Guía Docente: Técnicas de Análisis Forense

DATOS GENERALES	
Facultad	Facultad de Ciencias y Tecnología
Titulación	Grado en Ingeniería Informática
Plan de estudios	2012
Especialidad/Mención	Mención en Criptología y Seguridad de la Información
Materia	Criptología y Seguridad de la Información
Carácter	Optativo
Período de impartición	Segundo Trimestre
Curso	Cuarto
Nivel/Ciclo	Grado
Créditos ECTS	6
Lengua en la que se imparte	Castellano
Prerrequisitos	Ninguno

DATOS DEL PROFESORADO			
Profesor Responsable	Javier Martín Porras	**Correo electrónico**	javier.martin.porras@ui1.es
Área	Lenguajes y Sistemas Informáticos	**Facultad**	Facultad de Ciencias y Tecnología
Perfil Profesional 2.0	Es ingeniero Superior en Informática y Doctor en Ingeniería Informática. Es Profesor en varios grados de la Universidad Isabel I, y ejerce como perito en "Laboratorio Pericial Forense" en Alicante. Consultor Internacional de la Oficina de Naciones Unidas contra la Droga y el Delito. **Laboratorio Pericial Forense**		

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA	
Asignaturas de la materia	• Auditoría y seguridad avanzada de sistemas y redes de comunicaciones • Autenticación y Sistemas Biométricos • Criptografía y Criptoanálisis • Dirección de Proyectos de Seguridad Corporativos • Técnicas de Análisis Forense • Técnicas de auditoría, ataque y programación segura de aplicaciones web
Contexto y sentido de la asignatura en la titulación y perfil profesional	Esta asignatura ofrece a los alumnos la posibilidad de adquirir los conocimientos suficientes en materia de analisis forense informático. El alumno adquirirá los conocimientos necesarios para obtener y preservar las evidencias digitales necesarias para analizar en profundidad un ataque informático. Será capaz de: • Definir una metodología para proceder dentro de un análisis forense. • Identificar las técnicas y fuentes de información necesarias para obtener las evidencias digitales. • Preservar y extraer los datos relacionados con el análisis desde estas fuentes de información. • Documentar y presentar informes detallados que incluyan todos los aspectos valorados de la investigación (metodología, técnicas, hallazgos…).

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE	
Competencias de la asignatura	• CR10: Conocimiento de las características, funcionalidades y estructura de los Sistemas Operativos y diseñar e implementar aplicaciones basadas en sus servicios. • CMC04: Capacidad para plantear, desarrollar y dirigir el análisis forense de un sistema informático comprometido, firmando un informe con conclusiones fundamentadas y razonadas, que pueda ser posteriormente utilizado en un proceso legal. • CT03: Capacidad de comunicación oral y escrita en el ámbito académico y profesional, con especial énfasis en la redacción de documentación técnica • CT06: Capacidad de trabajo en equipo • CU03: Utilizar la expresión oral y escrita de forma adecuada en contextos personales y profesionales.
Resultados de aprendizaje de la asignatura	• Conoce los elementos internos esenciales de los diferentes sistemas operativos, que resultan necesarios a la hora de realizar un análisis forense. • Conoce las principales técnicas de ocultación y borrado de evidencias, así como las técnicas que pueden aplicarse para su recuperación. • Conoce y utiliza el concepto de cadena de custodia, los principales aspectos legales relacionados con ella, y cómo mantener y asegurar su integridad a lo largo de todo el proceso de un análisis forense. • Plantea, desarrolla y dirige el análisis forense de un sistema informático comprometido, generando un informe con conclusiones fundamentadas y razonadas.

