Universidad de Alcalá

GUÍA DOCENTE

Comunicaciones Seguras

Master Universitario en Ciberseguridad
Universidad de Alcalá

Curso Académico 2019/20

GUÍA DOCENTE

Nombre de la asignatura:	**Seguridad en las comunicaciones**
Código:	202556
Titulación en la que se imparte:	**Master Universitario en Ciberseguridad**
Departamento y Área de Conocimiento:	**Automática.** **Área de Ingeniería Telemática**
Carácter:	**Obligatorio**
Créditos ECTS:	**4,5**
Curso y cuatrimestre:	**Primer curso**
Profesorado:	Iván Marsá Maestre
Horario de Tutoría:	
Idioma en el que se imparte:	Español

1. PRESENTACIÓN

Las TIC se han vuelto esenciales para la vida personal y profesional de los ciudadanos. Individuos, negocios y gobiernos están cada vez más interconectados, intercambiando de forma constante información por medio de una diversidad de dispositivos en los hogares, en los lugares de trabajo, en espacios públicos y en el trayecto entre los mismos. Todos estos intercambios se sustentan en comunicaciones que se realizan a través de millones de redes individuales, que abarcan desde las redes domésticas a redes de alcance global. Dado que la confianza es un factor crucial en las interacciones económicas y sociales, para que las grandes oportunidades que brindan las TIC se mantengan, se consoliden y avancen, la seguridad de las comunicaciones va a jugar un papel fundamental.

Esta asignatura está dirigida a profundizar en los aspectos técnicos relacionados con la seguridad de las comunicaciones en diferentes entornos. Su objetivo principal será analizar los protocolos, hardware de red y mecanismos para la comunicación segura de información extremo a extremo sobre diferentes tipos de redes y soportes. Tras revisar los fundamentos generales de las comunicaciones seguras (e.g. autenticación mutua o intercambio de secretos), la asignatura abordará la seguridad de los protocolos de Internet en sus diferentes niveles, principalmente enlace, red y transporte. Finalmente, se estudiarán los desafíos particulares de la seguridad en las comunicaciones inalámbricas, tanto locales (Wi-Fi, Bluetooth) como móviles.

2. COMPETENCIAS

Competencias Generales (CG) y Básicas (CB)

Esta asignatura contribuye a alcanzar las siguientes competencias generales y básicas, tal y como se recoge en la memoria de verificación del estudio:

CG1	Capacidad para aplicar conocimientos y técnicas de seguridad de la información a la gestión, evaluación, cumplimiento de normativas y diseño de departamentos, programas y proyectos.
CG2	Capacidad para seleccionar y aplicar técnicas, métodos y tecnologías de protección de la información y las comunicaciones en contextos complejos y cambiantes.

CB6	Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación
CB7	Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

Competencias específicas (CE)

Esta asignatura contribuye a alcanzar las siguientes competencias específicas, tal y como se recoge en la memoria de verificación del estudio:

CE5	Capacidad para aplicar los fundamentos y las técnicas de ingeniería criptográfica a la selección, diseño y evaluación de la seguridad de la información y las comunicaciones.
CE6	Capacidad para diferenciar, seleccionar y desplegar tecnologías y arquitecturas de comunicaciones seguras de acuerdo con los requisitos de usuarios y organizaciones.

Competencias transversales (CT)

Esta asignatura contribuye a alcanzar las siguientes competencias transversales, tal y como se recoge en la memoria de verificación del estudio:

CT1	Gestión del tiempo
CT3	Trabajo en equipo
CT4	Resolución de problemas
CT5	Toma de decisiones

Resultados del aprendizaje

Al término de la asignatura, el alumno habrá alcanzado los siguientes resultados de aprendizaje:

RA1	Utilización de mecanismos criptográficos para gestionar riesgos de seguridad de la información, evaluando las implicaciones de uso de los diferentes mecanismos disponibles.
RA2	Construcción de soluciones de seguridad aceptables en escenarios concretos, utilizando diferentes mecanismos criptográficos.
RA3	Análisis y despliegue de mecanismos de seguridad preventivos, de detección y reactivos sobre dispositivos y servicios de red.
RA4	Selección e implementación de tecnologías y arquitecturas de comunicaciones seguras de acuerdo con los requisitos de diferentes usuarios y organizaciones.
RA5	Trabajar en equipo de forma colaborativa para la resolución de problemas relacionados con la seguridad de las comunicaciones y comunicar de manera eficaz sus conocimientos, procedimientos, resultados e ideas al respecto, tanto por escrito como de forma oral.

