UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD POLITÉCNICA
CONSEJO DIRECTIVO

Campus de la UNA
SAN LORENZO-PARAGUAY

RESOLUCIÓN 25/18/155-00
ACTA 1226/25/08/2025

"POR LA CUAL SE APRUEBA EL PROGRAMA DE ESTUDIO DE LA ASIGNATURA *SEGURIDAD EN REDES,* DE CARRERAS DE GRADO, SEDE SAN LORENZO, FILIAL VILLARRICA Y FILIAL CORONEL OVIEDO"

VISTO: El Memorando DA/1707/2025 del Director Académico de la FP-UNA, Prof. MSc. Felipe Santiago Uzabal Escurra, con el cual remite el Memorando CCPTCC/030/2025 de la Comisión Coordinadora del Proyecto de Transformación Curricular de Carreras de Grado de la FP-UNA, en el que presenta la propuesta de Programa de Estudio de Asignatura de las Carreras de Grado.

CONSIDERANDO: La Ley 4995/2013 de Educación Superior, el Estatuto de la Universidad Nacional de Asunción y las deliberaciones sobre el tema.

Que la Comisión Coordinadora del Proyecto de Transformación Curricular de Carreras de Grado, solicita la aprobación del Programa de Estudio de la asignatura ***"Seguridad en Redes"***, la cual es común entre Carreras de Grado.

Que los programas fueron elaborados conforme a las disposiciones establecidas por el Consejo Nacional de Educación Superior (CONES) en materia de **créditos académicos**, según lo dispuesto en la Resolución CONES N.° 221/2024, que regula el *Sistema de Créditos Académicos – Paraguay* y los criterios para su publicación en las carreras de grado.

EL CONSEJO DIRECTIVO DE LA FACULTAD POLITÉCNICA
RESUELVE:

25/18/155-01 APROBAR el Programa de Estudio de la Asignatura ***"Seguridad en Redes"***, de carreras de Grado, Sede San Lorenzo, Filial Villarrica y Filial Coronel Oviedo, detallado en el ANEXO 117 de la presente Acta.

25/18/155-02 COMUNICAR, copiar y archivar.

Prof. Abg. Joel Arsenio Benítez Santacruz
Secretario

Prof. Ing. Silvia Teresa Leiva León, MSc.
Presidenta

TEL/FAX: +595 21 5887000 – C.C. 1130 (Asunción) – 2111 (San Lorenzo)
www.pol.una.py

DEPARTAMENTO DE ENSEÑANZA DE INFORMÁTICA
PROGRAMA DE ESTUDIO

I. IDENTIFICACIÓN

Nivel	Grado				
Asignatura	Seguridad en Redes				
Carrera	**Plan**	**Sede/Filial**	**Carácter**	**Semestre**	**Prerrequisitos**
Ingeniería en Informática	2026	Sede San Lorenzo	Electiva 1	Séptimo	Seguridad Informática, Programación de Aplicaciones 2, Bases de Datos 2, Ingeniería de Software 1.
Licenciatura en Ciencias Informáticas	2026	Sede San Lorenzo/Filial Villarrica/Filial Coronel Oviedo	Electiva	***	Ingeniería de Software I, Base de Datos II, Seguridad Informática, Programación Frontend.

Semanal					**Periodo**				
HT	**HP**	**HTD**	**HTI**	**HS**	**PA**	**THTD**	**THTI**	**THA**	**CA-PY**
2	2	4	4	8	18	72	72	144	5

***HT: Horas Teóricas semanales.**
***HP: Horas Prácticas semanales.**
***HTD: Horas semanales de Trabajo académico con acompañamiento Docente.**
***HTI: Horas semanales de Trabajo académico Independiente del estudiante.**
***HS: Horas Semanales (HTD+HTI).**
***PA: Periodo Académico en semanas.**
*** THTD: Total de Horas de Trabajo académico con acompañamiento Docente (HTD*PA).**
*** THTI: Total de Horas de Trabajo académico Independiente del estudiante (HTI*PA).**
*** THA: Total de Horas de trabajo Académico (THTD+THTI).**
*** CA-PY: Créditos académicos de la asignatura.**

II. FUNDAMENTACIÓN

La asignatura de Seguridad en Redes es esencial para la formación integral de los futuros profesionales informáticos, dado el creciente protagonismo que la ciberseguridad ha adquirido en el ámbito de las tecnologías de la información. En un mundo cada vez más digitalizado, donde las amenazas y vulnerabilidades de seguridad evolucionan continuamente, es fundamental que los profesionales en informática adquieran una sólida comprensión de los principios, técnicas y herramientas para proteger redes y sistemas contra ataques maliciosos y brechas de seguridad.

