UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE ESTUDIOS SUPERIORES ACATLÁN

PLAN DE ESTUDIOS DE LA LICENCIATURA EN MATEMÁTICAS APLICADAS Y COMPUTACIÓN

PROGRAMA DE ASIGNATURA

SEMESTRE: 8(OCTAVO)

SEGURIDAD COMPUTACIONAL

CLAVE:

MODALIDAD	CARÁCTER	TIPO	HORAS AL SEMESTRE	HORAS SEMANA	HORAS TEÓRICAS	HORAS PRÁCTICAS	CRÉDITOS
Curso	Optativa	Teórica	64	4	4	0	8

CICLO DE FORMACIÓN	Optativa
CAMPO DE CONOCIMIENTO	Sistemas Computacionales

SERIACIÓN	Indicativa
ASIGNATURA(S) ANTECEDENTE	Desarrollo Web
ASIGNATURA(S) SUBSECUENTE(S)	Ninguna

Objetivo general: El alumno identificará los elementos de riesgo en la informática actual, así como las técnicas de prevención y corrección de incidentes informáticos.

Índice Temático		Horas	
Unidad	**Tema**	**Teóricas**	**Prácticas**
1	Introducción a la seguridad computacional	4	0
2	Análisis de riesgos tecnológicos	16	0
3	Criptografía	10	0
4	Seguridad de red	14	0
5	Seguridad a nivel sistema operativo y de aplicación	10	0
6	Seguridad en la Web	10	0
	Total de horas:	64	0
	Suma total de horas:	64	

HORAS		UNIDAD	CONTENIDO
T	P		
4	0	1	**INTRODUCCIÓN A LA SEGURIDAD COMPUTACIONAL** **Objetivo:** El alumno describirá los conceptos de seguridad, los recursos que requieren ser protegidos, y la normatividad internacional y nacional relacionada. **Temas:** 1.1 Conceptos básicos 1.1.1 Políticas y modelos de seguridad 1.1.2 Tríada de Seguridad: Confidencialidad, Integridad y Disponibilidad 1.1.3 Análisis de riesgo 1.2 Seguridad en una organización. 1.2.1 Seguridad física 1.2.2 Seguridad lógica 1.2.3 Amenazas intencionadas y no intencionadas 1.2.4 Ingeniería Social 1.3 Normas nacionales e internacionales acerca de la seguridad: rainbow books, normas CERT, acta de seguridad. 1.3.1 Norma ISO 27001 1.3.2 Norma ISO 17799 1.3.3 ISACA 1.3.4 BS7799-3
16	0	2	**ANÁLISIS DE RIESGOS TECNOLÓGICOS** **Objetivo:** El alumno analizará los principales factores para evaluación de riesgos de Tecnología y Sistemas **Temas:** 2.1. Clasificación de Información 2.1.1. Protección de activos de la empresa 2.2. Identificación de riesgos 2.4.1. Vulnerabilidad 2.4.2. Amenaza 2.4.3. Impacto 2.4.4. Riesgo 2.3. Controles 2.3.1. Control compensatorio 2.3.2. Riesgo inherente y riesgo residual 2.3.3. Validación de controles 2.4. Principios de auditoría informática 2.4.1. Auditoría 2.4.2. Auditoría forense 2.5. Planes de recuperación

10	0	3	**CRIPTOGRAFÍA** **Objetivo particular:** El alumno explicará los conceptos y algoritmos de encriptación, así como de certificados digitales. **Temas:** 3.1 Criptología 3.1.1 Esteganografía 3.1.2 Criptografía 3.1.3 Criptoanálisis 3.2 Algoritmos de llave simétrica: DES, AES y criptoanálisis. 3.3 Algoritmos de llave asimétrica: RSA. 3.4 Firmas digitales 3.5 PKI: certificados, autoridades de certificación y X.509 3.6 Estándares PKCS
14	0	4	**SEGURIDAD DE RED** **Objetivo Particular:** El alumno aplicará los procedimientos en el control y protección del tráfico hacia y desde la Internet, así como el hardware y software utilizado. **Temas:** 4.1 Sistemas de protección perimetral (Firewall) 4.2 Sistema de detección de intrusos (IDS) 4.3 Sistemas de protección de intrusos (IPS) 4.4 Protocolo Simple de Administración de Red (SNMP) 4.5 Seguridad en redes inalámbricas 4.5.1 WEP 4.5.2 WAP 4.5.3 WPA2 4.6 Analizadores de red
10	0	5	**SEGURIDAD A NIVEL SISTEMA OPERATIVO Y DE APLICACIÓN** **Objetivo Particular:** El alumno aplicará los conceptos para el aseguramiento de un sistema reduciendo los niveles de vulnerabilidad de un sistema computacional. **Temas:** 5.1 Autentificación 5.1.1 El username o login 5.1.2 Password: sistema, contraseña/reto y PAM 5.1.3 Tarjetas: código de barras, VPN y smartcard 5.1.4 Biometría 5.1.5 Tokens 5.2 Hardening del Sistema Operativo 5.2.1 Directivas de seguridad (Active directory, SE LINUX, UAC, LDAP) 5.2.2 Bugs en las aplicaciones 5.2.2.1 Buffer overflow (stack guard)

