



POLITÉCNICA

CAMPUS  
DE EXCELENCIA  
INTERNACIONAL

PROCESO DE  
COORDINACIÓN DE LAS  
ENSEÑANZAS PR/CL/001



E.T.S. de Ingeniería de  
Sistemas Informáticos

# ANX-PR/CL/001-01

## GUÍA DE APRENDIZAJE

### ASIGNATURA

**615000236 - Fundamentos de seguridad**

### PLAN DE ESTUDIOS

61IW - Grado en Ingeniería del Software

### CURSO ACADÉMICO Y SEMESTRE

2017/18 - Segundo semestre

## Índice

---

### Guía de Aprendizaje

1. Datos descriptivos.....	1
2. Profesorado.....	1
3. Conocimientos previos recomendados.....	3
4. Competencias y resultados de aprendizaje.....	3
5. Descripción de la asignatura y temario.....	4
6. Cronograma.....	7
7. Actividades y criterios de evaluación.....	10
8. Recursos didácticos.....	13
9. Otra información.....	14

## 1. Datos descriptivos

---

### 1.1. Datos de la asignatura

<b>Nombre de la asignatura</b>	615000236 - Fundamentos de seguridad
<b>No de créditos</b>	3 ECTS
<b>Carácter</b>	Obligatoria
<b>Curso</b>	Primer curso
<b>Semestre</b>	Segundo semestre
<b>Período de impartición</b>	Febrero-Junio
<b>Idioma de impartición</b>	Castellano
<b>Titulación</b>	61IW - Grado en Ingeniería del Software
<b>Centro en el que se imparte</b>	Escuela Técnica Superior de Ingeniería de Sistemas Informáticos
<b>Curso académico</b>	2017-18

## 2. Profesorado

---

### 2.1. Profesorado implicado en la docencia

<b>Nombre</b>	<b>Despacho</b>	<b>Correo electrónico</b>	<b>Horario de tutorías *</b>
Jorge Ramio Aguirre	1106	jorge.ramio@upm.es	Sin horario. Como los horarios de tutorías pueden variar en función de las necesidades de los alumnos a lo largo de la impartición de la asignatura, se publicarán en los

			cauces de comunicación con el alumnado al inicio de la impartición de la asignatura.
Maria Angeles Mahillo Garcia (Coordinador/a)	1110	mariaangeles.mahillo@upm.es	Sin horario. Como los horarios de tutorías pueden variar en función de las necesidades de los alumnos a lo largo de la impartición de la asignatura, se publicarán en los cauces de comunicación con el alumnado al inicio de la impartición de la asignatura.
Jesus Sanchez Lopez	1117	jesus.sanchezl@upm.es	Sin horario. Como los horarios de tutorías pueden variar en función de las necesidades de los alumnos a lo largo de la impartición de la asignatura, se publicarán en los cauces de comunicación con el alumnado al inicio de la impartición de la asignatura.

\* Las horas de tutoría son orientativas y pueden sufrir modificaciones. Se deberá confirmar los horarios de tutorías con el profesorado.

### 3. Conocimientos previos recomendados

---

#### 3.1. Asignaturas previas que se recomienda haber cursado

El plan de estudios Grado en Ingeniería del Software no tiene definidas asignaturas previas recomendadas para esta asignatura.

#### 3.2. Otros conocimientos previos recomendados para cursar la asignatura

- Aritmética modular
- Álgebra matricial

### 4. Competencias y resultados de aprendizaje

---

#### 4.1. Competencias que adquiere el estudiante al cursar la asignatura

CC1 - Capacidad para diseñar, desarrollar, seleccionar y evaluar aplicaciones y sistemas informáticos, asegurando su fiabilidad, seguridad y calidad, conforme a principios éticos y a la legislación y normativa vigente.

CT5 - Organización y planificación: Identificar y definir eficazmente las metas, objetivos y prioridades de una tarea o proyecto a desempeñar estipulando las actividades, los plazos y los recursos requeridos y controlando los procesos establecidos.