Esta asignatura introduce los conceptos básicos de la seguridad en redes, estableciendo las bases necesarias para entender los riesgos y amenazas a los que se enfrentan las redes modernas. Se cubren los fundamentos de la criptografía moderna, incluyendo algoritmos de cifrado simétrico y asimétrico, funciones hash, y técnicas de firma digital. La comprensión de estos conceptos permite a los estudiantes implementar medidas efectivas para proteger la integridad y confidencialidad de la información en tránsito y almacenada. Se estudian los firewall, sistemas de detección de intrusiones (IDS) y sistemas de prevención de intrusiones (IPS), los protocolos de seguridad en redes y por último se ofrece una visión

general sobre la gestión de la seguridad en redes, la planificación de la seguridad, la evaluación de riesgos, y la implementación de políticas de seguridad.

En relación a la naturaleza de la asignatura, se aborda de manera teórico-práctica, se combinarán conceptos teóricos con ejercicios prácticos. La organización de la asignatura se basa en los ejes temáticos, se incluyen conceptos fundamentales como: Firewall, IDS/IPS, VPN, protocolos seguros, análisis de tráfico y mitigación de ataques.

III. COMPETENCIAS DEL PERFIL DE EGRESO ASOCIADAS

1. Adaptarse respetuosamente a contextos nuevos o adversos, así como a diversidades personales, disciplinares y culturales.

2. Evaluar el comportamiento de diversos fenómenos disciplinares e interdisciplinares relacionados con la informática con una visión de sistema, mediante modelos teóricos validados y actualizados, capaces de abarcarlos integralmente en un contexto de incertidumbre.

3. Planificar, proyectar, diseñar y ejecutar proyectos sostenibles e integrales para la resolución de problemas, la mejora y la innovación en el ámbito de la informática.

IV. ORGANIZACIÓN DE LA ASIGNATURA

Unidades	Contenidos	Resultados de aprendizaje
1. Fundamentos de la Seguridad de Redes Informática.	1.1. Conceptos básicos de seguridad en redes. 1.2. Arquitectura de Seguridad OSI. 1.3. Ataques de Seguridad. Tipos de ataques. Amenazas. 1.4. Mecanismos de seguridad. 1.4.1. Cifrado 1.4.2. Firma digital 1.4.3. Control de Acceso 1.4.4. Autenticación 1.4.5. Confidencialidad 1.4.6. Integridad 1.4.7. Relleno del tráfico 1.4.8. Control de enrutamiento 1.4.9. No repudio 1.5. Servicios de Seguridad.	1. Comprende los conceptos fundamentales de la seguridad en redes. 2. Evalúa los servicios de seguridad para la protección 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 pseudoaleatorios. 2.4. Cifrado de flujo y cifrados de bloque. 2.5. Criptografía de clave simétrica. Principios. 2.6. Algoritmos de cifrado de clave	1. Conoce principios fundamentales de la criptografía y criptoanálisis. 2. Implementa y evalúa algoritmos de cifrado y autenticación de mensajes. 3. Utiliza algoritmos de clave pública y firmas digitales.

