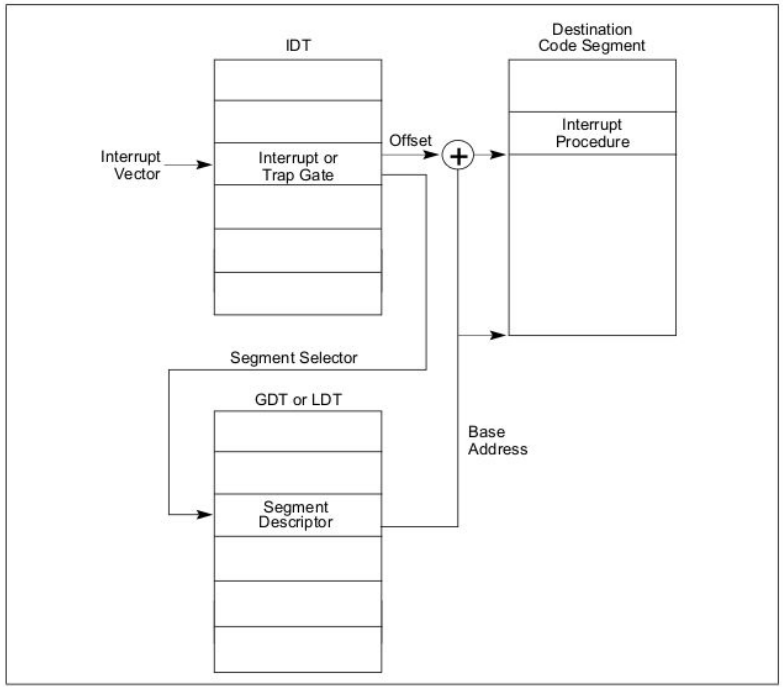


Figure 6-3. Interrupt Procedure Call

Fuente: Intel Vol 3A - C-6.12.1

IDT - Interrupt Call Flow

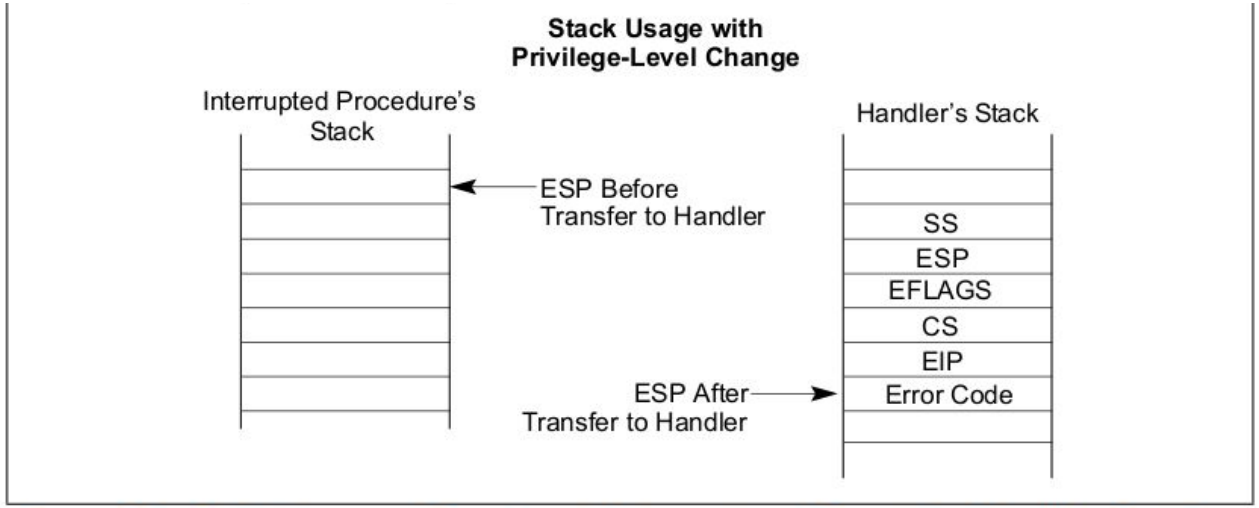


Figure 6-4. Stack Usage on Transfers to Interrupt and Exception-Handling Routines

Fuente: Intel Vol 3A - C-6.12.1

IDT - Exceptions Table

Table 6-1. Protected-Mode Exceptions and Interrupts

Vector	Mne-monic	Description	Type	Error Code	Source
0	#DE	Divide Error	Fault	No	DIV and IDIV instructions.
1	#DB	Debug Exception	Fault/ Trap	No	Instruction, data, and I/O breakpoints; single-step; and others.
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	UD instruction or reserved opcode.
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.[1]
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.

Fuente: Intel Vol 3A - C-6.3.1

Interrupciones en JOS

IDT - Syscall Flow