CENTRO UNIVERSITARIO DE TECNOLOGÍA Y ARTE DIGITAL

PLANIFICACIÓN DE LA DOCENCIA UNIVERSITARIA

GUÍA DOCENTE

Introducción a la Seguridad Informática

1. DATOS DE IDENTIFICACIÓN DE LA ASIGNATURA.

Título:	Grado en Ingeniería del Software
Facultad:	Centro Universitario de Tecnología y Arte Digital (U-TAD)
Materia:	Ciberseguridad
Denominación de la asignatura:	Introducción a la Seguridad Informática
Curso:	3
Cuatrimestre:	1
Carácter:	Obligatoria de mención
Créditos ECTS:	6
Modalidad/es de enseñanza:	Híbrido Presencial
Idioma:	Castellano
Profesor/a:	Eduardo Arriols Nuñez
E-mail:	eduardo.arriols@u-tad.com
Teléfono:	

2. DESCRIPCIÓN DE LA ASIGNATURA

2.1 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, especialmente, la información contenida en una computadora o circulante a través de las redes de computadoras. Para ello, los alumnos adquirirán los conocimientos relacionados con las técnicas de ataque y defensa de sistemas informáticos, así como las actividades relacionadas con el análisis forense de sistemas y el análisis del malware.

2.2 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 auditorias de seguridad y análisis de riesgos, necesarios para poder enfocar cualquier acción posterior de auditoria o bastionado.

3. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

3.1. COMPETENCIAS (Genéricas, específicas y transversales)

Competencias Básicas y Generales
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
Competencias Específicas
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.

4. CONTENIDOS

4.1. Temario de la asignatura

Tema 1. Introducción general

- Amenazas actuales
- Definiciones básicas
- Reconocimiento de un ataque
- Ámbitos de la seguridad
- Anonimato en red
- Repaso de redes
- Estructura de una organización

Tema 2. Sistemas de seguridad

- En red
- En sistemas
- En organizaciones
- Herramientas avanzadas

Tema 3. Análisis de riesgos y cumplimiento normativo

- Análisis de riesgo
- Principales leyes y normativas

Tema 4. Criptografía y Esteganografía

- Cifrado simétrico y asimétrico
- Funciones hash y firma digital
- Esteganografía
- Protección de datos

Tema 5. Fundamentos del hacking en sistemas

- Búsqueda de información
- Enumeración de servicios
- Análisis de vulnerabilidades
- Explotación de vulnerabilidades
- Proceso de post-explotación

Tema 6. Fundamentos del hacking en aplicaciones web

- Metodologías de auditoría
- Herramientas básicas
- Mapeo de una aplicación
- Principales vulnerabilidades (Enumeración de usuarios, XSS, SQLi, …)

Tema 7. Fundamentos del hacking en redes

- Seguridad en dispositivos de red
- Seguridad por capas
- Interceptación de tráfico de red
- Ataques de spoofing

Tema 8. Fundamentos del desarrollo seguro y exploiting

- Ciclo del desarrollo
- Funciones peligrosas
- Nociones básicas (arq. de sistemas, memoria y ensamblador)
- Desarrollo de un exploit

4.2. Desarrollo temporal

UNIDADES DIDÁCTICAS / TEMAS	PERÍODO TEMPORAL
Tema 1. Introducción a la Seguridad	Semana 1
Tema 2. Sistemas de seguridad	Semanas 2
Tema 3. Análisis de riesgos y cumplimiento	Semanas 3
Tema 4. Cripografía y esteganografía	Semana 4
Tema 5. Fund. del hacking de sistemas	Semanas 5, 6, 7 y 8
Tema 6. Fund. del hacking en aplicaciones web	Semanas 9, 10 y 11
Tema 7. Fund. del hacking en redes	Semanas 12 y 13
Tema 8. Fund. del desarrollo seguro y exploiting	Semanas 14 y 15

5. ACTIVIDADES FORMATIVAS Y MODALIDADES DE ENSEÑANZAS

5.1. Modalidades de enseñanza

La asignatura se desarrollará a través de los siguientes métodos y técnicas generales, que se aplicarán diferencialmente según las características propias de la asignatura:

- **Método expositivo/Lección magistral:** el profesor desarrollará, mediante clases magistrales y dinámicas los contenidos recogidos en el temario.
- **Estudio de casos:** análisis de casos reales relacionados con la asignatura.
- **Resolución de ejercicios y problemas:** los estudiantes desarrollarán las soluciones adecuadas aplicando procedimientos de transformación de la información disponible y la interpretación de los resultados.
- **Aprendizaje basado en problemas:** utilización de problemas como punto de partida para la adquisición de conocimientos nuevos.
- **Aprendizaje orientado a proyectos:** se pide a los alumnos que, en pequeños grupos, planifiquen, creen y evalúen un proyecto que responda a las necesidades planteadas en una determinada situación.
- **Aprendizaje cooperativo:** Los estudiantes trabajan en grupo para realizar las tareas de manera colectiva.

5.2. Actividades formativas

Actividad Formativa	Horas	Presencialidad
AF1 Clases teóricas / Expositivas	30	100%
AF2 Clases Prácticas	24	100%
AF3 Tutorías	6	50%
AF4 Estudio independiente y trabajo autónomo del alumno	57,5	0%
AF5 Elaboración de trabajos (en grupo o individuales)	28,5	0%
AF6: Actividades de Evaluación	4	100%

6. SISTEMA DE EVALUACIÓN

ACTIVIDAD DE EVALUACIÓN	VALORACIÓN MÍNIMA RESPECTO A LA CALIFICACIÓN FINAL (%)	VALORACIÓN MÁXIMA RESPECTO A LA CALIFICACIÓN FINAL (%)
SE1 Evaluación de la participación en clase, en prácticas o en proyectos de la asignatura	10%	30%
SE2 Evaluación de trabajos, proyectos, informes, memorias	40%	80%
SE3 Exámenes intermedios o final (no continua)	10%	60%

6.1. Criterios de calificación

ACTIVIDAD DE EVALUACIÓN	VALORACIÓN RESPECTO A LA CALIFICACIÓN FINAL (%)
SE1 Evaluación de la participación en clase, en prácticas o en proyectos de la asignatura	10%
SE2 Evaluación de trabajos, proyectos, informes, memorias	45%
SE3 Exámenes intermedios o final (no continua)	45%

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 45% 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:

- Práctica 1: 10%
- Práctica 2: 12,5%
- Práctica 3: 12,5%
- 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:

    - Examen 1: 10%
    - Examen 2: 12,5%
    - Examen 3: 12,5%
    - 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 50% restante.

- 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.

7. 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

8. MATERIAL, SOFTWARE Y HERRAMIENTAS NECESARIAS

VirtualBox

Espacio para el almacenamiento de máquinas virtuales