



Guía Docente

| Datos Identificativos | | | | | 2022/23 |
|-----------------------|---|--------------------|---------------------------------|----------|---------|
| Asignatura (*) | Análise Forense de Equipos | Código | 614530012 | | |
| Titulación | | | | | |
| Descritores | | | | | |
| Ciclo | Período | Curso | Tipo | Créditos | |
| Mestrado Oficial | 2º cuatrimestre | Primeiro | Optativa | 3 | |
| Idioma | CastelánGalego | | | | |
| Modalidade docente | Presencial | | | | |
| Prerrequisitos | | | | | |
| Departamento | Ciencias da Computación e Tecnoloxías da InformaciónComputación | | | | |
| Coordinación | 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 | | | | |
| Descrición xeral | <p>A análise forense de equipos consiste na aplicación de técnicas científicas e analíticas para identificar, preservar, analizar e presentar datos que sexan válidos dentro dun proceso legal.</p> <p>A materia "Análise Forense de Equipos" ten unha forte compoñente práctica. Comezarase con unha introdución a este campo, explicando conceptos clave. A continuación, estudaranse fundamentos e metodoloxías de análise forense dende un punto de vista xenérico e aplicable a novos casos, pero tamén se estudiarán exemplos concretos baseados en casos reais.</p> <p>Nas prácticas de laboratorio, o/a alumno/a aprenderá a manexar diferentes ferramentas de análise forense e realizará prácticas simulando problemas reais.</p> | | | | |

Competencias do título

| Código | Competencias do título |
|--------|------------------------|
| | |

Resultados da aprendizaxe

| Resultados de aprendizaxe | Competencias do título | | |
|---|------------------------|------------|-----|
| Coñecemento das metodoloxías adecuadas para a realización de traballos forenses con validez legal | AP6 | BP1 | CP4 |
| Capacidade para a realización de análise forense dos diferentes elementos que forman un sistema de información, en múltiples plataformas e sistemas operativos | AP6 | BP2 BP7 | CP4 |
| Capacidade para xerar informes como resultado da análise forense claros, concisos e intelixibles tanto por expertos como por persoas alleas ao ámbito da seguridade informática | AP6 | BP3 BP7 | CP4 |

Contidos

| Temas | Subtemas |
|------------------------------------|--|
| 1. Introducción ao análise forense | Introducción Fundamentos Normativa Clonado |
| 2. Análise Forense en Windows | Artefactos Memoria Ferramentas Aspectos avanzados de análise forense en Windows |



| | |
|---|---|
| 3. Análise Forense en Mac OS | Artefactos Memoria Ferramentas Aspectos avanzados de análise forense en Mac OS |
| 4. Análise Forense en dispositivos móbiles: Android | Artefactos Ferramentas Aspectos avanzados de análise forense en Android |
| 5. Análise Forense en dispositivos móbiles: iOS | Artefactos Ferramentas Aspectos avanzados de análise forense en iOS |

| Planificación | | | | |
|--------------------------|-------------------|-------------------|---|--------------|
| Metodoloxías / probas | Competencias | Horas presenciais | Horas non presenciais / traballo autónomo | Horas totais |
| Sesión maxistral | A6 C4 | 11 | 22 | 33 |
| Prácticas de laboratorio | A6 B1 B2 B3 B7 C4 | 10 | 20 | 30 |
| Proba obxectiva | A6 B1 B2 B3 B7 C4 | 2 | 0 | 2 |
| Atención personalizada | | 10 | 0 | 10 |

*Os datos que aparecen na táboa de planificación son de carácter orientativo, considerando a heteroxeneidade do alumnado

| Metodoloxías | |
|--------------------------|---|
| Metodoloxías | Descrición |
| Sesión maxistral | Clases expositivas de presentación dos coñecementos teóricos de cada un dos temas. Fomentarase a participación do alumnado. |
| Prácticas de laboratorio | Sesións prácticas en computador, nas que se deben resolver unha serie de boletíns de exercicios prácticos propostos polo profesor. Os exercicios buscan consolidar os coñecementos presentados nas sesións maxistras e tamén fomentar a aprendizaxe autónoma do alumno. Unha vez completado o boletín de exercicios, o profesor avaliará o traballo realizado polo alumno mediante unha sesión de traballo en computador. Os boletíns de exercicios publicaranse a través da plataforma de formación da Universidade da Coruña. Imporase unha data máxima de defensa para cada boletín, co obxectivo de fomentar o estudo continuo. |
| Proba obxectiva | Proba mediante a que se valorarán os coñecementos e capacidades adquiridos polo alumno. |

| Atención personalizada | |
|--------------------------|------------------------|
| Metodoloxías | Descrición |
| Prácticas de laboratorio | Resolución de dúbidas. |

| Avaliación | | | |
|--------------------------|-------------------|---|---------------|
| Metodoloxías | Competencias | Descrición | Cualificación |
| Prácticas de laboratorio | A6 B1 B2 B3 B7 C4 | Propoñeranse varias prácticas o longo do curso, relacionadas coa análise forense de equipos, nas que o/a alumno/a traballará con distintas ferramentas e deberá realizar procesos de clonado, de recuperación de información, redacción de informes, etc. No enunciado de cada práctica especificarase a data límite para a realización da mesma, así como a metodoloxía de avaliación, que pode ser a través da entrega dunha memoria, da realización dunha proba en ordenador, ou mediante ambas. | 50 |



| | | | |
|-----------------|-------------------|--|----|
| Proba obxectiva | A6 B1 B2 B3 B7 C4 | Exame final, tipo test ou de respostas curtas, mediante o que se valorarán os coñecementos e capacidades adquiridos polo alumno, tanto nas sesións de teoría coma nas sesións prácticas. | 50 |
|-----------------|-------------------|--|----|

Observacións avaliación

1. CONVOCATORIA DA PRIMEIRA OPORTUNIDADE

Ó longo do curso realizaranse unha serie de prácticas de laboratorio, coas características e peso indicados no cadro anterior.

Ó finalizar o curso realizarase unha proba obxectiva, coas características e peso indicados no cadro anterior.

2. CONVOCATORIA DA SEGUNDA OPORTUNIDADE E CONVOCATORIA EXTRAORDINARIA

Realizarase unha proba obxectiva, coas características e peso indicados no cadro anterior. A nota da proba obxectiva NON se conserva en ningunha convocatoria.

Con respecto ás prácticas de laboratorio, o/a alumno/a poderá conservar a nota obtida na primeira oportunidade (se fose o caso). Caso de non ter presentado as prácticas na primeira oportunidade, o/a alumno/a deberá contactar co coordinador da materia, con unha antelación mínima de 20 días naturais antes da data do exame.

3. PLAXIO

Si se detectase plaxio en calquera das probas de avaliación, a cualificación final da materia será de "suspenso (0)", feito que se comunicará á coordinación do título para adoptar as medidas oportunas.

4. CONDICIÓN DE "NON PRESENTADO"

Consideraranse como "non presentados" aos alumnos que non realicen a proba obxectiva.

Fontes de información

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

Recomendacións

Materias que se recomenda ter cursado previamente

Materias que se recomenda cursar simultaneamente

Materias que continúan o temario

Observacións

(*A Guía docente é o documento onde se visualiza a proposta académica da UDC. Este documento é público e non se pode modificar, salvo casos excepcionais baixo a revisión do órgano competente dacordo coa normativa vixente que establece o proceso de elaboración de guías