DATOS GENERALES DE LA ASIGNATURA

ASIGNATURA: Fundamentos de Seguridad Informática y Criptografía
PLAN DE ESTUDIOS: Grado en Ingeniería Informática (SGR-INFORM)
GRUPO: 2526-O1
CENTRO: Escuela Politécnica Superior
CARÁCTER DE LA ASIGNATURA: Obligatorio
ECTS: 6,0
CURSO: 3º
SEMESTRE: 2º Semestre
IDIOMA EN QUE SE IMPARTE:
Castellano, excepto las asignaturas de idiomas que se impartirán en el idioma correspondiente

DATOS DEL PROFESOR

NOMBRE Y APELLIDOS: RAÚL SERRANO GARCÍA
EMAIL: rserrano@uemc.es
TELÉFONO: 983 00 10 00

CV DOCENTE:
Máster Seguridad y Defensa. Universidad Antonio de Nebrija
Grado en Seguridad. Universidad Antonio de Nebrija

CV PROFESIONAL:
Administrador de sistemas e infraestructuras (Seguridad informática)

CV INVESTIGACIÓN:
Doctorando en Seguridad y Análisis de Riesgos y Conflictos. Universidad Antonio de Nebrija

DATOS ESPECÍFICOS DE LA ASIGNATURA

DESCRIPTOR DE LA ASIGNATURA:
La asignatura **Fundamentos de Seguridad y Criptografía** introduce los principios teóricos y prácticos necesarios para comprender y aplicar mecanismos de protección de la información en sistemas digitales. Se abordan los conceptos esenciales de seguridad informática, incluyendo confidencialidad, integridad, disponibilidad, autenticación y no repudio, así como los principales modelos de amenazas y vulnerabilidades en entornos computacionales.

En el ámbito criptográfico, el curso estudia los fundamentos matemáticos que sustentan los sistemas de cifrado, los algoritmos clásicos y modernos de criptografía simétrica y asimétrica, las funciones hash, las firmas digitales, la infraestructura de clave pública (PKI) y los protocolos criptográficos utilizados en redes y aplicaciones.

La asignatura combina contenidos teóricos con actividades prácticas orientadas al análisis, implementación básica y evaluación de mecanismos de seguridad. Se fomenta el pensamiento crítico frente a riesgos, ataques y vulnerabilidades, así como la aplicación de buenas prácticas en el diseño y uso seguro de sistemas de información.

Resultados de aprendizaje

Al finalizar la asignatura, el estudiante será capaz de:

- Comprender los principios fundamentales de la seguridad de la información.
- Identificar amenazas, vulnerabilidades y tipos de ataques comunes.
- Explicar el funcionamiento de los principales algoritmos criptográficos.
- Aplicar técnicas básicas de cifrado, firma digital y verificación de integridad.
- Analizar protocolos de seguridad en redes y aplicaciones.
- Evaluar riesgos y proponer medidas de protección adecuadas.

Contenidos generales

1. Introducción a la seguridad de la información
2. Criptografía clásica
3. Criptografía simétrica
4. Criptografía asimétrica
5. Funciones hash y firmas digitales
6. Infraestructura de clave pública (PKI)
7. Protocolos criptográficos y seguridad en redes
8. Gestión de riesgos y buenas prácticas de seguridad

CONTENIDOS DE LA ASIGNATURA:

1. **Introdución a la criptología**: Fundamentos
    1. Galois: Descripción
2. **Mecanismos para proporcionar confidencialidad a los mensajes**: Criptosistemas
    1. Flujo: Distribución
3. **Mecanismos para proporcionar integridad y autenticación de mensajes**: Infraestructuras
    1. Firma digital: Clave privada - pública
4. **Mecanismos para autenticar usuarios**: Autenticacion_OCW
    1. Bloques: Introducción

OBSERVACIONES CONTENIDO DE LA ASIGNATURA:

Aplicar la tecnología informática para proteger los sistemas, para que los ya recurrentes ataques que se están produciendo en todas las empresas para vulnerar nuestra seguridad.

