1.- DATOS DE LA ASIGNATURA

Nombre de la asignatura: **Seguridad Informática II**

Carrera: **Ingeniería en Sistemas Computacionales**

Clave de la asignatura: **SIF-1203**

(Créditos) SATCA: **3-2-5**

2.- PRESENTACIÓN

Caracterización de la asignatura.

Esta materia aporta al perfil del profesionista la visión de los aspectos que influyen en la seguridad informática. También proporcionará los conocimientos básicos de seguridad para el desarrollo de proyectos de tecnologías de información.

Se inicia recordando e investigando los mecanismos y sistemas de protección de seguridad informática, entre ellos se encuentran la Seguridad Física y la Seguridad lógica. También se incluyen temas como la seguridad en Redes de datos, seguridad en redes Inalámbricas y seguridad en sistemas de computo.

En la unidad siguiente es una introducción al monitoreo de la seguridad mediante la administración de políticas de seguridad, identificación de vulnerabilidades y conocimientos básicos sobre la detección de intrusos.

Subsecuentemente la unidad 3 presenta un control sobre la seguridad informática, es decir mediante conceptos como: auditoria de red, auditoria en sistemas; son investigadas y puesta en marcha alguna herramienta que permita realizar el análisis forense ya sea en una red de datos o un sistema operativo. También se hace una investigación sobre herramientas que permite realizar la detección de intrusos.

La unidad 4 nos da un panorama actual sobre la legislación en México y el mundo en materia de Seguridad Informática, tocando puntos clave como: el impacto social y Económico en las sociedades del mundo.

La materia concluye con la unidad 5 donde se investiga el estado de arte de la cultura de seguridad informática, analizando las nuevas tendencias en mecanismos de protección, ataques, vulnerabilidades y problemas de seguridad.

3.- COMPETENCIAS A DESARROLLAR

Competencias Específicas	**Competencias genéricas**
Desarrollar soluciones para problemas de seguridad informática, analizando el tipo de vulnerabilidades, proponiendo soluciones tanto teóricas como prácticas e implementando políticas de calidad como herramientas de seguridad.	**Competencias instrumentales:** • 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. **Competencias interpersonales:** • Capacidad crítica y autocrítica • Capacidad de trabajar en equipo • Capacidad de comunicar sus ideas • Capacidad de liderazgo **Competencias sistémicas:** • 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) • Liderazgo • Habilidad para trabajar en forma autónoma • Preocupación por la calidad

4.- HISTORIA DEL PROGRAMA

Lugar y Fecha	Participantes	Evento
Instituto Tecnológico de Tláhuac, México D.F. 18 de Mayo de 2012	Academia de Sistemas y Computación	

5.- OBJETIVO(S) GENERAL(ES) DEL CURSO (competencias específicas a desarrollar).

El alumno conocerá, identificará y aplicará los servicios y herramientas que le permitan implementar la seguridad informática dentro de una organización; conocerá, comprenderá y hará usos de las estrategias de monitoreo de los mecanismos de seguridad dentro de una organización, a la vez que podrá controlar los sucesos e incidentes de seguridad conociendo los aspectos sociales en el área de seguridad informática.

6.- COMPETENCIAS PREVIAS

Tener el conocimiento de conceptos sobre temas como el manejo de sistemas operativos, Seguridad informática lógica y física, y Redes de Telecomunicaciones.

7.- TEMARIO

Unidad	Temas	Subtemas
1	Implementación de la seguridad informática	1.1 Sistemas y mecanismos de protección 1.1.1 Seguridad física 1.1.1.1 Protección del hardware 1.1.1.1.1 Acceso físico 1.1.1.1.2 Desastres naturales 1.1.1.2 Contratación de personal 1.1.2 Seguridad lógica 1.1.2.1 Identificación y Autenticación 1.1.2.2 Modalidad de Acceso 1.1.2.3 Control de Acceso Interno 1.1.2.3.1 Contraseñas 1.1.2.3.2 Listas de Control de Acceso 1.1.2.3.3 Cifrado 1.1.2.4 Control Acceso Externo 1.1.2.4.1 Dispositivos de control de puertos 1.1.2.4.2 Firewalls 1.1.2.4.2.1 Selección de tipo de Firewall 1.1.2.4.2.2 Integración de las políticas de seguridad 1.1.2.4.2.3 Revisión y análisis del mercado 1.1.2.4.3 Proxies 1.1.2.4.4 Integridad del Sistema 1.1.2.4.5 VPN (Virtual Private Networks) 1.1.2.4.6 DMZ (Zona Desmilitarizada) 1.1.2.4.7 Herramientas de seguridad 1.2 Seguridad en Redes de Datos 1.2.1 Amenazas y Ataques a Redes 1.2.2 Elementos básicos de protección 1.2.3 Introducción a la Criptografía 1.2.4 Seguridad de la Red a nivel: 1.2.4.1 Aplicación 1.2.4.2 Transporte 1.2.4.3 Red 1.2.4.4 Enlace 1.2.5 Monitoreo 1.3 Seguridad en Redes Inalámbricas 1.3.1 Seguridad en el Access Point

