Proyecto/Guía docente de la asignatura

Se debe indicar de forma fiel cómo va a ser desarrollada la docencia. Esta guía debe ser elaborada teniendo en cuenta a todos los profesores de la asignatura. Conocidos los espacios y profesorado disponible, se debe buscar la máxima presencialidad posible del estudiante siempre respetando las capacidades de los espacios asignados por el centro y justificando cualquier adaptación que se realice respecto a la memoria de verificación. Si la docencia de alguna asignatura fuese en parte online, deben respetarse los horarios tanto de clase como de tutorías). La planificación académica podrá sufrir modificaciones de acuerdo con la actualización de las condiciones sanitarias.

Asignatura	CIBERSEGURIDAD		
Materia	Aseguramiento de la calidad y la seguridad del software		
Módulo	Tecnologías Informáticas (2)		
Titulación	MÁSTER EN INGENIERÍA INFORMÁTICA		
Plan	693 (No Presencial)	**Código**	55114
Periodo de impartición	1º CUATRIMESTRE	**Tipo/Carácter**	OBLIGATORIA
Nivel/Ciclo	MÁSTER	**Curso**	1
Créditos ECTS	3		
Lengua en que se imparte	CASTELLANO		
Profesor/es responsable/s	Amador Aparicio de la Fuente Blas Torregrosa García Jesús Vegas Hernández (Coordinador)		
Datos de contacto (E-mail, teléfono…)	jvegas@infor.uva.es		
Departamento	INFORMÁTICA (ATC, CCIA y LSI)		

1. Situación / Sentido de la Asignatura

1.1 Contextualización

Dentro de la perspectiva de los estudios de un máster sobre Informática de perfil profesionalizante, en esta asignatura se pretende ser una introducción a los problemas de seguridad en sistemas informáticos en un mundo hiper-conectado, cuyo pilar básico es la seguridad de los sistemas de información.

Esta asignatura permite obtener una panorámica sobre los principales problemas de seguridad existentes actualmente desde el punto de vista del hacker para que los profesionales de la Informática obtengan el conocimiento y las habilidades que hagan de los sistemas y de las aplicaciones de su responsabilidad más seguros y resilientes a ataques.

Esta asignatura pretende formar profesionales cuyo fin y objetivo es descubrir vulnerabilidades para corregirlas, comunicarlas e impedir que sean explotadas por ciberdelincuentes. Expondremos las principales técnicas para vulnerar los sistemas, así como estudiaremos el malware o software malicioso, sus diferentes variantes, comportamiento, vectores de ataque y como combatirlos.

1.2 Relación con otras materias

La materia guarda relación con asignaturas de sistemas operativos, administración de sistemas, seguridad, arquitectura de computadores, redes de computadores, programación y criptografía.

1.3 Prerrequisitos

Para hacer el seguimiento de esta asignatura hay que tener los conocimientos básicos de la Ingeniería Informática. En particular, hay que tener conocimientos de arquitecturas de ordenadores y sistemas operativos, de redes, de programación y de criptografía.

2. Competencias

2.1 Generales

CG1	Capacidad para proyectar, calcular y diseñar productos, procesos e instalaciones en todos los ámbitos de la Ingeniería Informática
CG7	Capacidad para la puesta en marcha, dirección y gestión de procesos de fabricación de equipos informáticos, con garantía de la seguridad para las personas y bienes, la calidad final de los productos y su homologación
CG8	Capacidad para la aplicación de los conocimientos adquiridos y de resolver problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinares, siendo capaces de integrar estos conocimientos
CG9	Capacidad para comprender y aplicar la responsabilidad ética, la legislación y la deontología profesional de la actividad de la profesión de Ingeniero en Informática

2.2 Transversales

CT2	Capacidad para trabajar bajo presión
CT3	Capacidad para afrontar tareas y situaciones críticas
CT5	Conocimiento de otras lenguas, sobre todo la inglesa
CT6	Capacidad de trabajo autónomo y toma de decisiones
CT7	Capacidades asociadas al trabajo en equipo: cooperación, liderazgo, saber escucha
CT8	Capacidad analítica, crítica y de síntesis
CT10	Capacidad de adaptación a situaciones cambiantes. Flexibilidad. Predisposición al cambio.

