ANX-PR/CL/001-02

GUÍA DE APRENDIZAJE

ASIGNATURA

Fundamentos de seguridad

CURSO ACADÉMICO - SEMESTRE

2015-16 - Segundo semestre

Datos Descriptivos

Nombre de la Asignatura	Fundamentos de seguridad
Titulación	61IW - Grado en Ingenieria del Software
Centro responsable de la titulación	E.T.S. de Ingenieria de Sistemas Informaticos
Semestre/s de impartición	Segundo semestre
Materia	Seguridad de la informacion
Carácter	Obligatoria
Código UPM	615000236
Nombre en inglés	Fundamentos de Seguridad

Datos Generales

Créditos	3	**Curso**	1
Curso Académico	2015-16	**Período de impartición**	Febrero-Junio
Idioma de impartición	Castellano	**Otros idiomas de impartición**	

Requisitos Previos Obligatorios

Asignaturas Superadas

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

Otros Requisitos

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

Conocimientos Previos

Asignaturas Previas Recomendadas

El coordinador de la asignatura no ha definido asignaturas previas recomendadas.

Otros Conocimientos Previos Recomendados

Aritmética modular

Algebra matricial

Competencias

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.

Resultados de Aprendizaje

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.

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.

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.

Profesorado

Profesorado

Nombre	Despacho	e-mail	Tutorías
Mahillo Garcia, Maria Angeles **(Coordinador/a)**	1110	mariaangeles.mahillo@upm.es	L - 13:00 - 15:00 M - 11:00 - 15:00 Los horarios de tutorías pueden variar en función de las necesidades de los alumnos a lo largo de la impartición de la asignatura
Camara Delgado, Mercedes De La	1109	mercedes.delacamara@upm.es	M - 15:00 - 16:00 X - 15:00 - 18:00 J - 18:00 - 20:00 Los horarios de tutorías pueden variar en función de las necesidades de los alumnos a lo largo de la impartición de la asignatura

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

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.

Temario

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.

Cronograma

Horas totales: 37 horas

Horas presenciales: 37 horas (47.4%)

Peso total de actividades de evaluación continua: 100%

Peso total de actividades de evaluación sólo prueba final: 100%

Semana	Actividad Prensencial en Aula	Actividad Prensencial en Laboratorio	Otra Actividad Presencial	Actividades Evaluación
Semana 1	**Clase de teoría: Impartición de contenidos** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
Semana 2	**Clase de teoría: Impartición de contenidos** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
Semana 3	**Clase de teoría: Impartición de contenidos** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
Semana 4	**Clase de teoría: Impartición de contenidos** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			**Competencia Transversal (R87)** Duración: 00:00 TI: Técnica del tipo Trabajo Individual Evaluación continua Actividad no presencial
Semana 5	**Clase de teoría: Impartición de contenidos** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			
Semana 6	**Clase de teoría: Impartición de contenidos** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			

Semana 7	**Clase de teoría: Impartición de contenidos** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			
Semana 8	**Clase de teoría: Impartición de contenidos** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			
Semana 9	**Clase de teoría: Impartición de contenidos** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			
Semana 10	**Clase de teoría: Impartición de contenidos** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			**Examen Tema 1 y 2 (Ev. Continua) (RA143, RA141, RA144)** Duración: 02:00 EX: Técnica del tipo Examen Escrito Evaluación continua Actividad presencial
Semana 11	**Clase de teoría: Impartición de contenidos** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			
Semana 12	**Clase de teoría: Impartición de contenidos** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			

Semana 13	**Clase de teoría: Impartición de contenidos** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			
Semana 14	**Clase de teoría: Impartición de contenidos** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			
Semana 15	**Clase de teoría: Impartición de contenidos** Duración: 01:30 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 00:30 PR: Actividad del tipo Clase de Problemas			
Semana 16	**Clase de teoría: Impartición de contenidos** Duración: 02:00 OT: Otras actividades formativas			
Semana 17				**Examen Tema 3 (Ev. Continua) (RA141, RA145, RA147, RA146)** Duración: 03:00 EX: Técnica del tipo Examen Escrito Evaluación continua Actividad presencial **Examen "Sólo prueba final" (RA87, RA141, RA143, RA144,,RA145, RA146, RA147)** Duración: 03:00 EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Actividad presencial **Asistencia a clases** Duración: 00:00 OT: Otras técnicas evaluativas Evaluación continua Actividad presencial

Nota.- El cronograma sigue una planificación teórica de la asignatura que puede sufrir modificaciones durante el curso.

Nota 2.- Para poder calcular correctamente la dedicación de un alumno, la duración de las actividades que se repiten en el tiempo (por ejemplo, subgrupos de prácticas") únicamente se indican la primera vez que se definen.

Actividades de Evaluación

Semana	Descripción	Duración	Tipo evaluación	Técnica evaluativa	Presencial	Peso	Nota mínima	Competencias evaluadas
4	Competencia Transversal (R87)	00:00	Evaluación continua	TI: Técnica del tipo Trabajo Individual	No	5%		CT5
10	Examen Tema 1 y 2 (Ev. Continua) (RA143, RA141, RA144)	02:00	Evaluación continua	EX: Técnica del tipo Examen Escrito	Sí	45%		CC1
17	Examen Tema 3 (Ev. Continua) (RA141, RA145, RA147, RA146)	03:00	Evaluación continua	EX: Técnica del tipo Examen Escrito	Sí	45%		CC1
17	Examen "Sólo prueba final" (RA87, RA141, RA143, RA144,,RA145, RA146, RA147)	03:00	Evaluación sólo prueba final	EX: Técnica del tipo Examen Escrito	Sí	100%	5 / 10	CT5, CC1
17	Asistencia a clases	00:00	Evaluación continua	OT: Otras técnicas evaluativas	Sí	5%		

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 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 20 de marzo de 2016.

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%	
TI: Técnica del tipo Trabajo Individual	Realización de actividades relacionadas con la competencia Planificación y Organización (CT_5)	5%	Semana 4. Fecha concreta 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.

Recursos Didácticos

Descripción	Tipo	Observaciones
Ramió Aguirre, Jorge. Seguridad Informática y Criptografía v 4.1 Dpto. de Publicaciones E.U.I., 2006 (edición impresa).	Bibliografía	Libro electrónico gratuito disponible en la página Web del autor. Aplicaciones Criptográficas. Segunda Edición)
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	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 Ramió y el Dr. Alfonso Muñoz

Otra Información

El equipo docente de la materia "Seguridad de la Información" de este plan de estudios (Dña.. Mercedes de la Cámara, Dña. María de los Angeles Mahillo y D. Jorge Ramió Aguirre) con el fin de ayudar a los alumnos a la preparación de la asignatura, elaborarán un cuaderno de ejercicios y/o prácticas con enunciado y solución para que ellos puedan seguir y desarrollar en aula dichos ejercicios prácticoso. 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.