



GUÍA DOCENTE

INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA

GRADO EN INGENIERÍA DEL SOFTWARE

MODALIDAD: PRESENCIAL

CURSO ACADÉMICO: 2023-2024

Denominación de la asignatura:	Introducción a la Seguridad Informática
Titulación:	Ingeniería del Software
Facultad o Centro:	Centro Universitario de Tecnología y Arte Digital
Materia:	Ciberseguridad
Curso:	3º
Cuatrimestre:	1
Carácter:	OBM
Créditos ECTS:	6
Modalidad/es de enseñanza:	Presencial
Idioma:	Castellano
Profesor/a - email	Eduardo Arriols Nuñez / eduardo.arriols@u-tad.com
Página Web:	http://www.u-tad.com/

DESCRIPCIÓN DE LA ASIGNATURA

Descripción de la materia

Esta materia incluye los conocimientos y las competencias de la seguridad informática que requeriría un profesional de nivel de graduado. Se dedica al estudio de la protección de la infraestructura computacional y todo lo relacionado con esta y, especialm

Descripción de la asignatura

Esta asignatura pretender servir como introducción general al mundo de la seguridad informática, mostrando los principios básicos, las amenazas actuales, ataques que han sido desarrollados, técnicas de ataque y auditoría, algoritmos criptográficos y sistemas de seguridad, etcétera. Se profundizará en las técnicas básicas que permitan desarrollar auditorías de seguridad y análisis de riesgos, necesarios para poder enfocar cualquier acción posterior de auditoria o bastionado

COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

Competencias (genéricas, específicas y transversales)

COMPETENCIAS BÁSICAS Y GENERALRES

CB1: Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio.

CB2: 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.

CB3: 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.

CB4: Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.

CB5: Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía

CG1 - Capacidad para entender, planificar y resolver problemas a través del desarrollo de soluciones informáticas.

CG2 - Desarrollo de soluciones informáticas respetuosas con el medio ambiente, los deberes sociales y los recursos naturales, además de cumplir con la legislación y la ética

CG3 - Conocimiento de los fundamentos científicos aplicables a la resolución de problemas informáticos

CG4 - Capacidad para simplificar y optimizar los sistemas informáticos atendiendo a la comprensión de su complejidad

CG9 - Capacidad para aprender, modificar y producir nuevas tecnologías informáticas

CG10 - Uso de técnicas creativas para la realización de proyectos informáticos

CG11 - Capacidad de buscar, analizar y gestionar la información para poder extraer conocimiento de la misma

COMPETIENCIAS ESPECIFICAS

CE10 - Capacidad para manejar un gestor de versiones de código y generar la documentación de una aplicación de forma automática.

COMPETENCIAS TRANSVERSALES

CT1 - Conocimiento de la definición, el alcance y la puesta en práctica de los fundamentos de las metodologías de gestión de proyectos de desarrollo tecnológico

CT2 - Conocimiento de los principales agentes del sector y del ciclo de vida completo de un proyecto de desarrollo y comercialización de contenidos digitales

CT4 - Capacidad de actualización del conocimiento adquirido en el manejo de herramientas y tecnologías digitales en función del estado actual del sector y de las tecnologías empleadas

CT5 - Desarrollo de las habilidades necesarias para el emprendimiento digital.

Resultados de aprendizaje

Al acabar la titulación, el graduado o graduada será capaz de:

- Entender qué son las ciber amenazas, cuál es su origen, qué buscan y cómo podemos identificarlas.
- Ser capaz de identificar las amenazas y vulnerabilidades de ciberseguridad de un sistema informático concreto, compuesto por elementos diversos de
 - hardware y software.
- Entender y aplicar los principios de la criptografía aplicada a la ciberseguridad.
- Conocer las herramientas y técnicas de auditoría forense.
- Conocer el entorno legal y de protección de datos en las aplicaciones de ciberseguridad
- Conocer experiencias documentadas de ciberataques y las contramedidas recomendadas-
- Entender los conceptos red team, blue team y estudiar su aplicación en escenarios concretos.
- Conocer los elementos y las buenas prácticas descritos en la familia de normas ISA/IEC -62443 e ISO/IEC-27000.
- Conocer y aplicar las técnicas para bastionar los sistemas ante ciberataques, usando detectores de intrusión y monitores.
- Aplicar conceptos de ciberseguridad para diseñar el hardware, la red de comunicaciones y el software de los sistemas en producción.
- Conocer las técnicas de análisis del malware.
- Ser capaz de desensamblar un código malicioso e identificar su origen
- Concebir, desarrollar y desplegar un proyecto de ciberseguridad integral para un sistema distribuid- o

