SEGURIDAD Y PRIVACIDAD EN REDES	**Carrera/ Plan:** Licenciatura en Sistemas Plan 2007, 2012 y 2017 Licenciatura en Informática Plan 2007, 2012 y 2017 **Área:** Arquitectura, Sistemas Operativos y Redes **Año:** 4º o 5º año **Régimen de Cursada:** *Semestral* **Carácter**: Optativa **Correlativas:** Sistemas Operativos Redes y Comunicaciones
Año 2017	**Profesor:** *Javier Díaz, Paula Venosa* **Hs semanales:** 6 hs

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 el 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 riegos existentes y analizar la seguridad en la organización
Estudiar normas, mecanismos y protocolos para proteger las redes y sus aplicaciones.

CONTENIDOS MINIMOS

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.

Unidad 2: 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 3: 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 4: Sniffing
Conceptos básicos de sniffing - Técnicas de sniffing en redes switcheadas - Herramientas - Técnicas de detección de sniffing - Análisis de muestras de tráfico

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 - Herramientas

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

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.
También se usa una plataforma virtual que sirve de apoyo 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 (coloquios) en la plataforma Moodle.
Además al final de la cursada se evalúan todos los temas que no hayan sido aprobados en los coloquios en un examen parcial escrito.
Los 4 coloquios 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.
Para la aprobación final de la asignatura se puede optar entre un trabajo práctico final integrador o de un exámen final integrador escrito.

BIBLIOGRAFÍA OBLIGATORIA

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

BIBLIOGRAFÍA COMPLEMENTARIA

CRONOGRAMA DE CLASES Y EVALUACIONES

Tema	Clases teóricas	Clases prácticas	Evaluación
Introducción - Conceptos Generales	Semana 14/8/2017	Semana 14/8/2017	
Amenazas sobre las personas y el hardware. Concientización	Semana 21/8/2017	Semana 21/8/2017	
Técnicas de Descubrimiento	Semana 28/8/2017 Semana 4/9/2017	Semana 28/8/2017 Semana 4/9/2017	
Sniffing	Semana 11/9/2017 Semana 18/9/2017	Semana 11/9/2017 Semana 18/9/2017	
Criptografía	Semana 25//9/2017 Semana 2/10/2017 Semana 9/10/2017	Semana 25/9/2017 Semana 2/10/2017 Semana 9/10/2017	
Seguridad de aplicaciones WEB	Semana 16/10/2017 Semana 23/10/2017	Semana 16/10/2017 Semana 23/10/2017 Semana 30/10/2017	
Mecanismos de protección	Semana 6/11/2017 Semana 13/10/2017	Semana 6/11/2017 Semana 13/11/2017 Semana 20/11/2017	
SGSI - ISO 27000 Repaso	Semana 20/11/2017		
Consulta			Semana 27/11/2017
Evaluación parcial			Semana 4/12/2017
Muestra y consulta			Semana 12/12/2017
Recuperatorio			Semana 5/2/2018
Muestra y consulta			Semana 5/2/2018

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

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

Prof. Francisco Javier Díaz
Prof. Paula Venosa: pvenosa@info.unlp.edu.ar

JTP Nicolás Macia: nmacia@info.unlp.edu.ar
JTP Damián Rubio: drubio@cert.unlp.edu.ar

Firmas del/los profesores responsables: