PROGRAMA EDUCATIVO:

LICENCIATURA EN INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN E INNOVACIÓN DIGITAL

EN COMPETENCIAS PROFESIONALES

PROGRAMA DE ASIGNATURA: INFORMÁTICA FORENSE

CLAVE: E-IFOR-3

Propósito de aprendizaje de la Asignatura	El estudiante analizará la infraestructura de tecnologías de la información ante eventos de seguridad ocurridos e implementará las acciones previstas para minimizar el impacto en la continuidad del negocio y evitar dichos eventos de seguridad en el futuro.
Competencia a la que contribuye la asignatura	Desarrollar soluciones innovadoras de integración de tecnologías de la información mediante metodologías y herramientas de seguridad informática, internet de las cosas, sistemas inteligentes y administración de proyectos; con base en las normas y estándares aplicables para atender las áreas de oportunidad, resolver las necesidades y optimizar los procesos y recursos de diversos sectores.

Tipo de competencia	Cuatrimestre	Créditos	Modalidad	Horas por semana	Horas Totales
Específica	**8**	**4.69**	**Escolarizada**	**5**	**75**

Unidades de Aprendizaje	Horas del Saber	Horas del Saber Hacer	Horas Totales
I. Fundamentos y procesos de cómputo forense.	8	12	20
II. Técnicas y herramientas para el análisis forense.	8	12	20
III. Casos de uso.	14	21	35
Totales	**30**	**45**	**75**

Funciones	Capacidades	Criterios de Desempeño
Implementar un plan maestro de seguridad de sistemas, datos e infraestructura mediante la evaluación de vulnerabilidad, pruebas de penetración y fortalecimiento de la seguridad para garantizar su protección.	Planificar un documento maestro de seguridad de sistemas, datos e infraestructura mediante la identificación y organización de requisitos de seguridad y la aplicación de defensa profunda.	Elaborar un plan maestro de seguridad de sistemas, datos e infraestructura que contenga lo siguiente: - Diagnóstico que identifique los requisitos de seguridad. - Análisis de riesgos. - Tabla de integración de estrategias, iniciativas y proyectos orientados a la mejora de la seguridad, con descripción detallada, justificación y presupuesto de recursos materiales y humanos para cada una de las siete capas: 1) Políticas y procedimientos recomendados. 2) Seguridad física. 3) Perímetro 4) Red interna 5) Host 6) Aplicación 7) Datos - Resultados de la valoración inicial de la organización - Análisis detallado de capacidades requeridas por el personal - Cronograma de implementación. - Conclusiones

	Implementar un plan maestro de seguridad de sistemas, datos e infraestructura mediante la creación la creación de políticas, seguridad física, perímetro de la red, procedimientos y controles para proteger la información.	Elaborar un informe técnico que documente la implementación del plan maestro de seguridad, que contenga lo siguiente: - Introducción - Justificación - Diagnóstico (detección de necesidades y análisis del contexto). - Contexto y análisis de riesgos. - Estructura organizacional de seguridad (roles, responsabilidades, etc.) - Controles de seguridad. - Listado y descripción de las políticas, procedimientos y controles - Bitácora y registro de la implementación de políticas, procedimientos y controles. - Costos de la inversión. - Conclusiones.
	Evaluar un plan maestro de seguridad de sistemas, datos e infraestructura mediante la determinación de la eficacia del sistema de gestión de seguridad, identificando áreas de oportunidad para aplicar mejoras a los procesos y controles del plan maestro de seguridad para proteger la información ante nuevas vulnerabilidades.	Informe técnico de la evaluación de la ejecución de un plan maestro de seguridad, que contenga lo siguiente: - Estrategias de monitoreo - Gestión de incidentes y respuesta a incidentes. - Evaluación de la efectividad y madurez de las estrategias implementadas por la organización en términos de seguridad. - Resultados de las pruebas tecnológicas simuladas aplicadas a las estrategias de seguridad de la organización en un ambiente controlado (pruebas de penetración y análisis de vulnerabilidades) - Cumplimiento y auditoría - Identificación de áreas de oportunidad - Plan de mejora continua - Conclusiones

UNIDADES DE APRENDIZAJE

Unidad de Aprendizaje	I. Fundamentos y procesos de cómputo forense.					
Propósito esperado	El estudiante identificará los fundamentos y procesos en el área de informática forense para responder a incidentes de seguridad mediante las fases del cómputo forense y presentar un peritaje informático.					
Tiempo Asignado	**Horas del Saber**	8	**Horas del Saber Hacer**	12	**Horas Totales**	20

