UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO
FACULTAD DE INGENIERÍA

PROGRAMA DE ESTUDIO

SEGURIDAD INFORMÁTICA BÁSICA	2934	9,10	8
Asignatura	Clave	Semestre	Créditos

INGENIERÍA ELÉCTRICA	INGENIERÍA EN COMPUTACIÓN	INGENIERÍA EN COMPUTACIÓN
División	Departamento	Licenciatura

Asignatura:
Obligatoria [ ]
Optativa [X]

Horas/semana:
Teóricas 4.0
Prácticas 0.0
Total 4.0

Horas/semestre:
Teóricas 64.0
Prácticas 0.0
Total 64.0

Modalidad: Curso teórico

Seriación obligatoria antecedente: Ninguna

Seriación obligatoria consecuente: Ninguna

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

Temario

NÚM.	NOMBRE	HORAS
1.	Fundamentos teóricos	10.0
2.	Amenazas y vulnerabilidades	10.0
3.	Identificación de ataques y técnicas de intrusión	14.0
4.	Políticas de seguridad informática de la organización	10.0
5.	Análisis y gestión de los riesgos	10.0
6.	Entorno social, ética informática e impacto económico de la seguridad informática	10.0
		64.0
	Actividades prácticas	0.0
	Total	64.0

1 Fundamentos teóricos

Objetivo: El alumno identificará los conceptos, objetivos y antecedentes históricos de la seguridad informática, mediante el marco histórico y con los modelos de seguridad existentes.

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 de la seguridad informática.
- **1.1.4** Principio de profundidad.

1.2 Normatividad de la seguridad informática.

- **1.2.1** Normas de seguridad a través de la historia.
- **1.2.2** Criterios comunes / ISO 15408.
- **1.2.3** COBIT.
- **1.2.4** Serie ISO 27000.

1.3 Esquema de seguridad basado en criterios comunes: perfiles de protección.

- **1.3.1** Definición y propósito.
- **1.3.2** Estructura.

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 explicará los diferentes tipos de amenazas y vulnerabilidades a través de las fuentes que las ocasionan.

Contenido:

2.1 Amenazas.

- **2.1.1** Definición.
- **2.1.2** Fuentes de amenaza.

2.2 Vulnerabilidades.

- **2.2.1** Definición.
- **2.2.2** Tipos de vulnerabilidades.

3 Identificación de ataques y técnicas de intrusión

Objetivo: El alumno explicará los métodos y técnicas de ataque e intrusión a redes y sistemas para utilizar los tipos de mecanismos de seguridad para evitarlos.

Contenido:

3.1 Ataques.

3.1.1 Definición.

3.1.2 Ataques inherentes a las redes.

3.1.3 Tipos.

3.1.4 Etapas de un ataque.

3.2 Reconocimiento y Obtención de Información.

3.2.1 Bases de datos públicas.

3.2.2 WEB.

3.2.3 DNS.

3.2.4 Keyloggers.

3.2.5 Ingeniería social.

3.2.6 Otros.

3.3 Identificación de vulnerabilidades.

3.3.1 Ataques a redes telefónicas.

3.3.2 Ataques a la telefonía inalámbrica.

3.3.3 Barrido de puertos.

3.3.4 Identificación de firewalls.

3.3.5 Identificación de sistemas operativos / Fingerprinting.

3.3.6 Escaneo a redes inalámbricas.

3.3.7 Instalaciones físicas.

3.3.8 Configuración de servicios y servidores.

3.3.9 Software.

3.3.10 Otros.

3.4 Explotación y obtención de acceso a sistemas y redes.

3.4.1 Introducción a Metasploit.

3.4.2 Metodología OSSSTM v.3.

3.4.3 Pentesting.

3.4.4 Manejo de exploits y análisis de vulnerabilidades en la red.

3.4.5 Promiscuidad en redes.

3.4.6 Robo de identidad.

3.4.7 Engaño a firewalls y detectores de intrusos.

3.4.8 Vulnerabilidades en el software.

3.4.9 Ataques a contraseñas.

3.4.10 Debilidad de los protocolos de red.

3.4.11 Ataques a servicios.

3.4.12 Negación de servicio.

3.4.13 Ataques a redes inalámbricas.

3.5 Mantener el acceso a sistemas comprometidos.

3.5.1 Puertas traseras.

3.5.2 Caballos de Troya.

3.5.3 Rootkits.

3.5.4 Otros.

3.6 Eliminación de evidencias.

3.6.1 Eliminación de evidencias.

3.6.2 Ocultar Información.

3.6.3 Estenografía.

3.6.4 Nuevos métodos.

3.7 Mecanismos de seguridad.

3.7.1 Definición y objetivos.

3.7.2 Tipos de mecanismos de seguridad.

4 Políticas de seguridad informática de la organización

Objetivo: El alumno recomendará las políticas de seguridad informática, así como los procedimientos y planes de contingencia para 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 y visión de la organización.

4.1.3 Principios fundamentales de las políticas de seguridad.

4.1.4 Modelos de seguridad.

4.1.5 Desarrollo de políticas orientadas a servicios de seguridad.

4.1.6 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.

5 Análisis y gestión de los riesgos

Objetivo: El alumno seleccionará las técnicas y métodos que le permitan llevar a cabo actividades concernientes para evaluar los 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.

5.5.1 Metodologías certificables

6 Entorno social, ética informática e impacto económico de la seguridad informática

Objetivo: El alumno resumirá los aspectos sociales y económicos en el campo de la seguridad informática para enmarcar su importancia como ambiente ético y profesional.

Contenido:

6.1 Delito informático.

6.2 Marco legal mexicano.

6.2.1 Acceso ilícito a sistemas.

6.2.2 Código Penal.

6.2.3 Derechos de Autor.

6.2.4 Actualidad de la legislación sobre delitos informáticos.

6.2.5 Protección de la información.

6.2.6 Instituto Federal de Acceso a la Información.

6.3 Ley Modelo (CNUDMI).

6.4 Legislaciones Internacionales.

6.4.1 Legislación de Estados Unidos de América en Materia Informática.

6.4.2 Legislación de Australia en Materia Informática.

6.4.3 Legislación de España en Materia Informática.

6.4.4 Otras legislaciones.

6.5 Ética informática.

6.5.1 Concepto de ética informática.

6.5.2 Códigos deontológico en informática.

6.5.3 Contenidos de la ética informática.

6.5.4 Actualidad de la ética informática.

6.5.5 Psicología del intruso.

6.5.6 Códigos de ética.

6.6 Impacto social de la seguridad informática.

6.7 Impacto económico de la seguridad informática.

Bibliografía básica

Temas para los que se recomienda:

ALEXANDER, Alberto