1. DATOS INFORMATIVOS

DOMINIO:			
CARRERA: Ingeniería en Ciberseguridad y Gestión de Tecnologías de la Información			
Asignatura/Módulo: Arquitectura de computadoras			
Paralelo:			**N° horas**
Plan de estudios:			H. aprendizaje en contacto con el docente: 32
Prerrequisitos: Matemáticas Discretas, Circuitos			
Periodo académico:			H. aprendizaje autónomo: 72
			H. aprendizaje práctico-experimental: 16
Docenteo o Co-Docente 1:	**Grado académico y título profesional:**	**Co-Docente 2:**	**Grado académico y título profesional:**
Javier Guaña Moya	Doctor en Ciencias Informáticas; Master en Ciberseguridad; Master en Redes y Telecomunicaciones		
Breve reseña de la actividad académica y/o profesional:		**Breve reseña de la actividad académica y/o**	
Experiencia Laboral: Gerente General y Presidente de la Compañía IYAYKUTEC Cía. Ltda.; Presidente Ejecutivo de la Compañía BASTCORP Cía. Ltda.; Administrador del área de Redes y Networking - Instituto Tecnológico Superior Japón; Coordinador del Área de Redes de Datos, Hardware y Arquitectura - Facultad de Ingeniería de la Pontificia Universidad Católica del Ecuador (PUCE); Director de Proyectos del Área de Networking en la empresa SYSTELCOM.		Experiencia Docente: Catedrático Universitario de Posgrado y Pregrado de la Pontificia Universidad Católica del Ecuador (PUCE); Universidad Central del Ecuador (UCE); Universidad Nacional de Chimborazo (UNACH), Universidad Politécnica Estatal del Carchi (UPEC); Universidad Técnica de Ambato (UTA); Universidad de las Américas (UDLA); Universidad Católica de Cuenca (UCC); Universidad Internacional del Ecuador (UIDE); Universidad Tecnológica Israel; Universidad Tecnológica Empresarial de Guayaquil (UTEG); Universidad Técnica Estatal de Quevedo (UTEQ); Universidad Metropolitana del Ecuador (UMET); Universidad Tecnológica América, Universidad Luis Vargas Torres, entre otras.	
Indicación de horario de atención al estudiante:			
Tutoría presencial:		**Teléfono:**	2991700 ext 2008
Tutoría virtual:		**Correo electrónico:**	eguana953@puce.edu.ec

2. DESCRIPCIÓN DE LA ASIGNATURA

La asignatura Arquitectura de Computadoras y Ciberseguridad introduce al estudiante de cuarto nivel en la comprensión del hardware como un componente crítico de la seguridad de la información. A partir de los principios de arquitectura, se analizan los componentes fundamentales del computador (CPU, memoria, almacenamiento y periféricos) para identificar puntos de fallo y superficies de ataque. Se estudia la arquitectura Von Neumann y cómo sus decisiones de diseño influyen en la ejecución de código malicioso y en la protección de datos. El curso aborda el funcionamiento interno del procesador, la ejecución de instrucciones y los niveles de privilegio usuario-kernel, conectándolo con riesgos de escalamiento. En gestión de memoria se revisan memoria virtual, paginación y segmentación, así como vulnerabilidades clásicas (buffer overflow y corrupción de memoria). Se profundiza en firmware y proceso de arranque (BIOS/UEFI), persistencia de malware y técnicas de protección, incluyendo Secure Boot y Trusted Boot como parte de la cadena de confianza. Además, se estudian almacenamiento (HDD/SSD/NVMe), borrado seguro y ataques al controlador; arquitectura de I/O y DMA con riesgos por dispositivos maliciosos. Finalmente, se introduce la virtualización (hipervisores, VMs y contenedores) y vulnerabilidades comunes como DoS y DDoS, con actividades prácticas orientadas a análisis y hardening básico.

