FACULTAD DE INGENIERÍA
ÁREA DE COMPUTACIÓN E INFORMÁTICA

Nombre de la materia: TELEMÁTICA B
Clave de la materia: 2831
Clave Facultad:
Clave U.A.S.L.P.: **Clave CACEI:** IA
Nivel del Plan de Estudios: II: 10 **No. de créditos:** 8
Horas/Clase/Semana: 3 **Horas totales/Semestre:** 80
Horas/Práctica (y/o Laboratorio): 2
Prácticas complementarias:
Trabajo extra-clase Horas/Semana: 3
Carrera/Tipo de materia: II: Optativa
No. de créditos aprobados:
Fecha última de Revisión Curricular: enero/2016
Materia y clave de la materia requisito: Telemática A (2830)

PROPÓSITO DEL CURSO

La información que manejan los sistemas de cómputo actuales representa un valor económico alto para sus organizaciones. Para limitar los daños que pudiera ocasionar a un sistema de cómputo un usuario malicioso, es necesario conocer las diferentes estrategias de seguridad que se deben seguir e implementar en la organización.

OBJETIVO DEL CURSO

Conocer las principales amenazas de seguridad que enfrentan actualmente los sistemas de información. Familiarizar al alumno con los mecanismos y estrategias a los que pueden recurrir las organizaciones para mantener la seguridad de sus sistemas informáticos.

CONTENIDO TEMÁTICO

1. Introducción

Tiempo estimado: 10 hrs.

Objetivo: Revisar los conceptos y elementos básicos de la seguridad informática.

1.1 Introducción a la seguridad informática.
1.2 Normas y estándares de seguridad: ISO/IEC 2700, COBIT, ITIL, SoGP
1.3 Implicaciones éticas y legales de la seguridad informática
1.4 Seguridad física y seguridad lógica

2. Criptografía

Tiempo estimado: 20 hrs.

Objetivo: Conocer los principios y técnicas de los métodos modernos de criptografía.

2.1 Elementos y funcionalidad de la criptografía
2.2 Métodos clásicos de criptografía
2.3 Criptografía de llave simétrica y ejemplo (DES)
2.4 Criptografía de llave asimétrica o pública y ejemplo (RSA)
2.5 Distribución de llaves
2.6 Métodos modernos de criptografía: curva elíptica

3. Protocolos de autentificación y resúmenes de mensaje

Tiempo estimado: 10 hrs.

Objetivo: Conocer protocolos de autentificación de mensajes y métodos de firma digital

3.1 Protocolos de autentificación
3.2 Firma digital
3.3 Resúmenes de mensaje y ejemplo (MD5)

4. Virus y programas maliciosos

Tiempo estimado: 10 hrs.

Objetivo: Conocer los diferentes tipos de virus y programas maliciosos que existen en la actualidad.

4.1 Virus informáticos
4.2 Programas maliciosos: gusano (worm), rootkit, zombie, caballo de Troya (Trojan horse), trap door, bomba lógica (logic bomb), stack and buffer overflow attack, keylogger, etc.
4.3 Ataques de seguridad en Internet: spam, phishing, pharming, etc.

5. Seguridad de los servidores

Tiempo estimado: 10 hrs.

Objetivo: Adquirir los conocimientos necesarios para mantener la integridad de un servidor.

5.1 Fases de los compromisos de seguridad de los servidores.
5.2 Claves de usuario (passwords)
5.3 Bitácora del sistema (log files)
5.4 Firewalls

6. Elementos administrativos de la seguridad informática

Tiempo estimado: 20 hrs.

Objetivo: Entender la metodología para implementar un programa de seguridad en una organización.

6.1 Estándares de seguridad para organizaciones
6.2 Análisis de un estándar de seguridad
6.3 Metodología para la implementación de un programa de seguridad

METODOLOGÍA

Exposición de temas por parte del profesor, problemas en clase para reforzar conceptos y prácticas de laboratorio para aplicar conceptos aprendidos en clase.

EVALUACIÓN

Los exámenes representan el 75% de la evaluación y las prácticas de laboratorio, el 25% restante. Se realizarán tres exámenes parciales en las fechas establecidas por la facultad y de acuerdo al Reglamento de Exámenes.

BIBLIOGRAFÍA

Bibliografía Básica:

R. Bejtlich. *El Tao de la Monitorización de Seguridad en Redes.* Prentice Hall, 2005.

W. Buchanan. *The Handbook of Data Communications and Networks*. 2a Ed. Springer, 2005.

J. F. Kurose y K. W. Ross. *Computer Networking: A Top-Down Approach.* 6a Ed. Addison-Wesley, 2013.

W. Stallings. *Cryptography and Network Security: Principles and Practice.* 5a Ed. Prentice Hall, 2011.

SecTools.Org: Top Network Security Tools
http://sectools.org/
(Consultado enero/2016)

Bibliografía Complementaria:

A. Leon-Garcia y I. Widjaja. *Redes de Comunicación: Conceptos Fundamentales y Arquitecturas Básicas.* McGraw-Hill, 2002.

C. Negus y E. Foster-Johnson. *Fedora 11 and Red Hat Enterprise Linux Bible*. Wiley, 2009.

W. Stalllings. *Sistemas Operativos: Aspectos Internos y Principios de Diseño*. 5a. Ed. Prentice Hall, 2005.