3. CONTENIDOS

Bloques de contenido
Revisión de fundamentos de comunicaciones seguras: protocolos de autenticación. Autenticación mutua
Seguridad en los protocolos de Internet. Identificación de dispositivos de red. Ataques a nivel de red. Ataques a nivel de enlace. Ataques a nivel de aplicación.
Mecanismos de protección extremo a estremo. Revisión de fundamentos de autenticación. SSL. IPsec. VPNs
Seguridad en redes inalámbricas. Seguridad en Wi-Fi. Seguridad en redes móviles. Seguridad en IoT

4. METODOLOGÍAS DE ENSEÑANZA-APRENDIZAJE.-ACTIVIDADES FORMATIVAS

4.1. Distribución de créditos (especificar en horas)

Número de horas presenciales:	Clases presenciales teórico prácticas, incluyendo trabajo en ordenador: 31,5 horas Tutorías: 9 horas Seminarios temáticos y conferencias: 4,5 horas Total: 45 horas presenciales
Número de horas del trabajo propio del estudiante:	Trabajo personal del estudiante: 45 horas Trabajo en grupos de estudiantes: 22,5 horas
Total horas	112,5 horas.

4.2. Estrategias metodológicas, materiales y recursos didácticos

Clases Presenciales	• Exposiciones en clase, de carácter teórico práctico. • Resolución de problemas. • Análisis y valoración de fuentes primarias y secundarias. • Actividades con ordenador orientadas a consolidar los conceptos presentados previamente, así como a familiarizar al estudiante

	con las herramientas y metodologías de apoyo al estudio de la materia y futuro desempeño profesional. • Presentaciones orales y otras actividades. • Actividades de trabajo en grupo.
Tutorías individuales, grupales y vía web (foro, correo, etc.)	• Resolución de dudas. • Apoyo al aprendizaje autónomo.
Trabajo autónomo	• Lectura crítica de recursos docentes. • Análisis y valoración de fuentes primarias y secundarias. • Resolución de ejercicios, prácticas o casos, de manera individual o colaborativa • Elaboración de trabajos e informes

5. EVALUACIÓN: Procedimientos, criterios de evaluación y de calificación

Procedimientos

El alumno dispone de dos convocatorias, una ordinaria y otra extraordinaria para la superación de la asignatura.

Convocatoria Ordinaria (Evaluación Continua y Evaluación Final)

En la convocatoria ordinaria, se distingues dos posibles vías para la evaluación: Evaluación Continua (EC) y Examen Final (EF). El alumno será evaluado preferentemente mediante el proceso descrito de evaluación continua. Para acogerse al proceso de examen final, el alumno debe solicitarlo por escrito al Director del Máster en las dos primeras semanas de su incorporación, indicando las razones que le impiden seguir el sistema de evaluación continua. El Director del Máster comunicará la resolución en un máximo de 15 días. En caso de no haber recibido respuesta, se considera estimada esta solicitud.

Convocatoria Extraordinaria

La convocatoria extraordinaria consistirá en una prueba similar al examen final.

Instrumentos de evaluación y Criterios de Calificación

Se plantea una evaluación continua del rendimiento del estudiante mediante el seguimiento del trabajo programado y la realización de una prueba parcial a mitad de cuatrimestre, más una prueba de conjunto a realizar al final del semestre.

- Actividades de seguimiento entregables (E): El seguimiento del trabajo del estudiante permite que el profesor conozca el grado de dedicación del estudiante respecto a las distintas actividades propuestas. A su vez, a los estudiantes les sirve para conocer si van alcanzando los objetivos marcados a lo largo del curso. Las actividades de seguimiento podrán plantearse para hacer en clase, o como trabajo personal para el alumno, y podrán temer carácter individual o grupal. Las actividades de seguimiento suponen un 40% de la calificación final.

