PUCE Virtual

CLASE
7

Arquitectura de computadoras

Riesgos asociados al DMA, incluyendo ataques con dispositivos maliciosos

QS WORLD UNIVERSITY RANKINGS

Educación de calidad

INTRODUCCIÓN DE LA CLASE

GRADO / POSGRADO / TECNOLOGÍAS

Estudia a tu tiempo
sin interrupciones

EDUCACIÓN EN LÍNEA DE CALIDAD

En los sistemas modernos de cómputo, gran parte del rendimiento y la seguridad dependen de cómo el hardware interactúa con la memoria y los dispositivos. Cuando un sistema utiliza mecanismos como el Acceso Directo a Memoria (DMA), los dispositivos pueden transferir datos directamente hacia la RAM sin pasar constantemente por la CPU, lo que mejora la eficiencia. Sin embargo, este mismo mecanismo abre la puerta a riesgos importantes si un dispositivo es malicioso o está comprometido, ya que podría acceder a zonas de memoria sensibles o interferir en la ejecución del sistema. En este contexto, también es importante entender que los periféricos no son elementos aislados: forman parte activa de la arquitectura y pueden convertirse en vectores de ataque si no se gestionan adecuadamente.

A partir de esta base, se introduce el mundo de la virtualización, donde el hardware físico se comparte entre múltiples entornos lógicos mediante hipervisores, máquinas virtuales y contenedores. Aquí surge una pregunta clave para el análisis: ¿cómo equilibrar eficiencia y seguridad cuando varios sistemas comparten los mismos recursos? La virtualización permite optimizar el uso del hardware, pero también introduce riesgos como el escape de máquinas virtuales, donde un atacante podría romper el aislamiento y afectar al hipervisor o a otras VMs. En esta clase se trabajará precisamente ese equilibrio, conectando estos conceptos con el resultado de aprendizaje: diseñar soluciones eficientes en consumo de recursos para diferentes tipos de aplicaciones, entendiendo que cada decisión arquitectónica implica un compromiso entre rendimiento, aislamiento y seguridad.

Reto # 4.

10.2. Riesgos asociados al DMA, incluyendo ataques con dispositivos maliciosos

El Acceso Directo a Memoria (DMA) permite que dispositivos de hardware accedan directamente a la memoria principal sin intervención constante de la CPU, mejorando el rendimiento y la eficiencia del sistema. Sin embargo, desde la ciberseguridad, representa una superficie de ataque crítica, ya que implica acceso privilegiado a la memoria (Hennessy et al., 2019).

En arquitecturas modernas, especialmente con buses como PCIe, un dispositivo con DMA puede acceder a datos sensibles si no existen controles adecuados, como credenciales o claves, convirtiéndolo en un vector de ataque peligroso, sobre todo cuando se conectan dispositivos externos (Stallings, 2019).

Para comprender integralmente los riesgos del DMA, se analizan las siguientes dimensiones:

A. Naturaleza de los riesgos asociados al DMA

El DMA permite acceso directo a la memoria sin control del sistema operativo, rompiendo el aislamiento entre procesos. Esto posibilita lecturas y escrituras no autorizadas, debilitando la seguridad del sistema y generando riesgos si no se aplican mecanismos adicionales de protección (Hennessy et al., 2019).

Esto genera tres tipos de riesgos fundamentales:

i. Pérdida de confidencialidad

Cuando un dispositivo DMA realiza operaciones de lectura, no distingue entre memoria de usuario, memoria del kernel y datos sensibles.

Esto significa que puede acceder a contraseñas en RAM, claves criptográficas, tokens de sesión o a buffers de aplicaciones.

