GUIA DOCENTE DE LA ASIGNATURA

SEGURIDAD Y PROTECCIÓN DE SISTEMAS INFORMÁTICOS

Curso 2015-16

MÓDULO	MATERIA	CURSO	SEMESTRE	CRÉDITOS	TIPO
Formación de Especialidad 5: Tecnologías de la Información	**Redes y Seguridad**	**4º**	**1º**	**6**	**Obligatoria**

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
Grado en Ingeniería Informática	

PRERREQUISITOS Y/O RECOMENDACIONES (Si ha lugar)
Se recomienda haber superado la asignatura ALEM (Algebra Lineal y Estructuras Matemáticas).

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 Internet: protocolos y herramientas.

Identidad digital e identificación biométrica en sistemas informáticos.

Aplicaciones y ejemplos.

COMPETENCIAS GENERALES Y ESPECÍFICAS

COMPETENCIAS ESPECÍFICAS DE LA ASIGNATURA
(SEGÚN MEMORIA DE VERIFICACIÓN DEL TÍTULO)
B1. Capacidad para la resolución de los problemas matemáticos que puedan plantearse en la
ingeniería. Aptitud para aplicar los conocimientos sobre: álgebra lineal; cálculo diferencial e
integral; métodos numéricos; algorítmica numérica; estadística y optimización.
B3. Capacidad para comprender y dominar los conceptos básicos de matemática discreta, lógica,
algorítmica y complejidad computacional, y su aplicación para la resolución de problemas propios
de La ingeniería.

COMPETENCIAS BÁSICAS
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;

COMPETENCIAS TRANSVERSALES
T5. Capacidad de trabajo en equipo, usando competencias demostrables mediante la elaboración y defensa de argumentos.

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.
Autentificación. Funciones hash. Firmas digitales. Protocolos de conocimiento mínimo. Compartición de secretos. Otros protocolos criptográficos.

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 Notaria Digital. Otras aplicaciones.

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. Seguridad y Privacidad en Internet.
Problemas de seguridad en redes. Autentificación e identificación. Token de seguridad. La seguridad de los medios de comunicación: línea telefónica, cable coaxial, fibra óptica, microondas, satélite. Problemas de seguridad en Internet. Protocolos seguros: IPSec, SSL y S-HTTP.

8. 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.

9. 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)

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: 20 horas presenciales (0.8 ECTS)

3. **Seminarios (grupo pequeño o grupo grande)**
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)

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: 55 horas no presenciales (2.2 ECTS)

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: 30 horas no presenciales (1.2 ECTS)

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)

REGIMEN DE ASISTENCIA

Se podrá requerir un mínimo de asistencia como parte de la evaluación continua.

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

En la convocatoria ordinaria, el alumno tendrá la posibilidad de elegir, durante el periodo de docencia, entre los siguientes métodos de evaluación:

1. 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.

2. Evaluación continua (recomendada si se quiere tener una visión y aprovechamiento de la asignatura que culmine en la superación de ésta) consistente en:
   - Para la parte teórica se realizarán exámenes finales o parciales, sesiones

de evaluación y entregas de ejercicios y/o retos de carácter teórico, 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/o retos de carácter práctico 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%. En caso de no ser aplicable, esta parte computará en la correspondiente a la evaluación de la parte teórica

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.

En la convocatoria extraordinaria, la evaluación por defecto será final única, aunque aquellos alumnos que hayan seguido el método de evaluación continua podrán elegir conservar la parte de calificación correspondiente a prácticas y proyectos.

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.

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.