



1. Datos Generales de la asignatura

Nombre de la asignatura:	Cómputo forense
Clave de la asignatura:	CBD-2410
SATCA¹:	2-3-5
Carrera:	Ingeniería en Ciberseguridad.

2. Presentación

Caracterización de la asignatura

Esta asignatura aporta el perfil del ingeniero en ciberseguridad las siguientes habilidades:

- Gestiona incidentes y eventos de seguridad de informática para reducir la afectación negativa de la seguridad de la información y dar continuidad a las operaciones de la organización, atendiendo los principios de no discriminación, Inclusión y equidad social.
- Aplica procedimientos y técnicas de auditoría informática para detectar si se protegen los activos y recursos de la organización, si se mantiene la integridad de los datos, si se utiliza eficientemente los recursos, si se atienden los principios de no discriminación, inclusión y equidad social y si se cumple con las leyes y regulaciones establecidas.

La asignatura es esencial para la formación del ingeniero en ciberseguridad, dotándolo de competencias para identificar, analizar y presentar evidencia digital en casos de incidentes y delitos cibernéticos, fortalece las habilidades técnicas, legales y metodológicas del ingeniero, facilitando la prevención, detección y respuesta a amenazas de seguridad.

Se complementa con asignaturas como "seguridad de sistemas", que se enfoca en proteger infraestructuras informáticas y fortalecer sistemas vulnerables; "redes y protocolos de seguridad", centrada en diseñar redes seguras y detectar intrusiones; y "legislación en ciberseguridad", que aborda el marco legal y ético de la seguridad digital. Estas asignaturas contribuyen a la especialización y profesionalización del ingeniero en ciberseguridad, permitiéndole abordar integralmente los desafíos del ámbito cibernético.

Intención didáctica

Se recomienda adoptar un enfoque práctico y teórico, combinando la exposición de conceptos fundamentales con la aplicación práctica mediante casos de estudio y simulaciones. Es esencial abordar los temas de manera multidisciplinaria, profundizando en técnicas avanzadas y aspectos legales del cómputo forense. Se deben destacar actividades como la resolución de casos prácticos, debates y proyectos para desarrollar competencias genéricas como el pensamiento crítico, la comunicación efectiva y la ética profesional. El docente debe actuar como facilitador del aprendizaje, proporcionando retroalimentación, actualizando contenidos y fomentando un ambiente colaborativo y constructivo en el aula, con el objetivo de ofrecer una formación integral y actualizada en cómputo forense que prepare a los estudiantes para enfrentar los desafíos de la ciberseguridad.

¹ Sistema de Asignación y Transferencia de Créditos Académicos



3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Tecnológico Nacional de México del 4 al 6 de marzo del 2024.	Representantes de los Institutos Tecnológicos de: Aguascalientes, Cerro Azul, Ciudad Juárez, La Paz, Jiquilpan, Mérida, Morelia, Tuxtla Gutiérrez, Villahermosa. Institutos Tecnológicos Superiores de La Región Carbonífera, Las Choapas	Propuesta sintética de la carrera de Ingeniería en Ciberseguridad.
Tecnológico Nacional de México del 22 al 26 de abril del 2024.	Representantes de los Institutos Tecnológicos de: Aguascalientes, Cerro Azul, Ciudad Juárez, La Paz, Jiquilpan, Mérida, Morelia, Tuxtla Gutiérrez, Villahermosa. Institutos Tecnológicos Superiores de La Región Carbonífera, Las Choapas. Representante de Ciencias Básica de los Institutos de: Celaya, Morelia CENIDET y CIIDET.	Diseño y/o desarrollo curricular de la carrera de Ingeniería en Ciberseguridad
Tecnológico Nacional de México del 27 al 31 de mayo del 2024.	Representantes de los Institutos Tecnológicos de: Aguascalientes, Cerro Azul, Jiquilpan, Mérida, Villahermosa. Institutos Tecnológicos Superiores de La Región Carbonífera, Las Choapas	Consolidación curricular de la carrera de Ingeniería en Ciberseguridad.

