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 :

Seguridad de las Comunicaciones por Internet
(2022 - 2023)

1. Datos descriptivos de la asignatura

Asignatura: Seguridad de las Comunicaciones por Internet	Código: 835871103

- 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:
  Arquitectura y Tecnología de Computadores
  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: HECTOR JAVIER REBOSO MORALES

- Grupo:

General
- Nombre: **HECTOR JAVIER**
- Apellido: **REBOSO MORALES**
- Departamento: **Ingeniería Informática y de Sistemas**
- Área de conocimiento: **Arquitectura y Tecnología de Computadores**

Contacto
- Teléfono 1:
- Teléfono 2:
- Correo electrónico: **hreboso@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		Miércoles	17:00	19:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.042
Todo el cuatrimestre		Viernes	15:00	17:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.042
Observaciones:						
Tutorías segundo cuatrimestre:						
Desde	**Hasta**	**Día**	**Hora inicial**	**Hora final**	**Localización**	**Despacho**
Todo el cuatrimestre		Miércoles	17:00	19:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.042
Todo el cuatrimestre		Viernes	15:00	19:00	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.042
Observaciones:						

Profesor/a: **JEZABEL MIRIAM MOLINA GIL**

- Grupo:

General
- Nombre: **JEZABEL MIRIAM**
- Apellido: **MOLINA GIL**
- Departamento: **Ingeniería Informática y de Sistemas**
- Área de conocimiento: **Ciencia de la Computación e Inteligencia Artificial**

Contacto
- Teléfono 1: **ext. 6686**
- Teléfono 2:
- Correo electrónico: **jmmolina@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	P2.022
Todo el cuatrimestre		Miércoles	10:30	13:30	Escuela Superior de Ingeniería y Tecnología - Módulo A - AN.4A ESIT	P2.022

Observaciones: El horario y lugar de tutorías es orientativo y prevalecerá la información que aparezca en el aula virtual de la asignatura. Se establecerá un sistema de cita previa para las tutorías.

Tutorías segundo cuatrimestre:

Desde	Hasta	Día	Hora inicial	Hora final	Localización	Despacho
30-01-2023	11-05-2023	Miércoles	14:30	16:30	Escuela Superior de Ingeniería y Tecnología - AN.4A ESIT	P2.022
30-01-2023	11-05-2023	Jueves	11:30	13:30	Escuela Superior de Ingeniería y Tecnología - AN.4A ESIT	P2.022
30-01-2022	11-05-2023	Jueves	14:30	16:30	Escuela Superior de Ingeniería y Tecnología - AN.4A ESIT	P2.022

11-05-2023	29-07-2023	Miércoles	09:30	12:30	Escuela Superior de Ingeniería y Tecnología - AN.4A ESIT	P2.022
11-05-2023	29-07-2023	Jueves	09:30	12:30	Escuela Superior de Ingeniería y Tecnología - AN.4A ESIT	P2.022
Observaciones: El horario y lugar de tutorías es orientativo y prevalecerá la información que aparezca en el aula virtual de la asignatura. Se establecerá un sistema de cita previa para las tutorías.						

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
CG4 - Diseñar y elaborar planes de intervención profesional o proyectos de investigación relacionados con el entorno de seguridad informática, e implementarlos y desarrollarlos mediante los métodos y procesos adecuados
CG5 - Adquirir el grado de especialización necesario para ejercer las funciones profesionales de experto en seguridad informática e inteligencia de datos, en el seno de entidades de TIC

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

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

Tema1. Necesidad de seguridad en entornos de red;

- Riesgos e impacto de ataques;
- Ataque por denegación de servicios;

Tema2. Mecanismos de protección;

- Cortafuegos
- SIEM

Tema3. Aplicación del Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica sobre las conexiones por Internet.

