Universidad Michoacana de San Nicolás de Hidalgo
Facultad de Ingeniería Eléctrica

| | |
|---|---|
| Nombre de la materia : | **Redes de Computadoras IV** |
| Clave: | **IA7603-T** |
| No. De horas /semana : | **4** |
| Duración semanas: | **16** |
| Total de Horas : | **64** |
| No. De créditos : | **8** |
| Prerrequisitos : | **IA7602-T Redes de Computadoras III** |

**Descripción:**

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).

**Objetivo**

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.

**Contenido sintético**

| Tema | Duración/Horas |
|---|---|
| 1. Amenazas de Seguridad en Redes Modernas. | 6 |
| 2. Aseguramiento de Dispositivos de Enrutamiento. | 7 |
| 3. Autenticación, Autorización y Auditoría (AAA). | 4 |
| *1ª. Evaluación Parcial* | *2* |
| 4. Implementación de Tecnologías de Firewall. | 6 |
| 5. Implementación Sistemas de Prevención de Intrusiones (IPS). | 5 |
| 6. Asegurado de Redes LAN. | 7 |
| *2ª Evaluación Parcial* | *2* |
| 7. Sistemas Criptográficos. | 5 |
| 8. Implementación de Redes Privadas Virtuales. | 3 |
| 9. Implementación de un ASA. | 4 |
| 10. Configuración Avanzada de un ASA. | 7 |
| 11. Administración de una Red Segura. | 2 |
| *3ª Evaluación Parcial* | *2* |
| *Proyecto de Programación de Tecnologías de Cifrado* | *2* |
| | --- |
| Total | 64 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


**Metodología 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 ) |
| Prácticas de laboratorio en una materia asociada: | ( ) |
| Visitas a la industria: | ( ) |

**Metodología de evaluación:**

| | |
|---|---|
| Asistencia: | 00% |
| Tareas: | 10% |
| Elaboración de reportes técnicos o proyectos: | 40% |
| Exámenes de Academia o Departamentales | 50% |

**Contenido desarrollado**

| | | | |
|---|---|---|---|
| 1. | Amenazas de Seguridad en Redes Modernas. | | 6 |
| | 1.1. Aseguramiento de Redes. | 1 | |
| | 1.2. Amenazas de Red. | 2.5 | |
| | 1.3. Mitigación de Amenazas. | 2.5 | |
| 2. | Aseguramiento de Dispositivos de Enrutamiento. | | 7 |
| | 2.1. Aseguramiento de Dispositivos de Acceso. | 1.25 | |
| | 2.2. Asignación de Roles Administrativos. | 0.5 | |
| | 2.3. Monitoreo y Administración de Dispositivos. | 2.25 | |
| | 2.4. Uso de Características de Seguridad Automatizadas. | 1.5 | |
| | 2.5. Aseguramiento del Plano de Control. | 1.5 | |
| 3. | Autenticación, Autorización y Auditoría (AAA). | | 4 |
| | 3.1. Propósito de AAA. | 0.5 | |
| | 3.2. Autenticación AAA Local. | 0.5 | |
| | 3.3. AAA Basada en Servidor. | 0.5 | |
| | 3.4. Autenticación AAA Basada en Servidor. | 2 | |
| | 3.5. Autorización y Auditoría AAA Basada en Servidor. | 0.5 | |
| 4. | Implementación de Tecnologías de Firewall. | | 6 |
| | 4.1. Listas de Control de Acceso (ACLs). | 1 | |
| | 4.2. Tecnologías de Firewall. | 2.5 | |
| | 4.3. Firewall de Políticas Basadas en Zonas (ZPFs). | 2.5 | |
| 5. | Implementación Sistemas de Prevención de Intrusiones (IPS). | | 5 |
| | 5.1. Tecnologías IPS. | 1 | |
| | 5.2. Firmas de IPSs. | 2 | |
| | 5.3. Implementación de IPSs. | 2 | |
| 6. | Asegurado de Redes LAN. | | 7 |