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
<ul style="list-style-type: none">Analiza y aplica técnicas y herramientas forenses para recolectar, preservar, analizar y presentar evidencia digital de manera ética y conforme a los estándares legales y metodológicos establecidos, para contribuir a la detección, investigación y resolución de incidentes de seguridad y delitos cibernéticos.



5. Competencias previas

- Diseñar y desarrollar soluciones criptográficas para garantizar la confidencialidad, integridad y autenticidad de la información.
- Conoce, selecciona y administra la seguridad de un sistema operativo en plataformas cliente-servidor, para resolver problemáticas reales y aplicar procedimientos de configuración de seguridad en plataformas de software.
- Desarrollar habilidades para identificar y resolver dilemas éticos, evaluar el impacto social de los ataques cibernéticos y aplicar la legislación nacional e internacional en ciberseguridad para garantizar el cumplimiento normativo y la protección de datos.

6. Temario

No.	Temas	Subtemas
1	Fundamentos de cómputo forense.	1.1. Concepto de cómputo forense. 1.2. Cadena de Eliminación cibernética. 1.3. El marco MITRE ATT&CK. 1.4. El modelo de diamante del análisis de intrusiones. 1.5. Marco legal.
2	El proceso forense digital.	2.1. Fases del proceso forense digital. 2.1.1. Identificación y adquisición. 2.1.2. Preservación. 2.1.3. Análisis. 2.1.4. Documentación. 2.1.5. Presentación del informe. 2.2. Manejo de evidencia. 2.2.1. Tipos de evidencia 2.2.2. Orden de recolección de evidencia 2.2.3. Integridad y preservación de los datos 2.2.4. Metodologías del proceso forense 2.2.5. Cadena de custodia
3	Respuesta a incidentes.	3.1. Definición de incidente de seguridad. 3.2. Fases de la respuesta a incidentes. 3.2.1. Identificación del incidente. 3.2.2. Contención y mitigación del incidente. 3.2.3. Erradicación del incidente. 3.2.4. Recuperación y restauración de los sistemas afectados. 3.3. Lecciones aprendidas y prevención de futuros incidentes. 3.4. Herramientas y técnicas para la respuesta a incidentes. 3.5. Ciclo de vida de respuesta a incidentes NIST.



4	Adquisición y duplicación de datos	<p>4.1. Criptografía aplicada a la informática forense.</p> <p>4.2. Adquisición lógica y física.</p> <p>4.3. Adquisición directa e indirecta.</p> <p>4.4. Adquisición por hardware.</p> <p>4.5. Adquisición por software.</p>
5	Análisis forense	<p>5.1. Conceptos.</p> <p>5.1.1. Sistemas de archivos.</p> <p>5.1.2. Slack Space.</p> <p>5.1.3. Recuperación de archivos borrados.</p> <p>5.1.4. Recuperación de particiones eliminadas.</p> <p>5.1.5. File Carving y Data Carving.</p> <p>5.2. Análisis.</p> <p>5.2.1. Análisis de metadatos de archivos.</p> <p>5.2.2. Análisis forense de Windows.</p> <p>5.2.3. Análisis forense de Linux y Mac.</p> <p>5.2.4. Análisis forense de redes.</p> <p>5.2.5. Análisis forense bases de datos.</p> <p>5.2.6. Análisis forense de correo electrónico.</p> <p>5.2.7. Análisis forense de la memoria.</p> <p>5.2.8. Análisis forense de teléfonos móviles.</p> <p>5.2.9. Análisis forense en la nube.</p>

7. Actividades de aprendizaje de los temas

1. Fundamentos de cómputo forense	
Competencias	Actividades de aprendizaje
<p>Específica(s):</p> <p>Aplicará los conceptos fundamentales del cómputo forense, la cadena de eliminación cibernética, el marco MITRE ATT&CK, el modelo de diamante del análisis de intrusiones y el marco legal para identificar, analizar y gestionar evidencia digital en casos de incidentes de seguridad, garantizando la integridad, autenticidad y preservación de la información en el proceso forense</p> <p>Genérica(s):</p> <ul style="list-style-type: none"> Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social. 	<ul style="list-style-type: none"> Conferencias y Presentaciones: El docente puede impartir conferencias y presentaciones sobre los conceptos fundamentales del cómputo forense, la cadena de eliminación cibernética, el marco MITRE ATT&CK, el modelo de diamante del análisis de intrusiones y el marco legal, proporcionando a los estudiantes una visión general de cada tema y su relevancia en el ámbito forense. Estudio de Casos Prácticos: Los estudiantes pueden analizar casos prácticos reales o simulados que involucren escenarios de eliminación cibernética, ataques identificados por el marco MITRE ATT&CK, análisis de intrusiones utilizando el modelo de diamante, y consideraciones legales relacionadas con la recopilación y presentación de evidencia digital.



