



Guía docente				
Datos Identificativos				2019/20
Asignatura (*)	Análisis Forense de Equipos	Código	614530012	
Titulación	Máster Universitario en Ciberseguridade			
Descriptorios				
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	faitic.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. Paralelamente, 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 CP4 BP7
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 CP4 BP7

Contenidos	
Tema	Subtema



1. Introducción al análisis forense	Introducción Fundamentos Normativa Clonado
2. Análisis Forense en Windows	Artefactos Memoria Herramientas Aspectos avanzados de análisis forense en Windows
3. Análisis Forense en Mac OS	Artefactos Memoria Herramientas Aspectos avanzados de análisis forense en Mac OS
4. Análisis Forense en dispositivos móviles: Android	Artefactos Herramientas Aspectos avanzados de análisis forense en Android
5. Análisis Forense en dispositivos móviles: iOS	Artefactos Herramientas 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. Una vez completado el boletín de ejercicios, el profesor evaluará el trabajo realizado por el alumno mediante una sesión de trabajo en ordenador. 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 escrita mediante la que se valorarán los conocimientos y capacidades adquiridos por el alumno.

Atención personalizada

Metodologías	Descripción
Prácticas de laboratorio	Resolución de dudas.

Evaluación



Metodoloxías	Competencias / Resultados	Descrición	Calificación
Prácticas de laboratorio	A6 B1 B2 B3 B7 C4	Realización e defensa das prácticas en ordenador, dentro das horas de prácticas e antes da data límite establecida. Es condición necesaria (pero non suficiente) obter unha puntuación mínima de 4 sobre 10 nas prácticas para poder superar a materia.	40
Proba obxectiva	A6 B1 B2 B3 B7 C4	Al finalizar o curso, se realizará unha proba escrita mediante a que se valorarán os coñecementos e capacidades adquiridos polo alumno. Es condición necesaria (pero non suficiente) obter unha puntuación mínima de 5 sobre 10 na proba obxectiva para poder superar a materia.	60

Observacións avaliación

1. PRIMEIRA OPORTUNIDADE

Os estudantes poden decidir ser avaliados de acordo a un modelo de avaliación continua ou de avaliación única. Se entenderá que un estudante elixe unha avaliación continua ao defender a primeira das prácticas da asignatura. Unha vez que os estudantes elixan o modelo de avaliación continua, a súa calificación nunca poderá ser "Non presentado".

1.a) Avaliación continua

Consiste na realización e defensa dunha serie de prácticas de laboratorio, durante todo o período en el que se imparte a materia, e na realización dunha proba obxectiva, cuxas características se describen anteriormente.

A calificación será o resultado de aplicar o promedio ponderado entre os resultados: (i) Proba obxectiva (60%) e (ii) prácticas de laboratorio (40%).

1.b) Avaliación única

Consiste en realizar unha proba obxectiva, con as mesmas características que a correspondente a la avaliación continua. Y, ademais, outra proba escrita, que se realizará a continuación, sobre a parte práctica, e que terá o mesmo peso que esta parte en la avaliación continua.

2. SEGUNDA OPORTUNIDADE

1.a) Avaliación continua

En el caso de que el estudiante siga el modelo de evaluación continua en la primera oportunidad, puede decidir mantener la nota de las prácticas. En este caso, tendrá que hacer el examen relativo a la parte de teoría (prueba obxectiva). O puede decidir renunciar a la nota de prácticas e evaluarse por la modalidade de avaliación única.

La nota de prácticas solo se conserva durante el curso académico.

La nota del examen de teoría no se conserva.

1.b) Avaliación única

Tiene las mismas características que la avaliación única de la primera oportunidad.

3. PLAGIO

Si se detectase plagio en cualquiera de las pruebas de avaliación, la calificación final de la asignatura será "suspenso (0)", que se comunicará a la dirección de la escuela para tomar las medidas apropiadas.

Fuentes de información

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
Complementaria	- Juan Garrido Caballero, Juan Luis García Rambla, Chema Alonso (2012). Análisis forense digital en entornos windows. Móstoles: Informática64 - Mattia Epifani, Pasquale Stirparo (2016). Learning iOS Forensics, 2nd Edition. Packt Publishing - Rohit Tamma, Donnie Tindall (2015). Learning Android Forensics. Packt Publishing

Recomendacións

Asignaturas que se recomenda 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