3. DESCRIPCIÓN DE COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

COMPETENCIAS TRANSVERSALES	COMPETENCIAS DISCIPLINARES DEL DOMINIO	RESULTADOS DE APRENDIZAJE DE LA CARRERA	RESULTADOS DE APRENDIZAJE DE LA ASIGNATURA
Creativo, crítico y analítico	**Evaluación del entorno complejo.** Valorar necesidades del entorno para dar respuestas a problematicas y desafios del habitat	5.Evaluar críticamente la efectividad y limitaciones de las soluciones tecnológicas actuales y emergentes en diferentes áreas de la computación.	Identificar los componentes fundamentales de una computadora y su funcionamiento.
Creativo, crítico y analítico	**Transformacion pertinente y sostenible del habitat** Aplicar conocimientos de forma pertinente y sostenible en relation con los desafios del habitat	7.Diseñar soluciones de seguridad en un entorno empresarial trabajando de manera colaborativa.	Comprender la arquitectura de la CPU, la memoria, el almacenamiento y los dispositivos de entrada y salida, así como la interacción entre el hardware y el software de una computadora.
Creativo, crítico y analítico	**Aplicación de lenguajes especiales objetuales, visuales y verbales.** Comunicar ideas, procesos y resultados a traves de lenguajes diversos aplicados al contexto	8.Aplicar de manera efectiva las nuevas tendencias y tecnologías en ciberseguridad y tecnologías de la información.	Diseñar soluciones eficientes en términos de consumo de recursos para diferentes tipos de aplicaciones.

4. EVALUACIÓN DE LOGROS DE APRENDIZAJE

PROYECTO DEL NIVEL	Retos	Resultado de aprendizaje	Pesos	Definición del criterio de evaluación del RdA	Ponderación criterios	Nivel de logro alcanzado al RdA				Observaciones (Alertas para tutorías académicas)
						Alcanzado con excelencia (A) (45-50)	Alcanzado muy bueno (B) (40-44)	Alcanzado bueno (C) (30-39)	Pendiente de alcanzar (D) (29 y menos)	
Tema del proyecto Cadena de confianza y superficies de ataque en un computador: del hardware al hipervisor Objetivo general Analizar la arquitectura de un computador desde una perspectiva de ciberseguridad para identificar superficies de ataque y riesgos asociados a CPU, memoria, firmware/arranque, almacenamiento, I/O, DMA y virtualización, proponiendo medidas básicas de protección.	Reto 1: Construir un modelo claro del computador para reconocer activos críticos, superficies de ataque y riesgos iniciales por componente	Identificar los componentes fundamentales de una computadora y su funcionamiento.	33.33	Criterio 1: Ubica la arquitectura del sistema (diagrama + inventario)	50%	Ubica la arquitectura del sistema, y el inventario completos, precisos y muy claros; incluye CPU, memoria, almacenamiento, periféricos e	Ubica la arquitectura del sistema casi completo y claro; mínimos faltantes o detalles menores	Ubica la arquitectura del sistema de forma básico; incluye lo principal pero con vacíos o generalidades; claridad aceptable	No ubica la arquitectura del sistema, y la información es incompleto/confuso; faltan componentes clave o hay errores relevantes	Para el nivel pendiente de alcanzar (D) el estudiante deberá realizar más trabajos que le permitan reforzar conocimiento teórico-práctico.
				Criterio 2: Identifica y prioriza superficies de ataque y riesgos	50%	Identifica y prioriza superficies de ataque y riesgos en base a la arquitectura de computadoras	Casi completo y claro; mínimos faltantes o detalles menores	Básico; incluye lo principal pero con vacíos o generalidades; claridad aceptable	Incompleto/confuso; faltan componentes clave o hay errores relevantes	Para el nivel pendiente de alcanzar (D) el estudiante deberá realizar más trabajos que le permitan reforzar conocimiento teórico-práctico.
	Reto 2: Comprender cómo CPU, niveles de privilegio y memoria (virtual/paginación/segmentación) se conectan con vulnerabilidades como buffer overflow y corrupción de memoria	Comprender la arquitectura de la CPU, la memoria, el almacenamiento y los dispositivos de entrada y salida, así como la interacción entre el hardware y el software de una computadora.	33.33	Criterio 1: Explica el CPU, ejecución y niveles de privilegio (usuario/kernel)	50%	Explica de forma clara, correcta y bien conectada con seguridad; distingue privilegios con precisión	Explica de forma general; algunas confusiones; se entiende lo esencial	Explica de forma básica; algunas confusiones; se entiende lo esencial	Explica de forma incompleta o incorrecta; no diferencia usuario/kernel o no lo vincula a seguridad	Para el nivel pendiente de alcanzar (D) el estudiante deberá realizar más trabajos que le permitan reforzar conocimiento teórico-práctico.
				Criterio 2: Reconoce la memoria y vulnerabilidades con controles básicos	50%	Reconoce la memoria y vulnerabilidades con controles básicos de forma clara, correcta y bien conectada con la	Reconoce la memoria y vulnerabilidades con controles básicos de forma general en base a la arquitectura del computador	Reconoce la memoria y vulnerabilidades de forma básica en base a la arquitectura del computador	No reconoce la memoria y vulnerabilidades con controles básicos y no se basa en la arquitectura del computador	Para el nivel pendiente de alcanzar (D) el estudiante deberá realizar más trabajos que le permitan reforzar conocimiento teórico-práctico.
	Reto 3: Analizar BIOS/UEFI y el proceso de arranque para proponer una cadena de confianza con Secure Boot/Trusted Boot y medidas básicas de Reto 4: Integrar riesgos en almacenamiento (HDD/SSD/NVMe), periféricos/I/O, DMA y virtualización (VMs/contenedores) para diseñar un checklist de protección básico.	Diseñar soluciones eficientes en términos de consumo de recursos para diferentes tipos de aplicaciones.	33.34	Criterio 1: Describe el proceso de arranque y la cadena de confianza	50%	Describe de forma completa y correcta por etapas; diagrama claro y coherente; explica el rol de cada fase	Describe de forma general, pero faltan detalles y no genera coherencia en cada fase	Describe de forma básica; omite pasos o confunde algunos términos, pero mantiene la idea central	Describe de forma incompleta/errónea; no se entiende la cadena de confianza	Para el nivel pendiente de alcanzar (D) el estudiante deberá realizar más trabajos que le permitan reforzar conocimiento teórico-práctico.
				Criterio 2: Analiza riesgos en almacenamiento, I/O, DMA y virtualización	50%	Analiza de forma integral y coherente; cubre todas las áreas; distingue VMs vs contenedores y explica escape de VM con claridad	Analiza de forma general; pocas omisiones; buena claridad técnica	Análisis básico; cubre lo mínimo con vacíos o superficialidad	Análisis incompleto o con errores; omite áreas clave (DMA/virtualización)	Para el nivel pendiente de alcanzar (D) el estudiante deberá realizar más trabajos que le permitan reforzar conocimiento teórico-práctico.

5. METODOLOGÍA

La asignatura se enseña con un enfoque de aprendizaje basado en retos y proyectos, articulando teoría y práctica para que el estudiante comprenda la arquitectura del computador desde la ciberseguridad. Cada unidad inicia con lecturas, cápsula breve y glosario, y continúa con microlecciones en clase para explicar conceptos clave (componentes, Von Neumann, CPU/privilegios, memoria, firmware/arranque, almacenamiento, I/O, DMA y virtualización). Luego se trabaja con casos y análisis guiado (tablas de riesgos, diagramas de flujo, cadena de confianza) para conectar cada componente con su superficie de ataque, amenazas típicas y consecuencias sobre la confidencialidad, integridad y disponibilidad. La enseñanza se orienta a un enfoque defensivo y ético, priorizando comprensión, verificación y hardening básico, sin prácticas ofensivas en sistemas reales.

La parte práctica se desarrolla en un laboratorio controlado (equipo real o máquinas virtuales) donde el estudiante debe observar, documentar y justificar: levantar inventario de hardware y periféricos, representar el arranque BIOS/UEFI y la cadena de confianza, revisar conceptos de memoria y permisos, y analizar riesgos en almacenamiento, I/O, DMA y virtualización (VMs/contenedores). El curso se organiza en cuatro retos progresivos, con productos verificables (diagramas, matriz de riesgos, checklist de controles e informe técnico) y evaluación continua mediante evidencias, retroalimentación y ajustes. Al cierre de cada tema se aplica una verificación breve (quiz o ticket de salida) y una reflexión técnica para consolidar aprendizajes y asegurar que el estudiante pueda explicar qué riesgo existe, por qué ocurre y qué medida básica lo reduce

6. RELACIÓN RESULTADOS DE APRENDIZAJE, EXPERIENCIAS DE APRENDIZAJES Y DIMENSIÓN DEL CONOCIMIENTO

PROYECTO DE NIVEL	RETOS	RESULTADOS DE APRENDIZAJE DE LA ASIGNATURA	Semanas	Experiencias / estrategias Aprendizaje en contacto con el docente	Horas	Recursos	Escenario	Experiencias / estrategias de aprendizaje práctico-experimental:	Horas	Recursos	Escenario	Experiencias / estrategias de aprendizaje autónomo	Horas	Recursos	Escenario	DIMENSIÓN DEL CONOCIMIENTO (conceptos, hecho, procedimientos o principios)
Tema del proyecto Cadena de confianza y superficies de ataque en un computador: del hardware al hipervisor Objetivo general Analizar la arquitectura de un computador desde una perspectiva de ciberseguridad para identificar superficies de ataque y riesgos asociados a CPU, memoria, firmware/arranque, almacenamiento, I/O, DMA y virtualización, proponiendo medidas básicas de protección.	Reto 1: Construir un modelo claro del computador para reconocer activos críticos, superficies de ataque y riesgos iniciales por componente	Identificar los componentes fundamentales de una computadora y su funcionamiento.	1	Tutorias sincrónicas por videoconferencia.	2	Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma	Entorno virtual de aprendizaje, weblabs, software especializado	Resolución de retos con el uso del Laboratorio de cómputo.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o	Entorno virtual de aprendizaje, weblabs, software especializado	Consulta e investigación, resolución de problemas sobre el tema en estudio	4	Computador personal, herramientas de software necesarias	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	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	Tutorias sincrónicas por videoconferencia.	2	Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma	Entorno virtual de aprendizaje, weblabs, laboratorio, software especializado	Resolución de problema práctico.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o	Entorno virtual de aprendizaje, weblabs, software especializado	Consulta e investigación, resolución de problemas sobre el tema en estudio	5	Computador personal, herramientas de software necesarias	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	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.
			3	Tutorias sincrónicas por videoconferencia.	2	Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma	Entorno virtual de aprendizaje, weblabs, software especializado	Resolución de retos con el uso del Laboratorio de cómputo.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o	Entorno virtual de aprendizaje, weblabs, software especializado	Consulta e investigación, resolución de problemas sobre el tema en estudio	4	Computador personal, herramientas de software necesarias	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	3. Arquitectura Von Neumann y su impacto en la seguridad 3.1. Comparación de modelos arquitectónicos y cómo influyen en la ejecución de código malicioso y en la protección de datos.
			4	Tutorias sincrónicas por videoconferencia.	2	Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma	Entorno virtual de aprendizaje, weblabs, software especializado	Resolución de problema práctico.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o	Entorno virtual de aprendizaje, weblabs, software especializado	Consulta e investigación, resolución de problemas sobre el tema en estudio	5	Computador personal, herramientas de software necesarias	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	4. Funcionamiento del procesador (CPU) 4.1. .Arquitectura interna del CPU 4.2. Ejecución de instrucciones y niveles de privilegio (usuario y kernel) desde una perspectiva básica.
