PLAN DOCENTE DE LA ASIGNATURA: **Seguridad Avanzada**
CÓDIGO: **501466**

CURSO ACADÉMICO: **2024/2025**

Identificación y características de la asignatura				
Código	501466		**Créditos ECTS**	6
Denominación (español)	Seguridad Avanzada			
Denominación (inglés)	Advanced Security			
Titulaciones	Grado de Ingeniería Telemática/ Grado en Ingeniería Informática en Tecnologías de la Información.			
Centro	Centro Universitario de Mérida			
Semestre	8º	**Carácter**	Optativa	
Módulo	Intensificación en Administración de Redes / Módulo Contenidos Optativos en Tecnologías de la Información.			
Materia	Redes I/Multimedia y Seguridad en Internet			

Profesor/es			
Nombre	**Despacho**	**Correo-e**	**Página web**
VACANTE	41		

Área de conocimiento	Ingeniería Telemática
Departamento	Ingeniería de Sistemas Informáticos y Telemáticos
Profesor coordinador (si hay más de uno)	

Competencias*

	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
	Competencias generales
✓	CG3 (En GIT) - CG8 (En GIITI) - Conocimiento de materias básicas y tecnologías, que le capacite para el aprendizaje de nuevos métodos y tecnologías, así como que le dote de una gran versatilidad para adaptarse a nuevas situaciones.

*** Los apartados relativos a competencias, breve descripción del contenido, actividades formativas, metodologías docentes, resultados de aprendizaje y sistemas de evaluación deben ajustarse a lo recogido en la memoria verificada del título y en la normativa de evaluación (DOE 12 de diciembre de 2016)

✓	CG4 (Grado IT) - Capacidad de resolver problemas con iniciativa, toma de decisiones, creatividad, y de comunicar y transmitir conocimientos, habilidades y destrezas, comprendiendo la responsabilidad ética y profesional de la actividad del Ingeniero Técnico de Telecomunicación. CG9 (Grado GIITI) - 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 InformáticaCG9 - 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
	CG5 - Conocimientos para la realización de mediciones, cálculos, valoraciones, tasaciones, peritaciones, estudios, informes, planificación de tareas y otros trabajos análogos en su ámbito específico de la telecomunicación.
Competencias específicas	
✓	CE6 (En GIT) - Capacidad para aprender de manera autónoma nuevos conocimientos y técnicas adecuados para la concepción, el desarrollo o la explotación de sistemas y servicios de telecomunicación. CEO12 (En GIITI): Capacidad para aprender de manera autónoma nuevos conocimientos y técnicas adecuados para la concepción, el desarrollo o la explotación de sistemas y servicios de telecomunicación.
	CE17 - Conocimiento y utilización de los conceptos de arquitectura de red, protocolos e interfaces de comunicaciones.
	CE19 - Conocimiento de los métodos de interconexión de redes y encaminamiento, así como los fundamentos de la planificación, dimensionado de redes en función de parámetros de tráfico.
✓	CE22 (En GIT) - Capacidad para aplicar las técnicas en que se basan las redes, servicios y aplicaciones telemáticas, tales como sistemas de gestión, señalización y conmutación, encaminamiento y enrutamiento, seguridad (protocolos criptográficos, tunelado, cortafuegos, mecanismos de cobro, de autenticación y de protección de contenidos), ingeniería de tráfico (teoría de grafos, teoría de colas y teletráfico) tarificación y fiabilidad y calidad de servicio, tanto en entornos fijos, móviles, personales, locales o a gran distancia, con diferentes anchos de banda, incluyendo telefonía y datos. CEO10 (En GIITI): Capacidad para aplicar las técnicas de seguridad avanzada (protocolos criptográficos, tunelado, cortafuegos, mecanismos de cobro, de autenticación y de protección de contenidos).
	CE23 - Capacidad de construir, explotar y gestionar servicios telemáticos utilizando herramientas analíticas de planificación, de dimensionado y de análisis.
	CEO1 - Analizar, diseñar e implementar sistemas operativos, mediante el diseño e implementación de componentes propios, teniendo presente en todo momento los principios teóricos y prácticos que lo rigen.
	CEO2 - Analizar, diseñar e implementar las funcionalidades requeridas para dispositivos de control de periféricos, aumentando la capacidad del sistema mediante la integración de nuevos recursos del sistema
	CEO3 - Analizar y determinar soluciones a problemas en sistemas de computación, implementando sistemas de protección de la información y de los propios sistemas de computación, aumentando la seguridad y eficiencia del sistema mediante facilidades que controlen el acceso a los recursos del sistema, mejorando y facilitando al usuario su uso.
	CEO4 - Comprender la importancia de los sistemas embebidos entendiendo sus requerimientos de diseño, áreas de aplicación, límites y restricciones.
	CEO5 - Desarrollar y analizar los sistemas embebidos, trabajando sobre las diferentes fases de desarrollo desde el proceso de especificación hasta el de implementación, para aplicaciones de una determinada complejidad buscando minimizar costes y maximizar la confiabilidad y seguridad.
	CEO6 - Aplicar las técnicas de modelado y simulación al desarrollo y testeo de sistemas embebidos
Competencias transversales	
✓	CT4. Resolución de problemas
	CT10. Comunicación escrita
	CT12. Diversidad e interculturalidad
	CT15. Comunicación interpersonal
✓	CT16. Trabajo en equipo
	CT19. Creatividad e innovación

