PUCE Virtual

CLASE

1

Arquitectura de computadoras

Introducción a la arquitectura de computadoras y ciberseguridad

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

En esta sección se establece una base técnica esencial para el análisis de la Arquitectura de Computadoras con enfoque en Ciberseguridad. El computador se aborda no solo como un conjunto de componentes físicos, sino como un sistema diseñado a partir de decisiones arquitectónicas que influyen directamente en el rendimiento, la confiabilidad y, de manera crítica, en la seguridad de la información. Comprender cómo funcionan internamente estos sistemas resulta indispensable para poder protegerlos, ya que muchas vulnerabilidades no se originan en el software, sino en la propia estructura y diseño del hardware.

A lo largo de la sesión se analizan los principios fundamentales de la arquitectura del computador y su relación con la seguridad, examinando el CPU, la memoria, el almacenamiento y los periféricos como activos críticos. Desde una perspectiva reflexiva, se invita al estudiante a cuestionar la confianza implícita en estos componentes y a reconocer cómo su explotación puede dar lugar a amenazas de bajo nivel. Este análisis permite identificar superficies de ataque, comprender la evolución de las amenazas a nivel hardware y desarrollar una visión inicial para anticipar riesgos, en coherencia con los objetivos formativos del reto y los resultados de aprendizaje de la asignatura.

1. INTRODUCCIÓN A LA ARQUITECTURA DE COMPUTADORAS Y CIBERSEGURIDAD

La arquitectura de computadoras estudia la organización y el funcionamiento interno de los sistemas de cómputo, abarcando componentes como el procesador, la memoria y los dispositivos de entrada/salida, así como las decisiones de diseño que determinan su rendimiento y confiabilidad. Comprender esta estructura es fundamental para interpretar cómo se ejecutan las instrucciones y cómo se administran los recursos del sistema, ya que dichas decisiones no solo impactan la eficiencia, sino también la forma en que la información es procesada y protegida dentro del computador (Martínez Amador, 2012).

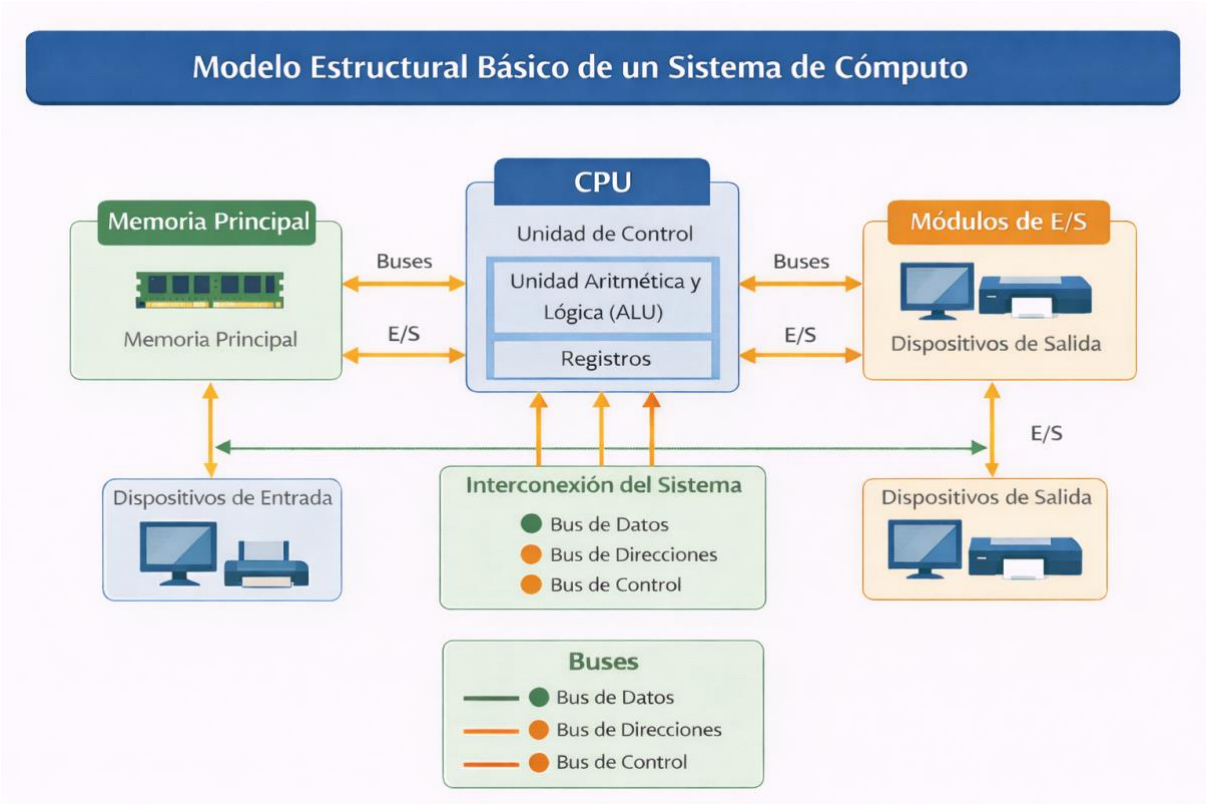
La evolución de las arquitecturas ha respondido a la necesidad de mejorar el desempeño y optimizar los recursos, incorporando nuevos modelos como arquitecturas más modulares y conjuntos de instrucciones eficientes. Sin embargo, cada avance tecnológico introduce también nuevos riesgos, pues los cambios en la forma de procesar y almacenar la información generan posibles puntos de fallo y superficies de ataque a nivel de hardware. Por ello, el estudio de la arquitectura resulta clave para comprender el origen de vulnerabilidades que no pueden ser mitigadas únicamente desde el software (Ibarra Mayorga, 2009).

