ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

615000236 - Fundamentos de Seguridad

PLAN DE ESTUDIOS

61IW - Grado En Ingenieria Del Software

CURSO ACADÉMICO Y SEMESTRE

2019/20 - Segundo semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	615000236 - Fundamentos de Seguridad
No de créditos	3 ECTS
Carácter	Obligatoria
Curso	Primer curso
Semestre	Segundo semestre
Período de impartición	Febrero-Junio
Idioma de impartición	Castellano
Titulación	61IW - Grado En Ingenieria Del Software
Centro responsable de la titulación	61 - Escuela Tecnica Superior de Ingenieria de Sistemas Informaticos
Curso académico	2019-20

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Maria Angeles Mahillo Garcia (Coordinador/a)	1110	mariaangeles.mahillo@upm.es	L - 09:00 - 15:00 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.
Jorge Ramio Aguirre	1106	jorge.ramio@upm.es	L - 09:00 - 15:00 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 Ingenieria del Software no tiene definidas asignaturas previas recomendadas para esta asignatura.

3.2. Otros conocimientos previos recomendados para cursar la asignatura

- Aritmética modular

- Algebra matricial

4. Competencias y resultados de aprendizaje

4.1. 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.

4.2. Resultados del aprendizaje

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

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** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
2	**Clase de teoría: Impartición de contenidos** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
3	**Clase de teoría: Impartición de contenidos** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
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			
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			**Competencia Transversal** TI: Técnica del tipo Trabajo Individual Evaluación continua y sólo prueba final Duración: 00:00
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			
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			

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			
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			**Examen Tema 1 y 2 (Ev. Continua)** EX: Técnica del tipo Examen Escrito Evaluación continua Duración: 02:00
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			
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			
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			
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			

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			
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			
16	**Clase de teoría: Impartición de contenidos** Duración: 02:00 LM: Actividad del tipo Lección Magistral			
17				**Examen Tema 3 (Ev. Continua)** EX: Técnica del tipo Examen Escrito Evaluación continua Duración: 02:00 **Examen "Sólo prueba final"** EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Duración: 02:30

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
5	Competencia Transversal	TI: Técnica del tipo Trabajo Individual	No Presencial	00:00	5%	0 / 10	CT5
9	Examen Tema 1 y 2 (Ev. Continua)	EX: Técnica del tipo Examen Escrito	Presencial	02:00	45%	0 / 10	CC1
17	Examen Tema 3 (Ev. Continua)	EX: Técnica del tipo Examen Escrito	Presencial	02:00	50%	0 / 10	CC1

7.1.2. Evaluación sólo prueba final

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
5	Competencia Transversal	TI: Técnica del tipo Trabajo Individual	No Presencial	00:00	5%	0 / 10	CT5
17	Examen "Sólo prueba final"	EX: Técnica del tipo Examen Escrito	Presencial	02:30	95%	0 / 10	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 .	EX: Técnica del tipo Examen Escrito	Presencial	02:30	95%	0 / 10	CC1

7.2. Criterios de evaluación

1. ELECCIÓN DEL SISTEMA DE EVALUACIÓN

De acuerdo con 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 cada asignatura, la elección entre el sistema de evaluación continua o el sistema de evaluación mediante una prueba final corresponde al estudiante. El sistema de evaluación continua será el que se aplique en general a todos los estudiantes de cada asignatura. El estudiante que desee seguir el sistema de evaluación mediante sólo una prueba final, deberá comunicarlo por escrito al coordinador de la asignatura o, por delegación de este, a los profesores de la misma mediante el procedimiento, y en el plazo, que se fijen en la Guía de Aprendizaje de la asignatura o, si la Guía de Aprendizaje no lo fijase, según lo que determine la Jefatura de Estudios del Centro responsable de la titulación. En todo caso, el plazo que se fije para que el estudiante pueda realizar esta opción deberá ser, al menos, de dos semanas a contar desde el inicio de la actividad docente de la asignatura para dicho 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 la indicada en el cronograma facilitado a los alumnos al inicio del curso. La competencia transversal se evaluará durante la impartición de las clases independientemente de la modalidad de evaluación elegida, la calificación se sumará a las obtenidas en la evaluación de las demás actividades.

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 TI: Técnica del tipo Trabajo Individual (Competencia Transversal)

Descripción: Realización de actividades relacionadas con la competencia Planificación y Organización
Peso: 5%
Fecha: Semana 5. La fecha concreta se indicará en la plataforma de la asignatura
Resultados de aprendizaje evaluados: 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.

Técnica evaluativa: EX: Técnica del tipo Examen Escrito
Descripción: Evaluación de los temas 1 y 2
Peso: 45%
Fecha: Fecha proporcionada por Sub. Ord. Académica
Resultados de aprendizaje evaluados: Conoce los conceptos de la seguridad de la información y las razones que la definen como un proceso. Analiza, clasifica y aplica los algoritmos de cifra clásica. Conoce y aplica métodos y algoritmos matemáticos que se usarán en las implementaciones criptográficas.

Técnica evaluativa: EX: Técnica del tipo Examen Escrito
Descripción: Evaluación del tema 3.
Peso: 50%
Fecha: Fecha proporcionada por Sub. Ord. Académica
Resultados de aprendizaje evaluados: Identifica los elementos básicos de la criptografía simétrica distinguiendo la cifra en flujo y bloque. Conoce y aplica los principios de la cifra en flujo y los algoritmos A5 y RC4. Conoce y aplica los principios de la cifra en bloque y los algoritmos DES, TDES, y AES.

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 PRUEBA 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. A la nota del examen se le sumará la nota obtenida en la evaluación de la competencia transversal.

Técnica evaluativa TI: Técnica del tipo Trabajo Individual (Competencia Transversal)
Descripción: Realización de actividades relacionadas con la competencia Planificación y Organización

Peso: 5%

Fecha: Semana 5. La fecha concreta se indicará en la plataforma de la asignatura

Resultados de aprendizaje evaluados: 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.

Técnica evaluativa: EX: Técnica del tipo Examen Escrito

Descripción: Evaluación de los temas 1, 2 y 3

Peso: 95%

Fecha: Fecha proporcionada por Sub. Ord. Académica

Resultados de aprendizaje evaluados: Conoce los conceptos de la seguridad de la información y las razones que la definen como un proceso. Analiza, clasifica y aplica los algoritmos de cifra clásica. Conoce y aplica métodos y algoritmos matemáticos que se usarán en las implementaciones criptográficas. Identifica los elementos básicos de la criptografía simétrica distinguiendo la cifra en flujo y bloque. Conoce y aplica los principios de la cifra en flujo y los algoritmos A5 y RC4. Conoce y aplica los principios de la cifra en bloque y los algoritmos DES, TDES, y AES.

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

2.2. CONVOCATORIA EXTRAORDINARIA.

De acuerdo con 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. A la nota del examen se le sumará la nota obtenida en la evaluación de la competencia transversal.

Técnica evaluativa: EX: Técnica del tipo Examen Escrito

Descripción: Evaluación de los temas 1, 2 y 3

Peso: 95%

Fecha: Fecha proporcionada por Sub. Ord. Académica

Resultados de aprendizaje evaluados: Conoce los conceptos de la seguridad de la información y las razones que la definen como un proceso. Analiza, clasifica y aplica los algoritmos de cifra clásica. Conoce y aplica métodos y algoritmos matemáticos que se usarán en las implementaciones criptográficas. Identifica los elementos básicos de la criptografía simétrica distinguiendo la cifra en flujo y bloque. Conoce y aplica los principios de la cifra en flujo y los algoritmos A5 y RC4. Conoce y aplica los principios de la cifra en bloque y los algoritmos DES, TDES, y AES.

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 (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
Fundamentos de Seguridad Tomo I	Bibliografía	Introducción a la seguridad de la información. Cifra Clásica. Cifra Moderna Simétrica
Transparencia utilizadas en clase	Bibliografía	Conjunto de transparencias utilizadas por los profesores de la asignatura

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 prácticas de los temas 1, 2 y 3, para que sean resueltas con el software libre proporcionado por la asignatura.