Guía Docente: Auditoría e Informática Forense

DATOS GENERALES	
Facultad	Facultad de Ciencias y Tecnología
Titulación	Máster en Ciberseguridad
Plan de estudios	2018
Materia	Análisis de la ciberseguridad
Carácter	Obligatorio
Período de impartición	Segundo Trimestre
Curso	Primero
Nivel/Ciclo	Máster
Créditos ECTS	6
Lengua en la que se imparte	Castellano
Prerrequisitos	No se prevén requisitos previos, por tanto los requisitos serán los propios del título.

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 e Informática Forense
Contexto y sentido de la asignatura en la titulación y perfil profesional	Esta asignatura del Máster de Ciberseguridad ofrece a los alumnos la posibilidad de adquirir conocimientos avanzados en materia de análisis forense informático. El alumno adquirirá los conocimientos avanzados para obtener y preservar las evidencias digitales necesarias para analizar en profundidad un ataque informático. Será capaz de: • Gestionar de forma adecuada los incidentes de seguridad cibernéticos. • 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…). Utilizando diversas normativas y estándares europeos (ISO-UNE) y norteamericanos (ASTM).

COMPETENCIAS QUE ADQUIERE EL ESTUDIANTE Y RESULTADOS DE APRENDIZAJE	
Competencias de la asignatura	• CB7: Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio. • CB8: Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios. • CB9: Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación. • CG1: Ser capaz de analizar, sintetizar y organizar la información dentro del área de seguridad informática y de las comunicaciones • CG3: Diseñar y elaborar concisa, clara y razonadamente planes y proyectos de trabajo en el ámbito de la ciberseguridad. • CE03: Analizar sistemas para encontrar evidencias digitales de ciberataques y adoptar las medidas para mantener la cadena de custodia de dichas evidencias. • CE10: Conocer los conceptos básicos de los principales procesos y respuestas ante incidentes y su aplicación a casos reales.
Resultados de aprendizaje de la asignatura	• Adquirir las competencias básicas y generales detalladas anteriormente. • Conocer la metodología de la informática forense y cómo aplicarla para la obtención de evidencias digitales y el mantenimiento de la cadena de custodia. • Saber aplicar la metodología forense en la preparación del informe pericial para su uso ante un tribunal de justicia. • Comprender cómo la informática forense ayuda a mantener y reforzar la seguridad del sistema informático.

PROGRAMACION DE CONTENIDOS	

Breve descripción de la asignatura	En esta asignatura se verá, entre otros:
	
	• Gestión de incidentes de seguridad:
	  ◦ Prevención del incidente.
	  ◦ Detección y análisis.
	  ◦ Recogida de información.
	• Análisis forense:
	  ◦ Evidencia digital.
	  ◦ Asegurar la escena.
	  ◦ Adquisición de evidencias digitales y recuperación de datos.
	  ◦ Análisis de la evidencia digital e investigación.
	• La Pericial Forense:
	  ◦ La cadena de custodia.
	  ◦ El informe pericial
	• Casos de estudio real

Contenidos	**Unidad 1. Ciberataques y estudio forense post-incidente.** • Convenio de Budapest. • Características de los ciberataques. • Riesgos y amenazas globales. • Perfiles de los atacantes. • Metodologia del estudio forense post-incidente. **Unidad 2**. **Elaboración de informes y dictámenes periciales.** • Protocolo de actuación para pericias informáticas. • Aplicación práctica UNE 197010-2015-JLN. • Criterios generales para la elaboración de informes y dictámenes periciales sobre tecnologías de la Información y las Comunicaciones (TIC). **Unidad 3. Preservación de la evidencia electrónica** • Introducción. • Adquisición y copia forense. • La cadena de custodia: fuente de prueba de dispositivos informáticos y electrónicos. **Unidad 4. Metodología de trabajo en el ámbito forense.** • Adquisición y gestión de la cadena de custodia. • Documentación y montaje del informe • Conclusiones • Ratificación en sede judicial **Unidad 5. Análisis forense avanzado aplicado a Windows/Linux/IOS** • Herramientas forenses • Herramientas genéricas • Criterios de decisión y estrategia **Unidad 6**. Análisis forense aplicado a sistemas operativos móviles • Tipología de extracción forense en dispositivos móviles, tabletas y drones. • Metodología UFED • Metodología MSAB XRY-XAMM

	• Extracción avanzada en dispositivos no funcionales y destruidos • Chip-off y microread de dispositivos Android y Apple.

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	Jhon R. Vacca (2013). Cyber Security and IT Infrastructure Protection 1st Edition. United States of America. SYNGRESS. Julie Lucas&Brian Moeller (2003), The Effective Incident Response Team Paperback. USA.ELSEVIER Schatz BL (2014), Wirespeed: Extending the AFF4 container format for scalable acquisition and live analysis. Digital Investigation. Schatz BL (2014), A visual approach to interpreting NAND flash memory Digital Investigation (preprint here). White A, Schatz BL, Foo E (2013),Integrity Verification of User Space Code DFRWS Conference, Monterey, USA. Heather Mahalik, Satish Bommisetty (2016), Practical Mobile Forensics - Second Edition Paperback 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

Rambla, J. L. (2013). *Un forense llevado a juicio*. España. http://www.sw-computacion.f2s.com/Linux/Un_forense_llevado_a_juicio.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