

Seguridad y Privacidad en Redes

Año 2023

Carrera/ Plan: (Dejar lo que corresponda)*Licenciatura en Informática Plan 2021/Plan 2015/Plan 2012
Licenciatura en Sistemas Plan 2021/Plan 2015/Plan 2012
Analista en Tecnologías de la Información y la Comunicación
Plan 2021/Plan 2017***Año:** 4to/5to**Régimen de Cursada:** Semestral**Carácter (Obligatoria/Optativa):** Optativa**Correlativas:** Redes y Comunicaciones y Sistemas
Operativos**Profesor/es:** Lic. Francisco Javier Díaz, Lic. Paula Venosa**Hs. semanales teoría:** 3**Hs. semanales de práctica:** 3**FUNDAMENTACIÓN**

Seguridad y Privacidad en redes es una asignatura optativa de cuarto y quinto año de la carrera Licenciatura en Informática y una asignatura optativa de cuarto año de la carrera Licenciatura en Sistemas. El alumno que cursa Seguridad y Privacidad en Redes cuenta con los conocimientos fundamentales de informática, en particular en lo que se refiere a redes y sistemas operativos. Seguridad y privacidad en redes forma a los alumnos en el análisis de problemas de seguridad de sistemas, redes y servicios así como en el diseño e implementación de soluciones a los mismos. Además, aporta al perfil profesional, más "herramientas" que sirvan al alumno para saber "resolver problemas" en el mundo del trabajo. El estudiante aprende normas, protocolos y herramientas que aplicará para implementar mecanismos de seguridad en los sistemas que él mismo desarrolle y/o en las redes y servicios que él administre, así como para analizar el nivel de seguridad de sistemas, redes y servicios.

OBJETIVOS GENERALES

Comprender conceptos básicos relacionados a la seguridad de la información Analizar distintas herramientas para comprender riesgos existentes y analizar la seguridad en la organización Estudiar normas, mecanismos y protocolos para proteger las redes y sus aplicaciones.

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 de seguridad y terminología relacionada.
- Legislación nacional relacionada a seguridad de la información.
- Criptografía y sus aplicaciones (Firma digital, PGP, Esteganografía).
- Amenazas: Técnicas de descubrimiento, scanning, sniffing, etc.
- Vulnerabilidades de los sistemas - Ataques. Seguridad de aplicaciones WEB .
- Mecanismos de protección: Firewalls, IDS e IPS y honeypots.
- Gestión de seguridad de la información: Serie ISO 27000.

PROGRAMA ANALÍTICO

Unidad I: Introducción

Seguridad y Privacidad - Conceptos básicos de seguridad - Atributos de seguridad: confidencialidad, integridad, autenticidad, no repudio - Vulnerabilidad, Amenaza, Incidente- Tipos de amenazas – Ejemplos. Seguridad Física.

Unidad 2: Descubrimiento

Técnicas de descubrimiento: Footprinting - Fingerprinting de SO y de servicios - Escaneo y técnicas de escaneo basadas en TCP y UDP - Herramientas de escaneo y análisis

Unidad 3: Sniffing

Conceptos básicos de sniffing - Técnicas de sniffing en redes switcheadas - Herramientas - Técnicas de detección de sniffing - Análisis de muestras de tráfico

Unidad 4: Criptografía

Definiciones - Historia - Criptografía Simétrica - Criptografía Asimétrica - Aplicaciones de la criptografía: Infraestructuras de clave pública - PGP - Firma Digital: Aspectos técnicos y legales -Uso de la criptografía en los servicios WWW, correo electrónico - Esteganografía

Unidad 5: Mecanismos de protección

Firewalls - Políticas de filtrado - Reglas de filtrado - Sistemas de detección de intrusiones (IDS) - Tipos de IDS - Sistemas de prevención de intrusiones - Tipos de IPS - Honeypots – WAF - Herramientas

Unidad 6: Gestión de seguridad de la información

Definiciones - ISO 27000 : Generalidades de la serie - ISO 27001: Ciclo de gestión de la seguridad de la información - Objetivos de control e implementación de controles - Aspectos claves de un SGSI

BIBLIOGRAFÍA

Principles of Information Security. 7th ed., Whitman, Michael E. y Mattord, Herbert J., Cengage Learning, 2022.

Network security assessment, Chris McNab O'Reilly 2007.

Cryptography and network security: principles and practice Stallings, William 3rd ed.

