PLAN DOCENTE DE LA ASIGNATURA

Curso académico: 2026/2027

Identificación y características de la asignatura					
Código	501466				
Denominación (español)	**Seguridad Avanzada**				
Denominación (inglés)	Advanced Security				
Titulaciones	- Grado en Ingeniería Telemática en Telecomunicación - 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	8

Profesorado		
Nombre	Despacho	Correo-e
Jesús Galeano Brajones	40	jgaleanobra@unex.es
Javier Carmona Murillo	42	jcarmur@unex.es

Área de conocimiento	Ingeniería Telemática
Departamento	Ingeniería de Sistemas Informáticos y Telemáticos
Profesor/a coordinador/a (si hay más de uno)	Jesús Galeano Brajones

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 (GITT), CG8 (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 (GITT) - 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 (GIITI) - Capacidad de 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 (GITT), CEO12 (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 (GITT) - Conocimiento y utilización de los conceptos de arquitectura de red, protocolos e interfaces de comunicaciones.
	CE19 (GITT) - 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 (GITT) - 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.
	CE23 (GITT) - Capacidad de construir, explotar y gestionar servicios telemáticos utilizando herramientas analíticas de planificación, de dimensionado y de análisis.
✓	CEO10 (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

Descripción general del contenido: Implementación de filtros de seguridad en sistemas de 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 de red**

Contenidos del tema 1:

1. Gestión de riesgos y superficie de ataque
2. Mecanismos de identificación y autenticación
3. Infraestructura de clave pública (PKI) y X.509

Descripción de las actividades prácticas del tema 1: Creación de una PKI y despliegue de certificados X.509

Denominación del tema 2: **Seguridad perimetral y filtrado**

Contenidos del tema 2:

1. Listas de control de acceso (ACLs) estándar y extendidas
2. Firewalls stateless, stateful, next-generation
3. Zonas de seguridad y DMZ
4. Diseño de políticas de filtrado

Descripción de las actividades prácticas del tema 2: Configuración de ACLs y firewalls en escenarios de red con zonas de seguridad

Denominación del tema 3: **Redes privadas virtuales (VPNs)**

Contenidos del tema 3:

1. Conceptos de tunneling
2. IPsec. Modos transporte y túnel, IKE, VPN site-to-site
3. SSL/TLS VPN. Evolución a TLS 1.3, VPN de acceso remoto
4. WireGuard

Descripción de las actividades prácticas del tema 3: Configuración de túneles VPN

Denominación del tema 4: **Seguridad integrada en dispositivos de red**

Contenidos del tema 4:

1. Hardening de routers y switches
2. Autenticación centralizada (RADIUS/TATACS+)
3. Control de acceso a la red (802.1X)
4. Protección del plano de gestión y del plano de control

Descripción de las actividades prácticas del tema 4: Configuración de autenticación centralizada con RADIUS y control de acceso 802.1X

Denominación del tema 5: **Seguridad en entornos inalámbricos**

Contenidos del tema 5:

1. Vulnerabilidades de redes Wi-Fi
2. Protocolos de seguridad (WPA2/WPA3-Enterprise)
3. Integración con RADIUS y 802.1X
4. Detección de puntos de acceso no autorizados

Descripción de las actividades prácticas del tema 5: Configuración y verificación de seguridad en entornos inalámbricos.

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	19	5	0	0	4	0	0	10
2	30	8	0	0	4	0	0	18
3	33	8	0	0	4	0	1	20
4	28	7	0	0	4	0	1	16
5	19	5,5	0	0	2,5	0	1	10
Evaluación	21	4	0	0	4	0	0	13
TOTAL	150	37,5	0	0	22,5	0	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

- 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

Sistemas de evaluación	Porcentaje
Examen	50% (Entre el 50 y el 65%)
Exposición oral de trabajos realizados	40% (Entre el 0 y el 40%)
Realización de trabajos dirigidos (informes, casos prácticos, ejercicios y problemas)	10% (Entre el 10 y el 30%)
Asistencia y/o participación en el aula, en el aula virtual, en las tutorías, etc.	0% (Entre el 0 y el 40%)

La evaluación de cada estudiante se realizará mediante evaluación continua a través de actividades teóricas y prácticas desarrolladas a lo largo del semestre. Estas actividades serán prácticas de laboratorio, trabajos dirigidos, una defensa oral y un examen final, tal y como se describe a continuación:

- El alumno deberá examinarse de los contenidos desarrollados tanto en las sesiones de gran grupo como en las actividades prácticas mediante **un examen final** que supondrá el **50% de la nota** (NE). El examen constará de dos partes: una parte teórica (NET), con un peso del 20% sobre la nota final, y una parte práctica (NEP), con un peso del 30%, similar a los trabajos realizados en las sesiones prácticas.
- Las prácticas de laboratorio se desarrollarán a lo largo del curso y serán de carácter formativo. La **realización de los trabajos dirigidos** asociados a cada práctica supondrá un **10% de la nota** (NTD). Esta nota **no es recuperable**, es decir, se obtiene exclusivamente mediante evaluación continua y no pueden ser objeto de evaluación en convocatorias extraordinarias. Estos trabajos deberán entregarse en los plazos establecidos. Las entregas fuera de plazo podrán ser objeto de penalización en la calificación. Es requisito necesario haber entregado y aprobado todos los trabajos dirigidos para acceder a la defensa oral.
- La **defensa oral individual** supondrá un **40% de la nota** (NDO). En ella, el alumno deberá resolver y explicar variaciones sobre los escenarios trabajados en el laboratorio, demostrando dominio de los mismos. Es requisito necesario obtener al menos un 50% de la puntuación en la defensa oral para acceder al examen práctico (NEP).

La nota final (NF) de la asignatura se calculará como:

$$NF = NET \times 0{,}20 + NEP \times 0{,}30 + NDO \times 0{,}40 + NTD \times 0{,}10$$

Para superar la asignatura, se deberá obtener al menos un 50% de la puntuación en ambas partes del examen (NET y NEP) para hacer suma de porcentajes. En caso de no alcanzar dicho mínimo en alguno de estos bloques, la asignatura estará suspensa, aunque la parte que esté aprobada se guardará para el resto de las convocatorias del mismo curso académico.

En convocatorias extraordinarias, los alumnos que no hayan alcanzado los requisitos mínimos en el bloque no recuperable (NAP) podrán optar por la modalidad de evaluación global, siendo evaluados mediante la prueba final descrita en dicho apartado.

Modalidad de evaluación global

Aunque la asignatura se recomienda realizarla siguiendo la evaluación continua, atendiendo al artículo 4.1 de la “Normativa de evaluación de las titulaciones oficiales

degrado y máster de la Universidad de Extremadura" (DOE 3/11/2020), existe la posibilidad de superarla a través de una prueba final que engloba todos los contenidos de la asignatura y que se realizará en la fecha oficial de cada convocatoria.

Según se indica también en el artículo 4.2 de dicha normativa, "la elección de la modalidad de evaluación global corresponde a los estudiantes, que podrán llevarla a cabo, durante los plazos establecidos", para cada una de las convocatorias de la asignatura. En el caso de ausencia de solicitud expresa por parte del estudiante, la modalidad asignada será la de evaluación continua.

Los plazos para la elección de la modalidad de evaluación son los siguientes:

- Para las asignaturas con docencia en el primer semestre, durante el primer cuarto del periodo de impartición de estas.
- Para las asignaturas con docencia en el segundo semestre, durante el primer cuarto del periodo de impartición de estas o hasta el último día del periodo de ampliación de matrícula si este acaba después de ese periodo.

La nota máxima que puede alcanzar el estudiante siguiendo este sistema de evaluación es del 100%. Por este motivo, la prueba final de carácter global constará de dos partes: un examen de certificación teórico, con un peso de un 40%, y un examen de certificación práctico, con un peso de un 60%. Es necesario tener al menos un 50% de la puntuación en cada una de las partes para hacer suma de porcentajes.

Bibliografía (básica y complementaria)

Bibliografía básica

- Stallings, W. *Network Security Essentials: Applications and Standards*, 6th Ed. Pearson, 2017. ISBN: 978-0-13-452733-8

Bibliografía complementaria

- McNab, C. *Network Security Assessment: Know Your Network*, 3rd Ed. O'Reilly, 2016. ISBN: 978-1-491-91095-5
- Oswalt, M., Adell, C., Lowe, S.S. y Edelman, J. *Network Programmability and Automation*, 2nd Ed. O'Reilly, 2023. ISBN: 978-1-098-11083-3

Otros recursos y materiales docentes complementarios

Documentación elaborada por el profesor disponible a través del Campus Virtual de la Universidad de Extremadura.