

PLAN DOCENTE DE LA ASIGNATURA: Arquitectura de Seguridad en los Sistemas

CÓDIGO: 503236

CURSO ACADÉMICO: **2026/2027**

## PLAN DOCENTE DE LA ASIGNATURA

Curso académico: 2026/2027

Identificación y características de la asignatura					
Código	503236				
Denominación (español)	Arquitectura de Seguridad en los Sistemas				
Denominación (inglés)	System Security Architecture				
Titulaciones	Grado en Ingeniería Informática en Tecnologías de la Información				
Centro	Centro Universitario de Mérida <a href="http://www.unex.es/conoce-la-uex/estructura-academica/centros/cum">http://www.unex.es/conoce-la-uex/estructura-academica/centros/cum</a>				
Módulo	Módulo Contenidos Optativos en Tecnologías de la Información				
Materia	Ciberseguridad				
Carácter	Optativa	ECTS	6	Semestre	7
Profesorado					
Nombre		Despacho		Correo-e	
Josefa Díaz Álvarez		17		mjdiaz@unex.es	
Área de conocimiento	Arquitectura y Tecnología de los Computadores <a href="http://www.unex.es/conoce-la-uex/estructura-academica/centros/cum/centro/departamentos">http://www.unex.es/conoce-la-uex/estructura-academica/centros/cum/centro/departamentos</a>				
Departamento	Tecnología de los Computadores y de las Comunicaciones				
Profesor/a coordinador/a (si hay más de uno)					
Competencias / Resultados de aprendizaje					
Competencias generales					
CG3 - Capacidad para diseñar, desarrollar, evaluar y asegurar la accesibilidad, ergonomía, usabilidad y seguridad de los sistemas, servicios y aplicaciones informáticas, así como de la información que gestionan.					
CG4 - Capacidad para definir, evaluar y seleccionar plataformas hardware y software para el desarrollo y la ejecución de sistemas, servicios y aplicaciones informáticas, de acuerdo con los conocimientos adquiridos, según lo establecido en el anexo-2 de la Resolución de 8 de junio de 2009 de la Secretaría General de Universidades (BOE de 4 de Agosto de 2009) en el ámbito de las Tecnologías de la Información.					
CG8 - Conocimiento de las materias básicas y tecnologías, que capaciten para el aprendizaje y desarrollo de nuevos métodos y tecnologías, así como las que les doten de una gran versatilidad para adaptarse a nuevas situaciones.					
CG9 - Capacidad para resolver problemas con iniciativa, toma de decisiones, autonomía y creatividad. Capacidad para saber comunicar y transmitir los conocimientos, habilidades y destrezas de la profesión de Ingeniero Técnico en Informática.					
Competencias básicas					

CB1 - Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio
CB2 - Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio
CB3 - Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía
<b>Competencias específicas</b>
CEO2: Implementar sistemas y utilizar herramientas para minimizar los riesgos de una organización en el ciberespacio ante amenazas de seguridad. Aplicar estándares y procedimientos para proteger la confidencialidad, integridad y disponibilidad de los sistemas de información. (ASS)
<b>Competencias transversales</b>
CT12 - Diversidad e interculturalidad
CT15 - Comunicación interpersonal
<b>Contenidos</b>
<p>Descripción general del contenido:</p> <p>Configuración y administración de sistemas y sus implicaciones en temas de seguridad. Identificación de los componentes del sistema informático y su relación con los riesgos de seguridad. Conocer los tipos de virtualización, arquitecturas de hipervisores, taxonomías de virtualización y seguridad en entornos virtuales. Identificar las principales vulnerabilidades de los sistemas operativos y las técnicas de Hacking. Aplicar técnicas de análisis a los sistemas de almacenamiento. Conocer las principales herramientas aplicadas a la investigación forense en entornos locales y remotos. Seguridad en la nube.</p>
<b>Temario</b>
<p><b>Denominación del tema 1:</b> Configuración y administración del sistema operativo Linux.</p> <p><b>Contenidos del tema 1:</b></p> <ol style="list-style-type: none"> <li>1. Introducción</li> <li>2. Arranque y Parada del Sistemas</li> <li>3. Gestión de usuarios y grupos</li> <li>4. Sistemas de Ficheros</li> <li>5. Monitorización y Evaluación del sistema</li> <li>6. Instalación y Actualización de software</li> <li>7. Copias de Seguridad</li> <li>8. Automatización y programación de tareas</li> </ol> <p><b>Descripción de las actividades prácticas del tema 1:</b> se propone un supuesto práctico que incluye las tareas de configuración y administración de sistemas (gestión de arranque, usuarios, sistemas de ficheros, almacenamiento, copias de seguridad, monitorización, automatización de tareas y evaluación del sistema).</p>
<b>Denominación del tema 2:</b> Virtualización.

