UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE ESTUDIOS SUPERIORES ACATLÁN

ACATLÁN

LICENCIATURA EN MATEMÁTICAS APLICADAS Y COMPUTACIÓN

PROGRAMA DE ASIGNATURA

CLAVE: 1070					SEMESTRE: 9 (NOVENO)
SEGURIDAD COMPUTACIONAL					
LÍNEA DE FORMACIÓN	**CIENCIAS DE LA COMPUTACIÓN**				
MODALIDAD (CURSO, TALLER, LABORATORIO, ETC.)	CARACTER	HORAS SEMESTRE	HORA / SEMANA TEÓRICA	PRÁCTICA	CRÉDITOS
CURSO	**OPTATIVO**	**64**	**4**	**0**	**8 (OCHO)**
ASIGNATURA PRECEDENTE	**NINGUNA**				
ASIGNATURA CONSECUENTE	**NINGUNA**				

OBJETIVO:
EL ALUMNO IDENTIFICARÁ LOS ELEMENTOS DE RIESGO EN LA INFORMÁTICA ACTUAL Y APRENDERÁ TÉCNICAS DE PREVENCIÓN Y CORRECCIÓN DE INCIDENTES INFORMÁTICOS.

Número de horas	***Unidad 1.*** **NOCIONES Y ELEMENTOS BÁSICOS**
4	*Objetivo: El alumno conocerá la definición de seguridad, su historia, las organizaciones que la estudian y la normatividad internacional y nacional relacionada.* Temas: 1.1 Definición de seguridad. 1.2 Historia. 1.3 Organizaciones nacionales e internacionales. 1.4 Normas nacionales e internacionales acerca de la seguridad: rainbow books, normas CERT, acta de seguridad y reglas del negocio de la empresa.

Número de horas	*Unidad 2.* **IDENTIFICACIÓN DE RIESGOS**
10	*Objetivo: El alumno identificará los recursos que requieren ser protegidos, el conjunto de amenazas informáticas y los elementos a calcular el costo de dar seguridad.* Temas: 2.1 Identificación de recursos: computacionales, humanos y económicos. 2.2 Identificación de riesgos. 2.3 Análisis costo–beneficio desde el punto de vista: operacional, económico, técnico y humano. 2.4 Concepto de amenaza. 2.5 Amenazas no intencionadas: catástrofes naturales, errores (bugs) y omisiones en el software, software no soportado o caduco (abandonedware), permisos ampliados y pérdida de equipo físico. 2.6 Amenazas intencionadas: suplantación de identidad, fraude, robo, sabotaje interno y externo de la organización, espionaje industrial y gubernamental, ciberterrorismo, malware, backdoors, spyware, hackers y crackers.

Número de horas	*Unidad 3.* **ATAQUES Y CRIPTOGRAFÍA**
14	*Objetivo: El alumno analizará el concepto y los tipos de ataques computacionales más comunes así como las causas que los permiten y conocerá los algoritmos de encriptación y certificados digitales.* Temas: 3.1 Nociones: ataques, scripts de ataque (exploits), colectado de información, ingeniería social y recolección de basura(dumpster diving). 3.2 Ataques más comunes: memory overflow, buffer overflood, bombas lógicas, passwords crackers, sniffers, spoofing, TCP/IP scanners, hijacking, virus, gusanos, caballos de troya, scripts web hostiles, SQL injection, spam, flooding, mail relay y DOS (denial of Service). 3.3 Criptografía: conceptos, cifrado de sustitución y de transposición, one-time pads y esteganografía. 3.4 Algoritmos de llave simétrica: DES, AES y criptoanálisis. 3.5 Algoritmos de llave asimétrica: RSA. 3.6 Firmas digitales: con llave privada y pública 3.7 PKI: certificados, autoridades de certificación y X.509.

Número de horas	*Unidad 4.* **AUTENTIFICACIÓN DE USUARIOS Y SEGURIDAD EN INTERNET**
10	*Objetivo: El alumno conocerá los procedimientos de identificación y autenticación de usuarios así como el hardware y software utilizado para controlar y proteger el tráfico a Internet* Temas: 5.1 El username o login. 5.2 Passwords: sistema, contraseña/reto y PAM. 5.3 Tarjetas: código de barras, VPN y smartcard. 5.4 Biometría. 5.5 Tokens. 5.6 Proxy. 5.7 Firewall. 5.8 VPN. 5.9 IP tunneling. 5.10 WEP.

