

Plan 413 GRADO EN INGENIERÍA INFORMÁTICA DE SERVICIOS Y APLICACIONES

Asignatura 40843 PROTOCOLOS Y COMUNICACIONES SEGURAS

Tipo de asignatura (básica, obligatoria u optativa)

OP (OPTATIVA)

Créditos ECTS

6 ECTS

Competencias que contribuye a desarrollar

2.1

Generales

- G01 : Conocimientos generales básicos.
- G03 : Capacidad de análisis y síntesis.
- G05 : Comunicación oral y escrita en la lengua propia.
- G06 : Conocimiento de una segunda lengua (Inglés).
- G07 : Habilidades básicas en el manejo del ordenador.
- G09 : Resolución de problemas.
- G16 : Capacidad de aplicar los conocimientos en la práctica.
- G18 : Capacidad de aprender.

2.2

Específicas

- E01 : 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.
- E02 : Comprensión y dominio de los conceptos básicos de matemática discreta, lógica, algorítmica y complejidad computacional, y su aplicación para el tratamiento automático de la información por medio de sistemas computacionales y para la resolución de problemas propios de la ingeniería.
- E03 : Conocimientos básicos sobre el uso y programación de los ordenadores, sistemas operativos, bases de datos y programas informáticos con aplicación en ingeniería.
- E11 : Conocimiento y aplicación de los procedimientos algorítmicos básicos de las tecnologías informáticas para diseñar soluciones a problemas, analizando la idoneidad y complejidad de los algoritmos propuestos.

Objetivos/Resultados de aprendizaje

P { margin-bottom: 0.21cm; }

- Plantear en lenguaje matemático y resolver problemas relacionados con la representación matemática de la información, su encriptación, y sus aplicaciones en la Seguridad Informática.
- Describir algorítmicamente la resolución de problemas relativos a la encriptación de datos, e implementarla eficientemente mediante software matemático.
- Comprender, discutir y expresar (oralmente y por escrito) conceptos y argumentos de tipo lógico matemático relacionados con la Seguridad Informática.
- Construcción de los modelos matemáticos necesarios para la resolución de problemas aplicados a la Seguridad Informática y su uso en la Empresa.
- Manejar software matemático en aplicaciones prácticas, con un énfasis especial en la interpretación de resultados y la escritura de informes.
- Comprender la interrelación de la Criptología con otras materias de la titulación.

## Contenidos

P { margin-bottom: 0.21cm; }

1. Criptología y comunicaciones seguras.

P { margin-bottom: 0.21cm; }

2. Criptografía simétrica.

P { margin-bottom: 0.21cm; }

3. Algoritmos básicos.

P { margin-bottom: 0.21cm; }

4. Criptografía de clave pública.

P { margin-bottom: 0.21cm; }

5. Protocolos criptográficos.

## Principios Metodológicos/Métodos Docentes

- Clases de teoría (26 horas)
- Prácticas en aula: resolución de problemas y prácticas con ordenador, realización de un Proyecto de Software en JAVA (30 horas)
- Actividades de evaluación continua (4 horas)

## Criterios y sistemas de evaluación

INSTRUMENTO/PROCEDIMIENTO

PESO EN LA NOTA FINAL

OBSERVACIONES

Realización de un Proyecto de software en grupo sobre los contenidos del curso.

80%

Se expondrá una demo la última semana del curso.

Realización de una práctica de ordenador, de carácter individual.

20%

Al finalizar el bloque temático 4.

Realización individual o en grupo de un trabajo de carácter teórico.

OPCIONAL

Para mejorar la nota obtenida en los apartados anteriores.

OBSERVACIONES:

La asignatura se podrá superar, con la asistencia al 80% de las clases, por la evaluación continua anteriormente descrita. En caso de no superar la asignatura mediante dicho método de evaluación, o que la asistencia a clase sea inferior al 80%, la evaluación de la asignatura se realizará en las convocatorias finales (ordinaria y extraordinaria), que consistirán en un examen teórico-práctico sobre los 5 bloques temáticos de la asignatura.

## Recursos de aprendizaje y apoyo tutorial

Recursos: Aula con pizarra y ordenador con proyector, sala de ordenadores con software matemático, biblioteca, sala de estudio, y despacho o seminario para tutorías.

Tutorías: consultar en el tablón virtual

[http://www.uva.es/opencms/portal/paginas/contenidoDinamico?funcion=C\\_Tutorias&cod\\_centro=321&carpeta=/contenidos/segovia/centros/EUInformatica/](http://www.uva.es/opencms/portal/paginas/contenidoDinamico?funcion=C_Tutorias&cod_centro=321&carpeta=/contenidos/segovia/centros/EUInformatica/)

Materiales del curso: en la plataforma virtual <http://campusvirtual.uva.es>

## Calendario y horario

El horario de clases, así como el calendario de exámenes, está publicado en los tablones y en la página web del centro: <http://www.eui.uva.es>

## Tabla de Dedicación del Estudiante a la Asignatura/Plan de Trabajo

ACTIVIDADES PRESENCIALES

HORAS

ACTIVIDADES NO PRESENCIALES

HORAS

Clases teórico-prácticas (T/M)

26

Estudio y trabajo autónomo individual

50

---

Clases prácticas de aula (A)

Estudio y trabajo autónomo grupal

40

Laboratorios (L)

30

Prácticas externas, clínicas o de campo

Seminarios (S)

Tutorías grupales (TG)

Evaluación

4

Total presencial

60

Total no presencial

90

---

Responsable de la docencia (recomendable que se incluya información de contacto y breve CV en el que aparezcan sus líneas de investigación y alguna publicación relevante)

José Ignacio Farrán Martín

Escuela Universitaria de Informática

Plaza de Santa Eulalia 9 y 11 - 40005 Segovia

Teléfono : (+34) 921 11 24 20

Fax : (+34) 921 11 24 01

e-mail : jifarran@eii.uva.es

web : <http://wmatem.eis.uva.es/~ignfar>

---

Idioma en que se imparte

Español

---