RESOLUCIÓN 25/18/156-00
ACTA 1226/25/08/2025

"POR LA CUAL SE APRUEBA EL PROGRAMA DE ESTUDIO DE LA ASIGNATURA *SEGURIDAD EN SISTEMAS OPERATIVOS,* 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 Sistemas Operativos"***, 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:

25/18/156-01 APROBAR el Programa de Estudio de la Asignatura ***"Seguridad en Sistemas Operativos"***, de carreras de Grado, Sede San Lorenzo, Filial Villarrica y Filial Coronel Oviedo, detallado en el ANEXO 118 de la presente Acta.

25/18/156-02 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 Sistemas Operativos				
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

El Sistema Operativo (S.O.) provee los mecanismos fundamentales y básicos para un procesamiento computacional seguro. Desde el año 1960 se ha estado trabajando y los diseñadores han explorado y propuesto mecanismos para construir S.O seguros y así protegerlos de un motivado adversario. Actualmente, los S.O. son diseñados teniendo en mente garantizar su funcionamiento seguro y el de otros sistemas que dependen de él.

En esta asignatura se presentan los fundamentos básicos de la construcción de los S.O. teniendo en cuenta su funcionamiento seguro. Se discuten no sólo las implementaciones sino también aspectos teóricos de seguridad que forman parte del funcionamiento y concepción de los mecanismos presentes en los S.O. actuales. Se discutirán además las amenazas y ataques más comunes a los que están expuestos estos sistemas. Además, se discutirán y abordarán las mejores prácticas para hacer que los S.O. sean seguros (S.O. hardening) de acuerdo al escenario de su funcionamiento.

Se presentarán los mecanismos implementados en los sistemas operativos más exitosos del mercado y que son de uso popular.

Finalmente por medio de proyectos sencillos de carácter práctico los estudiantes podrán explorar los detalles, los conceptos y el funcionamiento de varios mecanismos y funcionalidades orientadas a mantener seguros los sistemas operativos.

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: Privilegios, administración de acceso, auditorías, parches y actualizaciones, aislamiento y contenedores.

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. 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. Aplicar, producir y difundir conocimientos técnicos y científicos en el área de la informática.

IV. ORGANIZACIÓN DE LA ASIGNATURA

Unidades	Contenidos	Resultados de aprendizaje
1. Introducción a la Seguridad en S.O..	1.1. Revisión de conceptos básicos de funcionamiento interno S.O. (Kernel, Memoria, Procesos, etc). 1.2. Componentes de seguridad (CIA) aplicados a Sistemas Operativos. 1.3. Principios de diseño de seguridad de los S.O. (Saltzer&Schoroeder) 1.4. Definiciones de control de acceso: Modelo de la matriz de Control de acceso (MCA) 1.5. Control de Acceso Mandatorio y Control de Acceso Discrecional. 1.6. Modelo de Monitor de referencia (Reference Monitor: Monitoreo de acceso: mediación completa, prueba de integridad y verificabilidad.) 1.7. Inicios de modelos de Seguridad en S.O. en Multics	1. Describe los conceptos básicos de funcionamiento interno de un S.O. 2. Describe cómo los componentes de seguridad (Confidencialidad, Integridad y Disponibilidad) son aplicados en el diseño de un S.O. 3. Describe los principios de diseño de seguridad y cómo se aplican a los sistemas operativos. 4. Describe el modelo monitor de referencia y su impacto en la seguridad de los S.O. 5. Describe los modelos de Control de Acceso actuales. 6. Aplica los modelos de Control de Acceso para problemas asociados a la implementación de Seguridad en los S.O. 7. Explica las principales contribuciones seminales de los modelos de seguridad del S.O. Multics.
2. Amenazas sobre S.O.	2.1. Protección vs. Seguridad. 2.2. Modelo de Confianza 2.3. Modelo de amenazas 2.4. Caracterización de las vulnerabilidades en los	1. Identifica las diferencias entre las cuestiones de protección y de seguridad en un S.O. 2. Describe el modelo de confianza aplicado a un S.O. 3. Describe el modelo de amenazas