<ul style="list-style-type: none">• Habilidades de gestión de información (habilidad para buscar y analizar información proveniente de fuentes diversas)• Capacidad de aprender• Solución de problemas <p><i>Transversal(es):</i></p> <ul style="list-style-type: none">• Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social.• Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social.• Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano	<ul style="list-style-type: none">• Análisis de documentos y artículos: se pueden asignar lecturas de documentos y artículos especializados que aborden los conceptos clave del cómputo forense, la cadena de eliminación cibernética, el marco MITRE ATT&CK, el modelo de diamante del análisis de intrusiones y el marco legal, seguidas de discusiones en clase para profundizar en la comprensión de los temas.• Prácticas en laboratorio: los estudiantes pueden realizar prácticas en laboratorio donde apliquen los conocimientos adquiridos para llevar a cabo simulaciones de la cadena de eliminación cibernética, utilizar el marco MITRE ATT&CK para identificar tácticas de ataque, aplicar el modelo de diamante del análisis de intrusiones para investigar incidentes de seguridad, y analizar casos legales relacionados con la evidencia digital.• Debates y foros: se pueden organizar debates y foros donde los estudiantes discutan sobre temas éticos y legales asociados al cómputo forense, el marco MITRE ATT&CK y el modelo de diamante del análisis de intrusiones, fomentando el intercambio de ideas y perspectivas entre los participantes.
2. El proceso forense digital	
Competencias	Actividades de aprendizaje
<p><i>Específica(s):</i></p> <p>Aplicará las fases del proceso forense digital, el manejo adecuado de la evidencia, la preservación de la integridad de los datos, las metodologías del proceso forense y la cadena de custodia para identificar, adquirir, preservar, analizar, documentar y presentar de manera efectiva la evidencia digital en casos de incidentes de seguridad, garantizando la validez y confiabilidad del proceso forense y la integridad de la información recopilada</p>	<ul style="list-style-type: none">• Simulación de escenarios forenses: los estudiantes pueden participar en simulaciones de escenarios forenses donde se les presente un caso de incidente de seguridad y se les guíe a través de las diferentes fases del proceso forense digital, desde la identificación y adquisición de evidencia hasta la presentación del informe final. Esto les permitirá aplicar los conocimientos teóricos en situaciones prácticas y desarrollar habilidades de resolución de problemas.



<p><i>Genérica(s):</i></p> <ul style="list-style-type: none">• Habilidades de gestión de información (habilidad para buscar y analizar información proveniente de fuentes diversas)• Capacidad de aprender• Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano <p><i>Transversal(es):</i></p> <ul style="list-style-type: none">• Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social.• Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social.• Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.	<ul style="list-style-type: none">• Prácticas de laboratorio: se pueden realizar prácticas de laboratorio donde los estudiantes aprendan a utilizar herramientas y técnicas forenses para identificar, adquirir, preservar, analizar y documentar evidencia digital. Esto incluiría la utilización de software forense, técnicas de extracción de datos y métodos de preservación de la integridad de la evidencia.• Estudio de casos reales: los estudiantes pueden analizar casos reales de investigaciones forenses donde se hayan aplicado las diferentes fases del proceso forense digital. Esto les proporcionará una comprensión más profunda de cómo se utilizan los principios forenses en la práctica y les ayudará a desarrollar habilidades de análisis crítico.• Discusiones en grupo: se pueden organizar discusiones en grupo donde los estudiantes debatan sobre temas relacionados con el manejo de evidencia, como los diferentes tipos de evidencia, el orden de recolección de evidencia, la preservación de datos y la cadena de custodia. Esto les ayudará a comprender la importancia de seguir procedimientos adecuados en el proceso forense y a desarrollar habilidades de comunicación y trabajo en equipo.• Presentación de informes forenses: los estudiantes pueden trabajar en la elaboración de informes forenses donde documenten sus hallazgos y conclusiones obtenidas a partir del análisis de evidencia digital. Esto les permitirá practicar la comunicación efectiva de resultados forenses y desarrollar habilidades de redacción técnica.
---	---



