

Análisis Forense de Dispositivos

Número total de créditos ECTS	6	
Tipología	Obligatoria	
Organización temporal	Semestre 2	
Modalidad	Presencial	
Idioma	Castellano	
Contenidos	<ul style="list-style-type: none"> • Metodología de un análisis forense: <ul style="list-style-type: none"> ○ Fases de un análisis forense ○ Gestión y análisis de logs ○ Cadena de custodia de evidencias digitales • Proceso de adquisición <ul style="list-style-type: none"> ○ Triage ○ Sistema encendido (adquisición en caliente) ○ Sistema apagado (adquisición en frío) • Análisis forense de red <ul style="list-style-type: none"> ○ Logs de red ○ Tráfico de red • Elaboración del informe forense 	
Resultados de aprendizaje TÍTULO	Conocimientos y contenidos	<p>CC04 Comprender el funcionamiento de los diferentes tipos de malware existentes, así como las partes de los sistemas informáticos a las que afectan.</p> <p>CC05 Identificar los diferentes tipos de malware existentes según las trazas de comportamiento de los mismos</p> <p>CC06 Listar los principales artefactos forenses de los sistemas operativos más habituales.</p>
	Habilidades y destrezas	<p>HD04 Extraer indicadores de compromiso (IOCs) de códigos o ejecutables potencialmente maliciosos para su futura clasificación y detección temprana.</p> <p>HD05 Evaluar diferentes ataques informáticos gracias a las trazas que dejan los mismos en los diferentes mecanismos de detección y registro de los sistemas.</p> <p>HD06 Configurar diferentes herramientas de detección, prevención, contención y recuperación de ciberincidentes.</p> <p>HD07 Extraer evidencias de diversas fuentes de dispositivos involucrados en un ciberincidente.</p>
	Competencias	<p>CP01 Realizar un análisis forense detallado de los diferentes elementos que pueden estar involucrados en un incidente informático, desde sistemas informáticos convencionales hasta redes complejas y dispositivos móviles, identificando, recopilando y examinando de manera sistemática diversas evidencias digitales.</p> <p>CP02 Elaborar un informes técnicos, legales o ejecutivos, adecuados al público objetivo detallando las causas y consecuencias de un incidente informático haciendo uso de las evidencias obtenidas en la realización de un análisis forense.</p> <p>CP04 Comunicar las causas, consecuencias, mecanismos de contención empleados y medidas de prevención implementadas a raíz de un ataque informático.</p>
Resultados de aprendizaje ASIGNATURA		
<ul style="list-style-type: none"> • Mantener escrupulosamente la cadena de custodia de dispositivos electrónicos. • Detallar las acciones llevadas a cabo para analizar un dispositivo electrónico con el objetivo de que sean reproducibles. • Actuar como perito informático forense en procedimientos judiciales en los que se presenten como pruebas dispositivos electrónicos. 		

Actividades formativas	Horas totales
Clases Expositivas	22
Seminarios	2
Clases prácticas	10
Prácticas de laboratorio	12
Trabajo autónomo	102
Prueba de evaluación final	2
Total	150

Sistemas de evaluación	MÍNIMO	MÁXIMO
Evaluación final: prueba o examen virtual	50	50
Resolución problemas	10	30
Estudio casos / Proyectos	10	30
Otras actividades de evaluación continua	0	10
Total	60	110