UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD POLITÉCNICA
INGENIERIA EN INFORMÁTICA
PLAN 2008
PROGRAMA DE ESTUDIO
ANEXO 02

I. IDENTIFICACIÓN

1.	Asignatura	: Electiva 1 - Desempeño y Seguridad de las Redes
2.	Semestre	: Séptimo
3.	Horas semanales	: 7 horas
	3.1. Clases teóricas	: 4 horas
	3.2. Clases prácticas	: 3 horas
4.	Total real de horas disponibles	: 112 horas
	4.1. Clases teóricas	: 64 horas
	4.2. Clases prácticas	: 48 horas

II. JUSTIFICACIÓN

La generalización del uso de recursos públicos para la interconexión de sistemas corporativos como Internet o servicios de redes privadas virtuales y la transmisión de información altamente crítica a través de ellas, hace imprescindible que la seguridad de los sistemas informáticos se concentre principalmente en las redes y sistemas de comunicación.

Mientras que los modelos de provisión de servicios como Cloud Computing ofrecen más oportunidades de negocios, aumentan los riesgos en la seguridad de los datos, es importante al utilizarse recursos de redes y de computación compartidos.

El profesional de Ingeniería Informática debe, conocer a fondo la problemática de la Seguridad en Redes, y tener la capacidad de diseñar e implementar políticas de seguridad referidas a las mismas.

En esta materia se otorgará una fuerte base teórica en los principios generales de Criptografía para permitir una evaluación de nuevos protocolos y sistemas de Seguridad en las Redes, además de conocer los fundamentos de la Gestión de la Seguridad de la Información en las empresas.

III. OBJETIVOS GENERALES

1. Definir e interpretar los conceptos básicos de la Seguridad en las Redes de Computadoras en cuanto a servicios, ataques, mecanismos y amenazas a la Seguridad
2. Identificar e interpretar conceptos fundamentales de la Criptografía y el Criptoanálisis.
3. Enunciar y describir los protocolos y los servicios que se utilizan para proporcionar Seguridad a las distintas capas del modelo OSI.
4. Describir el funcionamiento de dispositivos de seguridad en redes, como firewalls y sistemas de detección de intrusos
5. Describir las técnicas para la gestión de la Seguridad en las Empresas.
6. Discutir y explicararticulos científicos relacionados al área de la Seguridad de la Información.

IV. OBJETIVOSESPECÍFICOS

CONOCIMIENTOS

1. Describir la base científica de la Criptografía y los principales algoritmos criptográficos.
2. Formular las técnicas en el diseño y evaluación de los protocolos de Seguridad en las Redes.
3. Formular las listas de acceso y configuraciones básicas para dispositivos de Seguridad en Redes.

HABILIDADES

1. Emplear las herramientas más adecuadas para implementar Seguridad en Redes Informáticas.
2. Determinar y emplear las fases y métricas apropiadas para cada caso.

COMPETENCIAS

1. Capacidad de aplicar los conocimientos en la práctica.
2. Disposición para el trabajo en equipo.
3. Capacidad de abstracción, análisis y síntesis y presentaciones orales.
4. Capacidad para identificar, plantear y resolver problemas
5. Capacidad de comunicación oral y escrita

V. PRE – REQUISITO

Aprobar el 55% de los Créditos

VI. CONTENIDO

6.1. Unidades programáticas

1.- Introducción a la Seguridad de Redes de Computadoras.
2.- Criptografía
3.- Aplicaciones y Herramientas en Seguridad de Redes.
4.- Introducción a la Gestión de la Seguridad de Redes.

