UNIVERSIDADE DA CORUÑA

Guía Docente					
Datos Identificativos					2019/20
Asignatura (*)	Análise Forense de Equipos			Código	614530012
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	faitic.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. A materia "Análise Forense de Equipos" ten unha forte compoñente práctica. Comezarase con unha introdución a este campo, 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. Paralelamente, 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
A6	CE6 - Desenvolver e aplicar métodos de investigación forense para o análisis de incidentes ou riscos de ciberseguridade
B1	CB1 - Posuír e comprender coñecementos que aporten unha base ou oportunidade de ser orixinais no desenvolvemento e aplicación de ideas, a miúdo nun contexto de investigación
B2	CB2 - Que os estudantes saiban aplicar os coñecementos adquiridos e a súa capacidade de resolución de problemas en contornas novas ou pouco coñecidas dentro de contextos más amplos (ou multidisciplinares) relacionados coa súa área de estudo
B3	CB3 - Que os estudantes sexan capaces de integrar coñecementos e enfrontarse á complexidade de formar xuízos a partir dunha información que, sendo incompleta ou limitada, inclúa reflexións sobre as responsabilidades sociais e éticas vinculadas á aplicación dos seus coñecementos e xuízos
B7	CG2 - Resolución de problemas. Ter capacidade de resolver, cos coñecementos adquiridos, problemas específicos do ámbito técnico da seguridade da información, as redes e/ou os sistemas de comunicacións
C4	CT4 - Valorar a importancia da seguridade da información no avance socioeconómico da sociedade

Resultados da aprendizaxe			
Resultados de aprendizaxe	Competencias / Resultados 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. Introdución ao análise forense	Introdución 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 / Resultados	Horas lectivas (presenciais e virtuais)	Horas 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 maxistrais 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 escrita 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 / Resultados	Descrición	Cualificación
Prácticas de laboratorio	A6 B1 B2 B3 B7 C4	Realización e defensa das prácticas en computador, dentro das horas de prácticas e antes da data límite establecida.	40
Proba obxectiva	A6 B1 B2 B3 B7 C4	Ao finalizar o cuadrimestre, realizarase unha proba escrita mediante a que se valorarán os coñecementos e capacidades adquiridos polo alumno.	60

Observacións avaliación
1. PRIMEIRA OPORTUNIDADE Os alumnos poden decidir ser avaliados segundo un modelo de avaliación continua ou ben de avaliación única. Entenderase que un alumno elixe avaliación continua ao defender a primeira das prácticas da materia. Unha vez os estudantes opten polo modelo de avaliación continua a súa cualificación non poderá ser nunca "Non presentado". 1.a) Avaliación continua Consiste na realización e defensa dunha serie prácticas de laboratorio, ao longo do período no que se imparte a materia, e na realización dunha proba obxectiva, cuxas características se describen máis arriba. A cualificación será o resultado de aplicar a media ponderada entre os resultados: (i) Proba obxectiva (60%), e (ii) prácticas de laboratorio (40%). 1.b) Avaliación única Consiste na realización dunha proba obxectiva, coas mesmas características da correspondente a avaliación continua. E, adicionalmente, outra proba escrita, que se realizará a continuación do anterior, sobre a parte práctica, e que terá o mesmo peso que esta parte na avaliación continua. 2. SEGUNDA OPORTUNIDADE 1.a) Avaliación continua No caso de que o alumno seguira o modelo de avaliación continua na primeira oportunidade, pode decidir conservar nota de prácticas. Neste caso so terá que facer o exame relativo á parte de teoría (proba obxectiva). Ou pode decidir renunciar á nota de prácticas e avaliarse pola modalidade de avaliación única. A nota de prácticas só se conserva durante o curso académico. A nota do exame de teoría non se conserva. No caso de que o alumno non seguira o modelo de avaliación continua na primeira oportunidade, debe acollerse ao modelo de avaliación única. 1.b) Avaliación única Ten as mesmas características que a avaliación única da primeira oportunidade. 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 dirección da escola para adoptar as medidas oportunas.

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 - Mattia Epifani, Pasquale Stirparo (2016). Learning iOS Forensics, 2nd Edition. Packt Publishing - Rohit Tamma, Donnie Tindall (2015). Learning Android Forensics. Packt Publishing

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