1. IDENTIFICACIÓN DEL CURSO

Nombre de la materia
SEMIARIO DE ACTUALIZACION TECNOLOGICA PERMANENTE PARA INGENIERO EN TELEINFORMATICA POR OPERACIÓN VIRTUAL III

Profesor(es)
José Guadalupe Alvarado Ornelas

Clave	NRC	Horas Teoría	Horas Práctica	Horas Totales	Créditos	Tipo de curso
IN255	54662	40	60	100		BCO

Flujo de materias	
Prerrequisito formal	Redes I
Prerrequisito recomendado	Seminario de actualizacion tecnologica permanente para ingeniero en teleinformatica por operacion virtual II
Consecutiva recomendado	(In259) seminario de actualizacion tecnologica permanente para ingeniero en teleinformatica por operacion virtual IV

Academia	TECNOLOGIA Y EDUCACION	
Historial de revisiones		
Acción	Fecha	Responsable
Evaluación	Junio 2023	José Guadalupe Alvarado Ornelas
Actualización	Junio 2024	José Guadalupe Alvarado Ornelas
Aprobación por la Academia		
Cargo	Nombre	Firma
Presidente	Mtro. Alfredo luna	
Secretario	Luis Alberto Ambriz	

Nivel		Clave	Descripción
	I	AE1	Aplica los conocimientos de matemáticas, informática y fundamentos de ingeniería, así como conceptos avanzados en sistemas de información y comunicación digital, para identificar, analizar y resolver problemas específicos en el ámbito de la Ingeniería Teleinformática.
	M		
	A		
	I	AE2	Identifica, analiza y resuelve problemas complejos de las áreas de sistemas de información y comunicación digital, aplicando conocimientos de ingeniería, matemática y ciencias básicas, además formula conclusiones fundamentadas en investigaciones y bibliografía especializada, considerando los principios integrales que promuevan el desarrollo sostenible.
	M		
	A		

	I	AE3	Diseña, desarrolla y administra sistemas de información y comunicación digital resolviendo problemas complejos de ingeniería a partir de la integración de soluciones creativas para satisfacer las necesidades identificadas, considerando cuando sea necesario aspectos clave como la salud y la seguridad pública, la eficiencia en el costo del ciclo de vida, la sostenibilidad ambiental, así como los impactos culturales, sociales y ambientales asociados al uso y gestión de las tecnologías de la información.
	M		
	A		
X	I	AE4	Reproduce ambientes simulados que facilitan la investigación de problemas complejos en las áreas de sistemas de información y comunicación digital utilizando métodos de investigación, diseño de experimentos y análisis e interpretación de datos, integrando conocimiento especializado para sintetizar información y obtener conclusiones fundamentadas y válidas.
	M		
	A		
	I	AE5	Crea, selecciona y aplica sistemas de información y comunicación digital reconociendo las limitaciones de estos recursos al aplicar métodos de predicción y modelización para abordar problemas complejos del área de la Ingeniería Teleinformática.
	M		
	A		
	I	AE6	Desarrolla ambientes simulados que permiten analizar e interpretar datos en sistemas de información y comunicación digital, evaluando los impactos sociales, económicos, legales, ambientales y de sostenibilidad, para proponer soluciones integrales a problemas complejos en el área de la Ingeniería Teleinformática.
	M		
	A		
	I	AE7	Practica su responsabilidad ética y profesional en los diferentes ámbitos de la Ingeniería en Teleinformática, considerando el impacto económico, social y ambiental de sus decisiones y cumpliendo con las leyes nacionales e internacionales pertinentes.
X	M		
	A		
	I	AE8	Se desempeña y trabaja efectivamente como individuo, miembro o líder en equipos diversos, inclusivos y multidisciplinarios, estableciendo metas, planeando tareas, y analizando riesgos e incertidumbres en entornos presenciales, remotos o distribuidos.
	M		
	A		
	I	AE9	Se comunica de manera efectiva e inclusiva, tanto de manera oral como escrita, adaptándose al tipo de audiencia. Además, tiene la capacidad de redactar informes y documentación técnica de manera clara y comprensible.
	M		
	A		
	I	AE10	Aplica los conocimientos y principios de la gestión y la toma de decisiones al desarrollar y/o gestionar proyectos de manera individual o como líder de un equipo en entornos multidisciplinarios.
	M		
	A		
	I	AE11	Reconoce la necesidad de aprendizaje continuo e independiente durante toda la vida, demostrando capacidad para localizar, evaluar, integrar y aplicar conocimiento de su área profesional de manera adecuada, así como para adaptarse a las tecnologías nuevas y emergentes.
X	M		
	A		

2. PRESENTACIÓN

Descripción
Este curso pretende fomentar la formación de profesionales capaces de conocer las principales técnicas de protección frente a ataques y amenazas en los sistemas operativos, las redes, el software de aplicación los sistemas Web y las bases de datos, así mismo conozca las herramientas que le permitan preservar la integridad, la confidencialidad y la disponibilidad de la información y de activos informáticas.

3. OBJETIVO

General
El alumno conocerá la utilización de la informática forense con una finalidad preventiva, en primer término. Asimismo, podrá detectar las vulnerabilidades de seguridad con el fin de corregirlas.

