

GUIA DOCENTE DE LA ASIGNATURA

# SEGURIDAD Y PROTECCIÓN DE SISTEMAS INFORMÁTICOS

MÓDULO	MATERIA	CURS O	SEMEST RE	CRÉDITOS	TIPO
<b>Formación de Especialidad 5: Tecnologías de la Información</b>	<b>Redes y Seguridad</b>	<b>4º</b>	<b>1º</b>	<b>6</b>	<b>Obligatoria</b>
PROFESOR(ES)		DIRECCIÓN COMPLETA DE CONTACTO PARA TUTORÍAS (Dirección postal, teléfono, correo electrónico, etc.)			
Alvaro Martinez Sevilla		Despacho 42, segunda planta, edif. Matemáticas. Facultad de Ciencias			
		HORARIO DE TUTORÍAS			
		Consultar en algebra.ugr.es			
GRADO EN EL QUE SE IMPARTE		OTROS GRADOS A LOS QUE SE PODRÍA OFERTAR			
<b>Grado en Ingeniería Informática</b>					
PRERREQUISITOS Y/O RECOMENDACIONES (Si ha lugar)					



## BREVE DESCRIPCIÓN DE CONTENIDOS (SEGÚN MEMORIA DE VERIFICACIÓN DEL GRADO)

Introducción a la seguridad de sistemas informáticos. Métodos de protección.

Técnicas criptográficas básicas y avanzadas.

Protocolos criptográficos y certificados digitales.

Aplicaciones de seguridad: Marcas de agua y comercio electrónico.

Seguridad en sistemas operativos, bases de datos y redes.

Seguridad en Internet: protocolos y herramientas.

Identidad digital e identificación biométrica en sistemas informáticos.

Aplicaciones y ejemplos.

## COMPETENCIAS GENERALES Y ESPECÍFICAS

**Competencias Específicas de la Asignatura**

**TI1.** Capacidad para comprender el entorno de una organización y sus necesidades en el ámbito de las tecnologías de la información y las comunicaciones.

**TI7.** Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos.

**Competencias Específicas del Título**

**E1.** Capacidad para concebir, redactar, organizar, planificar, desarrollar y firmar proyectos en el ámbito de la ingeniería en informática que tengan por objeto, de acuerdo con los conocimientos adquiridos, la concepción, el desarrollo o la explotación de sistemas, servicios y aplicaciones informáticas.

**E2.** Capacidad para dirigir las actividades objeto de los proyectos del ámbito de la informática de acuerdo con los conocimientos adquiridos.

**E3.** 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.

**E4.** Capacidad para definir, evaluar y seleccionar plataformas hardware y software para el desarrollo y la ejecución de sistemas, servicios y aplicaciones informáticas

**E7.** Capacidad para conocer, comprender y aplicar la legislación necesaria durante el desarrollo de la profesión de Ingeniero Técnico en Informática y manejar especificaciones, reglamentos y normas de obligado cumplimiento.

**E8.** 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.

**E9.** 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.

**E10.** Conocimientos para la realización de mediciones, cálculos, valoraciones, tasaciones, peritaciones, estudios, informes, planificación de tareas y otros trabajos análogos de informática

**E11.** Capacidad para analizar y valorar el impacto social y medioambiental de las soluciones técnicas, comprendiendo la responsabilidad ética y profesional de la actividad del Ingeniero Técnico en Informática.

### **Competencias Transversales o Generales**

**T1.** Capacidad de análisis y síntesis: Encontrar, analizar, criticar (razonamiento crítico), relacionar, estructurar y sintetizar información proveniente de diversas fuentes, así como integrar ideas y conocimientos.

**T2.** Capacidad de organización y planificación así como capacidad de gestión de la Información

**T3.** Capacidad de comunicación oral y escrita en el ámbito académico y profesional con especial énfasis, en la redacción de documentación técnica.

**T4.** Capacidad para la resolución de problemas

**T5.** Capacidad para tomar decisiones basadas en criterios objetivos (datos experimentales, científicos o de simulación disponibles) así como capacidad de argumentar y justificar lógicamente dichas decisiones, sabiendo aceptar otros puntos de vista.

**T6.** Capacidad para el uso y aplicación de las TIC en el ámbito académico y profesional.

**T7.** Capacidad de comunicación en lengua extranjera, particularmente en inglés.

**T8.** Capacidad de trabajo en equipo.

**T9.** Capacidad para el aprendizaje autónomo así como iniciativa y espíritu emprendedor.

**T10.** Motivación por la calidad y la mejora continua, actuando con rigor, responsabilidad y ética profesional.

**T11.** Capacidad para adaptarse a las tecnologías y a los futuros entornos actualizando las competencias profesionales.

