RESOLUCIÓN 25/18/107-00
ACTA 1226/25/08/2025

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

25/18/107-01 APROBAR el Programa de Estudio de la Asignatura **"Seguridad Informática"**, de carreras de Grado, Sede San Lorenzo, Filial Villarrica y Filial Coronel Oviedo, detallado en el ANEXO 69 de la presente Acta.

25/18/107-02 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

1. IDENTIFICACIÓN

Nivel	Grado				
Asignatura	Seguridad Informática				
Carrera	**Plan**	**Sede/Filial**	**Carácter**	**Semestre**	**Prerrequisitos**
Ingeniería en Informática	2026	Sede San Lorenzo	Obligatoria	Quinto	Redes de Computadoras
Licenciatura en Ciencias Informáticas	2026	Sede San Lorenzo/Filial Villarrica/Filial Coronel Oviedo	Obligatoria	Cuarto	Fundamentos de Redes de Computadoras

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 Informática se ha convertido en uno de los pilares fundamentales de la tecnología de la información en la sociedad actual. La creciente dependencia de sistemas digitales y la interconexión a nivel global han dado lugar a una proliferación de amenazas cibernéticas que van desde el robo de datos confidenciales hasta la interrupción de servicios críticos. En este contexto, la asignatura Seguridad Informática se presenta como un componente esencial de la formación de profesionales en el campo de la informática y la tecnología.

La asignatura en cuestión se fundamenta en los siguientes aspectos:

- **Relevancia en la actualidad:** La sociedad actual se encuentra altamente digitalizada, con organizaciones y personas dependientes de sistemas informáticos y de comunicación. La pérdida de datos sensibles, el robo de información, la interrupción de servicios y otros ataques cibernéticos pueden tener consecuencias graves en la privacidad y la seguridad de la información. La asignatura Seguridad Informática es esencial para preparar a los estudiantes a abordar estos desafíos y proteger la integridad y confidencialidad de la información.

- **Demanda en el mercado laboral:** La seguridad informática se ha convertido en un campo altamente demandado en el mercado laboral. Las organizaciones buscan profesionales con conocimientos sólidos en seguridad para garantizar la protección de sus activos digitales. La asignatura

Unidades	Contenidos	Resultados de aprendizaje
2. ontrol de acceso y autenticación.	2.1. Modelos de autenticación. 2.2. Control de acceso y autorización. 2.3. Autenticación multifactor (MFA). 2.4. Sistemas de gestión de identidad (IAM).	1. Implementa sistemas de autenticación segura, incluyendo autenticación multifactor (MFA) en un entorno de red. 2. Diseña y configura políticas de control de acceso que restrinjan adecuadamente el acceso a recursos sensibles.
3. riptografía.	3.1. Principios de criptografía. 3.2. Tipos de cifrado: simétrico y asimétrico. 3.3. Algoritmos criptográficos. 3.4. Protocolos criptográficos.	1. Aplica algoritmos criptográficos para cifrar y descifrar datos, protegiendo así la confidencialidad de la información. 2. Gestiona adecuadamente las claves criptográficas y valora la importancia de la seguridad de las claves.
4. eguridad en servidores.	4.1. Configuración segura de servidores. 4.2. Detección de intrusiones y prevención. 4.3. Actualizaciones y parches de seguridad. 4.4. Seguridad en servidores web y bases de datos.	1. Configura servidores de manera segura, aplicando prácticas recomendadas para prevenir intrusiones y proteger la integridad de los datos. 2. Evalúa y aplica actualizaciones y parches de seguridad en servidores.
5. nfraestructura de Clave Pública (PKI).	5.1. Conceptos de PKI. 5.2. Certificados digitales. 5.3. Autoridades de certificación (CA). 5.4. Implementación de PKI.	1. Implementa una infraestructura PKI, incluyendo la emisión y gestión de certificados digitales. 2. Explica y aplica los conceptos de autoridades de certificación (CA) en la infraestructura PKI.
6. eguridad en las redes de computadoras.	2.1. Modelos de seguridad de red. 2.2. Firewalls y sistemas de detección de intrusiones (IDS/IPS). 2.3. VPN (Redes Privadas Virtuales). 2.4. Seguridad inalámbrica.	1. Diseña y configura soluciones de seguridad de red, incluyendo firewalls y VPN, para proteger la red y los datos. 2. Identifica amenazas y aplica medidas de seguridad inalámbrica.
7. eguridad en las aplicaciones.	7.1. Principios de seguridad en desarrollo de software. 7.2. Pruebas de seguridad de aplicaciones. 7.3. Protección contra ataques web (SQL injection, XSS, CSRF). 7.4. Desarrollo seguro de aplicaciones.	1. Desarrolla aplicaciones seguras, incorporando prácticas de seguridad en el ciclo de desarrollo de software. 2. Identifica y corrige vulnerabilidades comunes en aplicaciones web.
8. plicaciones y herramientas en la seguridad de redes.	8.1. Herramientas de análisis de tráfico. 8.2. Escaneo de vulnerabilidades. 8.3. Monitorización de eventos de seguridad.	1. Utiliza herramientas de análisis de tráfico, escaneo de vulnerabilidades y monitorización de eventos de seguridad. 2. Gestiona registros de seguridad