Específicos
• Aplicar la informática forense para cuando la seguridad de la empresa ya ha sido vulnerada, • Utilizar herramientas forenses para recoger rastros probatorios y para averiguar, siguiendo las evidencias electrónicas, el origen de un ataque informático • Aprenderá técnicas para detectar posibles alteraciones, manipulaciones, fugas o destrucciones de datos a nivel interno de la empresa y para determinar las actividades realizadas

4. CONTENIDO

Temas y subtemas

1. Introducción a la seguridad informática
- 1.1. El valor de la información.
- 1.2. Definición y tipos de seguridad informática
- 1.3. Objetivos de la seguridad informática
- 1.4. Posibles riesgos
- 1.5. Técnicas de aseguramiento del sistema

2. Certificados y firmas digitales
- 2.1. Distribución de claves
- 2.2. Certificación
- 2.3. Arquitectura PKI
- 2.4. Estándares y protocolos de certificación
- 2.5. Ejemplos de un protocolo de seguridad

3. Seguridad en redes
- 3.1. Aspectos de seguridad en las comunicaciones
- 3.2. Debilidades de los protocolos TCP IP
- 3.3. Redes locales y amplias
- 3.4. Direcciones IP
- 3.5. Estándares para la seguridad en redes
- 3.6. Vulnerabilidad de los protocolos inalámbricos WEP, WPA, WPA2

4. Firewalls como herramientas de seguridad.
- 4.1. Tipos de firewall: de software y de hardware
- 4.2. Firewall de capas inferiores
- 4.3. Firewall de capa de aplicación
- 4.4. Firewall personal
- 4.5. Ventajas de un firewall
- 4.6. Limitaciones de un firewall
- 4.7. Políticas del firewall

5. Introducción a la informática forense
- 5.1. ¿Qué es la informática forense?
- 5.2. ¿Cuándo podemos aplicar la ciencia de informática forense?
- 5.3. Escena del crimen d. Evidencias
- 5.4. Equipo mínimo de trabajo f. Informática y crimen
- 5.5. Secuencia de análisis forense

6. Sistemas de archivos
- 6.1. Organización de los datos b. Particiones de disco
- 6.2. Capas de sistemas de archivos
- 6.3. Análisis del MBR
- 6.4. Datos alojados o sin alojar
- 6.5. Capas de metadatos
- 6.6. Apuntadores
- 6.7. Sistemas de archivo ext2/3, NTFS y FAT32/16
- 6.8. Entradas MFT

7. Uso de FTK, OSForensics, Helix y Autopsy
- 7.1. Generación de copias bit a bit
- 7.2. Montaje de imágenes
- 7.3. Análisis de registros

8. Evidencia digital
- 8.1. Evidencia digital
- 8.2. Memoria volátil
- 8.3. Metodologías y herramientas para generar imágenes de disco
- 8.4. Autentificación de la preservación de la evidencia
- 8.5. Reconocimiento del tipo de evidencia
- 8.6. Análisis de imágenes de disco y de RAM

9. Entornos Virtuales
- 9.1. Máquinas virtuales
- 9.2. Virtualización de entornos informáticos
- 9.3. Uso de software para virtualización

10. Análisis forense a dispositivos móviles
- 10.1. Análisis forense a dispositivos Android
- 10.2. Sistema de archivos y arquitectura
- 10.3. Configurando el laboratorio forense y los emuladores
- 10.4. Acceso a la información de los dispositivos
- 10.5. Adquiriendo la evidencia digital
- 10.6. Análisis de la evidencia adquirida
- 10.7. Análisis de Contactos, Llamadas, Mail, Fotos y Videos, Mensajes de Texto h. Calendario y demás información almacenada en el dispositivo
- 10.8. Análisis Con Herramientas libres y comerciales.

Prácticas	
1.-	Crear proceso en lotes para respaldar archivos
2.-	Analizar puertos abiertos en una red de computo utilizando Nmap
3.-	Copia Forense con OsForensic
4.-	Analizar metadatos de archivos de imágenes utilizando exifviewer
5.-	Extraer metadatos a cualquier archivo utilizando la FOCA
6.-	Creación de procesos en lotes avanzado
7.-	Recuperar archivos eliminados utilizando Easy Profesional Recovery
8.-	Analizando WIFI con Sistema operativo Kali Linux
9.-	Buscando evidenciasen disco duro con Autopsy

10.-	Analizando trafico de red con Wireshark
11.-	Buscando contraseñas con Beini
12.-	Análisis de sistema operativo Tequila y Agave

5. EVALUACIÓN

Ponderación de unidad de competencia para calificación	
Exposición de temas	Porcentaje
Examen práctico	10%
Tareas e investigaciones	30%
Prácticas	30%
Proyecto Final	30%

6. CRITERIOS Y MECANISMOS PARA LA ACREDITACIÓN

Descripción
De conformidad a lo que establece el Capítulo IV en los artículos 19 al 22 y Capítulo V en los artículos 23 al 29 del Reglamento General de Evaluación y Promoción de la Universidad de Guadalajara.

7. BIBLIOGRAFÍA

Básica

Autores	Título	Editorial	Año	Clasificación de Biblioteca
Cano Martínez, Jeimy J.	Computación forense: Descubriendo los rastros informáticos	Alfaomega,	2015	005.8 CAN 2015
Roger a. Grimes	Hackear al hacker	Marcombo	2018	005.8 GRI 2018

Complementaria

Autores	Título	Editorial	Año	Otra información
Jocsan Laguna	Fundamentos de la informática forense		2018	https://durivau.lpages.co/fif/
Iván M. Hidalgo Cajo	Informática Forense	Aval Espoch	2018	978-9942-35-224-8
Ramos Varón, Antonio Ángel.	Hacking práctico de redes wifi y radiofrecuencia	Ra-Ma	2014	978-84-9964-296-3