UNIVERSIDAD NACIONAL DEL SUR BAHÍA BLANCA	1/4
DEPARTAMENTO DE CIENCIAS E INGENIERÍA DE LA COMPUTACIÓN	
SEGURIDAD EN SISTEMAS	**CÓDIGO:7901** **ÁREA N°: IV**

CARRERAS
Ingeniería en Computación
Ingeniería en Sistemas de Computación

PROFESOR RESPONSABLE:
Dr. Diego Martinez – Profesor Adjunto con Dedicación Exclusiva
Lic. Leonardo de Matteis – Profesor Adjunto con Dedicación Simple

CARGA HORARIA	Teoría	Práctica	Laboratorio	CANTIDAD DE SEMANAS	
	64	64			16

CORRELATIVAS

PARA CURSAR LA MATERIA		PARA APROBAR LA MATERIA	
APROBADAS	**CURSADAS**	**APROBADAS**	**CURSADAS**
-Sistemas Operativos	-Redes y Teleprocesamiento	-Redes y Teleprocesamiento	

OBJETIVOS

- Comprender las nociones básicas de seguridad informática.
- Desarrollar la capacidad de evaluar y mejorar la seguridad de entornos existentes.

DESCRIPCIÓN

Debido a la creciente popularidad de Internet, la seguridad en sistemas es cada día más importante en nuestro campo. Este curso pretende lograr que el alumno comprenda los principales riesgos y vulnerabilidades de los sistemas actuales y las técnicas, mecanismos y herramientas necesarias para desarrollar y utilizar sistemas seguros.

METODOLOGÍA DE ENSEÑANZA

Los conceptos se presentan en clases teóricas utilizando presentaciones de diapositivas como recurso didáctico. Este material se publica en la página de la materia con la intención de que los alumnos dispongan de un resumen de toda la materia que les sirva de guía para luego ampliar sus conocimientos utilizando la bibliografía.
Las clases teóricas van seguidas de clases prácticas en los que se proponen ejercicios y problemas en los que se aplican los conceptos presentados y clases de laboratorio en los que se plantean proyectos destinados a reforzar la formación experimental.
Adicionalmente en clase se muestran sistemas operativos generales actuales (MS Windows 7, GNU/Linux y FreeBSD) y aplicaciones para mostrar vulnerabilidades, malware, sistemas criptográficos, vulnerabilidades web, etc.

ACTIVIDADES PRÁCTICAS

UNIVERSIDAD NACIONAL DEL SUR
BAHÍA BLANCA

DEPARTAMENTO DE CIENCIAS E INGENIERÍA DE LA COMPUTACIÓN

SEGURIDAD EN SISTEMAS

CÓDIGO:7901

ÁREA N°: IV

Resolución de trabajos prácticos que ilustran y complementan los temas desarrollados en las unidades teóricas.
Realización de un proyecto final. Se busca que el alumno investigue y analice un tema actual de entre los presentados en la teoría y/o en la práctica.
Implementación de laboratorios que ilustren problemas y soluciones inherentes a la seguridad informática.

MECANISMO DE EVALUACIÓN

Para el cursado:
1) Aprobación de trabajos prácticos.
2) Aprobación de un parcial, adicionalmente existe un examen remedial eliminatorio.
3) Aprobación del proyecto final.

Para el final:
1) Aprobación del examen escrito.

PROGRAMA SINTÉTICO

1. Introducción a la seguridad en sistemas.
2. Seguridad física.
3. Criptografía elemental.
4. Autorización, autenticación, control de acceso.
5. Vulnerabilidades de software y de hardware.
6. Introducción a la programación segura.
7. Seguridad en sistemas operativos.
8. Introducción a la seguridad en bases de datos.
9. Seguridad en redes (sniffing, spoofing, firewalls, VPNs, IPSec, auditorías, tests de penetración, detección de intrusos y seguridad en redes wireless).
10. Aplicaciones y seguridad en Internet.
11. Seguridad en *e-commerce*.
12. Privacidad y cuestiones legales y éticas.

PROGRAMA ANALÍTICO

1. Introducción a la seguridad en sistemas
Conceptos y terminología sobre seguridad de la información. CIA: Confidencialidad, integridad y disponibilidad de la información. Amenazas y métodos de defensa.

2. Seguridad física
Aplicación de barreras físicas y procedimientos de control como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Amenazas relacionadas con la seguridad física: desastres naturales, amenazas ocasionadas por el hombre, sabotajes internos y externos. Nociones básicas sobre seguridad e higiene en el trabajo.

DEPARTAMENTO DE CIENCIAS E INGENIERÍA DE LA COMPUTACIÓN

SEGURIDAD EN SISTEMAS

CÓDIGO:7901

ÁREA N°: IV

3. Criptografía elemental
Teoría de Números. Congruencia. Conjunto reducido de restos. Inversos. Teorema de Euler. (Pequeño) teorema de Fermat. Algoritmo extendido de Euclides. Teorema del Resto Chino. Generadores de un número primo.
Criptografía. Introducción. Complejidad. Criptoanálisis. Algoritmos básicos. Funciones hash (*one-way).* Ej: MD5, SHA-1. Cifrado en flujo y en bloque con clave secreta. Firma Digital. Ej: RSA. PKI. Sistemas criptográficos simétricos, asimétricos, e híbridos. Manejo y distribución de claves. Esteganografía.

