GUÍA DOCENTE DE LA ASIGNATURA
SEGURIDAD Y PROTECCIÓN DE SISTEMAS INFORMÁTICOS

Curso: 2020-2021
Fecha última actualización: 09/07/2020
Fecha de aprobación por el Consejo de Departamento: 14/07/2020

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

PROFESOR(ES)	DIRECCIÓN COMPLETA DE CONTACTO PARA TUTORÍAS (Dirección postal, teléfono, correo electrónico, etc.)	HORARIO PARA TUTORÍAS
Grado en Granada: (1) Fco. Miguel García Olmedo Grado en Ceuta: (2) Juan Jesús Barbarán Sánchez	(1) Departamento de Álgebra, Fac. de Ciencias, planta baja, despacho 2. folmedo@ugr.es https://www.ugr.es/local/folmedo (2) Facultad de Educación, Economía y Tecnología. Campus Universitario de Ceuta. Dpto. de Álgebra, 2a planta. Despacho 38. barbaran@ugr.es https://www.ugr.es/~barbaran	Consultar en http://algebra.ugr.es o seguir el código QR:

GRADO EN EL QUE SE IMPARTE	OTROS GRADOS EN LOS QUE SE PODRÍA OFERTAR
Grado en Ingeniería Informática	no se conoce

PRERREQUISITOS Y/O RECOMENDACIONES (Si ha lugar)
Tener cursada la asignatura ALEM. Se recomienda la superación de los contenidos y adquisición de competencias de las materias de formación básica y de rama.

BREVE DESCRIPCIÓN DE CONTENIDOS (SEGÚN MEMORIA DE VERIFICACIÓN DEL TÍTULO)

- 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 (cfr. aquí, y en lo que sigue, Doc. Verifica. Grado Ing. Inf.)

El título de Graduado/a en Ingeniería Informática de la Universidad de Granada ha obtenido, con fecha 5 de junio de 2019, el sello Euro-Inf, otorgado por ANECA en colaboración con el Consejo General de Colegios Profesionales de Ingeniería en Informática (CCII) y con el Consejo General de Colegios Oficiales de Ingeniería Técnica en Informática (CONCITI). Esta acreditación garantiza el cumplimiento de criterios y estándares reconocidos por los empleadores españoles y del resto de Europa, de acuerdo con los principios de calidad, relevancia, transparencia, reconocimiento y movilidad contemplados en el Espacio Europeo de Educación Superior.

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 específicas

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 transversales o generales

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 DE LA ASIGNATURA

Temario de Teoría

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.

Termario de Prácticas (Prácticas de Laboratorio)

P1) Cifrado de Vigenère.

P2) Criptosistemas simétricos.

P3) Criptosistemas asimétricos.

P4) Protocolos criptográficos.

P5) Certificados digitales.

P6) 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

ACTIVIDADES FORMATIVAS

Lección Magistral (Clases Teóricas-Expositivas):

Actividades Prácticas (Clases prácticas en Laboratorio):.

Actividades no presenciales Individuales.

Actividades no presenciales grupales.

Tutorías académicas.

METODOLOGÍA DOCENTE

Lección Magistral: Presentación en el aula de los conceptos propios de la materia haciendo uso de metodología expositiva con lecciones magistrales participativas ilustradas con variedad de ejemplos.

Resolución de problemas: Realización en el aula de distintos ejercicios donde se abordan los diferentes tópicos de la asignatura.

Prácticas en Laboratorio: En el laboratorio probaremos diferentes formas de resolver problemas y analizaremos la eficiencia y fortaleza de éstas.

Exposición de Trabajos Tutelados: Los estudiantes deberán realizar un trabajo en grupos (2-4 personas) sobre un tema elegido por ellos. Este trabajo deberán exponerlo ante los demás estudiantes, que podrán preguntar y debatir sobre el tema.

Tutorías académicas: En el horario establecido, los estudiantes podrán realizar consultas personalizadas al profesor, así como exponer los distintos trabajos prácticos que hayan realizado.