Unidades	Contenidos	Resultados de aprendizaje
	S.O. CVE y CWE. 2.5. Modelos de Integridad 2.6. Principales ataques a S.O.	aplicado a un S.O. 4. Aplica los estándares CVE y CWE para identificar las amenazas y vulnerabilidades en los S.O. 5. Identifica las características de los principales ataques actuales a los S.O.
3. Seguridad en los componentes de un S.O.	3.1. Seguridad en el proceso de arranque. 3.2. Seguridad en el Kernel. 3.3. Seguridad en la Memoria. 3.4. Seguridad en los procesos. 3.5. Protección de datos 3.6. Mecanismos de aislamiento en los S.O. basados en virtualización. 3.7. Mecanismos de aislamiento en los S.O. basados en contenedores.	1. Describe los criterios e implementaciones de seguridad en el proceso de arranque de un S.O. 2. Describe los modelos de Seguridad en el Kernel de un S.O. 3. Describe los modelos de seguridad en la gestión de memoria de un S.O. 4. Describe los modelos de seguridad en los procesos de un S.O. 5. Describe los modelos de seguridad en la protección de datos. 6. Identifica los mecanismos de aislamiento utilizados en los S.O. virtualizados. 7. Identifica los mecanismos de aislamiento utilizados en los S.O. basados en contenedores.
4. Mecanismos de seguridad en S.O. actuales.	4.1. Modelo de seguridad y mecanismos en Windows. 4.2. Modelo de seguridad y mecanismos en Linux. 4.3. Modelo y mecanismos de seguridad en iOS y Android.	1. Describe el funcionamiento de los mecanismos de seguridad presentes en los S.O. Linux. 2. Describe el funcionamiento de los mecanismos de seguridad presentes en el S.O. Windows. 3. Describe el funcionamiento de los mecanismos de seguridad presentes en los S.O. iOS y Android. 4. Experimenta con los mecanismos de seguridad presentes en los S.O. actuales.
5. Gestión de Seguridad en Sistemas Operativos.	5.1. Conceptos y aspectos relevantes y automatización 5.2. Hardening en Linux y automatización 5.3. Hardening en Windows y automatización. 5.4. Gestión de parches y actualizaciones de los S.O. 5.5. S.O. confiables y Criterios Comunes (CommonCriteria)	1. Describe los aspectos más relevantes sobre el fortalecimiento de seguridad en los S.O. y cómo automatizarlos. 2. Aplica mecanismos de hardening en Linux. 3. Aplica mecanismos de hardening en Windows. 4. Prepara herramientas de gestión de parches y actualizaciones para diversos S.O. 5. Identifica los principales usos de S.O. confiables y su mapeamiento en los Criterios Comunes (CommonCriteria).

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

- M. Bishop (2018). Introduction to Computer Security. Addison Wesley.
- OperatingSystem Security (2008). TrentJaeger. Morgan &Claypool
- OperatingSystems: ThreeEasyPieces. Version 1.1 Remzi H. Arpaci-Dusseau and Andrea C. Arpaci-Dusseau (University of Wisconsin-Madison) (2023) https://pages.cs.wisc.edu/~remzi/OSTEP/
- Security Engineering: A guide to buildingdependabledistributedsystems (2020). Ross J. Anderson..
- Windows Internals, Part 1: Systemarchitecture, processes, threads, memorymanagement, and more (2017). 7th Edition. Pavel Yosifovich, Alex Ionescu Mark E. Russinovich and David A. Solomon. Microsoft Press.
- Windows Internals, Part 2 (2021). Pavel Yosifovich, Alex Ionescu Mark E. Russinovich and David A. Solomon. Microsoft Press.
- Windows Security Internals: A Deep Diveinto Windows Authentication, Authorization, and Auditing (2024). James Forshaw. Publisher: No StarchPress.
- W. Stalling& L. Brown (2018). Computer Security. Principles and Practices. 3rd Edition. Pearson Educ. Inc.
- Mastering Linux Security and Hardening. A practicalguide to protectingyour Linux systemfromcyberattacks (2023). Donald A. Tevault. ThirdEdition. Packt. Publishing.