PROGRAMACION DE CONTENIDOS	
Breve descripción de la asignatura	Esta asignatura introduce al alumnado en un área poco conocida del estudio de la Seguridad de la Información. Presenta los conceptos básicos del análisis de un sistema comprometido, así como las peculiaridaades aplicables a los sistemas Unix y Windows. A continuación se analizan algunas de las herramientas más conocidas y utilizadas, finalizando con la realización de casos prácticos en sistemas reales.
Contenidos	**Unidad didáctica 1. Conceptos y bases del peritaje informático forense** • Introducción y definiciones • Conceptos legales útiles para un perito • Estándares UNE y procedimiento pericial **Unidad didáctica 2. El laboratorio forense** • Elementos básicos y suplementarios. • Gestión interna de un laboratorio • Cadena de custodia de la evidencia física y digital • Principios multidisciplinares del análisis forense **Unidad didáctica 3. Metodología de trabajo** • Adquisición y gestión de la cadena de custodia. • Documentación y montaje del informe • Conclusiones • Ratificación en sede judicial **Unidad didáctica 4. Análisis forense aplicado a Windows/Linux/IOS** • Análisis de memoria RAM • Modelo del sistema de archivos • Estructura interna del sistema operativo Linux • Análisis de datos específicos • Fundamentos técnicos del sistema • Datos en el espacio del usuario en sistemas operativos Mac • Almacenamiento y sistemas de ficheros HFS + para Mac OS • Artefactos específicos de Mac OS: Time Machine, KeyChain, Spotlight, FileVault 2 • Artefactos de internet para Mac OS: configuraciones de red, correo electrónico, mensajería, iCloud y navegadores **Unidad didáctica 5. Análisis forense aplicado a sistemas operativos móviles** • Tipología de extracción forense en dispositivos móviles • UFED • MSAB XRY-XAMM • Extracción avanzada en dispositivos no funcionales y destruidos **Unidad didáctica 6. Análisis forense de correos electrónicos y redes** • Estructura de un correo electrónico • Análisis de tráfico red • Herramientas forenses para análisis de tráfico de red • Propuesta de laboratorio forense low cost para análisis de tráfico de red

METODOLOGÍA	
Actividades formativas	**Actividades de descubrimiento inducido (Estudio de caso):** presentación de una situación motivadora que introduzca de manera atractiva y sugerente en una parcela de conocimiento, se plantea una posibilidad que pueda darse en la realidad en torno al tipo de saberes propios de la Unidad didáctica. La presentación del Caso al alumnado se asocia como una serie concatenada de preguntas, se le sugieren consultas, se le suministran textos, imágenes, gráficos… con datos suficientes como para que pueda ofrecer una solución o llegar a unas conclusiones lógicas. **Contenidos teóricos:** todas las unidades conjugan la presencia de contenidos teóricos y textos canónicos con desarrollos prácticos de los mismos. Consulta, lectura, aprendizaje, actividades y revisión de textos que contienen «las lecciones» de la Asignatura. Contendrá incentivaciones hacia competencias y adquisición de conocimientos. Es lo que el alumno/a «debe saber » y también «saber hacer». **Actividades de aplicación práctica (individuales). Cuestionarios de repaso:** se incluyen cuestionarios de autoevaluación a fin de consolidar y evaluar la adquisición de conocimientos a lo largo del curso. **Actividades de Interacción y colaboración** (**Foros de Debate):** actividades para debate y/o para resolución en común y compartida, propuestas de pensamiento crítico con destino de comunicación participativa. **Actividades de aplicación práctica (grupal online). Trabajo colaborativo:** Se plantea una actividad colaborativa, con la que los alumnos deberán de resolver el caso propuesto en grupos, aportando cada uno sus conocimientos y opinión sobre cómo sería la mejor forma de resolver la actividad propuesta. Ponen al alumnado ante el trabajo investigador, de búsqueda o de innovación. Implica una sugerencia de «Indagación en personal y en grupo» empleando las oportunidades que ofrece la red para su desarrollo.

EVALUACIÓN	
Sistema evaluativo	*En caso de que la situación sanitaria impida la realización presencial de los exámenes con todas las garantías, la Universidad Isabel I celebrará dichas pruebas en modalidad online. Para la realización de dichos exámenes, la universidad incorporará la herramienta de proctoring a nuestra plataforma tecnopedagógica, con el objetivo de garantizar los procesos de autentificación del alumno, como el control del entorno durante el desarrollo de las pruebas de evaluación. A su vez, la Universidad Isabel I pondrá a disposición del alumnado una Unidad de Exámenes Online específica para ofrecer apoyo técnico durante todo el proceso y así solventar todas las incidencias que se puedan presentar.* El sistema de evaluación se basará en una selección de las pruebas de evaluación más adecuadas para el tipo de competencias que se trabajen. El sistema de calificaciones estará acorde con la legislación vigente *(Real Decreto 1125/2003, de 5 de septiembre, por el que se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y de validez en todo el territorio nacional)*. El sistema de evaluación de la Universidad Isabel I queda configurado de la siguiente manera: **Sistema de evaluación convocatoria ordinaria** **Opción 1. Evaluación continua**

Los estudiantes que opten por esta vía de evaluación deberán realizar el **seguimiento de la evaluación continua (EC)** y podrán obtener hasta un **60 %** de la calificación final a través de las actividades que se plantean en la evaluación continua.

