Universidad Guadalajara

Centro Universitario del Sur

Programa de Estudio

1. IDENTIFICACIÓN DE LA UNIDAD DE APRENDIZAJE

División

División de Ciencias Exactas, Naturales y Tecnológicas.

Departamento

Ciencias Computacionales e Innovación Tecnológica.

Academia

Academia de Redes y Comunicaciones.

Programa(s) educativo(s)

Ingeniería en Telemática

Denominación de la unidad de aprendizaje:

Informática Forense

Clave de la materia:	Horas de teoría:	Horas de práctica:	Carga horaria global:	Valor en créditos:
IG211	27	53	80	8

Tipo de curso:		Nivel en que se ubica:	Prerrequisitos:
C = curso		Técnico Medio Técnico Superior Universitario **Licenciatura** Especialidad Maestría Doctorado	
CL = curso laboratorio			
L = laboratorio			
P = práctica			
T = taller			
CT = curso - taller			
N = clínica			
M = módulo			
S = seminario			

Área de formación:

Optativa Abierta

Perfil docente:

- Licenciatura en Informática, sistemas computacionales o afines.
- Maestría o Doctorado en áreas de computación, redes o afines.
- Experiencia en herramientas de seguridad informática.

Elaborado por:	Actualizado por:
Mtro. Jesús Enrique Ponce Corona	Mtro. Jesús Enrique Ponce Corona

Fecha de elaboración:	Fecha de última actualización:	Fecha de última evaluación:	Fecha de aprobación por Colegio Departamental:
01/ 08 /2021	10/08/2021	10/08/2021	

1. PRESENTACIÓN DE LA UNIDAD DE APRENDIZAJE

El propósito de esta unidad de aprendizaje es evaluar desde un dispositivos o hasta un sistemas de redes completos para la confiscación, aseguramiento, análisis, extracción y presentación de evidencias como parte de elementos que puedan ser presentados ante un juez o tribunal para fines legales o penales. Siguiendo también los lineamientos legales que competen al profesional para llevar a cabo sus actividades. Este propósito se relaciona con el perfil de egreso del Ingeniero en Telemática el cual menciona que “Implementa y administra redes para garantizar las telecomunicaciones con seguridad”.

2. OBJETIVO GENERAL/COMPETENCIA

Desarrollar habilidades y conocimientos basados en métodos calificados y aprobados por instancias y organismos autorizados para llevar a cabo procesos de separación, clasificación e incautación de dispositivos electrónicos que hayan sido involucrados en algún incidente delictivo para realizar diversos procesos de extracción de evidencia y generación de reportes que puedan ser válidos en un proceso penal.

- Entender las bases legales en lo que al uso de tecnologías y proteccion de datos se refiere.
- Realizar procesos de incautacion, aislamiento y revision de dispositivos electronicos, manteniendo la integridad de los datos del mismo.
- Establecer un dictamen sobre la extracción de evidencia, garantizando la fiabilidad de la misma.
- Asegurar, extraer, analizar y entregar evidencia digital que determine la causa de un incidente tecnológico con perdida, robo o modificación de datos y espionaje.
- Implementar el uso métodos y técnicas de extracción de información en equipos electrónicos que sean aprobados por organizaciones internacionales.

3. CAMPO DE APLICACIÓN PROFESIONAL DE LOS CONOCIMIENTOS

Aplicar los conocimientos y habilidades en el campo de la seguridad informática bajo el proceso de revisión post-incidencia o computo forense en una empresa privada u organismo de gobierno que atiendan a los casos de delincuencia informática o delitos electrónicos.

4. SABERES:

Prácticos	• Analiza las escenas donde el incidente se ha llevado a cabo y organiza a su personal de apoyo para la identificación de los dispositivos afectado o “testigos” • Confisca los equipos y aisla el área afectada para evitar manipulaciones que puedan alterarla evidencia. • Extrae y analiza los datos en busca de indicadores que señalen las formas y metodologías utilizadas para llevar a cabo el incidente. • Presenta de manera formal, diplomática y legal aquellos elementos que expongan y prueben la forma en la que se llevó a cabo un incidente, así como su autor y herramientas utilizadas para tal fin.
Teóricos	• Conocimiento de las distintas arquitecturas en los dispositivos de almacenamiento. • Identifica los sistemas de archivos de los sistemas operativos para prevenir errores o manipulaciones accidentales de la evidencia. • Presenta pruebas y documentación en una corte para que el jurado o juez determine la culpabilidad o inocencia de un grupo o individuo.
Formativos	• Fortalecerá la redacción de documentos técnicos. • Fortalecerá las habilidades para expresar y defender sus ideas mediante la presentación y defensa de un proyecto de diseño. • Fortalecerá las habilidades de comunicación y diplomacia.

