Especialización en Ciberseguridad y Redes – Modalidad a distancia

SEGURIDAD y PRIVACIDAD EN REDES **Año 2024**	Carga horaria: 100 hs. Cantidad de horas presenciales/VC: 40 hs. Cantidad de horas de actividades en línea y de trabajo final: 60 hs.

OBJETIVOS GENERALES

Cubrir los principales aspectos relacionados con la seguridad y la privacidad de las redes de datos, incluyendo aspectos relacionados con la seguridad de los servicios que se prestan así como conceptos de seguridad ligados a las organizaciones.
Los conceptos tratados porque dan una visión general de los problemas de seguridad a distintos niveles: usuarios, arquitectura de red, servicios, aplicaciones; y la forma de minimizar el riesgo que éstos suponen.

Pre-requisitos:
Conocimientos de Redes IP y de Sistemas Operativos. Manejo de lenguajes de programación.

COMPETENCIAS A DESARROLLAR EN RELACIÓN CON EL OBJETIVO DE LA CARRERA

CB3 - Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios

CEC1 - Capacidad para comprender el funcionamiento del nivel de red de las redes IP en el contexto de Internet y las redes seguras con soporte de calidad de servicio.

CEC2 - Capacidad para conocer el estado actual de la tecnología relacionada con la seguridad en redes de telecomunicación, analizando las amenazas a la seguridad de acceso y de la propia red en Internet y en las redes IP.

CONTENIDOS MÍNIMOS

Concepto y Alcance de Seguridad.
Criptografía. Inteligencia Artificial en Seguridad
Técnicas de descubrimiento

Seguridad en las aplicaciones

PROGRAMA ANALITICO

Módulo 1: Introducción
Conceptos básicos de seguridad.
Criptografía. Criptografía poscuántica
Estándares y recomendaciones
PKI-PGP y estenografía

Módulo 2: Inteligencia Artificial en Seguridad
Detección de amenazas y análisis de comportamiento
Respuesta automática y orquestación
Predicción de amenazas
Identificación y autenticación biométrica
Análisis de vulnerabilidades y pentesting automatizado
IA generativa y Ciberseguridad

Módulo 3: Técnicas
Técnicas de descubrimiento
Técnicas de Sniffing
Aplicaciones Web
Firewall, honeypots e IDS

Módulo 4: Gestión de la Seguridad
Privacidad de la Información y Gobernanza de datos
Desarrollo seguro de software
Inteligencia Artificial y Gestión de la seguridad
Casos de estudio

MODALIDAD DE ENSEÑANZA

La metodología se basa en clases sincrónicas a través del sistema contemplado en el SIED de la Facultad de Informática de la UNLP, combinadas con sesiones en el laboratorio remoto para aplicar los conceptos teóricos y que así el alumno adquiera las competencias y habilidades sobre cada uno de los temas que forman parte del contenido de la asignatura.

Las actividades prácticas desarrolladas consisten en talleres de trabajo y trabajos prácticos que resuelven los alumnos y cuyas resoluciones son tareas de entrega obligatoria. Respecto de los talleres, se instrumentan dentro de una sala de cómputo y en forma virtual por medio de técnicas de virtualización, abarcan desde la instalación y configuración de las

herramientas requeridas hasta la resolución de los problemas planteados y la anotación de las conclusiones.
Se proveen guías de instalación y configuración. Son pasos guiados que no requieren conocimientos previos de los alumnos y la guía sirve para una posterior implementación por parte del alumno en un ambiente productivo. En todos los casos se proveen máquinas virtuales, entorno y emuladores en caso de ser necesario.

