**Datos Generales de la asignatura**

| | |
|---|---|
| **Nombre de la asignatura:** | *Ciberseguridad* |
| **Clave de la asignatura:** | *TID-2304* |
| **SATCA[1]:** | *2-3-5* |
| **Carrera:** | *Ingeniería en Informática* |

**2. Presentación**

**Caracterización de la asignatura**

Esta asignatura aporta al ingeniero en informática los conocimientos necesarios para:

- Aprender diversas técnicas para el cifrado y descifrado de la información.
- Comprender, desarrollar, implementar y administrar herramientas que permitan mitigar, detectar o prevenir ataques a las vulnerabilidades que puedan presentar, sistemas, bases de datos, dispositivos de red o activos de las empresas.
- Aplicar técnicas relacionadas con la preservación de evidencia digital y el desarrollo de investigaciones de delitos informáticos.
- Reconocer, instalar, ejecutar y configurar las diversas pruebas de las distintas herramientas de software para el monitoreo de la red.

**Intención didáctica**

El temario está organizado en 5 unidades temáticas, en la primera se aborda el tema de Criptografía, donde se tratan temas relacionados con las bases de la criptografía moderna y las diversas técnicas para lograr la ocultación de la información.
El tema dos está enfocado en el estudio de las firmas digitales y los certificados digitales, permitiendo al estudiante abordar los conceptos relevantes a la seguridad de las aplicaciones mediante la certificación de las mismas, además conocerá las instituciones emisoras y validadoras de dichos certificados.
En el tema tres se abordan los temas relacionados con el hacking ético, para que el estudiante cuente con los conocimientos para identificar las vulnerabilidades que pueden existir en los sistemas de información y activos de una empresa, así como adquirir las habilidades para desarrollar o implementar herramientas que ayuden a prevenir o mitigar las amenazas que afecten las redes, sistemas o aplicaciones una empresa, así mismo las diferentes variantes de ataque o malware que existen, comprender su funcionamiento y como se ejecutan.
En tema cuatro, cómputo forense brinda los conceptos básicos, conocer las diferentes escenas del crimen en los sistemas más comunes para obtener las evidencias digitales, analizar e identificar el comportamiento de las herramientas técnicas para realizar un análisis en busca de evidencias digitales que lleven a localizar responsables o recuperación de información digital.
En el tema cinco, denominada sniffing y manejo de intrusiones, el estudiante apredeá a manejar las herramientas de sniffeo más comunes (Wireshark, Tcp-dump y Ettercap) para la detección y manejo de intrusiones.
Con estos temas y sus actividades de aprendizaje, el estudiante desarrollará su capacidad de análisis y síntesis en actividades seguridad de datos y búsqueda de evidencias digitales en los

[1] Sistema de Asignación y Transferencia de Créditos Académicos

| |
|---|
| diferentes medios informáticos, los cuales le permitan aplicar sus conocimientos en la práctica. |

**3. Participantes en la actualización, el diseño, consolidación y/o seguimiento curricular del programa**

| Lugar y fecha de elaboración o revisión | Participantes | Observaciones |
|---|---|---|
| Zacapoaxtla, Pue., abril 2023. | Academia de Ingeniería Informática del Instituto Tecnológico Superior de Zacapoaxtla. | Reunión para la elaboración de las asignaturas de la Especialidad. |

**4. Competencia(s) a desarrollar**

| Competencia(s) específica(s) de la asignatura |
|---|
| Selecciona, planifica e implementa herramientas de seguridad para la protección de la información de los usuarios, con el fin de mantener la integridad de la misma por medio de actividades preventivas, de recuperación, respuesta y la administración de incidentes. |

**5. Competencias previas**

- Selecciona, conoce y usa adecuadamente diferentes sistemas operativos.
- Implementa y administra sistemas de bases de datos.
- Desarrolla aplicaciones web.
- Configura y administra servicios de red.
- Configura máquinas virtuales y comprende su funcionamiento.
- Desarrolla aplicaciones móviles.
- Conocimiento sobre gestión de centro de datos y administración.

