PUCE Virtual

CLASE
5

Arquitectura de computadoras

Almacenamiento y Protección de datos

QS WORLD UNIVERSITY RANKINGS

Educación de calidad

INTRODUCCIÓN DE LA CLASE

GRADO / POSGRADO / TECNOLOGÍAS

Estudia a tu tiempo
son interrupciones

EDUCACIÓN EN LÍNEA DE CALIDAD

Imagina que enciendes tu computadora y comienzas a trabajar con archivos, aplicaciones y datos sin pensar demasiado en dónde se almacenan o cómo se protegen. Pero ¿qué pasaría si alguien pudiera acceder a esa información sin tu permiso o incluso recuperarla después de haberla eliminado? En esta clase vamos a explorar justamente eso: el mundo del almacenamiento y la protección de datos. Analizaremos los diferentes tipos de almacenamiento como HDD, SSD y NVMe, comprendiendo no solo sus diferencias en velocidad o capacidad, sino también sus implicaciones en el rendimiento del sistema y en la seguridad. Además, abordaremos cómo se protege la información almacenada y por qué técnicas como el cifrado, el control de acceso y la verificación de integridad son fundamentales en los sistemas actuales.

Pero no nos quedaremos solo en lo básico. También reflexionaremos sobre aspectos más críticos como el borrado seguro de datos, entendiendo por qué eliminar un archivo no significa que desaparezca realmente, y cómo esto puede convertirse en un riesgo de seguridad. Asimismo, discutiremos amenazas menos visibles, como los ataques al controlador de almacenamiento, que pueden comprometer la información desde niveles profundos del sistema. Todo esto se vincula directamente con el RDA3, ya que no se trata solo de elegir la tecnología más rápida, sino de diseñar soluciones eficientes que optimicen recursos y, al mismo tiempo, garanticen la seguridad de los datos. En este recorrido, comenzarás a ver el almacenamiento no solo como un componente técnico, sino como una pieza clave dentro de la arquitectura segura de un sistema computacional.

RDA 3: Diseñar soluciones eficientes en términos de consumo de recursos para diferentes tipos de aplicaciones.

RETO # 3

8. ALMACENAMIENTO Y PROTECCIÓN DE DATOS

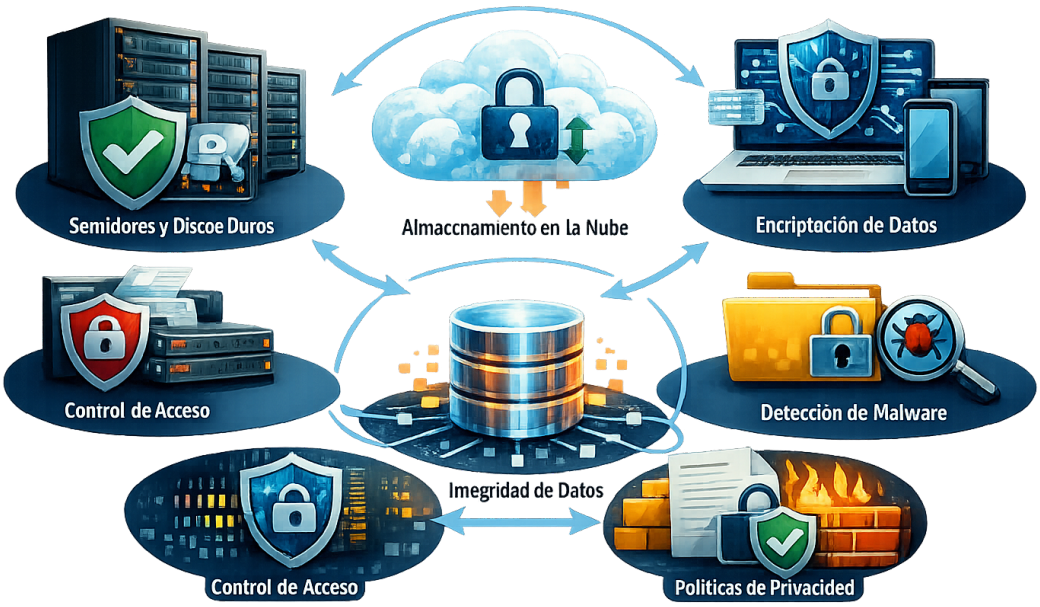
El almacenamiento de datos es un componente fundamental dentro de la arquitectura de computadoras, ya que no solo determina el rendimiento del sistema, sino también su nivel de seguridad. En la actualidad, la protección de la información almacenada se ha convertido en un aspecto crítico debido al aumento de amenazas como ransomware, exfiltración de datos y ataques persistentes (Stallings, 2019).