Contenidos

Breve descripción del contenido*

- Implementación de filtros de seguridad en redes.
- Redes VPN. Seguridad integrada de los dispositivos de interconexión.
- Seguridad en entornos inalámbricos.

Temario de la asignatura

Denominación del **Tema 1: Introducción a la seguridad avanz1a.daT**
Contenidos del tema 1:

1. Tipos de seguridad en las redes. Organizaciones.
2. Políticas y protocolos de seguridad

Denominación del **Tema 2: Administración de las comunicaciones y control de acceso**
Contenidos del tema 2:

1. Administración de acceso seguro. Redes VPN.
2. Auditorías de seguridad (AAA).

Denominación del **Tema 3: Seguridad de los dispositivos de red**
Contenidos del tema 3:

1. Seguridad de conmutadores y enrutadores.
2. Enfoques DMZ.
3. Firewalls software/hardware. Técnicas de filtrado.

Denominación del **Tema 4: Introducción a la Seguridad inalámbrica**
Contenidos del tema 4:

1. Amenazas a la seguridad inalámbrica.
2. Estándares IEEE-802.11

Denominación del **Tema 5: Métodos de Autenticación: Estándares y Protocolos.**
Contenidos del tema 5:

1. Medidas de autenticación y cifrado.
2. Medidas de protección y recomendaciones de seguridad.
3. Seguridad Personal/Enterprise - Servidor RADIUS

Temario práctico de la asignatura

- Administración de Certificados (1 h.)
- Configuración de túneles VPN (4 h.)
- Implementación de firewalls diversos (4 h.)
- Modo Monitor-Ocultación SSID y filtros MAC. (4 h.)
- Seguridad personal/corporativa a través de un servidor RADIUS con cliente inalámbrico (6 h.)

Actividades formativas*

Horas de trabajo del alumno por tema		Horas Teóricas	Actividades Prácticas				Actividad de seguimiento	NP
Tema	Total	GG	PCH	LAB	ORD	SEM	TP	EP
1	13	4			2			7
2	24	5			4			15
3	31	6			4		1	20
4	34	9			4		1	20
5	31	9			6		1	15
Evaluación	17	4,5			2,5			10
TOTAL	150	37,5			22,5		3	87

GG: Grupo Grande (85 estudiantes).
PCH: prácticas clínicas hospitalarias (7 estudiantes)
LAB: prácticas laboratorio o campo (15 estudiantes)