RECURSOS DE APRENDIZAJE:

Los recursos de aprendizaje que se utilizarán en todas las asignaturas de la titulación (salvo las prácticas externas) para facilitar el proceso de enseñanza-aprendizaje, son:

- Campus online de la UEMC (Open Campus)
- Plataforma de Webconference (Zoom work place)

Las comunicaciones con el profesor serán a través de Open Campus vía Mi correo, Tablón o/y Foro.

COMPETENCIAS Y RESULTADOS DE APRENDIZAJE A ADQUIRIR POR EL ALUMNO

COMPETENCIAS GENERALES:

- CG02. Capacidad y habilidad para la toma de decisiones en el ámbito tecnológico

COMPETENCIAS ESPECÍFICAS:

- CI1. 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
- ICO6. Capacidad para comprender, aplicar y gestionar la garantía y seguridad de los sistemas informáticos
- SI2. Capacidad para determinar los requisitos de los sistemas de información y comunicación de una organización atendiendo a aspectos de seguridad y cumplimiento de la normativa y la legislación vigente

RESULTADOS DE APRENDIZAJE:

El alumno será capaz de:

- Demostrar conocimiento de las principales técnicas de criptografía y su aplicación a los sistemas informáticos.
- Redactar informes de evaluaciones de los riesgos de los sistemas informáticos y elaboración de políticas de seguridad genéricas y especificadas para las distintas organizaciones.

BIBLIOGRAFÍA Y RECURSOS DE REFERENCIA GENERALES

BIBLIOGRAFÍA BÁSICA:

- William Stallings (2022): Cryptography and Network Security: Principles and Practice. Pearson . ISBN: 978-1-292-43748-4

BIBLIOGRAFÍA COMPLEMENTARIA:

- Alfred J. Menezes, Paul C. van Oorschot y Scott A. Vanstone. (1997 (primera edición).): Handbook of Applied Cryptography. CRC Press.. ISBN: ISBN-13: 978-0-8493-8523-0.

WEBS DE REFERENCIA:

Web / Descripcion

Pearson(https://www.pearson.com/store/p/cryptography-and-network-security-principles-and-practice/p200000003477/9780136707226)
Criptografía y seguridad de redes

PLANIFICACIÓN DEL PROCESO DE ENSEÑANZA-APRENDIZAJE DE LA ASIGNATURA

METODOLOGÍAS:

MÉTODO DIDÁCTICO:

El papel del profesor cobra importancia a través de la impartición de clases magistrales en tiempo real por videoconferencia que podrá utilizar para explicar los contenidos teóricos, resolver dudas que se planteen durante la sesión, ofrecer retroalimentación sobre las actividades de evaluación continua o realizar sesiones de tutoría de carácter grupal.

MÉTODO DIALÉCTICO:

Se caracteriza por la participación de los alumnos en las actividades de evaluación continua de debate y la intervención de éstos a través del diálogo y de la discusión crítica (seminarios, grupos de trabajo, etc.). Utilizando este método el alumno adquiere conocimiento mediante la confrontación de opiniones y puntos de vista. El papel del profesor consiste en proponer a través de Open Campus temas referidos a la materia objeto de estudio que son sometidos a debate para, posteriormente, evaluar el grado de comprensión que han alcanzado los alumnos.

MÉTODO HEURÍSTICO:

Este método puede desarrollarse de forma individual o en grupo a través de las actividades de evaluación continua (entregas de trabajos, resolución de ejercicios, presentaciones, etc.). El objetivo es que el alumno asuma un papel activo en el proceso de aprendizaje adquiriendo los conocimientos mediante la experimentación y la resolución de problemas.

