1. Identificación del Curso/ Módulo

Nombre del Curso/ Módulo: **INFORMATICA FORENSE**	Línea de conocimiento: **DEPE**	Código de materia: **DEPE 25029**	Número de creditos: **2**

Facultad/ Departamento	**FAC DE ESTUDIOS TECNI Y TECNOL**					
Programa que Administra el curso o módulo	**TECN EN INVES CRIM Y CIENC FO**					
Niveles de Formación	Técnico Profesional		Especialización			
	Tecnológico Profesional	X	Maestría			
	Profesional		Doctorado			
Modalidad	Presencial	X	Dual		Virtual	
Número de horas con acompañamiento del profesor: 2			Número de horas de trabajo independiente: 2			
Fecha de actualización de la guía: 22/03/2023						

2. Conocimientos previos requeridos para el curso

Ninguno.

3. Justificación

La informática forense es una disciplina crucial en la lucha contra los ciberataques y el crimen cibernético. En Colombia y en todo el mundo, la tecnología se ha convertido en una herramienta esencial para la realización de actividades económicas, sociales y gubernamentales. Sin embargo, también se ha convertido en una fuente de vulnerabilidad que ha permitido el surgimiento de amenazas digitales. La informática forense es un conjunto de técnicas, herramientas y metodologías que se utilizan para investigar y analizar delitos informáticos. Esta disciplina se enfoca en la recolección, preservación, análisis y presentación de pruebas digitales. La importancia de la informática forense radica en que permite identificar, rastrear y capturar a los delincuentes que han cometido crímenes cibernéticos. En Colombia, la informática forense es una herramienta importante para combatir el crimen cibernético. El país ha experimentado un aumento en el número de delitos informáticos en los últimos años, y la informática forense se ha convertido en una herramienta clave para investigar estos delitos. Los expertos en informática forense pueden rastrear y analizar la información en los sistemas informáticos para identificar a los responsables de los delitos cibernéticos y proporcionar pruebas válidas en los tribunales. En el mundo, la importancia de la informática forense se ha vuelto cada vez más evidente. Los ciberataques son una amenaza constante para las empresas, organizaciones y gobiernos. La informática forense es una herramienta importante para combatir estas amenazas y proporcionar pruebas que pueden ser utilizadas en la corte.

4. Competencias de formación

Id	Competencia	Resultado de aprendizaje esperado
1	Describe los conceptos relacionados con la ciberseguridad para aplicarlos a la gestión de los ciberataques.	1 - Comprende los conceptos relacionados con el cubo de destrezas de la ciberseguridad. 2 - Diferencia los tipos de ciberataques y sus contramedidas a través de análisis de casos. 3 - Emplea las actividades de las fases de respuesta ante un incidente de seguridad de la información para gestionarlo de manera efectiva a través de un estudio de caso.
2	Asocia la informática forense y la evidencia digital para la investigación de delitos informáticos en el marco legal colombiano.	1 - Explica los conceptos relacionados con la informática forense y la evidencia digital. 2 - Reconoce la normatividad asociada a la seguridad de la información y los delitos informáticos en el contexto penal colombiano. 3 - Establece la importancia de la informática forense y la evidencia digital para la investigación de delitos informáticos a través de los estudios de caso y la discusión en grupo.

Id	Competencia	Resultado de aprendizaje esperado
3	Emplea las herramientas forenses para la identificación, preservación, análisis y presentación de la evidencia digital.	1 - Determina las fuentes de información que deben ser preservadas para una investigación. 2 - Utiliza técnicas de cómputo forense para la recolección y generación de copias exactas de un dispositivo de almacenamiento determinado. 3 - Determina los hechos asociados a un evento (delito) a través del análisis y presentación de la información recolectada.

5. Contenidos

Id	Unidad de aprendizaje	Temáticas
1	Destrezas de ciberseguridad	Cubo de destrezas de la ciberseguridad, Estado de los datos y contramedidas de seguridad.
2	Ciberataques y consecuencias para los usuarios	Tipos de ataques y medidas de protección.
3	Protección de datos, dispositivos de seguridad informática e integridad de la información	Estándares internaciones de seguridad, encriptación, control de acceso, ocultamiento de datos, hacking y sus fases, dispositivos de seguridad y manejo de incidentes. Hash, firmas digitales, certificados digitales y alta disponibilidad.
4	Informática forense	Historia, conceptos, tipos de análisis y fases del análisis.
5	Marco legal	Ley 1273 de 2009. Ley 1581 de 2012. Ley estatutaria 1266 del 31 de diciembre de 2008. Decreto 1377 de 2013. Ley 527 de 1999. Decreto 333 de 2014. Ley 599 de 2000. Ley 906 de 2004.
6	Evidencia digital y cadena de custodia	Concepto de evidencia digital, características, fuentes de evidencia digital, clasificación, criterios de admisibilidad y cadena de custodia.
7	Etapa I: identificación	Búsqueda de información, preparación de herramientas, tipos de adquisición.
8	Etapa II: preservación	Medios de almacenamiento, imagen forense, algoritmos hash.
9	Etapa III: análisis	Análisis preliminar, sistema de archivos, imágenes parciales, depuración de la información, análisis del sistema operativo.
10	Etapa IV: presentación.	Organización de la información, informe de investigador de laboratorio, presentación ante autoridades o partes interesadas.

6. Evaluación y calificación

Actividades o tipos de actividades	Porcentaje
Examen parcial. Retroalimentación a través de: Ofrecer preguntas, describir el trabajo de los estudiantes y ofrecer sugerencias.	10

Actividades o tipos de actividades	Porcentaje
Talleres y exposiciones. Retroalimentación a través de: Ofrecer preguntas, describir el trabajo de los estudiantes y andamiaje.	50
Estudio de caso. Retroalimentación a través de: Ofrecer preguntas, describir el trabajo de los estudiantes, ofrecer sugerencias y valorar los avances y logros.	20
Examen final. Retroalimentación a través de: Ofrecer preguntas, describir el trabajo de los estudiantes y ofrecer sugerencias.	20

7. Bibliografía

Libro Computación forense. Descubriendo los rastros informáticos. Jeimy J Cano.

Manual de policía judicial y cadena de custodia.

Ley 1273 de 2009

Ley 1581 de 2015

Introducción a la informática forense del autor Francisco Lázaro Domínguez.

Guía metodológica sobre las técnicas y herramientas de software libre aplicadas a la informática forense. recurso electrónico del autor Díaz Jurado, Gerardo.

8. Observaciones

Ninguna