2.3 Específicas

CET4	Capacidad para diseñar, desarrollar, gestionar y evaluar mecanismos de certificación y garantía de seguridad en el tratamiento y acceso a la información en un sistema de procesamiento local o distribuido
CET2	Capacidad de comprender y saber aplicar el funcionamiento y organización de Internet, las tecnologías y protocolos de redes de nueva generación, los modelos de componentes, software intermediario y servicios.
CET3	Capacidad para asegurar, gestionar, auditar y certificar la calidad de los desarrollos, procesos, sistemas, servicios, aplicaciones y productos informáticos

3. Objetivos

- Conocer los principios básicos de la seguridad informática y aplicarlos para la seguridad y protección de la información en organizaciones.
- Identificar las vulnerabilidades en sistemas informáticos y corregirlas.
- Identificar los principales mecanismos que permiten la intrusión y ataques a los sistemas informáticos para poder proponer las contramedidas más adecuadas.
- Saber aplicar técnicas de ciberseguridad ofensiva y defensiva en entornos prácticos y realistas.
- Obtener los conocimientos necesarios para acceder a una certificación en ciberseguridad como Security+, Certified Ethical Hacking (CEH) u Offensive Security Certified Professional (OSCP).

4. Contenidos y/o bloques temáticos

La asignatura se plantea como la resolución de 3 retos. Cada uno de los cuales contiene unos materiales sobre los que el alumno tiene que trabajar, unos laboratorios en los que practicar las herramientas y unos ejercicios que resolver de forma autónoma.

Reto 1: "Cómo convertirse en hacker"

Carga de trabajo en créditos ECTS: 1

a. Contextualización y justificación

En este primer reto se plantean los conceptos básicos y las bases de la ciberseguridad, así como los mecanismos básicos de identificación de los usuarios (legítimos) en los sistemas informáticos.

b. Objetivos de aprendizaje

- Comprender la terminología básica de ciberseguridad
- Comprender modelos de ataques, riegos y amenazas.
- Identificar los diferentes tipos de actores de amenaza (hackers) y sus motivaciones.
- Comprender las formas de identificar a los usuarios y controlar el acceso a los sistemas informáticos.

c. Contenidos

Tema 1. Principios básicos de ciberseguridad

- Orígenes de ciberseguridad: de Juegos de Guerra hasta hoy.
- Definición de ciberseguridad.
- La triada CIA.
- Indicadores de compromiso (IOCs)
- Vulnerabilidades. Vectores de ataque.
- Modelos de amenazas. Ciber-cadena de la muerte.
- Hackers y tipos de hackers
- Tipos de ataques.

Tema 2. Gestión de identidad y control de acceso.

- Autenticación y autorización.
- Biometría.
- Identidad digital.
- Privacidad.

d. Métodos docentes

Ver apartado general de Métodos Docentes.

e. Plan de trabajo

- El profesor proporcionará los materiales que serán trabajados por los alumnos y resolverá las dudas que le planteen los mismos.
- Uso de la plataforma de docencia virtual.
- Los alumnos trabajarán individualmente y/o en grupo, resolviendo los casos propuestos y analizando la documentación que les sea facilitada por el profesor.

f. Evaluación

Ver apartado general de evaluación.

g Material docente

g.1 Bibliografía básica

Los materiales didácticos puestos a disposición de los alumnos por el profesor.

g.2 Bibliografía complementaria

- Ayala, Luis. **Cybersecurity Lexicon**. 1st ed. 2016. Berkeley, CA: Apress. https://doi-org.ponton.uva.es/10.1007/978-1-4842-2068-9
- Rothwell, William. **Linux Essentials for Cybersecurity Lab Manual**, 1st Edition. : Pearson IT Certification, October 2018. ISBN: 9780135305232.
- Steinberg, Joseph. **Cybersecurity For Dummies**. For Dummies Pub., october 2019. ISBN: 9781119560326.
- Svensson, Robert. **From Hacking to Report Writing An Introduction to Security and Penetration Testing** . 1st ed. 2016. Berkeley, CA: Apress.

g.3 Otros recursos telemáticos (píldoras de conocimiento, blogs, videos, revistas digitales, cursos masivos (MOOC), …)

- Artículos en Medium sobre ciberseguridad: https://medium.com/topic/cybersecurity

h. Recursos necesarios

Plataforma de docencia virtual a elegir al principio de la asignatura.
Laboratorio (Cyber-range) como plataforma de entrenamiento y simulación en ciberseguridad creada para la asignatura.

i. Temporalización

CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
1 ECTS	De la 1ª a la 3º semana del cuatrimestre

Reto 2: "Intrusión en sistemas"

Carga de trabajo en créditos ECTS: 1

a. Contextualización y justificación

b. Objetivos de aprendizaje

- Aprender a analizar las redes y sistemas informáticos en busca de vulnerabilidades.
- Identificar y explotar las principales vulnerabilidades de las aplicaciones web y del funcionamiento de la web y los navegadores.
- Proponer diferentes soluciones a las vulnerabilidades encontradas.