**6. Temario**

| No. | Temas | Subtemas |
|---|---|---|
| 1 | Criptografía | 1.1. Criptografía clásica.<br>1.1.1. En la antigüedad.<br>1.1.2. Cifradores del siglo XIX.<br>1.1.3. Criptosistemas clásicos.<br>1.1.4. Máquinas de cifrar (siglo XX) y estadística del lenguaje.<br>1.2. Esteganografía.<br>1.3. Criptosistemas Modernos.<br>1.3.1. Criptosistemas simétricos.<br>1.3.2. Criptosistemas asimétricos.<br>1.4. Criptoanálisis.<br>1.5. Cifrado de bloque.<br>1.6. Cifrado de flujo.<br>1.7. Cifrado de clave asimétrica.<br>1.8. Funciones Hash.<br>2. Firma digital. |

| | | |
|---|---|---|
| 2 | Certificados y firmas digitales | 2.1. Firma Electrónica.<br>2.1.1. Introducción.<br>2.1.2. Concepto de Firma Electrónica.<br>2.1.2.1. Tipos de Firma.<br>2.1.2.2. Usos de la Firma Electrónica.<br>2.1.2.3. Formatos de la Firma Electrónica<br>2.1.3. Dispositivos de de creación de Firma Electrónica.<br>2.1.4. Documentos firmados electrónicamente.<br>2.2. Certificado Electrónico.<br>2.2.1. Introducción.<br>2.2.2. Entidades emisoras certificadas<br>2.2.3. Tipos y clases de certificados electrónicos<br>2.2.4. Procedimientos de obtención de un certificado para persona física<br>2.2.5. Copias de seguridad de un certificado electrónico<br>2.2.6. Confidencialidad de un certificado electrónico.<br>2.2.7. Extinción de la vigencia de un certificado electrónico.<br>2.2.8. Suspensión de la vigencia de un certificado electrónico |
| 3 | Hacking ético | 3.1. Introducción a la ética hacker y la seguridad informática.<br>3.2. Pentesting.<br>3.3. Ataques de fuerza bruta y diccionario.<br>3.4. Explotación de vulnerabilidades comunes.<br>3.5. Técnicas de ingeniería social.<br>3.6. Análisis de vulnerabilidades de aplicaciones web y móviles<br>3.7. Vulnerabilidades comunes en las aplicaciones web y móviles.<br>3.8. Penetración en sistemas y redes<br>3.9. Seguridad inalámbrica y hacking de redes WiFi.<br>3.10. Protección y mitigación de ataques informáticos. |
| 4 | Cómputo forense | 4.1. Introducción al cómputo forense.<br>4.1.1. Definición, importancia y objetivos de la informática forense.<br>4.1.2. Metodología del análisis.<br>4.1.3. Identificación de la evidencia. |

| | | |
|---|---|---|
| | | 4.2. Metodologías para la investigación en cómputo forense.<br>4.2.1. Metodologías para la recolección, preservación y aseguramiento de la evidencia digital.<br>4.2.2. Metodologías para el análisis digital.<br>4.2.3. Documentación y redacción de reportes del cómputo forense.<br>4.3. Herramientas para el análisis forense<br>4.3.1. Análisis de imagen de dispositivo USB<br>4.3.2. Análisis de imagen de memoria RAM<br>4.3.3. Análisis de imagen del Disco Duro.<br>4.3.4. Análisis forense de dispositivos móviles. |
| 5 | Sniffing y manejo de intrusiones | 5.1. Sniffing.<br>5.1.1. Wireshark.<br>5.1.2. Tcp-dump.<br>5.1.3. Ettercap.<br>5.2. Manejo de intrusiones.<br>5.2.1 Sistemas de detección de intrusos.<br>5.2.2 Sistema de prevención de intrusos.<br>5.2.3 Honey pot. |