RECURSOS Y MATERIALES DE ESTUDIO

Como materiales de estudio, se dispone de:

- Presentaciones multimedia desarrolladas ad-hoc para introducir cada uno de los diferentes ejes temáticos.
- Ejemplos donde se aplican los conceptos teóricos
- Ejercicios prácticos que son desarrollados en clase
- Material de lectura para estudiar y profundizar conceptos abordados en las clases
- Enlaces a artículos de actualidad en repositorios reconocidos en el área

ACTIVIDADES EXPERIMENTALES Y APROPIACIÓN DE SABERES

Los trabajos experimentales pueden desarrollarse en cada clase o continuar en más de una clase. Parten de un cuestionario planteado para cada tema donde se resumen preguntas conceptuales, ejercicios prácticos o resolución de problemas y que es discutido a través del entorno virtual, con el docente conectado respondiendo dudas y consultas.
Estos trabajos pretenden desarrollar y/o fortalecer las aptitudes de opinión crítica en los temas relativos del curso. Los alumnos deberán sintetizar su comprensión de los temas, al realizar correctamente la tarea experimental propuesta.
También se pretende desarrollar la capacidad de poder comunicar y transmitir los resultados, en presentaciones pautadas a lo largo del curso.

MODALIDAD DE EVALUACIÓN

La modalidad de evaluación consiste en un trabajo final que se inicia con una propuesta de investigación o desarrollo por parte de cada estudiante, donde elige trabajar un tema vinculado a su labor profesional o interés de estudio y que implique aplicar los conceptos adquiridos en el curso.
Este trabajo debe presentarse con formato de paper científico, esto es, con una limitación de páginas, estructura de secciones, bibliografía debidamente referenciada y conclusiones.
Eventualmente, puede requerirse un coloquio individual con docentes para exponer el trabajo.

BIBLIOGRAFÍA

- ISO27000 family of information security standards. ISO 27001: 2005.
- Cryptography and Network Security, 4/E William Stallings – Publisher:PrenticeHall - Copyright: 2006
- Network security assessment Chris McNab O'Reilly
- Network Inside Perimeter: The Definitive Guide to Firewalls, VPNs, Routers and Instrusion Detection Systems– Northcutt, Zeltser, Winters, Frederic, Ritchey New Riders 2003
- OWASP Testing Guide 2002-2008 OWASP Foundation - Creative Commons Attribution-ShareAlike 3.0 license Architecture, 6th Edition, 2013.Prentice Hall
- https://csrc.nist.gov/Projects/Post-Quantum-Cryptography
- Cloudflare Research: Post-Quantum Key Agreement. https://pq.cloudflareresearch.com
- Y. Bengio, A. Courville and P. Vincent, "Representation Learning: A Review and New Perspectives," in IEEE Transactions on Pattern Analysis and Machine Intelligence, vol. 35, no. 8, pp. 1798-1828, Aug. 2013, doi: 10.1109/TPAMI.2013.50.
- https://www.marktechpost.com/2023/03/21/a-history-of-generative-ai-from-gan-to-gpt-4/
- “AI in Cybersecurity" edited by Leslie F. Sikos, Intelligent Systems Reference Library (ISRL, volume 151). Springer
- Halder, S. and Ozdemir, S. (2018) Hands-On Machine Learning for Cybersecurity. 1st edn. Packt Publishing. Available at: https://www.perlego.com/book/868340/handson-machine-learning-for-cybersecurity-safeguard-your-system-by-making-your-machines-intelligent-using-the-python-ecosystem-pdf (Accessed: 14 October 2022).
- Artificial Intelligence and Cybersecurity: Theory and Applications 1st ed. 2023 Edición
- de Tuomo Sipola (Editor), Tero Kokkonen (Editor), Mika Karjalainen (Editor), Springer, ISBN-13, 978-3031150296
- The Cybersecurity Dilemma: Hacking, Trust and Fear Between Nations 1st Edición de Ben Buchanan (Author), Springer, ISBN-13 978-0190665012
- Melaku, Henock Mulugeta. 2023. "A Dynamic and Adaptive Cybersecurity Governance Framework" *Journal of Cybersecurity and Privacy* 3, no. 3: 327-350. https://doi.org/10.3390/jcp3030017