UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE INGENIERÍA

PROGRAMA DE ESTUDIO

SEGURIDAD INFORMÁTICA I	0880	8°, 9°	06
Asignatura	Clave	Semestre	Créditos

Ingeniería Eléctrica	Ingeniería en Computación	Ingeniería en Computación
División	Departamento	Carrera en que se imparte

Asignatura:		Horas:		Total (horas):	
Obligatoria de elección	X	Teóricas	3.0	Semana	3.0
Optativa		Prácticas	0.0	16 Semanas	48.0

Aprobado: Consejo Técnico de la Facultad — Fecha: 25 de febrero, 17 de marzo y 16 de junio de 2005
Consejo Académico del Área de las Ciencias Físico Matemáticas y de las Ingenierías — 11 de agosto de 2005

Modalidad: Curso.

Asignatura obligatoria antecedente: Ninguna.

Asignatura obligatoria consecuente: Ninguna.

Objetivo(s) del curso:
El alumno comprenderá y aplicará los métodos y elementos que le permitan planificar el desarrollo de una arquitectura de seguridad, con base en la identificación y análisis de amenazas, ataques y vulnerabilidades en los sistemas y redes de cómputo, enmarcados en una base ética.

Temario

NÚM.	NOMBRE	HORAS
1.	Fundamentos teóricos	9.0
2.	Amenazas y vulnerabilidades	7.5
3.	Identificación de ataques y técnicas de intrusión	10.5
4.	Políticas de seguridad informática de la organización	7.5
5.	Análisis del riesgo	7.5
6.	Ética informática	6.0
		48.0
	Prácticas de laboratorio	0.0
	Total	48.0

1 Fundamentos teóricos

Objetivo: El alumno conocerá los conceptos, objetivos y antecedentes históricos de la Seguridad informática, así como el de los modelos de seguridad que le permitan adoptar los Estándares destinados a planificar un esquema de seguridad en una organización.

Contenido:

- **1.1** Introducción
  - **1.1.1** Concepto de la Seguridad Informática
  - **1.1.2** Evolución histórica de la Seguridad Informática
  - **1.1.3** Objetivos y misión de la Seguridad Informática
  - **1.1.4** Amenazas a las redes y sistemas computacionales
- **1.2** Normatividad de la Seguridad Informática
  - **1.2.1** Normas de Seguridad a través de la Historia
    - **1.2.1.1** TCSEC / Libro Naranja
    - **1.2.1.2** ITSEC
    - **1.2.1.3** CTCPEC
    - **1.2.1.4** FC-ITS
  - **1.2.2** Criterios Comunes / ISO 15408
  - **1.2.3** ISO 17799
  - **1.2.4** Nuevas Tendencias
    - **1.2.4.1** OCTAVE
- **1.3** Esquema de Seguridad basado en Criterios Comunes: Perfiles de Protección
  - **1.3.1** Definición y propósito
  - **1.3.2** Estructura
    - **1.3.2.1** Introducción
    - **1.3.2.2** Descripción del objeto de evaluación
    - **1.3.2.3** Entorno de seguridad
    - **1.3.2.4** Hipótesis
    - **1.3.2.5** Amenazas
    - **1.3.2.6** Políticas de la organización
    - **1.3.2.7** Nivel de Garantía general requerido
    - **1.3.2.8** Objetivos de Seguridad
    - **1.3.2.9** Requerimientos Funcionales y de Garantía
    - **1.3.2.10** Justificación
- **1.4** Servicios de Seguridad
  - **1.4.1** Confidencialidad
  - **1.4.2** Autenticación
  - **1.4.3** Integridad
  - **1.4.4** No repudio
  - **1.4.5** Control de Acceso
  - **1.4.6** Disponibilidad

2 Amenazas y vulnerabilidades

Objetivo: El alumno conocerá, identificará y explicará los diferentes tipos de amenazas y vulnerabilidades así como las fuentes que las ocasionan.

Contenido:

- **2.1** Amenazas
  - **2.1.1** Definición
  - **2.1.2** Fuentes de amenaza
    - **2.1.2.1** Factor humano
      - **2.1.2.1.1** Tipos: ingeniería social, robo, fraude, sabotaje, personal enterado, terroristas, curiosos, intrusos remunerados, etc.
      - **2.1.2.1.2** Hardware
      - **2.1.2.1.3** Tipos: mal diseño, errores de fabricación, suministro de energía, etc.
    - **2.1.2.2** Red de datos
      - **2.1.2.2.1** Tipos: topología seleccionada, sistema operativo, sistema de administración, monitoreo, etc.
    - **2.1.2.3** Software
      - **2.1.2.3.1** Tipos: software de desarrollo, software de aplicación, código malicioso, virus, etc.
    - **2.1.2.4** Desastres naturales
      - **2.1.2.4.1** Tipos: inundaciones, terremotos, fuego, viento, tormentas eléctricas, etc.
- **2.2** Vulnerabilidades
  - **2.2.1** Definición
  - **2.2.2** Tipos de Vulnerabilidades
    - **2.2.2.1** Física
    - **2.2.2.2** Natural
    - **2.2.2.3** Hardware
    - **2.2.2.4** Software
    - **2.2.2.5** Red

3 Identificación de ataques y técnicas de intrusión

Objetivo: El alumno conocerá, identificará y explicará los métodos y técnicas de ataque e intrusión a redes y sistemas; a su vez conocerá los mecanismos y herramientas para evitarlos.