5. CONTENIDO TEMÁTICO (TEÓRICO-PRÁCTICO)

1.- Introducción a la Informática Forense
- Definición de la informática forense.
- Objetivos de la informática Forense.
- Servicios de la informática forense.
- Tecnologías de la informática forense.
- Oficios y preparación para la informática forense.

2.- Metodología de la informática forense.
- Arquitectura de la información.
- Proceso de análisis e investigación.
- Legislación Internacional
- Modelo SKRAM.
- Herramientas y estación de trabajo.

3.- Recopilación de pruebas digitales.
- Asegurar y Evaluación de la escena
- Entrevistas preliminares
- Documentación de la escena
- Recolección de la Evidencia.
  - Análisis de Discos, Ficheros e Internet.
  - Extracción de Metadatos.
  - Adquisición de Imágenes.
  - Evidencias en equipos de red.
  - Evidencias en tráfico de red.

4.- Generación de reporte y respuesta a incidentes.
- Panorama de la seguridad informática.
- Ataques y Pentesting
- Preparación de respuesta a incidentes.
- Presentación de evidencias analizadas.
- Preparación de reporte legal.

6. ESTRATEGIAS DE ENSEÑANZA-APRENDIZAJE

- Exposiciones por parte del docente
- Ejercicios teórico-práctico en equipo/individual (solución de ejercicios), por parte de los alumnos
- Realización de trabajo en equipo, individual por parte del alumno.

7. EVALUACIÓN DEL APRENDIZAJE

8.1. Evidencias de aprendizaje	8.2. Criterios de desempeño
Ejercicio práctico de conceptos básicos.	Valoración de los factores de seguridad en la red de computadoras en casos académicos.
Muestras de incidente de perdida de datos en un dispositivo	Se requiere el análisis exhaustivo del equipo y el aseguramiento del dispositivo de almacenamiento.
Muestra de datos recuperados	Crear una copia fiel de los datos extraídos, este debe llevar firma digital y que demuestre su integridad en los datos.
Muestra de datos corruptos o modificados,	Extraer registros de acceso a módulos de memoria donde muestren acceso a los datos para su corrupción o modificación.

8. CALIFICACIÓN

Reportes de lecturas..... 20% Actividades de laboratorio .....40% Actividades Practicas .....30% Actividad extracurricular 5%

9. ACREDITACIÓN

Periodo ordinario. De conformidad con el artículo 20 del Reglamento General de Evaluación y Promoción de Alumnos de la Universidad de Guadalajara, para que el alumno tenga derecho al registro del resultado final de la evaluación en el periodo ordinario, establecido en el calendario escolar aprobado por el Consejo General Universitario, se requiere: I. Estar inscrito en el plan de estudios y curso correspondiente, y II. Tener un mínimo de asistencia del 80% a clases y actividades registradas durante el curso.	**Periodo extraordinario.** De conformidad con el artículo 27 del Reglamento General de Evaluación y Promoción de Alumnos de la Universidad de Guadalajara, para que el alumno tenga derecho al registro de la calificación en el periodo extraordinario, se requiere: I. Estar inscrito en el plan de estudios y curso correspondiente. II. Haber pagado el arancel y presentar el comprobante correspondiente. III. Tener un mínimo de asistencia del 65% a clases y actividades registradas durante el curso. Se exceptúan de este caso las materias de orden práctico que requerirán la repetición del curso (Art. 23 RGEYPA).

10. BIBLIOGRAFÍA

BIBLIOGRAFÍA BÁSICA

- Computer Forensics JumpStart, 2nd Edición (2011). Michael G. Solomon, K Rudolph. SYBEX.
- Computer Forensics with FTK (2014). Fernando Carbone. PACKT Publishing.
- EnCE Computer Forensics Study Guide 3rd Edición (2012). Steve Bunting. SYBEX.
- CHFI Exam 312-49 Study Guide (2007). Dave Kleiman. SYNGRESS

BIBLIOGRAFÍA COMPLEMENTARIA

- Hacking Expose Computer Forensics, Secret Solutions (2010). Aaron Philipp. McGraw Hill

11. RECURSOS COMPLEMENTARIOS (páginas web, mooc's, plataformas, objetos de aprendizaje)

Plataforma educativa Networking Academy (requiere registro). Curso "Introduction to Cibersecurity"
https://www.netacad.com/

Firma: **Vo.Bo.**

Presidente de Academia **Jefe de Departamento**