Informática Forense

Curso Académico: (2021 / 2022) **Fecha de revisión: 08-06-2021**

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: PERIS LOPEZ, PEDRO

Tipo: Optativa Créditos ECTS : 6.0

Curso : 4 Cuatrimestre :

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

Sistemas Operativos.
Redes de Ordenadores.
Seguridad en las Tecnologías de la Información.
Ingeniería de la Seguridad.

OBJETIVOS

El curso cubre las herramientas forenses, métodos y procedimientos utilizados para la investigación de delitos informáticos; técnicas de recuperación, análisis y protección de evidencias; y el desarrollo de habilidades cómo perito informático.

Una vez completado el curso, el estudiante será capaz de:
(PO a, b, c, d, e, f, g, j, k)

1. Conocer la metodología utilizada en investigaciones forenses informáticas.
2. Conocer y usar métodos de recuperación de evidencias.
3. Usar y evaluar diferentes técnicas de análisis de evidencias en sistemas de ficheros, memoria y red.
4. Instalar, configurar y usar herramientas de análisis forense.
5. Familiarizarse con diversos dispositivos hardware empleados en análisis forense de equipos informáticos.
6. Manipular y organizar evidencias forenses de forma sistemática.
7. Trabajar en equipo, redactar informes forenses y exponerlos en público.
8. Conocer los estándares y regulaciones legales asociados con las investigaciones forenses de equipos informáticos.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

1. Módulo 1:
   a. Introducción
   b. Conceptos técnicos clave

2. Módulo 2:
   a. Laboratorio y herramientas
   b. Obtención y archivado de evidencias

3. Módulo 3:
   a. Herramientas y técnicas anti-forense
   b. Internet y correo electrónico

4. Módulo 4:
   a. Forense en redes de ordenadores
   b. Forense en dispositivos móviles

5. Módulo 5:
   a. Estándares y normativas
   b. Aspectos legales

ACTIVIDADES FORMATIVAS, METODOLOGÍA A UTILIZAR Y RÉGIMEN DE TUTORÍAS

Clases magistrales, donde se presentarán los conocimientos que los alumnos deben adquirir. Para facilitar su desarrollo los alumnos recibirán las notas de clase y diversos documentos en la herramienta

web oportuna y tendrán textos básicos de referencia que les permita completar y profundizar en aquellos temas en los cuales estén más interesados.

Clases en aula informáticas donde se aprenderá el uso de herramientas de análisis forense, adquisición y custodia de herramientas forenses. El profesor podrá exponer casos reales de ejercicios forense y el alumno tendrá que resolver diferentes casos prácticos que le ayudarán a la consolidación de los conocimientos teóricos así como a la familiarización con las herramientas forenses.

SISTEMA DE EVALUACIÓN

La evaluación se basará en los siguientes criterios:

Resolución de prácticas de laboratorio (casos forenses) a lo largo de las clases en aulas informáticas: 50% de la nota final. Estas prácticas tienen carácter obligatorio y se evaluarán mediante la corrección de los trabajos correspondientes y los informes entregados. (PO a, b, c, d, e, f, g, j, k)

Examen final: 50%. La realización de examen final es obligatoria, siendo necesario obtener, al menos, el 50% de la nota máxima posible en este examen para poder superar la asignatura. (PO a,b,c,d,e,f,g,j,k)

Aquellos alumnos que no sigan la evaluación continua realizarán un examen de toda la materia, distinto del que realicen los que sigan la evaluación continua.

En la convocatoria extraordinaria, el alumno que no haya seguido la evaluación continua o no la haya superado podrá, si lo desea, entregar los trabajos correspondientes (incluidos los que atañen a las prácticas de laboratorio) y realizar un examen, calificándose la asignatura de la misma manera que en la convocatoria ordinaria. Alternativamente, podrá realizar exclusivamente un examen global de toda la materia (distinto al que realicen los que sigan la evaluación continua), y que valdrá el 100% de la nota final.

Peso porcentual del Examen Final:	50
Peso porcentual del resto de la evaluación:	50

BIBLIOGRAFÍA BÁSICA

- Brian Carrier File System Forensic Analysis, Addison-Wesley.
- Cory Altheide and Harlan Carvey Digital Forensics with Open Source Tools, Syngress Media.
- John Sammons The Basics of Digital Forensics. , Syngress.
- Nelson et al. Guide To Computer Forensics and Investigations. , Cengage Learning.

BIBLIOGRAFÍA COMPLEMENTARIA

- Eoghan Casey Handbook of Digital Forensics and Investigation, Academic Press Inc.
- Harlan Cavey Windows Registry Forensics: Advanced Digital Forensic Analysis of the Windows Registry, Syngress Media.