UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD POLITÉCNICA
CONSEJO DIRECTIVO

Campus de la UNA
SAN LORENZO-PARAGUAY

RESOLUCIÓN 25/18/143-00
ACTA 1226/25/08/2025

"POR LA CUAL SE APRUEBA EL PROGRAMA DE ESTUDIO DE LA ASIGNATURA *HACKING ÉTICO Y CIBERSEGURIDAD,* DE LA CARRERA INGENIERÍA EN INFORMÁTICA – PLAN 2026, SEDE SAN LORENZO"

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 las Asignaturas de la Carrera Ingeniería en Informática.

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 **"Hacking Ético y Ciberseguridad",** de la carrera Ingeniería en Informática – Plan 2026.

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:

25/18/143-01 APROBAR el Programa de Estudio de la Asignatura **"Hacking Ético y Ciberseguridad",** de la carrera Ingeniería en Informática – Plan 2026, Sede San Lorenzo, detallado en el ANEXO 105 de la presente Acta.

25/18/143-02 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	Hacking Ético y Ciberseguridad				
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.

Semanal					**Periodo**				
HT	**HP**	**HTD**	**HTI**	**HS**	**PA**	**THTD**	**THTI**	**THA**	**CA-PY**
3	1	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 "Hacking Ético y Ciberseguridad" emerge como una respuesta esencial ante el aumento exponencial de amenazas cibernéticas en la actualidad digital. En este contexto, la formación de profesionales capaces de comprender, prevenir y mitigar estas amenazas de manera ética y eficaz se vuelve crucial.

La asignatura se enfoca en cuatro áreas fundamentales. En primer lugar, aborda técnicas avanzadas de penetración, permitiendo a los estudiantes identificar vulnerabilidades y evaluar la resistencia de sistemas y redes. Posteriormente, se centra en el manejo de herramientas de hacking ético, brindando a los estudiantes la capacidad de llevar a cabo pruebas de penetración controladas y evaluar la seguridad de sistemas y aplicaciones.

Además, la asignatura se ocupa de estrategias para la detección, respuesta y defensa contra ciberataques, incluyendo la implementación de estrategias de defensa en profundidad. Por último, se explora la ética del hacking, donde se analizan códigos éticos específicos, se evalúan las consecuencias éticas y se destaca la importancia de la protección de la privacidad y los derechos digitales.

En conjunto, esta asignatura proporciona a los estudiantes conocimientos y habilidades cruciales para abordar los desafíos cambiantes del entorno digital. La combinación de técnicas avanzadas con una sólida base ética forma a profesionales capaces de contribuir de manera responsable y efectiva a la seguridad digital en diversos entornos y sectores..

En relación a la naturaleza de la asignatura, se aborda de manera teórico-práctico, se combinarán conceptos teóricos con ejercicios prácticos. La organización de la asignatura se basa en los ejes temáticos, se incluyen conceptos fundamentales como: Técnicas de penetración, herramientas, respuesta y defensa contra ciberataques, y ética del hacking.

III. COMPETENCIAS DEL PERFIL DE EGRESO ASOCIADAS

1. Aplicar en la práctica profesional los valores humanos, la ética y los mecanismos de seguridad laboral.
2. Actuar proactivamente frente a los problemas sociales y ambientales.
3. Adaptarse respetuosamente a contextos nuevos o adversos, así como a diversidades personales, disciplinares y culturales.
4. Actualizarse permanentemente mediante la obtención y gestión autónoma de información de calidad, utilizando tecnología de la información y comunicación.
5. Comunicarse en las lenguas oficiales del país y en una lengua extranjera.

