Escuela de Doctorado
y Estudios de Posgrado
Universidad de La Laguna

Escuela de Doctorado y Estudios de Posgrado

Máster Universitario en Ciberseguridad e Inteligencia de Datos

GUÍA DOCENTE DE LA ASIGNATURA (ESCENARIO 1):

Seguridad de las Comunicaciones Inalámbricas
(2021 - 2022)

1. Datos descriptivos de la asignatura

Asignatura: Seguridad de las Comunicaciones Inalámbricas	Código: 835871102

- Centro: **Escuela de Doctorado y Estudios de Postgrado**
- Lugar de impartición: **-**
- Titulación: **Máster Universitario en Ciberseguridad e Inteligencia de Datos**
- Plan de Estudios: **2018 (Publicado en 2018-09-19)**
- Rama de conocimiento: **Ingeniería y Arquitectura**
- Itinerario / Intensificación:
- Departamento/s:
  Ingeniería Informática y de Sistemas
- Área/s de conocimiento:
  Ciencia de la Computación e Inteligencia Artificial
- Curso: **1**
- Carácter:
- Duración: **Primer cuatrimestre**
- Créditos ECTS: **3,0**
- Modalidad de impartición: **Semipresencial**
- Horario: **Enlace al horario**
- Dirección web de la asignatura: **http://www.campusvirtual.ull.es**
- Idioma: **Castellano e Inglés (0,15 ECTS en Inglés)**

2. Requisitos para cursar la asignatura

3. Profesorado que imparte la asignatura

Profesor/a Coordinador/a: MARIA CANDELARIA HERNANDEZ GOYA

- Grupo:

General
- Nombre: **MARIA CANDELARIA**
- Apellido: **HERNANDEZ GOYA**
- Departamento: **Ingeniería Informática y de Sistemas**
- Área de conocimiento: **Ciencia de la Computación e Inteligencia Artificial**

Contacto
- Teléfono 1: **922 316 502 Ext 6827**
- Teléfono 2: **922 316 502 Ext 6827**
- Correo electrónico: **mchgoya@ull.es**
- Correo alternativo:
- Web: **http://www.campusvirtual.ull.es**

Tutorías primer cuatrimestre:

Desde	Hasta	Día	Hora inicial	Hora final	Localización	Despacho
Todo el cuatrimestre		Martes	09:30	12:30	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.026
Todo el cuatrimestre		Jueves	09:30	12:30	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.026
Observaciones: La modificaciones de este horario por casusas sobrevenidas se comunicarán a través del campus virtual.						
Tutorías segundo cuatrimestre:						
Desde	**Hasta**	**Día**	**Hora inicial**	**Hora final**	**Localización**	**Despacho**
Todo el cuatrimestre		Miércoles	12:00	14:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.026
Todo el cuatrimestre		Jueves	12:00	14:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.026
		Viernes	10:00	12:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.026
Observaciones: La modificaciones de este horario por casusas sobrevenidas se comunicarán a través del campus virtual.						

Profesor/a: **IGNACIO PELÁEZ PUERTO**
- Grupo:

General
- Nombre: **IGNACIO**
- Apellido: **PELÁEZ PUERTO**
- Departamento: **Ingeniería Informática y de Sistemas**
- Área de conocimiento: **Lenguajes y Sistemas Informáticos**

Contacto
- Teléfono 1:
- Teléfono 2:
- Correo electrónico: **ipelaezp@ull.es**
- Correo alternativo:
- Web: **http://www.campusvirtual.ull.es**

Tutorías primer cuatrimestre:

Desde	Hasta	Día	Hora inicial	Hora final	Localización	Despacho
Todo el cuatrimestre		Lunes	18:00	20:00	Escuela Superior de Ingeniería y Tecnología - Módulo B - AN.4A ESIT	
Todo el cuatrimestre		Miércoles	18:00	20:00	Escuela Superior de Ingeniería y Tecnología - Módulo B - AN.4A ESIT	
Todo el cuatrimestre		Viernes	18:00	20:00	Escuela Superior de Ingeniería y Tecnología - Módulo B - AN.4A ESIT	

Observaciones:

Tutorías segundo cuatrimestre:

Desde	Hasta	Día	Hora inicial	Hora final	Localización	Despacho
Todo el cuatrimestre		Lunes	18:00	20:00	Escuela Superior de Ingeniería y Tecnología - Módulo B - AN.4A ESIT	

Todo el cuatrimestre		Miércoles	18:00	20:00	Escuela Superior de Ingeniería y Tecnología - Módulo B - AN.4A ESIT	
Todo el cuatrimestre		Viernes	18:00	20:00	Escuela Superior de Ingeniería y Tecnología - Módulo B - AN.4A ESIT	
Observaciones:						

4. Contextualización de la asignatura en el plan de estudio

Bloque formativo al que pertenece la asignatura:
Perfil profesional:

5. Competencias

Generales

CG1 - Ser capaces de aplicar los conocimientos adquiridos para resolver problemas en entornos nuevos o poco conocidos dentro de contextos relacionados con seguridad informática o inteligencia de datos
CG2 - Integrar conocimientos para formular juicios a partir de información concreta, y a la vez, incluir reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de esos conocimientos y juicios en materia de asesoramiento en seguridad informática
CG3 - Mantener una actitud de permanente actualización, que les permita estudiar de manera autónoma mediante formación continua en su futuro desempeño profesional como expertos en seguridad informática e inteligencia de datos
CG7 - Desarrollar las capacidades de trabajo en equipo y las habilidades de comunicación para mantener relaciones con otros profesionales y con organizaciones relevantes
CG8 - Tener la capacidad analítica y de resolución para atender a los problemas reales de acuerdo con los valores éticos y sociales y con el máximo respeto a la legalidad vigente
CG9 - Manejar adecuadamente información relativa al sector de la seguridad informática atendiendo a la legislación vigente, estándares, certificaciones, documentos internos, etc.

Básicas

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
CB9 - Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

CB10 - Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo

Específicas

CE1 - Capacidad de seleccionar y aplicar adecuadamente diferentes mecanismos de cifrado y autenticación para garantizar la confidencialidad, integridad y autenticidad de los datos
CE2 - Capacidad de verificar el funcionamiento correcto de las medidas de seguridad, y el cumplimiento de las normas y las leyes que corresponden
CE5 - Conocimiento de sistemas de detección y prevención de intrusos en redes cableadas e inalámbricas

6. Contenidos de la asignatura

Contenidos teóricos y prácticos de la asignatura

Tema 1: Seguridad en redes inalámbricas de área extensa (Wireless Wide Area Networks, WWAN: GSM, UMTS, LTE)
Tema 2: Seguridad en Redes Inalámbricas de Área Local (Wireless Local Area Networks, WLAN: IEEE 802.11)
Tema 3: Seguridad en la Internet de las Cosas (BLE, NFC, etc.)

Actividades a desarrollar en otro idioma

En esta asignatura se impartirán 1,5 horas de clases en inglés.
Además se trabajará preferentemente sobre bibliografía en inglés y el alumnado deberá ser capaz de extraer la información necesaria para seguir la asignatura a partir de dicha documentación, junto con los apuntes del profesorado.

7. Metodología y volumen de trabajo del estudiante

Descripción

La metodología docente de las clases teóricas consistirá en sesiones en las que el profesorado explicará los conceptos fundamentales de cada tema que deben ser asimilados por el alumnado, bien presencialmente, o no presencialmente
mediante retransmisión online, en directo usando videoconferencia o en diferido a través de grabaciones colgadas en el entorno virtual.
La metodología docente de las clases prácticas consistirá en sesiones supervisadas en grupos reducidos en el laboratorio en las que se realizarán diversas prácticas informáticas de dificultad creciente aplicando los conceptos expuestos en las clases de teoría. Además, el alumnado aprenderá a usar diversas herramientas, en entornos reales o de simulación, así como metodologías relacionadas con el contexto de la materia.
La metodología docente de los informes consistirá en el desarrollo por parte del alumnado de su capacidad para la aplicación de los conocimientos adquiridos y la resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios y multidisciplinares, siendo capaces de integrar estos conocimientos.
Se plantea una metodología docente para los seminarios que consistirá en sesiones donde se llevará a cabo una explicación más detallada de determinados aspectos concretos de algunos temas teóricos o prácticos especialmente relevantes. Se

ofrecerán seminarios donde profesionales de esta materia harán charlas debates con el alumnado de los temas relacionados con el mundo profesional.
Las tutorías individuales ayudarán a reforzar los diferentes aspectos de la materia y ayudarán al alumnado en la comprensión de la teoría y la realización de las prácticas.

