RESOLUCIÓN 24/26/81-00
ACTA 1208/16/12/2024

"POR LA CUAL SE APRUEBA EL PROGRAMA DE ESTUDIO DE LA ASIGNATURA *CIBERSEGURIDAD*, DE LA CARRERA LICENCIATURA EN CIENCIAS INFORMÁTICAS – PLAN 2023 DE LA FP-UNA"

VISTO: El Memorando DA/2437/2024 del Director Académico de la FP-UNA, Prof. MSc. Felipe Santiago Uzabal Escurra, con el cual remite el Memorando CCPTCC/036/2024 de la Comisión Coordinadora del Proyecto de Transformación Curricular de Carreras de Grado de la FP-UNA, en el que presenta la propuesta de Programas de Estudio de las Asignaturas de la Carrera Licenciatura en Ciencias Informáticas.

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 **"Ciberseguridad"**, de la carrera Licenciatura en Ciencias Informáticas – Plan 2023, cuyo plan de estudio ya fue aprobado por el Consejo Superior Universitario.

EL CONSEJO DIRECTIVO DE LA FACULTAD POLITÉCNICA
RESUELVE:

24/26/81-01 APROBAR el Programa de Estudio de la Asignatura **"Ciberseguridad"**, de la carrera Licenciatura en Ciencias Informáticas – Plan 2023 de la FP-UNA, detallado en el ANEXO 73 de la presente Acta.

24/26/81-02 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

Asignatura	Ciberseguridad				
Carrera	**Plan**	**Sede/Filial**	**Carácter**	**Semestre**	**Prerrequisitos**
Licenciatura en Ciencias Informáticas	2023	Sede San Lorenzo / Filial Villarrica / Filial Coronel Oviedo	Electiva	***	Haber acumulado la cantidad de créditos académicos que corresponda a la aprobación de todas las asignaturas hasta el 5° semestre, resultante de la aplicación del Sistema Nacional de Créditos Académicos–Paraguay en la UNA.
Horas semanales	4				
Total de horas teóricas semestral	50				
Total de horas prácticas semestral	22				
Total de horas semestral	72				
Valor en créditos académicos	La valoración en créditos académicos será comunicada en su oportunidad ajustada al Reglamento General del Sistema de Créditos Académicos de la UNA, el cual se encuentra en proceso de elaboración conforme a las disposiciones de la Resolución CONES N° 221/2024, en su artículo N° 10.				
Actualización	Al egreso de la primera cohorte.				

II. FUNDAMENTACIÓN

La ciberseguridad se ha convertido en un pilar esencial en la era digital, donde la información y la tecnología desempeñan un papel fundamental en la mayoría de las actividades humanas. En este contexto, la creciente interconexión de sistemas y la sofisticación de las amenazas cibernéticas exigen profesionales altamente capacitados que comprendan a fondo los principios, las metodologías y las tecnologías necesarias para salvaguardar la información y los recursos digitales.

La creciente complejidad de los entornos tecnológicos ha llevado consigo un aumento significativo en las vulnerabilidades y amenazas cibernéticas. Desde ataques dirigidos por actores estatales hasta amenazas más comunes, como ransomware y phishing, la ciberseguridad se ha convertido en un desafío constante. Por tanto, la formación en este campo no solo es una necesidad, sino también un imperativo para garantizar la confianza y la integridad de los sistemas de información.

Esta asignatura de Ciberseguridad proporciona a los estudiantes un conocimiento integral de las diversas áreas críticas para la protección de la información. Desde la identificación de vulnerabilidades hasta la respuesta a incidentes y la aplicación de técnicas éticas de hacking, los estudiantes se sumergirán en un

enfoque práctico y teórico que les permitirá enfrentar los desafíos dinámicos y siempre cambiantes del panorama cibernético.

El desarrollo de habilidades éticas en hacking no solo se aborda como una capacidad técnica, sino como un medio para comprender las tácticas que los actores maliciosos emplean. Esto no solo fortalece la capacidad de defensa, sino que también promueve la conciencia ética y la responsabilidad en el uso de estas habilidades.

Además, la inclusión de temas como la gestión de eventos de seguridad, el monitoreo proactivo y la implementación de sistemas de detección y prevención de intrusos reflejan la necesidad de adoptar un enfoque holístico para garantizar la seguridad. Esto implica no solo reaccionar ante las amenazas, sino también anticiparse y prevenir activamente los posibles ataques.

En resumen, esta asignatura tiene como objetivo formar profesionales de la ciberseguridad que no solo sean capaces de abordar los desafíos actuales, sino que estén preparados para evolucionar con el panorama cibernético en constante cambio. La ética, la proactividad y la comprensión integral de la ciberseguridad son los pilares sobre los cuales se construye esta formación, proporcionando a los estudiantes las herramientas necesarias para proteger y fortalecer la infraestructura digital en un mundo cada vez más interconectado.

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:Análisis de vulnerabilidades, gestión de incidentes de seguridad, práctica de hacking ético, pen testing, monitoreo de seguridad, SIEM administración de eventos e información de seguridad, IDS sistemas de detección de intruso, e IPS sistema de prevención de intruso.

III. COMPETENCIAS DEL PERFIL DE EGRESO ASOCIADAS

1. Seleccionar, utilizar y construir instrumentos innovadores asociados al ejercicio de las ciencias informáticas.
2. Planificar, proyectar, diseñar y ejecutar proyectos sostenibles e integrales para la resolución de problemas, la mejora y la innovación en el ámbito de las ciencias informáticas.
3. Aplicar en la práctica profesional los valores humanos, la ética y los mecanismos de seguridad laboral.

IV. ORGANIZACIÓN DE LA ASIGNATURA

Unidades	Contenidos	Resultados de aprendizaje
1. Análisis de Vulnerabilidades.	1.1. Exploración de técnicas de identificación de vulnerabilidades. 1.2. Evaluación de riesgos y priorización de mitigaciones. 1.3. Casos prácticos de análisis de sistemas y redes.	1. Explora técnicas de identificación de vulnerabilidades, aplicando diversas metodologías y herramientas avanzadas. 2. Evalúa riesgos asociados a vulnerabilidades, considerando impacto y probabilidad de explotación. 3. Aplica conocimientos en casos prácticos de análisis de sistemas y redes, demostrando habilidades en situaciones del mundo real.
2. Gestión de Incidentes de Seguridad.	2.1. Desarrollo de protocolos de respuesta a incidentes. 2.2. Simulaciones de incidentes para la toma de decisiones efectivas. 2.3. Recuperación y lecciones aprendidas.	1. Desarrolla protocolos de respuesta a incidentes, estableciendo procedimientos efectivos para abordar amenazas de seguridad. 2. Participa en simulaciones de incidentes, aplicando los

Unidades	Contenidos	Resultados de aprendizaje
		protocolos establecidos para tomar decisiones informadas y eficientes. 3. Maneja procesos de recuperación post-incidente, identificando lecciones aprendidas y mejoras para fortalecer la postura de seguridad.
3. Práctica de Hacking Ético y Pen Testing.	3.1. Metodologías éticas para pruebas de penetración. 3.2. Laboratorios prácticos para el desarrollo de habilidades. 3.3. Énfasis en la ética y legalidad en la aplicación de técnicas de hacking.	1. Aplica metodologías éticas en pruebas de penetración, siguiendo un enfoque estructurado y autorizado. 2. Participa en laboratorios prácticos para el desarrollo y perfeccionamiento de habilidades de hacking ético. 3. Enfatiza la ética y legalidad en la aplicación de técnicas de hacking, asegurando prácticas responsables y conformes a normativas.
4. Monitoreo de Seguridad y SIEM.	4.1. Estrategias para el monitoreo proactivo de eventos de seguridad. 4.2. Configuración y administración de Sistemas de Información y Eventos de Seguridad (SIEM). 4.3. Interpretación y acción basada en datos de seguridad.	1. Explora técnicas de identificación de Desarrollar estrategias efectivas para el monitoreo proactivo de eventos de seguridad, anticipando posibles amenazas. 2. Configura y administra Sistemas de Información y Eventos de Seguridad (SIEM), asegurando una recopilación y análisis eficientes de datos. 3. Interpreta datos de seguridad generados por SIEM y tomar acciones basadas en análisis significativos para mantener la integridad y disponibilidad de los sistemas.
5. IDS - Sistemas de Detección de Intrusos e IPS - Sistema de Prevención de Intrusos.	5.1. Despliegue y configuración de sistemas IDS/IPS. 5.2. Análisis de alertas y respuestas efectivas. 5.3. Integración de sistemas de prevención de intrusos en la arquitectura de seguridad.	1. Despliega y configura sistemas de Detección de Intrusos (IDS) y sistemas de Prevención de Intrusos (IPS) de manera efectiva. 2. Analiza alertas generadas por IDS y responder de manera rápida y eficiente a posibles amenazas. 3. Integra sistemas de prevención de intrusos en la arquitectura de seguridad, fortaleciendo las defensas y reduciendo la superficie de ataque.

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:

- **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, principalmente sobre el uso de los comandos y su sintaxis. 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 publicados en la plataforma establecida, a ser accedidos mediante una planificación. Estos recursos cubrirán algunos de los conceptos teóricos fundamentales de la asignatura.

La elección particular de la estrategia didáctica aplicada será explícita en el plan de clases, 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 de Evaluación vigente en la institución que prevé valoraciones de proceso y final.

VII. MEDIOS AUXILIARES

Aula virtual, pizarrón, proyector, marcadores, equipo de audio, ordenadores, wifi, celulares, plataformas de videoconferencia, salas de chats.

VIII. BIBLIOGRAFÍA

- Romero Castro, M. I., Figueroa Morán, G. L., Vera Navarrete, D. S., Álava Cruzatty, J. E., Parrales Anzúles, G. R., Álava Mero, C. J., Murillo Quimiz, A. L., & Castillo Merino, M. A. (2018). Introducción a la seguridad informática y el análisis de vulnerabilidades.
- Chicano Tejada, E. (2022). Gestión de incidentes de seguridad informática. MF0488_3 (2ª Ed.)
- González Pérez, P. (2015). Ethical Hacking: Teoría y práctica para la realización de un pentesting.
- Quintero Martínez, M. I., & Tovar Balderas, S. A. (2019). Sistemas de gestión de información y eventos de seguridad (SIEM).
- Moreno García, M. (2022). Gestión de incidentes de ciberseguridad
- Clark, A. J., & White, B. (2017). Blue Team Field Manual (BTFM).
- Scolink, H. (2018). Qué es la seguridad informática.
- Fritzsche, K., Schneiderbauer, S., Bubeck, P., Kienberger, S., Buth, M., Zebisch, M., & Kahlenborn, W. (2018). El libro de la vulnerabilidad: Concepto y lineamientos para la evaluación estandarizada de la vulnerabilidad.