**Contenidos del tema 2:**

1. Introducción a la virtualización.
  - 1.1. Virtualización y Alta Disponibilidad
2. Taxonomías de virtualización.
  - 2.1. Virtualización de acceso
  - 2.2. Virtualización de aplicación
  - 2.3. Virtualización de procesamiento
  - 2.4. Virtualización de Red
  - 2.5. Virtualización de Almacenamiento
3. Arquitecturas hipervisor.
  - 3.1. Virtualización parcial
  - 3.2. Emulación
  - 3.3. Paravirtualización
  - 3.4. Virtualización completa
  - 3.5. Seguridad en entornos virtuales

**Descripción de las actividades prácticas del tema 2:** Parte práctica se trabaja con varios hipervisores de virtualización ampliamente utilizados en el ámbito profesional.

**Denominación del tema 3:** Vulnerabilidades del Sistema Operativo

**Contenidos del tema 3:**

1. Introducción
2. Casos prácticos en Windows, Linux y Mac
3. Ataques con virtualización
4. Logs, actualizaciones y copias de seguridad
5. Confidencialidad en Big Data

**Descripción de las actividades prácticas del tema 3:** estudio de herramientas de recuperación de contraseñas, elevación de permisos y hooking

**Denominación del tema 4:** Hacking

**Contenidos del tema 4:**

1. Introducción
2. Sistemas de información
3. Ingeniería social
4. Hacking ético
5. Técnicas de hacking
6. Tipos de atacantes y auditorías

**Descripción de las actividades prácticas del tema 4:** trabajo con herramientas utilizadas en hacking ético.

**Denominación del tema 5:** Análisis forense

**Contenidos del tema 5:**

1. Introducción
2. Métodos
3. Herramientas de análisis
  - a. Red
  - b. Memoria
  - c. Binarios
  - d. Sistema

**Descripción de las actividades prácticas del tema 5:** estudio de herramientas utilizadas en el análisis forense

**Actividades formativas**

Horas de trabajo del alumno/a por tema		Horas Gran grupo	Actividades prácticas				Actividad de seguimiento	No presencial
Tema	Total		CH	L	O	S		
1	36	10			6		1	19
2	23,5	6			3,5		0	14

3	25,5	5,5			4		0	16
4	27	6			4		1	16
5	30	8			4		1	17
<b>Evaluación</b>	8	2			1		0	5
<b>TOTAL</b>	150	37,5			22,5		3	87

GG: Grupo Grande (85 estudiantes).

CH: Actividades de prácticas clínicas hospitalarias (7 estudiantes)

L: Actividades de laboratorio o prácticas de campo (15 estudiantes)

O: Actividades en sala de ordenadores o laboratorio de idiomas (20 estudiantes)

S: Actividades de seminario o de problemas en clase (40 estudiantes).

TP: Tutorías Programadas (seguimiento docente, tipo tutorías ECTS).

EP: Estudio personal, trabajos individuales o en grupo, y lectura de bibliografía.

### Metodologías docentes

1. Clases expositivas de teoría y problemas: Presentación de los contenidos de la asignatura y planificación de la participación de todos los estudiantes en las distintas tareas. Discusión de aspectos teóricos. Adicionalmente, se realizarán charlas divulgativas realizadas por expertos y/o empresas de la materia.

2. Enseñanza participativa: Trabajos prácticos en grupos medianos o pequeños.

3. Tutorización: Actividad de seguimiento para tutela de trabajos dirigidos, consultas de dudas y asesoría en grupos pequeños o individuales.

4. Aprendizaje autónomo mediante el análisis de documentos escritos, la elaboración de memorias, el estudio de la materia impartida y desarrollo de los supuestos prácticos planteados.

5. Aprendizaje virtual. Uso de herramientas virtuales de comunicación entre profesor y estudiante e incluso entre los estudiantes entre sí.

### Resultados de aprendizaje

Saber configurar y administrar con seguridad los sistemas informáticos. Conocer las arquitecturas de los sistemas para identificar las vulnerabilidades de los mismos. Conocer y utilizar herramientas de seguridad y de análisis forense en entornos locales y remotos.

Vinculadas a las competencias transversales:

Demostrar convencimiento de que la diversidad cultural, consustancial a la convivencia genera cohesión e inclusión social. (CT12, 3er nivel de dominio)

Fomentar una comunicación empática y sincera encaminada al diálogo constructivo. (CT15, 3er nivel de dominio)

### Sistemas de evaluación

#### Modalidad Evaluación Continua

Sistemas de evaluación	Porcentaje
Examen.	(Entre el 0 y el 70%) 20%
Exposición oral de trabajos realizados.	(Entre el 0 y el 40%) 10%
Realización de trabajos dirigidos (informes, casos prácticos, ejercicios y problemas).	(Entre el 0 y el 80%) 60%

Asistencia y/o participación en el aula, en el aula virtual, en las tutorías, etc.	(Entre el 0 y el 30%) 10%
--	------------------------------

**Aclaraciones criterios de evaluación:**

1. Demostrar la adquisición, comprensión de los principales conceptos de la asignatura
2. Resolver supuestos mediante la aplicación de los conocimientos teóricos y experimentales
3. Exponer con claridad los trabajos teóricos/prácticos desarrollados.
4. Analizar críticamente y con rigor los resultados de las prácticas
5. Participar activamente en las actividades a desarrollar tanto en las sesiones prácticas como teóricas.