Desde la perspectiva de ciberseguridad, el almacenamiento no debe analizarse únicamente como un recurso físico, sino como un elemento dentro de una cadena de confianza, donde la integridad y confidencialidad de los datos deben garantizarse desde el arranque del sistema hasta su uso en aplicaciones (Hennessy et al., 2019).

La Figura 1, presenta una visión integral del almacenamiento y la protección de datos en sistemas informáticos, destacando cómo distintos componentes como servidores, nube, cifrado, control de acceso y políticas de seguridad trabajan de forma interconectada.

Figura 1

Almacenamiento y protección de datos



Autor: Milton Román

8.1 TIPOS DE ALMACENAMIENTO (HDD, SSD, NVME)

El almacenamiento constituye uno de los componentes más determinantes en el desempeño y la seguridad de un sistema computacional. Su evolución ha estado marcada por la necesidad de mejorar la velocidad de acceso a los datos, reducir el consumo de recursos y fortalecer los mecanismos de protección frente a amenazas. En este contexto, los dispositivos HDD, SSD y NVMe no solo representan distintas tecnologías, sino también diferentes implicaciones en términos de eficiencia y ciberseguridad (Hennessy et al., 2019).

La figura 2 presenta una comparación clara de los principales tipos de almacenamiento utilizados en computadoras: HDD, SSD y NVMe SSD. Se evidencia la evolución tecnológica en el almacenamiento de datos, destacando cómo cada opción responde a diferentes necesidades de rendimiento y uso en sistemas informáticos.

Figura 2

Tipos de almacenamiento

Autor: Milton Román

a) **Hard Disk Drive (HDD):** Los HDD son dispositivos de almacenamiento magnético que utilizan discos giratorios y cabezales mecánicos para leer y escribir datos. Su principal ventaja es el bajo costo por gigabyte, lo que los hace adecuados para almacenamiento masivo, como copias de seguridad o archivos históricos. Sin embargo, presentan limitaciones en velocidad, mayor consumo energético y vulnerabilidad a fallos mecánicos. Desde el punto de vista de la ciberseguridad, los HDD permiten la recuperación de datos eliminados mediante herramientas forenses, lo que representa un riesgo si no se aplican técnicas de borrado seguro.
Ejemplo: Una institución educativa almacena registros históricos en un HDD para reducir costos. Si decide desechar el disco sin aplicar un borrado seguro, un tercero podría recuperar información sensible como calificaciones o datos personales de estudiantes.

b) **Solid State Drive (SSD)**: Los SSD utilizan memoria flash, eliminando componentes mecánicos. Esto se traduce en mayor velocidad, menor consumo de energía y mayor resistencia física. Estas características los convierten en una opción ideal para sistemas operativos y aplicaciones críticas, contribuyendo a la eficiencia del sistema. Sin embargo, su arquitectura introduce retos en la eliminación definitiva de datos, debido a técnicas internas como el wear leveling, que redistribuyen la escritura en distintas celdas de memoria (Martínez Amador, 2012).
Ejemplo: Una empresa instala SSD en sus estaciones de trabajo para mejorar el rendimiento de aplicaciones empresariales. Aunque elimina archivos confidenciales, estos pueden permanecer en celdas no visibles, lo que exige el uso de herramientas especializadas de borrado o cifrado previo.

c) **Non-Volatile Memory Express (NVMe)**: En niveles más avanzados, los dispositivos NVMe representan la evolución del almacenamiento SSD, optimizando la comunicación mediante el bus PCIe. Esto permite un acceso mucho más rápido a los datos, con baja latencia y alto paralelismo, lo cual es fundamental en aplicaciones de alto rendimiento como inteligencia artificial, análisis de datos o sistemas distribuidos (Jaramillo Villegas et al., 2022).
Desde la perspectiva de ciberseguridad, la velocidad del NVMe implica que los mecanismos de protección deben ser igualmente eficientes. De lo contrario, procesos como el cifrado o la detección de amenazas pueden convertirse en cuellos de botella.