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

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 Secretaría General Preferentemente, la evaluación se ajustará al sistema de evaluación continua del aprendizaje del estudiante siguiendo el artículo 7 de la anterior Normativa.
El criterio de evaluación se especifica a continuación:

- Un 50 % de la evaluación se basará en las prácticas entregadas y defendidas por los alumnos dentro de los plazos que se fijarán a lo largo del curso.
- Un 30 % de la evaluación se basará en la elaboración y presentación ante el profesor y el resto de estudiantes de un trabajo sobre un tema elegido por el estudiante.
- Un 20 % de la nota vendrá dada por el examen teórico práctico que se realizará una vez finalizado el curso.

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.
En las convocatorias extraordinarias la evaluación consistirá en un examen general.

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.

RÉGIMEN DE ASISTENCIA

- La asistencia a las clases teóricas no será obligatoria, aunque la participación activa en clase y la entrega de ejercicios planteados por el profesor se tendrá en cuenta dentro del sistema de evaluación continua de la asignatura.
- La asistencia a las clases prácticas no será obligatoria, exceptuando las sesiones en las que se programen pruebas de evaluación. En cualquier caso, la asistencia y participación activa en clase se tendrá en cuenta dentro del sistema de evaluación continua de la asignatura.

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"
Según la normativa vigente, la evaluación única final, entendiendo por tal la que se realiza en un solo acto académico, podrá incluir cuantas pruebas sean necesarias para acreditar que el estudiante ha adquirido la totalidad de las competencias descritas en la Guía Docente de la asignatura.

ESCENARIO A (ENSEÑANZA-APRENDIZAJE PRESENCIAL Y NO PRESENCIAL)	
ATENCIÓN TUTORIAL	
HORARIO	HERRAMIENTAS PARA LA ATENCIÓN TUTORIAL
Consultar en http://algebra.ugr.es	A través de mensajería, plataforma docente y/o videoconferencia
MEDIDAS DE ADAPTACIÓN DE LA METODOLOGÍA DOCENTE	
■ De acuerdo con el modelo y horarios establecidos por el centro, se complementará la docencia presencial con el uso de plataforma docente y/o docencia online a través de videoconferencia.	
MEDIDAS DE ADAPTACIÓN DE LA EVALUACIÓN (Instrumentos, criterios y porcentajes sobre la calificación final)	
Convocatoria Ordinaria	
■ La evaluación será preferiblemente presencial, aunque no se descarta que alguna de las pruebas se lleve a cabo en modalidad online a través de la plataforma docente y/o videoconferencia.	
Convocatoria Extraordinaria	
■ La evaluación será preferiblemente presencial, aunque no se descarta que alguna de las pruebas se lleve a cabo en modalidad online a través de la plataforma docente y/o videoconferencia.	
Evaluación Única Final	
■ La evaluación será preferiblemente presencial, aunque no se descarta que alguna de las pruebas se lleve a cabo en modalidad online a través de la plataforma docente y/o videoconferencia.	

ESCENARIO B (SUSPENSIÓN DE LA ACTIVIDAD PRESENCIAL)	
ATENCIÓN TUTORIAL	
HORARIO	HERRAMIENTAS PARA LA ATENCIÓN TUTORIAL
Consultar en http://algebra.ugr.es	A través de mensajería, plataforma docente y/o videoconferencia
MEDIDAS DE ADAPTACIÓN DE LA METODOLOGÍA DOCENTE	
■ Distribución de materiales teóricos y prácticos a través de plataforma docente. ■ Clase a través de videoconferencia.	
MEDIDAS DE ADAPTACIÓN DE LA EVALUACIÓN (Instrumentos, criterios y porcentajes sobre la calificación final)	
Convocatoria Ordinaria	
■ La evaluación será online mediante plataforma docente y/o videoconferencia.	
Convocatoria Extraordinaria	
■ La evaluación será online mediante plataforma docente y/o videoconferencia.	
Evaluación Única Final	
■ La evaluación será online mediante plataforma docente y/o videoconferencia.	