Temas	Saber Dimensión Conceptual	Saber Hacer Dimensión Actuacional	Ser y Convivir Dimensión Socioafectiva
Procedimientos y fuentes de evidencia en el cómputo forense.	Explicar el concepto de cómputo forense. Identificar los tipos de cibercrímenes y los procedimientos de respuesta. Explicar el concepto de investigación y evidencia digitales.	Construir imágenes de un disco duro para investigación forense y recuperar los datos. Desarrollar peritajes informáticos	Desarrollar el pensamiento analítico a través de la identificación de conceptos para resolver problemas en su formación académica o su entorno. Asumir la Responsabilidad en la actuación al reconocer el valor de la información involucrada en los procesos de negocio del cliente. Desarrollar la Comunicación oral y escrita con el fin de que el cliente a través del Plan de Seguridad logre recibir la información adecuada para integrarlo a sus procesos diarios.
Roles y responsabilidades, código de ética.	Describir los roles y responsabilidades de un investigador forense.		
Normas y estándares sobre informática forense, legislación.	Identificar los estándares, mejores prácticas y código de ética relacionados con un investigador forense. Identificar las leyes y normas relacionadas con el cómputo forense.		
Fases involucradas en el cómputo forense.	Describir el proceso de investigación en cómputo forense, incluyendo: Primera respuesta, Fase de pre-investigación, Fase de investigación, y Fase de post-investigación.		
Peritaje informático.	Describir el proceso para publicar un peritaje informático.		

Proceso Enseñanza-Aprendizaje			
Métodos y técnicas de enseñanza	Medios y materiales didácticos	Espacio Formativo	
		Aula	
Análisis de caso de estudio.	Proyector Internet Plataforma LMS Pizarrón Aula Laboratorio con equipo de red, computadoras, software de monitoreo y seguridad Bibliografía Software de simulación	**Laboratorio / Taller**	X

Proceso de Evaluación		
Resultado de Aprendizaje	Evidencia de Aprendizaje	Instrumentos de evaluación
Los estudiantes comprenden la función del Informático Forense y verifican que las fases de respuesta en el proceso de investigación se encuentren contenidas en el peritaje informático.	A partir de un caso de estudio describir la función del Informático Forense, identificar cuáles son las fases de respuesta en el proceso de investigación y el cumplimiento de estas en el peritaje informático.	Estudio de caso Lista de cotejo

Unidad de Aprendizaje	II. Técnicas y herramientas para el análisis forense.					
Propósito esperado	El estudiante implementará las técnicas y herramientas para el análisis forense para recuperar datos y contrarrestar estrategias anti-forenses.					
Tiempo Asignado	**Horas del Saber**	8	**Horas del Saber Hacer**	12	**Horas Totales**	20

Temas	Saber Dimensión Conceptual	Saber Hacer Dimensión Actuacional	Ser y Convivir Dimensión Socioafectiva
Funcionamiento y recuperación de unidades de almacenamiento y archivos de sistema.	Describir los tipos de discos duros, sus características y estructura lógica. Describir el proceso de arranque y el sistema de archivos de los sistemas operativos Windows, Linux y macOS. Analizar el sistema de archivos. Identificar los sistemas de almacenamiento, estándares de codificación y formatos de archivos.	Recuperar archivos borrados a partir de evidencia digital de sistemas Windows y Linux.	Desarrollar el pensamiento analítico a través de la identificación de conceptos para resolver problemas en su formación académica o su entorno. Asumir la Responsabilidad en la actuación al reconocer el valor de la información involucrada en los procesos de negocio del cliente. Desarrollar la Comunicación oral y escrita con el fin de que el cliente a través del Plan de Seguridad logre recibir la información adecuada para integrarlo a sus procesos diarios.
Adquisición de datos y duplicación de la información.	Describir la metodología para la adquisición de datos y evidencia digital. Describir el proceso de preparación de una imagen de la información para su análisis.	Crear imágenes forenses para su análisis y convertirlas a diversos formatos de soporte para la adquisición de evidencia digital.	
Técnicas para contrarrestar estrategias anti-forenses.	Describir técnicas anti-forenses. Describir técnicas para recuperar información de particiones borradas. Describir técnicas para romper contraseñas. Identificar información oculta mediante estenografía, datos ocultos en la estructura del sistema, ofuscación, extensión de archivos.	Implementar técnicas para recuperar particiones, detectar información oculta, desempaquetar información y romper contraseñas para recuperar información protegida con contraseñas.	

Temas	Saber Dimensión Conceptual	Saber Hacer Dimensión Actuacional	Ser y Convivir Dimensión Socioafectiva
	Describir técnicas de empaquetado y minimización de huella.		

Proceso Enseñanza-Aprendizaje			
Métodos y técnicas de enseñanza	Medios y materiales didácticos	Espacio Formativo	
		Aula	
Análisis de caso de estudio Simulación	Proyector Internet Plataforma LMS Pizarrón Aula Laboratorio con equipo de red, computadoras, software de monitoreo y seguridad Bibliografía Software de simulación	**Laboratorio / Taller**	X

Proceso de Evaluación		
Resultado de Aprendizaje	Evidencia de Aprendizaje	Instrumentos de evaluación
Los estudiantes comprenden el funcionamiento del almacenamiento y recuperación de datos en situaciones de incidentes relacionados con la informática forense.	A partir de un caso de estudio: identificar evidencia digital, crear una imagen de la evidencia digital, recuperar archivos borrados, crear una imagen forense, extraer evidencia digital, recuperar particiones, detectar información oculta en la estructura del disco, desempaquetar información, y recuperar información protegida por contraseña.	Estudio de caso Rúbrica