   Ejemplo: Un centro de datos utiliza NVMe para procesar transacciones financieras en tiempo real. Si un atacante logra acceder al sistema, podría exfiltrar grandes volúmenes de datos en muy poco tiempo, lo que hace imprescindible implementar cifrado robusto y monitoreo continuo.

En síntesis, un diseño eficiente no solo optimiza recursos, sino que también garantiza la protección de la información en todo su ciclo de vida.

La tabla 1 resume cómo la elección de la tecnología no solo responde a criterios de rendimiento, sino también a la eficiencia en el uso de recursos y a la incorporación de medidas de ciberseguridad, alineadas con la cadena de confianza desde el arranque del sistema.

Tabla 1

Comparación orientada a eficiencia y seguridad

bbb	Velocidad	Consumo	Seguridad	Uso recomendado
HDD	Baja	Alto	Riesgo de recuperación de datos	Almacenamiento masivo
SSD	Media-Alta	Bajo	Riesgos en borrado	Sistemas operativos
NVMe	Muy alta	Bajo	Alta exposición si no se protege	Sistemas críticos

Autor: Milton Román

Refuerza el contenido estudiado en el siguiente video:

- **Título:** Tipos de almacenamiento de datos
- **Descripción:** Video que explica los diferentes tipos de almacenamiento de datos
- **Enlace:** https://youtu.be/lE-QvEgWAq8?si=wLxdHUkaK6hhOL2Q

8.2 SEGURIDAD DE LA INFORMACIÓN ALMACENADA

La seguridad de la información almacenada es esencial en la arquitectura de computadoras, ya que protege los datos, uno de los activos más valiosos. Esta protección debe abordarse de forma integral, considerando no solo el almacenamiento, sino también su relación con el firmware, el sistema operativo y el arranque seguro, garantizando la confidencialidad, integridad y disponibilidad desde las capas más bajas del sistema (Stallings, 2019).

Entre los mecanismos clave destacan el cifrado de datos y el control de acceso, que evitan accesos no autorizados, así como el uso de hashes y firmas digitales para asegurar la integridad. Estos se integran con tecnologías como Secure Boot y Trusted Boot, formando una cadena de confianza (Hennessy et al., 2019). Además, la protección se complementa con monitoreo, auditoría y copias de seguridad, que permiten enfrentar amenazas como ransomware y garantizar la disponibilidad de la información (Fabra Gallo et al., 2020). Un ejemplo claro es el uso de cifrado junto con Secure Boot, que impide el acceso a los datos si el sistema ha sido alterado.

La figura 3 muestra los principales mecanismos para garantizar la seguridad de la información almacenada, integrando elementos como encriptación, control de acceso, copias de seguridad y monitoreo. En conjunto, refleja cómo diferentes capas de protección trabajan para resguardar los datos frente a accesos no autorizados, pérdidas o ataques.

Figura 3

Seguridad de la información almacenada

Autor: Milton Román

Principales técnicas de seguridad en almacenamiento

a) Cifrado de datos

El cifrado es una de las técnicas más importantes para proteger la confidencialidad de la información. Consiste en transformar los datos en un formato ilegible sin una clave de acceso. Protege los datos incluso si el dispositivo es robado. El uso de aceleración por hardware (como AES-NI) mejora el rendimiento del cifrado.

