



Campus de la UNA
SAN LORENZO-PARAGUAY

UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD POLITÉCNICA
CONSEJO DIRECTIVO

RESOLUCIÓN 25/18/157-00
ACTA 1226/25/08/2025

“POR LA CUAL SE APRUEBA EL PROGRAMA DE ESTUDIO DE LA ASIGNATURA *SEGURIDAD Y PRIVACIDAD DE DATOS*, 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 y Privacidad de Datos”**, 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.º 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:**

25/18/157-01 APROBAR el Programa de Estudio de la Asignatura **“Seguridad y Privacidad de Datos”**, de carreras de Grado, Sede San Lorenzo, Filial Villarrica y Filial Coronel Oviedo, detallado en el ANEXO 119 de la presente Acta.

25/18/157-02 COMUNICAR, copiar y archivar.

Prof. Abg. Joel Arsenio Benítez Santacruz
Secretario



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



Campus de la UNA
SAN LORENZO-PARAGUAY

UNIVERSIDAD NACIONAL DE ASUNCIÓN
FACULTAD POLITÉCNICA
CONSEJO DIRECTIVO

Resolución 25/18/157-00 Acta 1226/25/08/2025
ANEXO 119

DEPARTAMENTO DE ENSEÑANZA DE INFORMÁTICA
PROGRAMA DE ESTUDIO

I. IDENTIFICACIÓN

Nivel				Grado									
Asignatura				Seguridad y Privacidad de Datos									
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 seguridad y la privacidad de los datos son esenciales en una sociedad cada vez más digitalizada porque permiten proteger a las personas, a las empresas y a la sociedad en general. Al garantizar la protección de los datos, se pueden alcanzar los beneficios de la digitalización sin poner en riesgo la seguridad y privacidad propias y la de terceros. A través de la aplicación de métodos y técnicas los datos pueden ser gestionados sin perder de vista la seguridad. Los profesionales involucrados en tecnología deben reforzar sus conocimientos en esta área así como ofrecer servicios adecuados a los nuevos desafíos alrededor de la gestión de datos.

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: Cifrado, tokenización, gestión de claves, protección de datos en reposo y en tránsito.

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. Seguridad de datos.	1.1. Identificación y clasificación de datos. 1.1.1. Datos sensibles. 1.1.2. Clasificación de datos. 1.1.3. Estado de los datos. 1.2. Requerimientos para el manejo de datos. 1.3. Controles para la seguridad de datos.	1. Explica el concepto de datos sensibles y su relación con la privacidad y la seguridad de la información. 2. Describe los distintos niveles de clasificación de datos y los criterios utilizados para asignarlos. 3. Describe los controles de seguridad más comunes para proteger los datos y prevenir incidentes. 4. Analiza casos reales de incidentes de seguridad relacionados con la gestión de datos y proponer soluciones. 5. Compara diferentes enfoques para la clasificación y protección de datos.
2. Protección de datos.	2.1. Roles aplicados a los datos. 2.2. Ciclo de vida de la gestión de datos. 2.3. Métodos de protección de datos. 2.4. Tokenización. 2.5. Protección de datos en uso, en reposo y en tránsito.	1. Compara las diferentes perspectivas de los roles en la toma de decisiones basadas en datos. 2. Evalúa la efectividad de la colaboración entre los diferentes roles. 3. Evalúa la eficacia de un plan de gestión de datos existente. 4. Identifica posibles cuellos de botella en el ciclo de vida. 5. Selecciona los métodos de protección adecuados para diferentes tipos de datos y escenarios. 6. Implementa medidas de protección de datos en un sistema de información. 7. Compara diferentes enfoques de tokenización. 8. Implementa medidas de seguridad para proteger los datos en cada estado. 9. Desarrolla una estrategia integral de protección de datos que abarque los tres estados.
3. Criptografía y	3.1. Fundamentos de la	1. Selecciona las técnicas

Unidades	Contenidos	Resultados de aprendizaje
aplicaciones.	criptografía. 3.2. Cifrado simétrico y asimétrico. 3.3. Funciones Hash. 3.4. Firma digital y la Infraestructura de Clave Pública y Privada. 3.5. Gestión de claves. 3.6. Criptografía aplicada.	criptográficas adecuadas para proteger diferentes tipos de información. 2. Implementa un esquema de cifrado simétrico y asimétrico para proteger la comunicación entre dos partes. 3. Evalúa las ventajas y desventajas de cada tipo de cifrado en diferentes escenarios. 4. Crea y verifica firmas digitales. 5. Utiliza una PKI para gestionar certificados digitales. 6. Evalúa la seguridad de un sistema criptográfico existente. 7. Propone mejoras a un sistema criptográfico.

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

- NIST Cybersecurity Framework (CSF) 2.0. 2024
- ISO/IEC 27001:2022 Informationsecurity, cybersecurity and privacyprotection — Informationsecuritymanagementsystems — Requirements. 2022



- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls. 2022.

