

---

**Curso Académico: ( 2019 / 2020 )****Fecha de revisión: 21/04/2020 14:53:20**

---

**Departamento asignado a la asignatura: Departamento de Informática****Coordinador/a: GONZALEZ MANZANO, LORENA****Tipo: Obligatoria Créditos ECTS : 6.0****Curso : 4 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

Las competencias que se pretende que adquiera el estudiante son las siguientes:

- 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. Vulnerabilidades intrínsecas y extrínsecas.
3. Análisis y clasificación de los ataques informáticos. Valoración de sus consecuencias.
4. Medidas, servicios y mecanismos de seguridad. Riesgos que previenen.
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

Las 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.

#### SISTEMA DE EVALUACIÓN

<b>Peso porcentual del Examen/Prueba Final:</b>	55
<b>Peso porcentual del resto de la evaluación:</b>	45

#### 1. Convocatoria ordinaria - evaluación continua

Evaluación del alumno en la resolución de las prácticas de laboratorio, mediante trabajo(s) o examen/exámenes, según se indique: 30%

Examen parcial de teoría: 15% (No liberatorio).

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: 55%

Para poder promediar las calificaciones obtenidas en las anteriores evaluaciones, hará falta obtener en la evaluación final, al menos, el 40% de la nota máxima posible de ésta. Deberán entregarse todos los trabajos. En caso contrario, se aplicará lo dispuesto para la evaluación no continua.

#### 2. Convocatoria ordinaria - evaluación no continua

Examen final (100% de la nota final)

- La calificación máxima obtenible será de 6 puntos

- Deberán obtenerse 5 puntos para aprobar la asignatura

Esta prueba incluirá partes específicas para comprobar las competencias asociadas a los trabajos de laboratorio

#### 3. Convocatoria extraordinaria

La calificación de los estudiantes en la convocatoria extraordinaria se ajustará a las siguientes reglas:

a. Si el estudiante siguió el proceso de evaluación continua, el examen tendrá el mismo valor porcentual que en la convocatoria ordinaria, y la calificación final de la asignatura tendrá en cuenta la nota de la evaluación continua y la nota obtenida en el examen final.

b. Si el estudiante no siguió el proceso de evaluación continua, tendrá derecho a realizar un examen en la convocatoria extraordinaria con un valor del 100 % de la calificación total de la asignatura. Las características de los ejercicios de la evaluación continua no permiten autorizar al estudiante su entrega en la convocatoria extraordinaria

c. Aunque el estudiante hubiera seguido el proceso de evaluación continua, tendrá derecho a ser calificado en la convocatoria extraordinaria teniendo en cuenta únicamente la nota obtenida en el examen final cuando le resulte más favorable.

#### BIBLIOGRAFÍA BÁSICA

- Anderson, Ross Security Engineering: A guide to Building Dependable Distributed Systems (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 edición), 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: <http://www.inteco.es/Seguridad/Observatorio> type="Reference"

- INTYPEDIA . INTYPEDIA: <http://www.intypedia.com/>

- NIST . NIST: <http://csrc.nist.gov/publications/PubsSPs.html>