## 4.2. Resultados del aprendizaje al cursar la asignatura

RA143 - Conoce y aplica métodos y algoritmos matemáticos que se usarán en las implementaciones criptográficas.

RA144 - Analiza, clasifica y aplica los algoritmos de cifra clásica.

RA145 - Identifica los elementos básicos de la criptografía simétrica distinguiendo la cifra en flujo y bloque.

RA87 - Identifica y define eficazmente las metas, objetivos y prioridades de una tarea o proyecto a desempeñar estipulando las actividades, los plazos y los recursos requeridos y controlando los procesos establecidos.

RA141 - Conoce los conceptos de la seguridad de la información y las razones que la definen como un proceso.

RA146 - Conoce y aplica los principios de la cifra en flujo y los algoritmos A5 y RC4.

RA147 - Conoce y aplica los principios de la cifra en bloque y los algoritmos DES, TDES, y AES.

## 5. Descripción de la asignatura y temario

---

### 5.1. Descripción de la asignatura

En esta asignatura se introducen los conceptos y principios básicos de la seguridad de la información, abarcando las temáticas relacionadas con su protección mediante técnicas de criptografía simétrica.

### 5.2. Temario de la asignatura

#### 1. Seguridad de la Información

- 1.1. Introducción a la Seguridad de la Información
- 1.2. Seguridad Informática versus Seguridad de la Información
- 1.3. Objetivos de la seguridad de la información
- 1.4. Servicios de la seguridad de la información
- 1.5. Amenazas, puntos débiles o vulnerabilidades
- 1.6. La Seguridad de la Información desde distintos puntos de vista

#### 2. Criptografía Clásica

- 2.1. Introducción

- 2.1.1. Definición, términos relacionados y usos de la criptografía
- 2.1.2. Historia de la criptografía y técnicas de cifrado clásicas
- 2.2. Cifrado por transposición
  - 2.2.1. Características. Un poco de historia
  - 2.2.2. Cifrado y descifrado por columnas
  - 2.2.3. Cifrado y descifrado por filas
- 2.3. Cifrado por sustitución
  - 2.3.1. Conceptos relacionados
  - 2.3.2. Clasificación de la cifra por sustitución
  - 2.3.3. Cifrado monoalfabético
    - 2.3.3.1. Un poco de historia
    - 2.3.3.2. Cifrado y descifrado por desplazamiento puro. Criptoanálisis
    - 2.3.3.3. Cifrado y descifrado por decimación pura. Criptoanálisis
    - 2.3.3.4. Cifrado y descifrado por decimación afín. Criptoanálisis
- 2.4. Cifrado polialfabético por sustitución
  - 2.4.1. El cifrador de Vigenère
  - 2.4.2. Ataque por el método de Kasiski
- 2.5. Cifrado monoalfabético poligramánico
  - 2.5.1. Cifrado de Hill
  - 2.5.2. Ataque Gauss Jordan a la cifra de Hill
- 3. Criptografía Moderna: Cifrado Simétrico
  - 3.1. Introducción. Hitos en la Criptografía
  - 3.2. Clasificación de los sistemas de cifra
  - 3.3. Características de la cifra simétrica
  - 3.4. Cifrado de Flujo
    - 3.4.1. Esquema de la cifra simétrica en flujo
    - 3.4.2. Fundamentos de la cifra en flujo
    - 3.4.3. Registros de desplazamiento FSR
    - 3.4.4. Ataque de Berlekamp-Massey

#### 3.4.5. Algoritmos A5 y RC4

### 3.5. Cifrado en Bloque

#### 3.5.1. Esquema de la cifra simétrica en bloque

#### 3.5.2. Características de la cifra en bloque

#### 3.5.3. Modos de cifra en bloque

#### 3.5.4. Algoritmos DES y 3DES

#### 3.5.5. Algoritmo AES

### 3.6. Comparativa de tasa de cifra entre algoritmos de bloque y flujo.

## 6. Cronograma

### 6.1. Cronograma de la asignatura \*

Sem	Actividad presencial en aula	Actividad presencial en laboratorio	Otra actividad presencial	Actividades de evaluación
1	<b>Clase de teoría: Impartición de contenidos</b> Duración: 02:00 LM: Actividad del tipo Lección Magistral			
2	<b>Clase de teoría: Impartición de contenidos</b> Duración: 02:00 LM: Actividad del tipo Lección Magistral			
3	<b>Clase de teoría: Impartición de contenidos</b> Duración: 02:00 LM: Actividad del tipo Lección Magistral			
4	<b>Clase de teoría: Impartición de contenidos</b> Duración: 01:30 LM: Actividad del tipo Lección Magistral  <b>Clase de resolución de cuestiones y/o ejercicios</b> Duración: 00:30 PR: Actividad del tipo Clase de Problemas			<b>Competencia Transversal (R87)</b> TI: Técnica del tipo Trabajo Individual Evaluación continua Duración: 00:00
5	<b>Clase de teoría: Impartición de contenidos</b> Duración: 01:30 LM: Actividad del tipo Lección Magistral  <b>Clase de resolución de cuestiones y/o ejercicios</b> Duración: 00:30 PR: Actividad del tipo Clase de Problemas			
6	<b>Clase de teoría: Impartición de contenidos</b> Duración: 01:30 LM: Actividad del tipo Lección Magistral  <b>Clase de resolución de cuestiones y/o ejercicios</b> Duración: 00:30 PR: Actividad del tipo Clase de Problemas			
7	<b>Clase de teoría: Impartición de contenidos</b> Duración: 01:30 LM: Actividad del tipo Lección Magistral  <b>Clase de resolución de cuestiones y/o ejercicios</b> Duración: 00:30 PR: Actividad del tipo Clase de Problemas			

8	<p><b>Clase de teoría: Impartición de contenidos</b> Duración: 01:30 LM: Actividad del tipo Lección Magistral</p> <p><b>Clase de resolución de cuestiones y/o ejercicios</b> Duración: 00:30 PR: Actividad del tipo Clase de Problemas</p>			
9	<p><b>Clase de teoría: Impartición de contenidos</b> Duración: 01:30 LM: Actividad del tipo Lección Magistral</p> <p><b>Clase de resolución de cuestiones y/o ejercicios</b> Duración: 00:30 PR: Actividad del tipo Clase de Problemas</p>			
10	<p><b>Clase de teoría: Impartición de contenidos</b> Duración: 01:30 LM: Actividad del tipo Lección Magistral</p> <p><b>Clase de resolución de cuestiones y/o ejercicios</b> Duración: 00:30 PR: Actividad del tipo Clase de Problemas</p>			<p><b>Examen Tema 1 y 2 (Ev. Continua) (RA143, RA141, RA144)</b> EX: Técnica del tipo Examen Escrito Evaluación continua Duración: 02:00</p>
11	<p><b>Clase de teoría: Impartición de contenidos</b> Duración: 01:30 LM: Actividad del tipo Lección Magistral</p> <p><b>Clase de resolución de cuestiones y/o ejercicios</b> Duración: 00:30 PR: Actividad del tipo Clase de Problemas</p>			
12	<p><b>Clase de teoría: Impartición de contenidos</b> Duración: 01:30 LM: Actividad del tipo Lección Magistral</p> <p><b>Clase de resolución de cuestiones y/o ejercicios</b> Duración: 00:30 PR: Actividad del tipo Clase de Problemas</p>			
13	<p><b>Clase de teoría: Impartición de contenidos</b> Duración: 01:30 LM: Actividad del tipo Lección Magistral</p> <p><b>Clase de resolución de cuestiones y/o ejercicios</b> Duración: 00:30 PR: Actividad del tipo Clase de Problemas</p>			

14	<p><b>Clase de teoría: Impartición de contenidos</b> Duración: 01:30 LM: Actividad del tipo Lección Magistral</p> <p><b>Clase de resolución de cuestiones y/o ejercicios</b> Duración: 00:30 PR: Actividad del tipo Clase de Problemas</p>			
15	<p><b>Clase de teoría: Impartición de contenidos</b> Duración: 01:30 LM: Actividad del tipo Lección Magistral</p> <p><b>Clase de resolución de cuestiones y/o ejercicios</b> Duración: 00:30 PR: Actividad del tipo Clase de Problemas</p>			
16	<p><b>Clase de teoría: Impartición de contenidos</b> Duración: 02:00 OT: Otras actividades formativas</p>			
17				<p><b>Examen Tema 3 (Ev. Continua) (RA141, RA145, RA147, RA146)</b> EX: Técnica del tipo Examen Escrito Evaluación continua Duración: 02:00</p> <p><b>Examen "Sólo prueba final" (RA87, RA141, RA143, RA144,,RA145, RA146, RA147)</b> EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Duración: 03:00</p> <p><b>Asistencia a clases</b> OT: Otras técnicas evaluativas Evaluación continua Duración: 00:00</p>

Las horas de actividades formativas no presenciales son aquellas que el estudiante debe dedicar al estudio o al trabajo personal.

Para el cálculo de los valores totales, se estima que por cada crédito ECTS el alumno dedicará dependiendo del plan de estudios, entre 26 y 27 horas de trabajo presencial y no presencial.

\* El cronograma sigue una planificación teórica de la asignatura y puede sufrir modificaciones durante el curso.

## 7. Actividades y criterios de evaluación

### 7.1. Actividades de evaluación de la asignatura

#### 7.1.1. Evaluación continua

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
4	Competencia Transversal (R87)	TI: Técnica del tipo Trabajo Individual	No Presencial	00:00	5%	/ 10	CT5
10	Examen Tema 1 y 2 (Ev. Continua) (RA143, RA141, RA144)	EX: Técnica del tipo Examen Escrito	Presencial	02:00	45%	/ 10	CC1
17	Examen Tema 3 (Ev. Continua) (RA141, RA145, RA147, RA146)	EX: Técnica del tipo Examen Escrito	Presencial	02:00	45%	/ 10	CC1
17	Asistencia a clases	OT: Otras técnicas evaluativas	Presencial	00:00	5%	/ 10	

#### 7.1.2. Evaluación sólo prueba final

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
17	Examen "Sólo prueba final" (RA87, RA141, RA143, RA144, RA145, RA146, RA147)	EX: Técnica del tipo Examen Escrito	Presencial	03:00	100%	5 / 10	CT5 CC1

#### 7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Evaluación de los temas 1, 2, 3 y de la competencial transversal (RA87, RA141, RA143, RA144, RA145, RA146, RA147)	EX: Técnica del tipo Examen Escrito	Presencial	03:00	100%	5 / 10	CT5 CC1

## 7.2. Criterios de evaluación

### 1. ELECCIÓN DEL SISTEMA DE EVALUACIÓN

De acuerdo con el artículo 20 de la normativa reguladora de los sistemas de evaluación en los procesos formativos vinculados a los títulos de grado y máster universitario con planes de estudio adaptados al R.D. 1393/2007.

En la convocatoria ordinaria de esta asignatura, la elección entre el sistema de evaluación continua o el sistema de evaluación mediante sólo prueba final corresponde al estudiante.

El alumno que desee seguir el sistema de evaluación mediante sólo prueba final, deberá comunicarlo respondiendo a la consulta que la asignatura formulará en la plataforma Moodle de la misma. Fecha tope para la solicitud **25 de mayo de 2018**.

El sistema de evaluación continua será el que se aplique en general a todos los estudiantes, si el alumno no comunica lo contrario por el medio anteriormente expuesto.

### 2. CRITERIOS DE CALIFICACIÓN.

#### 2.1. CONVOCATORIA ORDINARIA.

##### 2.1.1 EVALUACIÓN CONTINUA.

Los instrumentos que se van a utilizar en la evaluación de proceso de aprendizaje de los alumnos en evaluación continua se detallan a continuación

Técnica evaluativa	Descripción	Peso	Fecha
OT: Otras técnicas evaluativas	Asistencia y participación en el aula	5%	
TI: Técnica del tipo Trabajo	Realización de actividades	5%	Semana 4. Fecha concreta

Individual	relacionadas con la competencia Planificación y Organización (CT_5)		se indicará en la plataforma de la asignatura
EX: Técnica del tipo Examen Escrito	Evaluación de los temas 1 y 2.	45%	Fecha proporcionada por Sub. Ord. Académica y Doctorado
EX: Técnica del tipo Examen Escrito	Evaluación del tema 3.	45%	Fecha proporcionada por Sub. Ord. Académica y Doctorado

Para superar la asignatura se necesita obtener una nota igual o superior a 5 una vez evaluadas las actividades anteriores.

Para superar la competencia transversal deberán realizarse todas las actividades propuestas para la misma y obtener una calificación APTO. La calificación numérica a sumar a la nota de la asignatura vendrá dada por la evaluación de una o varias de las actividades propuestas.

### 2.1.2. EVALUACIÓN "SÓLO EXAMEN FINAL".

Los alumnos que hayan decidido no seguir la evaluación continua, tendrán la posibilidad de presentarse a un examen escrito final sobre 9,5 puntos. En el mismo se evaluará tanto los contenidos teóricos como las actividades prácticas realizadas durante el curso. Para aquellos que hayan sido evaluados de la competencia transversal, la nota numérica obtenida en la misma se sumará a la obtenida en el examen de la convocatoria ordinaria. Los alumnos que no hayan sido evaluados de la competencia transversal deberán entregar las actividades propuestas en la fecha que indique la asignatura.

### 2.2. CONVOCATORIA EXTRAORDINARIA.

De acuerdo con el artículo 19 de la normativa reguladora de los sistemas de evaluación en los procesos formativos vinculados a los títulos de grado y máster universitario con planes de estudio adaptados al R.D. 1393/2007

Todos los alumnos que no hayan superado la asignatura en la convocatoria ordinaria tendrán la posibilidad de presentarse a un examen escrito final sobre 9,5 puntos. En el mismo se evaluará tanto los contenidos teóricos

como las actividades prácticas realizadas durante el curso. Para aquellos que hayan sido evaluados de la competencia transversal, la nota numérica obtenida en la misma se sumará a la obtenida en el examen de la convocatoria ordinaria. Los alumnos que no hayan sido evaluados de la competencia transversal deberán entregar las actividades propuestas en la fecha que indique la asignatura.

## 8. Recursos didácticos

### 8.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
Plataforma Moodle de GATE para la asignatura	Equipamiento	Plataforma Moodle de GATE para la asignatura
Software	Equipamiento	Software: software de laboratorio propio de libre distribución ( <a href="http://www.criptored.upm.es/paginas/software.htm">http://www.criptored.upm.es/paginas/software.htm</a> )
Sitios web	Recursos web	Todos aquellos sitios web oficiales que estén relacionados con la materia impartida: Red Temática de Criptografía y Seguridad de la Información Inteco, Agencia de Protección de Datos, Normas UNE (NorWeb), etc.
Pildoras Formativas	Recursos web	Proyecto Thoth de la Red Temática Criptored, Dirigido por el Dr. Jorge Ramío y el Dr. Alfonso Muñoz
Fundamentos de Seguridad Tomo I	Bibliografía	Introducción a la seguridad de la información. Cifra Clásica. Cifra Moderna Simétrica

## 9. Otra información

---

### 9.1. Otra información sobre la asignatura

El equipo docente de la materia "Seguridad de la Información" de este plan de estudios con el fin de ayudar a los alumnos a la preparación de la asignatura, elaborarán hojas de ejercicios con enunciado y solución para que ellos puedan seguir y desarrollar en aula dichos ejercicios prácticos. Algunos ejercicios serán resueltos en horas de clase, mientras que otros, una vez que los alumnos hayan intentado su resolución podrán consultar su resolución en horas de tutorías.

Se elaborarán pequeñas prácticas de los temas 2 y 3, para que sean resueltas con el software libre proporcionado por la asignatura.