

CENTRO UNIVERSITARIO DE TECNOLOGÍA Y ARTE DIGITAL



**PLANIFICACIÓN DE LA DOCENCIA
UNIVERSITARIA**

GUÍA DOCENTE

BASTIONADO

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:	Bastionado
Curso:	4
Cuatrimestre:	1
Carácter:	Obligatoria de mención
Créditos ECTS:	6
Modalidad/es de enseñanza:	Híbrido Presencial
Idioma:	Castellano
Profesor/a:	Rafael Vida
E-mail:	rafael.vida@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

La asignatura de bastionado está orientada a entender el proceso de protección de sistemas, aplicaciones, redes y datos, así como conocer los marcos de referencia existentes y las herramientas que permiten implementar esa protección.

Se analizarán los procesos de bastionado basados en estándares internacionales además de los marcos de referencia disponibles, tanto orientados al cumplimiento normativo y estandarización como a la securización de los sistemas.

Se estudiarán, también, varias herramientas reconocidas internacionalmente como de referencia.

La orientación de la asignatura es muy práctica, por lo que se aplicarán los conceptos aprendidos a varios casos propuestos.

3. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

3.1. COMPETENCIAS (Genéricas, específicas y transversales)

Competencias Básicas y Generales
<p>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.</p> <p>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.</p> <p>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.</p> <p>CB4: Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.</p> <p>CB5: Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía</p> <p>CG1 - Capacidad para entender, planificar y resolver problemas a través del desarrollo de soluciones informáticas.</p> <p>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</p> <p>CG3 - Conocimiento de los fundamentos científicos aplicables a la resolución de problemas informáticos</p> <p>CG4 - Capacidad para simplificar y optimizar los sistemas informáticos atendiendo a la comprensión de su complejidad</p> <p>CG9 - Capacidad para aprender, modificar y producir nuevas tecnologías informáticas</p> <p>CG10 - Uso de técnicas creativas para la realización de proyectos informáticos</p> <p>CG11 - Capacidad de buscar, analizar y gestionar la información para poder extraer conocimiento de la misma</p>
Competencias Específicas
<p>CE10 - Capacidad para manejar un gestor de versiones de código y generar la documentación de una aplicación de forma automática.</p>
Competencias Transversales
<p>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</p> <p>CT2 - Conocimiento de los principales agentes del sector y del ciclo de vida completo de un proyecto de desarrollo y comercialización de contenidos digitales</p> <p>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</p> <p>CT5 - Desarrollo de las habilidades necesarias para el emprendimiento digital.</p>

4. CONTENIDOS

4.1. Temario de la asignatura

<ul style="list-style-type: none">1. Fundamentos<ul style="list-style-type: none">1.1. Problemas y objetivos del bastionado.1.2. Proceso1.3. Trade-off utilidad-seguridad2. Monitorización básica.<ul style="list-style-type: none">2.1. Audit.2.2. Monitorización.2.3. Correlaciones, detección de anomalías.3. Proceso general Hardening para servidores<ul style="list-style-type: none">3.1. Fases3.2. Principales retos4. Frameworks<ul style="list-style-type: none">4.1. CIS-CAT4.2. NIST4.3. Dev-Sec4.4. Otros5. Aplicación: casos prácticos:<ul style="list-style-type: none">5.1. Linux5.2. Windows6. Hardening de aplicaciones<ul style="list-style-type: none">6.1. Marcos de desarrollo seguro6.2. Metodología de hardening de aplicaciones7. Hardening de redes.<ul style="list-style-type: none">7.1. Capas y arquitectura desde el punto de vista de seguridad.7.2. Segregación.7.3. Redes complejas8. Hardening de los datos.<ul style="list-style-type: none">8.1. Datos personales. Marco legal.8.2. Tipos de ataque.8.3. Protección de datos independiente de plataforma

4.2. Desarrollo temporal

UNIDADES DIDÁCTICAS / TEMAS	PERÍODO TEMPORAL
<ul style="list-style-type: none">1. Fundamentos2. Monitorización básica.	2 semanas
<ul style="list-style-type: none">3. Proceso general Hardening para servidores4. Frameworks	5 semanas
<ul style="list-style-type: none">5. Aplicación: casos prácticos:	3 semanas
<ul style="list-style-type: none">6. Hardening de aplicaciones7. Hardening de redes.8. Hardening de los datos.	4 semanas

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

Convocatoria Ordinaria

ACTIVIDAD DE EVALUACIÓN	CRITERIOS DE EVALUACIÓN	VALORACIÓN RESPECTO A LA CALIFICACIÓN FINAL (%)
SE1 Evaluación de la participación en clase, en prácticas o en proyectos de la asignatura	Interés, participación en clase	10 %
SE2 Evaluación de trabajos, proyectos, informes, memorias	Ejercicios obligatorios.	30 %
SE3 Prueba Objetiva	Prueba final	60 %

Consideraciones generales acerca de la evaluación:

- El alumno irá demostrando con su trabajo en el aula, sus entregas parciales, sus ejercicios autónomos corregidos, y actitud general hacia su aprendizaje si está capacitado en las competencias que de él se esperan desarrollar en esta asignatura.
- Calificación numérica final de 0 a 10, será requisito indispensable alcanzar una calificación mínima de 5 puntos para poder obtener un aprobado.
- No se admitirán trabajos fuera de forma y fecha sin causa justificada, cada entrega se entiende como un examen y tendrá derecho a revisión. Y si se aceptan será con una reducción en la nota.
- El examen final (PRESENCIAL) y supondrá un 60% de la calificación definitiva. Se deberá tener al menos un 4 sobre 10 en el examen para poder hacer media con el resto de los apartados.

Convocatoria Extraordinaria

Los alumnos que no hayan superado la asignatura en convocatoria ordinaria podrán optar a una evaluación extraordinaria. Deberán realizar un examen extraordinario (PRESENCIAL) con las características y en las condiciones determinadas por el profesor. La calificación de la convocatoria extraordinaria será la obtenida en dicho examen.

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