Unidad de Aprendizaje	III. Casos de uso.					
Propósito esperado	El estudiante implementará análisis forense en diferentes plataformas incluyendo Windows, Mac, Linux, redes, la WEB, cómputo en la nube e IoT para minimizar el impacto de los incidentes de seguridad y la continuidad del negocio.					
Tiempo Asignado	**Horas del Saber**	14	**Horas del Saber Hacer**	21	**Horas Totales**	35

Temas	Saber Dimensión Conceptual	Saber Hacer Dimensión Actuacional	Ser y Convivir Dimensión Socioafectiva
Análisis forense en Windows, Mac y Linux.	Describir el proceso de recolección de información volátil y no-volátil en Windows, Mac y Linux. Describir el proceso de análisis de registros y memoria en Windows, Mac y Linux. Describir el proceso de análisis forense en navegadores WEB, archivos y metadatos.	Implementar técnicas de análisis forense a la memoria, registros y navegadores web en Windows, Linux y Mac.	Desarrollar el pensamiento analítico a través de la identificación de conceptos para resolver problemas en su formación académica o su entorno. Asumir la Responsabilidad en la actuación al reconocer el valor de la información involucrada en los procesos de negocio del cliente. Desarrollar la Comunicación oral y escrita con el fin de que el cliente a través del Plan de Seguridad logre recibir la información adecuada para integrarlo a sus procesos diarios.
Análisis forense para redes y ataques WEB.	Explicar el proceso de análisis forense para redes, en particular el análisis postmortem, análisis en tiempo real y los tipos de evidencia. Describir los eventos de correlación. Describir los indicadores de compromiso IoCs Identificar incidentes a partir del tráfico de la red alámbrica e inalámbrica.	Implementar técnicas análisis forense al tráfico de red y determinar ataques en la red.	
Análisis forense en mail y redes sociales.	Describir el proceso de envío y recepción de correos. Explicar el proceso de investigación de crímenes que utilizan correo electrónico.	Implementar técnicas de análisis forense para extraer evidencia de correos sospechosos.	

Temas	Saber Dimensión Conceptual	Saber Hacer Dimensión Actuacional	Ser y Convivir Dimensión Socioafectiva
	Explicar el análisis forense en medios electrónicos sociales.		
Análisis forense para cómputo en la nube.	Describir el análisis forense para sistemas en la nube. Explicar el análisis forense para AWS, Azure y Google Cloud.	Implementar técnicas de análisis forense a sistemas en la nube.	
Análisis forense en IoT.	Explicar el análisis forense para IoT.	Implementar técnicas de análisis forense a sistemas IoT.	

Proceso Enseñanza-Aprendizaje			
Métodos y técnicas de enseñanza	Medios y materiales didácticos	Espacio Formativo	
		Aula	
Análisis de caso de estudio Simulación	Proyector Internet Plataforma LMS Pizarrón Aula Laboratorio con equipo de red, computadoras, software de monitoreo y seguridad Bibliografía Software de simulación	**Laboratorio / Taller**	X

Proceso de Evaluación		
Resultado de Aprendizaje	Evidencia de Aprendizaje	Instrumentos de evaluación
Los estudiantes comprenden la implementación de herramientas para identificar incidentes en sistemas operativos, la red, el correo, las redes sociales y el internet de las cosas.	A partir de un caso de estudio implementar técnicas de análisis forense a memoria, registros y navegadores web, tráfico de la red, y correo electrónico.	Estudio de caso Rúbrica

Perfil idóneo del docente		
Formación académica	**Formación Pedagógica**	**Experiencia Profesional**
Ing. en Sistemas Computacionales Lic. en Informática Ing. en Tecnologías de la Información Ing. en Redes y Telecomunicaciones Deseable con maestría afín y con certificación Cyberops o afín.	Manejo de herramientas didácticas y de evaluación Experiencia en técnicas de manejo de grupos Conocimiento de educación basada en competencias	Experiencia laboral deseable en administración de Centro de Operaciones de Seguridad. Certificación en CCNA, CHFI. Formación continua en tecnologías de redes y telecomunicaciones especialidad seguridad.

Referencias bibliográficas					
Autor	Año	Título del documento	Lugar de publicación	Editorial	ISBN
Charles L. Brooks.	2015	All in one. CHFI. Computer Hacking Forensic Investigator Certification. Exam Guide.	USA	McGraw-Hill Education.	979-8374503111
David Ben Wilington.	2023	Computer Hacking Forensic Investigator (CHFI) – for Beginners: Learn how to identify, track, and prosecute computer criminals.	USA	N/A	N/A
Joakim Kävrestad, Marcus Birath, Nathan Clarke.	2023	Fundamentals of Digital Forensics.	USA	Springer.	978-3-031-53648-9

Referencias digitales			
Autor	Fecha de recuperación	Título del documento	Vínculo
EC-Council.	Junio, 2024	C|HFI Hacking Forensics Investigator.	https://www.eccouncil.org/train-certify/computer-hacking-forensic-investigator-chfi/#download-brochure
Cybrary.	Junio, 2024	Become an Incident Handler.	https://app.cybrary.it/browse/career-path/incident-handler