UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD POLITÉCNICA
INGENIERIA EN INFORMATICA
PLAN 2008
PROGRAMA DE ESTUDIOS

Resolución 25/07/09-00 Acta 1215/07/04/2025
ANEXO 05

I. IDENTIFICACIÓN

1.	Asignatura	: Electiva - Desempeño y Seguridad de las Redes
2.	Semestre	: Según la alternativa en la que se inscribe el estudiante
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

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

Para cursar esta asignatura, que se ofrece en la carrera como Electiva, el estudiante deberá cumplir con los prerrequisitos establecidos según la electiva en la que se inscribe, de acuerdo con la siguiente tabla:

Alternativa	Porcentaje de créditos aprobados	Cantidad de créditos requeridos
Electiva 1	55%	184
Electiva 2, Electiva 3, Electiva 4, Electiva 5	70%	235
Electiva 6, Electiva 7	80%	268

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

5.2.1.7. Principios de la Criptografía y el Criptoanálisis
5.2.1.8. Transformaciones básicas. Sustitución y Permutación
5.2.1.9. Generación de números aleatorios y pseudo-aleatorios
5.2.1.10. Cifrados de flujo y Cifrados de bloque.
5.2.1.11. Criptografía de clave simétrica. Principios.
5.2.1.12. Algoritmos de cifrado de clave simétrica
5.2.1.13. Modos de operación de cifrados de bloques.
5.2.1.14. Enfoques de la autenticación de mensajes
5.2.1.15. Funciones hash seguras. Principios y requerimientos
5.2.1.16. Códigos de autenticación de mensajes
5.2.1.17. Principios de cifrado de clave pública
5.2.1.18. Firmas Digitales
5.2.1.19. Algoritmos RSA y Diffie-Hellman
5.2.1.20. Distribución de claves simétricas y de claves públicas

5.2.3 Aplicaciones y herramientas de la Seguridad en Redes

5.2.1.21. Seguridad en la capa de Transporte
5.2.1.22. Protocolos SSL y TSL
5.2.1.23. HTTPS
5.2.1.24. Seguridad en el correo electrónico
5.2.1.25. PGP
5.2.1.26. S/MIME
5.2.1.27. Seguridad en la capa de red: IPsec
5.2.1.28. Políticas y requerimientos de la Seguridad en la capa de red
5.2.1.29. Protocolos ESP, AH, IKE
5.2.1.30. Asociaciones de Seguridad en IPsec
5.2.1.31. Firewalls. Tipos
5.2.1.32. Configuraciones y localización de firewalls
5.2.1.33. Detección de Intrusos.
5.2.1.34. Manejo de contraseñas
5.2.1.35. Tipos de detección de intrusos
5.2.1.36. Software Malicioso: Virus, Troyanos, Gusanos
5.2.1.37. Ataques de denegación de servicios distribuida
5.2.1.38. Seguridad en redes inalámbricas

5.2.4 Introducción a la gestión de la Seguridad en Redes

5.2.1.39. Necesidad de gestión de la Seguridad corporativa.
5.2.1.40. Documentación. Política de Seguridad
5.2.1.41. Gestión de Riesgos en la Seguridad de Redes
5.2.1.42. 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 sobre el aprendizaje y conocimiento adquiridos por el alumno se realizará de acuerdo a lo establecido en el reglamento de la Facultad Politécnica de la UNA.

IX. BIBLIOGRAFÍA

□ Behrouz A. Forouzan. (2007). Cryptography and Network Security. McGraw-Hill

- Christof Para, J. P. (2010). Understanding Cryptography: A Textbook for Students and Practitioners. London: Springer
- Tanenbaum, A. & Wetherhall, D. (2012). Redes de Computadoras. (5° Ed.). México: Pearson Education.
- William Stallings. (2001). Network Security Essentials: Applications and Standards. (4° Ed.). Boston: Pearson.

MATERIALES BIBLIOGRÁFICOS DISPONIBLES EN LA BIBLIOTECA DE LA FACULTAD POLITÉCNICA

- Comer, D. E. (2000). *Redes globales de información con Internet y TCP/IP: principios básicos, protocolos y arquitectura.* México: Prentice Hall.
- Halsall, F. (1998). *Comunicación de datos, redes de computadores y sistemas abiertos.* (4° ed.). México: Addison Wesley Iberoamericana.
- Martínez, J. (2004). *Redes de comunicaciones.* México: Alfaomega.
- Stallings, W. (2000). *Comunicaciones y redes de computadoras.* (6° Ed.). Madrid: Pearson Educación.
- Tanenbaum, A. S. & Wetherall, D. J. (2012). Redes de computadoras. (5° Ed.). México: Pearson Educación.
- Tanenbaum, A. S. (2009). *Computer networks.* (4° Ed.). New Jersey: Prentice Hall PTR

RECURSOS DISPONIBLES A TRAVÉS DE CICCO

- Berná Galiano, J. A., Pérez Polo, M., & Crespo Martínez, L. M. (2002). Redes de computadores para ingenieros en informática. [Alicante]: Digitalia.
- Iacono, L., Godoy, P., Marianetti, O., García Garino, C., & Párraga, C. (2012). Estudio de la Integración entre WSN y redes TCP/IP. (Spanish). *Memoria De Trabajos De Difusion Cientifica Y Técnica*, (10), 57.
- Torres Medina, F., Candelas Herías, F. A., & Puente Méndez, S. T. (2006). *Sistemas para la transmisión de datos.* [Alicante]: Digitalia.
- Yezid Enrique Donoso, M., Indira Acuña, R., Zulay Guardias, G., Marguie Martínez, D., & Luis Carlos, P. (2000). Especificación de la interconexión de redes TCP/IP (ETHERNET) a través de una red WAN Frame Relay. *Ingeniería Y Desarollo, Iss 8, Pp 33-48 (2000)*, (8), 33.

UNIVERSIDAD NACIONAL DE ASUNCION FACULTAD POLITÉCNICA 1979 CONSTRUYENDO EL FUTURO