| | | |
|---|---|---|
| 6.1. Seguridad de Puntos Finales. | 1 | |
| 6.2. Consideraciones de Seguridad Capa 2. | 6 | |
| 7. Sistemas Criptográficos. | | 5 |
| 7.1. Servicios Criptográficos. | 0.5 | |
| 7.2. Integridad y Autenticidad Básica. | 1.5 | |
| 7.3. Confidencialidad. | 1.5 | |
| 7.4. Criptografía de Llave Pública. | 1.5 | |
| 8. Implementación de Redes Privadas Virtuales. | | 3 |
| 8.1. VPNs. | 1 | |
| 8.2. Componentes y Operación de VPNs IPSec. | 1 | |
| 8.3. Implementación de VPNs IPSec Sitio-a-Sitio. | 1 | |
| 9. Implementación de un ASA. | | 4 |
| 9.1. Introducción al ASA. | 1 | |
| 9.2. Configuración de un Firewall en ASA. | 3 | |
| 10. Configuración Avanzada de un ASA. | | 7 |
| 10.1. Administrador de Dispositivos de Seguridad ASA. | 2 | |
| 10.2. Configuración de VPNs en ASA. | 5 | |
| 11. Administración de una Red Segura. | | 2 |
| 11.1. Pruebas de Seguridad de Red. | 0.5 | |
| 11.2. Desarrollo de Políticas de Seguridad Comprensivas. | 1.5 | |

**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.**

**Fecha de autorización por el H. Consejo Técnico:**

**Comentarios para la Academia y el H. Consejo Técnico:**

- Porcentaje de modificación respecto a la propuesta anterior: 80%

- Se cambia el contenido de los Capítulos para abordar tecnologías de seguridad en redes, dejando de lado protocolos de legado como Frame Relay, EIGRP, entre otros.

- Se puntualizan los cambios en base al temario anterior:
  - 1. Conexión a la WAN
    - Se trasladó el tema a Redes III por tratarse de un tópico relacionado a una interconexión de redes.
  - 2. Conexiones Punto-a-Punto
    - Se integra en el Capítulo 2 del temario de Redes III por tratarse un tópico relacionado a una interconexión de redes.
  - 3. Conexiones a Sucursal
    - Se integra en el Capítulo 11 del temario de Redes III por tratarse un tópico relacionado a una interconexión de redes.
  - 4. Listas de Control de Acceso
    - Se trasladó el tema a Redes III por tratarse de un tópico relacionado a una interconexión de redes.
  - 5. Monitoreo de Redes
    - Se replantea como capítulo 11 de la presente modificación.
  - 6. Calidad en el Servicio
    - Se trasladó el tema a Redes III por tratarse de un tópico relacionado a una interconexión de redes.
  - 7. Evolución de la Red
    - Se integra en el capítulo 11 de la presente modificación.
  - 8. Diagnóstico de Problemas de Redes WAN
    - Se trasladó el tema a Redes III por tratarse de un tópico relacionado a una interconexión de redes.

- Se puntualizan los cambios sobre nuevos temas agregados:
  - Se agregan nuevos temas para profundizar en las tecnologías de seguridad (para LANs y WANs), previamente introducidas en los anteriores cursos de Redes:
    1. Amenazas de Seguridad en Redes Modernas.
    2. Aseguramiento de Dispositivos de Enrutamiento.
    3. Autenticación, Autorización y Auditoría (AAA).
    4. Implementación de Tecnologías de Firewall.
    5. Implementación Sistemas de Prevención de Intrusiones (IPS).
    6. Asegurado de Redes LAN.
    7. Sistemas Criptográficos.
    8. Implementación de Redes Privadas Virtuales.
    9. Implementación de un ASA.
    10. Configuración Avanzada de un ASA.

- Se adecúa la descripción y objetivos a los cambios en el temario.

- Se redistribuyeron las horas, debido al reacomodo de temas en el contenido.