INTRODUCCIÓN A LA CIBERSEGURIDAD

Año 2025

Carrera/ Plan:

Licenciatura en Informática Plan 2021 / Plan 2015
Licenciatura en Sistemas Plan 2021 / Plan 2015
Analista en Tecnologías de la Información y la Comunicación *Plan 2021* / Plan 2017

Año: 4to/5to para licenciaturas y 3ro para ATIC
Régimen de Cursada: *Semestral*
Carácter: Optativa
Correlativas: Redes y comunicaciones
Profesor: Nicolás Macia
Hs. semanales: 3 horas teoría / 3 horas de práctica

FUNDAMENTACIÓN

"Introducción a la ciberseguridad" aporta a los alumnos de una visión global sobre los problemas de ciberseguridad que afectan los distintos componentes de un sistema informático: software, datos y comunicaciones.

Los temas abordados en esta materia son relevantes en la formación de futuros egresados, tanto a los que tendrán la oportunidad de trabajar en aspectos relacionados con seguridad de la información como a aquellos que trabajen en otras áreas.

OBJETIVOS GENERALES

- *Brindar un panorama general sobre ciberseguridad: amenazas existentes, controles posibles, ataques y gestión de incidentes de seguridad.*
- *Introducir conceptos de IC e IoT y poner en evidencia los riesgos que pueden provocar distintos problemas de ciberseguridad.*
- *Consolidar la formación experimental en los temas abordados, utilizando actividades prácticas basadas en competencias de tipo desafíos. Los temas abordados incluyen conceptos sobre:*
  - *Criptografía*
  - *Gestión de incidentes*
  - *Análisis de malware*
  - *Reversing*
  - *Explotación de binarios*

COMPETENCIAS

A lo largo de la cursada, se trabajan con temáticas que abordan las siguientes competencias designadas por el HCD:

- LI-CE7- Planificar, dirigir, realizar y/o evaluar proyectos de sistemas de seguridad en el almacenamiento y procesamiento de la Información. Especificación, diseño, desarrollo, implementación y mantenimiento de los componentes de seguridad de información embebidos en los sistemas físicos y en los sistemas de software de aplicación. Establecimiento y control de metodología de procesamiento de datos que mejoren la seguridad y privacidad incluyendo datawarehousing.

- LS-CE6- Planificar, dirigir, realizar y/o evaluar los sistemas de seguridad en el almacenamiento y procesamiento de la información. Realizar la especificación, diseño, desarrollo, implementación y mantenimiento de los componentes de seguridad de información embebidos en los sistemas físicos

y en los sistemas de software aplicados. Establecer y controlar las metodologías de procesamiento de datos orientadas a seguridad, incluyendo data-warehousing.

CONTENIDOS MINIMOS (de acuerdo al Plan de Estudios)

- *Conceptos básicos. Seguridad de la información. Ciberseguridad. Activos de información. Internet de las cosas. Vulnerabilidades en software, comunicaciones, configuraciones y en almacenamiento de la información. Impacto de vulnerabilidades en escenarios tradicionales, IC e IoT.*
- *CSIRTs: equipos de respuesta a incidentes de seguridad. Gestión operativa de incidentes de seguridad.*
- *Criptografía. Esteganografía. Problemas en la protección y ocultamiento de la información*
- *Análisis de malware. Análisis estático. Análisis dinámico.*
- *Reversing. Ingeniería inversa. Assembly. Disassembly. Debugging.*
- *Explotación de binarios. Regiones de memoria de un proceso. Buffer overflow. Protecciones.*
- *Explotación de vulnerabilidades.*
- *Ejercicios de ataque y defensa. Ejercicios tipo desafíos.*

PROGRAMA ANALÍTICO

Unidad I: Introducción a ciberseguridad:

- Conceptos generales. Definiciones. Atributos de la información. Activos de información.
- Vulnerabilidades, amenazas e incidentes.
- Seguridad de la información vs ciberseguridad.

Unidad II: Sistemas de cifrado clásicos y modernos

- *Codificación*
- *Criptografía clásica: sustitución, transposición*
- *Funciones de hash*
- *Criptografía moderna: algorítmos simétricos y asimétricos*
- *Firma digital*
- *Esteganografía.*

Unidad III: Gestión de incidentes de seguridad

- Problemas de ciberseguridad en el procesamiento de la información, en las comunicaciones y en el almacenamiento de la información.
- Problemas de ciberseguridad en escenarios complejos: Infraestructuras críticas e Internet de las cosas.
- Problemas de seguridad para las personas: Privacidad. Vigilancia. Manipulación. Robo de datos personales.
- Equipos de respuesta a incidentes de seguridad: CSIRTs / CERTs
- **Aspectos operativos en la gestión de incidentes.**
  PGP. DNS. Whois y RDAP. SMTP.

Unidad IV: Análisis de malware

- Indicadores de compromiso. Tipos de IOC.
- Técnicas de análisis estáticas. Packers y ofuscación. Herramientas utilizadas.
- Técnicas de análisis dinámicas. Armado de entorno de análisis. Herramientas utilizadas.

