UNIVERSIDAD NACIONAL DE LA MATANZA

CÓDIGO ASIGNATURA
1128-1

DEPARTAMENTO: ***Ingeniería e Investigaciones Tecnológicas***

ASIGNATURA: Seguridad en Redes

Ingeniería en Informática

Año: 5º **Cuatri:**

1. OBJETIVOS

- Desarrollar en el alumno una actitud crítica y reflexiva con referencia a la seguridad de las redes.
- Dar al alumno las herramientas necesarias para desarrollar las políticas, planificar los procedimientos de seguridad e implementar los planes de mitigación y contingencia en las redes.
- Facilitar al alumno los elementos necesarios para diseñar y configurar redes seguras.
- Proporcionar al alumno las metodologías y estándares de seguridad utilizando aplicaciones criptográficas.

2. CLASIFICACIÓN DE LA ACTIVIDAD CURRICULAR, FORMACIÓN PRÁCTICA Y CARGA HORARIA

2.1

	Carga horaria en horas reloj
Bloque de Ciencias Básicas	8
Bloque de Tecnologías Básicas	
Bloque de Tecnologías Aplicadas	56
Bloque de Complementarias	
Otros Contenidos	
Carga horaria total de la actividad curricular	64

2.2

Disciplina	Carga Horaria
Matemática	8
Física	
Química	
Sistemas de representación y fundamentos de informática	56
Biología	
Otros (ciencia de la tierra, geología, etc.)	

Total	64

2.3

Formación Práctica				
Formación Experimental	Resolución de problemas de ingeniería	Actividades de proyecto y diseño	Práctica profesional supervisada	Total
	24	8		32

2.4

Carga horaria semanal	4
Carga horaria semanal dedicada a la formación práctica	2

3. CONTENIDOS

Cifrado clásico. Cifrado simétrico de claves. Cifrado asimétrico. Funciones Hash. Firma Digital. Autenticación mediante servidor RADIUS. Protocolos EAP. Configuración de políticas de seguridad en Firewall. Protocolo WEP, WPA, WPA2. Ataques. Tipos de amenazas: acceso no autorizado, suplantación de la identidad, denegación de servicio. Tecnologías VPDN, VPN. Certificados, Estándar X.509. Distribución de certificados.

Unidad n° 1: Seguridad en redes

Introducción a la seguridad en redes. Vulnerabilidades de las Redes. Arquitectura segura de las redes. Hardware, software y procedimientos para asegurar las redes.

Unidad n° 2: Amenazas y vulnerabilidades

Hackers, crackers y distintos tipos de Malware. Técnicas de ataque. Accesos no autorizados. Suplantación de identidad. Denegación de Servicio. Ataques a través de redes peer-to-peer. Vulnerabilidades de Sistemas Operativos, Aplicativos y Software de Seguridad.

Unidad n° 3: Cifrado clásico

Evolución histórica de los métodos criptográficos. Clasificación de los criptosistemas. Métodos de sustitución y trasposición. Métodos monoalfabéticos y polialfabéticos. Criptoanálisis.

Unidad n° 4: Cifrado Simétrico

Cifrado tipo Feistel. Distintos métodos de cifrado simétrico. Algoritmo DES. Modos de operación de DES. Triple DES. Algoritmo IDEA. Algoritmo AES. Comparación de los distintos métodos.

Unidad n° 5: Cifrado Asimétrico

Conceptos de matemáticas discreta. Método de intercambio de claves de Diffie-Hellman. Método RSA. Ataques al cifrado RSA. Método DSS – El Gamal. Fortaleza de los métodos de cifrado asimétrico.

Unidad n° 6: Aplicaciones criptográficas
Comparación de los métodos simétricos y asimétricos. Distintos tipos de ataques. Vulnerabilidades en las implementaciones criptográficas. Algoritmos de Hash. Esteganografía.

Unidad n° 7: Protocolos de seguridad
Seguridad en la capa de red: IPSec. Seguridad en la capa de transporte: SSL/TLS. Seguridad en la capa de aplicación: HTTPS, S-MIME, PEM, SET, SSH. Autenticación mediante un servidor RADIUS. Kerberos. VPN: Virtual Private Network. VPDN: Virtual Private Dial-up Network.

Unidad n° 8: Infraestructura de Firma Digital
Legislación para ser una Autoridad de Certificación Licenciada. Estándares PKCS - Public-Key Cryptography Standards. Certificados X.509: estructura y estándares. AC: Autoridades de certificación. Jerarquía de las AC´s. PKI: Infraestructura de clave pública.

Unidad n° 9: Distribución de certificados
AR: Autoridad de Registro. Normas de implementación. Políticas de certificación. Sellado de tiempo. Enrolamiento, generación y distribución de certificados digitales. Política de renovación. Baja de un certificado digital.

