



## Guía docente

| Guia docente          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                    |                                 |           |
|-----------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------|---------------------------------|-----------|
| Datos Identificativos |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                    |                                 | 2022/23   |
| Asignatura (*)        | Análisis Forense de Equipos                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |                    | Código                          | 614530012 |
| Titulación            | Máster Universitario en Ciberseguridade                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |                    |                                 |           |
| Descriptores          |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                    |                                 |           |
| Ciclo                 | Periodo                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              | Curso              | Tipo                            | Créditos  |
| Máster Oficial        | 2º cuatrimestre                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Primero            | Optativa                        | 3         |
| Idioma                | CastellanoGallego                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |                    |                                 |           |
| Modalidad docente     | Presencial                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                    |                                 |           |
| Prerrequisitos        |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                    |                                 |           |
| Departamento          | Ciencias da Computación e Tecnoloxías da InformaciónComputación                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |                    |                                 |           |
| Coordinador/a         | Vázquez Naya, José Manuel                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Correo electrónico | jose.manuel.vazquez.naya@udc.es |           |
| Profesorado           | Vázquez Naya, José Manuel                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            | Correo electrónico | jose.manuel.vazquez.naya@udc.es |           |
| Web                   | moovi.uvigo.es                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |                    |                                 |           |
| Descripción general   | <p>El análisis forense de equipos consiste en la aplicación de técnicas científicas y analíticas para identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.</p> <p>La materia "Análisis Forense de Equipos" tiene una fuerte componente práctica. Se comenzará con una introducción a este campo, explicando conceptos clave. A continuación, se estudiarán fundamentos y metodologías de análisis forense desde un punto de vista genérico y aplicable a nuevos casos, pero también se estudiarán ejemplos concretos basados en casos reales.</p> <p>En las prácticas de laboratorio el/la alumno/a aprenderá a manejar diferentes herramientas de análisis forense y realizará prácticas simulando problemas reales.</p> |                    |                                 |           |

## Competencias / Resultados del título

| Código | Competencias / Resultados del título                                                                                                                                                                                                                                                                         |
|--------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| A6     | CE6 - Desarrollar y aplicar métodos de investigación forense para el análisis de incidentes o riesgos de ciberseguridad                                                                                                                                                                                      |
| B1     | CB1 - Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y aplicación de ideas, a menudo en un contexto de investigación                                                                                                                                |
| B2     | CB2 - 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                                                                |
| B3     | CB3 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formar 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 |
| B7     | CG2 - Resolución de problemas. Tener capacidad de resolver, con los conocimientos adquiridos, problemas específicos del ámbito técnico de la seguridad de la información, las redes y/o los sistemas de comunicaciones                                                                                       |
| C4     | CT4 - Valorar la importancia de la seguridad de la información en el avance socioeconómico de la sociedad                                                                                                                                                                                                    |

## Resultados de aprendizaje

| Resultados de aprendizaje                                                                                                                                                             | Competencias / Resultados del título |            |     |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|------------|-----|
| Conocimiento de las metodologías adecuadas para la realización de trabajos forenses con validez legal                                                                                 | AP6                                  | BP1        | CP4 |
| Capacidad para la realización de análisis forense de los diferentes elementos que forman un sistema de información, en múltiples plataformas y sistemas operativos                    | AP6                                  | BP2<br>BP7 | CP4 |
| Capacidad para generar informes como resultado del análisis forense claros, concisos e inteligibles tanto por expertos como por personas ajenas al ámbito de la seguridad informática | AP6                                  | BP3<br>BP7 | CP4 |

## Contenidos

| Tema | Subtema |
|------|---------|
|      |         |



|                                                      |                                                                                            |
|------------------------------------------------------|--------------------------------------------------------------------------------------------|
| 1. Introducción al análisis forense                  | Introducción<br>Fundamentos<br>Normativa<br>Clonado                                        |
| 2. Análisis Forense en Windows                       | Artefactos<br>Memoria<br>Herramientas<br>Aspectos avanzados de análisis forense en Windows |
| 3. Análisis Forense en Mac OS                        | Artefactos<br>Memoria<br>Herramientas<br>Aspectos avanzados de análisis forense en Mac OS  |
| 4. Análisis Forense en dispositivos móviles: Android | Artefactos<br>Herramientas<br>Aspectos avanzados de análisis forense en Android            |
| 5. Análisis Forense en dispositivos móviles: iOS     | Artefactos<br>Herramientas<br>Aspectos avanzados de análisis forense en iOS                |

| Planificación                                                                                                                      |                           |                                           |                        |               |
|------------------------------------------------------------------------------------------------------------------------------------|---------------------------|-------------------------------------------|------------------------|---------------|
| Metodologías / pruebas                                                                                                             | Competencias / Resultados | Horas lectivas (presenciales y virtuales) | Horas trabajo autónomo | Horas totales |
| Sesión magistral                                                                                                                   | A6 C4                     | 11                                        | 22                     | 33            |
| Prácticas de laboratorio                                                                                                           | A6 B1 B2 B3 B7 C4         | 10                                        | 20                     | 30            |
| Prueba objetiva                                                                                                                    | A6 B1 B2 B3 B7 C4         | 2                                         | 0                      | 2             |
| Atención personalizada                                                                                                             |                           | 10                                        | 0                      | 10            |
| (*) Los datos que aparecen en la tabla de planificación són de carácter orientativo, considerando la heterogeneidad de los alumnos |                           |                                           |                        |               |