Desde un enfoque de ciberseguridad, la arquitectura de computadoras permite analizar el sistema como un conjunto de activos críticos que deben ser protegidos desde su diseño. Arquitecturas abiertas como RISC-V facilitan el análisis y la verificación de mecanismos de seguridad, promoviendo una integración temprana de la protección de la información. En el ámbito académico, se reconoce la necesidad de fortalecer la enseñanza de la arquitectura con un enfoque en seguridad, de modo que los estudiantes desarrollen competencias para identificar componentes críticos, anticipar riesgos y comprender la importancia de la seguridad desde el nivel más básico del sistema (Jaramillo Villegas et al., 2022).

La figura 1 muestra la estructura básica de un sistema de cómputo.

Figura 1

Modelo estructural básico de un sistema de cómputo



Descripción: Relación entre CPU, memoria y dispositivos de entrada/salida.

Autor: Milton Román.

1.1 CONCEPTOS BÁSICOS DE ARQUITECTURA Y SU RELACIÓN CON LA SEGURIDAD DE LA INFORMACIÓN

La arquitectura de computadores es la disciplina que estudia la estructura y organización funcional de un sistema de cómputo, definiendo cómo interactúan sus componentes principales como el procesador, memoria y dispositivos de entrada/salida y qué atributos del sistema son visibles para el programador (Stallings, 2019).

La seguridad de la información se sustenta en tres pilares: confidencialidad, integridad y disponibilidad. Sin embargo, estos principios dependen directamente del diseño arquitectónico.

Por ejemplo:

- La segmentación de memoria evita accesos no autorizados.
- Los niveles de privilegio limitan operaciones críticas.
- El aislamiento de procesos reduce propagación de ataques.

La Seguridad de la Información no solo es un asunto de políticas o cifrado; es también una consecuencia del diseño del hardware.

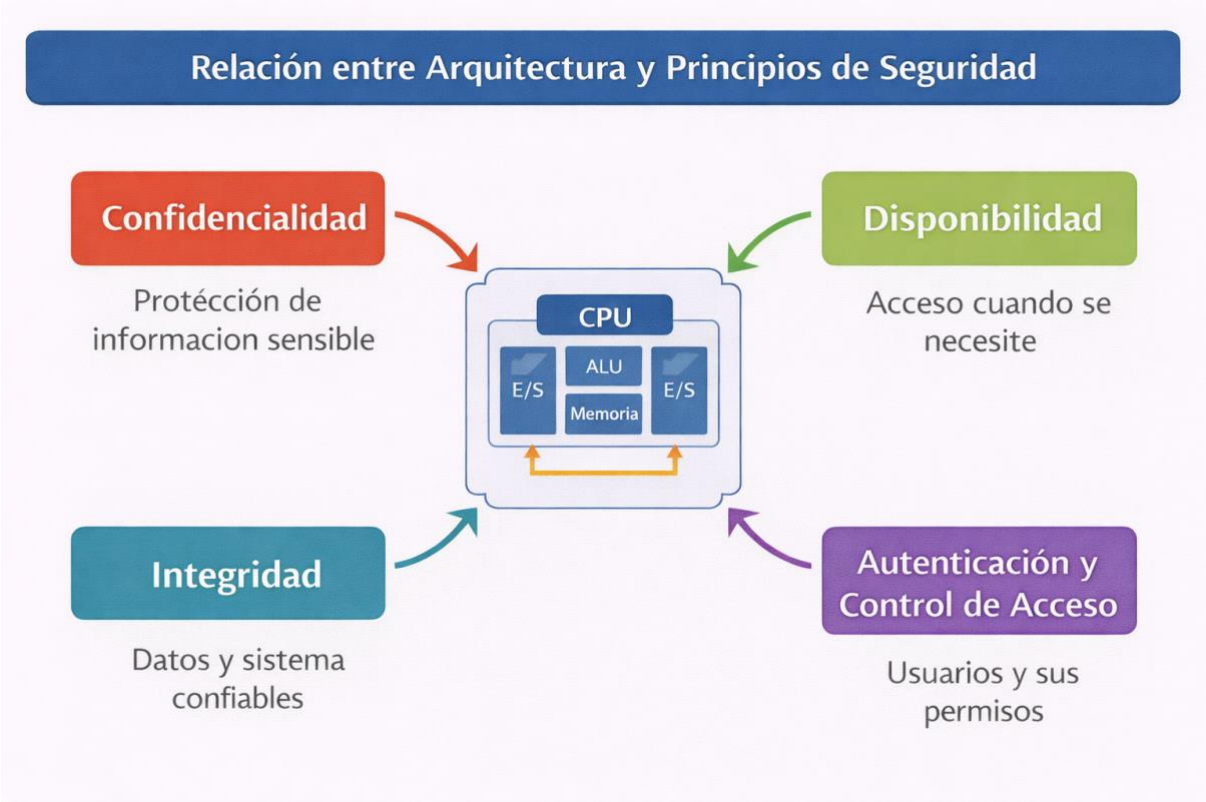
Un fallo en la gestión de memoria puede comprometer todo el sistema.

El hardware mal diseñado amplifica vulnerabilidades del software.