4. Autorización, autenticación, control de acceso
Principio de Menor privilegio (*need to know*). Mediación completa. Diseño abierto. Aceptación psicológica. *Fail-safe* defaults.
Autenticación: usuario a máquina y máquina a máquina. Sistemas de Autenticación. Kerberos. Passwords. Técnicas de identificación.
Control de Acceso Discreto (DAC). Políticas de Control de Acceso. Listas de Control de Acceso (ACLs). Introducción a la Seguridad en JDK 1.6.
Control de Acceso Mandatorio (MAC). Política de Seguridad Militar, Muralla China y Clark-Wilson. Seguridad Multinivel: modelos Bell-La Padula y Biba.
Políticas de Seguridad.

5. Vulnerabilidades de software y de hardware
Vulnerabilidades de software. Código Malicioso (worms, virus, bombas lógicas, *key loggers*, troyanos, *spyware*, *adware*, cookies). *Buffer overflow*, C*ross Site Scripting* (XSS), Cross Site Request Forgery (CSRF), *SQL Injection,* problemas de configuración. Programas con bugs.
Vulnerabilidades de hardware. Inapropiada operación, fallas en mantenimiento, inadecuada seguridad física. Métodos de ataque. TEMPEST (emanaciones electromagnéticas).

6. Introducción a la programación segura
Principios básicos para el desarrollo de código seguro. Comprobación de buenas prácticas en el código.

7. Seguridad en sistemas operativos
Seguridad en kernels. Protección de hardware. Sistemas de archivos. Diseño de sistemas operativos seguros. *Orange Book, Trusted Computer System Evaluation Criteria (TCSEC)* y *Common Criteria.* Estudio de casos de sistemas operativos tipo UNIX (*BSD y GNU/Linux) y MS Windows.

8. Introducción a la seguridad en bases de datos
Requerimientos de seguridad en bases de datos. Confiabilidad e integridad. Inferencia de datos. Bases de datos multinivel. Seguridad en bases de datos estadísticas. Criptografía y bases de datos.

9. Seguridad en redes
Historia de Internet. Vulnerabilidad de las redes. Virtual Private Networks (VPNs). IETF Security Architecture (IPSec). Sniffing, Spoofing (IP, ARP), ICMP Redirect. Proxies y Firewalls. Detección de Intrusos (IDS). Prevención de Intrusos (IPS). Tests de penetración (ethical hacking). Scanners de vulnerabilidades. Auditorías y pericias informáticas. Seguridad en redes wireless. Seguridad en código móvil (ActiveX, Java, Javascript, Ajax).
Tópicos en administración de sistemas.

10. Aplicaciones y seguridad en Internet
Ataques basados en aplicaciones. E-mail (PGP, PEM y S/MIME). Seguridad en la web (SET y SSL). Autoridades Certificantes (CAs).

UNIVERSIDAD NACIONAL DEL SUR
BAHÍA BLANCA

DEPARTAMENTO DE CIENCIAS E INGENIERÍA DE LA COMPUTACIÓN

SEGURIDAD EN SISTEMAS

CÓDIGO:7901
ÁREA N°: IV

11. Seguridad en *e-commerce*
Tendencias actuales en e-commerce, e-voting y online banking. *Phishing attacks*.

13. Privacidad y cuestiones legales y éticas
Privacidad. Ética profesional. Legislación Argentina: Ley de Delito Informático (Ley 26.388) y Ley de Firma Digital (Ley 25.506), Ley de Protección de Datos Personales (Ley 25.326), Ley de Confidencialidad (Ley 24.766).
Spam. Ingeniería social.
Estándares internacionales: familia de normas ISO/IEC 27000, COBIT, ITIL, HIPAA.

BIBLIOGRAFÍA

1. Security in Computing, 4th ed., C. Pfleeger, Prentice-Hall, 2006. ISBN 0132390779.
2. Cryptography and Network Security, 2nd ed., Stallings, Prentice Hall 1999, ISBN 0138690170.
3. Security Engineering: A Comprehensive Guide to Building Dependable Distributed Systems, R. Anderson, John Wiley & Son, 2001, ISBN 0471389226.
4. Fundamentals of Computer Security Technology, E. Amoroso, Prentice Hall, 1994, ISBN 0131089293.
5. Computer Security, D. Gollmann, Jhon Wiley & Son, 1999, ISBN 0471978442.
6. Applied Cryptography, B. Schneider, John Wiley & Son, 2nd ed., 1996, ISBN 0471117099.
7. Network Security Essentials: Applications and Standards, 2000, Prentice Hall, ISBN 0130160938.
8. Software Security: Building Security In, Gary McGraw, Addison-Wesley, 2006, ISBN 0321356705.
9. Risk Analysis and the Security Survey, 3rd ed., James F. Broder, Butterworth-Heinemann, 2006, ISBN 0750679220.
10. The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities, Mark Dowd, John McDonald, Justin Schuh, Addison-Wesley, 2006, ISBN 0321444426.
11. Principles of Information Security, 2nd ed., by Michael E. Whitman, Herbert J. Mattord, ISBN 0619216255.
12. Network Security: The Complete Reference, Mark Rhodes-Ousley, Roberta Bragg, Keith Strassberg, McGraw-Hill, 2003, ISBN 0072226978.
13. Computer Security Lab Manual (Information Assurance & Security), Vincent J. Nestler, Wm. Arthur Conklin, Gregory B. White, Matthew P. Hirsch, Career Education, 2005, ISBN 0072255080.

Otros: Papers suministrados por la cátedra.

AÑO	**FIRMA PROFESOR RESPONSABLE**
2019	

VISADO

COORDINADOR ÁREA	SECRETARIO ACADÉMICO	DIRECTOR DEPARTAMENTO
		Dr. MARCELO A. FALAPPA DIRECTOR-DECANO DPTO. DE CS. E ING. DE LA COMP. UNIVERSIDAD NACIONAL DEL SUR