Unidades	Contenidos	Resultados de aprendizaje
	simétrica. 2.7. Modos de operación de cifrado de bloques. 2.8. Enfoques de 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 DiffieHellman 2.14. Distribución de claves simétricas y de claves públicas.	
3. Firewalls.	3.1. Definición y tipos. 3.2. Configuración e implementación de Firewall. 3.3. DMZ. 3.4. Servicios de Firewalls.	1. Comprende los conceptos básicos y tipos de Firewalls. 2. Implementa un Firewall en un entorno de red 3. Analiza los servicios ofrecidos por un Firewall y su impacto en la seguridad de la red.
4. Detección y Prevención de Intrusiones en el Sistema.	4.1. Detección de Intrusos. 4.2. Sistemas de Detección de Intrusiones (IDS). 4.3. Tipos de Sistemas de Detección de Intrusiones. 4.4. Algoritmos de Machine Learning para la Detección de Intrusiones. 4.5. Sistemas de Prevención de Intrusiones (IPS).	1. Comprende los principios y funcionalidades de los Sistemas de Detección de Intrusiones. 2. Implementa Sistemas de Detección y Prevención de Intrusiones (IDS/IPS). 3. Aplica algoritmos de Machine Learning para la mejora en la Detección de Intrusiones.
5. Protocolos de Seguridad en Redes.	5.1. Seguridad a Nivel de Aplicación. 5.1.1. RADIUS, TACACS. 5.1.2. PGP, MIME, HTTPS. 5.1.3. SET, Kerberos. 5.2. Seguridad en la Capa de Transporte 5.2.1. SSL, TLS 5.3. Seguridad en la Capa de Red 5.3.1. IPSEC, VPN 5.3.2. PPTP, L2TP 5.4. Seguridad en la Capa Física 5.4.1. PPP.	1. Comprende el mecanismo de los protocolos de seguridad en redes . 2. Implementa soluciones de seguridad en redes utilizando protocolos en las distintas capas.
6. Introducción a la gestión de la Seguridad en Redes.	6.1. Necesidad de gestión de la Seguridad corporativa. 6.2. Documentación. Política de Seguridad.	3. Desarrolla políticas de seguridad efectivas para una organización. 4. Gestiona riesgos en la seguridad de redes informáticas.

Unidades	Contenidos	Resultados de aprendizaje
	6.3. Gestión de Riesgos en la Seguridad en Redes. 6.4. Estándares y Certificaciones. ISO 27001	5. Comprende los principios y requisitos de la norma ISO 27001 .

V. ESTRATEGIAS DIDÁCTICAS

En el desarrollo del programa se aplicarán estrategias didácticas conducentes a la apropiación teórica y la ejecución práctica de procesos y procedimientos, a saber:

- **Aprendizaje basado en problemas:** exposición por parte del docente de los conceptos básicos por unidad, con materiales de lectura y ejemplos orientados a la enseñanza de las competencias específicas de la asignatura. El estudiante buscará resolver un problema a través del conocimiento que adquirió en el aula.

- **Aprendizaje basado en proyectos:** el docente propondrá la realización de un proyecto que involucre todos los resultados de aprendizaje de la materia. De esta forma el estudiante participa activamente en su aprendizaje, desarrollando diferentes habilidades para solucionar un problema a través de este proyecto.

La elección particular de la estrategia didáctica aplicada será explícita en el Planeamiento de la Asignatura, de acuerdo con el perfil de los estudiantes, los recursos disponibles y el contexto educativo.

VI. ESTRATEGIAS EVALUATIVAS

Procesos de producción grupales e individuales, pruebas individuales orales y/o escritas durante el desarrollo de las unidades con diálogos e interpretaciones que los estudiantes realicen sobre los contenidos, debates, retroalimentación en casos necesarios y actividades que amplíen el conocimiento.

Con fines de calificación y promoción se aplicará el Reglamento Académico vigente en la institución que prevé valoraciones de proceso y final.

VII. MEDIOS AUXILIARES

Pizarras, marcadores, computadoras, proyector, parlantes para multimedia, plataforma virtual, sala de laboratorio equipada para prácticas con sistemas operativos Linux o Windows y acceso a Internet.

VIII. BIBLIOGRAFÍA

- Stallings, W. (2016). Network Security Essentials: Applications and Standards. Reino Unido: Pearson.
- Tanenbaum, A., Feamster, N., Wetherall, D. (2021). Redes de Computadores . 6th Edition. Pearson.
- Joseph MiggaKizza. Guide to Computer Network Security. Springer International Publishing, 202.
- Stallings, W. (2004). Comunicaciones y redes de computadores. 7ma Edición. Pearson
- Chen, Y., Wu, J., Yu, P., & Wang, X. (2024). Network Security Empoweredby Artificial Intelligence. Network Security. Springer