

## Ejercicio 1: (2 puntos)

V o F. Sin justificar

1. El pin IO/M es controlado por las instrucciones In, OUT.

**VERDADERO**

2. Cuando hay una falta de página el procesador busca el puntero de la excepción en la IDT.

**VERDADERO**

Modo protegido: "Las excepciones que se lanzan en la unidad de segmentación y de paginación por causa del bit *p* son distintas. Una es "segment not present" y la otra es "page not present"."

Como cualquier excepción, el procesador busca el puntero a la rutina en la IDT.

3. En una arquitectura de 64 los registros utilizados para el pasado de parámetros están definidos.

**VERDADERO**

4. En el registro CR3 están indicados los permisos de quién puede acceder a la tabla de directorios.

**FALSO: esta únicamente la dirección del directorio**

5. Una vez desactivada la segmentación, se puede usar solo la paginación.

**FALSO** : En modo protegido, no se puede desactivar la segmentación. Por otro lado, si es posible iniciar el procesador en "modo flat". En este modo, se configura la unidad de segmentación para que *todos los segmentos abarquen todo el espacio de direcciones*, haciendo que las direcciones lógicas coincidan con las direcciones lineales. De esta manera se "bypassee" la unidad de segmentación, y puede usarse "únicamente" la unidad de paginación.

6. El timer tick es un circuito integrado que se encuentra en la mother y está conectado directamente al PIC. **VERDADERO**
7. La función stack-chk-fail revisa toda la pila para verificar que nadie la haya alterado.

**FALSO:** revisa unicamente que no se haya alterado el canary

8. Los circuitos complejos de compuertas no son buenos para sistemas computacionales o de cálculo exacto.

**VERDADERO:** *es necesario un clock para que funcionen*

9. Intel proporciona un mecanismo para que el SO indique en qué sectores del disco se guardó la página.

**FALSO:** Intel proporciona la MMU, en la que se encuentran la unidad de segmentación y paginación. La unidad de paginación **únicamente** tiene la capacidad de traducir direcciones lineales a físicas, accediendo a las tablas de página y luego a las páginas, por medio de la información que obtiene al traducir las direcciones lineales. Luego, es el SO quien se encarga de administrar los sectores del disco donde se guardan las tablas de página y las páginas.

10. Los procesadores de Intel acceden a memoria con el mismo ancho del bus de datos pero usan direccionamiento de un byte.

**VERDADERO** Usan direccionamiento de un byte para mantener la retrocompatibilidad

## Ejercicio 2: (4 puntos)

### Justificar y explicar las afirmaciones:

1. Según Wikipedia: "Jazelle DBX (Direct Bytecode eXecution) es una extensión que permite a algunos procesadores ARM ejecutar bytecode Java en hardware como un tercer estado de ejecución junto con los modos ARM y Thumb.

Los procesadores ARM ofrecen tres estados de ejecución: ARM, THUMB y JAZELL. ARM es el estado de ejecución tradicional en donde se tiene acceso al set completo de instrucciones de 32 bits ARM. THUMB es un modo alternativo "comprimido" donde se usan instrucciones de 16 bits. Este modo permite ahorrar memoria y ofrece mejor rendimiento en algunas situaciones, pero ofrece un set de instrucciones reducido. Por ultimo, JAZELL permite ejecutar el bytecode de java (codigo "compilado" de java) directamente en el procesador, sin la necesidad de la JVM. Aun asi, para algunas aplicaciones es necesaria una combinación entre corre bytecode de manera nativa y la JVM.

2. La funcionalidad Jazelle fue especificada en la arquitectura ARMv5TEJ y el primer procesador con tecnología Jazelle fue el ARM926EJ-S. Jazelle se denota con una "J" añadida al nombre de la CPU, excepto en los núcleos posteriores a la versión v5 donde es necesario (aunque solo en forma trivial) para la conformidad de la arquitectura.
3. La etapa "fetch" puede ocasionar una demora si la etapa "execute" intenta usar los mismos recursos.

## Ejercicio 3 (4 puntos)

### Multiple choice: (Vale más de una)

1. Una interrupción NMI busca la rutina de atención en la posición:
  - a. 10h
  - b. 20h
  - c. 21h
  - **d. Ninguna de las anteriores.**

El cpu busca las rutinas de atencion para las NMI en la direccion INT 2h.

2. En un programa compilado por gcc, después de realizar un CALL, el registro ESP apunta a:
  - a. El canary
  - b. Al EBP
  - c. Al ESP anterior
  - **d. Ninguna de las anteriores.**

Ninguna, queda apuntando al RET de la funcion anterior (siempre!!!)

