RESOLUCIÓN 25/18/154-00
ACTA 1226/25/08/2025

"POR LA CUAL SE APRUEBA EL PROGRAMA DE ESTUDIO DE LA ASIGNATURA *SEGURIDAD EN HARDWARE,* 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 Hardware"***, 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:

25/18/154-01 APROBAR el Programa de Estudio de la Asignatura ***"Seguridad en Hardware"***, de carreras de Grado, Sede San Lorenzo, Filial Villarrica y Filial Coronel Oviedo, detallado en el ANEXO 116 de la presente Acta.

25/18/154-02 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 Hardware				
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

En la era digital actual, la ciberseguridad se ha convertido en un tema crucial, dado que los problemas de seguridad a nivel mundial se han vuelto una preocupación diaria. La convergencia de la informática y las comunicaciones, junto con el crecimiento exponencial en el volumen de datos en Internet, han convertido la seguridad en hardware en un área de creciente preocupación.

La seguridad en hardware aborda un amplio espectro de problemas y desafíos que abarcan todo el ciclo de vida del hardware electrónico, desde el diseño hasta la implementación. El hardware moderno, incluyendo circuitos integrados (ICs), placas de circuito impreso (PCBs) y otros componentes electrónicos, se está volviendo más complejo y distribuido globalmente, involucrando a múltiples entidades no confiables. Este contexto introduce múltiples problemas de seguridad, tales como cambios maliciosos, filtraciones de información, ataques de canal lateral, falsificación, ingeniería inversa y piratería.

El papel del hardware como ancla de confianza en los sistemas informáticos está siendo cada vez más cuestionado. Para proteger los sistemas contra estas amenazas emergentes, es esencial que los

El papel del hardware como ancla de confianza en los sistemas informáticos está siendo cada vez más cuestionado. Para proteger los sistemas contra estas amenazas emergentes, es esencial que los estudiantes y profesionales comprendan tanto los problemas de seguridad como las contramedidas disponibles.

La asignatura de Seguridad de Hardware es esencial para formar profesionales en informática capaces de enfrentar y mitigar los desafíos de seguridad en un entorno tecnológico cada vez más complejo. A través de una educación integral y práctica, los estudiantes estarán mejor preparados para contribuir al diseño y mantenimiento de sistemas informáticos seguros y confiables

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: Ataques físicos, TPM, protecciones de hardware, y seguridad en componentes críticos (CPU, RAM).

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. Introducción a la seguridad en hardware.	1.1. Descripción general de un sistema informático. 1.2. Capas de un sistema informático. 1.2.1. Hardware electrónico. 1.2.2. Tipos de hardware electrónico. 1.3. Seguridad en hardware 1.4. Ataques, vulnerabilidades y contramedidas. 1.4.1. Vectores de ataque. 1.4.2. Superficie de ataque. 1.4.3. Modelo de seguridad. 1.4.4. Vulnerabilidades 1.4.5. Contramedidas 1.5. Conflicto entre seguridad y prueba/depuración. 1.6. Evolución de la seguridad en hardware.	1. Comprende la arquitectura y las capas de un sistema informático. 2. Identifica vectores y superficies de ataque en sistemas de hardware.
2. Descripción general de la lógica combinacional, la lógica secuencial y la teoría de	2.1. Tecnología a Escala Nanométrica. 2.2. Lógica digital. 2.2.1. Lógica binaria. 2.2.2. Puerta Lógica Digital. 2.2.3. Algebra Booleana.	1. Comprende las bases de la tecnología a escala nanométrica. 2. Analiza circuitos digitales utilizando lógica binaria, puertas lógicas y álgebra booleana. 3. Entiende la interacción entre hardware, firmware y software en

Unidades	Contenidos	Resultados de aprendizaje
circuitos.	2.2.4. Circuito Secuencial. 2.3. Teoría de circuito. 2.4. ASICs, FPGA. 2.5. Sistema Embebido 2.6. Interacción entre Hardware, Firmware y Software. 2.7. Sistema en un Chip (SoC). 2.8. Placa de Circuito Impreso (PCB).	sistemas embebidos y en un chip (SoC).
3. Ataques de Hardware.	3.1. Flujo de diseño de SoC 3.2. Estructura del Troyano de Hardware. 3.2.1. Modelado de Troyanos. 3.2.2. Ejemplos de Troyanos de Hardware. 3.3. Troyanos de Hardware en Diseños FPGA. 3.4. Taxonomía de Troyanos de Hardware. 3.4.1. Fase de Inserción. 3.4.2. Nivel de Abstracción. 3.4.3. Mecanismo de Activación. 3.4.4. Payload. 3.4.5. Ubicación. 3.4.5.1. Unidad de Procesamiento. 3.4.5.2. Acelerador Criptográfico. 3.4.5.3. Unidades de Memoria. 3.4.5.4. Puerto de Entrada/Salida. 3.4.5.5. Fuente de Alimentación. 3.4.5.6. Rejilla de Reloj. 3.5. Contramedidas Contra Troyanos de Hardware. 3.6. Cadena de Suministro de Electrónica. 3.7. Ataques Side-Channel. 3.8. Ataques Orientados a Pruebas. 3.9. Ataques Físicos y Contramedidas. 3.10. Ataques en PCB.	1. Comprende el flujo de diseño de un Sistema en un Chip (SoC) y su relación con la seguridad de hardware. 2. Modela troyanos de hardware según su fase de inserción, mecanismo de activación y payload. 3. Evalua la seguridad de la cadena de suministro de electrónica y los riesgos asociados a ataques físicos y side-channel.
4. Contramedidas Contra Ataques de Hardware.	4.1. Primitivas de Seguridad en Hardware. 4.2. Función Física No Clonable. 4.3. Generador de Números Aleatorios Verdaderos. 4.4. Evaluación de Seguridad y Confianza. 4.5. Diseño para la Seguridad. 4.6. Ofuscación de Hardware. 4.7. Autenticación e Integridad del PCB.	1. Comprende las primitivas de seguridad en hardware y su aplicación. 2. Evalúa mecanismos de ofuscación de hardware y su impacto en la protección de diseños electrónicos. 3. Desarrolla estrategias de autenticación e integridad para placas de circuitos impresos (PCB).
5. Tendencias Emergentes en Ataques y	5.1. Antecedentes del Diseño de SoC. 5.2. Requisitos de Seguridad	1. Identifica requisitos de seguridad en SoC. 2. Implementa políticas de

Unidades	Contenidos	Resultados de aprendizaje
Protecciones de Hardware.	para SoC. 5.3. Aplicación de Políticas de Seguridad. 5.4. Proceso de Diseño Seguro de SoC. 5.5. Modelado de Amenazas.	seguridad. 3. Desarrolla modelos de amenazas.

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

- Tehranipoor, M. Bhunia, S.(2019). Hardware Security: A Hands-onLearningApproach, Morgan KaufmannPublishers. Elsevier.
- Tehranipoor, M., Pundir, N., Vashistha, N., &Farahmandi, F. (2023). Hardware securityprimitives. Switzerland: Springer.