CONSIDERACIONES DE LA PLANIFICACIÓN:

Las ACTIVIDADES FORMATIVAS que se realizan en la asignatura son las siguientes:

Clases teóricas: Actividad dirigida por el profesor que se desarrollará de forma sincrónica en grupo. Para la realización de esta actividad en OpenCampus, la UEMC dispone de herramientas de Webconference que permiten una comunicación unidireccional en las que el docente puede desarrollar sesiones en tiempo real con posibilidad de ser grabadas para ser emitidas en diferido.

Actividades prácticas: Actividades supervisadas por el profesor que se desarrollarán fundamentalmente de forma asíncrona, y de forma individual o en grupo:

- Actividades de debate. Se trata de actividades desarrolladas en el foro de Open Campus, en las que se genera conocimiento mediante la participación de los estudiantes en discusiones alrededor de temas de interés en las distintas asignaturas.
- Entregas de trabajos individuales o en grupo a partir de un enunciado o unas pautas de trabajo que establecerá el profesor.
- Resolución de ejercicios y problemas que el alumno debe realizar a través de Open Campus en un periodo de tiempo determinado. Esta actividad puede ser en formato test de evaluación.

Tutorías: Las tutorías podrán tener un carácter sincrónico o asíncrono y podrán desarrollarse de manera individual o en grupos reducidos.

Están previstas tres sesiones de tutoría por videoconferencia, una al inicio, otra antes de la evaluación parcial y otra al final del semestre. En la primera se presentará la asignatura y la guía docente y en la segunda, en las semanas previas a la evaluación final, se dedicará a la resolución de dudas de los estudiantes.

Además, el docente utiliza el Tablón, el Foro y el Sistema de correo interno de Open Campus para atender las necesidades y dudas académicas de los estudiantes.

SESIONES EN TIEMPO REAL

En la asignatura se planifican clases magistrales y tutorías a través de videoconferencias.

La asistencia a las videoconferencias no será obligatoria, pero si recomendable para un adecuado seguimiento de la asignatura, la comprensión de los materiales y el desarrollo óptimo de las actividades de aprendizaje. En cualquier caso, salvo circunstancias excepcionales, será posible acceder a ellas en diferido a las 48 horas máximo desde su celebración.

SESIONES EN TIEMPO REAL :

	Título
TU1	Presentación asignatura y Guía docente
CM1	Introducción a la seguridad y a la criptografía
CM2	Teoría de números, teoría de la información, complejidad algorítmica
CM3	Fundamentos e historia de la criptografía
CM4	Introducción a la criptografía moderna
CM5	tutoría intermedia de resolución de dudas
CM6	Criptografía simétrica

	Título
CM7	Criptografía asimétrica
CM8	Autenticación
TU2	Resolución de dudas antes de la evaluación

EVALUACIÓN CONVOCATORIA ORDINARIA:

Evaluación continua 60%
Evaluación final 40%

ACTIVIDADES Y SISTEMAS DE EVALUACIÓN :

Tipo Evaluación	Nombre Actividad	% Calif.
Evaluacion contínua (60 %)	1. Actividad 1 (Entrega individual)	18
	2. Defensa actividad 1 (Defensa)	12
	3. Actividad 3 (Entrega individual)	18
	4. Defensa actividad 3 (Defensa)	12
Evaluacion final (40 %)	1. Prueba de evaluación final (Prueba de evaluación final)	40

CONSIDERACIONES EVALUACIÓN CONVOCATORIA ORDINARIA:

A lo largo de la planificación de la asignatura el alumno realizará **actividades de evaluación continua** que forman parte de la calificación de la asignatura con un peso del 60% sobre la nota final.

Para superar la evaluación continua, el alumno deberá obtener al menos un 5 en la nota total de la evaluación continua, de lo contrario, deberá acudir a la convocatoria extraordinaria para superarla. Si una pareja de actividades (entrega individual o foro de debate y su defensa) tiene una nota de 5 o superior en la convocatoria ordinaria, dicha nota se conservará en la convocatoria extraordinaria, no pudiéndose volver a entregar por el estudiante. No se guardan notas de parejas de actividades suspensas.