c. Contenidos

Tema 3. Reconocimiento y fuentes de información

- Escaneo de redes y vulnerabilidades. Enumeración.
- Ingeniería social.
- Redes inalámbricas

Tema 4. Pruebas de penetración en aplicaciones web

- Funcionamiento de la web
- Inyección de SQL
- Cross-site Scripting (XXS)
- Cross-site Request Forgery (CSRF)
- Secuestro de sesión

d. Métodos docentes

Ver apartado general de Métodos Docentes.

e. Plan de trabajo

- El profesor proporcionará los materiales que serán trabajados por los alumnos y resolverá las dudas que le planteen los mismos.
- Uso de la plataforma de docencia virtual.
- Los alumnos trabajarán individualmente y/o en grupo, resolviendo los casos propuestos y analizando la documentación que les sea facilitada por el profesor.

f. Evaluación

Ver apartado general de evaluación.

g Material docente

g.1 Bibliografía básica

Los materiales didácticos puestos a disposición de los alumnos por el profesor.

g.2 Bibliografía complementaria

- Tanner, Nadean H. **Cybersecurity Blue Team Toolkit**. Wiley, April 2019. ISBN: 9781119552932
- O'Leary, Mike. **Cyber Operations Building, Defending, and Attacking Modern Computer Networks**. Second edition. Berkeley, CA: Apress, 2019.
- Sinha, Sanjib. **Beginning Ethical Hacking with Python**. Berkeley, CA: Apress, 2017.
- Sinha, Sanjib**. Beginning Ethical Hacking with Kali Linux Computational Techniques for Resolving Security Issues** . 1st ed. 2018. Berkeley, CA: Apress, 2018
- Sinha, Sanjib**. Bug Bounty Hunting for Web Security : Find and Exploit Vulnerabilities in Web Sites and Applications**. 1st ed. 2019. Place of publication not identified: Apress, 2019
- Rahalkar, Sagar Ajay. **Certified Ethical Hacker (CEH) Foundation Guide**. Berkeley, CA: Apress, 2016.

g.3 Otros recursos telemáticos (píldoras de conocimiento, blogs, videos, revistas digitales, cursos masivos (MOOC), …)

- OWASP Top Ten. https://owasp.org/www-project-top-ten/

h. Recursos necesarios

Plataforma de docencia virtual a elegir al principio de la asignatura.
Cyber-range es una plataforma de entrenamiento y simulación en ciberseguridad creada para la asignatura.

i. Temporalización

CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
1 ECTS	De la semana 4ª a la 5ª del cuatrimestre

Reto 3: "Técnicas de ciberseguridad ofensiva"

Carga de trabajo en créditos ECTS: 1

a. Contextualización y justificación

Los hackers utilizan técnicas que aprovechan fallos y vulnerabilidades en los diferentes servicios que nos ofrece internet como red global. El objetivo es conocer algunas de esas técnicas para detectar ataques y mitigar las consecuencias.

b. Objetivos de aprendizaje

- Comprender y determinar las características del software malicioso.
- Aprender técnicas utilizadas por el malware para ocultarse y propagarse.
- Comprender el funcionamiento de técnicas ofensivas y defensivas en entornos reales.

c. Contenidos

Tema 5. Software malicioso.

- Tipos de malware.
- Análisis de malware. Ingeniería inversa
- Comportamientos maliciosos
  - Puertas traseras
  - Empaquetadores y descargadores
  - Persistencia
  - Botnet con comando y control (C&C)
  - Ransomware
  - Amenazas Persistentes Avanzadas (APT)

Tema 6. Ataques y contramedidas

- Man in the middle
- Movimientos laterales
- Anonimización
- Threat hunting

d. Métodos docentes

Ver apartado general de Métodos Docentes.

e. Plan de trabajo

- El profesor proporcionará los materiales que serán trabajados por los alumnos y resolverá las dudas que le planteen los mismos.
- Uso de la plataforma de docencia virtual.
- Los alumnos trabajarán individualmente y/o en grupo, resolviendo los casos propuestos y analizando la documentación que les sea facilitada por el profesor.

f. Evaluación

Ver apartado general de evaluación.

g Material docente

.

g.1 Bibliografía básica

Los materiales didácticos puestos a disposición de los alumnos por el profesor.

