ANX-PR/CL/001-01
GUÍA DE APRENDIZAJE

ASIGNATURA

615000224 - Fundamentos De Seguridad

PLAN DE ESTUDIOS

61CI - Grado En Ingenieria De Computadores

CURSO ACADÉMICO Y SEMESTRE

2023/24 - 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....3
6. Cronograma....6
7. Actividades y criterios de evaluación....9
8. Recursos didácticos....13
9. Otra información....14

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	615000224 - 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	61CI - Grado en Ingenieria de Computadores
Centro responsable de la titulación	61 - Escuela Tecnica Superior De Ingenieria De Sistemas Informaticos
Curso académico	2023-24

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Maria Angeles Mahillo Garcia (Coordinador/a)		mariaangeles.mahillo@upm.es	- -

* 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 de Computadores 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

RA156 - Conoce y aplica métodos y algoritmos matemáticos que se usarán en las implementaciones criptográficas.

RA154 - Conoce los conceptos de la seguridad de la información y las razones que la definen como un proceso.

RA88 - 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.

RA157 - Analiza, clasifica y aplica los algoritmos de cifra clásica.

RA165 - Conoce y aplica los principios de la cifra en flujo y los algoritmos A5 y RC4.

RA159 - Identifica los elementos básicos de la criptografía simétrica distinguiendo la cifra en flujo y bloque.

RA166 - 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 en aula	Actividad en laboratorio	Tele-enseñanza	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: 01:00 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 01:00 PR: Actividad del tipo Clase de Problemas			
5	**Clase de teoría: Impartición de contenidos** Duración: 01:00 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 01:00 PR: Actividad del tipo Clase de Problemas			**Competencia Transversal (Actividad obligatoria para el alumnado en tiempo y forma. No recuperable)** TI: Técnica del tipo Trabajo Individual Evaluación continua y sólo prueba final No presencial Duración: 00:00
6	**Clase de teoría: Impartición de contenidos** Duración: 01:00 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 01:00 PR: Actividad del tipo Clase de Problemas			
7	**Clase de teoría: Impartición de contenidos** Duración: 01:00 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 01:00 PR: Actividad del tipo Clase de Problemas			**Examen Tema 1 y 2 (Evaluación Progresiva)** EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 01:30

8	**Clase de teoría: Impartición de contenidos** Duración: 01:00 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 01:00 PR: Actividad del tipo Clase de Problemas			
9	**Clase de teoría: Impartición de contenidos** Duración: 01:00 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 01:00 PR: Actividad del tipo Clase de Problemas			
10	**Clase de teoría: Impartición de contenidos** Duración: 01:00 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 01:00 PR: Actividad del tipo Clase de Problemas			
11	**Clase de teoría: Impartición de contenidos** Duración: 01:00 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 01:00 PR: Actividad del tipo Clase de Problemas			
12	**Clase de teoría: Impartición de contenidos** Duración: 01:00 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 01:00 PR: Actividad del tipo Clase de Problemas			
13	**Clase de teoría: Impartición de contenidos** Duración: 01:00 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 01:00 PR: Actividad del tipo Clase de Problemas			

14	**Clase de teoría: Impartición de contenidos** Duración: 01:00 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 01:00 PR: Actividad del tipo Clase de Problemas			
15	**Clase de teoría: Impartición de contenidos** Duración: 01:00 LM: Actividad del tipo Lección Magistral **Clase de resolución de cuestiones y/o ejercicios** Duración: 01:00 PR: Actividad del tipo Clase de Problemas			
16				
17				**Examen Tema 3 (Evaluación Progresiva)** EX: Técnica del tipo Examen Escrito Evaluación continua Presencial Duración: 01:30 **Examen Tema 1, 2 (Recuperación)** EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Presencial Duración: 01:30 **Examen Tema 3 (Evaluación Global)** EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Presencial Duración: 01:30

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.

7. Actividades y criterios de evaluación

7.1. Actividades de evaluación de la asignatura

7.1.1. Evaluación (progresiva)

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
5	Competencia Transversal (Actividad obligatoria para el alumnado en tiempo y forma. No recuperable)	TI: Técnica del tipo Trabajo Individual	No Presencial	00:00	5%	0 / 10	CT5
7	Examen Tema 1 y 2 (Evaluación Progresiva)	EX: Técnica del tipo Examen Escrito	Presencial	01:30	45%	4 / 10	CC1
17	Examen Tema 3 (Evaluación Progresiva)	EX: Técnica del tipo Examen Escrito	Presencial	01:30	50%	0 / 10	CC1

7.1.2. Prueba evaluación global

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
5	Competencia Transversal (Actividad obligatoria para el alumnado en tiempo y forma. No recuperable)	TI: Técnica del tipo Trabajo Individual	No Presencial	00:00	5%	0 / 10	CT5
17	Examen Tema 1, 2 (Recuperación)	EX: Técnica del tipo Examen Escrito	Presencial	01:30	45%	0 / 10	CC1
17	Examen Tema 3 (Evaluación Global)	EX: Técnica del tipo Examen Escrito	Presencial	01:30	50%	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	03:00	95%	4.5 / 10	CC1

7.2. Criterios de evaluación

1. SISTEMA DE EVALUACIÓN

De acuerdo con la normativa reguladora de evaluación del aprendizaje en las titulaciones oficiales de grado y máster universitario de la universidad politécnica de Madrid, aprobada por Consejo de Gobierno en su sesión del 26 de mayo de 2022, el sistema de evaluación que contribuye a favorecer el aprendizaje del estudiante y el logro de los resultados de aprendizaje y la adquisición de las competencias correspondientes es el sistema de evaluación distribuida o progresiva.

La asignatura tiene tres partes diferenciadas:

- Competencia Transversal. Actividad de participación obligatoria de los estudiantes que no puede recuperarse.
- Temas 1 y 2. Actividad de evaluación de los estudiantes que puede recuperarse (se evalúa en el periodo de docencia).
- Tema 3. Actividad de participación de los estudiantes que no puede recuperarse (se evalúa al finalizar el periodo de docencia)

No obstante en determinadas circunstancias, que se indican en los apartados siguientes, el alumnado podrá recuperar parte de la asignatura (Temas 1 y 2) coN el sistema global.

2. CRITERIOS DE CALIFICACIÓN.

2.1. CONVOCATORIA ORDINARIA.

2.1.1 EVALUACIÓN DISTRIBUIDA O PROGRESIVA.

Los instrumentos que se van a utilizar en la evaluación del proceso de aprendizaje del alumnado en la evaluación progresiva se detallan a continuación:

Técnica evaluativa TI: Técnica del tipo Trabajo Individual (Competencia Transversal. Actividad obligatoria para el alumnado en tiempo y forma. No recuperable)

Descripción: Realización de actividades relacionadas con la competencia Planificación y Organización

Peso: 5%

Fecha: Semana 5 del periodo de docencia

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: Examen Tema 1, 2. (Si la nota es >= 4 los alumnos no deben presentarse a esta parte en la convocatoria ordinaria del mismo curso)

Peso: 45%

Fecha: Semana 8 del periodo de docencia

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 indicada por la Subdirección de Ordenación Académica y de Postgrado.

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 GLOBAL

Los alumnos que no hayan obtenido una calificación superior a 4 en la evaluación de los temas 1 y 2, tendrán la posibilidad de examinarse de la misma materia mediante un examen escrito, además de tener que examinarse del tema 3. En dichos exámenes 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. Actividad obligatoria para el alumnado en tiempo y forma. No recuperable)

Descripción: Realización de actividades relacionadas con la competencia Planificación y Organización

Peso: 5%

Fecha: Semana 5 del periodo de docencia

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 (Recuperación)
Peso: 45%
Fecha: Fecha indicada por la Subdirección de Ordenación Académica y de Postgrado.
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 indicada por la Subdirección de Ordenación Académica y de Postgrado.
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.

2.2. CONVOCATORIA EXTRAORDINARIA.

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 TI: Técnica del tipo Trabajo Individual (Competencia Transversal)
Descripción: Realización de actividades relacionadas con la competencia Planificación y Organización
Peso: 5%
Fecha: Semana 5
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 indicada por la Subdirección de Ordenación Académica y de Postgrado.

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

Actuación ante comportamientos fraudulentos (Artículo 13)

Los exámenes se realizarán a nivel personal. Si se detecta copia en una prueba de evaluación, se calificará con la puntuación de cero al estudiante o estudiantes implicados (la norma se aplicará por igual tanto a los que copian como a los que se dejan copia, es responsabilidad del alumnado la protección de su propia información)en la calificación final de la convocatoria correspondiente a la celebración de la prueba (ordinaria o extraordinaria). Además, en función de la gravedad del caso, el Tribunal de la asignatura podrá acordar la realización de un examen especial y equivalente para evaluar los resultados de aprendizaje de la asignatura en la siguiente convocatoria oficial. Si la comprobación de fraude académico se produce durante el desarrollo de la prueba, ésta se podrá interrumpir inmediatamente para el/la estudiante o estudiantes implicados/as, debiendo el profesor o profesora comunicar el porqué de la interrupción. El Tribunal de la Asignatura podrá poner los hechos en conocimiento del Director/a del Departamento, y éste a su vez podrá elevarlos al Rector/a para que pudiera abrirse, en su caso, expediente disciplinario.

Publicación de las soluciones (Articulo 19. Punto 9)

En todas las pruebas de evaluación, salvo que el tipo de prueba no lo permita, la solución de las preguntas de la misma se hará pública dentro de los dos días hábiles siguientes a la finalización de la prueba por la totalidad del estudiantado que deben realizarla, en la plataforma Moodle de la asignatura debiendo permanecer publicada durante siete días hábiles o hasta la fecha prevista para la revisión.

Estudiantes que no puedan realizar una prueba de evaluación en la fecha prevista (Artículo 21)

Cuando un/a estudiante, con anterioridad a una prueba de evaluación sepa de una causa justificada que le impida asistir en la fecha programada a los de exámenes hecho público en su momento, o no pueda asistir a una prueba de evaluación programada de por una causa sobrevenida podrá solicitar ser examinado de dicha prueba en fecha distinta a la programada. Para ello deberá consultar el artículo 21 de la normativa reguladora de evaluación del aprendizaje en las titulaciones oficiales de grado y máster universitario de la universidad politécnica de Madrid, aprobada por Consejo de Gobiermo en su sesión del 26 de mayo de 2022, para comprobar que la causa está justificada y presentar solicitud junto con la justificación:

- En el caso de tratarse de pruebas fuera del periodo oficial de exámenes, mediante correo electrónico dirigido al coordinador/a de la asignatura, quien propondrá, de acuerdo con el profesor o profesora responsable, una forma alternativa de evaluar los resultados de aprendizaje correspondientes a dicha prueba de evaluación, mediante correo electrónico dirigido al coordinador/a de la asignatura, quien propondrá, de acuerdo con el profesor o profesora responsable, una forma alternativa de evaluar los resultados de aprendizaje correspondientes a dicha prueba de evaluación.
- En el caso de tratarse de una prueba de evaluación del periodo oficial de exámenes de la convocatoria ordinaria

o extraordinario que permita dejar constancia de la solicitud, mediante correo electrónico dirigido al Jefe/a de Estudios, quíen comunicará a la coordinación de la asignatura la posibildad de realizar otra prueba de evaluación.

Adelanto de la convocatoria extraordinaria (Articulo 12.4)

Aunque es poco probable para esta asignatura, se recuerda que con carácter excepcional, un/a estudiante podrá solicitar adelantar a la convocatoria de enero la convocatoria extraordinaria de julio de las asignaturas de segundo semestre que tuviera pendientes, siempre y cuando cumpla los siguientes requisitos:

- Que el/la estudiante esté matriculado de todos los créditos pendientes para finalizar sus estudios.
- Que, para concluir sus estudios de grado, le queden como máximo dos asignaturas del 2º semestre, o una asignatura del 1er semestre y otra del 2º semestre (además del TFG o TFM en su caso, de no haberlo defendido aún), en las que haya estado matriculado al menos una vez en un curso académico anterior.