Ministerio de Cultura y Educación
Universidad Nacional de San Luis
Facultad de Ciencias Físico Matemáticas y Naturales
Departamento: Informatica
Area: Area II: Sistemas de Computacion

(Programa del año 2009)
(Programa en trámite de aprobación)
(Presentado el 11/09/2010 15:25:00)

I - Oferta Académica

Materia	Carrera	Plan	Año	Período
(OPTATIVA) INTRODUCCION A LA SEGURIDAD DE REDES	TCO.UNIV.EN REDES DE COMP.		2009	2° cuatrimestre

II - Equipo Docente

Docente	Función	Cargo	Dedicación
CLERIGO, PATRICIA ADELA	Prof. Responsable	P.Adj Simp	10 Hs
TAFFERNABERRY, JUAN CARLOS	Prof. Co-Responsable	P.Adj Simp	10 Hs

III - Características del Curso

Credito Horario Semanal				
Teórico/Práctico	**Teóricas**	**Prácticas de Aula**	**Práct. de lab/ camp/ Resid/ PIP, etc.**	**Total**
Hs	4 Hs	1 Hs	1 Hs	6 Hs

Tipificación	Periodo
C - Teoria con prácticas de aula	2º Cuatrimestre

Duración			
Desde	**Hasta**	**Cantidad de Semanas**	**Cantidad de Horas**
25/08/2009	04/12/2009	15	90

IV - Fundamentación

La masiva utilización de las computadoras y redes como medios para almacenar, transferir y procesar información se ha incrementado espectacularmente en los últimos años, al grado de convertirse en un elemento indispensable para el funcionamiento de la sociedad actual. Como consecuencia, la información en todas sus formas y estados se ha convertido en un activo de altísimo valor, el cual se debe proteger y asegurar . Actualmente se ha incrementado en nuestro país el uso de aplicaciones electrónicas que abarcan: correo, comercio, transacciones y dinero electrónicos, firmas y certificados digitales, acceso seguro a bancos de información, comunicaciones seguras, entre otras. Por tal motivo, los requerimientos de seguridad son cada vez mayores, presentándose así un problema que la Seguridad Informática, trata de resolver implementando diversas herramientas.

V - Objetivos / Resultados de Aprendizaje

La finalidad de esta materia es ayudar al alumno a entender los fundamentos de la protección de una infraestructura de red. Transmitir los conceptos básicos del cifrado. Detallar las tecnologías de seguridad más comunes. Presentar las posibles amenazas y ataques de una infraestructura de red. Detallar consideraciones relativas a las Normas de seguridad. Describir como llevar a cabo un análisis sobre gestión de riesgos. Presentar las directrices y los procedimientos que se deben seguir para el diseño e implementación de las normas de seguridad. Como administrar la gestión de incidentes.

VI - Contenidos

1) Ataques a la seguridad – Servicios de seguridad – Mecanismos de seguridad – Un modelo de seguridad en redes

2) Cifrado Simétrico
a) Principios del Cifrado Simétrico
b) Algoritmos de Cifrado simétrico
c) Distribución de claves

3) Criptografía de clave pública y autentificación de mensajes
a) Enfoques para la autenticación de mensajes
b) Funciones hash seguras y HMAC
c) Principios de criptografía de clave pública
d) Algoritmos de criptografía de clave pública
e) Firmas Digitales
f) Gestión de Claves

4) Aplicaciones de Autenticación
a) Kerberos.
b) Servicio de Autentificación X.509.

5) Normas de seguridad
a) Dónde empezar – Gestión de riesgos – Marco de normativa de seguridad.

6) Seguridad en el correo electrónico
a) PGP (Pretty Good Privacy).
b) S/MIME

7) Seguridad en TCP/IP
a) Vulnerabilidades genéricas.
b) Protecciones y Herramientas.

8) Seguridad en la WEB
a) Consideraciones.
b) SSL (Secure Socket Layer) TLS (Transport Layer Security)
c) SET

VII - Plan de Trabajos Prácticos

Trabajo Práctico 1: cifrado simétrico
Trabajo Práctico 2: cifrado asimétrico
Trabajo Práctico 3: kerberos – PKI – firma digital - certificados
Trabajo Práctico 4: PGP – s-MIME
Presentaciones especiales 1: PKI - Kerberos
Presentaciones especiales 2: IP-Sec – SSL/TLS/SET

VIII - Regimen de Aprobación

Las condiciones para la obtención de la regularización y promoción directa de la materia son:
1) Tener satisfechas las condiciones académicas y de asistencias reglamentadas por la Facultad.
2) Tener aprobada la carpeta de Trabajos Prácticos de ejercicios de acuerdo a las modalidades de presentación que se indique. Para ello, se hará énfasis en el respeto a las fechas de presentación de los Trabajos Prácticos.
3) La nota final de cursado se obtendrá del siguiente cálculo a partir de las calificaciones de 1 (un) evaluación parcial y 1 (un) global de teoría y práctica (EP1, G1), y la de los trabajos prácticos (TP)

Las fechas y los temas previstos para las evaluaciones y globales se encuentran en un cronograma que se adjunta. Los parciales y globales tienen el carácter de exámenes, y la ausencia a los mismos se computa como 0 (cero). Los mismos son recuperables.

REQUISITOS PARA LA REGULARIDAD

Para la regularización:
- Como mínimo con 4 (cuatro).
- Todos los prácticos y laboratorios presentados.

ACERCA DE LA APROBACION
1. Promoción
2. Por regularización
3. Libre

1. Para la promoción:
- La nota final como mínimo 7 (siete),
- A lo sumo un parcial desaprobado.
- Todos los prácticos presentados y aprobados.
- 80% de asistencia.

2. Aprobando un examen final Teórico.
3. Rendir un examen Teórico y práctico.

IX - Bibliografía Básica

[1] Fundamentos de Seguridad en Redes – Aplicaciones y Estándares 2ºEd. (2004) W. Stallings.
[2] Diseño de Seguridad en Redes – Merike Kaeo Pearson (2003)
[3] Análisis e Seguridad de la familia de protocolos TCP/IP y sus servicios asociados 1º edición – Raúl Siles Peláez (2002)

X - Bibliografia Complementaria

[1] Apuntes de la Cátedra.

XI - Resumen de Objetivos

XII - Resumen del Programa

1) Ataques a la seguridad – Servicios de seguridad – Mecanismos de seguridad – Un modelo de seguridad en redes

2) Cifrado Simétrico
3) Criptografía de clave pública y autentificación de mensajes
4) Aplicaciones de Autenticación
5) Normas de seguridad
6) Seguridad en el correo electrónico
7) Seguridad en TCP/IP
8) Seguridad en la WEB

XIII - Imprevistos

XIV - Otros

ELEVACIÓN y APROBACIÓN DE ESTE PROGRAMA	
	Profesor Responsable
Firma:	
Aclaración:	
Fecha:	