Para la evaluación continua, la realización de los casos prácticos propuestos supone el 60 % de la nota. La asistencia y participación en el aula supone el 10% de la nota. La exposición de trabajos realizados supone el 10% de la nota. El 20% restante corresponde a exámenes tipo test que se realizará a lo largo del cuatrimestre.

Para aplicar los porcentajes, se deberá obtener al menos una nota igual o superior a 5 en el desarrollo de los supuestos prácticos.

Si se detecta que el estudiante ha realizado plagio (presentar prácticas ajenas como propias, copiar durante el examen, presentar trabajos descargados de internet, etc.), tanto en la parte práctica, presentación de trabajos, examen escrito, etc. se aplicará una nota final un cero.

Los estudiantes que aprueben una de las partes en convocatoria ordinaria, se le guardará dicha nota hasta la convocatoria extraordinaria de noviembre del siguiente curso académico.

**Competencias Transversales**

Las competencias transversales se evaluarán de forma continua tanto durante la realización de las sesiones teóricas como prácticas y ECTS.

Durante las sesiones teóricas y prácticas los estudiantes deben ir resolviendo problemas que les permita ir adquiriendo los resultados de aprendizaje de la asignatura, aportando soluciones de calidad. Las actividades tanto de interacción entre los estudiantes como en la documentación a elaborar estarán orientadas a garantizar el respeto y la convivencia, cuidando el lenguaje y promoviendo la interacción entre los estudiantes.

Con carácter general, se dará especial importancia a la comunicación constructiva tanto durante el proceso de aprendizaje como el ámbito laboral.

Los hitos en las tutorías programadas ECTS, nos sirven de referencia para comprobar el grado de consecución y, por tanto, detectar desviaciones y posibilitar la mejora, en cada tipo competencia.

**Modalidad de evaluación global**

Para los alumnos acogidos a la opción de prueba única final, se arbitra el siguiente procedimiento:

1. El alumno deberá realizar al final del semestre un examen final que tendrá una parte teórica y otra práctica.
  - 1.1. En la parte teórica, el estudiante deberá contestar cuestiones teóricas, bien temas a desarrollar y/o preguntas tipo test. Esta parte supone el 30% de la nota de la asignatura.
  - 1.2. En la parte práctica, el estudiante deberá resolver correctamente diferentes supuestos prácticos dentro de lo abordado en el temario práctico y relativos a las actividades

realizadas en las sesiones de laboratorio. Esta parte supone el 70% de la nota de la asignatura.

Para aplicar los porcentajes, se deberá obtener al menos una nota igual o superior a 5 en la parte práctica.

### **Bibliografía (básica y complementaria)**

#### **Bibliografía básica**

1. “Essential System Administration, 2nd Edition Revised & Updated” Eelen Frisch. Ed O'Reilly & associates, Inc.
2. Ciberseguridad : hacking ético. Maíllo Fernández, J. (2020). Ra-Ma.
3. Computer Security Fundamentals Fourth Edition. Dr. Chuck Easttorn. Pearson
4. Learn Computer Forensics: A beginner's guide to searching, analyzing, and securing digital evidence. William Oettinger. 2020. Packt.

#### **Bibliografía complementaria**

1. Administración de Sistemas Operativos Windows y Linux. Un enfoque práctico. Julio Gómez, Nicolás Padilla y Juan Antonio Gil. Ed. Rama.
2. Pentesting con Kali. David Santo Orcero
3. Learn Ethical Hacking from Scratch. Zaid Sabih. 2018. ISBN: 9781788622059
4. National Institute of Standards and Technology (NIST).
5. Josef Pieprzyk, Thomas Hardjono, and Jennifer Seberry. Fundamentals of Computer Security. Springer, 2003.
6. Oakley, J. (2019). Professional Red Teaming Conducting Successful Cybersecurity Engagements (1st ed. 2019.). Apress.
7. Roussev, V. (2017). Digital forensic science : issues, methods, and challenges . Morgan & Claypool Publishers
8. Oettinger, W. (2020). Learn Computer Forensics (1st edition). Packt Publishing.

### **Otros recursos y materiales docentes complementarios**

1. <http://campusvirtual.unex.es>
2. <https://books.google.es/>
  - “The Linux System Administrator’s Guide” Lars Wirzenius, Joanna Oja, Stephen Stafford. Disponible en <http://www.tldp.org/LDP/sag/index.html>
  - Cyber Security and Digital Forensics: Challenges and Future Trends. Wiley. 2022
  - Introduction to cyber security: stay safe online. The open university. 2016.