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. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración ó revisión	Participantes	Evento
Instituto Tecnológico de Tuxtepec, Enero de 2017	Academia de Sistemas y Computación.	Módulo de especialidad

4. 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.

5. 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.

6. 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.

7. Actividades de aprendizaje de los temas

1. Aspectos generales de la seguridad informática.	
Competencias	Actividades de aprendizaje
Específica(s): Dominar significados, temas y	• Investigar el significado de los términos más comunes empleados en seguridad informática.

aspectos básicos de la seguridad informática. Genéricas: • Capacidad de análisis y síntesis. • Capacidad de organizar y planificar. • Comunicación oral y escrita. • habilidad para buscar y analizar información • proveniente de fuentes diversas. • Solución de problemas. • Toma de decisiones. • Capacidad crítica y autocrítica. • Capacidad de trabajar en equipo. • Capacidad de comunicar sus ideas. • Capacidad de liderazgo. • Capacidad de aplicar los conocimientos en la • práctica. • Habilidades de investigación. • Capacidad de aprender. • Capacidad de adaptarse a nuevas situaciones. • Capacidad de generar nuevas ideas • (creatividad). • Habilidad para trabajar en forma autónoma. • Preocupación por la calidad. • Búsqueda del logro.	• Identificar los objetivos de la seguridad informática. • Identificar y emplear las técnicas de aseguramiento del sistema.
2. Tópicos actuales de seguridad informática.	
Competencias	Actividades de aprendizaje
Específica(s): Tomar conciencia de las amenazas que representan las intrusiones en los sistemas de información y de la importancia de concientizar sobre las buenas políticas para el manejo de datos personales.	• Distinguir las diferencias entre amenazas y vulnerabilidades. • Desarrollar un proyecto de concientización destinado al público en general. • Desarrollar una perspectiva sobre la manera en la que los riesgos evolucionan.

Genéricas: • Capacidad de análisis y síntesis. • Capacidad de organizar y planificar. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Solución de problemas. • Toma de decisiones. • Trabajo en equipo. • Capacidad de aplicar los conocimientos. • Habilidades de investigación. • Capacidad de generar nuevas ideas. • Liderazgo. • Habilidad para trabajar en forma Autónoma. • Búsqueda del logro.	
3. Criptografía.	
Competencias	Actividades de aprendizaje
Específica(s): Aprender diversas técnicas para el cifrado y descifrado de la información. Genéricas: • Capacidad de análisis y síntesis. • Capacidad de organizar y planificar. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Solución de problemas. • Toma de decisiones. • Trabajo en equipo. • Capacidad de aplicar los conocimientos. • Habilidades de investigación. • Capacidad de generar nuevas	• Dominar los términos básicos de criptografía. • Realizar el cifrado y descifrado de información. • Análisis de los Criptosistemas Modernos • Investigar ventajas y desventajas de aplicar Software para firmas digitales

ideas. • Liderazgo. • Habilidad para trabajar en forma Autónoma. • Búsqueda del logro.	
4. Sniffing y Manejo de Intrusiones.	
Competencias	Actividades de aprendizaje
Específica(s): Reconocer, instalar, ejecutar y configurar las diversas pruebas de las distintas herramientas de software para el monitoreo de la red. Genéricas: • Capacidad de análisis y síntesis. • Capacidad de organizar y planificar. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Solución de problemas. • Toma de decisiones. • Trabajo en equipo. • Capacidad de aplicar los conocimientos. • Habilidades de investigación. • Capacidad de generar nuevas ideas. • Liderazgo. • Habilidad para trabajar en forma Autónoma. • Búsqueda del logro.	• Instalar, Configurar, Manejar y Analizar resultado de las herramientas de Sniffing. • Identificar, monitorear y bloquear posibles intrusiones.
5. Servidores de Nombre de Dominio	
Competencias	Actividades de aprendizaje
Específica(s): Desarrollar un plan de contingencia ante una posible eventualidad con el	• Elaborar políticas de seguridad con respecto a los tipos de usuarios que tienen acceso al sistema de información. • Desarrollar un plan de contingencia contra

fin de proteger la información así como la integridad y disponibilidad de la misma. Genéricas: • Capacidad de análisis y síntesis. • Capacidad de organizar y planificar. • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Solución de problemas. • Toma de decisiones. • Trabajo en equipo. • Capacidad de aplicar los conocimientos. • Habilidades de investigación. • Capacidad de generar nuevas ideas. • Liderazgo. • Habilidad para trabajar en forma Autónoma. • Búsqueda del logro.	desastres naturales. • Desarrollar un plan de contingencia contra detección de incidentes. • Desarrollar un plan de recuperación en cada caso previo.

8. Práctica(s)

- Elaborar certificados digitales con herramientas de tipo PGP.
- Firmar documentos con certificados digitales.
- Cifrar documentos con certificados digitales, síncrona y asíncronamente.
- Validación de integridad de documentos.
- Elaborar estadísticas de tráfico mediante escaneo de redes.
- Identificar firmas de navegadores y sistemas operativos mediante escaneo de redes.
- Elaborar políticas de seguridad informática.
- Elaborar plan de recuperación de desastres.

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

La evaluación debe ser continua por lo que debe considerar el desempeño de cada una de las actividades de aprendizaje, haciendo énfasis en:

- Exposiciones de las investigaciones realizadas acorde a los temas del curso.
- Uso de plantillas e integración de conceptos en la definición de modelos y en la integración del documento del proyecto.
- Participación en clase.
- Ejercicios realizados en clase.
- Información obtenida durante las búsquedas encomendadas.
- Lectura y análisis de textos.
- Autoevaluación, Coevaluación y evaluación de las actividades.
- Revisión periódica del avance del proyecto (o proyectos) de la asignatura, de acuerdo a la metodología y fechas establecidas.
- Narrativa individual de las conclusiones y visión personal de la experiencia del proyecto desarrollado.

11. Fuentes de información

1. Chicano, E., Auditoría de Seguridad Informática. IFCT0109, IC Editorial, 2015, ISBN: 9788416433230.
2. Rault, R., Schalkwijk, L., Acissi, L., et. al. Seguridad informática - Hacking Ético: Conocer el ataque para una mejor defensa, Ediciones ENI, Ttercera edición, 2015, ISBN: 9782746097247.
3. Aguilera, P. Seguridad Informática., Editex, 2010, ISBN: 9788497717618.
4. Chicano, E., Gestión de incidentes de Seguridad Informática. IFCT0109, IC Editorial, 2015, ISBN: 9788416351701.
5. De Marcelo, J., Piratas cibernéticos: cyberwars, seguridad informática e Internet, Ra-Ma., Segunda edición, 2003. ISBN: 9788478975570.