(c2003)

CISSP certification exam guide Harris, Shon 2nd ed. (c2003)

OWASP Testing Guide OWASP Foundation Creative Commons Attribution-ShareAlike 3.0 license 2002-2008

METODOLOGÍA DE ENSEÑANZA

Las teorías son explicaciones conceptuales, se inician a partir de los contenidos previamente desarrollados y se articulan con los nuevos temas, presentación del tema, explicación del tema en forma dialogada que busca relacionar los temas presente con los anteriores. Se trabaja con ejercicios que ejemplifican el uso de las herramientas, aplicaciones y servicios que luego se estudiarán con detalle en la práctica. En la práctica se profundizan conceptos promoviendo la reflexión teórica y aplicación de los mismos, a través del uso de diferentes herramientas. Las explicaciones describen las principales herramientas a utilizar. El contenido de la práctica se publica con anterioridad y los alumnos concurren para resolver consultas y dudas sobre los mismos. Las prácticas son de carácter individual y grupal. Además hay entregas asociadas a cada práctica donde se integran en un caso hipotético (similar al de una organización real) los conceptos vistos en la práctica. También se usa una plataforma virtual para el desarrollo de la asignatura: la plataforma Moodle. En dicha plataforma se publican guías teóricas, trabajos prácticos, apuntes, videos y además es utilizada como medio de comunicación entre alumnos y docentes y entre los mismos alumnos. Se utilizan presentaciones en formato digital, cañón, guías de trabajos prácticos, apuntes complementarios elaborados por la cátedra, PCs, live Cds con distribuciones de seguridad Opensource, un live CD especialmente elaborado por los docentes del curso y el equipo LIHUEN de la Facultad para realizar algunos de los trabajos prácticos, distintas aplicaciones de seguridad open source.

EVALUACIÓN

Evaluación de la cursada mediante evaluaciones parciales de cada práctica (tests) en la plataforma Moodle. Además al final de la cursada se evalúan todos los temas que no hayan sido aprobados en los tests en un examen parcial escrito. Los 4 tests que se rinden en el marco de la clase desde la plataforma Moodle.

Consisten en preguntas de opción múltiple y casos prácticos a resolver sobre los temas desarrollados en la teoría y en la práctica. También hay una entrega correspondiente a cada práctica que forma parte del seguimiento y evaluación del alumno.

Para la aprobación final de la asignatura se puede rendir un coloquio integrador y realizar una presentación en una jornada, o rendir un examen final escrito.

Para la primer opción, se debe aprobar el coloquio integrador para poder realizar una presentación, en el marco de una jornada interna (incluyendo presentación previa de propuesta), de un tema elegido por ellos no desarrollado en la cursada o complementario a la cursada, en el marco de temáticas sugeridas por la cátedra.



Clase	Fecha	Contenidos/Actividades
1	Semana 14/8/2023	Introducción -Conceptos Generales
2	Semana 21/8/2023	Amenazas sobre las personas y el hardware. Concientización
3	Semana 28/8/2023	Introducción a la gestión de seguridad de la información
	Semana 4/9/2023	Técnicas de Descubrimiento
4	Semana 11/9/2023	Técnicas de Descubrimiento
5	Semana 18/9/2023	Sniffing
6	Semana 25/9/2023	Sniffing
7	Semana 2/10/2023	Criptografía
8	Semana 9/10/2023	Criptografía
9	Semana 16/10/2023	Criptografía
10	Semana 23/10/2023	Mecanismos de protección
11	Semana 30/10/2023	Mecanismos de protección
12	Semana 6/11/2023	SGSI- Segunda parte y cierre
14	Semana 13/11/2023	Repaso general Conclusiones de la materia
15	Semana 20/11/2023	Consulta Clase de cierre
16	Semana 27/11/2023	Consulta para el parcial
17	Semana 4/12/2023	Parcial
18	Semana 11/12/2023	Consulta para el parcial

Evaluaciones previstas	Fecha
------------------------	-------

Primera instancia del parcial (tests por tema)	A lo largo de la cursada, al finalizar cada unidad
Primer recuperatorio del parcial	Semana 18/12/2023
Segundo recuperatorio del parcial	Semana 5/02/2024

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

<https://catedras.info.unlp.edu.ar/> (sección “Categorías de Cursos”)

Prof. Paula Venosa: pvenosa@info.unlp.edu.ar

JTP Matias Ferrigno: mferrigno@linti.unlp.edu.ar

Firma del/los profesor/es

Paula Venosa

2018

Año del Centenario de la Reforma Universitaria