El riesgo aumenta porque datos sensibles pueden estar en memoria sin suficiente protección, y el DMA puede acceder a ellos sin respetar las reglas de la MMU, debilitando el modelo de seguridad de memoria (Hennessy et al., 2019).

ii. Pérdida de integridad

El DMA no solo lee, también escribe en memoria. Esto permite modificar:

- estructuras del kernel
- tablas de páginas
- punteros de ejecución
- buffers de entrada/salida

Un atacante puede, por ejemplo, alterar un puntero para redirigir la ejecución del programa, modificar permisos de memoria o inyectar código directamente en RAM. La implicación es crítica porque se rompe el principio de ejecución confiable, ya que el sistema puede ejecutar código que nunca fue validado por el sistema operativo.

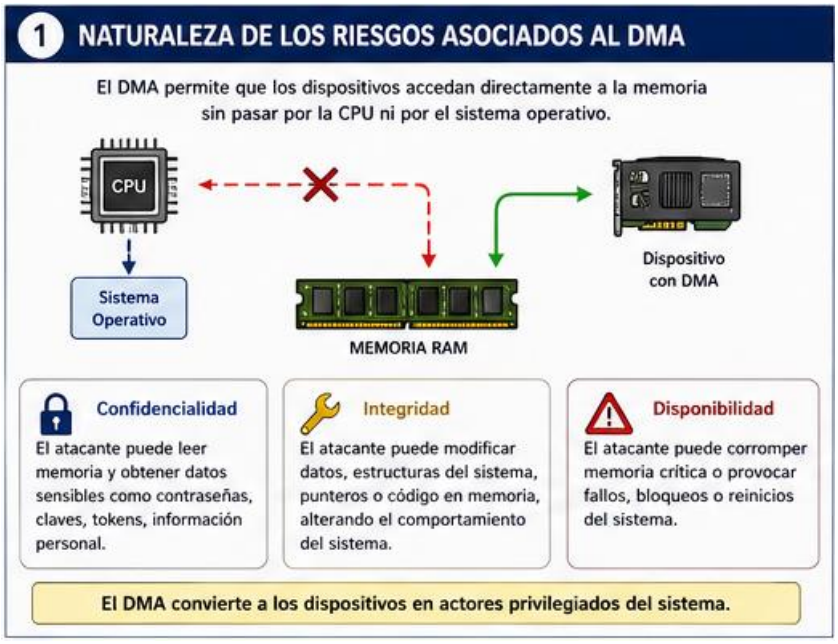
iii. Pérdida de disponibilidad

La disponibilidad se compromete cuando el DMA corrompe memoria crítica, provocando fallos, reinicios o bloqueos. Esto ocurre porque el daño escapa al control del sistema operativo, que depende de la integridad de la memoria para funcionar correctamente.

La figura 1 representa cómo el DMA permite acceso directo a la memoria, exponiendo riesgos de confidencialidad, integridad y disponibilidad.

Figura 1

Naturaleza de los riesgos asociados al DMA



Autor: Milton Román

El DMA convierte a los dispositivos en actores privilegiados del sistema, capaces de violar los tres pilares de la seguridad: Confidencialidad, Integridad y Disponibilidad.

B. Ataques con dispositivos maliciosos basados en DMA

Uno de los escenarios más preocupantes en ciberseguridad es el uso de dispositivos maliciosos conectados físicamente al sistema. Estos ataques suelen aprovechar interfaces como Thunderbolt, PCIe o incluso adaptadores USB modificados.

Estos ataques son especialmente peligrosos porque no requieren malware previo, pueden ejecutarse en segundos, funcionan incluso en sistemas bloqueados.

La figura 2 ilustra los principales ataques DMA: lectura de memoria, inyección de código, manipulación de datos y escape de máquinas virtuales.

Figura 2

Ataques con dispositivos maliciosos basados en DMA

Autor: Milton Román

Tipos de ataques relevantes:

i. Ataques tipo DMA Injection

Un atacante puede usar un dispositivo aparentemente legítimo para acceder a la memoria mediante DMA, leer datos sensibles o inyectar código malicioso. En ataques como los realizados con Thunderbolt, es posible extraer credenciales directamente desde la RAM sin autenticación, lo que los hace especialmente peligrosos cuando existe acceso físico al equipo.

ii. Ataques Cold Boot y DMA

En combinación con técnicas como el cold boot attack, el DMA puede facilitar la extracción de datos persistentes en memoria RAM.

