1. Datos Generales de la Asignatura

Nombre de la Asignatura:	**Seguridad Informática**
Calve de la Asignatura:	**SWC-1705**
SATCA[1]:	**2-2-4**
Carrera:	**Ingeniería en Sistemas Computaciones**

2. Presentación

Caracterización de la asignatura

Esta asignatura aporta al perfil del Ingeniero en Sistemas Computacionales las capacidades de aplicar conocimientos científicos y tecnológicos en la solución de problemas en el área informática con un enfoque interdisciplinario; de seleccionar y utilizar de manera óptima técnicas y herramientas computacionales actuales y emergentes; y la aplicación de normas, marcos de referencia y estándares de calidad y seguridad vigentes en el ámbito del desarrollo y gestión de tecnologías y sistemas de información.

Para conformarla, se ha hecho un análisis de las características que son necesarias conocer para implementar diferentes herramientas y técnicas de seguridad basados, sobre todo, en las características propias que tiene Internet con el fin de mantener la integridad de la información en sistemas de redes de computadoras.

Intención didáctica

El temario está organizado en 5 unidades, en la primera unidad se abordan aspectos muy generales de la seguridad informática, como los términos Información, Riesgos, Ingeniería Social; así como el significado de Seguridad Informática.

En la segunda unidad, se abarcan diversos tópicos actuales de seguridad informática básica como Vulnerabilidad y Amenaza, Cyber–Guerra y Hacktivismo; así como la concientización social.

En la tercera unidad correspondiente al tema de Criptografía se tratan temas relacionados con las bases de la Criptografía moderna y las diversas técnicas para lograr la ocultación de la información hoy en día.

En la cuarta unidad denominada Sniffing y Manejo de Intrusiones, se manejan las

[1] Sistema de Asignación y Transferencia de Créditos Académicos

herramientas de sniffeo más comunes (Wireshark, Tcp-dump y Ettercap) para la detección y manejo de intrusiones.

En la quinta y última unidad se tocan temas relacionados a la prevención, recuperación, respuesta y administración de incidentes, como métodos de contingencia ante intrusiones, accidentes o desastres naturales.

3. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
Seleccionar, planificar e implementar herramientas de seguridad en redes 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 administración de incidentes.

4. Competencias previas

- Conocer los conceptos básicos de Software Libre.
- Manejar sistemas operativos de tipo UNIX.
- Conocer las diferencias entre amenazas y vulnerabilidades y términos afines.
- Dominar conceptos básicos de redes informáticas.

5. Temario

Unidad	Temas	Subtemas
1	Aspectos generales de 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. 1.6. Ingeniería Social.
2	Tópicos actuales de seguridad informática.	2.1. Vulnerabilidades y Amenazas. 2.2. Cyber–Guerra y Hacktivismo. 2.3. El reto de la privacidad de la información. 2.4. Concientización social. 2.5. Evolución de riesgos: ¿Qué, cómo y de quién proteger?
3	Criptografía.	3.1. Criptografía clásica. 3.1.1. En la antigüedad. 3.1.2. Cifradores del siglo XIX. 3.1.3. Criptosistemas clásicos. 3.1.4. Máquinas de cifrar (siglo XX) y

		estadística del lenguaje. 3.2. Esteganografía 3.3. Criptosistemas Modernos. 3.3.1. Criptosistemas simétricos. 3.3.2. Criptosistemas asimétricos. 3.4. Criptoanálisis. 3.5. Cifrado de bloque. 3.6. Cifrado de flujo. 3.7. Cifrado de clave asimétrica. 3.8. Funciones Hash. 3.9. Firma digital.
4	Sniffing y Manejo de Intrusiones.	4.1. Sniffing. 4.1.1. Wireshark. 4.1.2. Tcp-dump. 4.1.3. Ettercap. 4.2. Manejo De Intrusiones. 4.2.1. Sistemas de detección de intrusos. 4.2.2. Sistema de prevención de intrusos. 4.2.3. Honey Pots.
5	Prevención, recuperación, respuesta y administración de incidentes.	5.1. Seguridad Perimetral. 5.2. Protección de Sistemas Operativos. 5.2.1. Equipos de Escritorio. 5.2.2. Servidores. 5.2.3. Dispositivos Móviles. 5.3. Seguridad en Servicios de Red. 5.4. Plan de recuperación de Desastres.