En la figura 2 se indica la relación entre la arquitectura de un sistema de cómputo con los principios de ciberseguridad.

Figura 2

Relación entre arquitectura y principios de seguridad



Descripción: Cómo los componentes arquitectónicos influyen en confidencialidad, integridad y disponibilidad.

Autor: Milton Román.

En arquitecturas modernas se incorporan mecanismos como:

- NX Bit (No Execute bit): Impide que el procesador ejecute código almacenado en regiones de memoria destinadas solo a datos, como la pila (stack) o el montón (heap)
- Trusted Platform Module (TPM): Chip de seguridad que protege claves criptográficas y garantiza que el sistema no ha sido alterado desde el arranque
- Arranque seguro (Secure Boot): Mecanismo de seguridad a nivel de firmware cuyo objetivo es garantizar que el sistema solo arranque software confiable y no modificado.

Estos elementos demuestran que la seguridad comienza en el hardware.

1.2 AMENAZAS A NIVEL HARDWARE Y EVOLUCIÓN DE LOS ATAQUES DE BAJO NIVEL

Las amenazas a nivel hardware comprenden aquellas vulnerabilidades que se originan en el diseño y funcionamiento interno de los componentes del sistema de cómputo, como el procesador, la memoria y los mecanismos de comunicación. A diferencia de los ataques de software, estas amenazas actúan en capas profundas del sistema, donde los controles tradicionales suelen ser insuficientes. El análisis de la arquitectura de computadoras permite comprender cómo ciertas decisiones de diseño pueden generar puntos débiles que afectan directamente la confidencialidad, integridad y disponibilidad de la información (Martínez Amador, 2012).

La evolución de las arquitecturas de computadoras ha impulsado mejoras significativas en rendimiento y eficiencia, incorporando mayor complejidad estructural y funcional. Sin embargo, estos avances también han ampliado la superficie de ataque, ya que nuevas técnicas como el paralelismo y la gestión avanzada de memoria introducen escenarios que pueden ser explotados por atacantes. En este contexto, las amenazas han dejado de centrarse exclusivamente en el software para dirigirse hacia el hardware, evidenciando que los componentes físicos ya no pueden considerarse intrínsecamente confiables (Ibarra Mayorga, 2009).

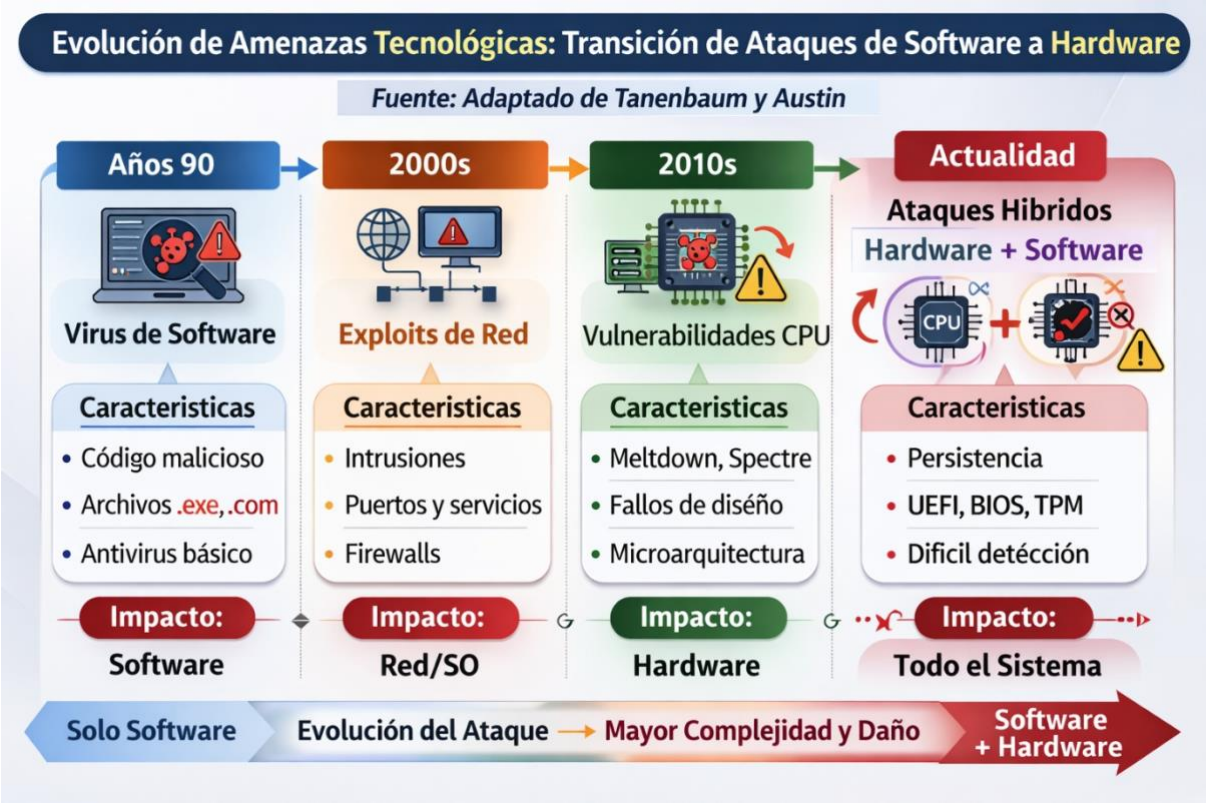
Los ataques de bajo nivel se caracterizan por aprovechar debilidades en los mecanismos internos del sistema, permitiendo evadir controles de seguridad implementados en capas superiores.