CONTENIDO

Introducción a la seguridad informática

Fundamentos de criptografía

Normativa y cumplimiento legal

Auditoría y gestión de la seguridad

Principios para la seguridad en sistemas, aplicaciones web y redes

Desarrollo de software seguro

TEMARIO

Tema 1: Introducción

1. Amenazas actuales
2. Definiciones básicas
3. Reconocimiento de un ataque
4. Anonimato en red

Tema 2: Dispositivos y sistemas de seguridad

1. En red
2. En sistemas
3. En organizaciones
4. Herramientas avanzadas

Tema 3: Análisis de riesgos y cumplimiento

1. Análisis de riesgo tradicional
2. Principales leyes y normativas
3. Sistemas modernos de evaluación

Tema 4: Criptografía y Esteganografía

1. Esteganografía
2. Cifrado simétrico y asimétrico
3. Funciones hash y firma digital
4. Protección de datos

Tema 5: Fundamentos del hacking en sistemas

1. Búsqueda de información
2. Enumeración de servicios
3. Análisis de vulnerabilidades
4. Explotación de vulnerabilidades
5. Post-explotación e intrusión

Tema 6: Fundamentos del hacking en aplicaciones

1. Metodología OWASP
2. Herramientas básicas
3. Mapeo de una aplicación

4. Principales vulnerabilidades web
5. Auditoría de seguridad en aplicaciones móviles
6. Auditoría de seguridad en entornos REST/API

Tema 7: Fundamentos del hacking en redes

1. Seguridad en dispositivos de red
2. Seguridad por capas
3. Técnicas de ataque MiTM y spoofing
4. Ataques en IPv4
5. Ataques en IPv6
6. Ataques sobre infraestructura Wireless

ACTIVIDADES FORMATIVAS Y METODOLOGÍAS DOCENTES

Actividades formativas

Actividad Formativa	Horas totales	Horas presenciales
<i>Clases teóricas / Expositivas</i>	29,38	29,38
<i>Clases Prácticas</i>	23,25	23,25
<i>Tutorías</i>	4,00	0,00
<i>Estudio independiente y trabajo autónomo del alumno</i>	50,00	0,00
<i>Elaboración de trabajos (en grupo o individuales)</i>	31,88	0,00
<i>Actividades de Evaluación</i>	5,25	5,25
<i>Seguimiento de Proyectos</i>	6,25	6,25
TOTAL	150	64,13

Metodologías docentes

Método expositivo o lección magistral

Aprendizaje de casos

Aprendizaje basado en la resolución de problemas

Aprendizaje basado en proyectos

Aprendizaje cooperativo o colaborativo
Aprendizaje por indagación
Metodología Flipped classroom o aula invertida
Gamificación
Just in time Teaching (JITT) o aula a tiempo
Método expositivo o lección magistral
Método del caso
Aprendizaje basado en la resolución de problemas
Aprendizaje basado en proyectos
Aprendizaje cooperativo o colaborativo
Aprendizaje por indagación
Metodología flipped classroom o aula invertida
Gamificación

DESARROLLO TEMPORAL

UNIDADES DIDÁCTICAS / TEMAS	PERÍODO TEMPORAL
Presentación de la asignatura	18/09/2023
Tema 1. Introducción	18/09/2023
Tema 2. Dispositivos de seguridad	25/09/2023
Tema 3. Análisis de riesgos	02/10/2023
Tema 4. Criptografía y esteganografía	02/10/2023
Examen temas 1-4	09/10/2023
Tema 5. Fundamentos del hacking en sistemas	09/10/2023
	16/10/2023
	23/10/2023
	30/11/2023
Examen tema 5	06/11/2023
Tema 6. Fundamentos del hacking en aplicaciones	06/11/2023
	13/11/2023

