RESOLUCIÓN 25/18/144-00
ACTA 1226/25/08/2025

"POR LA CUAL SE APRUEBA EL PROGRAMA DE ESTUDIO DE LA ASIGNATURA *INFORMÁTICA FORENSE,* 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 **"Informática Forense",** 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:

25/18/144-01 APROBAR el Programa de Estudio de la Asignatura **"Informática Forense",** de carreras de Grado, Sede San Lorenzo, Filial Villarrica y Filial Coronel Oviedo, detallado en el ANEXO 106 de la presente Acta.

25/18/144-02 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	Informática Forense				
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 informática forense es una disciplina que combina la informática y la ciencia forense jurídica para recopilar, preservar, analizar y presentar pruebas digitales de manera que sean admisibles en un tribunal, cuyo objetivo principal es investigar delitos cibernéticos y otros incidentes relacionados con la tecnología, asegurando que las evidencias digitales sean manejadas correctamente para mantener su integridad y validez legal.

Las competencias fundamentales de la asignatura se centran en desarrollar habilidades y conocimientos esenciales para comprender y abordar los delitos relacionados con la tecnología y la informática.

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: Recuperación de datos, análisis post-incidente, herramientas forenses y cadena de custodia.

III. COMPETENCIAS DEL PERFIL DE EGRESO ASOCIADAS

1. Comunicarse en las lenguas oficiales del país y en una lengua extranjera.
2. Liderar y trabajar en equipo con eficacia y responsabilidad tomando decisiones basadas en evidencias.
3. 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.
4. 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. Conceptos Básicos.	1.1. La ciencia forense. 1.2. Análisis Forense Digital. 1.3. Historia y evolución. 1.4. Incidente de seguridad informática, tipos de ataque. 1.5. Clasificación de Delitos Informáticos.	1. Define con precisión qué es la informática forense y su propósito dentro de las investigaciones digitales. 2. Comprende la evolución de la informática forense, identificando hitos clave que han influido en el desarrollo de esta área. 3. Comprende la importancia de la efectividad de las medidas de seguridad existentes y proponer mejoras basadas en los resultados de pruebas de penetración y simulacros de incidentes. 4. Identifica los tipos de ataque y la clasificación de este dentro del delito.
2. Principios Legales y Marco Normativo.	2.1. Leyes y regulaciones relacionadas con la evidencia digital. 2.2. Introducción a las leyes de cibercrimen y protección de datos en general. 2.3. Normas y estándar internacional (ISO/IEC 27037). 2.4. Marco legal en nuestro País para delitos cometidos por medios informáticos. 2.5. Procedimientos legales para la recolección de evidencia digital. 2.6. Elaboración correcta de Informes.	1. Identifica las principales leyes y regulaciones relacionadas con el cibercrimen a nivel global y nacional. 2. Conoce los procedimientos legales para la recolección de evidencias. 3. Elabora correctamente los informes obtenidos para su correcta presentación a las autoridades pertinentes.

Unidades	Contenidos	Resultados de aprendizaje
3. Levantamiento de evidencias, pericias.	3.1. Principios Básicos de una pericia. 3.2. Características principales de una pericia. 3.3. Reconocimiento de una evidencia digital. 3.4. Procedimientos antes, durante (escena del delito) y después de una recolección de evidencia. 3.5. Situaciones con diferentes tipos de equipos. 3.6. Conservación de evidencia, cadena de custodio.	1. Comprende las importancias de los principios de un experto en cuanto a la objetividad de la información y sus implicancias en contextos judiciales. 2. Aplica los procedimientos adecuados en todas las etapas de pericia desde el levantamiento de la evidencia hasta la finalización de la causa. 3. Comprende la importancia de la integridad de la evidencia.
4. Limpieza forense, borrado seguro, recuperación de archivo.	4.1. Proceso lógico. 4.2. Proceso Físico. 4.3. Recuperación de archivos.	1. Analiza el comportamiento de los datos en cuanto a su permanencia en el equipo 2. Aprende a utilizar las herramientas para limpieza segura de datos o recuperación de estos.
5. Análisis forense de sistemas libres y propietarios.	5.1. Análisis del sistema operativo para encontrar artefactos (artifacts), búsqueda de archivos específicos con herramienta seleccionada.	1. Aprende a recorrer las pistas en el sistema de tal forma a poder encontrar el elemento necesario para una investigación.

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:

- **Estudios de casos:** donde el estudiante deberá aplicar los conocimientos adquiridos a las problemáticas del contexto**.**

- **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

- Fisher, T. (2023). Data SanitizationMethods. A list of software based data destructionmethods. LifeWire. Recuperado de:https://www.lifewire.com/data-sanitization-methods-2626133.
- Domínguez, F. (2014). Introducción a la Informática Forense. Ra-Ma S.A. Editorial y Publicaciones. Madrid, España.
- Introducción a la informática forense. Dr. Santiago Acurio del pino, director nacional de tecnologías de la información de la fiscalía general del estado. 2009
- ISO/IEC 27037: InformationTechnology - Security Techniques - GuidelinesforIdentification, Collection, Acquisition, and Preservation of Digital Evidence
- Guide to ComputerForensics and Investigations de Bill Nelson, Amelia Phillips, Christopher Steuart
- Thebestpracticesforseizingelectronicevidence, versión 3.0, us. department of home landsecurity, and theunitedstatessecretservice
- Análisis Forense Digital, publicado, autor Miguel López Delgado, publicado en junio 2007 (segunda edición).