Frente a este panorama, resulta fundamental integrar la seguridad desde el diseño arquitectónico. Arquitecturas abiertas como RISC-V facilitan el análisis detallado del funcionamiento del procesador, favoreciendo la identificación temprana de vulnerabilidades y la aplicación de medidas de protección desde el nivel más básico del sistema (Jaramillo Villegas et al., 2022). Además, estudios sobre la enseñanza de la arquitectura de computadoras destacan la necesidad de formar profesionales capaces de reconocer estas amenazas y anticipar riesgos asociados al hardware, fortaleciendo así la seguridad integral de los sistemas informáticos (Fabra Gallo et al., 2020).

En la figura3 se representa la evolución histórica de las amenazas tecnológicas.

Figura 3

Evolución de amenazas tecnológicas



Descripción: Transición de ataques de software a ataques de hardware.

Fuente: Adaptado de Tanenbaum y Austin (2013).

En los años 90, los ataques se concentraban principalmente en virus de software, que afectaban aplicaciones y sistemas operativos. Durante los años 2000, el foco se desplazó hacia los exploits de red, aprovechando fallas en servicios conectados a Internet y en protocolos de comunicación.

En la década de 2010, surgieron amenazas más sofisticadas basadas en vulnerabilidades de la CPU, como ataques por canal lateral, que explotan características internas del hardware. Finalmente, en la actualidad, predominan los ataques híbridos hardware–software, donde se combinan debilidades del diseño arquitectónico con fallas del software.

La seguridad informática ya no puede limitarse al nivel del software, sino que debe abordarse desde la arquitectura del sistema, integrando mecanismos de protección en hardware, firmware y software de manera conjunta (Tanenbaum & Austin, 2013).

Este cambio obliga a los ingenieros en ciberseguridad a comprender profundamente la arquitectura interna del sistema.

Impacto estratégico en la ingeniería en ciberseguridad

La arquitectura moderna incorpora virtualización, múltiples niveles de privilegio y ejecución paralela. Cada uno de estos avances introduce nuevas superficies de ataque.

Por ejemplo:

- La virtualización mal configurada puede permitir escape de máquina virtual.
- El acceso directo a memoria (DMA) puede eludir controles del sistema operativo.
- El firmware comprometido puede persistir incluso tras reinstalar el sistema.

La protección efectiva requiere comprender cómo interactúan hardware, firmware y software.

La ciberseguridad actual exige dominio técnico del nivel más bajo del sistema.

En la figura 4 se explica de forma visual que la seguridad debe considerarse en todas las capas del sistema, no solo en las aplicaciones, porque cada nivel introduce riesgos distintos.

Figura 4

Capas del sistema y posibles puntos de ataque

Descripción: Representación por capas desde hardware hasta aplicaciones.

Autor: Milton Román.

La tendencia futura apunta hacia arquitecturas con seguridad integrada por diseño (Security by Design), donde los mecanismos de protección se implementan desde el nivel físico.

2. COMPONENTES FUNDAMENTALES DEL COMPUTADOR

Un computador está compuesto por distintos elementos de hardware que trabajan de manera coordinada para ejecutar instrucciones, procesar datos y comunicarse con el entorno. Desde una perspectiva de ciberseguridad, cada componente representa un activo que puede ser objetivo de ataque. Comprender su función es el primer paso para identificar riesgos.

2.1 ANÁLISIS DEL CPU, MEMORIA, DISPOSITIVOS DE ALMACENAMIENTO Y PERIFÉRICOS

Unidad Central de Procesamiento (CPU)

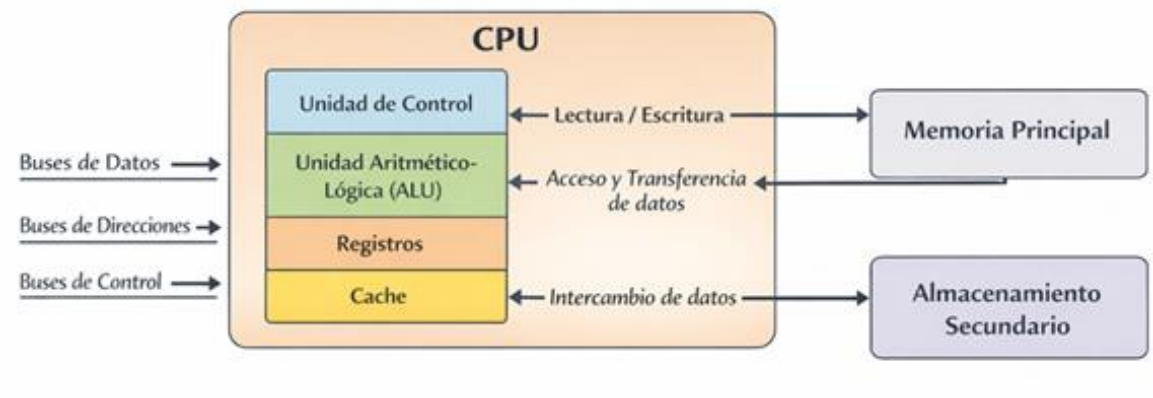
La CPU es el componente encargado de interpretar y ejecutar las instrucciones de los programas. Incluye la unidad de control, la unidad aritmética lógica y registros internos. Debido a su rol central, cualquier fallo o manipulación en la CPU afecta a todo el sistema (Stallings, 2019).

