

## Historia del programa

Lugar y fecha de elaboración	Participantes	Observaciones (Cambios y justificaciones)
Cancún, Quintana Roo 19 Mayo 2010	Dr. Luis Rizo Dominguez M.C Julio César Ramírez Pacheco Dra. Candelaria Sansores Perez M.C. David Flores Granados	Se actualizó el programa correspondiente a la asignatura Seguridad y Administración en Redes.

## Relación con otras asignaturas

Anteriores	Posteriores
Asignatura(s) Tema(s) a) Introducción a las redes b) Redes y protocolos de servicios	No aplica
Tema(s) a) La capa de red. b) El protocolo TCP/IP.	

Nombre de la asignatura	Departamento o Licenciatura
Seguridad y administración de redes	Ingeniería en Telemática

Ciclo	Clave	Créditos	Área de formación curricular
4 - 4	IT3434	6	Licenciatura Básica

Tipo de asignatura	Horas de estudio			
	HT	HP	TH	HI
Seminario	32	16	48	48

## Objetivo(s) general(es) de la asignatura

---

### Objetivo cognitivo

Revisar la teoría que sustenta los principales métodos de seguridad en redes de computadoras para la identificación de los componentes necesarios que aseguran la integridad, confidencialidad y autenticación de los datos que se transmiten.

### Objetivo procedimental

Determinar los mecanismos adecuados de seguridad en redes de computadoras para la implementación de aplicaciones, sistemas o configuraciones de dispositivos necesarios que proporcionen la integridad, confidencialidad y autenticación de los datos que se transmiten.

### Objetivo actitudinal

Fomentar la responsabilidad en la aplicación de normativas específicas para la operación de sistemas de seguridad en redes de computadoras.

## Unidades y temas

---

### Unidad I. EL PROCESO DE SEGURIDAD

Propósito de la unidad I: Describir la historia, procesos de seguridad e importancia del aseguramiento de la información para el diseño de políticas de seguridad en redes de computadoras.

- 1) Definición de seguridad en la información.
- 2) Definición de Riesgo y sus Implicaciones
- 3) Características de los Ataques e Intrusos
- 4) Servicios de Seguridad en Computadoras, Redes y Comunicaciones
- 5) Organismos reguladores para la seguridad en la información

### Unidad II. CONFIDENCIALIDAD Y AUTENTICIDAD

Explicar el funcionamiento de los principales servicios de Confidencialidad y Autenticidad en redes de comunicación así como sus características más importantes para su aplicación en la selección de equipos de seguridad.

- 1) Cifrado Simétrico para la Confidencialidad de la Información
- 2) Cifrado Asimétrico para la Autenticación de la Información

3) Claves Públicas

4) Aplicaciones de Confidencialidad

5) Aplicaciones de Autenticidad

### Unidad III. SEGURIDAD IP

Asociar la responsabilidad en la selección de protocolos y productos en diversas capas del modelo OSI para el ofrecimiento de seguridad en la capa de red.

1) Arquitecturas de Seguridad IP

2) Cabeceras de Autenticación

3) Encapsulamientos de Cargas Útiles

4) Seguridad en Dispositivos de la capa de red

5) Filtrado de Paquetes en la capa de red

### Unidad IV. SEGURIDAD DE LA WEB

Emplear los mecanismos necesarios para la implementación de seguridad en las aplicaciones que operan en la WEB.

1) Consideraciones sobre seguridad en la WEB

2) Secure Socket Layer y Transport Layer Security

3) Secure Electronic Transaction

4) Detección de Intrusos

5) Aplicaciones para la Seguridad de la WEB

### Unidad V. SEGURIDAD EN LA GESTIÓN DE REDES

Formular arquitecturas de seguridad integral para la gestión de redes de computadoras

- 1) Conceptos básicos de SNMP
- 2) Arquitecturas y aplicaciones de Cortafuegos
- 3) Planes de Contingencia

## Actividades que promueven el aprendizaje

### Docente

Revisar conceptos mediante preguntas guía a todo el grupo usando la bibliografía básica y complementaria.  
Describir los componentes de un sistema de seguridad en redes de computadoras así como sus características mediante una lectura dirigida con todo el grupo usando la bibliografía básica y complementaria

### Estudiante

Elaborar resúmenes sobre los temas de protocolos de seguridad mediante una investigación documental individual y por equipos usando como base la bibliografía básica y complementaria así como internet.

## Actividades de aprendizaje en Internet

Elaborar resúmenes sobre los temas de protocolos de seguridad mediante una investigación documental individual y por equipos usando como base la bibliografía básica y complementaria así como internet.

## Criterios y/o evidencias de evaluación y acreditación

### Criterios

Exámenes

Tareas

Investigaciones

### Porcentajes

30

20

20

Simulaciones	15
Participaciones	15
Total	100

## Fuentes de referencia básica

---

### Bibliográficas

Davies, D. & Price, W. (1989). Security for Computer Networks. New York: John Wiley & Sons.

Harrington, Jan L. (2005). Network Security: A Practical Approach. San Francisco, CA: Morgan Kaufman.

Kizza, Joseph Migga. (2009). A Guide to Computer Network Security. London: Springer-Verlag.

Poole, Owen. (2003). Network Security: A Practical Guide. Oxford: Butterworth/Heinemann.

Stallings, William. (2003). Network Security Essentials: Applications and Standards. Upper Saddle River, New Jersey: Prentice Hall.

### Web gráficas

<http://cseweb.ucsd.edu/~mihir/cse207/> (Consultado el 19/05/2010)

<http://cobweb.ecn.purdue.edu/~kak/compsec/Lectures.html> (Consultado el 19/05/2010)

<http://www.cs.bham.ac.uk/~mdr/teaching/modules06/netsec/> (Consultado el 20/05/2010)

## Fuentes de referencia complementaria

---

### Bibliográficas

Brenton, Chris & Hunt Cameron. (2003). Mastering Network Security. San Francisco: Sybex.

Cheswick, W & Bellovin, S. (2000). Firewalls and Internet Security: Repelling the Wily Hacker. Reading, MA: Addison Wesley.

Gollman, D. (1999). Computer Security. New York: John Wiley & Sons.

Nakhjiri, Madjid & Nakhjiri, Mahsa. (2005). AAA and Network security for Mobile Access. West Sussex, England: John Wiley & Sons.

### Web gráficas

<http://www.cacr.math.uwaterloo.ca/hac/> (Consultado el 19/05/2010)

<http://users.abo.fi/ipetre/crypto/> (Consultado el 20/05/2010)

<http://williamstallings.com/Crypto3e.html> (Consultado el 19/05/2010)

## Perfil profesiográfico del docente

---

### **Académicos**

Licenciatura en redes, informática, con maestría en computación o afín. Preferentemente con doctorado en computación.

### **Docentes**

3 años de experiencia docente en el área de redes de computadoras y administración de redes de computadoras.

### **Profesionales**

Experiencia comprobable mínima de 3 años en el área de redes, en particular en el área de administración de redes.