		1.3.2 SSID (Service Set Identifier) 1.3.3 WEP (Wired Equivalent Privacy) 1.3.4 Filtrado de MAC Address 1.3.5 RADIUS Authentication 1.3.6 WLAN VPN 1.3.7 Seguridad sobre 802.11(x) 1.3.8 Nuevas Tecnologías de Seguridad para Redes inalámbricas 1.4 Seguridad en Sistemas 1.4.1 Riesgos de Seguridad en Sistemas 1.4.2 Arquitectura de los Sistemas 1.4.3 Problemas Comunes de Seguridad 1.4.4 Instalación Segura de Sistemas 1.4.5 Administración de Usuarios y controles de acceso 1.4.6 Administración de Servicios 1.4.7 Monitoreo 1.4.8 Actualización de los sistemas 1.4.9 Mecanismos de Respaldo
2	Monitoreo de la seguridad informática	2.1 Administración de la Seguridad informática 2.1.1 Administración de cumplimiento de políticas 2.1.2 Administración de incidentes 2.1.3 Análisis de nuevas vulnerabilidades en la infraestructura 2.1.4 Monitoreo de los Mecanismos de Seguridad 2.2 Detección de intrusos 2.2.1 Sistemas de detectores de intrusos 2.2.2 Falsos Positivos 2.2.3 Falsos Negativos 2.2.4 Métodos de Detección de Intrusos 2.2.4.1 Análisis de tráfico 2.2.4.2 HIDS (Host Intrusion Detection System) 2.2.4.3 NIDS (Network Intrusion Detection System) 2.2.4.4 Nuevos métodos de detección 2.2.5 Identificación de Ataques 2.2.6 Análisis del tiempo de respuesta de IDS

3	Control de la seguridad informática	3.1 Auditoría de Red 3.1.1 Concepto de Auditoría sobre la Red 3.1.2 Herramientas de Auditoría 3.1.3 Mapeo de la Red 3.1.4 Monitoreo de Red 3.1.5 Auditoría a Firewalls 3.1.6 Pruebas de Penetración sobre redes 3.1.7 Análisis de información y resultados 3.2 Auditoría a Sistemas 3.2.1 Checklist de Seguridad 3.2.2 Baseline del Sistema 3.2.3 Auditoría a las políticas del sistema 3.2.4 Auditoría a usuarios 3.2.5 Comandos del sistema 3.2.6 Herramientas para realizar auditoría 3.2.7 Auditoría a los Registros y Bitácoras del Sistema 3.2.8 Auditoría a la Capacidad de Recuperación ante desastres 3.2.9 Auditoría a la Configuración del Sistema 3.2.10 Análisis de la Información y Resultados 3.3 Análisis forense a sistemas de cómputo 3.3.1 Introducción al Análisis Forense en Sistemas de Cómputo 3.3.2 Obtención y Protección de la Evidencia 3.3.3 Análisis Forense sobre Sistemas 3.3.3.1 Imágenes en Medios de Almacenamiento 3.3.3.2 Revisión de Bitácoras 3.3.3.3 Revisión del Sistema de Archivos 3.3.3.3.1 Tiempos de modificación, acceso y creación 3.3.3.4 Revisión de procesos 3.3.3.5 Herramientas y técnicas del Análisis forense 3.3.4 Herramientas para obtener

		información de la Red 3.3.5 Análisis de la Información y Resultados 3.3.6 Sistemas de detección de intrusos 3.3.6.1 Aplicación de los SDI en la SI 3.3.6.2 Tipos de sistemas de DI 3.3.6.3 Nivel de interacción de los SDI 3.4 Respuesta y Manejo de Incidentes 3.4.1 Respuesta a Incidentes 3.4.2 Creación de un equipo de respuesta a Incidentes de Seguridad Informática
4	Entorno social e impacto económico de la seguridad informática	4.1 Legislación Mexicana 4.1.1 Acceso Ilícito a Sistemas 4.1.2 Código Penal 4.1.3 Derechos de Autor 4.1.4 Actualidad de la legislación sobre delitos informáticos 4.2 Ley Modelo (CNUDMI) 4.3 Legislaciones Internacionales 4.3.1 Legislación de EUA en Materia Informática 4.3.2 Legislación de Australia en Materia Informática 4.3.3 Legislación de España en Materia Informática 4.3.4 Otras Legislaciones 4.4 Impacto Social de la Seguridad Informática 4.5 Impacto Económico de la Seguridad Informática
5	Nuevas tendencias y tecnologías	5.1 Cultura de la Seguridad Informática 5.2 Nuevas Tecnologías de Protección 5.3 Tendencias en Ataques y Nuevos Problemas de Seguridad 5.3.1 SPAM 5.3.2 Malware 5.3.3 Exploits de Días Cero 5.3.4 Metasploits 5.3.5 Otros

8.-SUGERENCIAS DIDÁCTICAS (desarrollo de competencias genéricas)

El profesor debe ser competente en la disciplina que está bajo su responsabilidad y aplicar los conceptos de la asignatura. Desarrollar la capacidad para coordinar y trabajar en equipo; orientar el trabajo del estudiante y potenciar en él la autonomía, el trabajo cooperativo y la toma de decisiones.