Unidades	Contenidos	Resultados de aprendizaje
	8.4. Gestión de logs y registros.	y lleva a cabo investigaciones de incidentes utilizando herramientas forenses.
9. nálisis forense.	2.1. Análisis forense digital. 2.2. Herramientas forenses. 2.3. Investigación de incidentes de seguridad. 2.4. Cadena de custodia y preservación de evidencia.	1. Realiza un análisis forense digital completo, incluyendo la recopilación y preservación de evidencia digital. 2. Identifica y documenta hallazgos en una investigación de incidentes de seguridad.
3. valuación y gestión de seguridad.	3.1. Evaluación de riesgos. 3.2. Gestión de seguridad: políticas, estándares y procedimientos. 3.3. Cumplimiento normativo. 3.4. Plan de respuesta a incidentes.	1. Evalúa riesgos de seguridad y propone medidas de mitigación adecuadas. 2. Desarrolla y gestiona políticas de seguridad, así como un plan de respuesta a incidentes.

VI. 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:

- **Clases Magistrales:** 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 docente asume el rol de expositor y buscará generar el debate a través de preguntas sobre lo expuesto y desde la participación de los estudiantes.
- **Aula Invertida:** se proporcionará a los estudiantes acceso a materiales de aprendizaje, como videos, lecturas y ejercicios a ser accedidos mediante una planificación. Estos recursos cubrirán los conceptos técnicos fundamentales de la asignatura.
- **Trabajos Colaborativos:** se realizarán trabajos prácticos por temáticas en equipos, se busca la cooperación y el trabajo grupal, incentivando la designación de roles y responsabilidades dentro de un equipo de trabajo, el compromiso grupal para el logro del objetivo del trabajo y la práctica de aplicación de la teoría a problemas reales para permitir validar la teoría con la práctica.
- **Estudios de casos:** se presentan varios estudios de casos de investigación que han aplicado diferentes tecnologías, permite identificar al estudiante un escenario real de aplicación, comprender la manera de cómo encarar la resolución de un problema en un escenario real y aprender en base a la experiencia previa de trabajos de investigación publicados.

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.

VII. ESTRATEGIAS EVALUATIVAS

Procesos de producción grupales, pruebas individuales y grupales orales y/o escritas y/o prácticas durante el desarrollo de las unidades con diálogos, interpretaciones y desarrollo de tareas que los estudiantes realicen sobre los contenidos, 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.

VI. MEDIOS AUXILIARES

Pizarras, marcadores, computadoras, equipo multimedia, aula virtual, entornos de laboratorio virtual, videos educativos, herramientas de simulación, software de seguridad, herramientas de prueba de penetración.

VI. BIBLIOGRAFÍA

- Center for Internet Security. (2022). CIS Critical Security Controls, Version 8.0. Center for Internet Security.
- Introduction to Computer Security (2018). M. Bishop Addison Wesley.
- Computer Security. Principles and Practices (2018). W. Stalling& L. Brown. 3rd Edition. Pearson Educ. Inc.