ORD: prácticas sala ordenador o laboratorio de idiomas (20 estudiantes)
SEM: clases problemas o seminarios o casos prácticos (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 en la materia.
2. **Enseñanza participativa**: Trabajos prácticos en grupos medianos o pequeños.
3. **Tutorización**: Actividad de seguimiento para tutela de trabajos dirigidos, consulta 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*

- Administrar y controlar la seguridad en dispositivos y servidores con los que tengan que trabajar fuera del aula, en entorno empresarial.
- Dominar filtros y cortafuegos aplicados a diferentes tipos de escenarios de redes.
- Gestionar y configurar técnicas seguras en entornos inalámbricos y móviles.
- Muestra una gran autonomía e integración en el seno de un equipo de trabajo, tiene una orientación a seguir aprendiendo a lo largo de la vida y tiene motivación por obtener resultados y productos de calidad.
- Tiene iniciativa para aportar y/o evaluar soluciones efectivas, alternativas o novedosas a los problemas, tomando decisiones basadas en criterios objetivos.
- Demuestra capacidad de razonamiento y comprensión en el ámbito teórico y práctico.
- Aprende autónomamente.
- Ser capaz de aplicar las técnicas seguridad avanzada (protocolos criptográficos, tunneling, cortafuegos, de autenticación y de protección de contenidos.

Sistemas de evaluación*

Modalidad de Evaluación Continua

Evaluación continua: Considerará la asistencia y participación del alumno o alumna en las actividades presenciales (Asistencia y/o participación en el aula, en el aula virtual, en las tutorías, supuestos prácticos etc.) en al menos un 80%, y supondrá un 40% de la nota final.

El examen de certificación se realiza al final y consiste en un examen escrito sobre la materia teórica 30% más un supuesto práctico de redes, otro 30% de la nota final.
Es requisito indispensable tener al menos un 40% de cada una de las partes, teoría/ prácticas aprobadas, para poder hacer la suma de porcentajes. Aquella parte que se apruebe se guardará hasta la siguiente convocatoria.

Sistemas de evaluación	Porcentaje
Examen.	(Entre el 50 y el 60%)
Exposición oral de trabajos realizados.	(Entre el 10 y el 20%)
Realización de trabajos dirigidos (informes, casos prácticos, ejercicios y problemas).	(Entre el 15 y el 20%)
Asistencia y/o participación en el aula, en el aula virtual, en las tutorías, etc.	(Entre el 15 y el 20%)

Modalidad de Evaluación Global

"Según la normativa vigente, la elección entre la modalidad de evaluación continua o evaluación global con una prueba final corresponde al estudiante durante las durante el primer cuarto del período de impartición de esta, para cada una de las convocatorias (ordinaria y extraordinaria). Y deberá comunicarlo al profesor a través de la consulta disponible en el espacio de la asignatura disponible en el campus virtual de la Universidad de Extremadura (CVUEx)".
En el caso de aquellos **alumnos que no puedan realizar las actividades presenciales** y no se acojan a la evaluación continua, irán a un **examen final** donde la materia teórica supondrá un 40% de la nota y la parte práctica un 60% de la nota final. Es requisito indispensable tener al menos un 40% de cada una de las partes, teoría/prácticas aprobadas, para poder hacer la suma de porcentajes.
Aquella parte que se apruebe se guardará hasta la siguiente convocatoria.

Bibliografía

Bibliografía básica

Implementing Cisco IOS Network Security (IINS 640-554) Foundation Learning Guide, 2nd Edition By Catherine Paquet. Published Nov 30, 2012 by Cisco Press.
Documentación certificación CISCO CCNA Security. Apuntes proporcionados por el profesor.

Bibliografía complementaria

- Guía avanzada firewalls Linux-Robert L. Ziegler-Prentice-Hall.
- Amenazas persistentes avanzadas-Antonio Villalón Huertas-Nau LLibres.

Otros recursos y materiales docentes complementarios