



Nombre de la materia:	Redes de Computadoras IV
Clave:	IA7603-T
No. de horas/semana:	4
Total de horas:	64
No. de créditos:	8
Prerrequisitos:	Redes de Computadoras II (IA7601-T), Redes de Computadoras III (IA7602-T)

Objetivo general: Este curso presenta la arquitectura, la estructura, las funciones, los componentes y las configuraciones básicas de Seguridad en Redes de Computadoras. Utiliza el modelo de seguridad propuesto por Cisco Systems (Empresa global con sede en San José, California, Estados Unidos, principalmente dedicada a la fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones).

Objetivos específicos: El alumno demostrará las habilidades requeridas para desarrollar una infraestructura de seguridad, reconocer amenazas y vulnerabilidades en redes de computadoras, así como mitigar amenazas de seguridad, mediante instalación, resolución de problemas y monitoreo de dispositivos de tecnologías de seguridad Cisco, para mantener integridad, confidencialidad y disponibilidad de datos y equipo.

Programa sintético

1. Amenazas de Seguridad en Redes Modernas.	6 hrs.
2. Aseguramiento de Dispositivos de Enrutamiento.	7 hrs.
3. Autenticación, Autorización y Auditoría (AAA).	4 hrs.
4. 1ª. Evaluación Parcial	2 hrs.
5. Implementación de Tecnologías de Firewall.	6 hrs.
6. Implementación Sistemas de Prevención de Intrusiones (IPS).	5 hrs.
7. Asegurado de Redes LAN.	7 hrs.
8. 2ª Evaluación Parcial	2 hrs.
9. Sistemas Criptográficos	5 hrs.
10. Implementación de Redes Privadas Virtuales.	3 hrs.
11. Implementación de un ASA.	4 hrs.
12. Configuración Avanzada de un ASA.	7 hrs.
13. Administración de una Red Segura.	2 hrs.
14. 3ª Evaluación Parcial	2 hrs.



15. Proyecto de Programación de Tecnologías de Cifrado 2 hrs.
Total: 64 hrs.

Programa desarrollado

1. Amenazas de Seguridad en Redes Modernas. 6 hrs.
 - 1.1 Aseguramiento de Redes.
 - 1.2 Mitigación de Amenazas.
2. Aseguramiento de Dispositivos de Enrutamiento. 7 hrs.
 - 2.1 Aseguramiento de Dispositivos de Acceso.
 - 2.2 Asignación de Roles Administrativos.
 - 2.3 Monitoreo y Administración de Dispositivos.
 - 2.4 Uso de Características de Seguridad Automatizadas.
 - 2.5 Aseguramiento del Plano de Control.
3. Autenticación, Autorización y Auditoría (AAA). 4 hrs.
 - 3.1 Propósito de AAA.
 - 3.2 Autenticación AAA Local.
 - 3.3 AAA Basada en Servidor.
 - 3.4 Autenticación AAA Basada en Servidor.
 - 3.5 Autorización y Auditoría AAA Basada en Servidor.
4. 1ª Evaluación Parcial 2 hrs.
5. Implementación de Tecnologías de Firewall. 6 hrs.
 - 5.1 Listas de Control de Acceso (ACLs).
 - 5.2 Tecnologías de Firewall.
 - 5.3 Firewall de Políticas Basadas en Zonas (ZPFs).
6. Implementación Sistemas de Prevención de Intrusiones (IPS). 5 hrs.
 - 6.1 Tecnologías IPS.
 - 6.2 Firmas de IPSs.
 - 6.3 Implementación de IPSs.
7. Asegurado de Redes LAN. 7 hrs.
 - 7.1 Seguridad de Puntos Finales.
 - 7.2 Consideraciones de Seguridad Capa 2.
8. 2ª Evaluación Parcial 2 hrs.
9. Sistemas Criptográficos 5 hrs.
 - 9.1 Servicios Criptográficos.
 - 9.2 Integridad y Autenticidad Básica.



9.3	Confidencialidad.	
9.4	Criptografía de Llave Pública.	
10.	Implementación de Redes Privadas Virtuales.	3 hrs.
10.1	VPNs	
10.2	Componentes y Operación de VPNs IPSec.	
10.3	Implementación de VPNs IPSec Sitio-a-Sitio.	
11.	Implementación de un ASA.	4 hrs.
11.1	Introducción al ASA.	
11.2	Configuración de un Firewall en ASA.	
12.	Configuración Avanzada de un ASA.	7 hrs.
12.1	Administrador de Dispositivos de Seguridad ASA.	
12.2	Configuración de VPNs en ASA.	
13.	Administración de una Red Segura.	2 hrs.
13.1	Pruebas de Seguridad de Red.	
13.2	Desarrollo de Políticas de Seguridad Comprensivas.	
14.	3ª Evaluación Parcial	2 hrs.
15.	Proyecto de Programación de Tecnologías de Cifrado	2 hrs.

Bibliografía básica:

- Santos, Omar & Stuppi, John; CCNA Security 210-260 Official Cert Guide; USA; Cisco Press; 2015.

Bibliografía complementaria:

- Odom, Wendell. CCNA 200-301 Official Cert Guide, Volume 1. Cisco Press. 2019.
- Odom, Wendell. CCNA 200-301 Official Cert Guide, Volume 2. Cisco Press. 2020.
- Odom, Wendell. Cisco CCENT/CCNA ICND1 100-101 Official Cert Guide. Pearson. 2013.

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 (tarefas) (X)
- Investigación documental (X)
- Elaboración de reportes técnicos o proyectos (X)



Metodologías de evaluación:

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

Revisores:

Programa anterior propuesto por: M.I. Samuel Pérez Aguilar, M.C. José Francisco Rico Andrade, Ing. Cesar Dionicio Arreola Rodríguez.

Fecha de autorización por el H. Consejo Técnico (programa anterior): 14/08/2015

Modificado por: M.C. José Francisco Rico Andrade, M.I. Samuel Pérez Aguilar.