Informática Forense

Curso Académico: (2023 / 2024) **Fecha de revisión: 28-04-2023**

Departamento asignado a la asignatura: Departamento de Informática

Coordinador/a: PERIS LOPEZ, PEDRO

Tipo: Optativa Créditos ECTS : 3.0

Curso : 4 Cuatrimestre : 2

REQUISITOS (ASIGNATURAS O MATERIAS CUYO CONOCIMIENTO SE PRESUPONE)

1. Programación.
2. Técnicas de Ocultación de la Información.
3. Marco Jurídico de la Seguridad.
4. Vulnerabilidades, Amenazas y Protocolos de Seguridad Informáticos.
5. Ciencias Forenses I.

OBJETIVOS

- Identificar los objetivos de seguridad y las vulnerabilidades, amenazas y riesgos de un sistema de información dado en un entorno operacional definido. Analizar las posibles medidas de seguridad a emplear en el mismo.
- Evaluar los servicios de seguridad a implementar en un sistema dado y diseñar y aplicar los mecanismos y protocolos consiguientes.
- Evaluar para un sistema dado las herramientas existentes de cifrado y esteganográficas para protegerlo.
- Usar los sistemas de firma y certificación en un entorno concreto. Evaluar y aplicar los mecanismos de autenticación pertinentes para acceder a un sistema específico.
- Diseñar un plan de seguridad, desarrollando las distintas partes del mismo, evaluando su cumplimiento a lo largo del tiempo y corrigiendo sus desviaciones. Analizar y gestionar los riesgos de una instalación determinada.
- Elaborar un plan de recuperación integral de una instalación real. Realizar una auditoría de cumplimiento de los ficheros y sistemas conteniendo datos de carácter personal.
- Usar los instrumentos que permiten el control de los sistemas operativos, principalmente Windows y Linux.
- Manejar las principales técnicas de recopilación, identificación y análisis de sucesos, garantizando el aseguramiento de las pruebas y preservando la cadena de custodia de las mismas. Evaluar y manejar los sistemas de borrado seguro y de recuperación de datos.
- Implementar bases de datos sobre un sistema gestor. Evaluar y emplear las diferentes técnicas que integran la minería de datos: técnicas de análisis y extracción de modelos.

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:

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. Redactar informes forenses.
8. Conocer los estándares y regulaciones legales asociados con las investigaciones forenses de equipos informáticos.

DESCRIPCIÓN DE CONTENIDOS: PROGRAMA

Módulo 1:

a. Introducción.
b. Conceptos técnicos clave.

Módulo 2:

a. Laboratorio y herramientas.
b. Obtención y archivado de evidencias.
c. Informe Forense.

Módulo 3:

a. Destrucción de datos.
b. Cifrado.
c. Esteganografía y Canales Encubiertos.

Módulo 4:

a. Internet & Correo Electrónico.
b. Registros (logs).
c. Evidencias de Red.
d. Cloud.

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

El sistema de evaluación incluye la evaluación continua del trabajo del alumno (pruebas de evaluación de habilidades y conocimientos teórico-prácticos e informes de prácticas de laboratorio) y la evaluación final a través de un examen escrito en que se evaluará de forma global los conocimientos, destrezas y capacidades adquiridas a lo largo del curso. La evaluación de la asignatura se realizará de acuerdo con los siguientes criterios:

1. Exámenes escritos de teoría y problemas: 70% de la nota final
   1.1. Exámenes de evaluación continua: 10% de la nota final. Aproximadamente a mediados del cuatrimestre.
   1.2. Examen escrito final de teoría y problemas: 60% de la nota final. Para superar la asignatura el alumno debe obtener un mínimo de 4 puntos en este examen.
2.Prácticas: 30% de la nota final

En la convocatoria extraordinaria, el alumno elegirá entre:
a) Un examen final escrito por valor del 100% de la nota, compuesto de teoría, problemas y conocimientos adquiridos en las sesiones de laboratorio; o
b) Un examen final escrito por valor del 60% de la nota, compuesto de teoría y problemas. El restante 40% provendrá de la nota obtenida durante el curso en el examen de evaluación continua (10%) y las prácticas (30%)

Peso porcentual del Examen Final:	60
Peso porcentual del resto de la evaluación:	40

BIBLIOGRAFÍA BÁSICA

- Brian Carrier File System Forensic Analysis., Addison-Wesley Professional.
- 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.