Además, deberán realizar un **examen final presencial (EX)** que supondrá el **40 %** restante. Esta prueba tiene una parte dedicada al control de la identidad de los estudiantes que consiste en la verificación del trabajo realizado durante la evaluación continua y otra parte en la que realizan diferentes pruebas teórico-prácticas para evaluar las competencias previstas en cada asignatura.

Para la aplicación de los porcentajes correspondientes, el estudiante debe haber obtenido una nota mínima de un 4 en cada una de las partes de las que consta el sistema de evaluación continua.

Se considerará que el estudiante supera la asignatura en la convocatoria ordinaria por el sistema de evaluación continua, siempre y cuando al aplicar los porcentajes correspondientes se alcance una calificación mínima de un 5.

Opción 2. Prueba de evaluación de competencias

Los estudiantes que opten por esta vía de evaluación deberán realizar una **prueba de evaluación de competencias (PEC)** y un **examen final presencial (EX)**.

La **PEC** se propone como una prueba que el docente plantea con el objetivo de evaluar en qué medida el estudiante adquiere las competencias definidas en su asignatura. Dicha prueba podrá ser de diversa tipología, ajustándose a las características de la asignatura y garantizando la evaluación de los resultados de aprendizaje definidos. Esta prueba supone el 50 % de la calificación final.

El **examen final presencial**, supondrá el **50 %** de la calificación final. Esta prueba tiene una parte dedicada al control de la identidad de los estudiantes que consiste en la verificación del seguimiento de las actividades formativas desarrolladas en el aula virtual y otra parte en la que realizan diferentes pruebas teórico-prácticas para evaluar las competencias previstas en cada asignatura.

Al igual que con el sistema de evaluación anterior, para la aplicación de los porcentajes correspondientes el estudiante debe haber obtenido una puntuación mínima de un 4 en cada una de las partes de las que consta la opción de prueba de evaluación de competencias.

Se considerará que el estudiante supera la asignatura en la convocatoria ordinaria por el sistema de la prueba de evaluación de competencias siempre y cuando al aplicar los porcentajes correspondientes se alcance una calificación mínima de un 5.

Sistema de evaluación convocatoria extraordinaria

Todos los estudiantes, independientemente de la opción seleccionada, que no superen las pruebas evaluativas en la convocatoria ordinaria tendrán derecho a una convocatoria extraordinaria.

La convocatoria extraordinaria completa consistirá en la realización de una **prueba de evaluación de competencias** que supondrá el **50 %** de la calificación final y un **examen final presencial** cuya calificación será el **50 %** de la calificación final.

Para la aplicación de los porcentajes correspondientes, el estudiante debe haber obtenido una nota mínima de un 4 en cada una de las partes de las que consta el sistema de evaluación de la convocatoria extraordinaria.

	Los estudiantes que hayan suspendido todas las pruebas evaluativas en convocatoria ordinaria (evaluación continua o prueba de evaluación de competencias y examen final) o no se hayan presentado deberán realizar la convocatoria extraordinaria completa, como se recoge en el párrafo anterior. En caso de que hayan alcanzado una puntuación mínima de un 4 en alguna de las pruebas evaluativas de la convocatoria ordinaria (evaluación continua o prueba de evaluación de competencias y examen final), se considerará su calificación para la convocatoria extraordinaria, debiendo el estudiante presentarse a la prueba que no haya alcanzado dicha puntuación o que no haya realizado. En el caso de que el alumno obtenga una puntuación que oscile entre el 4 y el 4,9 en las dos partes de que se compone la convocatoria ordinaria (EC o PEC y examen), solo se considerará para la convocatoria extraordinaria la nota obtenida en la evaluación continua o prueba de evaluación de competencias ordinaria (en función del sistema de evaluación elegido), debiendo el alumno realizar el examen extraordinario para poder superar la asignatura. Al igual que en la convocatoria ordinaria, se entenderá que el alumno ha superado la materia en convocatoria extraordinaria si, aplicando los porcentajes correspondientes, se alcanza una calificación mínima de un 5.

