PLAN DOCENTE DE LA ASIGNATURA: Seguridad de la Información

CÓDIGO: 501453

CURSO ACADÉMICO: **2024/2025**

PROGRAMA DE LA ASIGNATURA

Curso académico: 2024/2025

Identificación y características de la asignatura					
Código	501453			Créditos ECTS	6(4,5+1,5)
Denominación (español)	Seguridad de la Información				
Denominación (inglés)	Information Security				
Titulaciones	Grado en Ingeniería Telemática en Telecomunicación (GITT) Grado en Ingeniería Informática: Tecnologías de la Información (GIITI)				
Centro	Centro Universitario de Mérida				
Semestre	5º(GIITI) /7(GITT)	Carácter	Obligatoria		
Módulo	Tecnologías de la Información (GIITI) Tecnología Específica Telemática (GITT)				
Materia	Redes (GIITI) Telemática (GITT)				
Profesor/es					
Nombre		Despacho	Correo-e	Página web	
Juan Arias Masa		40	juanaria@unex.es	http://campusvirtual.unex.es/portal/	
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

* 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)

✓	CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía
Competencias generales. GITT	
	CG2 - Conocimiento, comprensión y capacidad para aplicar la legislación necesaria durante el desarrollo de la profesión de Ingeniero Técnico de Telecomunicación y facilidad para el manejo de especificaciones, reglamentos y normas de obligado cumplimiento.
✓	CG3 - 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 - 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.
	CG6 - Facilidad para el manejo de especificaciones, reglamentos y normas de obligado cumplimiento.
	CG7 - Capacidad de analizar y valorar el impacto social y medioambiental de las soluciones técnicas.
✓	CG8 - Conocer y aplicar elementos básicos de economía y de gestión de recursos humanos, organización y planificación de proyectos, así como de legislación, regulación y normalización en las telecomunicaciones.
	CG9 - Capacidad de trabajar en un grupo multidisciplinar y en un entorno multilingüe y de comunicar, tanto por escrito como de forma oral, conocimientos, procedimientos, resultados e ideas relacionadas con las telecomunicaciones y la electrónica.
Competencias generales GIITI	
✓	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.
	CG6 - Capacidad para concebir y desarrollar sistemas o arquitecturas informáticas centralizadas o distribuidas integrando hardware, software y redes 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 específicas GITT	
	CE11 - Capacidad de concebir, desplegar, organizar y gestionar redes, sistemas, servicios e infraestructuras de telecomunicación en contextos residenciales (hogar, ciudad y comunidades digitales), empresariales o institucionales responsabilizándose de su puesta en marcha y mejora continua, así como conocer su impacto económico y social.
	CE12 - Conocimiento y utilización de los fundamentos de la programación en redes, sistemas y servicios de telecomunicación
	CE17 - Conocimiento y utilización de los conceptos de arquitectura de red, protocolos e interfaces de comunicaciones.

	CE18 - Capacidad de diferenciar los conceptos de redes de acceso y transporte, redes de conmutación de circuitos y de paquetes, redes fijas y móviles, así como los sistemas y aplicaciones de red distribuidos, servicios de voz, datos, audio, vídeo y servicios interactivos y multimedia
	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.
	CE21 - Capacidad de construir, explotar y gestionar las redes, servicios, procesos y aplicaciones de telecomunicaciones, entendidas éstas como sistemas de captación, transporte, representación, procesado, almacenamiento, gestión y presentación de información multimedia, desde el punto de vista de los servicios telemáticos.
✓	CE22 - 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 - Capacidad de construir, explotar y gestionar servicios telemáticos utilizando herramientas analíticas de planificación, de dimensionado y de análisis.
	CE24 - Capacidad de describir, programar, validar y optimizar protocolos e interfaces de comunicación en los diferentes niveles de una arquitectura de redes
	CE25 - Capacidad de seguir el progreso tecnológico de transmisión, conmutación y proceso para mejorar las redes y servicios telemáticos.
	CE26 - Capacidad de diseñar arquitecturas de redes y servicios telemáticos.
	CE27 - Capacidad de programación de servicios y aplicaciones telemáticas, en red y distribuidas.
Competencias específicas GITI	
	CE26 - Capacidad para seleccionar, diseñar, desplegar, integrar, evaluar, construir, gestionar, explotar y mantener las tecnologías de hardware, software y redes, dentro de los parámetros de coste y calidad adecuados.
	CE28 - Capacidad para seleccionar, diseñar, desplegar, integrar y gestionar redes e infraestructuras de comunicaciones en una organización.
✓	CE31 - Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.
Competencias Transversales GITT	
	CT3. Gestión del tiempo
	CT4. Resolución de problemas
	CT7. Planificación
	CT16. Trabajo en equipo
	CT17. Orientación a la calidad

	CT18. Sostenibilidad y compromiso social
	CT19. Creatividad e innovación
	CT20. Iniciativa y espíritu emprendedor
Competencias Transversales GITI	
	CT3. Gestión del tiempo
✓	CT8. Uso de las TIC
✓	CT17. Orientación a la calidad
	CT21. Liderazgo

Temas y contenidos

Breve descripción del contenido

- GITT: Seguridad de la Información: Integridad y confidencialidad en la transmisión de la información. Criptografía. Historia y desarrollo actual de la seguridad informática.

