Vulnerabilidades, amenazas y protocolos de seguridad informáticos

Curso Académico: (2022 / 2023) **Fecha de revisión: 17-04-2023**

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: CAMARA NUÑEZ, MARIA CARMEN

Tipo: Obligatoria Créditos ECTS : 6.0

Curso : 3 Cuatrimestre : 2

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

- Matemáticas
- Estadística e Informática del Módulo I (Formación básica) y la materia (asignatura) de Estadística (Investigación Operativa) del Módulo III (Fundamentos de ingeniería)
- Técnicas de Ocultación de información

OBJETIVOS

- Identificar los objetivos de seguridad y las vulnerabilidades, amenazas y riesgos de un sistema de información dado en un entorno operacional definido. Analizar las posibles medidas de seguridad a emplear en el mismo.
- Evaluar los servicios de seguridad a implementar en un sistema dado y diseñar y aplicar los mecanismos y protocolos consiguientes.
- Evaluar para un sistema dado las herramientas existentes de cifrado y esteganográficas para protegerlo.
- Usar los sistemas de firma y certificación en un entorno concreto. Evaluar y aplicar los mecanismos de autenticación pertinentes para acceder a un sistema específico.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

1. Introducción a las redes y los sistemas distribuidos.
2. Situación de la seguridad de los sistemas y productos informáticos.
3. Análisis y clasificación de los ataques informáticos.
4. Medidas, servicios y mecanismos de seguridad.
5. Firma digital. Autoridades de certificación. Infraestructuras de clave pública.
6. Sistemas de autenticación de varios factores y basados en infraestructuras de clave pública.
7. Protocolos de seguridad.

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

La actividades formativas incluyen:
1. Clases magistrales, tutorías individuales o en grupo, trabajo personal y presentaciones de los alumnos, incluyendo pruebas y exámenes teórico-prácticos. Para facilitar su desarrollo los alumnos recibirán las notas de clase en la herramienta web oportuna y tendrán textos básicos de referencia que les permita completar y profundizar en los temas más importantes o de mayor calado.
2. Prácticas en aulas informáticas en grupos reducidos, tutorías individuales y trabajo personal del alumno, incluyendo pruebas y exámenes. Todo ello orientado a la adquisición de habilidades prácticas relacionadas con el programa de cada asignatura.

Debido a la incertidumbre sobre el formato docente al que las circunstancias sanitarias nos avocarán durante el próximo curso, se prevé el inicio del mismo en la modalidad semipresencial, pudiendo derivar hacia la formación 100% presencial o 100% on-line según evolucione la propagación o el control sobre la pandemia y las normas higiénico-sanitarias que dicten las Autoridades del sector.

SISTEMA DE EVALUACIÓN

El sistema de evaluación incluye la evaluación continua del trabajo del alumno (pruebas de evaluación de habilidades y conocimientos teórico-prácticos e informes de prácticas de laboratorio) y la evaluación final a través de un examen escrito en que se evaluará de forma global los conocimientos, destrezas y capacidades adquiridas a lo largo del curso. La evaluación de la asignatura se realizará de acuerdo con los siguientes criterios:

1. Exámenes escritos de teoría y problemas: 70% de la nota final
   1.1. Exámenes de evaluación continua: 10% de la nota final. Aproximadamente a mediados del cuatrimestre.
   1.2. Examen escrito final de teoría y problemas: 60% de la nota final. Para superar la asignatura el alumno debe obtener un mínimo de 4 puntos en este examen.
2. Entrega de resultados de las prácticas en aulas informáticas: 30% de la nota final

En la convocatoria extraordinaria, el alumno elegirá entre:
a) Un examen final escrito por valor del 100% de la nota, compuesto de teoría, problemas y conocimientos adquiridos en las sesiones de laboratorio; o
b) Un examen final escrito por valor del 60% de la nota, compuesto de teoría y problemas. El restante 40% provendrá de la nota obtenida durante el curso en el examen de evaluación continua (10%) y las prácticas (30%)

Peso porcentual del Examen Final:	60
Peso porcentual del resto de la evaluación:	40

BIBLIOGRAFÍA BÁSICA

- Anderson, Ross Security Engineering: A guide to Building Dependable Distributed Sistems (2nd edition), Wiley, 2008
- Kaufman, Charlie, et al. Network Security: Private Communication in a Public World. Second Edition., Prentice Hall, 2002
- Pfleeger, Charles et al Security in Computing (4ª edition), Prentice Hall, 2007
- Stallings, William Cryptography and Network Security: Principles and Practice, Prentice Hall, 2013
- Vacca, John R. (editor) Computer and Information Security Handbook, Elsevier (The Morgan Kaufmann Series in Computer Security), 2009

BIBLIOGRAFÍA COMPLEMENTARIA

- Bishop, Matt Computer Security: Art & Science. (cap 12), Addison-Wesley, 2015
- Caballero, Pino. Introducción a la criptografía, Ra-Ma, 1999
- Kurose, James F. Ross, Keith W. Redes de Computadoras, un enfoque descendente, Pearson, 2017

RECURSOS ELECTRÓNICOS BÁSICOS

- ENISA . ENISA: http://www.enisa.europa.eu/publications
- INTECO . INTECO: <a href=" http://www.inteco.es/Seguridad/Observatorio" type="Reference"
- INTYPEDIA . INTYPEDIA: http://www.intypedia.com/
- NIST . NIST: http://csrc.nist.gov/publications/PubsSPs.html