



Casa abierta al tiempo

UNIVERSIDAD AUTONOMA METROPOLITANA

PROGRAMA DE ESTUDIOS

UNIDAD	CUAJIMALPA	DIVISION	CIENCIAS NATURALES E INGENIERIA	1 / 3
NOMBRE DEL PLAN LICENCIATURA EN INGENIERIA EN COMPUTACION				
CLAVE	UNIDAD DE ENSEÑANZA-APRENDIZAJE	CRED.	8	
460040	SEGURIDAD	TIPO	OPT.	
H.TEOR. 3.0	SERIACION AUTORIZACION	TRIM.	VII al X	
H.PRAC. 2.0				

**OBJETIVO(S) :**

Objetivos Generales:

Que al final del curso el alumno sea capaz de:

1. Conocer el concepto general de seguridad informática.
2. Conocer los principales tipos de intrusos informáticos que existen, a partir de sus características psicológicas y sociológicas.
3. Comprender la mecánica de los principales tipos de ataque informático que existen.
4. Desarrollar planes de seguridad informática para una organización, incluyendo detección, corrección y prevención.

**CONTENIDO SINTETICO:**

1. Concepto de seguridad en informática:
  - Ataques informáticos.
  - Amenazas informáticas.
  - Temores.
2. El mundo de los intrusos informáticos (underground):
  - Tipos de intrusos.
  - Organización social del underground informático.
3. Tipos y técnicas de ataque informático:
  - Ingeniería social.
  - Ingeniería social inversa.
  - Trashing.
  - Ataques por monitoreo (monitorización).
  - Ataques de autenticación.



Casa abierta al tiempo

UNIVERSIDAD AUTONOMA METROPOLITANA

APROBADO POR EL COLEGIO ACADEMICO  
EN SU SESION NUM. 294

EL SECRETARIO DEL COLEGIO

CLAVE 460040

SEGURIDAD

- Ataques por Denegación de Servicio (DoS).
- Ataques de modificación-daño.

## 4. Virus, Troyanos y Gusanos:

- Definición.
- Principales tareas.
- Técnicas de construcción.
- Técnicas de detección y eliminación.

## 5. Piratería de software:

- Razones para el pirateo de software.
- Técnicas de protección contra copias.
- Ingeniería inversa y decompilación.

## 6. Seguridad en el comercio electrónico:

- Identificación digital.
- Criptografía.

## 7. Planes preventivos y correctivos:

- Creación de un CERT (Computer Emergency Response Team).
- Colaboración local, nacional e internacional.

**MODALIDADES DE CONDUCCION DEL PROCESO ENSEÑANZA-APRENDIZAJE:**

Clases teóricas a cargo del profesor con participación activa del alumno.

Clase teórica en aula.

- Exposiciones temáticas por parte del profesor con discusiones grupales con nivel de complejidad incremental y reportes de trabajos.
- Clase práctica en laboratorio.
- Diseño de experiencias de aprendizaje por problemas en donde el profesor conduce el proceso y los alumnos participan activamente poniendo en práctica las técnicas explicadas, tanto para salvaguardar la seguridad de una máquina o red como para tratar de romperla. Desarrollo de proyectos consistentes en la puesta en práctica de las técnicas de ataque/defensa vistas en clase.

Se recomiendan reuniones periódicas durante el trimestre, de los profesores y ayudantes de los diversos grupos de este curso y profesores que hayan impartido el curso con anterioridad, con el fin de discutir el desarrollo del curso, evaluando y mejorando el proceso de conducción del aprendizaje, concebir los ejemplos y ejercicios presentados, así como elaborar las tareas



Casa abierta al tiempo

UNIVERSIDAD AUTONOMA METROPOLITANA

APROBADO POR EL COLEGIO ACADEMICO  
EN SU SESION NUM. 274

EL SECRETARIO DEL COLEGIO

CLAVE 460040

SEGURIDAD

y notas de clase, las evaluaciones periódicas y la evaluación terminal.

**MODALIDADES DE EVALUACION:****Evaluación Global:**

Se ponderarán las siguientes actividades a criterio del profesor:

- Presentación de los avances de los proyectos, consistentes en la puesta en práctica de las técnicas de ataque/defensa vistas en clase.
- Análisis post-mortem de las técnicas puestas en práctica, fortalezas y debilidades.
- Evaluación terminal.

**Evaluación de Recuperación:**

- El alumno deberá presentar una evaluación crítica que contemple todos los contenidos de la unidad de enseñanza-aprendizaje.

**BIBLIOGRAFIA NECESARIA O RECOMENDABLE:**

1. Center for Information System Security, Department of Defense (DoD), Goal Security Architecture (DGSA); Documento electrónico disponible en Internet.
2. Cheswick Bill, An evening with berferd in which a cracker is lured, endured, and studied, Documento electrónico disponible en Internet.
3. Cobb Stephen, Manual de seguridad para PC y redes locales, McGraw-Hill, España, 1994.
4. Fahn Paul, Steven M. Bellovin y Michael Merritt, FAQ about today's cryptography, Documento electrónico disponible en Internet.
5. Garfinkel Simson y Gene Spafford, Seguridad y comercio en el Web. McGraw-Hill y O'Reilly, México, 1999.
6. Meyer Gordon, R. The social organization of the computer underground, Tesis de Maestria, Northern Illinois University, Documento electrónico disponible en Internet.



Casa abierta al tiempo

UNIVERSIDAD AUTONOMA METROPOLITANA

APROBADO POR EL COLEGIO ACADEMICO  
EN SU SESIÓN NUM. 2076

EL SECRETARIO DEL COLEGIO