Unidad V: Reversing

- *Reversing. Ingeniería inversa.*
- *Repaso de assembler .*
- *Assembly / Disassembly.*
- *Debugging.*

Unidad VI: Explotación de binarios

- Conceptos. Escalamiento de privilegios. Pruebas de concepto o PoC. Exploit. Shellcode.
- Problemas de seguridad en el desarrollo: *Buffer overflow, Integer overflow, Format strings.*
- *Explotación de vulnerabilidades*
- *Protecciones posibles.*

BIBLIOGRAFÏA

- Fundamentos de seguridad en redes. Stallings, W. 2a ed. Pearson, 2004
- HACKING: THE ART OF EXPLOITATION. Jon Erickson.
- Practical Malware Analysis: The Hands-On Guide to Dissecting Malicious Software. Sikorski, M y Honig, A. No Starch Press, 2012
- Practical Binary Analysis: Build Your Own Linux Tools for Binary Instrumentation, Analysis, and Disassembly. Andriesse, Dennis. No Starch Press, 2019.
- Diccionario de amenazas: https://www.sophos.com/es-es/medialibrary/PDFs/other/sophosthreatsaurusaz.pdf
- The Shellcoder's Handbook: Discovering and Exploiting Security Holes. Chris Anley, John Heasman, Felix Lindner & Gerardo Richarte
- “Aleph One”. Smashing The Stack For Fun And Profit. Phrack, 7(49), November 1996 http://phrack.org/issues/49/14.html
- Dr. Jorge Ramió Aguirre. (2006). Libro Electrónico de Seguridad Informática y Criptografía Versión 4.1.
- Dan Boneh and Victor Shoup. (2017). A Graduate Course in Applied Cryptography. Sitio web: http://toc.cryptobook.us/
- Libro crypto 101 - Laurens Van Houtven - https://www.crypto101.io/
- De la cifra clásica al cifrado RSA: http://www.criptored.upm.es/guiateoria/gt_m001a.htm
- Libro fundamentos de seguridad en redes 2da edición – Stallings
- Handbook for Computer Security Incident Response Teams (CSIRTs) https://resources.sei.cmu.edu/asset_files/Handbook/2003_002_001_14102.pdf
- Proyecto Amparo: Manual básico en Gestión de Incidentes de Seguridad Informática http://www.proyectoamparo.net/files/manual_seguridad/manual_basico_sp.pdf

METODOLOGÍA DE ENSEÑANZA

Las teorías son explicaciones conceptuales sobre las distintas temáticas abordadas. Las mismas se inician a partir de los contenidos previamente desarrollados y se articulan con los nuevos temas. La explicación de cada tema presentado, busca relacionar los temas presentes con los anteriores.

En la práctica se profundizan conceptos promoviendo la reflexión teórica y aplicación de los mismos, en situaciones concretas sobre las cuales se busca una solución.

Se utilizará la plataforma de e-learning Moodle (https://catedras.info.unlp.edu.ar) para:

- *Publicar las clases teóricas.*
- *Publicar enunciados de los talleres prácticos.*

Se utilizarán Discord para:

- *Disponer de canales públicos de comunicación para*
  - *Realizar consultas generales*
  - *Realizar las comunicaciones de la Cátedra a los alumnos.*

- *Disponer canales privados entre el docente y los distintos alumnos para:*
  - *Realizar consultas personalizadas en base a la resolución realizada por el alumno.*
  - *Realizar entregas previstas.*

Para las teorías se utilizarán presentaciones digitales. Las guías de trabajos prácticos tendrán referencias específicas a secciones de libro o material en Internet que el alumno podrá ir consultando a medida que avance en la complejidad de las mismas.

Se brindará indicaciones para que el alumno construya su entorno de trabajo en una máquina virtual GNU/Linux con las herramientas utilizadas para poder realizar el desensamblado y la explotación de binarios.

La modalidad de dictado se ajustará tanto a presencial/semipresencial o virtual.

EVALUACIÓN

Para aprobar la cursada será necesario cumplir con los siguientes requisitos:

- *Aprobar todas las entregas propuestas por la cátedra*

Para la evaluación final, se será necesario realizar, presentar y a aprobar un trabajo final.

La nota final se determinará en base a las notas obtenidas en las instancias pautadas y la de la evaluación final.

CRONOGRAMA DE CLASES Y EVALUACIONES

Semana	Unidad	Teoría	Práctica
1	1	Prensentacion y Introducción	Scripting
2	2	Cripto parte 1	Criptografía parte 1
3	2	Cripto parte 2	Criptografía parte 2
4	2	Cripto parte 3	Criptografía parte 3
5	2	CSIRTs (recursos de internet)	Criptografía parte 3
6	3 y 4	CSIRT (smtp + gestion de incidentes)	CSIRT / Análisis de Malware parte 1
7	3 y 4	Análisis de Malware	CSIRT / Análisis de Malware parte 2
8	3 y 4	Reversing parte 1	CSIRT / Análisis de Malware parte 3
9	3 y 4	Reversing parte 2	CSIRT / Análisis de Malware parte 3
10	5	Reversing parte 3	Reversing
11	5	Exploiting parte 1 (intro / buffer overflows)	Reversing
12	5	consulta / explicación prácticas	Reversing
13	5	Exploiting parte 2 (protecciones)	Reversing
14	6	Exploiting parte 3 (setuid / int overflow / format string)	Binary exploiting
15	6	consulta / explicación prácticas	Binary exploiting
16	6	Exploiting parte 4	Binary exploiting
17	6	consulta / explicación prácticas	Binary exploiting
18	6		Binary exploiting

Inicio de clases:
- 1er semana del 2do semestre según cronograma académico (Jueves 21/8)

Evaluación de prácticas

Práctica Cripto	24/9/2025	1ra evaluación
Práctica CSIRT/Malware	22/10/2025	
Práctica Reversing	19/11/2025	
Práctica pwn	17/12/2025	
Prácticas faltantes	22/12/2024	2da evaluación

Contacto de la cátedra (mail, sitio WEB, plataforma virtual de gestión de cursos):

- **Mail:** nmacia en info.unlp.edu.ar
- **Plataforma virtual de gestión de cursos:** https://catedras.info.unlp.edu.ar