Tomar en cuenta el conocimiento de los estudiantes como punto de partida y como obstáculo para la construcción de nuevos conocimientos.

- Propiciar actividades de búsqueda, selección y análisis de información en distintas fuentes y explicarlo mediante un mapa conceptual, mental o cuadro sinóptico.
- Proponer un caso de estudio de seguridad física y lógica, en el cual el estudiante determine las diferentes fases del mismo, para discutirlo en grupos de trabajo y proponer soluciones.
- Fomentar la participación del estudiante mediante tormenta de ideas, exposiciones que permita que propicie el uso adecuado de conceptos, y de terminología de la seguridad Informática.
- Proponer problemas que permitan al estudiante la integración de contenidos de la asignatura y entre distintas asignaturas, para su análisis y solución.
- Propiciar en el estudiante la lectura y reflexión de artículos relacionados con la asignatura.
- Proporcionar al estudiante la relación de los contenidos de temáticos con el desarrollo de cuestionarios de investigación y ensayos sobre el estado de arte en los temas de este programa de estudio.
- Exponer los proyectos finales.

9.-SUGERENCIAS DE EVALUACIÓN

Se sugiere que el estudiante proponga un proyecto, preferentemente que atienda un problema real, que de acuerdo a las especificaciones integre los puntos estudiados en las unidades de aprendizaje. Se recomienda que los proyectos sean desarrollados por equipos de trabajo cuidando la participación activa de cada uno de los integrantes. También debe de fomentarse y evaluarse la investigación e incluir los resultados de las mismas como sustento en la toma de decisiones en el desarrollo del proyecto. La evaluación debe ser continua y formativa por lo que se debe considerar el desempeño en cada una de las actividades de aprendizaje, haciendo especial énfasis en:

- Ponderar tareas y prácticas en laboratorio.
- Participación y desempeño del alumno en el aula
- Dar seguimiento al desempeño integral de alumno en desarrollo de programa (dominio de los conceptos, capacidad de la aplicación de los conocimientos en problemas reales en los laboratorios).
- Dar valor a la participación del alumno (exposición y debates).
- Exámenes Teóricos-Prácticos.
- Desarrollo de un proyecto final que integre todas las unidades de aprendizaje.

10.-UNIDADES DE APRENDIZAJE

UNIDAD 1.- Implementación de la Seguridad Informática

Competencia específica a desarrollar	Actividades de Aprendizaje
Explicar y aplicar los mecanismos de seguridad física y lógica	Investigar los requisitos necesarios para poder implementar mecanismos de seguridad informática de manera física y lógica.

UNIDAD 2.- Monitoreo de la Seguridad Informática

Competencia específica a desarrollar	Actividades de Aprendizaje
Conocer y aplicar las técnicas de administración de seguridad y las tecnologías para la detección de intrusos	Investigar y debatir los conceptos básicos de las técnicas para la administración de la seguridad informática, detección de intrusos e identificación de ataques, para poder llevarlo a la práctica dentro de una organización informática de manera física y lógica.

UNIDAD 3.- Control de la Seguridad Informática

Competencia específica a desarrollar	Actividades de Aprendizaje
Conocer los métodos y herramientas para el análisis forense en informática, así como mantener el control sobre redes y dispositivos	Realizar investigación sobre los distintos tipos de auditorías, que se aplican en los controles de la seguridad informática, tomando en cuenta prácticas en cada una de ellas.

UNIDAD 4.- Entorno social e impacto económico de la seguridad informática

Competencia específica a desarrollar	Actividades de Aprendizaje
Conocer los aspectos sociales y económicos en el campo de la seguridad informática.	Investigar todas las normas y leyes que se aplican en México y el mundo para poder implementar distintas técnicas de seguridad en sistemas informáticos y la repercusión en los diferentes aspectos sociales y económicos.

UNIDAD 5.- Nuevas tendencias y tecnologías

Competencia específica a desarrollar	Actividades de Aprendizaje
Conocer las nuevas tendencias en ataques hacia sistemas y redes de cómputo, así como las nuevas tecnologías.	Investigar y debatir las ideas mediante un ensayo sobre las tendencias y tecnologías en la seguridad informática. Comentar en clase sobre términos como SPAM, las amenazas en la actualidad, Malware, etc.

11-FUENTES DE INFORMACIÓN

- ANONYMOUS
  Maximun Security
  Fourth Edition
  USA, Sams Publishing, 2003
- BELLOVIN, Steven, CHESWICK, William, RUBIN, Aviel
  Firewalls and Internet Security: Repelling the Wily Hacker
  Second Edition, USA, Addison Wesley, 2003
- GARFINKEL, Simson, SCHWARTZ, Alan, SPAFFORD, Gene
  Practical UNIX & Internet Security
  Third Edition, USA, O'Reilly, 2003
- KING, Todd
  Security + Training Guide
  USA, Que, 2003
- LISKA, Allan
  The Practice of Network Security: Deployment Strategies for Production Enviroments
  USA, Prentice Hall, 2002