El sistema de evaluación de esta asignatura acentúa el desarrollo gradual de competencias y resultados de aprendizaje y, por tanto, se realizará una evaluación continua a través de las distintas actividades de evaluación propuestas. El resultado de la evaluación continua se calcula a partir de las notas obtenidas en cada actividad teniendo en cuenta el porcentaje de representatividad en cada caso.

Todas las actividades deberán entregarse en las fechas previstas para ello, teniendo en cuenta:

- Las actividades de evaluación continua se desarrollarán según se indica y, para ser evaluadas, los trabajos deberán ser entregados en la forma y fecha prevista y con la extensión máxima señalada. No se evaluarán actividades entregadas posteriormente a esta fecha o que no cumplan con los criterios establecidos por el profesor.
- La no entrega de una actividad de evaluación continua en forma y plazo se calificará con un 0 y así computarán en el cálculo de la nota de evaluación continua y final de la asignatura.
- Cualquier tipo de copia o plagio por mínimo que sea, así como un uso inapropiado de herramientas de inteligencia artificial, supondrá una calificación de 0 en la actividad correspondiente. Esta actuación podría suponer la apertura de un expediente disciplinario.
- Las actividades de evaluación continua se desarrollarán con anterioridad a la realización de las pruebas de

evaluación final de la asignatura
- Si la asignatura tuviera actividad de laboratorio presencial, su asistencia será obligatoria para superar la asignatura

Los alumnos accederán a través de Open Campus a las calificaciones de las actividades de evaluación continua en un plazo aproximado de 20 días lectivos desde la fecha fin de fecha de entrega, excepto causas de fuerza mayor en cuyo caso se informará al alumno a través del Tablón.

La evaluación continua se complementará con una **evaluación final** que se realizará al finalizar el periodo lectivo en cada asignatura. La prueba constará de parte práctica y teórica, suponiendo un 40% de la calificación sobre la nota final.

La evaluación final de la asignatura se desarrollará del siguiente modo:

- A mitad de cada semestre se ofrece al a alumno el poder realizar de forma voluntaria un parcial para eliminar materia.
- Para eliminar la materia es necesario que el alumno lo supere al menos con un 5. En este caso, se le guardaría la nota del parcial hasta la convocatoria extraordinaria. El alumno sólo podrá presentarse a la segunda parte de la asignatura bien en convocatoria ordinaria o extraordinaria.
- En convocatoria ordinaria, la prueba final constará de dos exámenes (primera y segunda parte de la asignatura)
  - En el caso de que el alumno hubiera superado y eliminado materia con el primer parcial, sólo se presentará a la segunda parte. Para superar la asignatura se hará la media siempre que en la segunda parte se obtenga al menos un 4 y la media supere el 5.
  - En el caso de que el alumno no hubiera superado el primer parcial, se podrá presentar a ambas partes. Para superar la asignatura se hará la media de ambas partes siempre que se obtenga al menos un 4 en cada una y la media supere el 5.
- El alumno tendrá la posibilidad, siempre dentro de los tres días siguientes a la publicación de las notas, a renunciar a su calificación, y presentarse en la siguiente convocatoria
- El alumno tendrá hasta 3 días después de la calificación para solicitar al docente más información sobre su calificación por el correo de la plataforma.
- Cualquier tipo de irregularidad o fraude en la realización de una prueba, así como un uso inapropiado de herramientas de inteligencia artificial, supondrá una calificación de 0 en la prueba/convocatoria correspondiente. Esta actuación podría suponer la apertura de un expediente disciplinario.
- El aplazamiento concedido por la Universidad para la realización de una evaluación final se regirá por lo establecido en el Manual de "Directrices y plazos para la tramitación de una solicitud"

La nota final se corresponderá con la media aritmética del resultado obtenido en cada una de las partes. En caso de no superación, se guarda la parte aprobada para la convocatoria extraordinaria.