	Reto 2: Comprender cómo CPU, niveles de privilegio y memoria (virtual/paginación/segmentación) se conectan con vulnerabilidades como buffer overflow y corrupción de memoria	Comprender la arquitectura de la CPU, la memoria, el almacenamiento y los dispositivos de entrada y salida, así como la interacción entre el hardware y el software de una computadora.	5	Tutorias sincrónicas por videoconferencia.	2	Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma	Entorno virtual de aprendizaje, weblabs, software especializado	Resolución de retos con el uso del Laboratorio de cómputo.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o	Entorno virtual de aprendizaje, weblabs, software especializado	Consulta e investigación, resolución de problemas sobre el tema en estudio	4	Computador personal, herramientas de software necesarias	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	5. Gestión de memoria y virtualización 5.1. Memoria física, memoria virtual, paginación y segmentación 5.2. Vulnerabilidades como buffer overflow y memory corruption.
			6	Tutorias sincrónicas por videoconferencia.	2	Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma	Entorno virtual de aprendizaje, weblabs, software especializado	Resolución de problema práctico.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o	Entorno virtual de aprendizaje, weblabs, software especializado	Consulta e investigación, resolución de problemas sobre el tema en estudio	5	Computador personal, herramientas de software necesarias	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	6. Firmware y proceso de arranque 6.1. BIOS y UEFI 6.2. Proceso de inicio del sistema y su importancia en la seguridad del computador.
			7	Tutorias sincrónicas por videoconferencia.	2	Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma	Entorno virtual de aprendizaje, weblabs, software especializado	Resolución de retos con el uso del Laboratorio de cómputo.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o	Entorno virtual de aprendizaje, weblabs, software especializado	Consulta e investigación, resolución de problemas sobre el tema en estudio	4	Computador personal, herramientas de software necesarias	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	6.3. Funcionamiento, riesgos de seguridad, persistencia de malware a nivel firmware y técnicas de protección.
			8	Tutorias sincrónicas por videoconferencia.	2	Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma	Entorno virtual de aprendizaje, weblabs, software especializado	Resolución de problema práctico.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o	Entorno virtual de aprendizaje, weblabs, software especializado	Consulta e investigación, resolución de problemas sobre el tema en estudio	5	Computador personal, herramientas de software necesarias	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	7. Arranque seguro (Secure Boot y Trusted Boot) 7.1. Mecanismos de verificación de integridad durante el arranque y su rol en la cadena de confianza.
	Reto 3: Analizar BIOS/UEFI y el proceso de arranque para proponer una cadena de confianza con Secure Boot/Trusted Boot y medidas básicas de protección	Diseñar soluciones eficientes en términos de consumo de recursos para diferentes tipos de aplicaciones.	9	Tutorias sincrónicas por videoconferencia.	2	Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma	Entorno virtual de aprendizaje, weblabs, software especializado	Resolución de retos con el uso del Laboratorio de cómputo.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o	Entorno virtual de aprendizaje, weblabs, software especializado	Consulta e investigación, resolución de problemas sobre el tema en estudio	4	Computador personal, herramientas de software necesarias	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	8. Almacenamiento y protección de datos 8.1. Tipos de almacenamiento (HDD, SSD, NVMe) 8.2. Seguridad de la información almacenada
			10	Tutorias sincrónicas por videoconferencia.	2	Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma	Entorno virtual de aprendizaje, weblabs, software especializado	Resolución de retos con el uso del Laboratorio de cómputo.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o	Entorno virtual de aprendizaje, weblabs, software especializado	Consulta e investigación, resolución de problemas sobre el tema en estudio	5	Computador personal, herramientas de software necesarias	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	8.3. Conceptos básicos de borrado seguro, seguridad de datos y ataques al controlador de almacenamiento.
			11	Tutorias sincrónicas por videoconferencia.	2	Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma	Entorno virtual de aprendizaje, weblabs, software especializado	Resolución de problema práctico.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o	Entorno virtual de aprendizaje, weblabs, software especializado	Consulta e investigación, resolución de problemas sobre el tema en estudio	4	Computador personal, herramientas de software necesarias	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	9. Arquitectura de entrada y salida (I/O) 9.1. Comunicación del sistema con dispositivos externos y riesgos de seguridad asociados a periféricos.
			12	Tutorias sincrónicas por videoconferencia.	2	Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma	Entorno virtual de aprendizaje, weblabs, software especializado	Resolución de retos con el uso del Laboratorio de cómputo.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o	Entorno virtual de aprendizaje, weblabs, software especializado	Consulta e investigación, resolución de problemas sobre el tema en estudio	5	Computador personal, herramientas de software necesarias	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	10. Acceso Directo a Memoria - DMA 10.1. Funcionamiento del Acceso Directo a Memoria (DMA)
	Reto 4: Integrar riesgos en almacenamiento (HDD/SSD/NVMe), periféricos, I/O, DMA y virtualización (VMs/contenedores) para diseñar un checklist de protección básico.		13	Tutorias sincrónicas por videoconferencia.	2	Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma	Entorno virtual de aprendizaje, weblabs, software especializado	Resolución de problema práctico.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o	Entorno virtual de aprendizaje, weblabs, software especializado	Consulta e investigación, resolución de problemas sobre el tema en estudio	4	Computador personal, herramientas de software necesarias	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	10.2. Riesgos asociados, incluyendo ataques con dispositivos maliciosos.
			14	Tutorias sincrónicas por videoconferencia.	2	Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma	Entorno virtual de aprendizaje, weblabs, software especializado	Resolución de retos con el uso del Laboratorio de cómputo.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o	Entorno virtual de aprendizaje, weblabs, software especializado	Consulta e investigación, resolución de problemas sobre el tema en estudio	5	Computador personal, herramientas de software necesarias	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	11. Virtualización y arquitectura de hipervisores 11.1. Arquitectura de máquinas virtuales, contenedores 11.2. Riesgos de escape de VM.
			15	Tutorias sincrónicas por videoconferencia.	2	Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma	Entorno virtual de aprendizaje, weblabs, software especializado	Resolución de problema práctico.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o	Entorno virtual de aprendizaje, weblabs, software especializado	Consulta e investigación, resolución de problemas sobre el tema en estudio	4	Computador personal, herramientas de software necesarias	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	12. Introducción a vulnerabilidades comunes 12.1. Desbordamientos de memoria
			16	Tutorias sincrónicas por videoconferencia.	2	Dispositivos electrónicos portátiles o de escritorio. Conexión a internet. Plataforma	Entorno virtual de aprendizaje, weblabs, software especializado	Resolución de retos con el uso del Laboratorio de cómputo.	1	Computadora, acceso a internet, acceso al aula virtual, guia de laboratorio, weblab y/o	Entorno virtual de aprendizaje, weblabs, software especializado	Consulta e investigación, resolución de problemas sobre el tema en estudio	5	Computador personal, herramientas de software necesarias	Entorno virtual de aprendizaje, weblabs, software especializado, acceso a la biblioteca virtual	12.2. Ataques DoS, DDoS

8. BIBLIOGRAFÍA

a. BÁSICA / LIBROS

Bibliografía (basarse en normas APA)	Código Biblioteca PUCESI	Nro. de ejemplares
Arquitectura de computadoras con RISC-V	https://www.digitaliapublishing.com/a/136758/	1
Evolución de las arquitecturas de las computadoras	s://elibro.puce.elogim.com/es/lc/puce/titulos/28	1
Arquitectura de computadoras: basado en competencias para nivel superior	s://elibro.puce.elogim.com/es/lc/puce/titulos/13	1
Estudio comparado de los contenidos de la asignatura Arquitectura de Computadoras: oportunidades de mejoras	://dialnet.unirioja.es/servlet/articulo?codigo=859	1

Elaborado por:

Javier Guaña Moya

f) Docente

Revisado y Aprobado por:

Damián Nicolalde R
Coordinador de la carrera