Unidad n° 10: Redes inalámbricas
Introducción a las Wireless LAN. Ataques y vulnerabilidades. Seguridad en las redes Wireless: 802.11x. Protocolo WEP. Protocolos WPA y WPA2. Protocolo EAP. Diseño de una arquitectura segura para instalar una red Wireless en una LAN corporativa.

4. BIBLIOGRAFÍA

Título	Autor(es)	Editorial	Año Edición	Ejemplares disponibles en UNLaM
Seguridad Informática	Sebastián Firtman	MP Ediciones	2005	
Seguridad en Redes Telemáticas	Justo Carracedo Gallardo	McGraw-Hill	2004	
Diseño de Seguridad en Redes	Merike Kaeo	Ciscopress	2003	
Criptografía	Ariel Maiorano	Alfaomega	2009	
Windows Server 2008. PKI and Certificate Security	Brian Komar	Microsoft Press	2008	

Fundamentos de seguridad en redes	William Stallings	Pearson Alhambra	2004	

5. DESCRIPCIÓN DE ACTIVIDAD CURRICULAR
5.1) MODALIDAD DE ENSEÑANZA EMPLEADA

Las clases se desarrollarán empleando el modelo deductivo de exposición con participación de los alumnos. Las clases serán teóricas y prácticas.

Se utilizarán las siguientes estrategias en diferentes momentos del proceso enseñanza-aprendizaje: presentación de los conceptos, desarrollo del tema, tormenta de ideas, estadísticas, ilustraciones funcionales, mapas conceptuales, organizadores previos, resúmenes, etc.

Participarán invitados de diferentes empresas proveedoras de Seguridad en Redes para la transferencia de sus experiencias metodológicas y prácticas.

Durante la cursada los alumnos desarrollarán Trabajos Prácticos Grupales que servirán como puente entre el marco teórico de la asignatura y su aplicación práctica permitiendo a los alumnos desarrollar las capacidades de trabajo en equipo; se utilizará la estrategia de Resolución de Casos.

También se desarrollarán actividades adicionales propuestas por los docentes y/o sugerencia de los alumnos.

5.2) MATERIALES DIDÁCTICOS NECESARIOS

Se entregarán guías para la realización de los trabajos prácticos y el material bibliográfico necesario.
Algunas prácticas requerirán el uso de un laboratorio de informática con PCs.

6. EVALUACIÓN

Los tipos de evaluación utilizadas serán:
a) Evaluación diagnóstica inicial: se desarrolla el primer día de clase.
b) De valoración cuantitativa: Parciales, dos en total con sus recuperatorios.
c) Complementarias: Guías para elaborar trabajos prácticos.

Para acreditar la asignatura los alumnos deberán:
a) Aprobar los trabajos prácticos
b) Contar con un 75 % de asistencia a clase
c) Aprobar dos exámenes parciales escritos con una calificación de 4 (cuatro) o superior. El alumno tendrá un recuperatorios por examen parcial.
d) Si la calificación es entre 4 (cuatro) y 6,99 (seis puntos con 99/100), el alumno tendrá reconocida la regularidad de la asignatura, debiendo rendir examen final de la misma en los turnos correspondientes.
e) Si la calificación de cada uno de los parciales es de 7 (siete) o superior, quedará eximido de la obligación del examen final, aprobándose la asignatura por promoción. Para lograr este derecho, el alumno deberá tener, a la finalización del dictado de la asignatura, aprobadas todas las asignaturas correlativas previas.

7. COMPOSICIÓN DEL EQUIPO DOCENTE ACTUAL

1 profesor titular
1 profesor asociado
1 JTP

7.1 Responsable a cargo de la actividad curricular:

Apellido y Nombre	Grado académico máximo	Cargo Docente	Situación	Dedicación en horas semanales al cargo
Donadello, Domingo	Magíster	Profesor titular		

7.2) PROFESORES

Apellido y Nombre	Grado académico máximo	Cargo Docente	Situación	Dedicación en horas semanales al cargo
Donadello, Domingo	Magíster	Profesor titular		
Eterovic, Jorge	Magíster	Profesor asociado	interino	4

Cantidad total de profesores: 2

7.3) AUXILIARES GRADUADOS

Apellido y Nombre	Grado académico máximo	Cargo Docente	Dedicación en horas semana-les al cargo
Pomar, Pablo	Ingeniero	JTP	4

Cantidad total de auxiliares: 1

7.4) AUXILIARES NO GRADUADOS

	Dedicación					
	Menor o igual a 9 horas	Entre 10 y 19 horas	Entre 20 y 29 horas	Entre 30 y 39 horas	Igual o mayor a 40 horas	Total
Auxiliares no graduados						
Otros						

	Designación					
	Regulares		Interinos		Contratados	
	Rentados	Ad Honorem	Rentados	Ad Honorem	Rentados	Total
Auxiliares no graduados						
Otros						

