Guia docente					
Datos Identificativos					2024/25
Asignatura (*)	Análisis Forense de Equipos			Código	614530112
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	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. Esta materia tiene una fuerte componente práctica. Se comenzará con una introducción a la informática forense, 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. En las prácticas de laboratorio el/la alumno/a aprenderá a manejar diferentes herramientas de análisis forense y realizará prácticas simulando problemas reales.				

Competencias / Resultados del título	
Código	Competencias / Resultados del título
A32	HD-12 - Identificar, preservar y analizar evidencias, realizar análisis forense de un sistema de información, y generar informes que sean claros, concisos e inteligibles tanto por expertos como por personas ajenas al ámbito de la seguridad informática
B28	K-12 - Conocer las técnicas y herramientas para la preservación y análisis de evidencias, así como las metodologías adecuadas para la realización de trabajos forenses con validez legal
C11	C-06 - Identificar vulnerabilidades en un sistema real, así como variar sus parámetros y configurarlo para su protección frente a ellas; limitando así la exposición a amenazas conocidas
C13	C-08 - Realizar test de intrusión en entornos prácticos complejos para la identificación de vulnerabilidades, así como para realizar ataques en entornos controlados con juicio crítico y ético
C14	C-09 - Aplicar métodos de investigación forense para el análisis de incidentes o riesgos de ciberseguridad mediante técnicas científicas y analíticas para identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal

Resultados de aprendizaje			
Resultados de aprendizaje	Competencias / Resultados del título		
Conocimiento de las metodologías adecuadas para la realización de trabajos forenses con validez legal	AP32	BP28	CP14
Capacidad para la realización de análisis forense de los diferentes elementos que forman un sistema de información, en múltiples plataformas y sistemas operativos	AP32	BP28	CP11 CP13
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	AP32		

Contenidos	
Tema	Subtema

1. Introducción al Análisis Forense	- Definición y objetivos del análisis forense - Importancia en el contexto de la ciberseguridad - Marco legal y ético - Casos de estudio y ejemplos prácticos
2. Proceso de Análisis Forense	- Estándares y buenas prácticas - Principales fases
3. Adquisición de evidencias	- Fundamentos - Creación de imágenes forenses - Adquisición de memoria
4. Análisis de evidencias	- Análisis del sistema de memoria - Análisis del sistema de almacenamiento
5. Forense en Sistemas Operativos	- Windows - Linux

Planificación				
Metodologías / pruebas	Competencias / Resultados	Horas lectivas (presenciales y virtuales)	Horas trabajo autónomo	Horas totales
Sesión magistral	A32 B28 C14	10	15	25
Prácticas de laboratorio	A32 B28 C11 C13 C14	10	20	30
Prueba práctica	A32 B28 C14	2	10	12
Prueba objetiva	A32 B28 C14	1	5	6
Atención personalizada		2	0	2
(*)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 alumnado. Por cada boletín, el alumnado debe entregar una memoria detallada indicando los pasos seguidos para resolver los ejercicios, aportando evidencias. Se valorará: la calidad de la memoria; la corrección del proceso descrito, de los comandos empleados y de las opciones probadas; la justificación de los pasos seguidos y la propuesta de soluciones alternativas. 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 práctica	Al finalizar la realización de las prácticas de laboratorio, se realizará una prueba en la que el alumnado deberá demostrar las competencias adquiridas, resolviendo una serie de ejercicios prácticos y respondiendo a una serie de preguntas.
Prueba objetiva	Prueba mediante la que se valorarán los conocimientos y capacidades adquiridos por el alumnado.

Atención personalizada	
Metodologías	Descripción
Prácticas de laboratorio	Resolución de dudas. El horario de tutorías puede consultarse en https://www.udc.es/es/centros_departamentos_servizos/centros/titorias/?codigo=614

Evaluación			
Metodologías	Competencias / Resultados	Descripción	**Calificación**
Prácticas de laboratorio	A32 B28 C11 C13 C14	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.	40
Prueba objetiva	A32 B28 C14	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.	40
Prueba práctica	A32 B28 C14	Al finalizar la realización de las prácticas de laboratorio, se realizará una prueba en la que el alumno deberá demostrar las competencias adquiridas, resolviendo una serie de ejercicios prácticos y respondiendo a una serie de preguntas.	20

Observaciones evaluación

Será necesario obtener como mínimo el 50% de la nota para aprobar la materia. Además, para aprobar la materia será preciso (en cualquier oportunidad) obtener un mínimo de un 40% de la nota en la prueba objetiva. En caso contrario, la nota máxima que se podrá obtener es de 4.5.
La nota de la prueba objetiva NO SE CONSERVA en ninguna convocatoria. El resto de notas se conservan para el resto de oportunidades del curso académico.
1. CONVOCATORIA DE LA PRIMERA OPORTUNIDAD - CONVOCATORIA ORDINARIA
A lo largo del curso se realizarán una serie de prácticas de laboratorio, una prueba práctica y una prueba objetiva, con las características y peso indicados en el cuadro anterior.
2. RESTO DE CONVOCATORIAS
Se realizará una prueba objetiva, con las características y peso indicados en el cuadro anterior.
La nota de prácticas de laboratorio podrá recuperarse mediante la realización de las prácticas que se determinen para esta convocatoria. La presentación de las prácticas en esta convocatoria implica la renuncia a la nota obtenida en la primera oportunidad, si la hubiera.
La nota de la prueba práctica podrá recuperarse mediante la realización de una nueva prueba práctica. La presentación a la prueba práctica en esta convocatoria implica la renuncia a la nota obtenida en la primera oportunidad, si la hubiera.
Caso de querer recuperar la nota de alguna parte en esta convocatoria, el alumnado deberá contactar con el coordinador de la materia, con una antelación mínima de 20 días naturales antes de la fecha del examen de la correspondiente convocatoria.
3. PLAGIO
Si se detectara plagio en cualquiera de las pruebas de evaluación, la calificación final de la materia será de "suspenso (0)", hecho que se comunicará a la coordinación del título para adoptar las medidas oportunas.
4. CONDICIÓN DE "NO PRESENTADO"
Se considerará como "no presentado" al alumnado que no se presente a ninguna de las actividades evaluables en una convocatoria dada.
5. ESTUDIANTES CON MATRÍCULA A TIEMPO PARCIAL O CON DISPENSA ACADÉMICA DE EXENCIÓN DE DOCENCIA
Deberán ponerse en contacto con los profesores de la materia para posibilitar la realización de las tareas fuera de la organización habitual de la materia.

Fuentes de información

Básica	Casey, Eoghan. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. 3rd ed., San Diego: Academic Press, 2011.Casey, Eoghan. Handbook of Digital Forensics and Investigation. Academic Press, 2009.Carrier, Brian. File System Forensic Analysis. Upper Saddle River: Addison-Wesley, 2005.Vila, Pilar. Técnicas de Análisis Forense Informático para Peritos Judiciales Profesionales. Madrid: 0xWord, 2018Farmer, Dan, and Wietse Venema. Forensic Discovery. Upper Saddle River, NJ: Addison-Wesley, 2005.McKemmish, Rodney. What is Forensic Computing?. Canberra: Australian Institute of Criminology, 1999.Sammons, John. The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Elsevier, 2012.Nelson, Bill, et al. Guide to computer forensics and investigations. Course Technology Cengage Learning, 2010.Johansen, Gerard. Digital forensics and incident response. Packt Publishing Ltd, 2017.Caballero, Juan Garrido, Juan Luis G. Rambla, and José Maria Alonso Cebrián. Análisis forense digital en entornos Windows. Informática 64, 2009.
Complementária	

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