Escenario:

- El atacante reinicia el equipo sin apagar completamente la memoria.
- Utiliza un dispositivo DMA para leer directamente los datos residuales en RAM.
- Recupera información sensible como claves de cifrado.

Este tipo de ataque demuestra cómo el DMA puede ser utilizado incluso fuera del contexto del sistema operativo activo.

iii. Ataques a máquinas virtuales (VM Escape mediante DMA)

En entornos virtualizados, el DMA puede romper el aislamiento si no se configura correctamente. Un dispositivo con passthrough puede acceder a memoria fuera de su VM, comprometer el hipervisor y escalar privilegios hacia otras máquinas. Esto introduce desafíos de seguridad al combinar virtualización con técnicas de alto rendimiento como el DMA (Jaramillo Villegas et al., 2022).

C. Factores que incrementan la vulnerabilidad

Los riesgos asociados al DMA no son constantes, además no solo dependen de la tecnología, dependen del contexto del sistema, se ven amplificados en ciertos contextos:

- Equipos portátiles sin protección física adecuada.
- Sistemas sin configuración de IOMMU (Unidad de Gestión de Memoria de Entrada/Salida).
- Uso de dispositivos externos no confiables.
- Ambientes corporativos con múltiples periféricos conectados.

Además, la tendencia hacia arquitecturas de alto rendimiento (como NVMe o GPUs) incrementa el uso del DMA, lo que también amplía la superficie de ataque (Fabra Gallo et al., 2020).

La figura 3 muestra los factores críticos que aumentan el riesgo, como ausencia de IOMMU, acceso físico, interfaces expuestas y mala configuración de virtualización.

Figura 3

Factores que incrementan la vulnerabilidad

Autor: Milton Román

La vulnerabilidad no depende solo del DMA, sino de configuración, arquitectura y contexto operativo.

D. Mecanismos de mitigación

Para reducir los riesgos del DMA, se han desarrollado diversas soluciones a nivel de hardware y software:

i. Nivel Hardware:

La IOMMU permite controlar y restringir el acceso de los dispositivos DMA a regiones específicas de memoria, actuando como un filtro que traduce direcciones y limita accesos. De este modo, cada dispositivo solo puede acceder al espacio asignado, restaurando el aislamiento y mejorando la seguridad del sistema (Hennessy et al., 2019).

ii. Nivel sistema operativo

La Kernel DMA Protection bloquea accesos DMA antes de la autenticación del usuario, reforzando la seguridad en sistemas modernos. Junto con la IOMMU, que filtra y restringe el acceso a memoria asignando regiones específicas a cada dispositivo, se evita el acceso no autorizado y se restaura el aislamiento del sistema (Hennessy et al., 2019).

iii. Nivel físico

Desactivación de puertos externos sensibles como Thunderbolt en entornos de alta seguridad. Restringir acceso, políticas de seguridad.

Importancia: Muchos ataques DMA requieren presencia física.