**T12.** Capacidad para innovar y generar nuevas ideas.

**T15.** Capacidad para proyectar los conocimientos, habilidades y destrezas adquiridos para promover una sociedad basada en los valores de la libertad, la justicia, la igualdad y el pluralismo.



**OBJETIVOS (EXPRESADOS COMO RESULTADOS DE APRENDIZAJE)**

- Conocimiento de los servicios de seguridad básicos en los sistemas informáticos
- Conocimiento y comprensión de las vulnerabilidades y riesgos involucrados en los sistemas informáticos.
- Comprensión de los riesgos e implicaciones de las vulneraciones de la seguridad de los sistemas.
- Comprensión de las metodologías de ataque a la seguridad de los sistemas informáticos desde el punto de vista de la información.
- Conocimiento de las técnicas criptográficas basadas en algoritmos simétricos y asimétricos y su aplicación en los sistemas informáticos.
- Capacidad para definir y desplegar políticas de seguridad, orientadas tanto a la privacidad como a la confidencialidad, a la integridad, a la autenticación y a la disponibilidad.
- Conocimiento de las características de seguridad básicas de sistemas operativos, bases de datos y redes.
- Conocimiento y capacidad de uso de las técnicas de securización de la información.
- Conocimiento de los protocolos criptográficos y aspectos de seguridad en sus aplicaciones.
- Capacidad para desplegar infraestructuras de llave pública y mecanismos de autenticación.
- Conocimiento de los modelos y métodos de autorización de acceso a la información.
- Conocimiento de técnicas de autenticación y acceso seguras, incluyendo las basadas en certificados digitales e identificación biométrica.
- Conocimiento y capacidad de uso de las técnicas de certificación digital en diversos entornos de aplicaciones.
- Conocimiento y capacidad para desplegar soluciones para la protección digital de archivos multimedia mediante técnicas de "watermarking".
- Conocimiento y capacidad para desplegar técnicas de prevención, detección y mitigación de ataques.
- Conocimiento y capacidad de uso y configuración de herramientas para el análisis de vulnerabilidades y la mejora de la seguridad de los sistemas informáticos.
- Conocimiento del concepto y usos de la identificación digital en sistemas informáticos.
- Capacidad de uso de los servicios y tecnologías de seguridad existentes en el contexto actual de las TIC: firma digital e identificación electrónica.
- Familiarización y capacidad de uso del principal software criptográfico y de seguridad existente.
- Capacidad de uso de las principales aplicaciones de seguridad disponibles en Internet.



## TEMARIO DETALLADO DE LA ASIGNATURA

**1. Introducción a la seguridad de sistemas informáticos.**

Problemas de seguridad en sistemas informáticos. Amenazas. Métodos de control y protección. Terminología.

**2. Técnicas criptográficas de llave secreta.**

Introducción histórica a la criptografía. Criptosistemas clásicos. Algoritmos de llave simétrica: DES, RC5 y Rijndael (AES). Aspectos de seguridad y eficiencia. Modos de funcionamiento.

**3. Técnicas criptográficas de llave pública.**

Algoritmos de llave pública: RSA, El Gamal y otros. Comparación con los de llave privada. Necesidades de seguridad en las llaves.

**4. Protocolos criptográficos.**

Autenticación. Funciones hash. Firmas digitales. Protocolos de conocimiento mínimo. Compartición de secretos.

**5. Certificados Digitales y aplicaciones.**

Conceptos básicos. Autoridades de Certificación (CA). Estructura de Certificados: X.509. Distribución y renovación. Caducidad, Suspensión y Revocación. Aplicaciones: Sellado de Tiempos. Servicios de Notaría Digital.

**6. Marcas de Agua.**

El problema de la identificación de archivos. Esteganografía. Propiedades de las Marcas de Agua. Aplicaciones. Métodos de implementación.

**7. Seguridad en redes y comunicaciones.**

Problemas de seguridad en redes. Autenticación e identificación. Token de seguridad: Tarjetas Inteligentes. La seguridad de los medios de comunicación: línea telefónica, cable coaxial, fibra óptica, microondas, satélite.

**8. Seguridad y Privacidad en Internet.**

Problemas de seguridad en Internet. Protocolos seguros: IPSec, SSL y S-HTTP.