GIITI: (Nueva propuesta verifica) SI: Integridad y confidencialidad en la transmisión de la información, riesgos y políticas de seguridad en redes telemáticas. Historia y desarrollo actual de la seguridad de la Información.

Temario de la asignatura

Tema 1. Introducción.
Tema 2. Criptografía Clásica.
Tema 3. Criptografía Moderna.
Tema 4. Criptografía de Clave Privada
Tema 5. Criptografía de Clave Pública
Tema 6. Firmas Digitales
Tema 7. Seguridad Perimetral.
Tema 8. Autenticación
Tema 9. Seguridad en el Correo electrónico
Tema 10. ISO 27000

Practica I. Presentación de los entornos de programación de las prácticas.
Práctica II. Utilización y análisis de algunas herramientas de seguridad
Práctica III. Codificación de un algoritmo de cifrado.
Práctica IV. Herramienta PGP.

Actividades formativas*

Horas de trabajo del alumno por tema		Horas teóricas	Actividades prácticas				Actividad de seguimiento	No presencial
Tema	**Total**	**GG**	**CH**	**L**	**O**	**S**	**TP**	**EP**
Presentación	1	1			0			0
1	4	2			0			2
2	11	5			0		1	5
3	11	5			0			6
4	13	6			0			7
5	10	4			0			6
6	10	4			0			6
7	9	4			0			5
8	10	4			0		1	5
9	9	4			0			5

10	8	4			0			4
P1	3	0			1			2
P2	10	0			3		1	6
P3	13	0			6			7
P4	9	0			3			6
Evaluación **	19	2			2			15
TOTAL	150	45			15		3	87

GG: Grupo Grande (85 estudiantes).
CH: prácticas clínicas hospitalarias (7 estudiantes)
L: prácticas laboratorio o campo (15 estudiantes)
O: prácticas sala ordenador o laboratorio de idiomas (20 estudiantes)
S: 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

- 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.
- Enseñanza participativa: Trabajos prácticos en grupos medianos o pequeños.
- Tutorización: Actividad de seguimiento para tutela de trabajos dirigidos, consultas de dudas y asesoría en grupos pequeños o individuales.
- 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.
- Aprendizaje virtual. Uso de herramientas virtuales de comunicación entre profesor y estudiante e incluso entre los estudiantes entre si.

Resultados del Aprendizaje

GITT

- Conocer las técnicas básicas de criptografía clásica.
- Conocer los principios de seguridad de la información y seguridad informática.
- Conocer las principales técnicas criptográficas para asegurar la integridad y privacidad de las comunicaciones en red, como el uso de infraestructura de clave pública, certificados y firma digital.
- Utilizar su experiencia y criterio para analizar las causas de un problema y construir una solución eficiente y eficaz
- Planificar con método y acierto el desarrollo de un proyecto complejo.
- Participar e integrarse en el desarrollo organizado de un trabajo en grupo, previendo las tareas, tiempos y recursos para conseguir los resultados deseados
- Contribuir en la consolidación y desarrollo del equipo, favoreciendo la comunicación, el reparto equilibrado de tareas, el clima interno y la cohesión

GIITI

- Conocer las amenazas exteriores o restricciones internas relacionadas con las políticas de seguridad de la información en los entornos de red e implementar escenarios seguros basados en listas de control de acceso.
- Conocer las principales técnicas criptográficas para asegurar la integridad y privacidad de las comunicaciones en red, como el uso de infraestructura de clave pública, certificados y firma digital
- Conocer los principios de seguridad de la información y seguridad informática.
- Conocer las técnicas básicas de criptografía clásica.
- Participar e integrarse en el desarrollo organizado de un trabajo en grupo, previendo las

** Indicar el número total de horas de evaluación de esta asignatura.

tareas, tiempos y recursos para conseguir los resultados deseados. (CT8, 2do nivel de dominio)
- Mejorar sistemáticamente el trabajo personal. (CT17, 2do nivel de dominio)

Sistemas de evaluación

Es de aplicación la normativa publicada en el DOE 212 de martes 3 de noviembre de 2020 en su capitulo II Sistemas de Evaluación.

La normativa oficial publicada en el título GRADO EN INGENIERÍA EN TELEMÁTICA dice:

Sistema de Evaluación	Ponderación mínima	Ponderación máxima
Examen	50	70
Exposición oral de trabajos realizados	0	30
Realización de trabajos dirigidos (informes, casos prácticos, ejercicios y problemas)	10	50
Asistencia y/o participación en el aula, en el aula virtual, en las tutorías, etc.	10	35

La normativa oficial publicada en el título GRADO EN INGENIERÍA EN TECNOLOGIAS DE LA INFORMACION Y COMUNICACIÓN dice:

Sistema de Evaluación	Ponderación mínima	Ponderación máxima
Examen	0	70
Exposición oral de trabajos realizados	0	40
Realización de trabajos dirigidos (informes, casos prácticos, ejercicios y problemas)	0	80
Asistencia y/o participación en el aula, en el aula virtual, en las tutorías, etc.	0	30