g.2 Bibliografía complementaria

- Bettany, Andrew., and Mike. Halsey. **Windows Virus and Malware Troubleshooting**. 1st ed. 2017. Berkeley, CA: Apress.
- Collins, Michael. **Threat Hunting**. O'Reilly Media, Inc., May 2018. ISBN: 9781492028253
- Hassan, Nihad A. **Ransomware Revealed : a Beginner's Guide to Protecting and Recovering from Ransomware Attacks** .1st ed. 2019. Place of publication not identified: Apress, 2019
- Oakley, Jacob G**. Professional Red Teaming: Conducting Successful Cybersecurity Engagements**. Apress, 2019.
- Raims, Tim. **Cybersecurity Threats, Malware Trends, and Strategies**. Packt Publishing, May 2020. ISBN: 9781800206014
- Tanner, Nadean H. **Cybersecurity Blue Team Toolkit**. Wiley, April 2019. ISBN: 9781119552932
- Tiirmaa-Klaar, Heli. et al. **Botnets**. 1st ed. London: Springer London, 2013.
- Wrightson, Tyler. **Advanced Persistent Threat Hacking**. McGraw-Hill, December 2014. ISBN: 9780071828376.

g.3 Otros recursos telemáticos (píldoras de conocimiento, blogs, videos, revistas digitales, cursos masivos (MOOC), …)

- UN INFORMÁTICO EN EL LADO DEL MAL. BLOG PERSONAL DE CHEMA ALONSO SOBRE SUS COSAS. (https://www.elladodelmal.com/)

h. Recursos necesarios

Plataforma de docencia virtual a determinar al principio de la asignatura.
Cyber-range es una plataforma de entrenamiento y simulación en ciberseguridad creada para la asignatura.

i. Temporalización

CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
1 ECTS	De la semana 6ª a la 7ª del cuatrimestre

5. Métodos docentes y principios metodológicos

Esta asignatura se impartirá en modo no presencial u online.

Se utilizarán los siguientes recursos y medios:

- Resolución de casos prácticos mediante el uso de herramientas de enseñanza online de la universidad.
- Laboratorios (ciber-range) de resolución de casos prácticos.
- Tutorías con posibilidad del uso de herramientas online y de solicitud previa.

6. Tabla de dedicación del estudiante a la asignatura

ACTIVIDADES PRESENCIALES o PRESENCIALES A DISTANCIA(1)	HORAS	ACTIVIDADES NO PRESENCIALES	HORAS
Clases teórico-prácticas	6	Trabajo autónomo sobre contenidos teóricos	10
Laboratorios	17	Trabajo autónomo sobre laboratorios	20
Seminarios	2	Elaboración de trabajos	20
Total presencial	**25**	Total no presencial	**50**
		TOTAL presencial + no presencial	**75**

(1) Actividad presencial a distancia es cuando un grupo sigue una videoconferencia de forma síncrona a la clase impartida por el profesor para otro grupo presente en el aula.

7. Sistema y características de la evaluación

Criterio: cuando al menos el 50% de los días lectivos del cuatrimestre transcurran en normalidad, se asumirán como criterios de evaluación los indicados en la guía docente. Se recomienda la evaluación continua ya que implica minimizar los cambios en la planificación.

La medición del rendimiento del estudiante en esta asignatura se hará mediante **evaluación continua** y será realizada mediante el siguiente conjunto de instrumentos: exámenes de teoría, realización y presentación de prácticas y ejercicios prácticos individuales.

El contenido **teórico** se evaluará mediante exámenes online de teoría compuestos por preguntas de tipo test sobre cada uno de los retos abordados y en conjunto tendrán un peso del 25% de la nota.

Las competencias **prácticas** se evaluarán mediante proyectos y prácticas asociadas a cada uno de los retos y en total la evaluación de la parte práctica supondrá el 75% de la nota de la asignatura.

INSTRUMENTO/PROCEDIMIENTO	PESO EN LA NOTA FINAL	OBSERVACIONES
Exámenes de teoría	25%	Pruebas parciales (cuestionarios y supuestos prácticos) asociados a cada reto.
Exámenes de contenido práctico	75%	Supuestos prácticos a resolver asociados a cada reto.

CRITERIOS DE CALIFICACIÓN

• **Convocatoria ordinaria:**
  ○ Exentos los que hayan superado la asignatura por evaluación continua
  ○ Cuestionario teórico/práctico (25% de la nota)
  ○ Supuestos prácticos (75% de la nota)
• **Convocatoria extraordinaria:**
  ○ Cuestionario teórico/práctico (25% de la nota)
  ○ Supuestos prácticos (75% de la nota)

8. Consideraciones finales

N/A