

1. Datos Generales de la asignatura

Nombre de la asignatura:	Cómputo Forense
Clave de la asignatura:	CID2605
SATCA¹:	2 -3 - 5
Carrera:	<ul style="list-style-type: none">• Ingeniería en Sistemas Computacionales• Ingeniería en Tecnologías de la Información y Comunicaciones• Ingeniería en Inteligencia Artificial• Ingeniería en Ciencia de Datos• Ingeniería en Desarrollo de Aplicaciones.• Ingeniería en Informática

2. Presentación

Caracterización de la asignatura

La asignatura **Cómputo Forense** contribuye significativamente al perfil de egreso del ingeniero especializado en ciberseguridad, al dotarlo de las competencias necesarias para identificar, recolectar, preservar, analizar y presentar evidencia digital en el contexto de incidentes de seguridad. Estas habilidades permiten que el egresado pueda intervenir de manera efectiva en la respuesta y gestión de crisis cibernéticas dentro de industrias clave y servicios estratégicos, garantizando la protección de infraestructuras críticas y la mitigación de riesgos tecnológicos.

La importancia de la asignatura radica en su papel como componente esencial dentro del marco de la seguridad digital, puesto que fortalece la capacidad del profesional para prevenir, detectar y responder a incidentes de seguridad. Además, fomenta un enfoque holístico que incluye consideraciones legales, técnicas y metodológicas, todas esenciales para abordar la ciberseguridad en sectores estratégicos. Esta asignatura, al centrarse en el análisis forense digital, permite la aplicación de soluciones preventivas y reactivas que mejoran la resiliencia de las infraestructuras de información ante posibles ciberataques.

El contenido de la asignatura cubre cinco áreas fundamentales: Fundamentos de **Cómputo Forense**, que introduce los conceptos clave y marcos legales asociados; El proceso forense digital, que aborda las fases de adquisición, preservación, análisis y reporte de evidencia digital; Respuesta a Incidentes, que incluye el ciclo de vida de la respuesta, contención y mitigación de eventos de seguridad; Adquisición y duplicación de datos, con énfasis en técnicas avanzadas de recolección y preservación de información digital, y finalmente, Análisis forense, que profundiza en la investigación y

¹ Sistema de Asignación y Transferencia de Créditos Académicos

recuperación de datos en diversos sistemas y plataformas, incluyendo redes, dispositivos móviles y la nube.

La asignatura se relaciona transversalmente con otras áreas de la ciberseguridad, como "Seguridad de Sistemas Operativos" y "Seguridad en Redes Inalámbricas", en los temas de identificación y prevención de amenazas, fortaleciendo las competencias específicas de auditoría de seguridad y mitigación de vulnerabilidades. Además, se vincula con "Aspectos Legales y Éticos en Ciberseguridad" para garantizar el cumplimiento normativo en el manejo de evidencia y el marco jurídico que regula el ciberespacio. Estas relaciones permiten identificar oportunidades para generar proyectos integradores, como la implementación de investigaciones forenses a nivel organizacional, la creación de políticas de respuesta a incidentes o el análisis de casos reales bajo un enfoque interdisciplinario.

La asignatura también fomenta una visión holística que incorpora los criterios orientadores de responsabilidad social, equidad de género, inclusión y excelencia, así como la aplicación de soluciones innovadoras para las industrias clave, alineándose con los principios de innovación social y vanguardia tecnológica. Se promueve la interculturalidad mediante el análisis de normativas y prácticas de ciberseguridad a nivel global, y la asignatura se evalúa bajo un enfoque de mejora continua para mantener su relevancia en un campo que evoluciona constantemente.

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.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Tecnológico Nacional de México, campus Tuxtla Gutiérrez del 18 septiembre al 26 de octubre de 2024	Representantes de los Institutos Tecnológicos de: Tuxtla Gutiérrez, Tapachula y Frontera Comalapa. Jesús Carlos Sánchez Guzmán Ezequiel Cruz Wong Carlos Alberto López Escobar Brenda Guadalupe Pinto Vázquez	Foro Estatal Actualización Curricular para la Consolidación de Proyectos Estratégicos del TecNM en el Estado de Chiapas

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
El estudiante, al finalizar la asignatura "Cómputo Forense", debe ser capaz de identificar, analizar y aplicar técnicas y herramientas forenses para recolectar, preservar, analizar y presentar evidencia digital de manera ética y conforme a los estándares legales y metodológicos establecidos, con el fin de contribuir a la detección, investigación y resolución de incidentes de seguridad y delitos cibernéticos.

5. Competencias previas

<ul style="list-style-type: none"> Identificar Vulnerabilidades y Controles de Seguridad Administrar y Proteger Redes Inalámbricas Aplicar Legislación y Ética en Ciberseguridad Implementar Técnicas de Criptografía

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

7. Actividades de aprendizaje de los temas

1. Fundamentos de Cómputo Forense	
Competencias	Actividades de aprendizaje
<p>Específica(s): asignatura</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>Genéricas:</p> <ul style="list-style-type: none"> - Aplica los conocimientos en la práctica, identificando aquellos que incorporen el compromiso con la responsabilidad social. - Habilidades de gestión de información (habilidad para buscar y analizar información proveniente de fuentes diversas) - Capacidad de aprender - Solución de problemas 	<p>1. 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.</p> <p>2. 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.</p> <p>3. 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.</p> <p>4. 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</p>

	<p>ataque, aplicar el modelo de diamante del análisis de intrusiones para investigar incidentes de seguridad, y analizar casos legales relacionados con la evidencia digital.</p> <p>5. 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.</p>
2. El proceso forense digital	
Competencias	Actividades de aprendizaje
<p>Específica(s):</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> <p>Genéricas:</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 	<p>1. 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> <p>2. 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.</p> <p>3. Estudio de Casos Reales: Los estudiantes pueden analizar casos reales</p>

<p>innovación social que fortalezcan el desarrollo humano.</p>	<p>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.</p> <p>4. 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.</p> <p>5. 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.</p>
<p>3. Respuesta a Incidentes</p>	
<p>Competencias</p>	<p>Actividades de aprendizaje</p>
<p>Específica(s):</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</p>	<p>1. 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</p>

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.

Genéricas:

- 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

desarrollar habilidades de toma de decisiones bajo presión.

2. 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.

3. 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.

4. 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.

5. 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>Específica(s):</p> <p>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>Genéricas:</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>1. 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.</p> <p>2. 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.</p> <p>3. 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.</p> <p>4. 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,</p>

	<p>herramientas de extracción de datos de dispositivos móviles y aplicaciones de adquisición remota de datos, entre otras.</p> <p>5. 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.</p>
5. Análisis forense	
Competencias	Actividades de aprendizaje
<p>Específica(s):</p> <p>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>Genéricas:</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 	<p>1. 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.</p> <p>2. 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.</p> <p>3. Simulaciones de Casos Forenses: Los estudiantes pueden participar en simulaciones de casos forenses donde se les presente un escenario de investigación</p>

	<p>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.</p> <p>4. 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.</p> <p>5. 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.</p>
--	---

8. Práctica(s)

Práctica 1: Simulación de Investigación Forense en Equipo

Objetivo: Aplicar los conocimientos adquiridos durante el curso para llevar a cabo una investigación forense completa en un escenario simulado, trabajando en equipos multidisciplinarios.

Actividades:

1. Formación de Equipos: Los estudiantes se dividen en equipos de trabajo, cada uno con roles específicos como analistas forenses, expertos en redes, coordinadores de respuesta, entre otros.

2. Presentación del Escenario: Se presenta a cada equipo un escenario de incidente de seguridad simulado, como una intrusión de red, robo de datos, o malware.

3. Análisis de la Evidencia: Los equipos llevan a cabo la investigación forense, aplicando técnicas aprendidas durante el curso para identificar, recopilar, preservar, analizar y documentar la evidencia digital relacionada con el incidente.

4. Coordinación de Respuesta: Los equipos coordinan la respuesta al incidente, tomando medidas para contener, mitigar y erradicar la amenaza, siguiendo un plan de respuesta establecido.

5. Presentación de Resultados: Cada equipo prepara un informe detallado de la investigación, que incluye hallazgos, conclusiones, recomendaciones y lecciones aprendidas.

6. Debates y Discusiones: Se lleva a cabo una sesión de debate donde los equipos presentan sus hallazgos y se discuten los diferentes enfoques y decisiones tomadas durante la investigación.

Práctica 2: Desarrollo de un Proyecto de Investigación Forense

Objetivo: Realizar un proyecto de investigación forense independiente sobre un tema relevante en el campo de la informática forense, aplicando metodologías y técnicas aprendidas durante el curso.

Actividades:

1. Selección de Tema: Los estudiantes eligen un tema de investigación forense de su interés, relacionado con tendencias, desafíos o tecnologías emergentes en el campo.

2. Recolección de Datos: Los estudiantes recopilan datos relevantes para su investigación, utilizando fuentes como estudios de casos, informes técnicos, artículos científicos y datos de laboratorio.

3. Análisis y Experimentación: Los estudiantes aplican metodologías de investigación forense para analizar los datos recopilados, realizar experimentos y extraer conclusiones.

4. Elaboración del Informe: Los estudiantes preparan un informe detallado de su investigación, que incluye el contexto del problema, objetivos, metodología, resultados, análisis y conclusiones.

5. Presentación del Proyecto: Cada estudiante presenta su proyecto ante sus compañeros de clase y el profesor, compartiendo los hallazgos y discutiendo las implicaciones de su investigación.

9. Proyecto de asignatura

El objetivo del proyecto que planteé el docente que imparta esta asignatura, es demostrar el desarrollo y alcance de la(s) competencia(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 las competencias genéricas y específicas 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”, la metacognición, el desarrollo del pensamiento crítico y reflexivo en los estudiantes.

10. Evaluación por competencias

Son las técnicas, instrumentos y herramientas sugeridas para constatar los desempeños académicos de las actividades de aprendizaje.

- Análisis de casos.
- Análisis y solución de problemas.
- 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.
- Solución de cuestionarios
- Ensayos y/o trabajos de diverso tipo
- Elaboración de controles de lectura
- Simulaciones y/o demostraciones.
- Resúmenes
- Juegos de roles.
- Esquemas gráficos (mapas conceptuales, mapas mentales, mapas procedimentales, cuadros sinópticos, diagramas de flujo, etc.)
- Fichas de observación para prácticas
- Investigaciones documentales o de campo.

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.