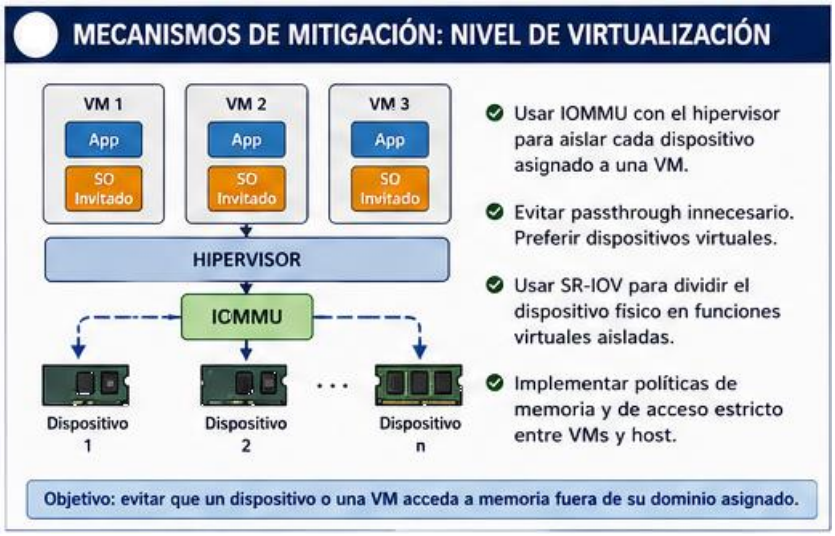
iv. Nivel de virtualización

En entornos virtualizados, el uso de DMA añade complejidad, ya que el acceso directo a hardware (passthrough) puede debilitar el aislamiento entre máquinas virtuales. Un dispositivo con capacidades DMA puede intentar acceder a memoria fuera de su VM, reduciendo el control del hipervisor y posibilitando ataques como VM Escape, donde se compromete el host u otras máquinas virtuales (Jaramillo Villegas et al., 2022).

En la figura 4 se ilustra los mecanismos de mitigación a nivel de virtualización.

Figura 4

Mecanismos de mitigación



Autor: Milton Román

v. Nivel de datos

Este nivel busca minimizar el impacto del acceso DMA a datos sensibles, incluso si ocurre un ataque. El riesgo radica en que el DMA puede leer directamente la memoria, donde la información crítica suele permanecer más tiempo del necesario, haciéndola vulnerable.

Estrategias de mitigación a nivel de datos:

- Minimización de datos en memoria
- Uso de buffers seguros
- Evitar texto plano en memoria
- Segmentación de datos sensibles
- Técnicas de limpieza de memoria (memory wiping)

vi. Cifrado de memoria

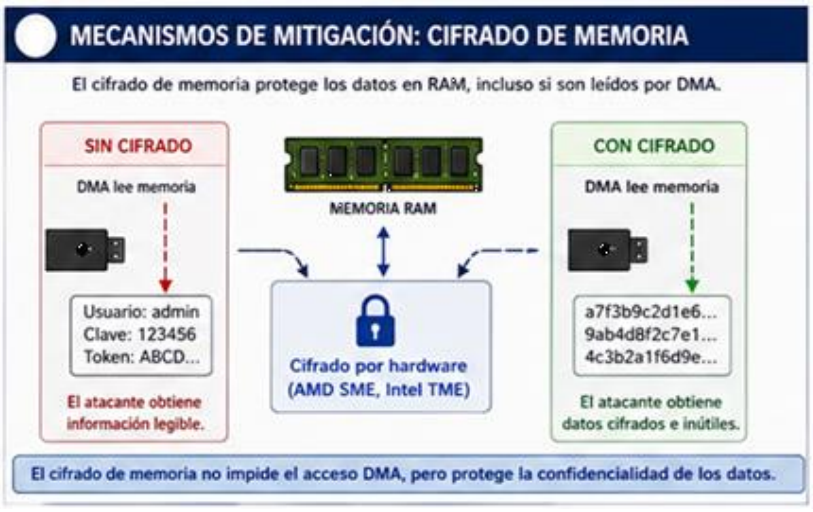
Reduce el impacto de ataques que intentan leer datos directamente desde RAM.

Hennessy y Patterson (2019) destacan que la seguridad en arquitecturas modernas debe integrarse desde el diseño, no como un componente adicional.

La figura 5 compara escenarios con y sin cifrado, mostrando cómo el cifrado protege la información incluso si el DMA accede a la memoria.

Figura 5

Mecanismos de mitigación: cifrado de memoria



Autor: Milton Román

El resultado es la reducción significativa del riesgo, porque, no requiere hardware adicional, el consumo de recursos es bajo y el impacto en seguridad es alto.

El DMA mejora el rendimiento, pero puede convertirse en una vulnerabilidad si no se controla adecuadamente. Por ello, es clave analizar sus riesgos en escenarios reales e implementar mecanismos como IOMMU y políticas de seguridad para proteger el sistema sin afectar su eficiencia.

El siguiente enlace tiene la finalidad de conocer cómo proteger los dispositivos de los ciberdelincuentes que buscan aprovecharse de los datos y usarlos en actividades ilícitas:

- **Título**: Los riesgos de un dispositivo hackeado. Cómo evitar su uso ilícito | Ciberseguridad
- **Descripción:** Cómo proteger los dispositivos de los ciberdelincuentes que buscan aprovecharse de los datos y usarlos en actividades ilícitas. Descubre los riesgos de tener un dispositivo comprometido, desde fraudes financieros hasta ataques a tu privacidad.
- **Enlace**: Los riesgos de un dispositivo hackeado. Cómo evitar su uso ilícito | Ciberseguridad

11. VIRTUALIZACIÓN Y ARQUITECTURA DE HIPERVISORES

La virtualización permite abstraer el hardware para crear múltiples entornos independientes, optimizando recursos. Sin embargo, también introduce desafíos de ciberseguridad al combinar riesgos de almacenamiento, periféricos, DMA y entornos virtualizados.

Desde el enfoque de la ciberseguridad, es imprescindible analizar cómo estos elementos interactúan, ya que una vulnerabilidad en cualquiera de ellos puede comprometer todo el sistema.

11.1 Arquitectura de máquinas virtuales y contenedores

a) Concepto y funcionamiento de la virtualización

La virtualización permite ejecutar múltiples sistemas operativos sobre un mismo hardware mediante una capa de abstracción, optimizando recursos y mejorando la escalabilidad (Ibarra Mayorga, 2009).

El componente central es el hipervisor, que gestiona y asigna CPU, memoria y dispositivos, siendo crítico para la seguridad y el control del sistema (Stallings, 2019). Existen dos tipos: los de tipo 1, que se ejecutan directamente sobre el hardware y ofrecen mayor rendimiento y seguridad, y los de tipo 2, que funcionan sobre un sistema operativo anfitrión, brindando más flexibilidad, pero también mayor superficie de ataque. Esta diferencia es clave para diseñar infraestructuras seguras y eficientes.

b) Arquitectura de máquinas virtuales (VMs)

Las máquinas virtuales replican un computador completo, ofreciendo alto aislamiento y beneficios en seguridad. Sin embargo, este aislamiento implica mayor consumo de recursos, lo que puede generar sobrecarga si no se gestiona adecuadamente (Hennessy et al., 2019). Aunque permiten contener ataques dentro de cada entorno, un compromiso del hipervisor puede afectar a todas las VMs.