Modalidad de Evaluación Continua

Concreción de la normativa:

Sistema de Evaluación	Ponderación
Examen	50%
Exposición oral de trabajos realizados	5%
Realización de trabajos dirigidos (informes, casos prácticos, ejercicios y problemas)	35%
Asistencia y/o participación en el aula, en el aula virtual, en las tutorías, etc.	10%

- Parte teórica 50%. Examen final de la asignatura que deberá ser superado con una nota igual o superior a 5 puntos sobre 10.
- Parte práctica 30%
  - La parte práctica se compondrá de los trabajos o tareas entregadas de cada práctica (20% de la nota total) y un examen final de las mismas (10% de la nota total) que deberá superarse para poder

computar el 30% de la nota total.
    - Las tareas podrán superarse en evaluación continua más el examen final de prácticas, o bien
    - Entregando la tarea de práctica no_presencial más el correspondiente examen final en cualquiera de las convocatorias ordinarias o extraordinarias del presente curso.
    - En cualquiera de las dos modalidades anteriores, esta parte deberá ser superada independientemente con una nota que sea igual o superior a 5 puntos sobre 10.
- La participación en clase, en foros del aula virtual, grupos de trabajo, etc., tendrá un peso del 10% sobre la nota final, entrando aquí el 50% la evaluación de las competencias transversales asignadas a esta asignatura.
- Las actividades ECTS se evaluarán con una memoria (5% de la nota final) y exposición oral/final del trabajo realizado (5% de la nota final), y el cómputo total tendrá un valor del 10% de la nota, entrando aquí el 50% la evaluación de las competencias transversales asignadas a esta asignatura.

Modalidad de evaluación global

Es de aplicación la normativa publicada en el DOE 212 de martes 3 de noviembre de 2020, que resumidamente dice:
Los plazos para elegir la modalidad global serán los siguientes:
Para las asignaturas con docencia en el primer semestre, durante el primer cuarto del periodo de impartición de las mismas.
Para las asignaturas con docencia en el segundo semestre, durante el primer cuarto del periodo de impartición de las mismas o hasta el último día del periodo de ampliación de matrícula si este acaba después de ese periodo.

- Entregas de Laboratorio (PL)(30%).
Deberá entregar la práctica final funcionando correctamente y realizar una modificación sobre la misma. La evaluación se realizará sobre la entrega realizada.

- Examen final (EF)(70%).
Se realizará una prueba final por escrito que recogerá tanto los contenidos teóricos como prácticos de la asignatura. Este examen podrá ser distinto al examen de la evaluación continua.

Deberán superarse las dos partes con una nota superior a 5 sobre 10 de forma independiente, y además en la misma convocatoria. Si cualquiera de las dos partes está suspensa se deberá recuperar la asignatura completa.

Bibliografía (básica y complementaria)

- Básica:
    - Tanenbaum, 2010. Andrew S. Tanenbaum. Redes de Computadoras. Prentice-Hall, Quinta Edición. ISBN: ISBN-10: 0-13-212695-8 Published: 27 septiembre 2010
    - Carracedo,04 Justo Carracedo Gallardo "Seguridad en Redes Telemáticas" McGraw-Hill, Madrid 2004
    - Pfleeger,89 Charles P. Pfleeger "Security in Computing" 2ª Edición, Prentice Hall International, Inc., 1997
    - Schneier,93 B. Schneier "Applied Criptography" John Weley & Sons Ltd., 1993 (Ba-2424)
    - Díaz,04 G. Díaz, F. Mur, E. Sancristóbal, M-A. Castro y J. Peire "Seguridad en las Comunicaciones y en la Información" UNED, 2004
- Complementaria:

- Aula virtual de la Asignatura:
  i. http://campusvirtual.unex.es/zonauex/avuex/my/
- Menezes, Alfred; Oorsschof, Paul; Vanstone, Scott. Handbook of Applied Cryptography. CRC Press, 1977. Libro electrónico gratuito disponible en la página Web del autor
- Stallings, William. Cryptography and Network Security. Principles and Practice. Third ed., Prentice Hall International Editions, 2003.
- Pastor, José; Sarasa, Miguel Angel. Criptografía Digital. Colección Textos Docentes; Prensas Universitarias de Zaragoza, 1998.
- Schneier, Bruce. Applied Cryptography. Protocols, Algorithms, and Source Code in C. 2nd ed., John Wiley & Sons, Inc., 1996
- Fúster, A.; De la Guía, D.; Hernández, L.; Montoya, F.; Muñoz, J. Técnicas Criptográficas de Protección de Datos. 2ª ed, Ra-Ma, 2000
- Caballero, Pino. Introducción a la Criptografía. Ra-Ma, Textos Universitarios, 1996.
- Cariacedo Gallardo, Justo. Seguridad en Redes Telemáticas. McGraw Hill, 2004.
- Areitio, Javier. Seguridad de la Información. Redes, informática y sistemas de información. Paraninfo, 2008.

Otros recursos y materiales docentes complementarios

- Se facilitan en el Aula virtual de la Asignatura