La **nota global** de la asignatura se obtiene ponderando la calificación de la evaluación continua y de la evaluación final según los siguientes porcentajes, y debiendo tener aprobadas ambas partes, continua y final, para superar la asignatura.

Si un alumno no se presenta a la prueba de evaluación final, su calificación en la convocatoria será de “No presentado”, con independencia de que haya realizado alguna actividad de evaluación continua.

De igual modo si el alumno no entrega ninguna actividad de evaluación continua, obtendrá la calificación de “No presentado”, con independencia de que haya aprobado la prueba de evaluación final, en cuyo caso, se le guardaría su calificación para la convocatoria extraordinaria

EVALUACIÓN CONVOCATORIA EXTRAORDINARIA:

Evaluación continua	60%
Evaluación final	40%

ACTIVIDADES Y SISTEMAS DE EVALUACIÓN :

Tipo Evaluación	Nombre Actividad	% Calif.
Evaluacion contínua (60 %)	1. Actividad 1 (Entrega individual)	18
	2. Defensa actividad 1 (Defensa)	12
	3. Actividad 3 (Entrega individual)	18
	4. Defensa actividad 3 (Defensa)	12
Evaluacion final (40 %)	1. Prueba de evaluación final (Prueba de evaluación final)	40

CONSIDERACIONES EVALUACIÓN CONVOCATORIA EXTRAORDINARIA:
Los estudiantes que no hayan superado la asignatura en la convocatoria ordinaria, porque hayan suspendido la evaluación continua o la prueba de evaluación final, podrán presentarse a las pruebas establecidas por el profesor en la convocatoria extraordinaria.

Para la convocatoria extraordinaria se guardan las calificaciones de las parejas de actividades de evaluación continua y pruebas de evaluación (parcial y final), superadas por el estudiante (nota superior o igual a 5), no permitiéndose volver a realizarlas.

- En convocatoria extraordinaria, la prueba final también constará de dos exámenes (primera y segunda parte de la asignatura)
  - En el caso de que el alumno hubiera superado el parcial (al menos un 5) o una de las partes en convocatoria ordinaria (al menos un 5), esta calificación se mantiene para la extraordinaria, presentándose el alumno sólo a lo suspenso. Para superar la asignatura se hará la media entre lo aprobado en ordinaria y la calificación que haya sacado en extraordinaria siempre que se obtenga al menos un 4 y la media supere el 5.
  - En el caso de que el alumno tuviera que presentarse a ambas partes, para superar la asignatura se hará la media siempre que se obtenga al menos un 4 en cada parte y la media supere el 5.
- En convocatoria extraordinaria, el alumno solo podrá entregar las parejas de actividades de evaluación continua no superadas, guardándose la calificación de las aprobadas.
- El alumno tendrá hasta 3 días después de la calificación para solicitar al docente más información sobre su calificación por el correo de la plataforma.
- Cualquier tipo de irregularidad o fraude en la realización de una prueba, supondrá una calificación de 0 en la prueba/convocatoria correspondiente.
- El aplazamiento concedido por la Universidad para la realización de una evaluación final se regirá por lo establecido en el Manual de "Directrices y plazos para la tramitación de una solicitud".

En la convocatoria extraordinaria, la **nota global** de la asignatura se obtiene ponderando la calificación de la evaluación continua y de la evaluación final, de la misma forma que en la convocatoria ordinaria.

Al igual que en la convocatoria ordinaria, en la convocatoria extraordinaria es necesario superar tanto la evaluación continua como la evaluación final para aprobar la asignatura.

Si un alumno no se presenta a la prueba de evaluación final, su calificación en la convocatoria será de “No presentado”, con independencia de que haya realizado alguna actividad de evaluación continua.

SISTEMAS DE EVALUACIÓN:

SISTEMA DE EVALUACIÓN	PORCENTAJE (%)
Ejecución de prácticas	52,4%
Pruebas escritas	38%
Pruebas orales	9,6%