



MAESTRIA EN CIENCIAS DE LA COMPUTACION

Área: Sistemas Distribuidos

Programa de Asignatura: Calidad de Servicio y Seguridad en Redes

Código: MCOM 22209

Tipo: Optativa

Créditos: 9

Fecha: Noviembre 2012



1. DATOS GENERALES

Nombre del Programa Educativo:	Maestría en Ciencias de la Computación
Modalidad Académica:	Escolarizada
Nombre de la Asignatura:	Calidad de Servicio y Seguridad en Redes de Computadoras
Ubicación:	Segundo o tercer semestre (Optativa)

2. REVISIONES Y ACTUALIZACIONES

Autores:	Dr. Miguel Ángel León Chávez
Fecha de diseño:	Noviembre 2012
Fecha de la última actualización:	Marzo 2019
Revisores:	Dr. Miguel Ángel León Chávez
Sinopsis de la revisión y/o actualización:	Contenido y referencias: se incluyó la arquitectura de calidad de servicio (unidad 2) y de seguridad (unidad 8) del IEEE 802.11



3. OBJETIVOS

Generales

El estudiante conocerá y aplicará los principios de la calidad de servicio y seguridad en las redes de computadoras.

Específicos:

El alumno será capaz de:

- 1.- Definir los requerimientos de calidad y seguridad de las redes de computadoras
- 2.- Comprender la arquitectura y los servicios que ofrece TCP/IP
- 3.- Adquirir los conocimientos sobre las arquitecturas de calidad de servicio definidos para Internet y el IEEE 802.11
- 4.- Definir los servicios de seguridad del modelo de referencia OSI (ISO-7498-2)
- 5.- Comprender las vulnerabilidades de seguridad de Internet y del IEEE 802.11
- 6.- Adquirir los conocimientos sobre teoría de números y campos finitos que son la base de la criptología moderna
- 7.- Conocer las características de los criptosistemas de llave privada.
- 8.- Conocer las características de los criptosistemas de llave pública.
- 9.- Adquirir los conocimientos sobre funciones Hash
- 10.- Identificar e implementar algoritmos y protocolos para que una red, alámbrica e inalámbrica, sea segura.



4. CONTENIDO

Unidad	Contenido Temático/Actividades de aprendizaje
1. Redes de computadoras	1.1 Modelo OSI 1.2 Modelo TCP/IP 1.3 Modelo IEEE 802
2. Modelos de Calidad de Servicio	2.1 Modelo de servicios integrados de TCP/IP 2.2 Modelo de servicios diferenciados de TCP/IP 2.3 Multiprotocolo de conmutación de etiquetas (MPLS) 2.3 Ingeniería de tráfico 2.4 Arquitectura de calidad de servicio del IEEE 802.11
3. Seguridad	3.1 Amenazas y ataques 3.2 Arquitectura de seguridad de OSI de ISO 3.3 Arquitectura de seguridad de TCP/IP 3.4 Criptosistemas clásicos
4. Teoría de números	4.1 Definición y ejemplos 4.2 Aritmética modular 4.3 Campos finitos 4.4 Curvas elípticas
5. Criptosistemas de llave privada	5.1 Definición y ejemplos 5.2 Algoritmos de cifrado por bloque (DEA, 3DEA, AES) 5.3 Algoritmos de cifrado por flujo 5.4 Modos de operación
6. Criptosistemas de llave pública	6.1 Definición y ejemplos 6.2 Algoritmo Diffie-Hellman 6.3 Algoritmo RSA 6.4 Algoritmo El Gammal 6.5 Firma digital
7. Funciones Hash	7.1 SHA-1 7.2 SHA-2 7.3 SHA-3
8. Aplicaciones	8.1 Arquitectura de seguridad de IPv6 8.2 Arquitectura de seguridad del IEEE 802.11 8.2 Dinero electrónico 8.3 Votaciones electrónicas 8.4 Facturación electrónica



Bibliografía	
Básica	Complementaria
1. Tanenbaum, A.S. and D. Wetherall. "Redes de Computadoras" Pearson, 5a Edición, 2012 2. Stallings, W. "Foundations of Modern Networking", Pearson. 2016. 3. Stallings, W. "Cryptography and Network Security", Pearson, 7a Edition, 2017. 4. Trappe, W. & L.C Washington. "Introduction to Cryptography with Coding Theory". Pearson, 2 edition, 2006.	1. Stallings, W. "Effective Cybersecurity: A guide to using best practices and standards". Pearson, 2019.

5. CRITERIOS DE EVALUACIÓN

Criterios	Porcentaje
• Exámenes	40%
• Participación en clase	
• Tareas	
• Exposiciones	
• Simulaciones	
• Trabajo de investigación y/o de intervención	
• Prácticas de laboratorio	40%
• Visitas guiadas	
• Reporte de actividades académicas y culturales	
• Mapas conceptuales	
• Portafolio	
• Proyecto final	20%
• Otros	
Total	100%