Programa de asignatura
por competencias de educación superior

Sección I. Identificación del Curso

Tabla 1. Identificación de la Planificación del Curso.

Actualización:	Marzo 13, 2024						
Carrera:	Ingeniería en Desarrollo de Software			**Asignatura:**	Informática forense		
Academia:	Desarrollo de software /			**Clave:**	19SDSSI03		
Módulo formativo:	Internet de las cosas			**Seriación:**	- -		
Tipo de curso:	Presencial			**Prerrequisito:**	- -		
Semestre:	Séptimo	**Créditos:**	6.75	**Horas semestre:**	108 horas		
Teoría:	2 horas	**Práctica:**	2 horas	**Trabajo indpt.:**	2 horas	**Total x semana:**	6 horas

Sección II. Objetivos educacionales

Tabla 2. Objetivos educacionales

Objetivos educacionales		Criterios de desempeño	Indicadores
1	Los egresados gestionarán recursos relacionados con el desarrollo de software en alguna organización.	Los egresados podrán aplicar metodologías en el desarrollo de proyectos en el contexto laboral.	20% de los egresados aplicarán metodologías en el desarrollo de software en su contexto laboral.
2	Los egresados diseñarán e implementarán soluciones innovadoras mediante el uso de tecnologías de la información.	Los egresados participarán activamente en el ciclo de desarrollo e integración continuos	25% de los egresados desempeñarán labores de desarrollo e integración continuos.
3	Los egresados desarrollarán conocimiento especializado que les permite enfocarse en un área del conocimiento específico del desarrollo de software.	Los egresados desempeñarán actividades orientadas al aseguramiento de los activos de información de manera resiliente, la gestión de la infraestructura de redes y comunicaciones, o integrando hardware y software para crear soluciones IoT; así como el uso de inteligencia artificial para gestionar datos y reconocer patrones que determinen oportunidades de negocio en las organizaciones.	5% de los egresados desempeñarán labores en desarrollo de soluciones IoT.
4	Los egresados serán capaces de emprender un negocio basado en el desarrollo de un producto o servicio de tecnologías de la información, aportando valor a la generación de empleos e incrementar el bienestar económico y social, de forma ecológica y sustentable.	Los egresados serán capaces de emprender un negocio basado en el desarrollo propio de un producto o servicio de tecnologías de la información.	2% de los egresados tendrán participación en el acta constitutiva de una empresa creada a partir del desarrollo de software para ofrecer un producto o servicio.

Atributos de egreso de plan de estudios		Criterios de desempeño	Componentes
1	Desarrollar una experimentación adecuada para recopilar, almacenar y analizar grandes cantidades de información basándose en el juicio ingenieril para crear productos o servicios innovadores mediados por software.	- Podrán aplicar metodologías en el desarrollo de proyectos en el contexto laboral. - Dirigirán procesos de informática forense en los que tiene personal a su cargo.	1.1 Evolución de la informática forense. 1.2 Delito informático. 1.3 La informática forense. 1.4 Procesos de la informática forense. 1.5 Tipos de Informática forense. 1.6 Principales ámbitos de aplicación. 1.6.1 Cadena de custodia. 1.6.2 Definición de indicio. 1.6.3 Desarrollo de reporte de cadena de custodia.
2	Identificar su responsabilidad ética y profesional con el entorno sociocultural y ambiental para aplicar estándares, así como fundamentos legales y normativos, aportando valor al contexto social y sustentable.	- Analizará los sistemas informáticos corporativos y los programas con el fin de encontrar evidencias en la seguridad de una empresa.	2.1 Preservación y embalaje de los indicios. 2.1.1 Jaulas Faraday. 2.1.2 Sellado físico de puertos. 2.1.3Fotografías desde los 4 puntos cardinales. 2.1.4 Documentación detallada física del indicio. 2.2 Documentación del proceso. 2.3 Extracción de firmas hash de la información. 2.3.1 SHA256. 2.3.2 SHA128. 2.3.3 MD5 (hay que explicar que es débil). 2.3.4 Copias forenses de la información. 2.3.5 Memoria volátil y rígida (RAM y HDD). 2.3.6 Documentación del proceso. 2.4 Transportes y traslados del indicio. 2.5 Quien da y quien recibe. 2.6 Documentación del proceso.