Tipos:

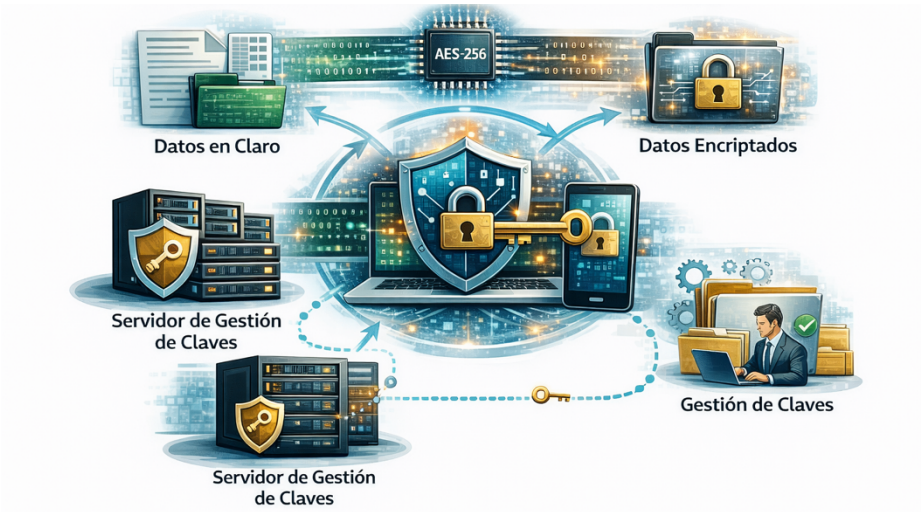
- Cifrado de disco completo (Full Disk Encryption)
- Cifrado a nivel de archivo o carpeta

Por ejemplo, una laptop corporativa es robada. Si el disco está cifrado, el atacante no podrá acceder a la información sin la clave, incluso si extrae físicamente el almacenamiento.

La figura 4 muestra cómo el cifrado de datos protege la información al transformar datos legibles en datos seguros mediante algoritmos y claves, destacando la importancia de la gestión de claves para garantizar la seguridad.

Figura 4

Cifrado de datos



Autor: Milton Román

b) Control de acceso y autenticación
Consiste en restringir quién puede acceder a los datos y qué acciones puede realizar. Tiene relación con BIOS/UEFI porque se puede restringir el arranque desde dispositivos externos para evitar accesos no autorizados.

Mecanismos:

- Usuarios y roles
- Autenticación multifactor (MFA)
- Políticas de permisos

Por ejemplo, en un servidor empresarial, solo los administradores pueden acceder a bases de datos críticas, mientras que otros usuarios tienen permisos limitados de lectura.

c) Integridad de datos (Hash y firmas digitales)
Garantiza que la información no ha sido modificada de forma no autorizada. Estas técnicas son fundamentales en Secure Boot y Trusted Boot, donde se verifica cada componente antes de ejecutarlo.

Técnicas**:**

- Funciones hash (ejemplo: SHA-256)
- Firmas digitales

Por ejemplo, en sistema calcula el hash de un archivo crítico. Si un atacante lo modifica, el hash cambia, permitiendo detectar la alteración.

d) Copias de seguridad (Backup y recuperación)
Permiten restaurar la información en caso de pérdida, corrupción o ataque.

Tipos:

- Completo
- Incremental
- En la nube

Por ejemplo, una empresa sufre un ataque de ransomware. Gracias a sus copias de seguridad, puede recuperar sus datos sin pagar el rescate.

e) Borrado seguro de datos
Eliminar un archivo no garantiza su desaparición. El borrado seguro sobrescribe los datos para evitar su recuperación.

Importancia en HDD y SSD:

- En HDD: sobrescritura múltiple.
- En SSD: uso de comandos como secure erase.

Por ejemplo, antes de vender un disco duro, una empresa aplica borrado seguro para evitar la recuperación de información confidencial.

f) Monitoreo y auditoría
Consiste en supervisar continuamente el acceso y uso de los datos.

Herramientas:

- Sistemas SIEM
- Logs de acceso

Por ejemplo, un sistema detecta múltiples intentos fallidos de acceso a una base de datos y genera una alerta de posible ataque.

g) Protección contra malware (ransomware y rootkits)
El almacenamiento es uno de los principales objetivos de malware.

Medidas:

- Antivirus/EDR
- Segmentación de red
- Validación desde el arranque
- Secure Boot evita la ejecución de malware desde el inicio.
- Trusted Boot detecta alteraciones en el sistema.

