INFORMACIÓN ESPACIO ACADÉMICO						
Nombre de asignatura	**Análisis Forense - Electiva IV**					
Código	11504002					
Definición de asignatura	***Obligatorio***	***X***	***Básico***		***Complementario***	
	Electivo		***Intrínseco***	***X***	***Extrínseco***	
Número de créditos	*3*	***Horas***	*144*	***Semanas***	*16*	
Distribución créditos	***HTD***	*64*	***HTC***	*32*	***HTA***	48
	HORAS DE TRABAJO COOPERATIVO					
Metodología	Virtual					

PROGRAMACIÓN DEL CONTENIDO

CONOCIMIENTOS PREVIOS

- Conceptos de Ciberseguridad
- Conceptos de Sistemas Operativos
- Registros de Eventos
- Eventos de usuario
- Sistemas de archivos
- Conceptos de nube o Cloud
- Conocimientos en bases de datos
- CLI
- Redes – Networking
- Dispositivos de almacenamiento
- Infraestructura (servidores)
- Conceptos básicos de criptografía

DESCRIPCIÓN DEL CURSO

En este curso se abordarán los componentes implicados en una investigación o análisis forense digital, partiendo desde lo más básico como lo son los fundamentos de la informática forense, hasta considerar la creciente importancia de los dispositivos móviles y el uso de la tecnología de almacenamiento en la nube. Se revisarán diversas técnicas de recolección, preservación, análisis y presentación de pruebas o evidencias digitales basadas en las buenas prácticas y recomendaciones dadas por las distintas normativas vigentes asociadas a la informática forense. También se explorará el marco legal nacional en relación a los aspectos legales involucrados, con

el objetivo de llevar a cabo el debido proceso de adquisición, procesamiento y puesta a disposición de evidencias digitales cumpliendo con los requerimientos legales correspondientes. El análisis, aplicación de diferentes metodologías de recolección o adquisición se estudiarán en diferentes áreas tales como: sistemas operativos, redes y bases de datos.

ÁREAS DE CONOCIMIENTO

- Ciberseguridad y Ciberdefensa
- Sistemas Operativos
- Bases de datos
- Redes - Networking
- Informática Forense
- Infraestructura de comunicaciones
- Seguridad de la Información
- Normatividad
- Análisis de datos
- Gestión de registros (logs)

COMPETENCIAS EN FORMACIÓN

- Obtención de información, diseño de prácticas y laboratorios y posterior análisis de resultados.
- Identificación de métodos de investigación aplicados en el área del cómputo forense.
- Identificación del marco jurídico y legal que rige la informática forense en el ámbito nacional e internacional.
- Resolución de problemas asociados al análisis forense.
- Capacidad técnica y analítica de identificación de mensajes de datos que puedan ser parte de una evidencia digital o convertirse en un elemento material probatorio.
- Reconocimiento de documentación asociada a las diferentes etapas dentro del análisis forense basado en el modelo EDRM (Electronic Discovery Reference Model).
- Investigación digital basado en evidencias digitales recolectadas
- Identificación de fundamentos y principios de elaboración de un informe de análisis forense
- Manejo y aprendizaje de herramientas utilizadas en las diferentes etapas del análisis forense

ESTRUCTURA DEL MÓDULO

UNIDAD 1. FUNDAMENTOS DE INFORMÁTICA FORENSE

OBJETIVO DE APRENDIZAJE	*TÍTULO DE TEMA*
Estudiar los fundamentos de la informática forense basados en el entendimiento del concepto de imagen forense.	FUNDAMENTOS DE INFORMÁTICA FORENSE
	CIBESEGURIDAD Y CIBERDEFENSA
	SISTEMAS DE ARCHIVOS
	IMÁGENES FORENSES

UNIDAD 2. ADQUISICIÓN DE IMÁGENES FORENSES	
OBJETIVO DE APRENDIZAJE	***TÍTULO DE TEMA***
Estudiar los diferentes tipos de adquisición de evidencia digital y conocer algunas herramientas utilizadas para esta tarea.	MODELO EDRM
	FORMATOS Y DOCUMENTACIÓN
	BUENAS PRÁCTICAS Y PROCEDIMIENTOS
	HERRAMIENTAS FORENSES
UNIDAD 3. DERECHO INFORMÁTICO	
OBJETIVO DE APRENDIZAJE	***TÍTULO DE TEMA***
Conocer toda la normatividad y apartado legal que rige los principios y actuaciones de la informática forense y seguridad digital.	ISO 27037
	EVIDENCIA DIGITAL
	INVESTIGACIÓN DE DELITOS INFORMÁTICOS
	PROTECCIÓN DE DATOS EN EL ANÁLISIS FORENSE
UNIDAD 4. ANÁLISIS FORENSE	
OBJETIVO DE APRENDIZAJE	***TÍTULO DE TEMA***
Comprender los diferentes tipos de análisis forense, así como algunas herramientas utilizadas en esta área en distintos dispositivos.	TIPOS DE ANÁLISIS FORENSE
	DISPOSITIVOS DE ALMACENAMIENTO
	CLOUD
	HERRAMIENTAS FORENSES