**7. Actividades de aprendizaje de los temas**

| Criptografía | |
|---|---|
| Competencias | Actividades de aprendizaje |
| Específica(s): Aprender diversas técnicas para el cifrado y descifrado de la información.<br>Genéricas:<br>• Capacidad de análisis y síntesis<br>• Habilidad para buscar y analizar<br>• información proveniente de fuentes diversas.<br>• Solución de problemas.<br>• Trabajo en equipo.<br>• Capacidad de aplicar los conocimientos.<br>• Habilidad para trabajar en forma autónoma. | • Dominar los términos básicos de criptografía.<br>• Realizar el cifrado y descifrado de información.<br>• Análisis de los Criptosistemas Modernos<br>• Investigar ventajas y desventajas de aplicar Software para firmas digitales. |
| Certificados y firmas digitales | |
| Competencias | Actividades de aprendizaje |
| Específica(s): Aprender el concepto, funcionamiento y utilidad de los Certificados Digitales, así como aprender el mecanismo de la Firma Digital. | • Realizar una investigación en diferentes fuentes de información sobre los conceptos relevantes a los temas.<br>• Presentar en plenaria las conclusiones sobre la investigación |

| | |
|---|---|
| Genéricas:<br>• Capacidad de análisis y síntesis<br>• Habilidad para buscar y analizar<br>• información proveniente de fuentes diversas.<br>• Solución de problemas.<br>• Trabajo en equipo.<br>• Capacidad de aplicar los conocimientos.<br>• Habilidad para trabajar en forma autónoma. | • Realizar actividades prácticas en sesiones de laboratorio en el que aplique los conocimientos adquiridos para la implementación de algún certificado en una aplicación web o móvil.<br>• Concentrar información sobre las empresas prestadoras de servicios de certificación y discutirlos en clase. |
| Hacking Ético | |
| Competencias | Actividades de aprendizaje |
| Específica(s): Identifica y aplica conocimientos que le permitan identificar vulnerabilidades en los sistemas informáticos mediane el haking ético y ser capaz de desarrollar y aplicar técnicas que permitan la protección de los activos y sistemas de información.<br><br>Genéricas:<br>• Capacidad de análisis, sintetizar información dentro del área de la seguridad informática.<br>• Habilidades para utilizar herramientas tecnológicas que le ayuden a la búsqueda de información.<br>• Capacidad de integración en equipos de trabajo interdisciplinario.<br>• Capacidad de investigación y trabajo colaborativo.<br>• Capacidad de continuar el aprendizaje autodirigido o autónomo.<br>• Comprender y conocer las nuevas herramientas del hacking ético.<br>• Conocer las tendencias en ataques y la implementación de la inteligencia artificial en la protección de datos. | • Lectura e investigación de los conceptos fundamentales del hacking ético, conocer las amenazas como el phishing, ataques, malware, conocer a personas que se dediquen al hacking ético y compartan sus experiencias.<br>• Realizar reconocimiento de vulnerabilidades, realizando reconocimiento, escaneo, exploración y documentar lo encontrado, todo esto mediante el uso de herramientas tecnológicas.<br>• Realizar hacking a servidores web, aplicaciones web y aplicaciones móviles.<br>• Creación de dinámicas de Role-playing en la que los estudiantes actúen como atacantes y el otro como defensor en el que se apliquen casos de ingeniería social que permitan identificarlos y prevenirlos.<br>• Análisis y creación de correos electrónicos de phising, aprender a identificar los signos reveladores de un correo malicioso.<br>• Realizar prácticas en laboratorio, con dispositivos de simulación web y móvil que permitan explotar e identificar las vulnerabilidades y cómo prevenirlas.<br>• Escaneo y análisis de las redes inalámbricas en búsqueda de vulnerabilidades en la configuración de la red, como contraseñas, configuraciones de cifrado incorrecto, filtrado MAC.<br>• Análisis de los protocolos de comunicación inalámbricas como Wi-Fi, |