3. El procesador revisa los permisos cuando:
  - **a. Accede a un segmento**
  - **b. Hace una interrupción (modo protegido IDT)**
  - **c. Accede una página - estan los permisos en los bits**
  - d. Ninguna de las anteriores.

a) La direccion logica se parte en segment selector y offset. El CPU va la GDT o LDT, dependiendo del bit **TI** en el segment selector. Luego, suma el offset al comienzo de esa tabla y obtiene el *segment descriptor*. En el segment descriptor, estan contenidos los permisos necesarios para acceder a ese segmento (los bits **DPL** - descriptor permission level). Antes de realizar el acceso, el cpu compara los permisos necesarios del DPL con los permisos del contexto actual, contenidos los registros de segmento de codigo (CS), dados por los bits **CPL (current permission level)**.

b) En modo protegido, para conseguir la rutina de excepcion es necesario pasar por la unidad de segmentacion. Las excepciones tienen segment descriptors unicos (uno para cada tipo de excepcion, fault, trap o abort). Antes de saltar a la rutina, el CPU compara los bits CPL (current permission level) de los registros de CS con los bits DPL del segment descriptor de la excepcion. El CPU puede permitir que se ejecute una rutina en situaciones donde el  $CPL > DPL$  (O sea se tienen **menos permisos** que los necesarios)\*\* dependiendo de la fuente de la interrupción (hardware, software o excepcion); Una interrupcion de hardware, por ejemplo, puede cambiar el nivel de privilegios.

\*\*Recordar que los permisos van de 0 (KERNEL/SO) a 3 (USUARIO)

c) Como en segmentacion, la unidad de paginacion maneja permisos para el acceso a paginas por medio del bit **P** en la direccion lineal **chequear no se si es asi**

4. Para la utilización de instrucciones condicionales en ARM:

- a. Es necesario THUMB
- b. Es necesario Jazell
- c. Es necesario TDMI
- **d. Ninguna de las anteriores.**

**REPASAR ESTO - se que las instrucciones condicionales siempre estan**

5. Para los procesadores multicore, las interrupciones son:

- **a. Individuales en cada procesador**
- **b. Centralizadas por APIC**
- c. Centralizadas por 2 PIC
- d. Ninguna de las anteriores.

Individuales en c/procesador por los LOCAL APICS, y centralizadas por I/O APIC. Este ultimo se conecta a los periféricos y a todos los nucleos, y decide que interrupcion debe enviar a cada uno.

6. La cantidad de IDT máximas en un momento indicado son:

- **a. Una**
- b. Dos
- c. Tres
- d. Ninguna de las anteriores.

7. En los procesadores ARM:

- a. Todos los periféricos están mapeados en memoria y todas las operaciones son condicionales.
- **b. Todos los periféricos están mapeados en memoria y algunas operaciones son opcionales.**
- c. Algunos periféricos están mapeados en memoria y algunas operaciones son condicionales.
- d. Ninguna de las anteriores.

8. Las RAM que se utilizan en las PC son:

- **a. DRAM ok!!**
- b. SRAM
- c. FRAM
- d. Ninguna de las anteriores.

Se utiliza DRAM (DYNAMIC RAM), la cual necesita ser refrescada constantemente para mantener los datos. Es un tipo de memoria menos complejo y mas barato que la SRAM, aunque mas lento, por lo que es la opcion preferida de memoria en las PC. La SRAM es mas compleja, mas cara y mas rapida que la DRAM, se usa para la memoria cache.

---

## Final 2018 2do cuatrimestre primer llamado

### V o F

1. Las rutinas de interrupción en BIOS no dejan de existir al instalarse el SO.

**FALSO - El SO sobrescribe la IDT con sus propias interrupciones**

2. Frente a falta de página se genera una interrupción.

Modo protegido: "Las excepciones que se lanzan en la unidad de segmentación y de paginación por causa del bit *p* son distintas. Una es "segment not present" y la otra es "page not present"."

3. En 64 bits, los parámetros en C pasan tanto por los registros como la pila.

**VERDADERO - Primero por registros, si se acaban por la pila**

4. IOPL contiene el nivel de privilegio de quien puede acceder a las instrucciones de E/S.

**VERDADERO**: Los bits IOPL en el registro de EFLAGS contienen el nivel de privilegio necesario para ejecutar instrucciones de E/S - Esta dado por su nombre: **Input Output Privilege Level**. Estos bits pueden ser modificados por código ejecutándose con CPL (Current privilege level) 0, kernel/SO.

5. Con paginación habilitada, dejan de usarse las direcciones físicas por las lineales.

**VERDADERO**: Al habilitarse la paginación, las direcciones lógicas son convertidas por la unidad de segmentación en direcciones lineales, para luego convertirse en direcciones físicas por la unidad de paginación.