**9. Identidad Digital e Identificación biométrica.**

La Identidad Digital. Soluciones federativas para la identificación. Identificación biométrica. Tasas de falsa aceptación y falso rechazo. Técnicas de identificación biométrica: reconocimiento facial, de voz, huella dactilar, iris, geometría de la mano. Aplicación: El DNI electrónico.



**10. Comercio electrónico.**

Introducción y terminología. Clasificación de los Medios de Pago en el CE. Dinero Digital. Micropagos. Tarjetas de Crédito. Cheques electrónicos. Tarjetas Inteligentes. Protocolos de CE. Otros sistemas.

## BIBLIOGRAFÍA

**BIBLIOGRAFÍA FUNDAMENTAL:**

1. Menezes, Alfred J., Paul C. van Oorschot y Scott A. Vanstone  
**Handbook of Applied Cryptography.** CRC Press. 1997.
2. Pastor Franco, José , M.A. Sarasa López y J.L. Salazar  
**Criptografía digital: Fundamentos y aplicaciones.** Prensas Univ. De Zaragoza. 2ª ed. 2001.
3. Pieprzyk, J., T. Hardjono y J. Seberry  
**Fundamentals of Computer Security.** Springer. 2002.

**BIBLIOGRAFÍA COMPLEMENTARIA:**

4. Ashbourn, J.  
**Biometrics: Advanced identity verification. The complete guide.** Springer. 2000.
5. Schneier, Bruce  
**Applied Cryptography.** John Wiley & Sons. 2ª ed. 1997.
6. Wu, M. y B. Liu  
**Multimedia Data Hiding.** Springer. 2002.

## ENLACES RECOMENDADOS



## METODOLOGÍA DOCENTE

### 1. Lección magistral (Clases teóricas-expositivas) (grupo grande)

Descripción: Presentación en el aula de los conceptos propios de la materia haciendo uso de metodología expositiva con lecciones magistrales participativas y medios audiovisuales. Evaluación y examen de las capacidades adquiridas.

Propósito: Transmitir los contenidos de la materia motivando al alumnado a la reflexión, facilitándole el descubrimiento de las relaciones entre diversos conceptos y formarle una mentalidad crítica

Contenido en ECTS: 30 horas presenciales (1.2 ECTS)

Competencias: **TI1, TI7, E1, E2, E3, E4, E7, E8, E9, E10, E11, T1, T2, T3, T4, T5, T6, T7, T8, T9, T10, T11, T12, T15.**

### 2. Actividades prácticas (Clases prácticas de laboratorio) (grupo pequeño)

Descripción: Actividades a través de las cuales se pretende mostrar al alumnado cómo debe actuar a partir de la aplicación de los conocimientos adquiridos

Propósito: Desarrollo en el alumnado de las habilidades instrumentales de la materia.

Contenido en ECTS: 15 horas presenciales (0.6 ECTS)

Competencias: **TI1, TI7, E1, E2, E3, E4, E7, E8, E9, E10, E11, T1, T2, T3, T4, T5, T6, T7, T8, T9, T10, T11, T12, T15.**

### 3. Seminarios (grupo pequeño)

Descripción: Modalidad organizativa de los procesos de enseñanza y aprendizaje donde tratar en profundidad una temática relacionada con la materia. Incorpora actividades basadas en la indagación, el debate, la reflexión y el intercambio.

Propósito: Desarrollo en el alumnado de las competencias cognitivas y procedimentales de la materia.

Contenido en ECTS: 10 horas presenciales (0.4 ECTS)

Competencias: **TI1, TI7, E1, E2, E3, E4, E7, E8, E9, E10, E11, T1, T2, T3, T4, T5, T6, T7, T8, T9, T10, T11, T12, T15.**

### 4. Actividades no presenciales individuales (Estudio y trabajo autónomo)

Descripción: 1) Actividades (guiadas y no guiadas) propuestas por el profesor a través de las cuales y de forma individual se profundiza en aspectos concretos de la materia posibilitando al estudiante avanzar en la adquisición de determinados conocimientos y procedimientos de la materia, 2) Estudio individualizado de los contenidos de la materia 3) Actividades evaluativas (informes, exámenes, ...)

Propósito: Favorecer en el estudiante la capacidad para autorregular su aprendizaje, planificándolo, diseñándolo, evaluándolo y adecuándolo a sus especiales condiciones e intereses.