Tenga en cuenta las siguientes **estrategias de aprendizaje** para el planteamiento de las actividades de evaluación:

- **Estudio autónomo**: lectura y revisión de las unidades, de los recursos tales como videos, lecturas, hipervínculos, investigación, exploración en redes académicas
- **Tutoría:** revisión de clases magistrales virtuales, asistencia a tutoría virtuales presenciales, comunicación con el tutor y aclaración de dudas.
- **Autoevaluaciones:** cuestionarios de evaluación en línea
- **Prácticas:** actividades durante el desarrollo del curso de diferente índole, orientadas a proyectos, problemas, investigación, estudio de caso, entre otras
- **Trabajo final**: elaboración de una actividad que integra lo desarrollado durante el curso, la cual se debe entregar la última semana del curso.
- **Notas**: las actividades se pueden desarrollar tanto individual como grupal, según criterio del docente.

EVALUACIÓN		
TIPO	**EVALUACIÓN/ACTIVIDAD**	**PORCENTAJE**
Formativa	Evaluación Unidad 1	10%
Formativa	Evaluación Unidad 2	10%
Formativa	Evaluación Unidad 3	10%
Formativa	Evaluación Unidad 4	10%
Formativa	Prácticas y/o Laboratorios	20%

Tutorías	Asistencia	10%
Formativa	Trabajo Final	30%
	Total del curso	**100 %**

BIBLIOGRAFÍA	
1	DOMINGUEZ, F. L. (2013). Introducción a la Informática Forense.
2	NIKKEL, B. (2021). Practical Linux Forensics: A Guide for Digital Investigators.
3	PHILIPP, A., COWEN, D., & DAVIS, C. (2009). Hacking Exposed Computer Forensics, Second Edition: Computer Forensics Secrets & Solutions
4	HAYES, D. R. (2014). A Practical Guide to Computer Forensics Investigations.
5	CASEY, E. (2001). Handbook of Computer Crime Investigation: Forensic Tools and Technology.
6	International Organization for Standardization. (2012). Information technology — Security techniques — Guidelines for identification, collection, acquisition and preservation of digital evidence (ISO 27037).
7	International Organization for Standardization. (2015). Information technology — Security techniques — Guidelines for the analysis and interpretation of digital evidence (ISO 27042).
8	National Institute of Justice. (2004). Forensic Examination of Digital Evidence: A Guide for Law Enforcement (NIJ 199408).
9	Fiscalía General de la Nación. (2012). Manual de Procedimientos para Cadena de Custodia.
10	ROMERO CASTRO, M. I., FIGUEROA MORÁN, G.G., VERA NAVARRETE, D.S., ÁLVALA CRUZATTY, J.E., PARRALES ANZULES, G.R., ÁLAVA MERO, C.J., MURILLO QUIMIZ, Á.L., & CASTILLO MERINO, M.A. (2018). Introdución a la seguridad informática y el análisis de vulnerabilidades.
11	GUERRA SOTO, M. (2021). Análisis Forense Informático.
12	Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales. 18 de octubre de 2012. D.O. No. 48587.
13	CHEN, L. (2019). Security, Privacy, and Digital Forensics in the Cloud (LEI CHEN, H. TABAKI, & N.-A. LE-KHAC, Eds.). JOHN WILEY & SONS.

ORGANIZACIÓN / TIEMPOS																
PROGRAMA SINTÉTICO		**SEMANAS ACADÉMICAS**														
		1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**	**14**	**15**	**16**
1.	FUNDAMENTOS DE INFORMÁTICA FORENSE	X	X	X	X												
2.	ADQUISICIÓN DE IMÁGENES FORENSES					X	X	X	X								
3.	DERECHO INFORMÁTICO									X	X	X	X				
4.	ANÁLISIS FORENSE													X	X	X	X

ELABORÓ: Diego Fernando Espinel Gómez
15/06/2023