20/11/2023

27/11/2023

Examen tema 6 04/12/2023

Tema 7. Fundamentos del hacking en redes 04/12/2023

11/12/2023

Examen tema 7 18/12/2023

SISTEMA DE EVALUACIÓN

ACTIVIDAD DE EVALUACIÓN	VALORACIÓN MÍNIMA RESPECTO A LA CALIFICACIÓN FINAL (%)	VALORACIÓN MÁXIMA RESPECTO A LA CALIFICACIÓN FINAL (%)
<i>Evaluación de la participación en clase, en prácticas o en proyectos de la asignatura</i>	10	30
<i>Evaluación de trabajos, proyectos, informes, memorias</i>	40	80
<i>Prueba Objetiva</i>	10	60

CRITERIOS ESPECÍFICOS DE EVALUACIÓN

ACTIVIDAD DE EVALUACIÓN	CONVOCATORIA ORDINARIA	CONVOCATORIA EXTRAORDINARIA
<i>Evaluación de la participación en clase, en prácticas o en proyectos de la asignatura</i>	10	10
<i>Evaluación de trabajos, proyectos, informes, memorias</i>	50	50
<i>Prueba Objetiva</i>	40	40

Consideraciones generales acerca de la evaluación

- La evaluación de la participación en clase, en prácticas o en proyectos de la asignatura se realizará a partir de la asistencia y la participación activa en clase y en el resto de las actividades desarrolladas durante el curso. Este aspecto representará el 10% de la calificación final de la asignatura en la convocatoria ordinaria.

- A lo largo del curso se plantearán actividades, ejercicios y problemas que deberán ser entregadas antes de la fecha indicada a través de la plataforma virtual. Este trabajo se evaluará a través de la propia plataforma virtual y supondrá un 50% de la calificación final de la asignatura en la convocatoria ordinaria. Serán desarrolladas un total de 4 prácticas durante el desarrollo de la asignatura, que seguirán los siguientes pesos en la calificación final de la asignatura:
 - o Práctica 1: 10%
 - o Práctica 2: 15%
 - o Práctica 3: 15%
 - o Práctica 4: 10%

- Durante el desarrollo de la asignatura serán realizados un total de 4 exámenes parciales, que serán liberatorios si así lo desea el alumno con la condición de obtener al menos una calificación de 5.0 en dicho examen. Aquellos alumnos que no superen esa nota o que decidan descartarla voluntariamente, deberán realizar los exámenes correspondientes a los dos parciales en la fecha asignada para la convocatoria ordinaria de enero. Los cuatro exámenes parciales representarán los siguientes pesos en la calificación final de la asignatura:
 - o Examen 1: 10%
 - o Examen 2: 10%
 - o Examen 3: 10%
 - o Examen 4: 10%

- Para aprobar la asignatura en la convocatoria ordinaria, es imprescindible que la nota final (incluyendo los exámenes parciales y las prácticas) sea al menos 5.0 (sobre 10). Además de ese requisito, es necesario que la media de los exámenes parciales y la práctica sea al menos 5.0 (sobre 10). En caso de no cumplirse alguno de estos requisitos, la asignatura se considerará automáticamente suspensa independientemente del resto de calificaciones.

- En caso de no conseguir el aprobado en la convocatoria ordinaria de enero, el alumno podrá presentarse a la convocatoria extraordinaria de julio, donde realizará un examen final que representará el 50% de su calificación en dicha convocatoria, junto con una serie de ejercicios y prácticas que representarán el 40%.

- La evaluación de la participación en clase, en prácticas o en proyectos de la asignatura se realizará a partir de la asistencia y la participación activa en clase y en el resto de las actividades desarrolladas durante el curso. Este aspecto representará el 10% de la calificación final de la asignatura en la convocatoria ordinaria.

