UNIVERSIDADE DA CORUÑA

Guía Docente					
Datos Identificativos					2018/19
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	Computación				
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	www.munics.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 do título	
Código	Competencias 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 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. Fundamentos	Fundamentos
2. Metodología de Análisis Forense	Metodología de Análisis Forense

3. Ferramentas de Análise Forense: Entornos Linux e Windows	Ferramentas de Análise Forense: Entornos Linux e Windows
4. Casos	Casos

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 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	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. É 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	Ao finalizar o cuadrimestre, realizarase unha proba escrita mediante a que se valorarán os coñecementos e capacidades adquiridos polo alumno. É condición necesaria (pero non suficiente) obter unha puntuación mínima de 5 sobre 10 na proba obxectiva para poder superar a materia.	60

Observacións avaliación

Alumnos a tempo parcial Alumnado con recoñecemento de dedicación a tempo parcial e dispensa académica de exención de asistencia, segundo establece a "NORMA QUE REGULA O RÉXIME DE DEDICACIÓN AO ESTUDIO DOS ESTUDANTES DE GRAO NA UDC (Art. 2.3; 3.b e 4.5)(29/5/2012)". Os alumnos que cursen a materia a tempo parcial deben realizar as mesmas probas de avaliación que os alumnos que as cursen a tempo completo, coas seguintes consideracións: Quedan exentos da asistencia a clase.En canto á defensa das prácticas, se o alumno non puidese asistir á defensa no horario de prácticas, convirase con el un horario alternativo.O alumno deberá notificar ao coordinador da materia a súa condición de estudante a tempo parcial tan pronto como lle sexa recoñecida, de xeito que o profesor poida realizar unha correcta planificación das actividades docentes. Segunda oportunidade e oportunidade adiantada de Decembro Aspectos a ter en conta: En caso de non presentar (ou non superar) as prácticas de laboratorio en primeira oportunidade, o/a alumno/a deberá someterse a un (novo) exame de prácticas, con computador. Para iso, o/a alumno/a debe contactar co coordinador, como mínimo 15 días antes da data do exame oficial da asignatura para a convocatoria en cuestión (Xullo ou Decembro), e convir con el unha data e hora para a realización do exame de prácticas.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 - 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