Contenido en ECTS: 45 horas no presenciales (1.8 ECTS)

Competencias: **TI1, TI7, E1, E2, E3, E4, E7, E8, E9, E10, E11, T1, T2, T3, T4, T5, T6, T7, T8, T9, T10, T11, T12, T15.**

### 5. Actividades no presenciales grupales (Estudio y trabajo en grupo)

Descripción: Actividades (guiadas y no guiadas) propuestas por el profesor a través de las cuales y de forma grupal se profundiza en aspectos concretos de la materia posibilitando a los estudiantes avanzar en la adquisición de determinados conocimientos y procedimientos de la materia.

Propósito: Favorecer en los estudiantes la generación e intercambio de ideas, la identificación y análisis de diferentes puntos de vista sobre una temática, la generalización o transferencia de conocimiento y la valoración crítica del mismo.

Contenido en ECTS: 45 horas no presenciales (1.8 ECTS)



Competencias: **TI1, TI7, E1, E2, E3, E4, E7, E8, E9, E10, E11, T1, T2, T3, T4, T5, T6, T7, T8, T9, T10, T11, T12, T15.**

#### 6. Tutorías académicas (grupo pequeño)

Descripción: manera de organizar los procesos de enseñanza y aprendizaje que se basa en la interacción directa entre el estudiante y el profesor

Propósito: 1) Orientan el trabajo autónomo y grupal del alumnado, 2) profundizar en distintos aspectos de la materia y 3) orientar la formación académica-integral del estudiante

Contenido en ECTS: 5 horas presenciales, grupales e individuales (0.2 ECTS)

Competencias: **TI1, TI7, E1, E2, E3, E4, E7, E8, E9, E10, E11, T1, T2, T3, T4, T5, T6, T7, T8, T9, T10, T11, T12, T15.**

#### EVALUACIÓN (INSTRUMENTOS DE EVALUACIÓN, CRITERIOS DE EVALUACIÓN Y PORCENTAJE SOBRE LA CALIFICACIÓN FINAL, ETC.)

Se utilizarán alguna o algunas de las siguientes técnicas de evaluación:

- Para la parte teórica se realizarán exámenes finales o parciales, sesiones de evaluación y entregas de ejercicios sobre el desarrollo y los resultados de las actividades propuestas. La ponderación de este bloque será del 30%.
- Para la parte práctica se realizarán prácticas de laboratorio, resolución de problemas y desarrollo de proyectos (individuales o en grupo), y se valorarán las entregas de los informes/memorias realizados por los alumnos, o en su caso las entrevistas personales con los alumnos y las sesiones de evaluación. La ponderación de este bloque será del 40%.
- En su caso, la parte de trabajo autónomo y los seminarios se evaluarán teniendo en cuenta la asistencia a los seminarios, los problemas propuestos que hayan sido resueltos y entregados por los alumnos, en su caso, las entrevistas efectuadas durante el curso y la presentación oral de los trabajos desarrollados. La ponderación será del 30%.

La calificación global corresponderá por tanto a la puntuación ponderada de los diferentes aspectos y actividades que integran el sistema de evaluación. Por tanto, el resultado de la evaluación será una calificación numérica obtenida mediante la suma ponderada de las calificaciones correspondientes a una parte teórica, una parte práctica y, en su caso, una parte relacionada con el trabajo autónomo de los alumnos, los seminarios impartidos y el aprendizaje basado en proyectos.

Todo lo relativo a la evaluación se regirá por la normativa sobre planificación docente y organización de exámenes vigente en la Universidad de Granada.

El sistema de calificaciones se expresará mediante calificación numérica de acuerdo con lo establecido en el art. 5 del R. D 1125/2003, de 5 de septiembre, por el que se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y validez en el territorio nacional.

Para los estudiantes que se acojan a la evaluación única final, esta modalidad de evaluación estará



formada por todas aquellas pruebas que el profesor estime oportunas, de forma que se pueda acreditar que el estudiante ha adquirido la totalidad de las competencias generales y específicas descritas en el apartado correspondiente de esta Guía Docente.

Todo lo relativo a la evaluación se regirá por la Normativa de evaluación y calificación de los estudiantes vigente en la Universidad de Granada, que puede consultarse en: Normativa de Evaluación y Calificación de los Estudiantes de la UGR

#### INFORMACIÓN ADICIONAL

Definición de grupo grande y grupo pequeño:

Los grupos grandes son grupos de 45 a 60 estudiantes.

Los grupos pequeños son grupos de 15 a 20 estudiantes.

