Casa abierta al tiempo
UNIVERSIDAD AUTONOMA METROPOLITANA

PROGRAMA DE ESTUDIOS

UNIDAD	DIVISION	1 / 3
NOMBRE DEL PLAN **LICENCIATURA EN TECNOLOGIAS Y SISTEMAS DE INFORMACION**		
CLAVE	UNIDAD DE ENSEÑANZA-APRENDIZAJE	CRED. 8
450210	**SEMINARIO DE SEGURIDAD**	TIPO **OBL.**
H.TEOR. **3.0**		TRIM.
H.PRAC. **2.0**	SERIACION **460020**	**VI AL XII**

OBJETIVO(S):

Objetivo General:

Que al final del curso el alumno sea capaz de:

Manejar los diferentes mecanismos y alternativas de servicios de seguridad que ofrecen los sistemas informáticos y las distintas redes de comunicaciones, en especial en Internet.

Objetivos Específicos:

Que al final del curso el alumno sea capaz de:

1. Entender e identificar los principios básicos de la seguridad computacional.
2. Conocer las diferentes técnicas criptográficas y mecanismos de identificación y control que las utilizan.
3. Identificar los principales problemas de seguridad en los sistemas operativos y bases de datos.
4. Aplicar los estándares de seguridad actuales para diseñar y construir aplicaciones seguras.

CONTENIDO SINTETICO:

1. Principios básicos de la seguridad computacional.
2. Introducción a la criptografía.
3. Autentificación, gestión de claves y control de acceso.
4. Seguridad en Internet.
5. Seguridad de bases de datos y sistemas operativos.

6. Seguridad en redes inalámbricas.
7. Intranets y firewalls.
8. Perspectivas en la seguridad computacional.

MODALIDADES DE CONDUCCION DEL PROCESO ENSEÑANZA-APRENDIZAJE:

Exposiciones temáticas por parte del profesor.

- Discusión grupal.
- Prácticas activas por parte del alumno.
- Reportes de trabajos.
- Proyecto final.

MODALIDADES DE EVALUACION:

Evaluación Global.

Se ponderarán las siguientes actividades a criterio del profesor:

- Reportes escritos de los trabajos realizados.
- Tareas individuales.
- Evaluaciones periódicas.
- Participación tanto en las sesiones teóricas como prácticas.
- Evaluación terminal.
- Evaluación del proyecto final.

Evaluación de Recuperación:

- El alumno deberá presentar una evaluación que contemple todos los contenidos de la UEA.
- No requiere inscripción previa a la UEA.

BIBLIOGRAFIA NECESARIA O RECOMENDABLE:

1. Bishop M., (2003), Computer Security - Art and Science, Addison Wesley.

2. Bragg R., Rhodes-Ousley M., Strassberg K., (2004), Network Security, The Complete Reference, McGraw Hill, New York.

3. Cheswick W. R., Bellovin S. M., Rubin A. D., (2003), Firewalls and Internet Security, Repelling the Wily Hacker, 2nd edition, Addison Wesley,

Reading.

4. Günter S., (2003), Security in Fixed and Wireless Networks, John Wiley & Sons.

5. Maiwald E., (2003), Fundamentals of Network Security, Mc Graw Hill, New York.

6. Oppliger R., (2001), Internet and Intranet security, 2nd edition, Artech House.

7. Ribagorda M., Sancho J., (1994), Seguridad y protección de la información, Centro de Estudios Ramón Areces.

8. Stallings W., (1999), Cryptography and network security principles and practice, 2nd edition, Prentice Hall.

9. Stallings W., (2003), Fundamentos de Seguridad en Redes, Aplicaciones y Estándares, 2a edición, Prentice Hall.

UNIVERSIDAD AUTÓNOMA METROPOLITANA

Casa abierta al tiempo

APROBADO POR EL COLEGIO ACADEMICO
EN SU SESION NUM. 219

EL SECRETARIO DEL COLEGIO