GUIA DOCENTE DE LA ASIGNATURA

SEGURIDAD Y PROTECCIÓN DE SISTEMAS INFORMÁTICOS

Curso 2017-2018

(Fecha última actualización: 28/06/2017)
(Fecha de aprobación en Consejo de Departamento: 28/06/2017)

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

PROFESORES[1]	DIRECCIÓN COMPLETA DE CONTACTO PARA TUTORÍAS (Dirección postal, teléfono, correo electrónico, etc.)
Francisco Javier Lobillo Borrero	Dpto. Álgebra, 2ª planta, ETSI Informática y de Telecomunicación. Despacho nº 13. Correo electrónico: jlobillo@ugr.es
	HORARIO DE TUTORÍAS Y/O ENLACE A LA PÁGINA WEB DONDE PUEDAN CONSULTARSE LOS HORARIOS DE TUTORÍAS[1]
	Las horas de tutoría pueden consultarse en https://oficinavirtual.ugr.es en el apartado Ordenación Docente.
GRADO EN EL QUE SE IMPARTE	OTROS GRADOS A LOS QUE SE PODRÍA OFERTAR
Grado en Ingeniería Informática	

PRERREQUISITOS Y/O RECOMENDACIONES (si procede)

Tener cursada la asignatura ALEM

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.

[1] Consulte posible actualización en Acceso Identificado > Aplicaciones > Ordenación Docente

[2] Esta guía docente debe ser cumplimentada siguiendo la "Normativa de Evaluación y de Calificación de los estudiantes de la Universidad de Granada" (http://secretariageneral.ugr.es/pages/normativa/fichasugr/ncg7121/!)

- 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 ESPERABLES DE LA ENSEÑANZA)

- 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

TEMARIO TEÓRICO:

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: Bloque y flujo. 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, TLS y SHTTP.
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.

TEMARIO PRÁCTICO:

Prácticas de Laboratorio

Práctica 1. Cifrado de Vigenere.
Práctica 2. Criptosistemas simétricos.
Práctica 3. Criptosistemas asimétricos.
Práctica 4. Protocolos criptográficos.
Práctica 5. Certificados digitales.
Práctica 6. Conexiones seguras.

BIBLIOGRAFÍA

BIBLIOGRAFÍA FUNDAMENTAL:

- Hans Delfs and Helmut Knebl. *Introduction to Cryptography. Principles and Applications*. Information Security and Cryptography. Springer, 3rd edition, 2015.
- Joseph Migga Kizza. *Guide to Computer Network Security*. Computer Communications and Networks. Springer, 3rd. edition, 2015.
- Josef Pieprzyk, Thomas Hardjono, and Jennifer Seberry. *Fundamentals of Computer Security*. Springer, 2003.
- Ingemar J. Cox, Matthew L. Miller, Jeffrey A. Bloom, Jessica Fridrich, and Ton Kalker. *Digital Watermarking and Steganography*. The Morgan Kaufmann Series in Multimedia Information and Systems. Elsevier, 2nd edition, 2008.

BIBLIOGRAFÍA COMPLEMENTARIA:

- National Institute of Standards and Technology (NIST).
- C. Adams, P. Cain, D. Pinkas, and R. Zuccherato. Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP). IETF, August 2001.
- D. Cooper, S. Santesson, S. Farrell, S. Boeyen, R. Housley, and W. Polk. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. IETF, May 2008
- Kresimir Delac and Mislav Grgic. A survey of biometric recognition methods. In 46th International Symposium Electronics in Marine, ELMAR-2004, pages 184–193, 2004.
- T. Dierks and E. Rescorla. The Transport Layer Security (TLS) Protocol Version 1.2. IETF, August 2008
- Satoshi Nakamoto. Bitcoin: un sistema de dinero en efectivo electrónico peer-to-peer. Technical report, bitcoin.org. Traducido por @breathingdog.

ENLACES RECOMENDADOS

METODOLOGÍA DOCENTE

- **Lección magistral (Clases teóricas) (grupo amplio)** Presentación en el aula de los conceptos propios de la materia haciendo uso de metodología expositiva con lecciones magistrales participativas. Evaluación. Contenido en ECTS: 30 horas presenciales (1.2 ECTS)
- **Actividades prácticas (Clases prácticas de laboratorio) (grupo reducido)** Actividades a través de las cuales se pretende mostrar al alumnado cómo debe actuar a partir de la aplicación de los conocimientos adquiridos. Contenido en ECTS: 30 horas presenciales (1.2 ECTS)
- **Actividades no presenciales individuales (Estudio y trabajo autónomo)** Estudio individualizado de los contenidos de la materia. Realización individual de algunas de las tareas prácticas. Contenido en ECTS: 55 horas no presenciales (2.2 ECTS)
- **Actividades no presenciales grupales (Estudio y trabajo en grupo)** Horas de estudio grupal y realización por parejas de algunas de las actividades prácticas. Contenido en ECTS: 30 horas no presenciales (1.2 ECTS)
- **Tutorías académicas (individuales y grupales)** Resolución de dudas y orientación en la resolución de las tareas propuestas. Contenido en ECTS: 5 horas presenciales, grupales e individuales (0.2 ECTS)

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

La evaluación de la asignatura se basará en las siguientes pruebas:

- Examen teórico/práctico. El examen final de la asignatura será un examen escrito que comprenderá preguntas y ejercicios relativos a los contenidos impartidos en las lecciones magistrales utilizadas en el grupo amplio. Este examen se realizará tanto en la convocatoria ordinaria como en las extraordinarias.
- Prácticas. Las sesiones prácticas impartidas en grupos reducidos se basarán en tareas que deberán ser entregadas para su evaluación. La última práctica podrá ser considerada opcional a criterio del profesor.
- Trabajos. Los alumnos podrán opcionalmente proponer la realización de trabajos sobre temas que deberán ser aprobados por el profesor. Estos trabajos deberán ser presentados mediante exposición oral además de por escrito.

El porcentaje de cada una de las actividades anteriores en la convocatoria ordinaria depende de la realización o no de la última tarea:

- Modo A: Examen 30%, Prácticas 40%, Trabajo 30%.
- Modo B: Examen 40%, Prácticas 60%.

En las convocatorias extraordinarias se evaluará según el Modo B o mediante evaluación final única.

Los alumnos podrán en cualquier momento acogerse al método de evaluación final única.

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.

DESCRIPCIÓN DE LAS PRUEBAS QUE FORMARÁN PARTE DE LA EVALUACIÓN ÚNICA FINAL ESTABLECIDA EN LA "NORMATIVA DE EVALUACIÓN Y DE CALIFICACIÓN DE LOS ESTUDIANTES DE LA UNIVERSIDAD DE GRANADA"

Este modelo de evaluación consistirá en el examen teórico/práctico, que ponderará al 60%, junto con una tarea práctica, ponderable en un 40%, que será propuesta en el examen y para la que los alumnos dispondrán de un máximo de dos días naturales.

INFORMACIÓN ADICIONAL