Tema 4. Políticas y actuaciones de seguridad.
Tema 5. Seguridad en servicios web;

- TLS/SSL;
- HTTPS;

Tema 6. Redes Privadas Virtuales;

- IPSec;

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, juntos 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	[CE5], [CE2], [CE1], [CG2], [CG1]
Clases prácticas (aula / sala de demostraciones / prácticas laboratorio)	8,00	8,00	16,0	[CE5], [CE2], [CE1], [CB7], [CG5], [CG1]
Realización de seminarios u otras actividades complementarias	1,00	1,00	2,0	[CE5], [CG2]
Estudio/preparación de clases teóricas	0,00	10,00	10,0	[CE5], [CE2], [CE1], [CG2], [CG1]
Estudio/preparación de clases prácticas	0,00	6,00	6,0	[CE5], [CE2], [CE1], [CB7], [CG5], [CG1]
Realización de exámenes	1,00	0,00	1,0	[CE5], [CB7], [CG1]
Asistencia a tutorías	0,00	6,00	6,0	[CE5], [CE2], [CE1], [CG2], [CG1]
Informes, trabajos y proyectos	0,00	24,00	24,0	[CE5], [CE2], [CE1], [CB7], [CG5], [CG4], [CG2], [CG1]
Total horas	15,00	60,00	75,00	
		Total ECTS	3,00	

8. Bibliografía / Recursos

Bibliografía Básica

Autor: Stewart, James Michael.
Título: Network security, firewalls, and VPNs / J. Michael Stewart.
Editorial: Sudbury, Mass. : Jones & Bartlett Learning, cop. 2011.

Bibliografía Complementaria

Autor: García Rambla, Juan Luis.
Título: Ataques en redes de datos IPv4 e IPv6 / Juan Luis García Rambla ; colaboración de Chema Alonso en el capítulo V.
Edición: 2ª ed.
Editorial: Móstoles (Madrid) : ZeroxWord computing, 2014.

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 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.

Estrategia Evaluativa

Tipo de prueba	Competencias	Criterios	Ponderación
Pruebas objetivas	[CE5], [CG2], [CG1]	Calidad del trabajo desarrollado Concreción en la redacción Nivel de aplicabilidad Nivel de conocimientos adquiridos Adecuación a lo solicitado	40,00 %
Trabajos y proyectos	[CE5], [CE2], [CE1], [CB7]	Calidad del trabajo desarrollado Concreción en la redacción Nivel de aplicabilidad Nivel de conocimientos adquiridos Adecuación a lo solicitado	20,00 %

Informes memorias de prácticas	[CE5], [CE2], [CE1], [CB7], [CG5]	Calidad del trabajo desarrollado Concreción en la redacción Nivel de aplicabilidad Nivel de conocimientos adquiridos Adecuación a lo solicitado	20,00 %
Pruebas de ejecuciones de tareas reales y/o simuladas	[CE2], [CE1], [CG4]	Calidad del trabajo desarrollado Concreción en la redacción Interés demostrado Nivel de aplicabilidad Nivel de conocimientos adquiridos Participación activa Adecuación a lo solicitado	20,00 %

10. Resultados de Aprendizaje

Al finalizar la asignatura el alumnado debe: entender las vulnerabilidad de seguridad que existen en las comunicaciones por internet, conocer las posibles vulnerabilidades en los sistemas de comunicación y las redes, manejar los diferentes mecanismos de protección y prevención de riesgos para evitar y proteger los sistemas frente a vulnerabilidad, conocer los diferentes protocolos, sistemas y estándares relacionados con la seguridad informática, y conocer las diferentes políticas, actuaciones e iniciativas de seguridad vigentes y hacer uso de ellas.

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:	1,	Clases teóricas y prácticas y seminarios presenciales.	2.00	2.00	4.00
Semana 9:	1 y 2	Clases teóricas y prácticas y seminarios presenciales.	3.00	7.00	10.00

Semana 10:	2	Clases teóricas y prácticas y seminarios presenciales. Actividades con material disponible en el aula virtual.	3.00	7.00	10.00
Semana 11:	5	Clases teóricas y prácticas y seminarios presenciales. Actividades con material disponible en el aula virtual.	3.00	7.00	10.00
Semana 12:	5 y 6	Clases teóricas y prácticas y seminarios presenciales. Actividades con material disponible en el aula virtual.	3.00	7.00	10.00
Semana 13:	6	Actividades con material disponible en el aula virtual. Seminarios utilizando el campus virtual y realización de cuestionarios on-line. Vídeotutoriales y foro para la resolución de dudas.	0.00	10.00	10.00
Semana 14:	3 y 4	Actividades con material disponible en el aula virtual. Seminarios utilizando el campus virtual y realización de cuestionarios on-line. Vídeotutoriales y foro para la resolución de dudas.	0.00	10.00	10.00
Semana 15:	3 y 4	Actividades con material disponible en el aula virtual. Seminarios utilizando el campus virtual y realización de cuestionarios on-line. Vídeotutoriales y foro para la resolución de dudas.	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