6. El timer tick es la salida de un contador en motherboard.

**VERDADERO**: El timer tick es un integrado en la motherboard el cual esta conectado al IRQ0 del Master PIC, interrumpiendolo cada 55ms.

7. La función stack-chk-fail revisa toda la pila para verificar que nadie la haya alterado.

**FALSO**: Solo chequea que no se haya modificado el canary

8. Los circuitos complejos de compuertas no son buenos para sistemas computacionales o de cálculo exacto.

**VERDADERO**: Necesitan un clock para funcionar.

9. Intel proporciona un mecanismo para que el SO indique en qué sectores del disco se guardó la página.

**FALSO:** Intel proporciona la MMU, compuesta por la unidad de segmentación y la unidad de paginación. La unidad de paginación tiene la capacidad de traducir direcciones lineales a físicas para obtener los datos necesarios, pero es el SO quien se encarga de ubicar en disco (y memoria) la tabla de página y las páginas.

10. Los procesadores de Intel acceden a memoria con el mismo ancho del bus de datos pero usan direccionamiento de un byte.

**VERDADERO:** Intel aprovecha el Bus de Datos entero para realizar accesos a memoria, pero mantienen el direccionamiento de un byte para mantener retrocompatibilidad.

## Justificar las afirmaciones

1. *Existen direcciones numéricamente iguales en mapa de memoria y mapa de E/S que habilitan dispositivos distintos.*

Asumiendo que estamos en un procesador INTEL: Esto se debe a que el mapa de E/S se activa con instrucciones distintas que el mapa de memoria, las cuales activan la patita de I/O. El circuito decodificador debe armarse con esta patita de I/O en mente, creando así un segundo mapa de memoria, el “mapa de entrada y salida”, independiente al original, e idéntico en direcciones y tamaño al mapa de memoria. Las instrucciones IN y OUT activan dispositivos del mapa de E/S, mientras que, por ejemplo, MOV activa dispositivos del mapa de memoria.

2. *Existen 2 arquitecturas de 64 bits de Intel.*

Existen 2 arquitecturas de 64 bits de Intel: IA-64 y x86\_64.

IA-64 Utiliza el conjunto de instrucciones EPIC (Explicitly Parallel Instruction Computing), que es significativamente diferente de la arquitectura x86 tradicional. Esta arquitectura no es compatible de manera nativa con las aplicaciones x86, aunque puede ejecutar aplicaciones x86 mediante emulación.

Por otro lado, x86\_64 tiene un set de instrucciones compatible con el de la arquitectura x86 intel, lo que logra que se puedan ejecutar programas escritos para x86 de manera nativa. Los registros de 64 bits son extensiones de los de 32 bits, y comparten el set de instrucciones.

## Multiple-Choice

1. La entrada INTR del micro puede ser enmascarada con:
  - retf
  - cli

- sti
- Ninguna de las anteriores

**CLI “Clear interruptions” establece el flag de interrupciones en 0, lo que logra que las interrupciones que llegan por INTR sean ignoradas. Las interrupciones de INTR son las enmascarables. Las NMI no son enmascarables.**

2. Luego de realizar CALL para correr una función compilada en gcc, el registro EBP:
  - **Es igual al ESP (armado de stack frame)**
  - Apunta a la dirección de retorno
  - Mantiene el valor
  - Ninguna de las anteriores
3. El modelo de actualización que escribe en caché y RAM al mismo tiempo se llama:
  - Write late
  - Write back
  - Write through
  - Ninguna de las anteriores

## **APRENDER MEMORIA CACHE**

4. La dirección lineal puede ser:
  - **Igual a la lógica: en modo flat**
  - Igual al selector
  - **Igual a la física: si se desactiva la paginacion**
  - Ninguna de las anteriores

*Dirección lógica —(segmentacion) —> dirección lineal*

*— (paginacion) —> dirección física*

5. La cantidad de IDT máximas en un momento indicado son:
  - **1**
  - 2
  - 3
  - Ninguna de las anteriores

## **Siempre hay exactamente una IDT**

6. Para los procesadores multicore, las interrupciones son:
  - **Individuales en cada procesador**
  - **Centralizadas por APIC**
  - Centralizadas por 2 PIC
  - Ninguna de las anteriores

**En procesadores multi-core, las interrupciones son individuales para cada procesador, pero centralizadas por el APIC.**

7. En un micro con 32 buses de address, si tengo un dispositivo desde FEDEF000h hasta FEDEFFFFh necesito \_\_\_\_\_ decodificadores de 4 entradas:
- ☐ 4
  - ☐ 5
  - ☐ 6
  - ☐ Ninguna de las anteriores