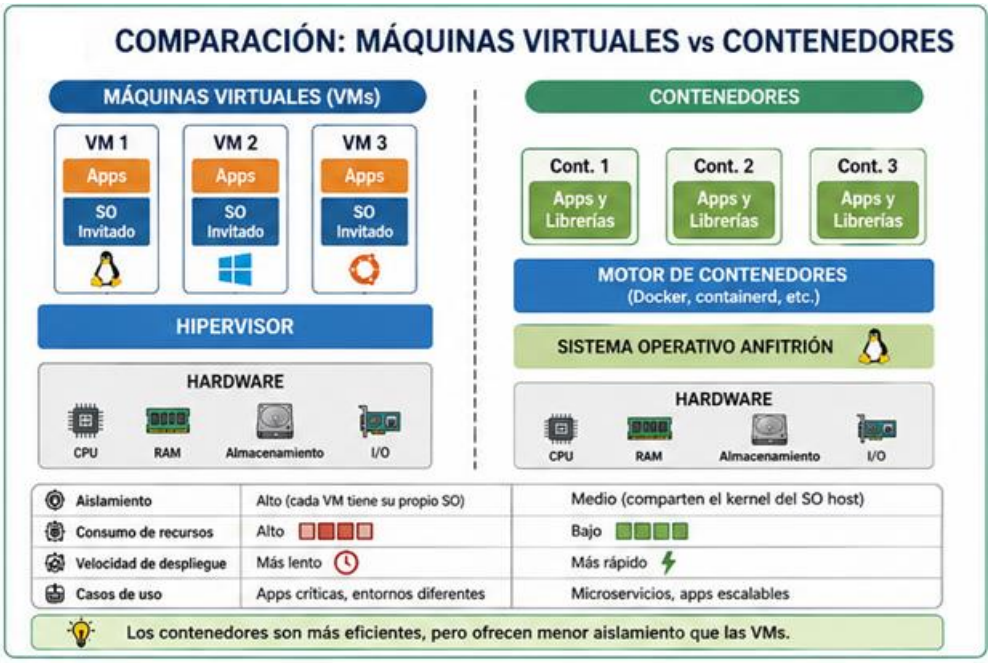
c) Arquitectura de contenedores

Los contenedores son una alternativa ligera a las máquinas virtuales, ya que comparten el kernel del sistema operativo y aíslan solo las aplicaciones, lo que mejora el rendimiento y reduce el consumo de recursos. Sin embargo, ofrecen menor nivel de aislamiento, lo que incrementa los riesgos de seguridad y exige configuraciones más estrictas, especialmente en entornos escalables y de microservicios (Jaramillo Villegas et al., 2022).

La figura 6 compara el nivel de aislamiento, consumo de recursos y arquitectura entre máquinas virtuales y contenedores.

Figura 6

Comparación: máquinas virtuales vs contenedores



Autor: Milton Román

11.2 Riesgos de escape de VM

a) Concepto de escape de máquina virtual

El escape de máquina virtual (VM escape) es una de las amenazas más críticas en entornos virtualizados. Este ataque ocurre cuando un proceso dentro de una máquina virtual logra acceder al hipervisor o a otras máquinas virtuales, rompiendo el aislamiento.

Este tipo de vulnerabilidad compromete la base misma de la virtualización. Según (Hennessy et al., 2019), la seguridad de estos entornos depende en gran medida de la correcta implementación de mecanismos de aislamiento y del fortalecimiento del hipervisor.

b) Relación con DMA y periféricos

El riesgo de escape de máquinas virtuales aumenta con el uso de DMA, ya que este permite acceso directo a la memoria sin control de la CPU, lo que puede ser explotado para leer o modificar datos sensibles y afectar al hipervisor u otras VMs (Martínez Amador, 2012). Además, los periféricos como USB o tarjetas de red también actúan como vectores de ataque, permitiendo la introducción de malware o la interceptación de información.

c) Riesgos en almacenamiento (HDD, SSD, NVMe)

El almacenamiento también juega un papel importante en la seguridad de entornos virtualizados. Cada tecnología presenta riesgos específicos:

- HDD: Vulnerables a fallos mecánicos y recuperación de datos.
- SSD: Riesgos asociados a desgaste y recuperación de datos residuales.
- NVMe: Mayor velocidad, pero también mayor exposición a ataques de firmware.

Cuando múltiples máquinas virtuales comparten el mismo dispositivo físico, existe el riesgo de fuga de información si no se implementan mecanismos adecuados de aislamiento.

d) Integración de riesgos y diseño de checklist de protección

La integración de riesgos implica analizar cómo interactúan los diferentes componentes del sistema. No basta con asegurar cada elemento de forma aislada; es necesario comprender sus interdependencias.

