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	Roberto Cuesta Calvo	**Correo electrónico**	roberto.cuesta@ui1.es
Área		**Facultad**	Facultad de Ciencias y Tecnología
Perfil Profesional 2.0	En la Actualidad Comandante de la Guardia Civil desempeñando labor en la Jefatura Servicios Técnicos (Dirección General de la GC). Mi formación, entre otras es la de: • Ingeniero Informático. Universidad de Burgos [2006]. • Máster Universitario en Dirección TIC para la Defensa. Universidad de Vigo [Marín, 2019-2021] • Ingeniería Técnica en Informática de Gestión. Universidad de Burgos. [2003]. • ... Publicaciones, conferencias: • Conferencia “Plataforma de Gestión y Ciberseguridad para dispositivos Móviles” dentro del I Curso Universitario en Competencias Digitales Docentes en Centro Universitario de Guardia Civil en Aranjuez, Madrid. [2023] • Publicación Primeros Resultados Tesis sobre la Delincuencia en España, Revista CAEPIA. [2018] • XVIII Conferencia de la Asociación Española de Intelifencia Artificial - Predicción de delincuencia con datos públicos. [Granada 2018] • Conferencia “Integración continua en la Guardia Civil” en la Universidad de Vigo, Campus Orense [2019]. • Conferencia “Ingeniería Informática como marca de calidad en la Guardia Civil” en la Universidad de Vigo, en la escuela de Aeronaútica en el Campus de Orense [2019]. • Conferencia “Ingeniería Informática como marca de calidad en la Guardia Civil” en la Universidad de Vigo, en la escuela de Aeronaútica en el Campus de Orense [2019]. • Conferencia “Ingeniería Software y desarrollo de Proyectos” en la Universidad de Vigo, en la escuela de Ingeniería en Telecomunicación en el Campus Vigo [2020]. • Libro de estudio sobre Protección de Informaciones, Ciberseguridad con déposito legal: DL ZA 31-2020. [2020] • Libro de estudio sobre Laboratorio Práctico de análisis de ciberataque y procesos decisionales con déposito legal. • Publicación y demostración resultados y tecnologías GIS GC en reunión anual ESRI-España. [2015-2021] Para más información sobre experiencia laboral u otros: https://www.linkedin.com/in/roberto-cuesta-calvo-924ab915		

CONTEXTUALIZACIÓN Y JUSTIFICACIÓN DE LA ASIGNATURA	
Asignaturas de la materia	• Auditoría e Informática Forense • Hacking Ético
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, NIST).

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: Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades. • 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. • Riesgos y amenazas globales. • Gestión del incidente: etapas. • Definición de procesos críticos de negocio. **Unidad 2. Elaboración de informes y dictámenes periciales.** • Protocolo de actuación para pericias informáticas. • Aplicación práctica UNE 197010:2015. **Unidad 3. Preservación de la evidencia electrónica.** • ¿Qué es un perito informático? • Preservación de la evidencia electrónica. • 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 del informe. • Ratificación en sede judicial. **Unidad 5. Análisis forense avanzado aplicado a Windows/Linux/IOS.** • Análisis de la memoria RAM. • Análisis de sistemas Windows. • Análisis de sistemas Linux. • Análisis de sistemas. **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	Para el desarrollo de la asignatura se llevarán a cabo las siguientes actividades: **Foros de debate:** actividad en la que se discutirá y argumentará acerca de diferentes temas relacionados con la asignatura. **Estudio de caso:** actividad en la que el alumno podrá llevar a cabo un aprendizaje contextualizado trabajando una situación real o simulada que le servirá para guiar el proceso de descubrimiento inducido. **Trabajo colaborativo:** en esta tarea se deberá reflexionar sobre alguno de los temas planteados y entablar un diálogo y debate con el resto de estudiantes para presentar un trabajo conjunto. **Cuestionarios:** cuestionario evaluable que servirán para poner a prueba los conocimientos adquiridos. **Actividades de contenidos:** Al igual que el cuestionario, pone a prueba los conocimientos adquiridos mediante la resolución de ejercicios prácticos. **Videotutorías**: sesiones en directo, que pueden visualizarse en diferido, donde se expone la resolución de las dudas presentadas al profesor previamente. **Lectura crítica, análisis e investigación**: se trata de actividades en las que el alumno se acerca a los diferentes campos de estudio con una mirada crítica que le permite un acercamiento a la investigación. **Prueba de Evaluación por Competencias (PEC)**: En el caso de optar por la opción de evaluación (PEC+ examen final), el estudiante tendrá que realizar la prueba de evaluación de competencias (PEC). Esta prueba se define como una actividad integradora a través de la cual el estudiante deberá demostrar la adquisición de competencias propuestas en la asignatura, vinculadas principalmente al «saber hacer». Para ello hará entrega de un conjunto de evidencias en respuesta a los retos propuestos en esta prueba. La entrega se realizará antes de finalizar la asignatura.