La CPU no solo ejecuta código legítimo, también puede ejecutar instrucciones maliciosas si estas logran cargarse en memoria. Además, optimizaciones como la ejecución especulativa o el uso de caché introducen comportamientos temporales que pueden ser observados externamente (Tanenbaum & Austin, 2013).

En la figura 5 se muestra la estructura de la CPU y su relación con la memoria.

Figura 5

Estructura básica de la CPU y su relación con la memoria y almacenamiento secundario (Tanenbaum & Austin, 2013).



Autor: Milton Román adaptado de Tanembaum.

Para reforzar el conocimiento sobre el funcionamiento del procesador, te invito a ver el siguiente video:

Título: ¿Qué es un procesador y cómo funciona?

Descripción: Video que explica qué es un procesador CPU y cómo funciona.

Enlace: https://www.youtube.com/watch?v=6Zhrgq5jiAs

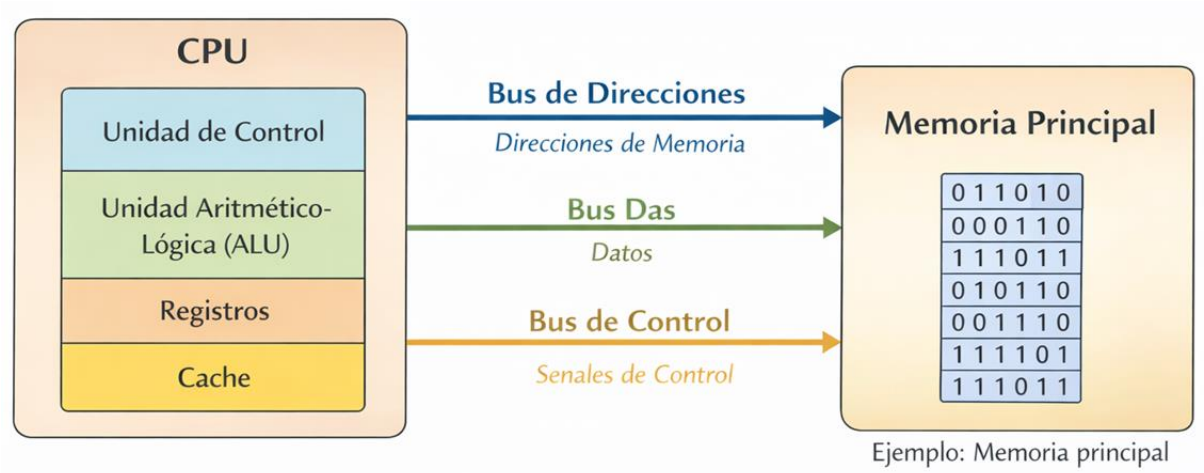
Memoria principal (RAM)

La memoria RAM almacena temporalmente datos e instrucciones en uso. Es volátil y altamente accesible para la CPU, lo que la convierte en un componente crítico desde el punto de vista de seguridad (Stallings, 2019).

Un manejo incorrecto de la memoria puede permitir que datos sensibles permanezcan accesibles más tiempo del necesario. Desde la arquitectura, la forma en que se direcciona y protege la memoria influye directamente en la exposición del sistema a ataques (Tanenbaum & Austin, 2013). La figura 6 destaca la relación entre la CPU y la memoria principal.

Figura 6

Relación entre CPU y memoria principal en la arquitectura Von Neumann (Stallings, 2018).