3. Respuesta a Incidentes

Competencias	Actividades de aprendizaje
<p><i>Específica(s):</i></p> <p>Aplicará las fases de respuesta a incidentes, el ciclo de vida de respuesta a incidentes NIST, las herramientas y técnicas especializadas para la identificación, contención, mitigación, erradicación, recuperación y restauración de los sistemas afectados, y la implementación de lecciones aprendidas para prevenir futuros incidentes de seguridad, garantizando una respuesta eficaz y oportuna frente a los incidentes cibernéticos y la minimización de impactos en la organización</p> <p><i>Genérica(s):</i></p> <ul style="list-style-type: none">• Habilidades de gestión de información (habilidad para buscar y analizar información proveniente de fuentes diversas)• Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.• Trabajo en equipo• Búsqueda del logro <p><i>Transversal(es):</i></p> <ul style="list-style-type: none">• Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social.• Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social.	<ul style="list-style-type: none">• Simulaciones de incidentes: los estudiantes pueden participar en simulaciones de incidentes de seguridad donde se les presente un escenario de ataque y se les solicite que sigan las fases de respuesta a incidentes, desde la identificación hasta la recuperación. Esto les permitirá aplicar los conocimientos teóricos en situaciones prácticas y desarrollar habilidades de toma de decisiones bajo presión.• Estudio de casos reales: los estudiantes pueden analizar casos reales de incidentes de seguridad donde se haya aplicado el ciclo de vida de respuesta a incidentes del NIST. Esto les proporcionará una comprensión más profunda de cómo se lleva a cabo la respuesta a incidentes en la práctica y les ayudará a identificar lecciones aprendidas y mejores prácticas.• Pruebas de penetración controladas: los estudiantes pueden realizar pruebas de penetración controladas en entornos de laboratorio para identificar vulnerabilidades y evaluar la eficacia de las herramientas y técnicas utilizadas en la respuesta a incidentes. Esto les permitirá familiarizarse con las herramientas y técnicas disponibles y adquirir experiencia práctica en la detección y mitigación de amenazas.• Talleres de herramientas y técnicas: se pueden organizar talleres donde los estudiantes aprendan a utilizar herramientas y técnicas especializadas para la respuesta a incidentes, como sistemas de detección de intrusiones, análisis de malware y herramientas de recuperación de datos. Esto les proporcionará experiencia práctica en el uso de herramientas forenses y les ayudará a desarrollar habilidades técnicas.



<ul style="list-style-type: none"> Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano. 	<ul style="list-style-type: none"> Debates y foros: se pueden organizar debates y foros donde los estudiantes discutan sobre temas relacionados con la respuesta a incidentes, como la importancia de la preparación y la coordinación, la gestión de comunicaciones durante un incidente y la implementación de lecciones aprendidas para prevenir futuros incidentes. Esto les ayudará a desarrollar habilidades de pensamiento crítico y análisis de situaciones complejas.
4. Adquisición y duplicación de datos	
Competencias	Actividades de aprendizaje
<p><i>Específica(s):</i> Aplicará técnicas de criptografía aplicada a la informática forense, realizará adquisiciones lógicas y físicas de datos mediante métodos directos e indirectos, y empleará herramientas y técnicas de adquisición por hardware y software para obtener copias forenses precisas y fiables de los dispositivos y sistemas, garantizando la integridad, autenticidad y preservación de la evidencia digital en el proceso forense</p> <p><i>Genérica(s):</i></p> <ul style="list-style-type: none"> Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social. Solución de problemas Compromiso ético <p><i>Transversal(es):</i></p> <ul style="list-style-type: none"> Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social. Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social. 	<ul style="list-style-type: none"> Talleres prácticos de criptografía: los estudiantes pueden participar en talleres prácticos donde aprendan los principios de la criptografía aplicada a la informática forense. Pueden realizar ejercicios de cifrado y descifrado de datos, así como aprender a identificar y analizar la criptografía utilizada en diferentes dispositivos y sistemas. Simulaciones de adquisición de datos: se pueden organizar simulaciones donde los estudiantes practiquen la adquisición lógica y física de datos utilizando diferentes técnicas y herramientas forenses. Pueden enfrentarse a escenarios simulados de recolección de evidencia digital y aprender a seleccionar la mejor estrategia de adquisición según el caso. Pruebas de hardware forense: los estudiantes pueden participar en pruebas de hardware forense donde aprendan a utilizar dispositivos especializados para la adquisición de datos, como grabadoras de discos, dispositivos de duplicación y dispositivos de lectura de tarjetas de memoria. Pueden practicar la adquisición de datos físicos de dispositivos de almacenamiento y aprender a preservar la integridad de la evidencia digital.

<ul style="list-style-type: none"> • Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano. 	<ul style="list-style-type: none"> • Ejercicios de adquisición por software: los estudiantes pueden realizar ejercicios prácticos de adquisición de datos por software utilizando herramientas forenses especializadas. Pueden aprender a utilizar software de imagenización de discos, herramientas de extracción de datos de dispositivos móviles y aplicaciones de adquisición remota de datos, entre otras. • Estudio de casos reales: los estudiantes pueden analizar casos reales donde se haya aplicado la adquisición y duplicación de datos en investigaciones forenses. Pueden estudiar cómo se seleccionaron y aplicaron las técnicas de adquisición en diferentes escenarios y aprender de las mejores prácticas y lecciones aprendidas.
5. Análisis forense	
Competencias	Actividades de aprendizaje
<p><i>Específica(s):</i> Aplicará los conceptos y técnicas avanzadas de análisis forense, incluyendo el análisis de sistemas de archivos, slack space, recuperación de archivos y particiones eliminadas, file carving y data carving, para realizar un análisis detallado de metadatos de archivos, sistemas operativos como Windows, Linux y Mac, redes, bases de datos, correo electrónico, memoria, teléfonos móviles y entornos en la nube, identificando y documentando evidencias digitales relevantes de manera precisa y eficiente en el proceso forense.</p> <p><i>Genérica(s):</i></p> <ul style="list-style-type: none"> • Capacidad de análisis y síntesis • Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social. • Capacidad de aplicar los conocimientos en la práctica 	<ul style="list-style-type: none"> • Estudio de conceptos fundamentales: los estudiantes pueden realizar lecturas y discusiones en clase sobre los conceptos fundamentales del análisis forense, incluyendo sistemas de archivos, slack space, recuperación de archivos borrados, recuperación de particiones eliminadas, file carving y data carving. Pueden estudiar casos prácticos y ejemplos para comprender cómo se aplican estos conceptos en situaciones reales. • Prácticas de laboratorio: se pueden organizar prácticas de laboratorio donde los estudiantes aprendan a realizar análisis forenses en diferentes plataformas y dispositivos. Pueden practicar el análisis de metadatos de archivos, análisis forense de sistemas operativos como Windows, Linux y Mac, análisis forense de redes, bases de datos, correo electrónico, memoria, teléfonos móviles y entornos en la nube.



Transversal(es):

- Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social.
- Usa comunicación oral y escrita atendiendo los principios de no discriminación, Inclusión y equidad social.
- Diseña e implementa soluciones a problemas propios de ámbito de su área de aplicación integrando aprendizajes, rasgos y capacidades de excelencia, vanguardia e innovación social que fortalezcan el desarrollo humano.

- Simulaciones de casos forenses: los estudiantes pueden participar en simulaciones de casos forenses donde se les presente un escenario de investigación y se les solicite que apliquen las técnicas de análisis forense aprendidas para resolver el caso. Pueden trabajar en equipo para analizar la evidencia digital, identificar posibles sospechosos y presentar sus conclusiones.
- Proyectos de investigación: se pueden asignar proyectos de investigación donde los estudiantes elijan un tema específico dentro del análisis forense y realicen una investigación en profundidad. Pueden investigar nuevas técnicas y herramientas, estudiar casos de estudio relevantes o analizar tendencias y desafíos en el campo del análisis forense.
- Presentaciones y debates: los estudiantes pueden preparar presentaciones sobre temas específicos de análisis forense y participar en debates sobre cuestiones controvertidas o emergentes en el campo. Pueden investigar y presentar diferentes perspectivas sobre temas como la privacidad de datos, la integridad de la evidencia digital y los desafíos éticos del análisis forense en la era digital.

8. Práctica(s)

- Simulación de investigación forense en equipo.
- Desarrollo de un proyecto de investigación forense.

9. Proyecto de asignatura

El objetivo del proyecto que planteé el docente que imparta esta asignatura, es demostrar el desarrollo y alcance del(los) logro(s) formativo(s) de la asignatura, considerando las siguientes fases:

Fundamentación: marco referencial (teórico, conceptual, contextual, legal) en el cual se fundamenta el proyecto de acuerdo con un diagnóstico realizado, mismo que permite a los estudiantes lograr la comprensión de la realidad o situación objeto de estudio para definir un proceso de intervención o hacer el diseño de un modelo.

Planeación: con base en el diagnóstico en esta fase se realiza el diseño del proyecto por parte de los estudiantes con asesoría del docente; implica planificar un proceso: de intervención empresarial, social o comunitario, el diseño de un modelo, entre otros, según el tipo de proyecto, las actividades a realizar los recursos requeridos y el cronograma de trabajo.



Ejecución: consiste en el desarrollo de la planeación del proyecto realizada por parte de los estudiantes con asesoría del docente, es decir en la intervención (social, empresarial), o construcción del modelo propuesto según el tipo de proyecto, es la fase de mayor duración que implica el desempeño de los saberes, habilidades y destrezas a desarrollar.

Evaluación: es la fase final que aplica un juicio de valor en el contexto laboral-profesión, social e investigativo, ésta se debe realizar a través del reconocimiento de logros y aspectos a mejorar se estará promoviendo el concepto de “evaluación para la mejora continua”, el desarrollo del pensamiento crítico y reflexivo en los estudiantes.

10. Evaluación de saberes, habilidades y destrezas

- Análisis de casos.
- Entrevistas a expertos
- Solución de problemas realizados en forma individual o en equipo.
- Discusiones y debates en equipos.
- Paneles de presentaciones de temas.
- Reportes de proyectos, investigaciones, trabajos, etc.
- Simulaciones y/o demostraciones.
- Esquemas gráficos (mapas conceptuales, mapas mentales, mapas
- Procedimentales, cuadros sinópticos, diagramas de flujo, etc.)

11. Fuentes de Información

1. Casey, E. (2011). "Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet." Academic Press.
2. Nelson, B., Phillips, A., & Steuart, C. (2017). "Guide to Computer Forensics and Investigations." Cengage Learning.
3. Carrier, B. (2005). "File system forensic analysis." Addison-Wesley Professional.
4. Jones, A. (2015). "Art of memory forensics: Detecting malware and threats in Windows, Linux, and Mac memory." John Wiley & Sons.
5. Sammons, J. (2014). "The basics of digital forensics: The primer for getting started in digital forensics." Syngress.
6. Pearson, D., & Watson, M. (2018). "Principles of Cybercrime." Cambridge University Press.
7. Casey, E., & Stellatos, G. J. (2017). "Handbook of digital forensics of multimedia data and devices." John Wiley & Sons.
8. Bejtlich, R. (2013). "The Practice of Network Security Monitoring: Understanding Incident Detection and Response." No Starch Press.
9. Ligh, M. H., Adair, S., Hartstein, B., & Richard, M. (2014). "Malware Analyst's Cookbook and DVD: Tools and Techniques for Fighting Malicious Code." John Wiley & Sons.
10. Stevens, D., & Yason, J. (2018). "Placing the Suspect Behind the Keyboard: Using Digital Forensics and Investigative Techniques to Identify Cybercrime Suspects." Syngress.
11. Asociación Nacional de Instituciones de Educación en Tecnologías de Información A.C. (2024). Modelo curricular por competencias. ANIEI