Actividades formativas en créditos ECTS, su metodología de enseñanza-aprendizaje y su relación con las competencias que debe adquirir el estudiante

Actividades formativas	Horas presenciales	Horas de trabajo autónomo	Total horas	Relación con competencias
Clases teóricas	5,00	5,00	10,0	[CG3], [CB10], [CE1], [CE2], [CE5]
Clases prácticas (aula / sala de demostraciones / prácticas laboratorio)	8,00	8,00	16,0	[CG1], [CG2], [CG3], [CG7], [CG8], [CB7], [CE1], [CE2], [CE5]
Realización de seminarios u otras actividades complementarias	1,00	1,00	2,0	[CG1], [CG2], [CG3], [CG8], [CB7], [CE1], [CE2], [CE5]
Estudio/preparación de clases teóricas	0,00	10,00	10,0	[CG9], [CB10], [CE1], [CE2], [CE5]
Estudio/preparación de clases prácticas	0,00	6,00	6,0	[CG1], [CG2], [CG3], [CG8], [CG9], [CB7], [CB10], [CE1]
Realización de exámenes	1,00	0,00	1,0	[CG1], [CG2], [CG9], [CB7], [CE1], [CE2], [CE5]
Asistencia a tutorías	0,00	6,00	6,0	[CG1], [CG2], [CE1], [CE2], [CE5]
Informes, trabajos y proyectos	0,00	24,00	24,0	[CG1], [CG2], [CG3], [CG7], [CG9], [CB9], [CE1], [CE2], [CE5]
Total horas	15,00	60,00	75,00	
		Total ECTS	3,00	

8. Bibliografía / Recursos

Bibliografía Básica

Jyrki T. J. Penttinen, Wireless Communications Security: Solutions for the Internet of Things, 978-1-119-08439-6, Wiley

José Picó García y David Pérez Conde,Hacking y Seguridad en comunicaciones móviles GSM / GPRS / UMTS / LTE. 2ª Edición. Revisada y ampliada, 978-84-616-9195-1, 0xWord

Bibliografía Complementaria

Maurizio Martellini, Stanislav Abaimov, Sandro Gaycken, Clay Wilson, Information Security of Highly Critical Wireless Networks, 978-3-319-52905-9, Springer

Otros Recursos

9. Sistema de evaluación y calificación

Descripción

La evaluación de la teoría contribuirá a la evaluación de la asignatura con un 40%, mientras que la evaluación de la práctica lo hará con un 60%.
Las herramientas utilizadas en la evaluación continua serán las siguientes.
La Calificación de Teoría (CT) se obtendrá mediante pruebas escritas (40%), mientras que la Calificación de Prácticas (CP) se obtendrá con Informes memorias de prácticas (20%) + seminarios con tareas reales y/o simuladas (20%) + trabajos y proyectos (20%).
Ambas calificaciones serán valores entre 0 y 10, de forma que la Calificación Final (CF) se obtendrá mediante la fórmula: CF= 0,40*CT + 0,60*CP, si y solo si CT>=5 y CP>=5. En otro caso, CF= min(CT, CP)
El alumnado que no supere la evaluación continua podrá realizar en las diferentes convocatorias pruebas de evaluación destinadas exclusivamente a evaluar las mismas competencias y resultados de aprendizaje de la asignatura.
La Evaluación de la asignatura se rige por el Reglamento de Evaluación y Calificación de la Universidad de La Laguna (BOC de 19 de enero de 2016), o el que la Universidad tenga vigente, además de por lo establecido en la Memoria de Verificación inicial o posteriores modificaciones.
En cumplimiento de lo establecido en el Reglamento de Evaluación y Calificación de la Universidad de La Laguna, al alumnado podrá conocer, y en su caso revisar, las calificaciones de las actividades evaluables integradas en la evaluación continua con anterioridad al último día lectivo del cuatrimestre correspondiente o, en el caso de no existir una prueba final, antes de que las calificaciones finales adquieran el carácter de definitivas.

