1. IDENTIFICACIÓN DEL CURSO

Nombre de la materia

Análisis Forense Digital

Clave de la materia:	Horas de teoría:	Horas de práctica:	Total de Horas:	Valor en créditos:
IC464	**40**	**40**	**80**	**8**

Tipo de curso: (Marque con una X)											
C= curso		P= practica		**CT = curso–taller**	**x**	M= módulo		C= clínica		S= seminario	

Nivel en que ubica: (Marque con una X)			
L=Licenciatura	**x**	P=Posgrado	

Prerrequisitos formales (Materias previas establecidas en el Plan de Estudios)	Prerrequisitos recomendados (Materias sugeridas en la ruta académica aprobada)
Ninguno	

Departamento:

Ciencias Exactas y Tecnología (DCET)

Carrera(s):

Licenciatura en Tecnologías de la Información (LTIN)

Área de formación:

Área de formación básica común obligatoria.		Área de formación básica particular obligatoria.		Área de formación básica particular selectiva.		**Área de formación especializante selectiva.**	**X**	Área de formación optativa abierta.	

Historial de revisiones:

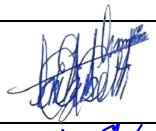
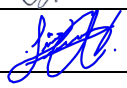
Acción: **Revisión, Elaboración**	**Fecha:**	**Responsable**
Elaboración	**13/03/2018**	**Mtro. Víctor Becerra Córdoba**

Revisión	**15/01/2019**	**Dr. Héctor Alfonso Juárez López**
Revisión	**Enero 2021**	**Mtra. María del Rocío Ramírez**
Revisión	**Enero 2023**	**Mtra. María del Rocío Ramírez**

Academia:

Cómputo

Aval de la Academia:

Marzo 2023		
Nombre	**Cargo** Presidente, Secretario, Vocales	**Firma**
Mtra. Larisa ElizabethLara Ramírez	**Presidente**	
Dra. Auria Lucia JiménezGutiérrez	**Secretario**	

2. PRESENTACIÓN

El presente curso tiene como fin introducir al alumno al campo del cómputo forense, así como darle elemento de reflexión y habilidades técnicas para trabajar seguridad en sistemas informáticos

3. OBJETIVO GENERAL

Que el alumno adquiera los conocimientos necesarios para realizar un análisis forense digital, con un enfoque teórico práctico, aplicando técnicas de cómputo forense, abarcando las áreas legales e informáticas

4. OBJETIVOS ESPECÍFICOS

- El alumno conozca algunas leyes relacionadas con el quehacer informático yciberdelitos en general

- Que el alumno conozca los elementos básicos del proceso de análisis forense

- Que el alumno maneje aplicaciones y scripts que le permitan realizar análisis forense adispositivos Windows, Linux y Mac

- Que el alumno conozca los elementos básicos para realizar análisis forense a redes y adispositivos móviles.

5. CONTENIDO

Temas y Subtemas
Módulo I. Derecho Informático y Ciberdelitos
1.1 Introducción al Derecho Informático
1.2 Ciberdelitos
1.3 Legislación actual
Módulo II. Introducción al cómputo forense
2.1 Conceptos básicos
2.2 Cadena de custodia
2.3 Dictamen pericial
Módulo III. Configurando el sistema de análisis
3.1 Software e interpretes
3.2 Usando Linux como sistema base (kali)
3.3 Usando Windows como sistema base
Módulo IV. Análisis del disco y sistema de archivos
4.1 Modelo abstracto del sistema de archivos
4.2 Autopsy y The sleuth kit
4.3 Particionado y contenedores especiales
4.4 Hashing y carving
4.5 Imágenes forenses de disco
Módulo V. Sistemas y sus artefactos
5.1 Sistema de archivos de Windows
5.2 Registros y eventos
5.3 Ejecutables de Windows

5.4 Sistema de archivos Linux

5.5 Propiedad, permisos y otros atributos de archivos

5.6 Cuentas de usuario

5.7 Logs

5.8 Estructura de archivos HFS+

5.9 Artefactos de usuario

Módulo VI. Otros temas

6.1 Análisis de dispositivos móviles

6.2 Análisis de redes

6.3 Datos volátiles

6. TAREAS, ACCIONES Y/O PRÁCTICAS DE LABORATORIO

a) Aprendizaje grupal y autogestivo
b) Investigación grupal e individual.
c) Integración individual de productos de aprendizaje (reportes de lectura, ensayos, trabajos de investigación, exposición de temas, prácticas de algunos temas, portafolio, entre otros).
d) Exposición por parte del maestro sobre los temas (pizarrón, diapositivas, etc.).

7. BIBLIOGRAFÍA BÁSICA (Preferentemente ediciones recientes, 5 años)

1	Richard Boddington, Practical Digital Forensics, Packt Publishing Ltd, 2016,ISBN 978-1-78588-710-9
2	Carvey, Harlan autor. Windows Forensic Analysis Toolkit Advanced Analysis Techniques for Windows 8. MA, USA Syngress, ELSEVIER 2014.
2	Fonseca Vivas, Alvaro. Auditoría forense aplicada al campo administrativo y financiero, medio ambiente, cultural, social, política y tecnología Álvaro Fonseca Vivas. -- Bogotá, Colombia Ediciones de la U. ©2015.

8. BIBLIOGRAFÍA COMPLEMENTARIA (Preferentemente ediciones recientes, 5 años)

1	Christopher L. T. Brown, Computer Evidence: Collection And Preservation, Second Edition, Cengage Learning, 2011
2	Michael Hale Ligh, Andrew Case, Jamie Levy, AAron Walters, The Art of Memory Forensics: Detecting Malware and Threats in Windows, Linux, and Mac Memory, Wiley, 2014, ISBN: 978-1-118-82509-9

3	P. W. Singer And Allan Friedman, Cybersecurity And Cyberwar: What Everyone Needs ToKnow, Oxford University Press, 2014, ISBN 978–0–19–991809–6

9. CRITERIOS Y MECANISMOS PARA LA ACREDITACION

- Aprendizaje grupal y autogestión.

- Integración de equipos para la solución de problemas

- Integración individual de productos de aprendizaje (reportes de lectura, ensayos, formatos de intervención, trabajos de investigación, presentaciones, entre otros).

10. EVALUACIÓN Y CALIFICACIÓN

Unidad de Competencia	Porcentaje
Trabajo final	35%
Promedio de Tareas	35%
Entrega de prácticas	30%
Total	**100%**

11. ATRIBUTOS DEL EGRESADO RELACIONADOS CON EL PROGRAMA DE ESTUDIOS

1. Identificar, formular y resolver problemas de ingeniería aplicando los principios de las ciencias básicas e ingeniería.

2. Aplicar, analizar y sintetizar procesos de diseño de ingeniería que resulten en proyectos que cumplen las necesidades especificadas.

3. Reconocer la necesidad permanente de conocimiento adicional y tener la habilidad para localizar, evaluar, integrar y aplicar este conocimiento adecuadamente.

4. Trabajar efectivamente en equipos que establecen metas, planean tareas, cumplen fechas límite y analizan riesgos e incertidumbre.

12. INDICADORES DE RESULTADOS DE APRENDIZAJE

Principales resultados de aprendizaje: ¿Qué es lo que seespera que aprenda el estudiante?	1	El alumno conozca algunas leyes relacionadas con el quehacer informático yciberdelitos en general.
	2	Que el alumno conozca los elementos básicos del proceso de análisis forense.
	3	Que el alumno maneje aplicaciones para el análisis forense.