Continuación: Tabla 2. Objetivos educacionales (continuación			
No.	Atributos de egreso de plan de estudios	Criterios de desempeño	Componentes
3	Reconocer la mejora continua como parte de su desarrollo profesional para mantener un perfil actualizado en desarrollo de software para el diseño e implementación de productos y servicios basados en tecnologías con las tendencias emergentes.	- Analizará los sistemas informáticos corporativos y los programas con el fin de aclarar el estado de la seguridad de una empresa. Conocer y seguir el proceso legal de obtención, documentación y entrega de evidencias informáticas forenses.	3.1 Traspaso del indicio. 3.1.1 Laboratorios y fiscalías. 3.1.2 Quien da y quien recibe. 3.1.3 Documentación del proceso. 3.2 Custodia y preservación. 3.2.1 Documentación del proceso. 3.3 Autopsy. 3.3.1 Instalación de autopsy. 3.3.2 Casos de uso y fuentes de datos. 3.3.3 Uso de la UI. 3.3.4 Analizando fuentes de datos. 3.3.5 Hash lookup module. 3.3.6 Tipos de archivos. 3.3.7 Actividad reciente. 3.3.8 Búsqueda de palabras clave. 3.3.9 Repositorio central. 3.3.10 Analizador de Android. 3.3.11 Interfaz de línea de tiempo. 3.3.12 Galería de imágenes.

Sección III. Atributos de la asignatura

Tabla 3. Atributos de la asignatura

<table>
<tr><th colspan="3">Problema a resolver</th></tr>
<tr><td colspan="3">Desarrollar en los estudiantes las habilidades y conocimientos necesarios para comprender, analizar y aplicar los principios, técnicas y herramientas utilizadas en la investigación y análisis de evidencia digital en casos de delitos informáticos, asegurando así la preservación, integridad y autenticidad de la información recolectada durante el proceso forense.</td></tr>
<tr><th colspan="3">Atributos (competencia específica) de la asignatura</th></tr>
<tr><td colspan="3">Aplicar técnicas de recolección, preservación y análisis de evidencia digital, utilizando herramientas y metodologías especializadas, con el fin de identificar, documentar y presentar hallazgos forenses de manera precisa y rigurosa en contextos legales y judiciales.</td></tr>
<tr><th colspan="2">Aportación a la competencia específica</th><th>Aportación a las competencias transversales</th></tr>
<tr><td>Saber</td><td>Saber hacer</td><td>Saber Ser</td></tr>
<tr><td>- Comprender los fundamentos teóricos y legales de la informática forense, incluyendo los conceptos de cadena de custodia, preservación de evidencia digital y procedimientos legales aplicables.</td><td>- Aplicar técnicas y herramientas especializadas de informática forense para la recolección, preservación, análisis y presentación de evidencia digital en investigaciones de delitos informáticos.
- Realizar análisis forenses de sistemas informáticos y dispositivos digitales utilizando metodologías y procedimientos establecidos, garantizando la integridad y autenticidad de los datos recolectados.</td><td>- Desarrollar habilidades de ética y responsabilidad profesional al manejar información confidencial y sensible durante las investigaciones forenses.
- Demostrar integridad, imparcialidad y objetividad en el manejo de la evidencia digital y en la presentación de los hallazgos forenses ante autoridades judiciales y legales.
- Fomentar la colaboración, el trabajo en equipo y la comunicación efectiva con colegas, clientes y autoridades durante el proceso de investigación y análisis forense.</td></tr>
<tr><th colspan="3">Producto integrador de la asignatura, considerando los avances por unidad</th></tr>
<tr><td colspan="3">Proyecto de investigación y análisis forense de un caso de delito informático simulado o real, donde los estudiantes apliquen los conocimientos adquiridos a lo largo del curso. Este proyecto incluirá las siguientes etapas:
Selección del caso: Los estudiantes eligen un caso de delito informático relevante y apropiado para el análisis forense.
Recolección de evidencia: Los estudiantes recopilan y preservan la evidencia digital relacionada con el caso, siguiendo los procedimientos adecuados de cadena de custodia y preservación de la integridad de los datos.
Análisis forense: Utilizando herramientas y técnicas especializadas, los estudiantes realizan un análisis exhaustivo de la evidencia digital para identificar patrones, anomalías y posibles artefactos digitales relevantes para la investigación.</td></tr>
</table>