Estrategia Evaluativa

Tipo de prueba	Competencias	Criterios	Ponderación
Pruebas objetivas	[CG3], [CB9], [CB10], [CE1], [CE2], [CE5]	• Adecuación a lo solicitado • Calidad del trabajo desarrollado • Concreción en la redacción • Nivel de conocimientos adquiridos	40,00 %

Trabajos y proyectos	[CG1], [CG2], [CG3], [CG7], [CG8], [CG9], [CB7], [CB10], [CE1], [CE2], [CE5]	• Adecuación a lo solicitado • Calidad del trabajo desarrollado • Concreción en la redacción • Interés demostrado • Nivel de aplicabilidad • Nivel de conocimientos adquiridos	20,00 %
Informes memorias de prácticas	[CG7], [CE1], [CE2], [CE5]	• Adecuación a lo solicitado • Calidad del trabajo desarrollado • Concreción en la redacción • Nivel de conocimientos adquiridos • Participación activa	20,00 %
Pruebas de ejecuciones de tareas reales y/o simuladas	[CG7], [CB7], [CE1], [CE2], [CE5]	• Adecuación a lo solicitado • Calidad del trabajo desarrollado • Interés demostrado • Nivel de aplicabilidad • Nivel de conocimientos adquiridos • Participación activa	20,00 %

10. Resultados de Aprendizaje

Al finalizar la asignatura el alumnado debe ser capaz de: demostrar conocimiento de los principales conceptos relacionados con las propiedades de seguridad en redes inalámbricas, mecanismos, protocolos y aplicaciones usados actualmente, y de relacionar sus conocimientos con los problemas de seguridad de red en escenarios reales.

11. Cronograma / calendario de la asignatura

Descripción

Debido al carácter semipresencial del máster, está previsto que las clases presenciales se desarrollen de la forma siguiente: el alumnado tendrá 3 horas diarias las semanas 1 a 5 y 8 a 12 del primer cuatrimestre, y 3 o 4 horas diarias las semanas 1 a 5 del segundo cuatrimestre. Todas las asignaturas se desarrollarán en bimestres, y concretamente esta asignatura se impartirá en el bimestre 2. El cronograma que se presenta es a título estimativo, de modo que el profesorado podrá modificar dicha planificación temporal si así lo demanda el desarrollo de la asignatura.

Primer cuatrimestre					
Semana	**Temas**	**Actividades de enseñanza aprendizaje**	**Horas de trabajo presencial**	**Horas de trabajo autónomo**	**Total**

Semana 8:	Tema 1: Seguridad en redes inalámbricas de área extensa (Wireless Wide Area Networks, WWAN: GSM, UMTS, LTE)	Clases teóricas y prácticas y seminarios presenciales.	2.00	2.00	4.00
Semana 9:	Tema 1: Seguridad en redes inalámbricas de área extensa (Wireless Wide Area Networks, WWAN: GSM, UMTS, LTE)	Clases teóricas y prácticas y seminarios presenciales. Actividades con material disponible en el aula virtual.	3.00	7.00	10.00
Semana 10:	Tema 2: Seguridad en Redes Inalámbricas de Área Local (Wireless Local Area Networks, WLAN: IEEE 802.11)	Clases teóricas y prácticas y seminarios presenciales. Actividades con material disponible en el aula virtual.	3.00	7.00	10.00
Semana 11:	Tema 2: Seguridad en Redes Inalámbricas de Área Local (Wireless Local Area Networks, WLAN: IEEE 802.11)	Clases teóricas y prácticas y seminarios presenciales. Actividades con material disponible en el aula virtual.	3.00	7.00	10.00
Semana 12:	Tema 3: Seguridad en la Internet de las Cosas (BLE, NFC, etc.)	Clases teóricas y prácticas y seminarios presenciales. Actividades con material disponible en el aula virtual.	3.00	7.00	10.00
Semana 13:	Tema 1: Seguridad en redes inalámbricas de área extensa (Wireless Wide Area Networks, WWAN: GSM, UMTS, LTE)	Actividades con material disponible en el aula virtual. Seminarios utilizando el campus virtual y realización de cuestionarios on-line. Videotutoriales y foro para la resolución de dudas.	0.00	10.00	10.00
Semana 14:	Tema 2: Seguridad en Redes Inalámbricas de Área Local (Wireless Local Area Networks, WLAN: IEEE 802.11)	Actividades con material disponible en el aula virtual. Seminarios utilizando el campus virtual y realización de cuestionarios on-line. Videotutoriales y foro para la resolución de dudas.	0.00	10.00	10.00

Semana 15:	Tema 3: Seguridad en la Internet de las Cosas (BLE, NFC, etc.). Evaluación	Actividades con material disponible en el aula virtual. Seminarios utilizando el campus virtual y realización de cuestionarios on-line. Videotutoriales y foro para la resolución de dudas. Evaluación del alumnado	0.00	10.00	10.00
Semana 16 a 18:	Evaluación	Evaluación del alumnado	1.00	0.00	1.00
		Total	15.00	60.00	75.00