INTRODUCCIÓN A LA CIBERSEGURIDAD	**Carrera/ Plan:** *Licenciatura en Informática* Plan 2015/Plan 2012/Plan 2003-07 *Licenciatura en Sistemas* Plan 2015/Plan 2012/Plan 2003-07 *Analista en TIC* Plan 2017
Año 2019	**Año:** 2019 **Régimen de Cursada:** *Semestral* **Carácter:** Optativa **Correlativas**: Redes y comunicaciones **Profesor:** Nicolás Macia **Hs. semanales**: 6 horas

FUNDAMENTACIÓN

"Introducción a la ciberseguridad" aporta a los alumnos de una visión global sobre los problemas de seguridad que afectan al software en general.

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 y ataques.*
- *Introducir conceptos de IC e IoT y poner en evidencia los riesgos que pueden provocar distintos problemas de ciberseguridad.*
- *Consolidar la formación experimental en actividades prácticas sobre los temas abordados, utilizando competencias en los distintos conceptos prácticos tratados:*
  - *Criptografía*
  - *Gestión de incidentes*
  - *Análisis de malware*
  - *Reversing*
  - *Explotación de binarios*

COMPETENCIAS

- 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. Infraestructuras críticas. Internet de las cosas.*
- *Criptografía. Esteganografía. Problemas en la protección y ocultamiento de la información*
- *CSIRTs: equipos de respuesta a incidentes de seguridad. Gestión operativa de incidentes de seguridad.*
- *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.*

PROGRAMA ANALÍTICO

Unidad I: Introducción a ciberseguridad:

- Conceptos generales. Definiciones. Atributos de la información. Activos de información.
- Cibercriminales. Espías. Hacktivistas. Otro tipo de atacantes.
- Seguridad de la información vs ciberseguridad.
- Vulnerabilidades, amenazas e incidentes.

Unidad II: Los problemas de la ciberseguridad

- 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.
- *Criptografía. Esteganografía.*
- *Problemas en la protección y ocultamiento de la información*

Unidad III: Gestión de incidentes de seguridad

- Equipos de respuesta a incidentes de seguridad: CSIRTs / CERTs
- Aspectos operativos en la gestión de incidentes.
  PGP. DNS. Whois y RDAP. SMTP.
- Detección de incidentes. Feeds de información.
- Procesamiento de logs

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.
- *Regiones de memoria de un proceso. Buffer overflow.* Explotación.
- *Protecciones.*

BIBLIOGRAFÏA

- “Aleph One”. Smashing The Stack For Fun And Profit. Phrack, 7(49), November 1996 http://phrack.org/issues/49/14.html
- HACKING: THE ART OF EXPLOITATION. Jon Erickson.
- The Shellcoder's Handbook: Discovering and Exploiting Security Holes. Chris Anley, John Heasman, Felix Lindner & Gerardo Richarte
- Practical Malware Analysis. Sikorski, Honig.
- Diccionario de amenazas: https://www.sophos.com/es-es/medialibrary/PDFs/other/sophosthreatsaurusaz.pdf
- 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.*
- *Realizar las entregas previstas.*
- *Realizar consultas en los foros.*
- *Realizar las comunicaciones de la Cátedra a los alumnos.*

Para las teorias se utilizarán presentaciones en formato digital y cañón. 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.

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

Clase	Fecha	Contenidos/Actividades
1	15/8	**Unidad 1**
2	22/8	**Unidad 2 / Práctica 1**
3	29/8	**Práctica 1**
4	5/9	**Práctica 1**
5	12/9	**Unidad 3 / Práctica 2**
6	19/9	**Práctica 2**
7	26/9	**Unidad 4 / Práctica 3**
8	3/10	**Practica 3**
9	10/10	**Practica 3**
10	17/10	**Practica 3**
11	24/10	**Unidad 4 / Práctica 4**
12	31/10	**Práctica 4**
13	7/11	**Práctica 4**
14	14/11	**Práctica 4**
15	21/11	**Unidad 5 / Practica 5**
16	28/11	**Práctica 5**
17	5/12	**Práctica 5**

Evaluaciones previstas	Fecha
Entrega práctica 1	12/9
Entrega práctica 2	26/9
Entrega práctica 3	24/10
Entrega práctica 4	21/11

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

Firma del profesor

Nicolás Macia