Autor: Milton Román

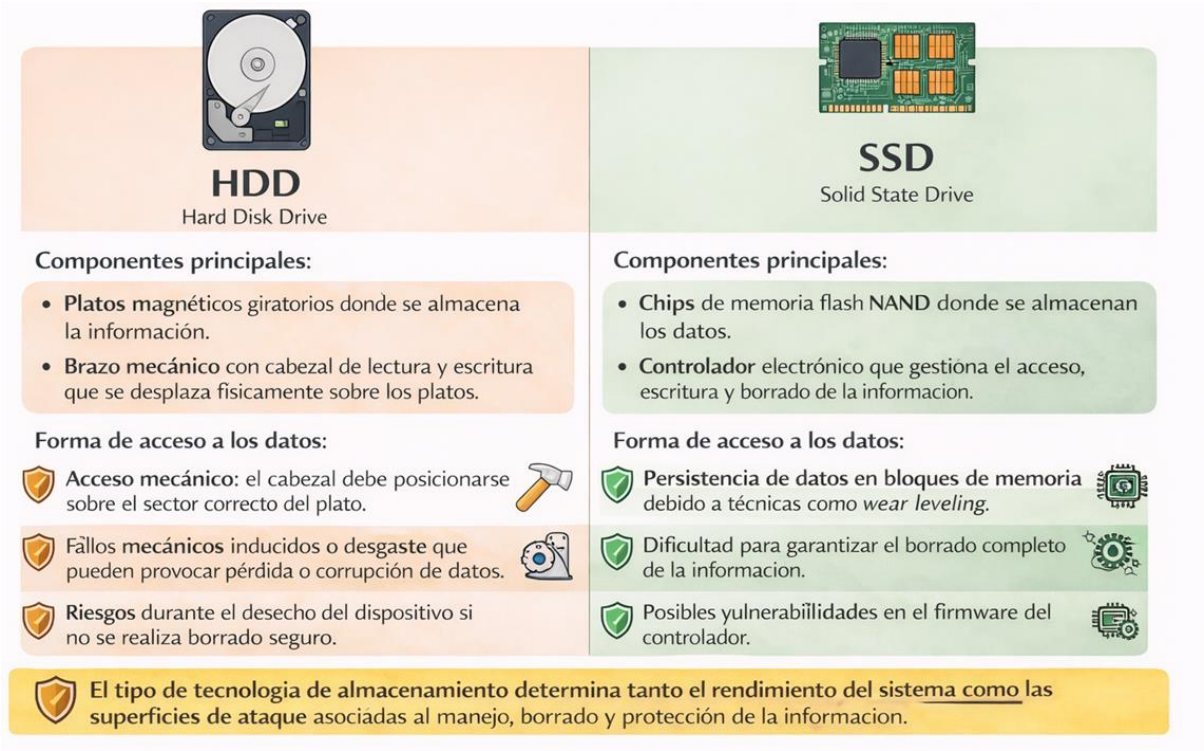
Dispositivos de almacenamiento

El almacenamiento (HDD - Hard Disk Drive, SSD - Solid State Drive, NVMe - Non-Volatile Memory Express) permite conservar información de forma persistente. Aquí residen el sistema operativo, aplicaciones y datos del usuario. A diferencia de la memoria, su contenido permanece incluso cuando el sistema se apaga (Stallings, 2019).

La persistencia del almacenamiento lo convierte en un objetivo prioritario para atacantes que buscan robar o alterar información. Además, los controladores de almacenamiento también forman parte de la superficie de ataque (Tanenbaum & Austin, 2013). En la figura 7 se realiza una comparación conceptual entre un HDD y SDD.

Figura 7

Comparación conceptual entre HDD y SSD.



Autor: Milton Román

Periféricos y dispositivos de entrada/salida

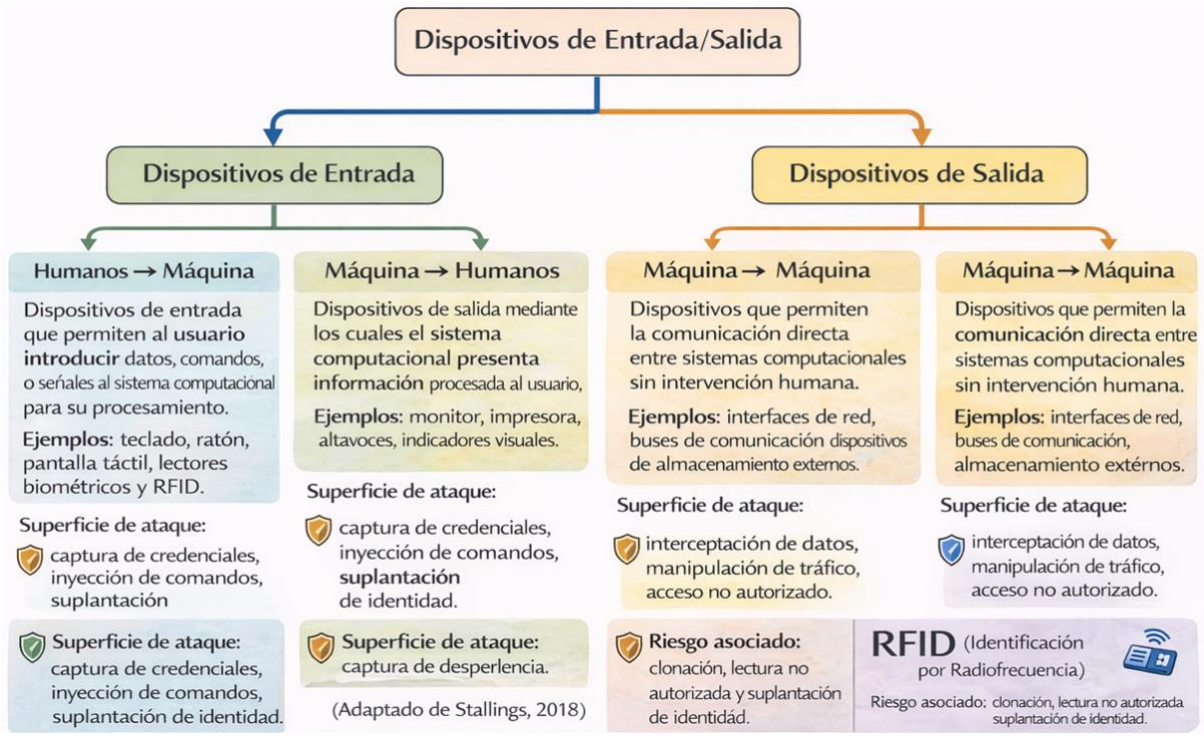
Los periféricos permiten la interacción del computador con el entorno: teclado, mouse, impresoras, cámaras, dispositivos USB, entre otros. Aunque suelen considerarse elementos secundarios, representan una de las principales puertas de entrada para ataques físicos y lógicos (Stallings, 2019).

Un periférico malicioso puede introducir código o manipular el comportamiento del sistema sin necesidad de explotar software (Tanenbaum & Austin, 2013).

La figura 8 muestra una descripción de la clasificación de dispositivos de entrada salida de un equipo de cómputo.

Figura 8

Clasificación de dispositivos de entrada y salida (Stallings, 2018).