Contenido:

- **3.1** Reconocimiento y Obtención de Información
  - **3.1.1** Bases de Datos Públicas
  - **3.1.2** WEB
  - **3.1.3** DNS
  - **3.1.4** Keyloggers
  - **3.1.5** Ingeniería Social
  - **3.1.6** Otros
- **3.2** Identificación de Vulnerabilidades
  - **3.2.1** Ataques a Redes Telefónicas
  - **3.2.2** Ataques a la Telefonía Inalámbrica
  - **3.2.3** Barrido de Puertos

- **3.2.4** Identificación de Firewalls
  - **3.2.4.1** Interpretación de reglas y filtros
- **3.2.5** Identificación de Sistemas Operativos / Fingerprinting
  - **3.2.5.1** Métodos de Identificación
- **3.2.6** Escaneo a Redes Inalámbricas
- **3.2.7** Instalaciones Físicas
- **3.2.8** Configuración de Servicios y Servidores
- **3.2.9** Software
- **3.2.10** Otros

3.3 Explotación y obtención de acceso a Sistemas y Redes
- **3.3.1** Promiscuidad en Redes
- **3.3.2** Robo de Identidad
- **3.3.3** Engaño a Firewalls y Detectores de Intrusos
- **3.3.4** Vulnerabilidades en el Software
  - **3.3.4.1** Buffer Overflows
  - **3.3.4.2** Heap Overflows
  - **3.3.4.3** Formato de Cadena
  - **3.3.4.4** Race Conditions
  - **3.3.4.5** SQL Injection
  - **3.3.4.6** Cross-Site & Cross-Domain Scripting
  - **3.3.4.7** Virus y Gusanos
  - **3.3.4.8** Otros
- **3.3.5** Ataques a Contraseñas
- **3.3.6** Debilidad de los Protocolos de Red
- **3.3.7** Ataques a Servicios
- **3.3.8** Negación de Servicio
- **3.3.9** Ataques a Redes Inalámbricas
  - **3.3.9.1** Denegación de Servicio
  - **3.3.9.2** Ataque de Hombre en Medio
  - **3.3.9.3** ARP Poisoning
  - **3.3.9.4** WEP key-cracking
  - **3.3.9.5** Nuevos Métodos de Ataque en Redes Inalámbricas

3.4 Mantener el Acceso a Sistemas Comprometidos
- **3.4.1** Puertas Traseras
- **3.4.2** Caballos de Troya
- **3.4.3** Rootkits
- **3.4.4** Otros

3.5 Eliminación de Evidencias
- **3.5.1** Edición de bitácoras
- **3.5.2** Ocultar Información
- **3.5.3** Estenografía
- **3.5.4** Nuevos métodos

4 Políticas de seguridad informática de la organización

Objetivo: El alumno entenderá, explicará, valorará y adquirirá la capacidad para desarrollar políticas de seguridad informática así como los procedimientos y planes de contingencia que le permitan mantener el control de la seguridad en una organización.

Contenido:

- **4.1** Políticas de Seguridad Informática
  - **4.1.1** Objetivo de una política de seguridad
  - **4.1.2** Misión, visión y objetivos de la organización
  - **4.1.3** Principios fundamentales de las políticas de seguridad
    - **4.1.3.1** Responsabilidad individual
    - **4.1.3.2** Autorización
    - **4.1.3.3** Mínimo privilegio
    - **4.1.3.4** Separación de obligaciones
    - **4.1.3.5** Auditoría
    - **4.1.3.6** Redundancia
  - **4.1.4** Políticas para la confidencialidad
  - **4.1.5** Políticas para la integridad
  - **4.1.6** Modelos de Seguridad: abstracto, concreto, de control de acceso y de flujo de información
  - **4.1.7** Desarrollo de políticas orientadas a servicios de seguridad
  - **4.1.8** Publicación y Difusión de las Políticas de Seguridad
- **4.2** Procedimientos y Planes de Contingencia
  - **4.2.1** Procedimientos Preventivos
  - **4.2.2** Procedimientos Correctivos
  - **4.2.3** Planes de Contingencia
    - **4.2.3.1** Objetivos y Características de un Plan de Contingencias
    - **4.2.3.2** Fases del Plan de Contingencia
      - **4.2.3.2.1** Análisis y Diseño
      - **4.2.3.2.2** Desarrollo de un plan de contingencias
      - **4.2.3.2.3** Pruebas y Mantenimiento

5 Análisis del riesgo

Objetivo: El alumno conocerá, identificará, seleccionará y aplicará las técnicas y métodos que le permitan llevar a cabo actividades concernientes a la evaluación de riesgos dentro de una organización.

Contenido:

- **5.1** Terminología básica
  - **5.1.1** Activos
  - **5.1.2** Riesgo
  - **5.1.3** Aceptación
  - **5.1.4** Análisis del riesgo
  - **5.1.5** Manejo del riesgo
  - **5.1.6** Evaluación
  - **5.1.7** Impacto
  - **5.1.8** Pérdida esperada

- **5.1.9** Vulnerabilidad
- **5.1.10** Amenaza
- **5.1.11** Riesgo residual
- **5.1.12** Controles

5.2 Análisis cuantitativo
5.3 Análisis cualitativo
5.4 Pasos del análisis de riesgo

- **5.4.1** Identificación y evaluación de los activos
- **5.4.2** Identificación de amenazas
- **5.4.3** Identificación de vulnerabilidades
- **5.4.4** Impacto de la ocurrencia de una amenaza
- **5.4.5** Controles en el lugar
- **5.4.6** Riesgos residuales
- **5.4.7** Identificación de los controles adicionales
- **5.4.8** Preparación de un informe del análisis del riesgo.

5.5 Análisis costo-beneficio

6 Ética informática

Objetivo: El alumno comprenderá y conocerá la importancia de enmarcar la Seguridad Informática en un ambiente ético y profesional.

Contenido:

6.1 Concepto de Ética Informática
6.2 Códigos Deontológico en Informática
6.3 Contenidos de la Ética Informática
6.4 Actualidad de la Ética Informática
6.5 Psicología del Intruso
6.6 Códigos de Ética
6.7 Casos de Estudio

Bibliografía básica: **Temas para los que se recomienda**

ANONYMOUS
Maximun Security
4rd. Edition
U.S.A.
Sams Publishing, 2003. **Todos**

FACCIN, Stefano, et al.
IP in Wireless Networks
U.S.A.
Prentice Hall, 2003. **Todos**

FLICKENGER, Rob **Todos**
Linux Server Hacks
U.S.A.
O'Reilly, 2003.

GARFINKEL, Simson, SCHWARTZ, Alan, SPAFFORD, Gene. **Todos**
Practical UNIX & Internet Security
3rd. Edition
U.S.A.
O'Reilly, 2003.

KING, Todd **Todos**
Security + Training Guide
U.S.A.
Que, 2003.

SUMMERS, Rita **Todos**
Secure Computing, Threats and Safeguards
U.S.A.
McGraw Hill, 1997

LOPEZ, Jaquelina y QUEZADA, Cintia **Todos**
Apuntes de Seguridad Informática
México
Facultad de Ingeniería – UNAM, 2005

Todos

McCARHY, Linda
IT security: risking the corporation
U.S.A.
Prentice Hall, 2003.

Bibliografía complementaria:

BHASKAR, K. **2, 4 y 5**
Threats and countermeasures
England
NCC Blackwell, 1993

ELEGIDO M,. Juan
Fundamentos de Ética de Empresa **5**
México
IPADE, 1998.

FACCIN, Stefano, et al.
IP in Wireless Networks
U.S.A. **2**
Prentice Hall, 2003.

FOGIE, Seth; PEIKARI, Cyrus
Maximum Wireless Security
U.S.A. **2**
Sams Publishing, 2002.

Sugerencias didácticas:

Exposición oral	X	Lecturas obligatorias	X
Exposición audiovisual	X	Trabajos de investigación	X
Ejercicios dentro de clase	X	Prácticas de taller o laboratorio	X
Ejercicios fuera del aula	X	Prácticas de campo	
Seminarios	X	Otras	

Forma de evaluar:

Exámenes parciales	X	Participación en clase	X
Exámenes finales	X	Asistencias a prácticas	X
Trabajos y tareas fuera del aula	X	Otras	

Perfil profesiográfico de quienes pueden impartir la asignatura

El profesor deberá contar con licenciatura, preferentemente de las carreras: Ingeniero en Computación, Ingeniero en Electrónica, Ingeniero en Telecomunicaciones, Licenciado en Ciencias Computacionales o formación equivalente y contar con amplia experiencia en seguridad en informática, desarrollo de esquemas de seguridad y aplicaciones de seguridad informática.