- Prueba de evaluación Intermedia (PEI): La prueba de Evaluación Intermedia tiene un peso del 30% sobre la calificación final.
- Prueba de Evaluación Final (PEF): La Prueba de Evaluación Final tiene un peso del 30% de la calificación final, y persigue un doble objetivo: evaluar la capacidad de relación de los conceptos aprendidos y revisar los conceptos evaluados en la prueba parcial. Por ello, si se ha obtenido al menos un 20% de calificación en las actividades de seguimiento, la prueba de conjunto permitirá además mejorar la calificación final si se obtiene un resultado superior al obtenido al aplicar la media de todas las calificaciones.

Competencia	Resultado Aprendizaje	Instrumento de Evaluación	Peso en la calificación
CG1, CG2, CB6, CB7, CE5, CE6, CT1, CT3, CT4, CT5	RA1-RA5	E	40%
CG1, CG2, CB6, CB7, CE5, CE6, CT4, CT5	RA1-RA4	PEI	30%
CG1, CG2, CB6, CB7, CE5, CE6, CT4, CT5	RA1-RA4	PEF	30%

Aquellos estudiantes que tengan reconocido el derecho a evaluación final, según fija la normativa de la UAH, deben realizar una prueba de evaluación final (PEF) que incluye cuestiones teóricas y la realización de uno o más ejercicios, con un peso del 60% de la calificación final. Asimismo, deberán entregar un Trabajo de la Asignatura (TA), que se realizará preferentemente en grupo, y que supondrá un 40% de la calificación final.

Competencia	Resultado Aprendizaje	Instrumento de Evaluación	Peso en la calificación
CG1, CG2, CB6, CB7, CE5, CE6, CT4, CT5	RA1-RA4	PEF	60%
CG1, CG2, CB6, CB7, CE5, CE6, CT1, CT3, CT4, CT5	RA1-RA5	TA	40%

La convocatoria extraordinaria plantea una única prueba de evaluación extraordinaria (PEE), que incorpora cuestiones teóricas y la resolución de uno o más ejercicios, con un peso del 70%

de la calificación final. Asimismo, deberán entregar un Trabajo de la Asignatura (TA), que se realizará preferentemente en grupo, y que supondrá un 40% de la calificación final. Para los estudiantes que hayan seguido el proceso de evaluación continua y hayan obtenido al menos un 20% en las actividades de seguimiento, la PEE tendrá un peso del 60%, tomándose el 40% restante de calificación de las actividades de seguimiento.

Competencia	Resultado Aprendizaje	Instrumento de Evaluación	Peso en la calificación
CG1, CG2, CB6, CB7, CE5, CE6, CT1, CT3, CT4, CT5	RA1-RA5	E	40%
CG1, CG2, CB6, CB7, CE5, CE6, CT4, CT5	RA1-RA4	PEE	60%
CG1, CG2, CB6, CB7, CE5, CE6, CT1, CT3, CT4, CT5	RA1-RA5	TA	40%

6. BIBLIOGRAFÍA

Textos recomendados.

- Anderson, Ross. *Security engineering*. John Wiley & Sons, 2008.
- Shostack, Adam. *Threat modeling: Designing for security*. John Wiley & Sons, 2014.
- García Rambla, Juan Luis. "Ataques en redes de datos IPv4 e IPv6.". 0xWord. 2014
- Neil, Ian. *CompTIA Security+ Certification Guide: Master IT security essentials and exam topics for CompTIA Security+ SY0-501 certification*. Packt Publishing Ltd, 2018.
- Himanshu Sharma *Kali Linux - An Ethical Hacker's Cookbook.* Packt Publishing Ltd, 2018.
- Bullock, Jessey, and Jeff T. Parker. *Wireshark for Security Professionals: Using Wireshark and the Metasploit Framework*. John Wiley & Sons, 2017.