Universidad Europea del Atlántico

GUÍA DOCENTE 2024-2025

DATOS GENERALES DE LA ASIGNATURA

ASIGNATURA:	Seguridad Informática y criptografía
PLAN DE ESTUDIOS:	Grado en Ingeniería Informática
FACULTAD:	Escuela Politécnica Superior
CARÁCTER DE LA ASIGNATURA:	Básica
ECTS:	6
CURSO:	Tercero
SEMESTRE:	Segundo
IDIOMA EN QUE SE IMPARTE:	Español
PROFESORADO:	Fco. Javier Bel Blesa
DIRECCIÓN DE CORREO ELECTRÓNICO:	Javier.bel@uneatlantico.es

DATOS ESPECÍFICOS DE LA ASIGNATURA

REQUISITOS PREVIOS:
No aplica
CONTENIDOS:
1. FUNDAMENTOS DE LA SEGURIDAD INFORMATICA. 1.1. INTRODUCCIÓN. 1.2. LA NECESIDAD DE APLICAR MECANISMOS DE SEGURIDAD. 1.3. ELEMENTOS A PROTEGER. 1.4. DEFINICIONES. 1.5. ESTRUCTURAS BÁSICAS DE SEGURIDAD INFORMÁTICA.

1.6. SEGURIDAD PASIVA
1.7. SEGURIDAD ACTIVA.
1.8. HACKERS, TIPOS DE HACKERS.
1.9. RECONOCIMIENTO DE AMENAZAS. CONTRAMEDIDAS.
1.10. BUENAS PRÁCTICAS.
2. CRIPTOGRAFIA.CRIPTOGRAFIA DE CLAVE SECRETA.
2.1. INTRODUCCIÓN.
2.2. CRIPTOGRAFÍA.
2.3. CRIPTOGRAFÍA SIMÉTRICA O DE CLAVE SECRETA.
2.4. ALGORITMOS PARA LA CRIPTOGRAFÍA SIMETRICA DE BLOQUE.
3. CRIPTOGRAFIA.CRIPTOSOSTEMAS SIMETRICOS DE CIFRADO EN FLUJO.
3.1. INTRODUCCIÓN.
3.2. ALGORITMOS PARA LA CRIPTOGRAFÍA SIMETRICA DE FLUJO.
4. CRIPTOGRAFIA.CRIPTOSOSTEMAS DE CLAVE PÚBLICA.
4.1. INTRODUCCIÓN.
4.2. APLICACIONES PRINCIPALES DE LA CRIPTOGRAFÍA DE CLAVE PÚBLICA.
4.3. ALGORITMOS DE CLAVE PÚBLICA
5. FUNCIONES DE AUTENTICACION E INTEGRIDAD.
5.1. INTRODUCCIÓN.
5.2. MÉTODOS Y FACTORES DE AUTENTICACION
5.3. INTEGRIDAD. FUNCIONES HASH O RESUMEN.
6. FIRMA DIGITAL Y CERTIFICADOS DIGITALES.
6.1. INTRODUCCIÓN.
6.2. FIRMA DIGITALIZADA Y FIRMA ELECTRÓNICA
6.3. FIRMA DIGITAL.
6.4. CERTIFICADOS DIGITALES.
6.5. TIPOS DE CERTIFICADOS.
6.6. EJEMPLO DE PKI. El DNI Electrónico (DNIe)
7. APLICACIONES SEGURAS.
7.1. INTRODUCCIÓN.
7.2. IDENTIFICACIÓN DE LOS REQUISITOS DE SEGURIDAD.
7.3. HITOS EN LA SEGURIDAD DEL SOFTWARE
7.4. ERRORES FRECUENTES DE CODIFICACIÓN
7.5. APLICACIONES WEB
7.6. SOLUCIONES POSIBLES AL CONTROL DE APLICACIONES
8. ACRONIMOS
9. BIBLIOGRAFIA

COMPETENCIAS

COMPETENCIAS GENERALES:

Que los estudiantes sean capaces de:

- Capacidad para concebir y desarrollar sistemas o arquitecturas criptográficas.

- Capacidad de desarrollar y establecer un Sistema de Gestión de Seguridad de la Información (SGSI).
- Capacidad para detectar intrusiones en la seguridad, y aplicar alguno de los algoritmos criptográficos para solventar estos problemas.
- Que los estudiantes hayan demostrado poseer y comprender conocimientos tanto en el entorno de la necesidad y aplicación de la Seguridad Informática como en los medios para garantizar esta seguridad.
- Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio.
- Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.
- Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado, sobre todo en la importancia de la aplicación de sistemas de seguridad en el ámbito tecnológico.
- Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía

COMPETENCIAS ESPECÍFICAS:

Que los estudiantes sean capaces de:

- Capacidad de explicar y aplicar los procedimientos de aplicación de medidas de seguridad informática básicas en los sistemas de información, con capacidad de identificar futuros problemas y diseñar soluciones a los mismos.
- Capacidad de entender y utilizar de forma eficiente los algoritmos y sistemas de encriptación más adecuados a la resolución de un problema en concreto.
- Capacidad para analizar, diseñar, construir y mantener sistemas de seguridad informática de forma robusta, segura y eficiente, eligiendo las estrategias de definición de seguridad y algoritmos de criptografía más adecuados.

