Guía Docente					
Datos Identificativos					2024/25
Asignatura (*)	Análise Forense de Equipos			Código	614530112
Titulación	Máster Universitario en Ciberseguridade				
Descriptores					
Ciclo	Período	Curso		Tipo	Créditos
Mestrado Oficial	2º cuadrimestre	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	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. Esta materia ten unha forte compoñente práctica. Comezarase con unha introdución á informática forense, explicando conceptos clave. A continuación, estudiaranse 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. Nas prácticas de laboratorio, o/a alumno/a aprenderá a manexar diferentes ferramentas de análise forense e realizará prácticas simulando problemas reais.				

Competencias / Resultados do título	
Código	Competencias / Resultados do 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 da aprendizaxe			
Resultados de aprendizaxe	Competencias / Resultados do título		
Coñecemento das metodoloxías adecuadas para a realización de traballos forenses con validez legal	AP32	BP28	CP14
Capacidade para a realización de análise forense dos diferentes elementos que forman un sistema de información, en múltiples plataformas e sistemas operativos	AP32	BP28	CP11 CP13
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	AP32		

Contidos	
Temas	Subtemas

1. Introdución á Análise Forense	- Definición e obxectivos da análise forense - Importancia no contexto da ciberseguridade - Marco legal e ético - Casos de estudo e exemplos prácticos
2. Proceso de Análise Forense	- Estándares e boas prácticas - Principais fases
3. Adquisición de evidencias	- Fundamentos - Creación de imaxes forenses - Adquisición de memoria
4. Análise de evidencias	- Análise da memoria do sistema - Análise do sistema de almacenamento
5. Forense en Sistemas Operativos	- Windows - Linux

Planificación				
Metodoloxías / probas	Competencias / Resultados	Horas lectivas (presenciais e virtuais)	Horas traballo autónomo	Horas totais
Sesión maxistral	A32 B28 C14	10	15	25
Prácticas de laboratorio	A32 B28 C11 C13 C14	10	20	30
Proba práctica	A32 B28 C14	2	10	12
Proba obxectiva	A32 B28 C14	1	5	6
Atención personalizada		2	0	2
*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 maxistrais e tamén fomentar a aprendizaxe autónoma do alumnado. Por cada boletín, o alumnado debe entregar unha memoria detallada indicando os pasos seguidos para resolver os exercicios, achegando evidencias. Valorarase: a calidade da memoria; a corrección do proceso descrito, dos comandos empregados e das opcións probadas; a xustificación dos pasos seguidos e a proposta de solucións alternativas. 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 práctica	Ao remate da realización das prácticas de laboratorio, realizarase unha proba na que el alumnado deberá demostrar as competencias adquiridas, resolvendo unha serie de exercicios prácticos e respondendo a unha seria de preguntas.
Proba obxectiva	Proba mediante a que se valorarán os coñecementos e capacidades adquiridos polo alumnado.

Atención personalizada	
Metodoloxías	Descrición
Prácticas de laboratorio	Resolución de dúbidas. O horario de titorías pode consultarse en https://www.udc.es/es/centros_departamentos_servizos/centros/titorias/?codigo=614

Avaliación			
Metodoloxías	Competencias / Resultados	Descrición	**Cualificación**
Prácticas de laboratorio	A32 B28 C11 C13 C14	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.	40
Proba obxectiva	A32 B28 C14	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.	40
Proba práctica	A32 B28 C14	Ao remate da realización das prácticas de laboratorio, realizarase unha proba na que o alumno deberá demostrar as competencias adquiridas, resolvendo unha serie de exercicios prácticos e respondendo a unha serie de preguntas.	20

Observacións avaliación
Será necesario obter como mínimo o 50% da nota para aprobar a materia. Ademais, para aprobar a materia será preciso (en calquera oportunidade) obter un mínimo dun 40% da nota na proba obxectiva. En caso contrario, a nota máxima que se poderá obter é de 4.5. A nota da proba obxectiva NON SE CONSERVA en ningunha convocatoria. O resto de notas consérvanse para o resto de oportunidades do curso académico. 1. CONVOCATORIA DA PRIMEIRA OPORTUNIDADE - CONVOCATORIA ORDINARIA Ao longo do curso realizaranse unha serie de prácticas de laboratorio, unha proba práctica e unha proba obxectiva, coas características e peso indicados no cadro anterior. 2. RESTO DE CONVOCATORIAS Realizarase unha proba obxectiva, coas características e peso indicados no cadro anterior. A nota de prácticas de laboratorio poderá recuperarse mediante a realización das prácticas que se determinen para esta convocatoria. A presentación das prácticas nesta convocatoria implica a renuncia á nota obtida na primeira oportunidade, se a houbera. A nota da proba práctica poderá recuperarse mediante a realización dunha nova proba práctica. A presentación á proba práctica nesta convocatoria implica a renuncia á nota obtida na primeira oportunidade, se a houbera. No caso de querer recuperar a nota dalgunha parte nesta convocatoria, o alumnado deberá contactar co coordinador da materia, cunha antelación mínima de 20 días naturais antes da data do exame da correspondente convocatoria. 3. PLAXIO Se se detectara 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" Considerarase como "non presentado" ao alumnado que non se presente a ningunha das actividades avaliables nunha convocatoria dada. 5. ESTUDANTES CON MATRÍCULA A TEMPO PARCIAL OU CON DISPENSA ACADÉMICA DE EXENCIÓN DE DOCENCIA Deberán poñerse en contacto cos profesores da materia para posibilitar a realización das tarefas fóra da organización habitual da materia.

Fontes de información

Bibliografía 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.
Bibliografía complementaria	

Recomendacións
Materias que se recomenda ter cursado previamente
Materias que se recomenda cursar simultaneamente
Materias que continúan o temario
Observacións