BENÉMERITA UNIVERSIDAD AUTÓNOMA DE PUEBLA
FACULTAD DE CIENCIAS DE LA COMPUTACION

MAESTRIA EN CIENCIAS DE LA COMPUTACION

Área: Sistemas Distribuidos

Programa de Asignatura: Calidad de Servicio y Seguridad en Redes de Computadoras

Código: MCOM

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 2017
Revisores:	Dr. Miguel Ángel León Chávez
Sinopsis de la revisión y/o actualización:	Contenido y referencias

3. OBJETIVOS GENERALES:

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

ESPECIFICOS

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
4.- Definir los servicios de seguridad del modelo de referencia OSI (ISO-7498-2)
5.- Comprender las vulnerabilidades de seguridad de Internet
6.- Adquirir los conocimientos sobre teoría de números que es 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 para que una red sea segura
11.- Conocer los elementos principales con los que se asegura que una red 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
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 RSA 6.3 Algoritmo El Gammal 6.4 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 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.,"Data & Computer Communications", Pearson, 8a edition, 2006 3. Stallings, W. "Cryptography and Network Security", Pearson, 7a Edition, 2017. 4. W. Trappe & L.C Washington. "Introduction to Cryptography with Coding Theory". Prentice-Hall, 2a edition, 2006.	

5. CRITERIOS DE EVALUACIÓN

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