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 0):

### Hacking Ético y Análisis Forense
### (2021 - 2022)

## 1. Datos descriptivos de la asignatura

| Asignatura: Hacking Ético y Análisis Forense | Código: 835871203 |
|---|---|

- 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: **Segundo 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: CANDIDO CABALLERO GIL**

- Grupo:

**General**
- Nombre: **CANDIDO**
- Apellido: **CABALLERO GIL**
- Departamento: **Ingeniería Informática y de Sistemas**
- Área de conocimiento: **Arquitectura y Tecnología de Computadores**

**Contacto**
- Teléfono 1: **922 319191**
- Teléfono 2:
- Correo electrónico: **ccabgil@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 | 09:30 | 13:30 | Escuela Superior de Ingeniería y Tecnología - Módulo C - AN.4A ESIT | P2.104 |
| Todo el cuatrimestre | | Viernes | 09:30 | 11:30 | Escuela Superior de Ingeniería y Tecnología - Módulo C - AN.4A ESIT | Online |
| Observaciones: Las dos horas de tutoría de los viernes serán online debido a la participación en el Programa de Apoyo a la Docencia Presencial mediante Herramientas TIC, modalidad B Tutorías Online. Para llevar a cabo la tutoría online, usaremos la herramienta Hangouts con el usuario ccabgil@ull.edu.es Este horario es orientativo. Prevalecerá el que se ponga en las aulas virtuales de las asignaturas. | | | | | | |
| **Tutorías segundo cuatrimestre:** | | | | | | |
| **Desde** | **Hasta** | **Día** | **Hora inicial** | **Hora final** | **Localización** | **Despacho** |
| Todo el cuatrimestre | | Miércoles | 09:30 | 13:30 | Escuela Superior de Ingeniería y Tecnología - Módulo C - AN.4A ESIT | P2.104 |
| Todo el cuatrimestre | | Viernes | 09:30 | 11:30 | Escuela Superior de Ingeniería y Tecnología - Módulo C - AN.4A ESIT | Online |
| Observaciones: Las dos horas de tutoría de los viernes serán online debido a la participación en el Programa de Apoyo a la Docencia Presencial mediante Herramientas TIC, modalidad B Tutorías Online. Para llevar a cabo la tutoría online, usaremos la herramienta Hangouts con el usuario ccabgil@ull.edu.es Este horario es orientativo. Prevalecerá el que se ponga en las aulas virtuales de las asignaturas. | | | | | | |

| **Profesor/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.

## 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
**CG6** - Evaluar los recursos necesarios, planificar y organizar las actividades, sin olvidar la continua revisión del proceso que conlleva la seguridad informática y la inteligencia de datos
**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
**CB8** - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios
**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

**CE3** - Capacidad de aplicación de metodologías y herramientas para el análisis, evaluación y gestión de riesgos, y de realización de auditorías informáticas

**CE5** - Conocimiento de sistemas de detección y prevención de intrusos en redes cableadas e inalámbricas
**CE6** - Capacidad de detección y evaluación de vulnerabilidades que afectan a los sistemas informáticos y de aplicación de técnicas y herramientas de análisis forense

## 6. Contenidos de la asignatura

### Contenidos teóricos y prácticos de la asignatura

Profesores: Candelaria Hernández Goya y Cándido Caballero Gil

Temas:
1. Modelos de seguridad y vulnerabilidades.
2. Detección de agujeros de seguridad.
3. Detección de intrusos.
4. Tests de penetración.
5. Auditoría del sistema operativo.
6. Gestión de incidentes.
7. Ingeniería inversa aplicada a la seguridad.
8. Marco de buenas prácticas.
9. Introducción al análisis forense y sus procedimientos.
10. Adquisición y análisis de evidencias.
11. Tendencias en análisis forense.

### 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 las asignaturas 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** de laboratorio 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, trabajos y proyectos** 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.

