Análisis Forense de Dispositivos

Número total de créditos ECTS	6	
Tipología	Obligatoria	
Organización temporal	Semestre 2	
Modalidad	Virtual	
Idioma	Castellano	

Contenidos	• Metodología de un análisis forense:
	  ○ Fases de un análisis forense
	  ○ Gestión y análisis de logs
	  ○ Cadena de custodia de evidencias digitales
	• Proceso de adquisición
	  ○ Triaje
	  ○ Sistema encendido (adquisición en caliente)
	  ○ Sistema apagado (adquisición en frío)
	• Análisis forense de red
	  ○ Logs de red
	  ○ Tráfico de red
	• Elaboración del informe forense	

Resultados de aprendizaje TÍTULO	**Conocimientos y contenidos**	CC04 Comprender el funcionamiento de los diferentes tipos de malware existentes, así como las partes de los sistemas informáticos a las que afectan. CC05 Identificar los diferentes tipos de malware existentes según las trazas de comportamiento de los mismos CC06 Listar los principales artefactos forenses de los sistemas operativos más habituales.
	Habilidades y destrezas	HD04 Extraer indicadores de compromiso (IOCs) de códigos o ejecutables potencialmente maliciosos para su futura clasificación y detección temprana. HD05 Evaluar diferentes ataques informáticos gracias a las trazas que dejan los mismos en los diferentes mecanismos de detección y registro de los sistemas. HD06 Configurar diferentes herramientas de detección, prevención, contención y recuperación de ciberincidentes. HD07 Extraer evidencias de diversas fuentes de dispositivos involucrados en un ciberincidente.
	Competencias	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. 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. CP04 Comunicar las causas, consecuencias, mecanismos de contención empleados y medidas de prevención implementadas a raíz de un ataque informático.
Resultados de aprendizaje ASIGNATURA • 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 síncronas	10
Recursos didácticos audiovisuales	6
Seminarios síncronos	2
Clases prácticas síncronas	10
Resolución de ejercicios, casos y proyectos	6
Prácticas de laboratorio asíncronas	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	**70**	**120**