			5.2.2.2 Memory overflow (stack guard) 5.3 Seguridad en Base de Datos 5.3.1 Modelo de control de acceso (sistema R) 5.3.2 Roles y permisionamiento (Grant, Revoke) 5.3.3 Vistas y control de acceso basado en contenido 5.3.4 Disparadores
10	0	6	**SEGURIDAD EN LA WEB** **Objetivo:** El alumno aplicará los conceptos de programación segura en las aplicaciones utilizadas en Internet **Temas:** 6.1 Manejo de confianza (Validación y verificación) 6.2 Inyección de SQL 6.3 Cross Site Scripting (XSS) 6.4 Metodología SDL (Microsoft) 6.5 Seguridad en la Nube 6.6 Organizaciones de seguridad 6.6.1 OWASP 6.6.2 CGI Security 6.6.3 WEB Aplication Security Consortium 6.6.4 Common Weakness Enumeration (no sólo Web) 6.7 Firewall de aplicación 6.7.1 Mod security 6.7.2 Paros Proxy

Referencias básicas:

- Andrews, Mike and. Whittaker, James A (2006). *How to Break Web Software: Functional and Security Testing of Web Applications and Web Services*. USA: Pearson Education Inc.
- Barrett y Silverman,(2001). SSH, *The secure shell: the definitive guide*. E.U.A.: O'Reilly.
- Fernández Hanse, Yago, Ramos Varón, Antonio, García Jean Paul (2009). *A A/Radius/802.1x Sistemas basados en la autenticación en Windows y Linux/GNA*. Alfaomega Ra -Ma
- Garfinkel y Spafford (2003). Practical UNIX & internet security, O'Reilly, Alemania,
- Hoglund, Greg and McGraw, Gary (2004). Exploiting Software: How to Break Code USA: Pearson Education Inc.
- Howwlett, Tony. (2005). Software Libre Herramientas de seguridad. Madrid: Anaya-multimedia.
- Kurose y Keith. (2003). Computer networking: a top-down approach featuring the internet, E.U.A.: Addison Wesley.
- National Institute of Standars and Technology, (2000). An introduction to computer security, Special Publication 800-12, E.U.A.: US Department of Commerce.
- Randall y Panos, (2003). Seguridad para comunicaciones inalámbricas, México, McGraw Hill,
- Scambray et al. (2001). Secretos y soluciones para la seguridad de redes, España: McGraw Hill.
- Theriault y William, (2001). Oracle security, E.U.A.: McGraw Hill.
- Vacca, John R. (2010).Network and System Security. USA: Syngress
- Zwicky et al.(2000), Building internet firewall, E.U.A.: O'Reilly.

Referencias complementarias:

- Anónimo, (2001) Maximum security: A hackers Guide to protecting your internet site and Network. E.U.A.
- McClure, et al. (2003). Hacking Exponed: Network Security Secrets & Solutions. E.U.A.: McGraw Hill.
- Scambray, J. (2003). Hackers de sitios Web. España: McGraw Hill.
- Sterling, B. (1995). The hacker crackdown: law and disorder on the electronic frontier, E.U.A.: Bantam Books.

Sugerencias didácticas:	**Sugerencias de evaluación del aprendizaje:**
Clase magistral Ejercicios dentro y fuera de clase Estudio de caso Exposición audiovisual Exposición oral Interrogatorio Técnicas grupales Trabajo colaborativo Trabajo de investigación Visitas de observación Uso de recursos didácticos en línea	Examen final oral o escrito Exámenes parciales Informes de prácticas Informes de investigación Participación en clase Rúbricas Solución de ejercicios Trabajos y tareas En el sistema presencial es obligatoria la asistencia mínima al 80% de clases.

Perfil Profesiográfico: El profesor que imparta la asignatura deberá tener el título de licenciado en Matemáticas Aplicadas y Computación o carrera afín, con experiencia profesional y docente en la materia, contar con actualización en el área y preferentemente tener estudios de posgrado.