Por ejemplo, un ransomware intenta cifrar archivos del sistema, pero es bloqueado porque el sistema detecta comportamiento anómalo y restringe el acceso.

La figura 5 ilustra la protección contra malware, destacando dos amenazas principales: ransomware y rootkits. En el centro se representa un sistema de antivirus/antimalware como una barrera de defensa, mientras que alrededor se muestran mecanismos técnicos como la detección y eliminación, el análisis en tiempo real, la protección de copias de seguridad y el bloqueo de exploits, evidenciando un enfoque integral de seguridad.

Figura 5

Protección contra malware

Autor: Milton Román

h) Uso de hardware seguro (TPM y Root of Trust)

El Trusted Platform Module (TPM) almacena claves criptográficas y permite verificar la integridad del sistema. Su función es asegurar que el sistema arranque en un estado confiable.

Por ejemplo, si el sistema detecta una modificación en el firmware o sistema operativo, el TPM puede bloquear el acceso a los datos cifrados.

En conjunto, la seguridad de la información almacenada no depende de una sola técnica, sino de la integración de múltiples mecanismos que trabajan en conjunto. Desde el cifrado hasta el arranque seguro, cada capa refuerza la protección del sistema.

Diseñar soluciones eficientes implica equilibrar seguridad y rendimiento, asegurando que los datos estén protegidos sin comprometer la operatividad del sistema. En este sentido, la relación entre almacenamiento, firmware y cadena de confianza es clave para enfrentar las amenazas actuales en ciberseguridad.

Refuerza tus conocimientos sobre borrado seguro, seguridad de datos y ataques al controlador de almacenamiento ingresando al siguiente video:

8.3 CONCEPTOS BÁSICOS DE BORRADO SEGURO, SEGURIDAD DE DATOS Y ATAQUES AL CONTROLADOR DE ALMACENAMIENTO

La protección de la información no termina cuando los datos dejan de utilizarse; por el contrario, una de las fases más críticas del ciclo de vida de los datos es su eliminación. En este contexto, el borrado seguro de datos, la seguridad durante el almacenamiento y la protección frente a ataques al controlador de almacenamiento se convierten en elementos clave dentro de la arquitectura de computadoras. Estos aspectos adquieren mayor relevancia si se consideran las amenazas actuales, donde los atacantes buscan explotar tanto el software como los componentes de bajo nivel del sistema (Stallings, 2019).

Implementar estas medidas implica diseñar soluciones que no solo sean seguras, sino también eficientes en el uso de recursos. Asimismo, en relación con el análisis de BIOS/UEFI y la cadena de confianza, es fundamental garantizar que los datos no sean comprometidos ni durante su uso ni después de su eliminación (Hennessy et al., 2019).

La figura 6 presenta una visión integrada de la ciberseguridad aplicada a los sistemas de almacenamiento dentro de la arquitectura de computadoras. Se destacan tres pilares fundamentales: el borrado seguro de datos, enfocado en la eliminación definitiva de la información; la protección de datos, mediante mecanismos como el cifrado y el control de acceso; y los ataques al controlador de almacenamiento, que representan amenazas directas al hardware y al manejo interno de la información.

Figura 6

Ciberseguridad en Sistemas de Almacenamiento

Autor: Milton Román

1. Borrado seguro de datos

El borrado seguro es el proceso mediante el cual los datos se eliminan de forma irreversible, evitando que puedan ser recuperados mediante técnicas forenses. A diferencia del borrado convencional, que solo elimina las referencias del sistema de archivos, el borrado seguro actúa directamente sobre el contenido físico del almacenamiento (Martínez Amador, 2012).

Técnicas de borrado seguro

a) **Sobrescritura de datos:** Consiste en escribir datos aleatorios o patrones específicos sobre la información existente.
   - Más común en HDD
   - Puede requerir múltiples pasadas

   Por ejemplo, una institución financiera sobrescribe varias veces un disco duro antes de desecharlo para evitar la recuperación de datos sensibles.

b) **Comandos de borrado seguro:** Utilizados principalmente en SSD, donde la sobrescritura tradicional no es efectiva debido al wear leveling.
   Por ejemplo, un administrador utiliza herramientas del fabricante para ejecutar un comando secure erase en un SSD antes de reutilizarlo.

c) **Destrucción física:** Método extremo que consiste en dañar físicamente el dispositivo.
Por ejemplo, una empresa destruye discos que contenían información altamente confidencial mediante trituración.

