UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD POLITÉCNICA
LICENCIATURA EN CIENCIAS INFORMÁTICAS
PLAN 2009
PROGRAMA DE ESTUDIOS

Resolución 25/07/10-00 Acta 1215/07/04/2025
ANEXO 06

I.- IDENTIFICACIÓN

1.	Asignatura	: Electiva - Desempeño y Seguridad de las Redes
2.	Horas semanales	: 5 horas
2.1.	Clases teóricas	: 2,5 horas
2.2.	Clases prácticas	: 2,5 horas
3.	Total de horas cátedras	: 90 horas
3.1.	Total de clases teóricas	: 45 horas
3.2.	Total de clases prácticas	: 45 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 Ciencias Informáticas 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 asignatura 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

3.1 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
3.2 Identificar e interpretar conceptos fundamentales de la Criptografía y el Criptoanálisis.
3.3 Enunciar y describir los protocolos y los servicios que se utilizan para proporcionar Seguridad a las distintas capas del modelo OSI.
3.4 Describir el funcionamiento de dispositivos de seguridad en redes, como firewalls y sistemas de detección de intrusos
3.5 Describir las técnicas para la gestión de la Seguridad en las Empresas.
3.6 Discutir y explicar artículos científicos relacionados al área de la Seguridad de la Información.

IV. - PRE – REQUISITO

De acuerdo con el Proyecto Académico, el énfasis y la elección del número de electiva a cursar, el estudiante deberá cumplir:

Descripción	Prerrequisito	Énfasis
Electiva I - Desempeño y Seguridad de las Redes	Programación de Aplicaciones en Redes	Programación de Computadoras
Electiva I - Desempeño y Seguridad de las Redes	Administración III	Análisis de Sistemas Informáticos
Electiva II - Desempeño y Seguridad de las Redes	Electiva I, Base de Datos II	Análisis de Sistemas Informáticos
Electiva III - Desempeño y Seguridad de las Redes	Ingeniería de Software I, Base de Datos III	Análisis de Sistemas Informáticos
Electiva IV - Desempeño y Seguridad de las Redes	Ingeniería de Software II, Electiva III	Análisis de Sistemas Informáticos

V. -CONTENIDO

5.1 Unidades programáticas

5.1.1 Introducción a la Seguridad de Redes de Computadoras.
5.1.2 Criptografía
5.1.3 Aplicaciones y Herramientas en Seguridad de Redes.
5.1.4 Introducción a la Gestión de la Seguridad de Redes.

5.2. Desarrollo de las unidades programáticas

5.2.1 Introducción a la Seguridad de Redes de Computadoras

5.2.1.1 Conceptos de Seguridad en Redes
5.2.1.2 La Arquitectura de Seguridad OSI
5.2.1.3 Ataques de Seguridad. Tipos de ataques. Amenazas.
5.2.1.4 Servicios de Seguridad.
5.2.1.5 Mecanismos de Seguridad
5.2.1.6 Modelos para la Seguridad de Redes

5.2.2. Criptografía

5.2.2.1. Principios de la Criptografía y el Criptoanálisis
5.2.2.2. Transformaciones básicas. Sustitución y Permutación
5.2.2.3. Generación de números aleatorios y pseudo-aleatorios
5.2.2.4. Cifrados de flujo y Cifrados de bloque.
5.2.2.5. Criptografía de clave simétrica. Principios.
5.2.2.6. Algoritmos de cifrado de clave simétrica
5.2.2.7. Modos de operación de cifrados de bloques.
5.2.2.8. Enfoques de la autenticación de mensajes
5.2.2.9. Funciones hash seguras. Principios y requerimientos
5.2.2.10. Códigos de autenticación de mensajes
5.2.2.11. Principios de cifrado de clave pública
5.2.2.12. Firmas Digitales
5.2.2.13. Algoritmos RSA y Diffie-Hellman
5.2.2.14. Distribución de claves simétricas y de claves públicas

5.2.3 Aplicaciones y herramientas de la Seguridad en Redes

5.2.3.1. Seguridad en la capa de Transporte
5.2.3.2. Protocolos SSL y TSL
5.2.3.3. HTTPS
5.2.3.4. Seguridad en el correo electrónico
5.2.3.5. PGP
5.2.3.6. S/MIME
5.2.3.7. Seguridad en la capa de red: IPsec
5.2.3.8. Políticas y requerimientos de la Seguridad en la capa de red
5.2.3.9. Protocolos ESP, AH, IKE
5.2.3.10. Asociaciones de Seguridad en IPsec
5.2.3.11. Firewalls. Tipos
5.2.3.12. Configuraciones y localización de firewalls
5.2.3.13. Detección de Intrusos.
5.2.3.14. Manejo de contraseñas
5.2.3.15. Tipos de detección de intrusos
5.2.3.16. Software Malicioso: Virus, Troyanos, Gusanos
5.2.3.17. Ataques de denegación de servicios distribuida
5.2.3.18. Seguridad en redes inalámbricas

5.2.4. Introducción a la gestión de la Seguridad en Redes

5.2.4.1. Necesidad de gestión de la Seguridad corporativa.
5.2.4.2. Documentación. Política de Seguridad
5.2.4.3. Gestión de Riesgos en la Seguridad de Redes
5.2.4.4. Estándares y Certificaciones. ISO 27001

VI.- ESTRATEGIAS METODOLÓGICAS

6.1 Clases magistrales
6.2 Trabajos grupales,
6.3 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.
6.4 Presentación y defensa de memorias de prácticas de laboratorio y de artículos científicos relacionados con el área en cuestión.
6.5 Enseñanza basada en trabajo y evaluación continua, que incluyen el aprendizaje basado en problemas y el trabajo en grupo.

VII.- MEDIOS AUXILIARES

7.1. Proyector de diapositivas
7.2. Computadoras
7.3. Pizarra
7.4. Marcadores
7.5. Borrador de pizarra
7.6. Herramientas de software para simulación de redes de computadoras

VIII.- EVALUACIÓN

La evaluación se realizará de acuerdo a las reglamentaciones vigentes de la Facultad Politécnica FP- UNA.

IX. - 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. "UnderstandingCryptography". Springer
- ❑ Behrouz A. Forouzan. "Cryptography and Network Security". McGraw-Hill
- ❑ Documentación proveída por los docentes.