



SEGURIDAD INFORMÁTICA II

0916

8°, 9°

06

Asignatura

Clave

Semestre

Créditos

Ingeniería Eléctrica

Ingeniería en Computación

Ingeniería en Computación

División

Departamento

Carrera en que se imparte

Asignatura:

Horas:

Total (horas):

Obligatoria

Teóricas

Semana

Optativa
de elección

Prácticas

16 Semanas

Modalidad: Curso

Asignatura obligatoria antecedente: Seguridad Informática I

Asignatura obligatoria consecuente: Ninguna

Objetivo(s) del curso: 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 uso de las estrategias de monitoreo de los mecanismos de seguridad para administrar la 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 la seguridad informática.

Temario

NÚM.	NOMBRE	HORAS
1.	Implementación de la seguridad informática	12.0
2.	Monitoreo de la seguridad informática	12.0
3.	Control de la seguridad informática	12.0
4.	Entorno social e impacto económico de la seguridad informática	6.0
5.	Nuevas tendencias y tecnologías	6.0
		48.0
	Prácticas	0.0

Total

48.0





1 Implementación de la seguridad informática

Objetivo: El alumno conocerá, explicará y aplicará los mecanismos y herramientas de protección para cuidar de la seguridad informática en una organización de manera física y lógica.

Contenido:

- 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 de 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 del Tipo de Firewall
 - 1.1.2.4.2.2 Integración de las Políticas de Seguridad al Firewall
 - 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

Objetivo: El alumno conocerá y aplicará las técnicas que le permitan administrar la seguridad y las tecnologías de detección de intrusos para la protección de redes y sistemas dentro de una organización.

Contenido:

- 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 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 Intrusión Detection System)
 - 2.2.4.3 NIDS (Network Intrusión 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 los IDS

3 Control de la seguridad informática

Objetivo: El alumno conocerá y comprenderá la utilidad de mantener el control sobre redes y dispositivos dentro de una organización a través de la realización de auditorías; así mismo aprenderá y conocerá los métodos y herramientas para el análisis forense en informática que le permitan comprender los mecanismos y técnicas que utilizan los intrusos para vulnerar los sistemas.

Contenido:

- 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 Monitores de Red
 - 3.1.5 Auditoría a Firewalls



- 3.1.6 Pruebas de Penetración sobre redes
- 3.1.7 Análisis de la 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 Configuración del Sistema
 - 3.2.9 Auditoría a la Capacidad de Recuperación ante Desastres
 - 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 Sistemas de Detección de Intrusos en la Seguridad Informática
 - 3.3.6.2 Tipos de Sistemas de Detección de Intrusos
 - 3.3.6.3 Nivel de Interacción de los Sistemas de Detección de Intrusos
- 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

Objetivo: El alumno conocerá y comprenderá los aspectos sociales y económicos en el campo de la seguridad informática.

Contenido:

- 4.1 Legislación Mexicana
 - 4.1.1 Acceso Ilícito a Sistemas
 - 4.1.1 Código Penal
 - 4.1.2 Derechos de Autor
 - 4.1.3 Actualidad de la legislación sobre delitos informáticos
- 4.2 Ley Modelo (CNUDMI)
- 4.3 Legislaciones Internacionales
 - 4.3.1 Legislación de Estados Unidos de América 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

Objetivo: El alumno conocerá las nuevas tendencias en ataques hacia sistemas y redes de cómputo, así como las nuevas tecnologías que puedan minimizar estas amenazas.

Contenido:

- 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

Bibliografía básica:

Temas de la asignatura para los que se recomienda

ANONYMOUS <i>Maximun Security</i> Fourth Edition USA Sams Publishing, 2003	Todos
BELLOVIN, Steven, CHESWICK, William, RUBIN, Aviel <i>Firewalls and Internet Security: Repelling the Wily Hacker</i> Second Edition USA Addison Wesley, 2003	Todos
GARFINKEL, Simson, SCHWARTZ, Alan, SPAFFORD, Gene <i>Practical UNIX & Internet Security</i> Third Edition USA O'Reilly, 2003	Todos
KING, Todd <i>Security + Training Guide</i> USA Que, 2003	Todos

LISKA, Allan

Todos

The Practice of Network Security: Deployment Strategies for Production Enviroments

USA

Prentice Hall, 2002

**Bibliografía complementaria:**

FINE, LEONARD H.

2

Seguridad en Centros de Cómputo, Políticas y Fundamentos

Segunda Edición

México

Trillas, 1997

KOZIOL, Jack

2

Intrusion Detection with Snort

USA

Que, 2003

PEIKARI Cyrus, FOGIE Seth

1, 3

Maximum Wireless Security

USA

Sams Publishing, 2002

PATIL, Basavaraj, SAIFULLAH, Yousuf, FACCIN, STEFANO, MONOMEN Risto

1, 3

IP in Wireless Networks

USA

Prentice Hall, 2003

SKOUDIS, ED; ZELTSER, Lenny

5

Malware Fighting Malicious Code

First Edition

USA

Prentice may, 2004

DRIMES Roger A.

5

Malicious Mobile Code

USA

O'Reilly, 2001



Sugerencias didácticas:

Exposición oral	X
Exposición audiovisual	X
Ejercicios dentro de clase	X
Ejercicios fuera del aula	X
Seminarios	X

Lecturas obligatorias	X
Trabajos de investigación	X
Prácticas de taller o laboratorio	X
Prácticas de campo	
Otras	

Forma de evaluar:

Exámenes parciales	X
Exámenes finales	X
Trabajos y tareas fuera del aula	X

Participación en clase	X
Asistencias a prácticas	X
Otras	

Perfil profesiográfico de quienes pueden impartir la asignatura

El profesor deberá contar con licenciatura, preferentemente maestría de las siguientes carreras; Ingeniería en computación, Ingeniería en Comunicaciones y Electrónica, Ingeniería en Telecomunicaciones, Ingeniería en Ciencias Computacionales o formación equivalente y contar con amplia experiencia en redes de computadoras, seguridad informática, desarrollo de proyectos y aplicaciones de la seguridad informática.