FICHA DE LA ASIGNATURA ANÁLISIS FORENSE			
CARÁCTER:	**Prácticas Externas**	**LENGUA/S EN LA/S QUE SE IMPARTE:**	**Español**
ECTS:	**5**	**CUATRIMESTRE**	**1**
Asignatura de la MATERIA TECNOLOGÍAS EN SEGURIDAD			
PROFESORES QUE IMPARTEN LA ASIGNATURA			
Personal de la empresa Deloitte.			
COMPETENCIAS QUE SE ADQUIEREN: *(indicar código)*			
Comp. Básicas	**Comp. Generales**	**Comp. Específicas**	**Comp. Transversales**
CB6 CB7 CB8 CB9 CB10	**CG1 CG2 CG3 CG4 CG5**	**CE5**	

RESULTADOS DE APRENDIZAJE:
Conocer el mecanismo para obtener evidencias digitales válidas en procedimientos legales
Desarrollar técnicas y herramientas necesarias para la investigación forense.

CONTENIDOS:

1. Introducción a la ciencia forense
– Introducción al ámbito forense
– Repaso histórico
– Riesgos y desafíos
– Cibercrimen
– Rol del investigador forense
– Metodología

2. Leyes y ciencia forense
– Introducción a las ciberleyes
– Cibercrimen: Historia reciente
– Leyes específicas
– Investigación de incidentes de seguridad

3. Proceso de investigación
– Metodología
– Evaluación del caso
– Plan de investigación
– Órdenes judiciales y políticas de seguridad
– Valor de la adquisición y software
– Implementación de la investigación
– Evaluación y cierre del caso

4. Laboratorio forense
– Características
– Entorno
– Equipamiento
– Estandarización
– Certificación

5. Adquisición de evidencias
– Cadena de custodia

– Formato de evidencias
– Expert Witness Format (EWF)
– Contenedores virtuales
– Advanced Forensic Format (AFF)
– Orden de volatilidad
– Host Protected Area (HPA) y Device Configuration Overlay (DCO)
– Herramientas software
– Herramientas hardware

6. Recolección de evidencias volátiles en Microsoft Windows
– Volatilidad de la información
– CLI vs GUI
– Suite sysinternals
– Usuarios logueados
– Ficheros abiertos
– Información de red
– Información de procesos
– Información de DLLs
– Autoarranque
– Herramientas nativas de Microsoft Windows
– LiveView

7. Herramientas de análisis forense
Análisis forense con TSK y Autopsy
– Introducción a TSK
– Comandos de TSK
– Prácticas con TSK
– Introducción a Autopsy
– Funcionalidades de Autopsy
– Prácticas con Autopsy
Análisis forense con PyFLAG
– Introducción a PyFLAG
– Estructura de PyFLAG
– Uso de PyFLAG
– Menús y funcionalidades
– Registros en PyFLAG
– Comunicaciones en PyFLAG
– Memoria en PyFLAG

8. Discos duros y sistemas de ficheros (FAT y NTFS)
– Discos duros
– Interfaces
– Particiones y Master Boot Record (MBR)
– Slack Space
– File Allocation Table (FAT)
· Estructura
· Area FAT
– New Technology File System (NTFS)
– Master File Table (MFT)

9. Análisis forense en sistemas Microsoft Windows
– Papelera de reciclaje
– Accesos directos

– Carpetas por defecto
– Carpetas de interés
– Cookies
– Index.dat
– Ficheros Prefetch
– Carpetas OLK
– Spooler de impresión
– Shadow Volume Copy
– Eventos
– Otros ficheros de registro
– Análisis de las firmas de ficheros
– Análisis de hashes
– Montaje de ficheros
– NTFS Alternate Data Streams (ADS)
– Registro de Windows
– Fichero SAM

10. Análisis forense de memoria RAM
– Crash dumps
– Virtualización
– Ficheros de hibernación
– Volatility
– Memoryze

11. Análisis forense en sistemas GNU/Linux
– Introducción a GNU/Linux: Distribuciones
– Sistemas de ficheros EXT
– Estructura de EXT
– Bloques y superbloques
– Inodos
– Dispositivos hardware
– Proceso de arranque
– Ficheros y jerarquía
– Cuentas de usuario
– Ficheros de registro

12. Análisis de ficheros
– Introducción
– Identificación del contenido
– Metadatos
– Documentos ofimáticos
– Portable Document Format (PDF)
– Imágenes
– Herramientas de metadatos
– Esteganografía
– Tipos
– Herramientas esteganográficas

13. Análisis de correos electrónicos
– Introducción
– Correo electrónico
· Cabecera
· Mensaje

– Personal Storage Table (PST)
– Formatos mbox y maildir
– Formato EML

14. Análisis de perfiles de navegación web
– Introducción
– Análisis forense de Microsoft Internet Explorer
– Análisis forense de Mozilla Firefox
– Análisis forense de Google Chrome
– Análisis forense de Apple Safari
– Análisis forense de Opera Software

OBSERVACIONES / REQUISITOS PREVIOS:
Algunas de las actividades podrán realizarse en inglés.

El sistema de evaluación consiste en un examen final de certificación que se realizará al final del curso. Dicho examen final será el examen de DCFIA (Deloitte Certified Forensic Investigator Associate en el que el alumno debe contestar correctamente a una batería de 50 preguntas de distinto tipo. En el examen se pueden encontrar preguntas de respuesta múltiple, única, verdadero/falso y desarrollo. Para aprobar la asignatura se necesitara un 50% de dicho examen final. Para obtener la certificación el alumno debe de obtener un 70% en dicho examen final. El certificado se emitirá, en su caso, junto al título del Máster.

	Id de la Actividad Formativa	Nº de horas	Presencialidad (%)
ACTIVIDADES FORMATIVAS CON SUS CRÉDITOS ECTS:	Clases de teórico-prácticas	25	100%
	Actividades académicas no presenciales	96	0%
	Evaluación	4	100%

METODOLOGÍAS DOCENTES:
Lección magistral expositiva
Resolución de problemas y casos prácticos
Prácticas de laboratorio

SISTEMAS DE EVALUACIÓN DE ADQUISIÓN DE COMPETENCIAS:

Denominación Sistema Evaluación	Ponderación Mínima	Ponderación Máxima
Prácticas de laboratorio	0%	70%
Pruebas escritas u orales	30%	100%

BIBLIOGRAFÍA RECOMENDADA:

a. Material teórico:
    i. Libro oficial de la certificación profesional D-CFIA 101 Análisis Forense
b. Material complementario para antes de la sesión:
    i. Blogs de análisis forense:
        1. http://conexioninversa.blogspot.com/

2. http://www.informaticoforense.eu/

ii. Casos prácticos de SANS Forensics:
   1. https://digital-forensics.sans.org/blog/category/computer-forensics
   2. https://digital-forensics.sans.org/community/webcasts
   3. https://digital-forensics.sans.org/community/whitepapers