IV. ORGANIZACIÓN DE LA ASIGNATURA

Unidades	Contenidos	Resultados de aprendizaje
1. Introducción a la Ciberseguridad	1.1. Conceptos clave de ciberseguridad. 1.2. Importancia de la seguridad en la era digital. 1.3. Evolución de las amenazas cibernéticas.	1. Define conceptos clave de ciberseguridad. 2. Reconoce la importancia de la seguridad digital. 3. Identifica y explica amenazas cibernéticas comunes.
2. Fundamentos del Hacking Ético.	2.1. Definición y principios del hacking ético. 2.2. Ética en la ciberseguridad. 2.3. Marco legal y regulaciones.	1. Explica la definición y los principios fundamentales del hacking ético. 2. Analiza la importancia de la ética en la ciberseguridad y su aplicación en el hacking ético. 3. Identifica y comprende el marco legal y las regulaciones asociadas al hacking ético y la ciberseguridad
3. Técnicas de Penetración	3.1. Reconocimiento y recopilación de información. 3.2. Escaneo de redes y sistemas. 3.3. Vulnerabilidades y análisis de riesgos. 3.4. Explotación de vulnerabilidades.	1. Aplica técnicas efectivas de reconocimiento y recopilación de información. 2. Realiza escaneo de redes y sistemas de manera precisa y eficiente. 3. Identifica vulnerabilidades y realizar análisis de riesgos. 4. Demostra habilidades en la explotación de vulnerabilidades de forma ética y controlada
4. Herramientas de Hacking Ético.	4.1. Principales herramientas de hacking ético. 4.2. Uso de herramientas para	1. Identifica y describe las principales herramientas utilizadas en el hacking ético.

Unidades	Contenidos	Resultados de aprendizaje
	pruebas de penetración. 4.3. Herramientas de análisis forense.	2. Aplica el uso efectivo de herramientas para realizar pruebas de penetración de manera controlada y ética..
5. Respuesta y Defensa contra Ciberataques.	5.1. Detección de incidentes y respuesta rápida. 5.2. Estrategias de defensa en profundidad. 5.3. Desarrollo de políticas de seguridad	1. Implementa técnicas efectivas de detección de incidentes y responder rápidamente a amenazas cibernéticas. 2. Desarrolla estrategias de defensa en profundidad para proteger sistemas y redes. 3. Crea políticas de seguridad sólidas y adaptativas para prevenir y mitigar ciberataques.
6. Proyecto Final - Simulación de Ataque y Respuesta.	6.1. Diseño y ejecución de un escenario de ataque controlado. 6.2. Implementación de medidas de defensa. 6.3. Análisis post-incidente y lecciones aprendidas.	1. Diseña y ejecuta un escenario de ataque controlado de manera efectiva y ética. 2. Implementa medidas de defensa adecuadas para mitigar el impacto del ataque simulado. 3. Realiza un análisis post-incidente detallado, identificando lecciones aprendidas y áreas de mejora en la respuesta a ciberataques.

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:

- **Debate:** 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 docente asume el rol de expositor y buscará generar el debate a través de preguntas sobre lo expuesto y desde la participación de los estudiantes.

- **Clase invertida:** con materiales didácticos dispuestos en el aula virtual previamente y aplicando en clases presenciales, analizando y respondiendo a planteamientos con estudio de casos a través de trabajos grupales, orientadas especialmente a la utilización apropiada de las diversas técnicas existentes en cada una de las fases del proceso de la extracción de conocimiento a partir de los datos, para asimilar los contenidos de la asignatura.

- **Aprendizaje** basado en proyectos: Desarrollo de proyectos para evaluar las capacidades adquiridas.

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

- Mitnick, K. (2017). El arte de la invisibilidad. Barcelona: Paidós.
- Engebretson, P. (2013). TheBasics of Hacking and PenetrationTesting: Ethical Hacking and PenetrationTestingMadeEasy. Syngress.
- Evans, L. (2018). Ciberseguridad. IndependentlyPublished.
- KA, M. (2018). Learning Malware Analysis. Packt Publishing.
- Schneier, B. (2018). ClickHere to KillEverybody: Security and Survival in a Hyper-connectedWorld. W. W. Norton &CompanyvisedLearningwith Quantum Computers. Springer. 2018
- Clark, A. J., & White, B. (2017). Blue Team Field Manual (BTFM). CreateSpaceIndependent Publishing Platform.
- Sallis, E., Caracciolo, C., & Rodríguez, M. (2018). Ethical Hacking. Un enfoque metodológico para profesionales. IndependentlyPublished.
- Salas, A. (2019). Los hombres que susurraban a las máquinas. IndependentlyPublished