# ANX-PR/CL/001-01

# GUÍA DE APRENDIZAJE

## ASIGNATURA

**615000244 - Seguridad de la informacion**

## PLAN DE ESTUDIOS

61IW - Grado en Ingenieria 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....2
4. Competencias y resultados de aprendizaje....2
5. Descripción de la asignatura y temario....4
6. Cronograma....6
7. Actividades y criterios de evaluación....8
8. Recursos didácticos....11

# 1. Datos descriptivos

## 1.1. Datos de la asignatura

| | |
|---|---|
| **Nombre de la asignatura** | 615000244 - Seguridad de la informacion |
| **No de créditos** | 3 ECTS |
| **Carácter** | Obligatoria |
| **Curso** | Segundo curso |
| **Semestre** | Cuarto semestre |
| **Período de impartición** | Febrero-Junio |
| **Idioma de impartición** | Castellano |
| **Titulación** | 61IW - Grado en Ingenieria del Software |
| **Centro en el que se imparte** | Escuela Tecnica Superior de Ingenieria de Sistemas Informaticos |
| **Curso académico** | 2017-18 |

# 2. Profesorado

## 2.1. Profesorado implicado en la docencia

| Nombre | Despacho | Correo electrónico | Horario de tutorías * |
|---|---|---|---|
| Jorge Ramio Aguirre (Coordinador/a) | 1106 | jorge.ramio@upm.es | M - 13:00 - 17:00<br>X - 09:00 - 11:00 |
| Maria Angeles Mahillo Garcia | 1110 | mariaangeles.mahillo@upm.es | L - 14:00 - 17:00<br>J - 13:00 - 14:00<br>V - 14:00 - 16:00 |

* 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

- Fundamentos de seguridad

- Algebra

- Logica y matematica discreta

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

El plan de estudios Grado en Ingenieria del Software no tiene definidos otros conocimientos previos para esta asignatura.

# 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.

CT8 - Trabajo en equipo: Ser capaz de trabajar como miembro de un equipo interdisciplinar con la finalidad de contribuir a desarrollar proyectos con pragmatismo y sentido de la responsabilidad, asumiendo compromisos teniendo en cuenta los recursos disponibles.

## 4.2. Resultados del aprendizaje al cursar la asignatura

RA195 - Conoce y analiza el funcionamiento de las funciones hash MD5 y SHA-1, aplicando los algoritmos..

RA198 - Analiza y aplica el algoritmo RSA para la firma digital.

RA199 - Conoce y calcula los NNC y las CP en el uso del algoritmo de cifrado RSA y realiza diferentes ataques al sistema.

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

RA200 - Conoce formas y mecanismos de autenticación así como la utilidad de los certificados digitales

RA201 - Desarrollar sistemas de gestión de la seguridad de la información SGSI, de acuerdo a estándares y normas internacionales

RA118 - Es capaz de trabajar como miembro de un equipo con la finalidad de contribuir a desarrollar proyectos con pragmatismo y sentido de la responsabilidad, asumiendo compromisos y teniendo en cuenta los recursos disponibles. Se desenvuelve de modo que logra generar confianza y credibilidad en un grupo de colaboradores, además del compromiso para el logro de la visión corporativa a través de negociaciones y motivaciones, y no de manera coercitiva e individualista.

RA197 - Compara los sistemas de cifra simétrica con los de cifra asimétrica y es capaz de aplicar los algoritmos adecuados a cada situación

RA85 - Conoce y aplica los esquemas de protección de la información basados en la aplicación de técnicas criptográficas

# 5. Descripción de la asignatura y temario

## 5.1. Descripción de la asignatura

En esta asignatura se estudia la protección de la información utilizando técnicas de criptografía asimétrica, firma digital y certificados digitales. Tambien introduce en las fases e implantación de un Sistema de Gestión de la Seguridad de la Información.

## 5.2. Temario de la asignatura

1. Funciones hash
    1.1. Características y propiedades de las funciones hash.
    1.2. Funciones hash MD5, SHA1, SHA256, SHA3
    1.3. Ataques a las funciones hash
2. Criptografía Asimétrica o de clave pública.
    2.1. Introducción
    2.2. Intercambio de clave de Diffie y Hellman.
    2.3. Caracteristicas. Ventajas y desventajas frente al cifrado simétrico
3. Principios del algoritmo (Rivest, Shamir y Adleman)
    3.1. Generación de claves y operaciones típicas con RSA
    3.2. Algoritmo para el cálculo de inversos
    3.3. Algoritmo de exponenciación rápida
4. Cifrado y descifrado con RSA
    4.1. Cifrar y descifrar mensajes de texto
    4.2. Claves parejas
    4.3. Números no cifrables
5. Ataques al RSA
    5.1. Ataque basado en la factorización del módulo n
    5.2. Ataque por cifrado cíclico con la clave pública