- A lo largo del curso se plantearán actividades, ejercicios y problemas que deberán ser entregadas antes de la fecha indicada a través de la plataforma virtual. Este trabajo se evaluará a través de la propia

plataforma virtual y supondrá un 50% de la calificación final de la asignatura en la convocatoria ordinaria. Serán desarrolladas un total de 4 prácticas durante el desarrollo de la asignatura, que seguirán los siguientes pesos en la calificación final de la asignatura:

- o Práctica 1: 10%
- o Práctica 2: 15%
- o Práctica 3: 15%
- o Práctica 4: 10%

- Durante el desarrollo de la asignatura serán realizados un total de 4 exámenes parciales, que serán liberatorios si así lo desea el alumno con la condición de obtener al menos una calificación de 5.0 en dicho examen. Aquellos alumnos que no superen esa nota o que decidan descartarla voluntariamente, deberán realizar los exámenes correspondientes a los dos parciales en la fecha asignada para la convocatoria ordinaria de enero. Los cuatro exámenes parciales representarán los siguientes pesos en la calificación final de la asignatura:

- o Examen 1: 10%
- o Examen 2: 10%
- o Examen 3: 10%
- o Examen 4: 10%

- Para aprobar la asignatura en la convocatoria ordinaria, es imprescindible que la nota final (incluyendo los exámenes parciales y las prácticas) sea al menos 5.0 (sobre 10). Además de ese requisito, es necesario que la media de los exámenes parciales y la práctica sea al menos 5.0 (sobre 10). En caso de no cumplirse alguno de estos requisitos, la asignatura se considerará automáticamente suspensa independientemente del resto de calificaciones.

- En caso de no conseguir el aprobado en la convocatoria ordinaria de enero, el alumno podrá presentarse a la convocatoria extraordinaria de julio, donde realizará un examen final que representará el 50% de su calificación en dicha convocatoria, junto con una serie de ejercicios y prácticas que representarán el 450% restante.

- La calificación de la evaluación de la participación en clase, en prácticas o en proyectos en la convocatoria ordinaria, se conservará en convocatoria extraordinaria, siendo de un 10%.

- En los exámenes no se permite el uso de apuntes a menos que se especifique lo contrario, para lo que el alumno debe remitirse a las instrucciones específicas del profesor sobre este tema.

- No se conservarán calificaciones de ningún tipo entre distintos cursos académicos, aunque si entre la convocatoria de Enero y Julio. Pudiendo el alumno presentarse a los exámenes, prácticas o ambas.

- En los exámenes no se permite el uso de apuntes a menos que se especifique lo contrario, para lo que el alumno debe remitirse a las instrucciones específicas del profesor sobre este tema.

- No se conservarán calificaciones de ningún tipo entre distintos cursos académicos, aunque si entre la convocatoria de Enero y Julio. Pudiendo el alumno presentarse a los exámenes, prácticas o ambas.

Consideraciones generales acerca del desarrollo de las clases:

- No está permitido el uso de teléfonos móviles en el aula durante el período de evaluación continua, excepto indicación expresa en sentido contrario del profesor. Los ordenadores portátiles podrán utilizarse únicamente para actividades relacionadas con la asignatura. El profesor podrá retirar el derecho al uso del ordenador a aquellos alumnos que lo utilicen para actividades que no estén relacionadas con la asignatura (consulta de correos, noticias o redes sociales, consulta o elaboración de actividades de otras asignaturas, etc.).
- No está permitido consumir bebidas ni comidas en el aula. Tampoco está permitida la presencia de cualquier tipo de bebida en las mesas, incluso en envases cerrados.
- Se demandará del alumno una participación activa, necesaria para el desarrollo de las clases.
- Se exigirá al alumno un buen comportamiento en todo momento durante el desarrollo de las clases. El mal comportamiento que impida el normal desarrollo de la clase puede conllevar la expulsión del aula por un tiempo a determinar por el profesor.

BIBLIOGRAFÍA / WEBGRAFÍA

Bibliografía Básica:

- Hacking Exposed 7: Network Security Secrets Solutions, Editorial: McGraw-Hill
- The Web Application Hacker's Handbook (Second Edition), Editorial: Wiley

Bibliografía Recomendada:

- Metasploit, Penetration Testers Guide, Editorial: No Starch Press
- Violent Python A Cookbook for Hackers Forensic, Editorial: Syngress
- Mastering Kali Linux for Advanced Penetration Testing, Editorial: Wiley

MATERIALES, SOFTWARE Y HERRAMIENTAS NECESARIAS

Tipología del aula

Aula teórica

Equipo de proyección y pizarra

Materiales:

Ordenador personal

Software:

VirtualBox

Espacio para el almacenamiento de máquinas virtuales