Continuación: Tabla 3. Atributos de la asignatura
Producto integrador de la asignatura, considerando los avances por unidad
Elaboración de informe: Los estudiantes preparan un informe detallado que documente los hallazgos del análisis forense, incluyendo una descripción del caso, la metodología utilizada, los resultados obtenidos y las conclusiones alcanzadas. Presentación: Los estudiantes presentan sus hallazgos y conclusiones ante un panel de expertos, simulando un entorno profesional donde deben defender y justificar su trabajo de manera clara y convincente. Este proyecto integrador permitiría a los estudiantes aplicar de manera práctica los conceptos y técnicas aprendidas en la asignatura, desarrollando habilidades de investigación, análisis crítico, trabajo en equipo y comunicación efectiva, mientras abordan un problema real o simulado en el campo de la informática forense.

Sección IV. Desglose específico por cada unidad formativa

Tabla 4.1. Desglose específico de la unidad "Informática forense."

Número y nombre de la unidad:	1. Informática forense.					
Tiempo y porcentaje para esta unidad:	Teoría:	10 horas	Práctica:	10 horas	Porcentaje del programa:	27.78%
Aprendizajes esperados:	- Comprender la evolución histórica y los antecedentes de la informática forense, incluyendo su desarrollo y aplicación en el ámbito de la seguridad informática y la investigación criminal. - Identificar los diferentes tipos de delitos informáticos, sus características y las implicaciones legales y sociales asociadas. - Conocer los principios y procesos fundamentales de la informática forense, incluyendo la recolección, preservación y análisis de evidencia digital; familiarizarse con los tipos de informática forense y los principales ámbitos de aplicación, como la seguridad de la información, la respuesta a incidentes y la investigación de fraudes para entender los conceptos de cadena de custodia, indicio y reporte forense, así como la importancia de documentar detalladamente cada paso del proceso forense. - Desarrollar habilidades para aplicar técnicas y procedimientos forenses de manera ética, rigurosa y legalmente válida, garantizando la integridad y autenticidad de la evidencia digital.					

Temas y subtemas (secuencia)	Criterios de desempeño	Estrategias didácticas	Estrategias de evaluación	Producto Integrador de la unidad (Evidencia de aprendizaje de la unidad)
1.1 Evolución de la informática forense. 1.2 Delito informático. 1.3 La informática forense. 1.4 Procesos de la informática forense. 1.5 Tipos de Informática forense. 1.6 Principales ámbitos de aplicación. 1.6.1 Cadena de custodia. 1.6.2 Definición de indicio.	Saber: - Comprender la evolución histórica de la informática forense, desde sus orígenes hasta su estado actual, incluyendo los avances tecnológicos y legales que han influido en su desarrollo.	- Clases Expositivas: Presentación de los conceptos fundamentales sobre la evolución de la informática forense, tipos de delitos informáticos, procesos forenses y principios de la cadena de custodia. - Discusión en Grupo: Sesiones de discusión para explorar casos de estudio y ejemplos prácticos que	Evaluación diagnóstica: - Rescate de conocimientos previos. Evaluación formativa: - Trabajos Prácticos: Evaluación de las habilidades prácticas mediante la revisión de los reportes de cadena de custodia elaborados por los estudiantes, valorando	Elaboración de un informe de investigación sobre un caso de delito informático seleccionado por los estudiantes. Este informe deberá incluir: - Descripción del caso y sus implicaciones. - Análisis de la evidencia digital recolectada.

Continuación: Tabla 4.1. Desglose específico de la unidad "Informática forense."				
Temas y subtemas (secuencia)	Criterios de desempeño	Estrategias didácticas	Estrategias de evaluación	Producto Integrador de la unidad
1.6.3 Desarrollo de reporte de cadena de custodia.	- Conocer los diferentes tipos de delitos informáticos, sus características y las implicaciones legales y sociales asociadas. Saber hacer: - Aplicar los procesos y metodologías de la informática forense para la recolección, preservación y análisis de evidencia digital en casos de delitos informáticos. - Desarrollar reportes de cadena de custodia de manera precisa y detallada, siguiendo estándares y protocolos establecidos en elámbito forense. Ser: - Demostrar un compromiso ético y profesional en el manejo de la evidencia digital, respetando la confidencialidad y la	ilustren los temas abordados, fomentando la participación activa de losestudiantes y el intercambio de ideas y perspectivas. - Actividades Prácticas: Realización de ejercicios prácticos donde los estudiantes apliquen los conceptos aprendidos, como la elaboración de reportes de cadena de custodia y la identificación de indicadores de delitos informáticos.	la precisión y el cumplimiento de los estándares forenses. - Participación en Clase: Evaluación de la participación y el compromiso de los estudiantes en las discusiones grupales y actividades prácticas, valorando su capacidad para analizar y aplicar los conceptos discutidos en clase. Evaluación sumativa: - Pruebas Escritas: Evaluación del conocimiento teórico mediante pruebas escritas que abarquen los conceptos fundamentales de la unidad, como la evolución de la informática forense y los tipos de delitos informáticos.	- Desarrollo de la cadena de custodia y reporte correspondiente. - Conclusiones y recomendaciones basadas en los hallazgos.

Continuación: Tabla 4.1. Desglose específico de la unidad "Informática forense."				
Temas y subtemas (secuencia)	Criterios de desempeño	Estrategias didácticas	Estrategias de evaluación	Producto Integrador de la unidad
	integridad de la información recolectada. - Cultivar una actitud de responsabilidad y rigor en el trabajo forense, reconociendo la importancia de la imparcialidad y la objetividad en la investigación de delitos informáticos.			

Bibliografía

- Vacca, J. R. (2012). Computer Forensics: Investigating File and Operating Systems, Wireless Networks, and Storage. Elsevier.
- Nelson, B., Phillips, A., & Steuart, C. (2016). Guide to Computer Forensics and Investigations. Cengage Learning.
- Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2017). Digital Forensics and Cyber Crime: An Introduction. Routledge.
- Carrier, B. (2005). File System Forensic Analysis. Addison-Wesley Professional.
- Sammons, J. (2014). The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Syngress.

Sección IV. Desglose específico por cada unidad formativa

Tabla 4.2. Desglose específico de la unidad "Recolección de información."

Número y nombre de la unidad:	2. Recolección de información.					
Tiempo y porcentaje para esta unidad:	Teoría:	12 horas	Práctica:	12 horas	Porcentaje del programa:	33.33%
Aprendizajes esperados:	- Comprender los conceptos y principios fundamentales de la preservación y embalaje de indicios digitales en el contexto de la investigación de delitos informáticos. - Conocer las técnicas y procedimientos para la preservación adecuada de la evidencia digital, incluyendo el uso de jaulas Faraday, el sellado físico de puertos y la toma de fotografías desde los 4 puntos cardinales. - Documentar detalladamente el proceso de preservación y embalaje de indicios digitales, incluyendo la identificación de los elementos clave y la redacción de informes técnicos. - Familiarizarse con los conceptos de extracción de firmas hash de la información y su importancia en la verificación de la integridad de los datos. Identificar y aplicar diferentes algoritmos de hash, como SHA256, SHA128 y MD5, y comprender las limitaciones y debilidades de cada uno. - Desarrollar habilidades para realizar copias forenses de la información de manera segura y precisa, tanto de memoria volátil (RAM) como de almacenamiento rígido (HDD).					