En este contexto, un checklist de protección básico debe considerar los siguientes aspectos:

- El aseguramiento del hipervisor mediante actualizaciones constantes, configuración segura y monitoreo continuo. Se recomienda el uso de hipervisores tipo 1 en entornos críticos.
- La gestión segura del DMA mediante tecnologías como IOMMU, que restringen el acceso de los dispositivos a la memoria.
- El fortalecimiento del aislamiento en máquinas virtuales y contenedores. En contenedores, esto incluye el uso de namespaces, cgroups y escaneo de imágenes.
- La protección del almacenamiento mediante cifrado, control de accesos y eliminación segura de datos.
- El control de periféricos mediante autenticación, restricciones de uso y monitoreo constante.

La figura 7 resume las medidas clave de protección: seguridad del hipervisor, control de DMA, aislamiento, protección de datos y periféricos.

Figura 7

Checklist de protección en entornos virtualizados

Autor: Milton Román

e) Eficiencia y seguridad: equilibrio necesario

Uno de los principales desafíos en la arquitectura de sistemas es lograr un equilibrio entre eficiencia y seguridad. Las máquinas virtuales ofrecen mayor aislamiento, pero consumen más recursos. Los contenedores son más eficientes, pero requieren mayores controles de seguridad.

Según (Hennessy et al., 2019), el diseño eficiente de sistemas implica tomar decisiones informadas sobre el uso de recursos, sin comprometer la seguridad.

En este sentido, la elección entre VMs y contenedores debe basarse en el tipo de aplicación, el nivel de riesgo aceptable y los requerimientos de rendimiento.

La virtualización transforma la manera en que se diseñan y gestionan los sistemas informáticos, pero también introduce nuevas superficies de ataque. El análisis conjunto de riesgos en

almacenamiento, periféricos, DMA y entornos virtualizados permite construir estrategias de protección más robustas.

Ingresando al siguiente enlace encontramos información sobre virtualización, máquina virtual, hipervisores, contenedores, orquestadores y cloud computing:

- **Título**: Virtualización, máquina virtual, hipervisores, contenedores, orquestadores y cloud computing
- **Descripción**: El video presenta una introducción a la virtualización y sus tecnologías relacionadas, explicando de forma general las máquinas virtuales, contenedores, hipervisores, orquestadores y la computación en la nube, destacando cómo estas soluciones han transformado la gestión y el despliegue de recursos de TI.
- **Enlace**: VIRTUALIZACIÓN | MÁQUINA VIRTUAL | HIPERVISORES | CONTENEDORES | ORQUESTADORES | CLOUD COMPUTING

• **Fabra Gallo, J. M., Martínez Márquez, Y., & Valcárcel Izquierdo, N. (2020).** Estudio comparado de los contenidos de la asignatura Arquitectura de Computadoras: oportunidades de mejoras. Dialnet. Obtenido de https://dialnet.unirioja.es/servlet/articulo?codigo=8590371

• **Hennessy, Hennessy, J. L., & Patterson, D. A. (2019).** ARQUITECTURA DE COMPUTADORES: Un enfoque cuantitativo. McGrawHill. https://doi.org/1-55860-069-8

• **Ibarra Mayorga, M. F. (2009).** Evolución de las arquitecturas de las computadoras. eLibro. Obtenido de https://elibro.puce.elogim.com/es/lc/puce/titulos/28671

• **Jaramillo Villegas, J. A., Zuluaga Bucheli, H. M., & Sepúlveda Caviedes, C. (2022).** Arquitectura de computadoras con RISC-V. Universidad Tecnológica de Pereira. Digitalia. Obtenido de https://www.digitaliapublishing.com/a/136758/

• **Martínez Amador, H. (2012).** Arquitectura de computadoras: basado en competencias para nivel superior. Obtenido de https://elibro.puce.elogim.com/es/lc/puce/titulos/130397

• **Stallings, W. (2019).** Computer organization and architecture : designing for performance (11ava ed.). Pearson Education. Obtenido de https://os.ecci.ucr.ac.cr/ci0114/material/Stallings/Computer-Organization-Architecture-11th.pdf

PUCE Virtual

síguenos en:

www.pucevirtual.puce.edu.ec