•En los **seminarios y otras actividades complementarias** se plantea una metodología docente 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], [CB10], [CB8], [CG9], [CG2] |
| Clases prácticas (aula / sala de demostraciones / prácticas laboratorio) | 8,00 | 8,00 | 16,0 | [CE6], [CE3], [CB10], [CB8], [CB7], [CG8], [CG6], [CG1] |
| Realización de seminarios u otras actividades complementarias | 1,00 | 1,00 | 2,0 | [CB8] |
| Estudio/preparación de clases teóricas | 0,00 | 10,00 | 10,0 | [CE5], [CB10], [CB8], [CG9], [CG2] |
| Estudio/preparación de clases prácticas | 0,00 | 6,00 | 6,0 | [CG8], [CG6], [CG2], [CG1] |
| Realización de exámenes | 1,00 | 0,00 | 1,0 | [CE6], [CE3], [CB7], [CG8], [CG1] |
| Asistencia a tutorías | 0,00 | 6,00 | 6,0 | [CE6], [CE3], [CB8], [CB7], [CG1] |
| Informes, trabajos y proyectos | 0,00 | 24,00 | 24,0 | [CE6], [CE3], [CB8], [CB7], [CG8], [CG2], [CG1] |
| Total horas | 15,00 | 60,00 | 75,00 | |
| | | Total ECTS | 3,00 | |

## 8. Bibliografía / Recursos

### Bibliografía Básica

García-Moran, Jean Paul. Hacking Y Seguridad En Internet. Paracuellos De Jarama, Madrid: Ra-ma, 2011. Print.

Zemánek, Jakub. Cracking Sin Secretos : Ataque Y Defensa De Software. Madrid: Ra-Ma, 2004. Print.

Redondo Gil, Juan José, Universitat Politècnica De Catalunya. Departament D'Enginyeria Telemàtica, and Muñoz Tapia, José Luis. "Herramientas Para Hacking ético; Ethical Hacking Tools; Eines per Hacking ètic." Web.

### Bibliografía Complementaria

Analyzing Computer Security
Charles P. Pfleeger ; Shari Lawrence Pfleeger 25 August 2011

### Otros Recursos

Mastering Wireshark
Charit Mishra 30 March 2016

HACKING ÉTICO 101: Como Hackear Profesionalmente en 21 Días o Menos

Iniesta Archidona, Miguel, Oltra Gutiérrez, Juan Vicente, and Universitat Politècnica De València. Escola Tècnica Superior D'Enginyeria Informàtica.
Seguridad WIFI. Agresiones Posibles
(2010). Web
https://riunet.upv.es/handle/10251/8596

## 9. Sistema de evaluación y calificación

### Descripción

La evaluación de la teoría contribuirá a la evaluación de la asignatura con un 50%, mientras que la evaluación de la práctica lo hará con un 50%.
A continuación se enumeran las herramientas utilizadas en la evaluación continua:
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 (10%).

Ambas calificaciones serán valores entre 0 y 10, de forma que la Calificación Final (CF) se obtendrá mediante la fórmula: CF= 0,50*CT + 0,50*CP, si y solo si CT>=5 y CP>=5. En otro caso, CF= min(CT, CP)

El alumnado que no haya superado la evaluación continua podrán realizar en las diferentes convocatorias pruebas de evaluación alternativa adicionales destinadas exclusivamente a evaluar las mismas competencias / resultados de aprendizaje

de la asignatura.