<table>
<tr><td></td><td>Bluetooth, NFC y los nuevos protocolos que se generen en la industria.<br>• Crear un informe detallado de las vulnerabilidades encontradas, reportar que tan graves pueden ser y cómo corregirlas.</td></tr>
<tr><td colspan="2">Cómputo forense</td></tr>
<tr><td>Competencias</td><td>Actividades de aprendizaje</td></tr>
<tr><td>Específica(s): Comprender los conceptos e identificar las técnicas y metodologías de análisis implementadas en la aplicación del cómputo Forense<br>Genéricas:<br>• Capacidad de análisis y s<br>• Habilidad para buscar y analizar información proveniente de fuentes diversas.<br>• Capacidad de aplicar los conocimientos en la práctica.<br>• Compromiso ético.<br>• Trabajo en equipo.<br>• Capacidad de organizar y planificar.<br>• Comunicación oral y escrita en su propia lengua.<br>• Búsqueda del logro.</td><td>• Realiza una síntesis de los conceptos básicos de la informática forense.<br>• Elabora un Mapa conceptual sobre técnicas de recolección de evidencias informáticas<br>• Elabora y presenta un informe técnico, a partir de un caso de estudio que incluya descripción de:<br>• Procedimiento de cadena de custodia de la evidencia digital, metodología de análisis forense utilizada.<br>• Realiza análisis forense en computadora o dispositivo móvil y genera informe.</td></tr>
<tr><td colspan="2">Sniffing y manejo de intrusiones</td></tr>
<tr><td>Competencias</td><td>Actividades de aprendizaje</td></tr>
<tr><td>Específica(s): Reconocer, instalar, ejecutar y configurar las diversas pruebas de las distintas herramientas de software para el monitoreo de la red.<br>Genéricas:<br>• Capacidad de análisis y síntesis<br>• Habilidad para buscar y analizar información proveniente de fuentes diversas.<br>• Solución de problemas.<br>• Trabajo en equipo.<br>• Capacidad de aplicar los conocimientos.<br>• Habilidad para trabajar en forma autónoma.</td><td>• Instalar, configurar, manejar y analizar resultado de las herramientas de Sniffing.<br>• Identificar, monitorear y bloquear posibles intrusiones.</td></tr>
</table>

**8. Práctica(s)**

1. Realizar ejercicios para recabar información sobre las vulnerabilidades de una empresa.
2. Realizar simulaciones de acceso de fuerza bruta como técnica para descubrir alguna información.
3. Practicas donde el estudiante pueda crear máquinas virtuales y pueda simular un ataque o visualizar el funcionamiento de algún malware.
4. Identificar las vulnerabilidades y amenazas que existen en los sistemas web o aplicaciones móviles en determinados contextos
5. A partir de casos prácticos, justificar la selección de una metodología adecuada para aplicarse en el análisis informático e identificar la evidencia encontrada y clasificarla.
6. Prácticas de laboratorio en donde el estudiante conozca la forma de extraer evidencias de los distintos medios de almacenamiento.

**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 especificas 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**

- Para evaluar las actividades de aprendizaje se recomienda solicitar: mapas conceptuales, reportes de prácticas, estudios de casos, exposiciones en clase, ensayos, problemarios, reportes de visitas, portafolio de evidencias y cuestionarios, cuadro sinóptico.
- Para verificar el nivel del logro de las competencias del estudiante se recomienda utilizar: listas de cotejo, listas de verificación, matrices de valoración, guías de observación, coevaluación y autoevaluación.

**11. Fuentes de información**

1. Biswas, A. (2020). Ultimate Mobile Hacking: basic to advanced. Amlan Biswas.
2. Chicano, E., Gestión de incidentes de Seguridad Informática. IFCT0109, IC Editorial, 2015, ISBN: 9788416351701.
3. Chapple, M., & Seidl, D. (2021). CompTIA Security+ Certification Kit: Exam SY0-601. Sybex.
4. Erickson, J. (2008). Hacking: The Art of Exploitation, 2nd Edition. No Starch Press.
5. Guerra, M (2021), Análisis forense informático, Editorial RA-MA, ISBN 9788418971242.
6. Hadnagy, C. (2018). Social Engineering: The Science of Human Hacking. John Wiley & Sons.
7. Kim, P. (2015). The Hacker Playbook 2: Practical Guide to Penetration Testing. Createspace Independent Publishing Platform.
8. Sikorski, M., & Honig, A. (2012). Practical Malware Analysis.
9. Stuttard, D., & Pinto, M. (2011). The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws. John Wiley & Sons.