Guía docente de la asignatura

Seguridad y Protección de Sistemas Informáticos (Especialidad Tecnologías de la Información) (296114P)

Fecha de aprobación: **28/06/2023**

Grado	Grado en Ingeniería Informática	**Rama**	Ingeniería y Arquitectura
Módulo	Formación de Especialidad 5: Tecnologías de Información	**Materia**	Redes y Seguridad

Curso	4º	**Semestre**	1º	**Créditos**	6	**Tipo**	Obligatoria

PRERREQUISITOS Y/O RECOMENDACIONES

Es recomendable 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 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 de Sistemas Informáticos.
- Aplicaciones y ejemplos.

COMPETENCIAS ASOCIADAS A MATERIA/ASIGNATURA

COMPETENCIAS ESPECÍFICAS

- CE01 - 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.
- CE03 - 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

- CT05 - Capacidad de trabajo en equipo, usando competencias demostrables mediante la elaboración y defensa de argumentos.

RESULTADOS DE APRENDIZAJE (Objetivos)

- 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.

PROGRAMA DE CONTENIDOS TEÓRICOS Y PRÁCTICOS

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, ElGamal y otros. Comparación con los de llave privada. Necesidades de seguridad en las llaves.
4. Protocolos criptográficos. Autentificación. Funciones hash. Firmasdigitales. 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.

PRÁCTICO

- Cifrado de Vigenère.
- Criptosistemas simétricos.
- Criptosistemas asimétricos.
- Protocolos criptográficos.
- Certificados digitales.
- 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, 5th. 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

- 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

National Institute of Standards and Technology (NIST)

METODOLOGÍA DOCENTE

- MD01 - Lección Magistral (Clases Teóricas-Expositivas)
- MD02 - Actividades Prácticas (Resolución de Problemas, Resolución de Casos Prácticos, Desarrollo de Proyectos, Prácticas en Laboratorio, Taller de Programación, Aula de Informática, Prácticas de Campo).
- MD03 - Seminarios (Debates, Demos, Exposición de Trabajos Tutelados, Conferencias, Visitas Guiadas, Monografías).
- MD04 - Actividades no presenciales Individuales.
- MD05 - Actividades no presenciales Grupales.
- MD06 - Tutorías Académicas.

EVALUACIÓN (instrumentos de evaluación, criterios de evaluación y porcentaje sobre la calificación final)

EVALUACIÓN ORDINARIA

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 la prueba teórico-práctica que se realizará una vez finalizado el curso, la cual podría ser individual o en grupos.

Dadas las condiciones específicas de la asignatura, su docencia y las características del material evaluable, todas y cada una de las pruebas de evaluación serán en línea a través de los medios proporcionados por la plataforma oficial docente PRADO y salas de G-Meet creadas al efecto, las cuales serán suficientemente publicitadas.

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.

EVALUACIÓN EXTRAORDINARIA

En la convocatoría extraordinaria la evaluación consistirá en un examen general, que 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.

EVALUACIÓN ÚNICA FINAL

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.

INFORMACIÓN ADICIONAL

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.