**Estrategia Evaluativa**

| Tipo de prueba | Competencias | Criterios | Ponderación |
|---|---|---|---|
| Pruebas objetivas | [CE6], [CE5], [CB8], [CG9], [CG8], [CG2], [CG1] | • Adecuación a lo solicitado<br>• Calidad del trabajo desarrollado<br>• Concreción en la redacción<br>• Interés demostrado<br>• Nivel de aplicabilidad<br>• Nivel de conocimientos adquiridos<br>• Participación activa | 50,00 % |
| Trabajos y proyectos | [CE6], [CE3], [CB10], [CB8], [CB7], [CG8], [CG6] | • Adecuación a lo solicitado<br>• Concreción en la redacción<br>• Asistencia Activa e interés demostrado<br>• Nivel de conocimientos adquiridos | 20,00 % |
| Informes memorias de prácticas | [CB7], [CG9], [CG6], [CG2] | • Adecuación a lo solicitado<br>• Concreción en la redacción<br>• Asistencia Activa e interés demostrado<br>• Nivel de conocimientos adquiridos | 20,00 % |
| Pruebas de ejecuciones de tareas reales y/o simuladas | [CE6], [CE3], [CB8], [CB7], [CG8], [CG6] | • Adecuación a lo solicitado<br>• Asistencia activa e interés demostrado<br>• Nivel de conocimientos adquiridos<br>• Nivel de aplicabilidad | 10,00 % |

## 10. Resultados de Aprendizaje

Al finalizar la asignatura, el alumnado será capaz de planificar, dirigir, coordinar y gestionar en los ámbitos de la seguridad informática y prevención de ataques: caracterizando modelos de seguridad relacionados con el control de acceso, identificando arquitecturas de seguridad de los sistemas operativos actuales, entendiendo la importancia de definir una política de seguridad dentro del sistema, conociendo los mecanismos del lenguaje de política de seguridad que permiten seguridad Multinivel y seguridad condicional, saber escribir módulos de política de seguridad para un sistema, conocer los procesos y herramientas necesarias para identificar los problemas de seguridad que existan en un sistema, identificar la importancia del análisis forense en el contexto actual, identificar las técnicas utilizadas para recolectar, analizar y presentar evidencias, identificar los pasos necesarios para la construcción de software seguro, e identificar los usos de la ingeniería inversa desde el punto de vista de la seguridad del sistema con objeto de poder detectar problemas y detener posibles ataques.

## 11. Cronograma / calendario de la asignatura

**Descripción**

Debido al carácter semipresencial del máster, está previsto que las claves presenciales se desarrollen de la forma siguiente: el alumnado tendrá 3 horas diarias las semanas 1 a 5 y 8 a 12, y 3 o 4 horas diarias las semanas 16 a 20.
Todas las asignaturas se desarrollarán en bimestres, y concretamente esta asignatura se impartirá en el bimestre 3.
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.

| Segundo cuatrimestre | | | | | |
|---|---|---|---|---|---|
| Semana | Temas | Actividades de enseñanza aprendizaje | Horas de trabajo presencial | Horas de trabajo autónomo | Total |
| Semana 1: | 1 y 2 | Clases teóricas y prácticas y seminarios presenciales. | 2.00 | 2.00 | 4.00 |
| Semana 2: | 3 y 4 | Clases teóricas y prácticas y seminarios presenciales.<br>Actividades con material disponible en el aula virtual. | 3.00 | 7.00 | 10.00 |
| Semana 3: | 5 y 6 | Clases teóricas y prácticas y seminarios presenciales.<br>Actividades con material disponible en el aula virtual. | 3.00 | 7.00 | 10.00 |
| Semana 4: | | 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. | 3.00 | 10.00 | 13.00 |
| Semana 5: | 7 y 8 | Clases teóricas y prácticas y seminarios presenciales.<br>Actividades con material disponible en el aula virtual. | 3.00 | 7.00 | 10.00 |
| Semana 6: | 9, 10 y 11 | Clases teóricas y prácticas y seminarios presenciales.<br>Actividades con material disponible en el aula virtual. | 0.00 | 7.00 | 7.00 |
| Semana 7: | | 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 8: | | 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 9: | | | 0.00 | 0.00 | 0.00 |
| Semana 16 a 18: | Evaluación | Evaluación del alumnado | 1.00 | 0.00 | 1.00 |
| | | Total | 15.00 | 60.00 | 75.00 |