5.3. Ataque basado en la paradoja del cumpleaños

6. Sistemas de Autenticación

6.1. Firma digital RSA y Elgamal

6.2. Mecanismos de autenticación

7. Sistema de Gestión de la Seguridad de la Información

7.1. Introducción a políticas y planes de seguridad.

7.2. Implantación de un SGSI.

7.3. Fases de un SGSI.

# 6. Cronograma

## 6.1. Cronograma de la asignatura *

| Sem | Actividad presencial en aula | Actividad presencial en laboratorio | Otra actividad presencial | Actividades de evaluación |
|---|---|---|---|---|
| 1 | **Clase de teoría: Impartición de contenidos**<br>Duración: 01:00<br>LM: Actividad del tipo Lección Magistral | | | |
| 2 | **Clase de teoría: Impartición de contenidos**<br>Duración: 01:00<br>LM: Actividad del tipo Lección Magistral | **Resolución de Ejercicios**<br>Duración: 01:00<br>PR: Actividad del tipo Clase de Problemas | | |
| 3 | **Clase de teoría: Impartición de contenidos**<br>Duración: 01:00<br>LM: Actividad del tipo Lección Magistral | **Resolución de Ejercicios**<br>Duración: 01:00<br>PR: Actividad del tipo Clase de Problemas | | |
| 4 | **Clase de teoría: Impartición de contenidos**<br>Duración: 01:00<br>LM: Actividad del tipo Lección Magistral | **Resolución de Ejercicios**<br>Duración: 01:00<br>PR: Actividad del tipo Clase de Problemas | | |
| 5 | **Clase de teoría: Impartición de contenidos**<br>Duración: 01:00<br>LM: Actividad del tipo Lección Magistral | **Resolución de Ejercicios**<br>Duración: 01:00<br>PR: Actividad del tipo Clase de Problemas | | |
| 6 | **Clase de teoría: Impartición de contenidos**<br>Duración: 01:00<br>LM: Actividad del tipo Lección Magistral | **Resolución de Ejercicios**<br>Duración: 01:00<br>PR: Actividad del tipo Clase de Problemas | | |
| 7 | **Clase de teoría: Impartición de contenidos**<br>Duración: 01:00<br>LM: Actividad del tipo Lección Magistral | **Resolución de Ejercicios**<br>Duración: 01:00<br>PR: Actividad del tipo Clase de Problemas | | |
| 8 | **Clase de teoría: Impartición de contenidos**<br>Duración: 01:00<br>LM: Actividad del tipo Lección Magistral | **Resolución de Ejercicios**<br>Duración: 01:00<br>PR: Actividad del tipo Clase de Problemas | | |
| 9 | **Clase de teoría: Impartición de contenidos**<br>Duración: 01:00<br>LM: Actividad del tipo Lección Magistral | **Resolución de Ejercicios**<br>Duración: 01:00<br>PR: Actividad del tipo Clase de Problemas | | **Examen Tema 1, 2, 3 (Ev. Continua) (RA85, RA143, RA195, RA197)**<br>EX: Técnica del tipo Examen Escrito<br>Evaluación continua<br>Duración: 02:00 |
| 10 | **Clase de teoría: Impartición de contenidos**<br>Duración: 01:00<br>LM: Actividad del tipo Lección Magistral | **Resolución de Ejercicios**<br>Duración: 01:00<br>PR: Actividad del tipo Clase de Problemas | | |

| | | | | |
|---|---|---|---|---|
| 11 | **Clase de teoría: Impartición de contenidos**<br>Duración: 01:00<br>LM: Actividad del tipo Lección Magistral | **Resolución de Ejercicios**<br>Duración: 01:00<br>PR: Actividad del tipo Clase de Problemas | | |
| 12 | **Clase de teoría: Impartición de contenidos**<br>Duración: 01:00<br>LM: Actividad del tipo Lección Magistral | **Resolución de Ejercicios**<br>Duración: 01:00<br>PR: Actividad del tipo Clase de Problemas | | **Competencia Transversal (R141))**<br>TG: Técnica del tipo Trabajo en Grupo<br>Evaluación continua<br>Duración: 00:00 |
| 13 | **Clase de teoría: Impartición de contenidos**<br>Duración: 01:00<br>LM: Actividad del tipo Lección Magistral | **Resolución de Ejercicios**<br>Duración: 01:00<br>PR: Actividad del tipo Clase de Problemas | | |
| 14 | **Clase de teoría: Impartición de contenidos**<br>Duración: 01:00<br>LM: Actividad del tipo Lección Magistral | **Resolución de Ejercicios**<br>Duración: 01:00<br>PR: Actividad del tipo Clase de Problemas | | |
| 15 | **Clase de teoría: Impartición de contenidos**<br>Duración: 02:00<br>LM: Actividad del tipo Lección Magistral | | | |
| 16 | **Clase de teoría: Impartición de contenidos**<br>Duración: 02:00<br>OT: Otras actividades formativas | | | |
| 17 | | | | **Examen Tema 4, 5, 6, 7 (Ev. Continua) (RA85, RA198, RA200,RA199, RA201)**<br>EX: Técnica del tipo Examen Escrito<br>Evaluación continua<br>Duración: 02:00<br><br>**Examen "Sólo prueba final" (RA85, RA118, RA143,RA195, RA197, RA198, RA199, RA200, RA201)**<br>EX: Técnica del tipo Examen Escrito<br>Evaluación sólo prueba final<br>Duración: 03:00<br><br>**Asistencia a clases**<br>OT: Otras técnicas evaluativas<br>Evaluación continua<br>Duración: 00:00 |

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 |
|---|---|---|---|---|---|---|---|
| 9 | Examen Tema 1, 2, 3 (Ev. Continua) (RA85, RA143, RA195, RA197) | EX: Técnica del tipo Examen Escrito | Presencial | 02:00 | 35% | 0 / 10 | CC1 |
| 12 | Competencia Transversal (R141)) | TG: Técnica del tipo Trabajo en Grupo | No Presencial | 00:00 | 10% | 5 / 10 | CT8 |
| 17 | Examen Tema 4, 5, 6, 7 (Ev. Continua) (RA85, RA198, RA200,RA199, RA201) | EX: Técnica del tipo Examen Escrito | Presencial | 02:00 | 50% | 5 / 10 | CC1 |
| 17 | Asistencia a clases | OT: Otras técnicas evaluativas | Presencial | 00:00 | 5% | 0 / 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" (RA85, RA118, RA143,RA195, RA197, RA198, RA199, RA200, RA201) | EX: Técnica del tipo Examen Escrito | Presencial | 03:00 | 100% | 5 / 10 | CC1<br>CT8 |

### 7.1.3. Evaluación convocatoria extraordinaria

| Descripción | Modalidad | Tipo | Duración | Peso en la nota | Nota mínima | Competencias evaluadas |
|---|---|---|---|---|---|---|
| Examen "Convocatoria Extraordinaria (RA85, RA118, RA143,RA195, RA197, RA198, RA199, RA200, RA201) | EX: Técnica del tipo Examen Escrito | Presencial | 03:00 | 100% | 5 / 10 | CC1<br>CT8 |

## 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, 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 por escrito al coordinador de la asignatura o bien responder 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 de cada asignatura si el alumno no comunica lo contrario por los medios anteriormente expuestos

### 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% | Durante todo el curso |
| TI: Técnica del tipo Trabajo Grupo | Realización de actividades relacionadas con la competencia Trabajo en equipo (CT_8) | 10% | Fecha publicada en la plataforma |
| | | | |

| | | | |
|---|---|---|---|
| EX: Técnica del tipo Examen Escrito | Evaluación de los temas 1, 2, 3 | 35% | Fecha proporcionada por Sub. Ord. Académica y Doctorado |
| EX: Técnica del tipo Examen Escrito | Evaluación del tema 4, 5, 6 y 7 | 50% | 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.

**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 9,0.. 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.

**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 9.0 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 extraordinaria.

# 8. Recursos didácticos

## 8.1. Recursos didácticos de la asignatura

| Nombre | Tipo | Observaciones |
|---|---|---|
| Fundamentos de Seguridad Tomo II | Bibliografía | Autenticación, hash, cifra asimétrica, cuaderno de prácticas |
| Fundamentos de Seguridad Tomo I | Bibliografía | Seguridad de la Información. Criptografia Clásica, Criptografía Moderna: Cifrado Simétrico. |
| Seguridad de la Información. Redes, informática y sistemas de información. Areitio, Javier. Paraninfo, 2008 | Bibliografía | Ampliación conocimientos |
| Criptografía Digital. Pastor, José; Sarasa, Miguel Angel. Colección Textos Docentes; Prensas Universitarias de Zaragoza | Bibliografía | Ampliación conocimientos |
| 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 (http://www.criptored.upm.es/paginas/software.htm) |
| Sitios web | Recursos web | Todas aquellos sitios web oficiales que estén relacionados con la materia impartida: Red Temática Iberoamericana de Criptografía y Seguridad de la Información Inteco, Agencia de Protección de Datos, Normas UNE (NorWeb), etc. |