| Metodologías             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|--------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Metodologías             | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Sesión magistral         | Clases expositivas de presentación de los conocimientos teóricos de cada uno de los temas. Se fomentará la participación del alumnado.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Prácticas de laboratorio | Sesiones prácticas en ordenador, en las que se deben resolver una serie de boletines de ejercicios prácticos propuestos por el profesor. Los ejercicios buscan consolidar los conocimientos presentados en las sesiones magistrales y también fomentar el aprendizaje autónomo del alumno.<br>Una vez completado el boletín de ejercicios, el profesor evaluará el trabajo realizado por el alumno mediante una sesión de trabajo en ordenador.<br>Los boletines de ejercicios se publicarán a través de la plataforma de formación del máster. Se impondrá una fecha máxima de defensa para cada boletín, con el objetivo de fomentar el estudio continuo. |
| Prueba objetiva          | Prueba mediante la que se valorarán los conocimientos y capacidades adquiridos por el alumno.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |

| Atención personalizada   |                      |
|--------------------------|----------------------|
| Metodologías             | Descripción          |
| Prácticas de laboratorio | Resolución de dudas. |

| Evaluación |
|------------|
|------------|



| Metodologías             | Competencias / Resultados | Descripción                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | Calificación |
|--------------------------|---------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------|
| Prácticas de laboratorio | A6 B1 B2 B3 B7 C4         | Se propondrán varias prácticas a lo largo del curso, relacionadas con el análisis forense de equipos, en las que el/la alumno/a trabajará con distintas herramientas y deberá realizar procesos de clonado, de recuperación de información, redacción de informes, etc. En el enunciado de cada práctica se especificará la fecha límite para la realización de la misma, así como la metodología de evaluación, que puede ser a través de la entrega de una memoria, de la realización de una prueba en ordenador, o mediante ambas. | 50           |
| Prueba objetiva          | A6 B1 B2 B3 B7 C4         | Examen final, tipo test o de respuestas cortas, mediante el que se valorarán los conocimientos y capacidades adquiridos por el alumno, tanto en las sesiones de teoría como en las sesiones prácticas.                                                                                                                                                                                                                                                                                                                                | 50           |

## Observaciones evaluación

### 1. CONVOCATORIA DE LA PRIMERA OPORTUNIDAD

A lo largo del curso se realizarán una serie de prácticas de laboratorio, con las características y peso indicados en el cuadro anterior.

Al finalizar el curso se realizará una prueba objetiva, con las características y peso indicados en el cuadro anterior.

### 2. CONVOCATORIA DE LA SEGUNDA OPORTUNIDAD Y CONVOCATORIA EXTRAORDINARIA

Se realizará una prueba objetiva, con las características y peso indicados en el cuadro anterior. La nota de la prueba objetiva NO se conserva en ninguna convocatoria.

Con respeto las prácticas de laboratorio, el/la alumno/a podrá conservar la nota obtenida en la primera oportunidad (si fuese el caso). Caso de no haber presentado las prácticas en la primera oportunidad, el/la alumno/a deberá contactar con el coordinador de la materia, con una antelación mínima de 20 días naturales antes de la fecha del examen.

### 3. PLAGIO

Sí se detectara plagio en cualquiera de las pruebas de evaluación, la calificación final de la materia será de "suspense (0)", hecho que se comunicará a la coordinación del título para adoptar las medidas oportunas.

### 4. CONDICIÓN DE "NO PRESENTADO"

Se considerarán como "no presentados" a los alumnos que no realicen la prueba objetiva.

## Fuentes de información

|                       |                                                                                                                                                                                                                         |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Básica</b>         | - Pilar Vila Avendaño (2018). Técnicas de Análisis Forense informático para Peritos Judiciales profesionales. Madrid : 0xWORD<br>- Eoghan Casey (2009). Handbook of Digital Forensics and Investigation. Academic Press |
| <b>Complementaria</b> | - Juan Garrido Caballero, Juan Luis García Rambla, Chema Alonso (2012). Análisis forense digital en entornos windows. Móstoles: Informática64                                                                           |

## Recomendaciones

### Asignaturas que se recomienda haber cursado previamente

### Asignaturas que se recomienda cursar simultáneamente

### Asignaturas que continúan el temario

### Otros comentarios

(\*) La Guía Docente es el documento donde se visualiza la propuesta académica de la UDC. Este documento es público y no se puede modificar, salvo cosas excepcionales bajo la revisión del órgano competente de acuerdo a la normativa vigente que establece el proceso de elaboración de guías