RESOLUCIÓN 25/18/142-00
ACTA 1226/25/08/2025

"POR LA CUAL SE APRUEBA EL PROGRAMA DE ESTUDIO DE LA ASIGNATURA *GESTIÓN DE SISTEMAS DE SEGURIDAD,* 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 **"Gestión de Sistemas de Seguridad",** 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:

25/18/142-01 APROBAR el Programa de Estudio de la Asignatura **"Gestión de Sistemas de Seguridad",** de carreras de Grado, Sede San Lorenzo, Filial Villarrica y Filial Coronel Oviedo, detallado en el ANEXO 104 de la presente Acta.

25/18/142-02 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	Gestión de Sistemas de Seguridad				
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 despliegue de tecnología y conectividad ha puesto en un punto de interés la ciberseguridad. Esta área está en permanente análisis y evolución por parte de proveedores y desarrolladores de servicios, como las diversas áreas de las organizaciones y sus clientes. La ciberseguridad es tan amplia que abarca no solo aspectos técnicos, sino legales y culturales. Esta situación obliga a que los profesionales involucrados en áreas de tecnologías cuenten con aptitudes que les permitan incorporar criterios de ciberseguridad en cualquier tipo de emprendimiento que involucre tecnología.

El curso se enfoca en incorporar los principios y fundamentos de la ciberseguridad a través de laboratorios y trabajos prácticos. Se da particular énfasis a la elaboración de trabajos de investigación aplicando metodologías de investigación.

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,

temáticos, se incluyen conceptos fundamentales como: Políticas, gestión de identidad, protocolos de respuesta a incidentes, auditorías de seguridad.

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. Política de seguridad organizacional.	1.1. La seguridad como apoyo estratégico a los fines de la organización. 1.2. Política de Seguridad en la Organización 1.3. Política de la gestión de riesgos en la organización. 1.4. Actualización de la política de gestión de riesgos para responder a los cambios. 1.5. Establecimiento, comunicación y revisión de la Política de Seguridad 1.6. La política de seguridad como parte de estándares de seguridad.	1. Evalúa el impacto de los incidentes de seguridad en la reputación y rentabilidad de una organización. 2. Evalúa la efectividad de una política de seguridad existente. 3. Revisa y actualiza el plan de tratamiento de riesgos de forma periódica. 4. Adapta la política de gestión de riesgos a los cambios en el entorno empresarial. 5. Establece un proceso para la creación, aprobación y comunicación de la política de seguridad. 6. Utiliza los estándares de seguridad como referencia para el desarrollo de la política de seguridad.
2. Gestión de Identidad.	2.1. Definición de incidente. 2.2. Pasos para la gestión de incidentes. 2.3. Implementación de medidas de detección y prevención. 2.4. Registro y monitoreo. 2.5. Automatización en la respuesta a incidentes.	1. Clasifica un evento como incidente de seguridad basado en criterios establecidos. 2. Implementa cada fase del ciclo de vida de la gestión de incidentes en un escenario real o simulado. 3. Implementa controles de acceso y autenticación. 4. Analiza los datos de registro para identificar patrones y anomalías. 5. Analiza los datos de registro para identificar patrones y anomalías.
3. Protocolos de respuesta a incidentes.	3.1. Definición de incidente. 3.2. Pasos para la gestión de incidentes. 3.3. Implementación de medidas de detección y prevención. 3.4. Registro y monitoreo. 3.5. Automatización en la respuesta a incidentes.	1. Clasifica un evento como incidente de seguridad basado en criterios establecidos. 2. Documenta los pasos tomados durante la gestión de un incidente. 3. Configura y utiliza herramientas de detección de incidentes. 4. Analizar los datos de registro para

Unidades	Contenidos	Resultados de aprendizaje
		identificar patrones y anomalías. 5. Utiliza herramientas de automatización para responder a incidentes de forma rápida y eficiente.
4. Auditorías de Seguridad.	4.1. Construcción del programa para evaluar y probar la seguridad 4.2. Auditorías internas, externas y de terceros. 4.3. Realizar la evaluación de vulnerabilidades. 4.4. Test de seguridad del software 4.5. Implementación del proceso de gestión de seguridad.	1. Integra las diferentes actividades de evaluación y pruebas en un plan coherente. 2. Selecciona y contrata a auditores externos. 3. Desarrolla planes de remediación para las vulnerabilidades identificadas. 4. Diseña y ejecuta pruebas de seguridad de software. 5. Integra el programa de evaluación y pruebas de seguridad en el SGSI.

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 Informationsecurity, cybersecurity and privacyprotection — Informationsecuritycontrols. 2022