2. Seguridad de datos en almacenamiento

La seguridad de los datos almacenados implica proteger la información frente a accesos no autorizados, alteraciones y pérdidas.

Técnicas principales

a) **Cifrado de datos:** Protege la confidencialidad mediante algoritmos criptográficos.
Por ejemplo, un disco NVMe en un servidor empresarial utiliza cifrado por hardware para proteger información financiera.

b) **Control de acceso:** Define permisos y autenticación para acceder a los datos.
Por ejemplo, usuarios autorizados pueden acceder a bases de datos críticas mediante autenticación multifactor.

c) **Integridad de datos:** Uso de funciones hash para detectar modificaciones.
Estos mecanismos se integran con Secure Boot y Trusted Boot, asegurando que el sistema que accede a los datos sea confiable (Hennessy et al., 2019).

d) **Copias de seguridad:** Garantizan la disponibilidad ante fallos o ataques.
Por ejemplo, una empresa recupera su información tras un ataque ransomware gracias a backups.

3. Ataques al controlador de almacenamiento

El controlador de almacenamiento es el componente encargado de gestionar la comunicación entre el sistema operativo y el dispositivo de almacenamiento. Debido a su bajo nivel de operación, se ha convertido en un objetivo atractivo para atacantes.

Tipos de ataques

a) **Firmware malicioso en dispositivos de almacenamiento:** Los atacantes pueden modificar el firmware del disco para ocultar malware.
Por ejemplo, un atacante instala código malicioso en el firmware de un disco duro, el cual persiste incluso después de formatear el sistema.

b) **Manipulación del controlador** (driver attacks): Consiste en explotar vulnerabilidades en los controladores del sistema.
Por ejemplo, un malware aprovecha un controlador vulnerable para acceder directamente a los datos almacenados.

c) **Ataques de canal lateral:** Se basan en analizar el comportamiento del hardware para obtener información.
Ejemplo: Un atacante analiza patrones de acceso al disco para inferir datos sensibles.

d) **Exfiltración de datos:** Especialmente crítica en dispositivos de alta velocidad como NVMe.
Ejemplo: Un atacante copia grandes volúmenes de datos en segundos aprovechando la alta velocidad del almacenamiento.

4. Relación con BIOS/UEFI y cadena de confianza

La protección del almacenamiento no puede separarse del proceso de arranque:

- BIOS/UEFI inicializa los dispositivos de almacenamiento
- Secure Boot evita la ejecución de software no autorizado
- Trusted Boot verifica la integridad del sistema
- TPM asegura la gestión de claves criptográficas

Esto permite establecer una cadena de confianza, donde solo sistemas verificados pueden acceder a los datos (Ibarra Mayorga, 2009).

El borrado seguro, la protección de datos y la seguridad del controlador de almacenamiento son componentes esenciales en la defensa de los sistemas modernos. Ignorar estos aspectos puede permitir ataques persistentes y recuperación no autorizada de información.

Por ello, es fundamental implementar técnicas adecuadas y comprender que la seguridad no solo se aplica durante el uso de los datos, sino también en su almacenamiento y eliminación, garantizando así una protección integral del sistema.

Sobre borrado seguro, refuerza tu conocimiento en el siguiente documento:

- **Título**: Borrado seguro de datos: Métodos y herramientas profesionales
- **Descripción**: Este documento explora a fondo los métodos profesionales de borrado de datos, las herramientas más utilizadas en el mercado, los protocolos y las buenas prácticas a seguir para garantizar que tu información esté verdaderamente eliminada.
- **Enlace**: Borrado seguro de datos: métodos y herramientas profesionales - Elsetec

Educación de calidad

REFERENCIAS

- **Fabra Gallo, J. M., Martínez Márquez, Y., & Valcárcel Izquierdo, N. (2020).** Estudio comparado de los contenidos de la asignatura Arquitectura. 13. https://doi.org/ISSN-e 2306-2495
- **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