EVALUACIÓN	
Sistema evaluativo	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.

Características de los exámenes

Los exámenes constarán de 30 ítems compuestos por un enunciado y cuatro opciones de respuesta, de las cuales solo una será la correcta. Tendrán una duración de 90 minutos y la calificación resultará de otorgar 1 punto a cada respuesta correcta, descontar 0,33 puntos por cada respuesta incorrecta y no puntuar las no contestadas. Después, con el

resultado total, se establece una relación de proporcionalidad en una escala de 10.

* Los estudiantes que realicen el máster por formación bonificada (FUNDAE) deberán acogerse a la opción 1 del sistema de evaluación, evaluación continua (EC)+ examen final (EX).

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	[1] C. Altheide and H. A. Carvey, «Digital forensics with open source tools». Syngress, 2012. Disponible en: https://dcatalogo.ui1.es/cgi-bin/koha/opac-detail.pl?biblionumber=1339 [2] Schatz, Bradley L., «Wirespeed: Extending the AFF4 forensic container format for scalable acquisition and live analysis». Proceedings of the Digital Forensic Research Conference, DFRWS. 2015, vol. 14, pp. S45-S54. Disponible en: https://www.sciencedirect.com/science/article/pii/S1742287615000614?via%3Dihub
Bibliografía complementaria	[1] J. Vacca, «Cyber security and IT infrastructure protection», 1st ed. Syngress. Elsevier, 2014. Disponible en: https://dcatalogo.ui1.es/cgi-bin/koha/opac-detail.pl?biblionumber=1925 [2] R. Chandramouli, A. Singhal, D. Wijesekera, y C. Liu, «A Methodology for Enabling Forensic Analysis Using Hypervisor Vulnerabilities Data», NISTIR 8221 , jun. 2019. [3] M. Guerra Soto, Análisis forense informático. RA-MA EDITORIAL, 2021. [4] Y. Diogenes and E. Ozkaya, «Cybersecurity, attack and defense strategies». Packt Publishing, 2019. Disponible en: https://dcatalogo.ui1.es/cgi-bin/koha/opac-detail.pl?biblionumber=2697
Otros recursos	UNE 71505-1:2013. Sistema de Gestión de Evidencias Electrónicas. Parte 1: Vocabulario y principios generales. https://tienda.aenor.com/norma-une-71505-1-2013-n0051411 UNE 71505-2:2013. Sistema de Gestión de Evidencias Electrónicas. Parte 2: Buenas prácticas en la gestión de las evidencias electrónicas. https://tienda.aenor.com/norma-une-71505-2-2013-n0051412 UNE 71505-3:2013. Sistema de Gestión de Evidencias Electrónicas. Parte 3: Formatos y mecanismos técnicos. https://tienda.aenor.com/norma-une-71505-3-2013-n0051413 UNE 71506:2013. Metodología para el análisis forense de las evidencias electrónicas. https://tienda.aenor.com/norma-une-71506-2013-n0051414 UNE 197001. Criterios generales para la elaboración de dictámenes periciales. https://tienda.aenor.com/norma-une-197001-2019-n0062378