COMPETENCIAS PROPIAS DE LA ASIGNATURA:

No aplica

RESULTADOS DE APRENDIZAJE:

En esta asignatura se espera que los alumnos alcancen los siguientes resultados de aprendizaje:

- Conocer los principales algoritmos de encriptación y sus vulnerabilidades para resolución de problemas comunes.
- Reconocer y paliar o evitar posibles ataques o intrusiones a los sistemas informáticos.

- Comprender y saber utilizar eficientemente los distintos modelos de implantación de la Seguridad Informática (los Sistemas de Gestión de Seguridad de la Información).

METODOLOGÍAS DOCENTES Y ACTIVIDADES FORMATIVAS

METODOLOGÍAS DOCENTES:

En esta asignatura se ponen en práctica diferentes metodologías docentes con el objetivo de que los alumnos puedan obtener los resultados de aprendizaje definidos anteriormente:

- MD2 - Estudio y análisis de casos.
- MD7 - Trabajo autónomo

ACTIVIDADES FORMATIVAS:

A partir de las metodologías docentes especificadas anteriormente, en esta asignatura, el alumno participará en las siguientes actividades formativas:

Actividades formativas		Horas
Actividades autónomas	Preparación de clases	15,0
	Estudio personal y lecturas	37,5
	Elaboración de trabajos	30,0
	Trabajo en campus virtual	7,5
Actividades dirigidas	Clases expositivas	15,0
	Clases prácticas	18,8
	Seminarios y talleres	11,3
Actividades de Evaluación	Actividades de Evaluación	7,5
Actividades supervisadas	Supervisión de actividades	3,8
	Tutorías (individual / en grupo)	3,8
	Prácticas externas	0,0
	Trabajo final de grado	0,0

El primer día de clase, el profesor proporcionará información más detallada al respecto.

SISTEMA DE EVALUACIÓN

CONVOCATORIA ORDINARIA:

En la convocatoria ordinaria de esta asignatura se aplican los siguientes instrumentos de evaluación:

Actividades de evaluación		Ponderación
Evaluación continua	Un examen Parcial	25 %
	Entrega de portfolios y ejercicios	20 %
	Interés y participación del alumno en la asignatura	5 %
Evaluación final	Ejercicio de programación que será entregado el día anterior a la prueba escrita teórico-práctica de la convocatoria ordinaria.	15 %
	Prueba escrita teórico-práctica.	35%

La calificación de la prueba escrita teórico-práctica de la convocatoria ordinaria **no podrá ser inferior, en ningún caso, a 4,0 puntos** (escala 0 a 10) para aprobar la asignatura y consecuentemente poder realizar el cálculo de porcentajes en la calificación final.

CONVOCATORIA EXTRAORDINARIA:

La convocatoria extraordinaria tendrá lugar durante el mes de julio (consúltese el calendario académico fijado por la universidad). Esta consistirá en la realización de una prueba teórico-práctica con un valor del 50 % de la nota final de la asignatura. En el caso de acudir a la convocatoria extraordinaria, **la nota obtenida en el ejercicio de programación de la convocatoria ordinaria no será tenida en cuenta**. La prueba teórico-práctica de la convocatoria extraordinaria será equivalente al 50% de la evaluación final de la convocatoria ordinaria.

El resto de la nota se complementará con la calificación obtenida en la evaluación continua de la convocatoria ordinaria.

La calificación de la prueba escrita teórico-práctica de la convocatoria ordinaria **no podrá ser inferior, en ningún caso, a 4,0 puntos** (escala 0 a 10) para aprobar la asignatura y consecuentemente poder realizar el cálculo de porcentajes en la calificación final.

BIBLIOGRAFÍA Y RECURSOS DE REFERENCIA GENERALES

BIBLIOGRAFÍA BÁSICA:

Las siguientes referencias son de consulta obligatoria:

1. Técnicas criptográficas de protección de datos, 3ª edición", Fuster Sabater, A., De la Guía, D., Hernández L., Montoya F,
Editor: Ra-Ma; Edición: 3rd edicion. (2004)

ISBN-10: 8478975942

ISBN-13: 9788478975945

2. Seguridad Informática. Roa, J.F.,
Editor: Mc. Graw Hill. 2013

ISBN-10: 8448183967

ISBN-13: 9788448171377

BIBLIOGRAFÍA COMPLEMENTARIA:

1. Empire: Hacking avanzado en el Red Team, 1ª edición, Castro, S., González, P.

Editor: ZeroXword Computing

ISBN-13: 978-84-09-14088-6

2. Hacking web technologies, 2ª edición revisada y ampliada, Rando, E., Gonzalez, P., Aparicio, A., Martín, R., Alonso, C.

Editor: ZeroXword Computing

ISBN-13: 978-84-697-7701-5

WEBS DE REFERENCIA:

OTRAS FUENTES DE CONSULTA: