Nombre de la materia:	Seguridad Informática
Clave:	IA7750-T
No. de horas/semana:	4
Total de horas:	64
No. de créditos:	8
Prerrequisitos:	Redes de Computadoras (IA7600-T), Sistemas Operativos (CI7200-T)

Objetivo general: Proporcionar al estudiante los conocimientos básicos sobre los conceptos principales de la seguridad informática así como de la aplicación de las técnicas y herramientas adecuadas para preservar la confidencialidad, integridad y disponibilidad de la información y de los sistemas de información.

Contribución a los atributos de egreso y su nivel de aportación

- **AE1.** Aplicar los conocimientos de ingeniería adquiridos durante sus estudios para elaborar proyectos de ingeniería que resuelvan problemas específicos. **(Avanzado)**
- **AE2.** Identificar, formular y resolver problemas de ingeniería mediante un pensamiento crítico y asertivo, basados en los principios de ciencias básicas e ingeniería. **(Medio)**
- **AE3.** Presentar y defender su trabajo en diversos foros, tanto académicos como profesionales. **(Inicial)**
- **AE4.** Intercambiar su conocimiento y puntos de vista con profesionales del área e integrarse en equipos de trabajo multidisciplinarios. **(Medio)**
- **AE5.** Respetar su entorno social y disciplinar, enmarcado siempre por valores humanos y de ética profesional, con una actitud creativa y positiva para enfrentar nuevos retos. **(Avanzado)**

Programa sintético

1. I – ARQUITECTURA DE SEGURIDAD INFORMATICA ..... 8 hrs.
2. II – TECNOLOGIA CRIPTOGRAFICA ..... 8 hrs.
3. III – SEGURIDAD EN SERVIDORES ..... 8 hrs.
4. IV – CONTROL DE ACCESO Y CORTAFUEGOS ..... 8 hrs.
5. V – ACCESO REMOTO Y REDES PRIVADAS VIRTUALES. ..... 8 hrs.
6. VI – DETECCION DE INTRUSOS ..... 8 hrs.

Total: 48 hrs.

Programa desarrollado

1. I – ARQUITECTURA DE SEGURIDAD INFORMATICA ..... 8 hrs.
   - 1.1 Introducción a la seguridad informática.
   - 1.2 Amenazas y contramedidas.
   - 1.3 Desarrollo de la arquitectura de seguridad informática.
   - 1.4 Análisis de riesgos.
   - 1.5 Políticas, estándares, guías y su clasificación.

1.6 Desarrollo de la política de seguridad.
1.7 Aspectos de implementación de políticas de seguridad.
1.8 Planificación de continuidad del negocio (BCP) y recuperación de desastres (DRP).
1.9 Fundamentos de la auditoria de seguridad.
1.10 Adiestramiento en seguridad, educación y certificaciones.

2. II – TECNOLOGIA CRIPTOGRAFICA ..... 8 hrs.
2.1 Criptología: Criptografía y criptoanálisis.
2.2 Criptografía simétrica.
2.3 Compendio de mensajes.
2.4 Criptografía de clave pública.
2.5 Firmas digitales.
2.6 Administración y distribución de claves simétricas.
2.7 Sistema de autenticación Kerberos.
2.8 Certificados digitales. Estándar X.509.
2.9 Infraestructura de clave pública (PKI).
2.10 Estándares de clave pública (PKCS, PKIX).
2.11 Implementación de PKI.

3. III – SEGURIDAD EN SERVIDORES ..... 8 hrs.
3.1 Seguridad física.
3.2 Seguridad en UNIX.
3.3 Control de acceso y contraseñas. Permisos en directorios.
3.4 Principio de mínimo privilegio.
3.5 Aseguramiento de servicios de red en UNIX.
3.6 Análisis de bitácoras.
3.7 Seguridad en Windows 2000. Infraestructura de Seguridad.
3.8 Autenticación en W2K.
3.9 Configuración segura de W2K. Seguridad de recursos.
3.10 Registro de eventos de seguridad en W2K.
3.11 Seguridad de servicios de red en W2K. Seguridad en IIS.

4. IV – CONTROL DE ACCESO Y CORTAFUEGOS ..... 8 hrs.
4.1 Ruteo en el protocolo IP.
4.2 Ruteadores y listas de control de acceso.
4.3 Filtraje de paquetes. NAT y enmascaramiento.
4.4 Clasificación de firewalls: Dual Homed Gateway, Screened Host Gateway, Screened Subnets.
4.5 Diseño de DMZ.
4.6 Criterios de certificación de cortafuegos ITSEC, CC, AISEP e ICSA.
4.7 Niveles de aseguramiento Ex y EALx.
4.8 Implementaciones de cortafuegos.
4.9 Cortafuegos y pruebas de penetración.

4.10 Pruebas de penetración con ISS, Nessus, SARA.

5. V – ACCESO REMOTO Y REDES PRIVADAS VIRTUALES. ..... 8 hrs.

5.1 Protocolos de autenticación criptográfica. Protocolos de clave pública.

5.2 Protocolos de seguridad de la capa de aplicación. SSH.

5.3 Protocolos de seguridad de la capa de transporte. SSL/TLS.

5.4 Seguridad en redes inalámbricas. WTLS y WAP.

5.5 Protocolos de seguridad de la capa de enlace: PPTP, L2TP.

5.6 Protocolos de seguridad de la capa de red. IPSec.

5.7 Redes privadas virtuales e Internet.

5.8 Implementación de redes privadas virtuales.

6. VI – DETECCION DE INTRUSOS ..... 8 hrs.

6.1 Sistemas detectores de intrusos: basados en host y basados en red.

6.2 Técnicas de detección de intrusiones.

6.3 Verificación de integridad.

6.4 Análisis de tráfico.

6.5 Sistemas actuales de detección de intrusos.

6.6 Detección activa. Honeypots.

6.7 Respuesta a incidentes.

6.8 Técnicas de informática forense.

6.9 Recursos: CERT, CIRT, etc.

Bibliografía básica:

UNIDAD I
1. Michael Whitman, Herbert Mattord, Principles of Information Security, Course Technology, 1st edition, 2002.
2. Thomas R. Peltier,Information Security Policies, Procedures and Standards: Guidelines for Effective Information Security Management, CRC Press, 1st Edition, 2001.
3. Thomas R. Peltier, Information Security Risk Analysis, Auerbach Publications, 1st Edition, 2001.
4. Micki Krause, Harold F. Tipton, Information Security Management Handbook,Fourth Edition, Volume I, Auerbach Publications, 1999.
5. Jack Killmeyer Tudor, Information Security Architecture: An Integrated Approach to Security in the Organization. CRC Press, 2000.
6. Christopher King, Ertem Osmanaglu, Curtis Dalton, Security Architecture: Design, Deployment and Operations, McGraw Hill Osborne Media, 1st Ed. 2001.
7. Scott Barman, Writing Information Security Policies, QUE, 1st Edition, 2001.
8. Jay Ramachandran, Designing Security Architecture Solutions, John Wiley & Sons, 1st edition, 2002.
9. Jon William Toigo, Disaster Recovery Planning: Strategies for Protecting Critical Information Assets, Prentice Hall, 3rd ed, 2002.
10.Eric Maiwald, William Seiglen, Security Planning and Disaster Recovery, Mc Graw-Hill Osborne Media, 2002.
11.Floyd Piedad, Michael Hawkins, High Availability: Design, Techniques and Processes, Prentice Hall, 1st edition, 2000.
12.Evan Marcus, Hal Stern, Blueprints for High Availability: Designing Resilient Distributed Systems, John Wiley & Sons, 1st edition, 2000.
UNIDAD II
1. Bruce Schneier, Applied Cryptography: Protocols, Algorithms, and Source Code in C, John Wiley & Sons, 2nd Ed, 1995.

2. Alfred J. Menezes, Paul C. Van Oorschot, Scott A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.
3. William Stallings, Cryptography and Network Security: Principles and Practice, Prentice Hall, 3rd Edition, 2002.
4. Niels Ferguson, Bruce Schneier, Practical Cryptography, John Wiley & Sons, 1st edition, 2003.
5. Douglas Stinson, Cryptography: The

Metodologías de enseñanza-aprendizaje:

- Revisión de conceptos, análisis y solución de problemas en clase (X)
- Lectura de material fuera de clase (X)
- Ejercicios fuera de clase (tareas) (X)
- Investigación documental (X)
- Elaboración de reportes técnicos o proyectos (X)

Metodologías de evaluación:

- Asistencia (X)
- Tareas (X)
- Elaboracion de reportes técnicos o proyectos (X)
- Exámenes de academia o departamentales (X)