BIBLIOGRAFÍA Y OTROS RECURSOS	
Bibliografía básica	• Altheide, C. y Carvey, H. (2011). *Digital forensics with open source tools*. Elsevier. • Carrier, B. (2005). *Filesystem Forensic Analysis*. Addison Wesley.
Bibliografía complementaria	ISO/IEC 27037. Information technology — Security techniques — Guidelines for identification, collection, acquisition, and preservation of digital evidence. https://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0057481&PDF=Si#.WGoZmbn6nHc Garrido Caballero, J. (2011) *Análisis forense digital en entornos Windows*. Editorial: Zeroxword Computing S.L Lázaro Rodríguez, F. (2015). *Introducción a la informática forense*. España: Editorial RA-MA Lázaro Rodríguez, F. (2015). *Investigación forense de dispositivos Android*. España: Editorial RA-MA. Ludgens, J. T. (2014). *Incident Response and Computer Forensics*. Editorial: McGraw-Hill Education. Martínez Retenaga, A. INCIBE. (2014) *Guía de toma de evidencias en entornos Windows*. https://www.incibe.es/extfrontinteco/img/File/intecocert/ManualesGuias/incibe_toma_evidencias_analisis_forense.pdf Sammons, J. (2014). *The Basics of Digital Forensics*. Editorial: Syngress.

	UNE 71505:2013. Sistema de Gestión de Evidencias Electrónicas. http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0051411#.V86XRzUm_9k UNE 71506:2013. Metodología para el análisis forense de las evidencias electrónicas. http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0051414#.V86XSDUm_9k UNE 197001. Criterios generales para la elaboración de dictámenes periciales. http://www.aenor.es/aenor/actualidad/actualidad/noticias.asp?campo=4&codigo=18886#.WGoZvLn6nHc
Otros recursos	https://www.ccn-cert.cni.es/: Centro Nacional de Respuesta ante Amenazas Informáticas. http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-101r1.pdf: documento del NIST sobre análisis forense en dispositivos móviles. http://www.cftt.nist.gov/: Computer Forensic Testing Tools. http://www.incibe.es: Instituto Nacional de Ciberseguridad de España. http://www.sans.org: página web del Sans Institute con gran cantidad de información sobre seguridad informática. http://www.criptored.upm.es: red temática de seguridad y criptografía, coordinada por el Dr. Jorge Ramió Aguirre y el Dr. Alfonso Muñoz, con interesantes contenidos de nivel tanto técnico como divulgativo. http://www.schneier.com: blog del *hacker* Bruce Schneier, con temas de actualidad sobre seguridad informática. http://www.elladodelmal.com: blog del *hacker* Chema Alonso, con temas de actualidad sobre seguridad informática. https://www.rootedcon.com: página oficial de las conferencias RootedCon, en la que se publican los vídeos de las charlas de ediciones anteriores. http://www.blackhat.com: página oficial de las conferencias BlackHat, en la que se publican los vídeos de las charlas de ediciones anteriores. https://www.defcon.org: página oficial de las conferencias Defcon, en la que se publican los vídeos de las charlas de ediciones anteriores. https://www.youtube.com/watch?v=HHM66N2P0j4: el trabajo de informático forense. https://www.youtube.com/watch?v=ZDJXsiLjIxY: *webminar* sobre informática forense de Caballero Alonso. https://www.wired.com/author/andygreenberg/: artículos de Andy Greenberg sobre seguridad para la revista *Wired*. http://www.forbes.com/security/: noticias de seguridad en la revista *Forbes*. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802fa41c: Convenio sobre la Ciberdelincuencia 2001.

	http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0051414#.V86XSDUm_9k: UNE 71506:2013. http://www.aenor.es/aenor/normas/normas/fichanorma.asp?tipo=N&codigo=N0051411#.V86XRzUm_9k: UNE 71505-1:2013. http://jlrivas.webs.uvigo.es/downloads/publicaciones/Analisis%20forense%20de%20sistemas%20informaticos.pdf: análisis forense de sistemas informáticos de Helena Rifa Pous, Jordi Serra Ruiz y José Luis Rivas López.