Temas y subtemas (secuencia)	Criterios de desempeño	Estrategias didácticas	Estrategias de evaluación	Producto Integrador de la unidad (Evidencia de aprendizaje de la unidad)
2.1 Preservación y embalaje de los indicios 2.1.1 Jaulas Faraday 2.1.2 Sellado físico de puertos 2.1.3Fotografías desde los 4 puntos cardinales 2.1.4 Documentación detallada física del indicio 2.2 Documentación del proceso	Saber: - Comprender los procedimientos y técnicas de preservación y embalaje de indiciosdigitales, así como los protocolos de documentación forense asociados. - Identificar y explicar los diferentes algoritmos de hash utilizados en la	- Clases teóricas para introducir los conceptos de preservación, documentación y extracción de firmas hash. - Demostraciones prácticas y ejercicios de laboratorio para que los estudiantes apliquen las técnicas aprendidas. - Estudio de casos y análisis de situaciones	Evaluación formativa: - Evaluación de informes y registros de laboratorio para verificar la correcta aplicación de las técnicas prácticas. - Participación en discusiones y actividades grupales para evaluar la comprensión y	Elaboración de un protocolo de preservación y embalaje de indicios digitales para uncaso de delito informático simulado. Este protocolo incluirá: - Instrucciones detalladas sobre la preservación de indicios utilizando jaulas

Continuación: Tabla 4.2. Desglose específico de la unidad "Recolección de información."				
Temas y subtemas (secuencia)	Criterios de desempeño	Estrategias didácticas	Estrategias de evaluación	Producto Integrador de la unidad
2.3 Extracción de firmas hash de la información 2.3.1 SHA256 2.3.2 SHA128 2.3.3 MD5 (hay que explicar que es débil) 2.3.4 Copias forenses de la información 2.3.5 Memoria volátil y rígida (RAM y HDD) 2.3.6 Documentación del proceso 2.4 Transportes y traslados del indicio 2.5 Quien da y quien recibe 2.6 Documentación del proceso	extracción de firmas digitales y su importancia en la integridad de la información. Saber hacer: - Aplicar correctamente las técnicas depreservación y embalaje de indicios digitales, incluyendo el uso de jaulas Faraday,sellado físico de puertos y toma de fotografías desde los 4 puntos cardinales. - Realizar extracciones de firmas hash utilizando algoritmos como SHA256, SHA128 y MD5, y generar copias forenses de lainformación para preservar la evidencia digital de manera adecuada. Ser: - Desarrollar una actitud meticulosa y rigurosa en la documentación del proceso	reales para comprender la importancia de la documentación del proceso y los transportes del indicio.	aplicación de los procedimientos de documentación y transporte del indicio. Evaluación sumativa: - Pruebas escritas para evaluar el conocimiento teórico sobre los conceptos y técnicas de preservación, documentación y extracción de firmas hash.	Faraday, sellado físico de puertos y toma de fotografías desde los 4 puntos cardinales. - Procedimientos para la extracción de firmas hash utilizando algoritmos como SHA256, SHA128 y MD5, con explicaciones sobre su debilidad. - Guías para la documentación detallada del proceso y los transportes del indicio, identificando claramente quién da y quiénrecibe la evidencia en cada etapa.