6.2. Desarrollo de las Unidades Programáticas

1.- Introducción a la Seguridad de Redes de Computadoras

1.1 Conceptos de Seguridad en Redes
1.2 La Arquitectura de Seguridad OSI
1.3 Ataques de Seguridad. Tipos de ataques. Amenazas.
1.4 Servicios de Seguridad.
1.5 Mecanismos de Seguridad
1.6 Modelos para la Seguridad de Redes

2.- Criptografía

2.1 Principios de la Criptografía y el Criptoanálisis
2.2 Transformaciones básicas. Sustitución y Permutación
2.3 Generación de números aleatorios y pseudo-aleatorios
2.4 Cifrados de flujo y Cifrados de bloque.
2.5 Criptografía de clave simétrica. Principios.
2.6 Algoritmos de cifrado de clave simétrica
2.7 Modos de operación de cifrados de bloques.
2.8 Enfoques de la autenticación de mensajes
2.9 Funciones hash seguras. Principios y requerimientos
2.10 Códigos de autenticación de mensajes
2.11 Principios de cifrado de clave pública
2.12 Firmas Digitales
2.13 Algoritmos RSA y Diffie-Hellman
2.14 Distribución de claves simétricas y de claves públicas

3.- Aplicaciones y herramientas de la Seguridad en Redes

3.1 Seguridad en la capa de Transporte
3.2 Protocolos SSL y TSL
3.3 HTTPS
3.4 Seguridad en el correo electrónico
3.5 PGP
3.6 S/MIME
3.7 Seguridad en la capa de red: IPsec
3.8 Políticas y requerimientos de la Seguridad en la capa de red
3.9 Protocolos ESP, AH, IKE
3.10 Asociaciones de Seguridad en IPsec
3.11 Firewalls. Tipos
3.12 Configuraciones y localización de firewalls
3.13 Detección de Intrusos.
3.14 Manejo de contraseñas
3.15 Tipos de detección de intrusos
3.16 Software Malicioso: Virus, Troyanos, Gusanos
3.17 Ataques de denegación de servicios distribuida
3.18 Seguridad en redes inalámbricas

4.- Introducción a la gestión de la Seguridad en Redes

4.1 Necesidad de gestión de la Seguridad corporativa.
4.2 Documentación. Política de Seguridad
4.3 Gestión de Riesgos en la Seguridad de Redes
4.4 Estándares y Certificaciones. ISO 27001

VII. ESTRATEGIAS METODOLÓGICAS

1. Clases magistrales
2. trabajos grupales,

Además los estudiantes participarán activamente de las clases al realizar lecturas previas de un tema determinado. Los estudiantes realizarán los trabajos de laboratorios realizados en grupos o individuales y serán supervisados por los docentes.
Presentación y defensa de memorias de prácticas de laboratorio y de artículos científicos relacionados con el área en cuestión.
Enseñanza basada en trabajo y evaluación continua, que incluyen el aprendizaje basado en problemas y el trabajo en grupo.

VIII. MEDIOS AUXILIARES

1.- Proyector de diapositivas
2.- Computadoras
3.- Pizarra
4.- Marcadores
5.- Borrador de pizarra
6.- Herramientas de software para simulación de redes de computadoras

IX. EVALUACIÓN

Para la evaluación de la asignatura se tendrá en cuenta lo siguiente:

1.- Examen final (teoría y ejercicios) con un porcentaje asignado
2.- Evaluación contínua de la teoría, obtenida a través de tests semanales.
3.- Nota de Trabajos prácticos, donde se ponga de manifiesto la habilidad del estudiante en modelar y resolver un ataque a la Seguridad de Redes
4.- Clases de laboratorio, utilizando simuladores de redes de computadoras.
5.- Las calificaciones se basan en el Reglamento de Cátedra de la Facultad
6.- Es imprescindible la entrega de todos los trabajos prácticos y la asistencia a clases de laboratorios.

X. BIBLIOGRAFÍA

William Stallings. "Network Security Essentials – Applications and Standards". 5ta Edición, Pearson.
Andrew Tanenbaum – David Wetherhall "Redes de Computadoras" – 5ta Edición, Pearson
Christof Para, Jan Petzl. "Understanding Cryptography". Springer
Behrouz A. Forouzan. "Cryptography and Network Security". McGraw-Hill
Documentación proveída por los docentes.