# PLAN DOCENTE DE LA ASIGNATURA

## Curso académico: 2025/2026

| Identificación y características de la asignatura | | | | | |
|---|---|---|---|---|---|
| Código | 501466 | | | | |
| 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 | | | | |
| Módulo | Intensificación en Administración de Redes /Módulo Contenidos Optativos en Tecnologías de la Información | | | | |
| Materia | Redes I/Multimedia y Seguridad en Internet | | | | |
| Carácter | Optativa | ECTS | 6 | Semestre | 8º |
| Profesorado | | | | | |
| Nombre | | Despacho | | Correo-e | |
| José Antonio Gómez de la Hiz | | 40 | | jagomezdh@unex.es | |
| Área de conocimiento | Ingeniería Telemática | | | | |
| Departamento | Ingeniería de Sistemas Informáticos y Telemáticos | | | | |
| Profesor/a coordinador/a (si hay más de uno) | | | | | |

## Competencias / Resultados de aprendizaje

### 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
- **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.
- **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

**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.
- **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).

**Competencias transversales**

- **CT4.** Resolución de problemas
- **CT16.** Trabajo en equipo

## Contenidos

- 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 avanzada**

Contenidos del tema 1:

1. Fundamentos de seguridad
2. Administración de sistemas operativos

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 4:

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 (2 h.)
- Configuración de túneles VPN (4 h.)
- Implementación de firewalls diversos (5 h.)
- Modo Monitor-Ocultación SSID y filtros MAC. (4 h.)
- Seguridad personal/corporativa a través de un servidor RADIUS con cliente inalámbrico (4 h.)

## Actividades formativas

| Horas de trabajo del alumno/a por tema | | Horas Gran grupo | Actividades prácticas | | | | Actividad de seguimiento | No presencial |
|---|---|---|---|---|---|---|---|---|
| **Tema** | **Total** | **GG** | **CH** | **L** | **O** | **S** | **TP** | **EP** |
| 1 | 13 | 4 | | | 2 | | | 7 |
| 2 | 24 | 6 | | | 4 | | | 15 |
| 3 | 31 | 6 | | | 4 | | 1 | 20 |
| 4 | 34 | 17 | | | 5 | | 1 | 20 |
| 5 | 31 | | | | 5 | | 1 | 15 |
| **Evaluación** | 17 | 2 | | | 2,5 | | | 10 |
| **TOTAL** | 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 problema**s: 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

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 **20%** de la nota final.

El examen de certificación se realiza al final y consiste en un examen escrito sobre la materia teórica **50%** 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.

### 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 (básica y complementaria)

Bibliografía básica: Apuntes proporcionados por el profesor.

Bibliografía complementaria:

- 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.

**Otros recursos y materiales docentes complementarios**

Recursos: Aula virtual de la asignatura, disponible en el Campus Virtual de la Universidad de Extremadura.