Continuación: Tabla 4.2. Desglose específico de la unidad "Recolección de información."				
Temas y subtemas (secuencia)	Criterios de desempeño	Estrategias didácticas	Estrategias de evaluación	Producto Integrador de la unidad
	forense, demostrando responsabilidad y compromiso ético en el manejo de la evidencia digital. - Cultivar habilidades de comunicación efectiva y trabajo en equipo al coordinar los transportes y traslados del indicio, asegurando una cadena de custodia sólida y transparente.			

Bibliografía

- Vacca, J. R. (2012). Computer Forensics: Investigating File and Operating Systems, Wireless Networks, and Storage. Elsevier.
- Nelson, B., Phillips, A., & Steuart, C. (2016). Guide to Computer Forensics and Investigations. Cengage Learning.
- Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2017). Digital Forensics and Cyber Crime: An Introduction. Routledge.
- Carrier, B. (2005). File System Forensic Analysis. Addison-Wesley Professional.
- Sammons, J. (2014). The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Syngress.

Sección IV. Desglose específico por cada unidad formativa

Tabla 4.3. Desglose específico de la unidad "Traspaso del indicio."

Número y nombre de la unidad:	3. Traspaso del indicio.					
Tiempo y porcentaje para esta unidad:	Teoría:	14 horas	Práctica:	14 horas	Porcentaje del programa:	38.89%
Aprendizajes esperados:	- Comprender los procesos y protocolos involucrados en el traspaso del indicio entre laboratorios y fiscalías en el contexto de la investigación de delitos informáticos. - Familiarizarse con los procedimientos de custodia y preservación de la evidencia digital, incluyendo la documentación detallada del proceso y la aplicación de medidas de seguridad. - Adquirir habilidades para la instalación, configuración y uso de herramientas forenses como Autopsy para el análisis de fuentes de datos digitales. - Identificar los diferentes casos de uso de Autopsy y sus funcionalidades para el análisis forense de archivos, dispositivos y sistemas operativos. - Aplicar técnicas de análisis forense utilizando Autopsy, incluyendo la búsqueda de palabras clave, la identificación de actividades recientes y el análisis de dispositivos Android. - Desarrollar habilidades de documentación y reporte de los procesos de traspaso del indicio, custodia de evidencia y análisis forense utilizando Autopsy.					

Temas y subtemas (secuencia)	Criterios de desempeño	Estrategias didácticas	Estrategias de evaluación	Producto Integrador de la unidad (Evidencia de aprendizaje de la unidad)
3.1 Traspaso del indicio. 3.1.1 Laboratorios y fiscalías. 3.1.2 Quien da y quien recibe. 3.1.3 Documentación del proceso. 3.2 Custodia y preservación. 3.2.1 Documentación del proceso. 3.3 Autopsy. 3.3.1 Instalación de autopsy. 3.3.2 Casos de uso y fuentes de datos.	Saber: - Comprender los procedimientos y protocolos involucrados en el traspaso del indicio entre laboratorios y fiscalías, así como en la custodia y preservación de la evidencia digital.	- Clases Teóricas y Demostraciones Prácticas: Presentación de los conceptos teóricos sobre el traspaso del indicio, la custodia y preservación de la evidencia digital, así como la instalación y uso de Autopsy.	Evaluación formativa: - Trabajos Prácticos: Evaluación de la capacidad de los estudiantes para aplicar los protocolos de traspaso del indicio, la custodia de la evidencia y el análisis forense	Elaboración de un informe detallado sobre un caso de delito informático, que incluya: - Descripción del traspaso del indicio entre laboratorios y fiscalías, con la documentación del proceso.