Número de horas	*Unidad 5.* **ANTIVIRUS Y RESPALDOS**
8	*Objetivo: El alumno conocerá el hardware y software utilizado para controlar y proteger de virus al trafico de red así como el hardware y software utilizado para generar respaldos.* Temas: 5.1 Conceptos de antivirus. 5.2 Nodos. 5.3 SMTP. 5.4 Trafico PTT. 5.5 Tareas administrativas: definiciones de virus y actualizaciones de software. 5.6 Conceptos de respaldos: rotación de medios. 5.7 RAID. 5.8 NAS. 5.9 SAN. 5.10 Software.

Número de horas	*Unidad 6.* **PRUEBA, VALIDACIÓN, BASE DE DATOS Y SERVICIOS DE INTERNET**
18	*Objetivo: El alumno aprenderá los conceptos de programación segura, de seguridad para base de datos así como los tópicos de seguridad de los servicios más utilizados en internet.* Temas: 6.1 Bugs. 6.2 Validación y verificación.

6.3 Seguridad del software.
6.4 Disponibilidad en BD.
6.5 RAID en BD: OLTP y dataware house.
6.6 Arquitectura multicapa.
6.7 Técnicas de respaldo.
6.8 Técnicas de recuperación.
6.9 Usuarios, roles y profiles.
6.10 FTP.
6.11 HTTP.
6.12 DNS.
6.13. SMB.
6.14 SMTP, POP, IMAP

BIBLIOGRAFÍA BÁSICA

Barrett y Silverman, *SSH, The secure shell: the definitive guide*, O'Reilly, E.U.A., 2001

Garfinkel y Spafford, *Practical UNIX & internet security*, O'Reilly, Alemania, 2003

Kurose y Keith, *Computer networking: a top-down approach featuring the internet*, Addison Wesley, E.U.A.,2003

Menezes et al., *Handbook of applied criptography*, CRC Press, E.U.A., 1997

National Institute of Standars and Technology, *An introduction to computer security*, Special Publication 800-12, US Department of Commerce, E.U.A., 2000

Radcom, *Guía completa de protocolos de telecomunicaciones*, McGraw Hil, México, 2003

Randall y Panos, *Seguridad para comunicaciones inalámbricas*, México, McGraw Hill, 2003

Scambray et al., *Secretos y soluciones para la seguridad de redes*, McGraw Hill, España, 2001

Tanenbaum, A., *Computer networks*, Pearson Education, E.U.A., 2003

Theriault y William, *Oracle security*, McGraw Hill, E.U.A., 2001

Zwicky et al., *Building internet firewall*, O'Reilly, E.U.A., 2000

BIBLIOGRAFÍA COMPLEMENTARIA

Anónimo, *Maximum security: A hackers Guide to protecting your internet site and network*, E.U.A., 2001

McClure, et al., *Hacking Exponed: Network Security Secrets & Solutions*, McGraw Hill, E.U.A., 2003

Scambray, J., *Hackers de sitios Web*, McGraw Hill, España, 2003

Sterling, B., *The hacker crackdown: law and disorder on the electronic frontier*, Bantam Books, E.U.A., 1995

SUGERENCIAS DIDÁCTICAS

- Introducir y exponer los temas y contenidos de las diferentes unidades, con ejemplos claros y sencillos.
- Propiciar la participación de los alumnos a través del empleo de diferentes técnicas de trabajo en grupo.
- Desarrollar programas mediante el uso de paquetes computacionales aplicando los métodos estudiados en el curso.
- Fomentar en los alumnos la investigación relacionada con la materia, así como tratar temas relevantes que se encuentren en revistas especializadas o en diversas fuentes bibliográficas.

SUGERENCIAS DE EVALUACIÓN

- Exámenes parciales
- Examen final
- Participación en clase
- Investigaciones
- Proyecto final

PERFIL PROFESIOGRÁFICO QUE SE SUGIERE

El profesor que impartirá el curso deberá tener el título de licenciado en Matemáticas Aplicadas y Computación, Ingeniero en Computación o carreras afines.