



GUÍA DOCENTE

BASTIONADO

GRADO EN INGENIERÍA DEL SOFTWARE

MODALIDAD: PRESENCIAL

CURSO ACADÉMICO: 2023-2024

| | |
|--------------------------------|---|
| Denominación de la asignatura: | Bastionado |
| Titulación: | Ingeniería del Software |
| Facultad o Centro: | Centro Universitario de Tecnología y Arte Digital |
| Materia: | Ciberseguridad |
| Curso: | 4º |
| Cuatrimestre: | 1 |
| Carácter: | OBM |
| Créditos ECTS: | 6 |
| Modalidad/es de enseñanza: | Presencial |
| Idioma: | Castellano |
| Profesor/a - email | Iñaki Lasa / inaki.lasa@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

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 referencia.

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

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

Fundamentos del Bastionado

Dispositivos de seguridad, monitorización y correlación de eventos

Bastionado en sistemas informáticos

Bastionado en webs y aplicaciones móviles

Bastionado en redes

TEMARIO

1. Introducción al bastionado
 - 1.1. Repaso de conceptos básicos
 - 1.2. Problemas y objetivos del bastionado
2. Seguridad en Linux: servidor y cliente
 - 2.1. Acceso al hardware
 - 2.2. Control de aplicaciones
 - 2.3. Herramientas de seguridad
3. Seguridad en Windows: servidor y cliente
 - 3.1. Acceso al hardware
 - 3.2. Configuración de Active Directory
 - 3.3. Herramientas de seguridad
4. Gestión de incidentes de seguridad
 - 4.1. Prevención: firewall, IDS, IPS
 - 4.2. Identificación
 - 4.3. Contención y erradicación
 - 4.4. Informe y mejora
5. Deception
 - 5.1. Diseño del entorno
 - 5.2. Creación de breadcrumbs
 - 5.3. Obtención de información
 - 5.4. Generar un incidente

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

1. Introducción al bastionado 2 semanas
2. Seguridad en Linux
3. Seguridad en Windows 7 semanas
4. Gestión de incidentes 3 semanas
5. Deception 2 semanas

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> | 40 | 40 |
| <i>Prueba Objetiva</i> | 50 | 50 |

Consideraciones generales acerca de la evaluación

Convoactoria Ordinaria

- "• 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.
- En la calificación numérica final de 0 a 10, será requisito indispensable alcanzar una calificación mínima de 5 puntos para poder obtener un aprobado.
- Las prácticas obligatorias supondrán el 40% de la calificación definitiva. No se aceptarán entregas fuera de plazo, y si se aceptan, será con una reducción en la nota. Todas las prácticas obligatorias deben tener una calificación superior o igual a 5 sobre 10 para aprobar la asignatura.
- Los exámenes parciales supondrán el 50% de la calificación definitiva. Se deberá tener al menos un 4 sobre 10 en cada examen para poder aprobar la asignatura, y, entre los dos exámenes la media deberá ser superior a 5 sobre 10.
- La participación en clase supondrá un 10% de la calificación definitiva. Esta participación será evaluada por actividades realizadas en el horario de clase. Será necesaria una calificación mínima de 0 sobre 10 para poder aprobar la asignatura

Convocatoria Extraordinaria

- El examen final será una prueba única de hasta 4 horas que supondrá el 60% de la calificación definitiva.
- En caso de haber obtenido una nota media superior o igual a 5 sobre 10 en los exámenes parciales de la convocatoria ordinaria y un 4 sobre 10 en cada uno de ellos, NO será necesario realizar el examen final en convocatoria extraordinaria. En ese caso, la calificación del examen final será la nota media obtenida en los exámenes de convocatoria ordinaria.
- Las prácticas obligatorias serán las mismas de la convocatoria ordinaria, de tal manera que las prácticas con nota superior o igual a 5 sobre 10 en la convocatoria ordinaria conservarán su nota en convocatoria extraordinaria.
- 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%.
-

BIBLIOGRAFÍA / WEBGRAFÍA

0

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