Continuación: Tabla 4.3. Desglose específico de la unidad "Traspaso del indicio."				
Temas y subtemas (secuencia)	Criterios de desempeño	Estrategias didácticas	Estrategias de evaluación	Producto Integrador de la unidad
3.3.3 Uso de la UI. 3.3.4 Analizando fuentes de datos. 3.3.5 Hash lookup module. 3.3.6 Tipos de archivos. 3.3.7 Actividad reciente. 3.3.8 Búsqueda de palabras clave. 3.3.9 Repositorio central. 3.3.10 Analizador de Android. 3.3.11 Interfaz de línea de tiempo. 3.3.12 Galería de imágenes.	- Familiarizarse con las funcionalidades y herramientas disponibles en Autopsy para el análisis forense de fuentes de datos digitales. Saber hacer: - Aplicar los protocolos establecidos para el traspaso del indicio, asegurando una transferencia segura y documentada entre los diferentes actores involucrados en el proceso. - Implementar medidas de custodia y preservación adecuadas para garantizar la integridad y autenticidad de la evidencia digital durante su almacenamiento y manipulación. - Utilizar efectivamente Autopsy para realizar análisis forenses de diferentes tipos de archivos, investigar actividades recientes, buscar palabras clave y analizar dispositivos Android.	Demostraciones prácticas de los procedimientos y herramientas. - Estudio de Casos: Análisis de casos reales y simulados para comprender los desafíos yconsideraciones éticas involucradas en el traspaso del indicio, la custodia de la evidencia y el análisis forense. - Laboratorios Prácticos: Ejercicios prácticos donde los estudiantes participarán en la instalación de Autopsy, la exploración desus características y la realización de análisisforenses utilizando la interfaz.	utilizando Autopsy en escenarios prácticos. - Participación y Discusión: Evaluación de la participación activa de los estudiantes endiscusiones grupales y actividades prácticas relacionadas con el traspaso del indicio, la custodia y el análisis forense. Evaluación sumativa: - Pruebas Escritas: Evaluación del conocimiento teórico sobre los procedimientos de traspaso del indicio, custodia y preservación de evidencia digital, así como el uso de Autopsy.	- Procedimientos y medidas de custodia y preservación implementadas para garantizar la integridad de la evidencia digital. - Análisis forense realizado utilizando Autopsy, incluyendo casos de uso, fuentes de datos analizadas, resultados obtenidos y conclusiones.

Continuación: Tabla 4.3. Desglose específico de la unidad "Traspaso del indicio."				
Temas y subtemas (secuencia)	Criterios de desempeño	Estrategias didácticas	Estrategias de evaluación	Producto Integrador de la unidad
	Ser: - Desarrollar una actitud de responsabilidad y profesionalismo en el manejo del traspaso del indicio y la custodia de la evidenciadigital, asegurando la confiabilidad y transparencia del proceso. - Fomentar habilidades de colaboración y comunicación efectiva con colegas y autoridades durante el traspaso del indicio y la colaboración en investigaciones forenses.			

Bibliografía

- Vacca, J. R. (2012). Computer Forensics: Investigating File and Operating Systems, Wireless Networks, and Storage. Elsevier.
- Nelson, B., Phillips, A., & Steuart, C. (2016). Guide to Computer Forensics and Investigations. Cengage Learning.
- Holt, T. J., Bossler, A. M., & Seigfried-Spellar, K. C. (2017). Digital Forensics and Cyber Crime: An Introduction. Routledge.
- Carrier, B. (2005). File System Forensic Analysis. Addison-Wesley Professional.
- Sammons, J. (2014). The Basics of Digital Forensics: The Primer for Getting Started in Digital Forensics. Syngress.

V. Perfil docente

Tabla 5. Descripción del perfil docente

Perfil deseable docente para impartir la asignatura
Carrera(s): - Ingeniería en Computación. - Licenciatura en Informática. - Licenciatura en Sistemas de Información o carreras afines. o carrera afín - Amplia práctica en análisis digital, pericia forense, y enseñanza. Conocimientos actualizados en tecnología y legislación. - Experiencia mínima de dos años - Ingeniero en Computación, Licenciado en Informática, Licenciado en Sistemas de Información o carreras afines.