Descripción: *Dispositivos de entrada salida*

Autor: Milton Román (adaptado de Stallings)

2.2 IDENTIFICACIÓN DE POSIBLES PUNTOS DE FALLO Y SUPERFICIES DE ATAQUE

La identificación de posibles puntos de fallo y superficies de ataque constituye un aspecto central en el análisis de la arquitectura de computadoras desde la perspectiva de la ciberseguridad. Un punto de fallo se refiere a cualquier componente o mecanismo del sistema cuya falla, mal funcionamiento o compromiso pueda afectar la disponibilidad, integridad o confidencialidad de la información. Por su parte, la superficie de ataque corresponde al conjunto de interfaces, componentes y rutas a través de las cuales un atacante puede intentar explotar vulnerabilidades del sistema. Ambos conceptos están directamente condicionados por las decisiones arquitectónicas adoptadas en el diseño del computador (Martínez Amador, 2012).

Desde el nivel de hardware, componentes como el CPU, la memoria principal, los dispositivos de almacenamiento y los periféricos representan puntos críticos que pueden convertirse en superficies de ataque si no se diseñan y gestionan adecuadamente. Por ejemplo, la forma en que el procesador administra los privilegios de ejecución o cómo se controla el acceso a la memoria puede permitir la ejecución de código no autorizado o la exposición de datos sensibles. La arquitectura define estos mecanismos de control y, por tanto, determina en gran medida la resistencia del sistema frente a ataques de bajo nivel que explotan debilidades estructurales (Ibarra Mayorga, 2009).

La evolución de las arquitecturas de computadoras ha demostrado que el incremento en complejidad y rendimiento suele ir acompañado de un aumento en la superficie de ataque. Nuevas funcionalidades, mayor paralelismo y arquitecturas más sofisticadas introducen múltiples puntos de interacción entre componentes, lo que incrementa las posibilidades de fallo o explotación. En este sentido, comprender cómo han evolucionado las arquitecturas permite anticipar riesgos y entender por qué las amenazas actuales ya no se limitan al software, sino que también apuntan directamente al hardware y a sus mecanismos internos (Ibarra Mayorga, 2009).

El enfoque moderno en la enseñanza de la arquitectura de computadoras resalta la necesidad de analizar estos riesgos desde una perspectiva integral. Según (Martínez Amador, 2012), el

estudiante debe desarrollar competencias que le permitan no solo identificar los componentes fundamentales del sistema, sino también evaluar cómo su funcionamiento interno puede convertirse en una debilidad si no se consideran aspectos de seguridad desde el diseño. Esto implica reconocer dependencias críticas, cuellos de botella y elementos cuya falla comprometería el sistema completo.

Arquitecturas abiertas como RISC-V ofrecen una oportunidad relevante para el análisis de puntos de fallo y superficies de ataque, ya que permiten estudiar con mayor transparencia el diseño del procesador y sus mecanismos de control. Al conocer en detalle el conjunto de instrucciones y la organización interna del sistema, es posible identificar con mayor precisión dónde podrían surgir vulnerabilidades y cómo mitigarlas desde el nivel arquitectónico. Este enfoque favorece una visión de seguridad desde el diseño, en la cual la protección de la información se integra como un principio fundamental del sistema y no como una medida correctiva posterior (Jaramillo Villegas et al., 2022).

Finalmente, diversos estudios sobre la enseñanza de la arquitectura de computadoras destacan la importancia de incorporar explícitamente el análisis de superficies de ataque en el currículo. El estudio comparado de (Fabra Gallo et al., 2020) evidencia que fortalecer estos contenidos permite formar profesionales capaces de identificar riesgos tempranos, comprender el impacto de los fallos arquitectónicos y diseñar sistemas más resilientes frente a amenazas tecnológicas. De este modo, la identificación de puntos de fallo y superficies de ataque se consolida como una competencia esencial para el desarrollo de soluciones informáticas seguras.

Para ampliar el conocimiento sobre ataques en hardware, se recomienda leer el siguiente artículo:

Título: Superficies de ataque.

Descripción: Artículo que explica lo que es una superficie de ataque y cómo reducirlo.

Enlace: https://ccnadesdecero.es/superficie-ataque-que-es-como-reducirlo/

Glosario:

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

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

Tanenbaum, A. S., & Austin, T. (2013). *Structured computer organization* (6ta ed.). Pearson. Obtenido de https://drive.google.com/file/d/0B1NiEWRZUkn1MjJLNzBHY2FNczA/view?resourcekey=0-ukOVGpbozeyE1U3HemKDPg

Von Neumann, J. (1945). *First draft of a report on the EDVAC.* University of Pennsylvania. Obtenido de https://www.cs.virginia.edu/~robins/FirstDraft.pdf

Definicion de términos destacados:

- **Arquitectura de Computadoras:** Conjunto de atributos funcionales visibles al programador que determinan cómo opera un sistema de cómputo, incluyendo su conjunto de instrucciones y organización básica.
- **Superficie de ataque**: Conjunto de puntos de un sistema donde un atacante puede intentar explotar vulnerabilidades.

Recursos de profundización:

Recurso 1:

Guía: Preguntas y respuestas

Descripción: Arquitectura de Computadoras y su relación con la Ciberseguridad

Enlace: Recurso de profundización 1.docx

Recurso 2:

Título del recurso relacionado: Ejercicio

Descripción del recurso: Identificación de puntos de fallo y superficies de ataque.

Enlace: Recurso de profundización 2.docx

ACTIVIDAD DE EVALUACIÓN:

PREGUNTAS DE AUTOEVALUACIÓN

<table>
<tr><td>INSTRUCCIONES:</td><td colspan="6">Lea cuidadosamente cada pregunta y seleccione una sola opción. Luego de responder, revise la retroalimentación asociada a cada alternativa para reforzar su aprendizaje.</td></tr>
<tr><td>Titulo:</td><td colspan="6">Arquitectura de Computadoras y Ciberseguridad</td></tr>
<tr><td>Dificultad:</td><td>x</td><td>Baja</td><td>x</td><td>Media</td><td></td><td>Alta</td></tr>
<tr><td rowspan="3">RDAs Evaluados:</td><td>x</td><td colspan="5">RDA 1</td></tr>
<tr><td></td><td colspan="5">RDA 2</td></tr>
<tr><td></td><td colspan="5">RDA 3</td></tr>
<tr><td>Reto:</td><td colspan="6">1</td></tr>
<tr><td>Secciones evaluadas:</td><td>1</td><td colspan="5">1. Introducción a la Arquitectura de Computadoras y Ciberseguridad
1.1 Conceptos básicos de arquitectura y su relación con la seguridad de la información
1.2 Amenazas a nivel hardware y evolución de los ataques de bajo nivel
2. Componentes fundamentales del computador
2.1 Análisis del CPU, memoria, dispositivos de almacenamiento y periféricos
2.2 Identificación de posibles puntos de fallo y superficies de ataque</td></tr>
</table>

PREGUNTA 1	¿Cuál es el principal objetivo de la arquitectura de computadoras desde el punto de vista de la seguridad de la información?
CORRECTA	Definir la estructura del sistema y los atributos visibles que influyen en la protección de los datos.
Incorrecta 1	Optimizar únicamente el rendimiento del hardware sin considerar la seguridad.
Incorrecta 2	Garantizar la seguridad solo a nivel de aplicaciones.
Incorrecta 3	Reemplazar las funciones del sistema operativo.
Retroalimentación de las respuestas	
Correcta	La arquitectura de computadoras establece cómo se organizan y comunican los componentes del sistema, definiendo atributos visibles para el programador que influyen directamente en la confidencialidad, integridad y disponibilidad de la información (Stallings, 2019).
Incorrecta 1	Aunque el rendimiento es un objetivo de la arquitectura, la seguridad no puede excluirse, ya que decisiones arquitectónicas influyen en la superficie de ataque del sistema.
Incorrecta 2	La seguridad no debe limitarse a las aplicaciones; debe considerarse desde el diseño del hardware, firmware y sistema operativo.
Incorrecta 3	La arquitectura define la base estructural del sistema, pero no sustituye las funciones del sistema operativo.
PREGUNTA 2	¿Cuál de las siguientes opciones corresponde a una amenaza a nivel hardware?
CORRECTA	Explotación de vulnerabilidades en la CPU mediante ejecución especulativa.
Incorrecta 1	Inyección SQL en una aplicación web.
Incorrecta 2	Robo de contraseñas por phishing.
Incorrecta 3	Error de validación en formularios de entrada.
Retroalimentación de las respuestas	
Correcta	Este tipo de amenaza explota características internas del procesador, afectando directamente al hardware y comprometiendo la seguridad del sistema desde su nivel más bajo (Tanenbaum & Austin, 2013).
Incorrecta 1	La inyección SQL es una vulnerabilidad de software a nivel de aplicación, no de hardware.
Incorrecta 2	El phishing es un ataque de ingeniería social, no una amenaza relacionada con el hardware.
Incorrecta 3	Este tipo de error corresponde a fallas en el desarrollo de software, no a vulnerabilidades de bajo nivel.

PREGUNTA 3	¿Cuál es la función principal del CPU dentro del sistema de cómputo?
CORRECTA	Ejecutar instrucciones y controlar el funcionamiento general del sistema.
Incorrecta 1	Almacenar permanentemente la información del usuario.
Incorrecta 2	Gestionar exclusivamente los dispositivos de entrada y salida.
Incorrecta 3	Proveer conectividad de red al sistema.
Retroalimentación de las respuestas	
CORRECTA	El CPU ejecuta instrucciones, coordina operaciones y controla el flujo de datos, siendo un componente crítico tanto para el funcionamiento como para la seguridad del sistema.
Incorrecta 1	El almacenamiento permanente corresponde a dispositivos como discos duros o memorias secundarias, no al CPU.
Incorrecta 2	Aunque el CPU participa en la gestión de E/S, esta no es su única ni principal función.
Incorrecta 3	La conectividad de red es responsabilidad de dispositivos y controladores específicos, no del CPU como función principal.
PREGUNTA 4	¿Qué se entiende por superficie de ataque en un sistema de cómputo?
CORRECTA	El conjunto de puntos del sistema donde puede producirse un ataque.
Incorrecta 1	La capacidad máxima de procesamiento del hardware.
Incorrecta 2	El número de aplicaciones instaladas en el sistema.
Incorrecta 3	El nivel de rendimiento del sistema operativo.
Retroalimentación de las respuestas	
CORRECTA	La superficie de ataque incluye hardware, firmware, sistema operativo y aplicaciones, y aumenta con la complejidad del sistema.
Incorrecta 1	La capacidad de procesamiento se relaciona con rendimiento, no con seguridad.
Incorrecta 2	Aunque más aplicaciones pueden aumentar la superficie de ataque, esta no se define únicamente por su cantidad.
Incorrecta 3	El rendimiento no define la superficie de ataque, aunque decisiones de diseño pueden influir en ella.

PUCE Virtual

síguenos en:

www.pucevirtual.puce.edu.ec