UNIVERSIDAD NACIONAL DE LA PLATA
FACULTAD DE INFORMÁTICA

INTRODUCCIÓN A LA CIBERSEGURIDAD	**Carrera/ Plan:** *Licenciatura en Informática* Plan 2015 *Licenciatura en Sistemas* Plan 2015 *Licenciatura en Informática* Plan 2003-07/Plan 2012 *Licenciatura en Sistemas* Plan 2003-07/Plan 2012 *Analista en TIC Plan 2017*
Año 2018	**Año:** **Régimen de Cursada:** *Semestral* **Carácter:** *Optativa* **Correlativas**: *Redes y comunicaciones* **Profesores:** *Nicolás Macia y Einar Lanfranco*
	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 para la formación de futuros egresados que tendrán la oportunidad de trabajar en aspectos relacionados a seguridad de la información.

OBJETIVOS GENERALES

- *Brindar un panorama general sobre ciberseguridad: Controles posibles, amenazas existentes, ataques y riesgos.*
- *Introducir conceptos de IC e IoT y poner en evidencia el impacto de los problemas de ciberseguridad sobre estos.*
- *Consolidar la formación experimental en actividades prácticas sobre los temas abordados. Utilizar plataformas de juego como disparador a distintos tipos de problemas relacionados.*
- *Propiciar las condiciones para que el alumno pueda identificar amenazas que puedan poner en riesgo la información, ya sea al momento en el que la misma es procesada, almacenada y/o transportada entre los distintos sistemas de información interconectados.*

CONTENIDOS MINIMOS (de acuerdo al Plan de Estudios)

- *Conceptos básicos: Seguridad de la información. Ciberseguridad. Activos de información. Infraestructuras críticas. Internet de las cosas.*
- *Vulnerabilidades y amenazas en el procesamiento, almacenamiento y transporte de información. Análisis y explotación.*

- *Riesgos. Problemas de ciberseguridad aplicados en escenarios tradicionales, en Internet de las cosas (IoT), en infraestructuras críticas (IC) y en las personas.*
- *CSIRTs: equipos de respuesta a incidentes de seguridad.*

PROGRAMA ANALÍTICO

Unidad I: Introducción a ciberseguridad:

- *Conceptos generales. Definiciones. Atributos de la información.*
- *Ciberseguridad en los sistemas de información, en las comunicaciones y en el almacenamiento de la información.*
- *Vulnerabilidades, amenazas e incidentes.*
- *Cibercriminales. Espías. Hacktivistas. Otro tipo de atacantes*

Unidad II: Los problemas de la ciberseguridad

- Activos de información. Tipos de atacantes.
- Escenarios complejos: Infraestructuras críticas, Internet de las cosas.
- Riesgo.
- Problemas de seguridad para las personas: Privacidad. Vigilancia. Manipulación. Robo de datos personales.
- *Normativas, leyes y Estrategias de ciberseguridad.*
- *Buenas prácticas: SGSI*

Unidad III: *Ciclo de vida de las vulnerabilidades*

- *La industria tras el descubrimiento de problemas*
- *Los parches de seguridad*
- *Índices internacionales*
- *Búsqueda de problemas de seguridad*
- *Buscadores en linea*

Unidad IV: Tratamiento de incidentes de seguridad

- *Equipos de respuesta a incidentes de seguridad: CSIRTs / CERTs*
- *Gestión de incidentes. Whois, RDAP, SMTP.*
- *Detección de incidentes. Feeds de información.*
- *Procesamiento de logs*

Unidad V: Formación de recursos

- *Competencias de seguridad tipo CTF.*
- *Ejercicios de ataque/defensa. Ejercicios sólo ataque*
- *Competencias tipo jeopardy o desafío*

Unidad VI: Explotación

- *Conceptos: Escalamiento de privilegios, Payloads, PoC*
- *Problemas de seguridad en el desarrollo.*
- *Buffer overflow*
- *Exploit*

BIBLIOGRAFÍA

- Diccionario de amenazas: https://www.sophos.com/es-es/medialibrary/PDFs/other/sophosthreatsaurusaz.pdf
- Convenio sobre cibercriminalidad: https://www.oas.org/juridico/english/cyb_pry_convenio.pdf
- Estrategia de ciberseguridad nacional: http://www.dsn.gob.es/es/estrategias-publicaciones/estrategias/estrategia-ciberseguridad-nacional
- Proyecto de Estrategia de Seguridad Interior de la Unión Europea: "Hacia un modelo europeo de seguridad" http://register.consilium.europa.eu/doc/srv?l=ES&f=ST%205842%202010%20REV%202
- 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
- “Aleph One”. Smashing The Stack For Fun And Profit. Phrack, 7(49), November 1996 http://phrack.org/issues/49/14.html
- SANS - Buffer Overflows for Dummies https://www.sans.org/reading-room/whitepapers/threats/buffer-overflows-dummies-481
- OWASP Mobile Security Project https://www.owasp.org/index.php/OWASP_Mobile_Security_Project
- OWASP Top Ten Project https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

- Metasploit: The Penetration Tester's Guide - David Kennedy, Jim O'Gorman, Devon Kearns, and Mati Aharoni - ISBN-13: 978-1-59327-288-3
- Buffer Overflow Attacks: Detect, Exploit, Prevent - James C. Foster - SYNGRESS

METODOLOGÍA DE ENSEÑANZA

Las teorías son explicaciones conceptuales, se inician a partir de los contenidos previamente desarrollados y se articulan con los nuevos temas. En 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, a través del uso de diferentes herramientas. Las prácticas son de carácter individual y grupal.

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

- *Publicar las clases teóricas.*
- *Publicar los enunciados de los talleres prácticos.*
- *Realizar las entregas de los talleres prácticos.*
- *Realizar las consultas en los foros.*
- *Realizar las comunicaciones de la Cátedra a los alumnos.*

Se utilizan presentaciones en formato digital, cañón, guías de trabajos prácticos, apuntes complementarios elaborados por la cátedra, PCs, distribuciones Linux a medida para aplicar conceptos de la materia y contenido online sobre las distintas temáticas.

EVALUACIÓN

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

- *Entrega de ejercicios entregables propuestos por la cátedra*
- *Participar en las distintas plataformas de juego propuestas por la cátedra*
- *Realizar un test sobre los distintos temas vistos en la materia*

Para la nota de final de la materia, es necesario, luego de aprobar la cursada realizar un trabajo final integrador sobre los temas abordados en la cursada e incluye una exposición del mismo.

CRONOGRAMA DE CLASES Y EVALUACIONES

Fechas	Clase	Contenido/Actividades	Actividad Práctica
23/08/18	1	Unidad I	
30/08/18	2	Unidad I	Práctica 1
06/09/18	3	Unidad II	Consulta
13/09/18	4	Unidad II	Consulta
20/09/18	5	Unidad III	Práctica 2
27/09/18	6	Unidad IV	Práctica 3
04/10/18	7	Unidad IV	Consulta
11/10/18	8	Unidad V	Práctica 4
18/10/18	9	Unidad V	Consulta
25/10/18	10	Unidad VI	Consulta
01/11/18	11	Unidad VI – Presentación trabajo final	Consulta
08/11/18	12		Consulta
15/11/18	13		Consulta
22/11/18	14		Consulta
29/11/18	15	Exposición de trabajos finales	
06/12/18	16		Test escrito

Para contactar a la cátedra:

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

Firma del los profesores

Einar Lanfranco *Nicolás Macia*