8. ALUMNOS

C: Cursantes por primera vez
R: Recursantes

8.1) TOTAL DE ALUMNOS QUE CURSARON LA ACTIVIDAD CURRICULAR

Año	2002		2003		2004		2005	
	C	R	C	R	C	R	C	R
Inscriptos								
Aprobaron la cursada								
Promocionaron								

Año	2006		2007		2008		2009	
	C	R	C	R	C	R	C	R

Inscriptos								
Aprobaron la cursada								
Promocionaron								

8.2) Alumnos que cursaron la asignatura discriminados por carrera (si corresponde)

Denominación de la carrera	Plan de Estudios	2002	2003	2004	2005	2006	2007	2008	2009
Ing. Informática									
Ing. Electrónica									
Ing. Industrial									

8.3) TOTAL DE ALUMNOS INVOLUCRADOS EN EXÁMENES FINALES

AÑO	2002	2003	2004	2005	2006	2007	2008	2009
Alumnos que rindieron final							---	---
Aprobaron							---	---

8.4) Alumnos que rindieron la asignatura discriminados por carrera (si corresponde)

Denominación de la carrera	Plan de Estudios	2002	2003	2004	2005	2006	2007	2008	2009
Ing. Informática									
Ing. Electrónica									
Ing. Industrial									

9. CANTIDAD DE COMISIONES

Turno	Cantidad de Comisiones	Promedio alumnos por comisión
Mañana		
Tarde		
Noche		

10. SUFICIENCIA Y ADECUACION DE LOS ÁMBITOS

11. INSCRIPCIÓN Y PROMOCIÓN DE ALUMNOS

12. EVALUACIÒN CAPACIDAD DE CATEDRA

13. ACCIONES, REUNIONES, COMISIONES

14. CALENDARIO DE ACTIVIDADES (semanas a planificar: cursada anual 52 semanas, cursada cuatrimestral 26 semanas)

Nº de Clase	Semana de Clase	Unidad Temática o Actividad
1	1	Presentación de la asignatura – Normas de cátedra. Programa – Actividades – Bibliografía. Unidad 1: Introducción a la Seguridad en Redes.
2	2	Unidad 2: Amenazas y vulnerabilidades
3	3	Trabajo práctico nº 1
4	4	Unidad 3: Cifrado clásico
5	5	Trabajo práctico nº 2
6	6	Unidad 4: Cifrado simétrico
7	7	Trabajo práctico nº 3
8	8	Unidad 5: Cifrado asimétrico
9	9	Trabajo práctico nº 4
10	10	Unidad 6: Aplicaciones criptográficas
11	11	Trabajo práctico nº 5
12	12	Entrega y revisión de los trabajos prácticos nº 1, 2, 3, 4 y 5.
13	13	1º examen parcial
14	14	Unidad 7: Protocolos de seguridad
15	15	Unidad 7: VPN y VPDN
16	16	Trabajo práctico nº 6
17	17	Unidad 8: Infraestructura de firma digital
18	18	Unidad 9: Autoridades de Registro
19	19	Unidad 9: Normativa legal argentina para firma digital
20	20	Trabajo práctico nº 7
21	21	Unidad 10: Redes inalámbricas
22	22	Entrega y revisión de los trabajos prácticos nº 6 y 7
23	23	2º examen parcial
24	24	Recuperatorio del 1º examen parcial
25	25	Recuperatorio del 2º examen parcial
26	26	Entrega de notas de los recuperatorios y revisión. Cierre de la materia.

INFORMACIÓN PROPIA CÁTEDRA

15. REUNIOINES DE CÁTEDRA (2 X AÑO)

16. GUIAS DE TP (TODAS)

17. APUNTES ELABORADOS POR LA CÁTEDRA

18. EJEMPLOS DE TP DE LOS ALUMNOS

19. EJEMPLOS DE PARCIALES TOMADOS

20. PRÁCTICA FORMACIÓN EXPERIMENTAL

21. PRÁCTICA RESOL. PROBL. ING.

22. PRÁCTICA PROYECTO Y DISEÑO

23. PRÁCTICA SUPERV. EN SECT. PRODUCTIVOS

24. DOCENTES AFECTADOS A INVESTIGACIÓN

Apellido y Nombre del Docente	Tipo de Proyecto	Cod. De Proyecto asignado por el DIIT	Nombre del Proyecto	Fecha de Inicio	Fecha de Finaliza-ción

25. ACLARACIÓN, CARGO Y FECHA

"Certifico que el presente programa de estudios de la asignatura Auditoria y Seguridad Informática es el vigente para el ciclo lectivo 2011, guarda consistencia con los contenidos mínimos del plan de estudios y se encuentra convenientemente actualizado"

Firma *Aclaración* *Cargo* *Fecha*