100 2019 · Año del Centenario de la Universidad Nacional del Litoral

SANTA FE, 21 de octubre de 2019.-

VISTO el expediente de referencia mediante el cual, Secretaría Académica, propone la incorporación de la asignatura “Seguridad Informática” como asignatura optativa para la carrera Ingeniería en Informática, y

CONSIDERANDO:

QUE se cuenta con los antecedentes y el programa de la asignatura propuesto;

QUE la Comisión de Seguimiento Académico de la carrera avala la propuesta;

POR ELLO, y teniendo en cuenta despacho de las Comisiones de Enseñanza, y de Interpretación y Reglamentos,

EL CONSEJO DIRECTIVO
De la Facultad de Ingeniería y Ciencias Hídricas
Resuelve:

ARTÍCULO 1º.- Aprobar la incorporación de la asignatura “Seguridad Informática” como asignatura optativa para la carrera Ingeniería en Informática, la que tendrá una carga horaria semanal de 4 horas (haciendo un total de 60 horas), requiriéndose para su cursado tener aprobado el 6º cuatrimestre de la carrera y la asignatura “Redes y Comunicación de Datos I”, y regularizada la asignatura “Redes y Comunicación de Datos II”.

ARTÍCULO 2º.- Inscríbase, comuníquese, dese a publicidad. Tome nota Secretaría Académica, Departamento Alumnado, Bedelía, Director del Departamento Informática e Ing. Gastón MARTÍN. Cumplido, archívese.-

RESOLUCIÓN CD Nº **355/19**

Universidad Nacional del Litoral
Facultad de Ingeniería y Ciencias Hídricas
Consejo Directivo

Ciudad Universitaria – C.C. 217
Ruta Nacional N° 168 – Km 472,4
(3000) Santa Fe – Argentina
Tel: (54)(0342) 4575 233 / 245 / 246 – int. 213
Fax: (54) (0342) 4575 224
E-mail: consejo@fich.unl.edu.ar

ANEXO Resol CD Nº 355/19

CARGA HORARIA SEMANAL:

TEORÍA:	20 Horas
PRÁCTICA (total):	40 Horas
Formación experimental	4 Horas
Resolución de ejercicios prácticos	25 Horas
Resolución de problemas abiertos	15 Horas
Proyecto y Diseño	6 Horas

CARGA HORARIA TOTAL: 60 horas

JUSTIFICACIÓN

El crecimiento exponencial que han tenido las diferentes tecnologías, así como sus protocolos, aplicaciones, estándares y otros recursos, han traído implícito un elevado número de ataques y nuevas formas de comprometer los recursos computacionales.

Actualmente, las organizaciones modernas que operan o centran gran parte de su actividad en el negocio a través de Internet necesitan dotar sus sistemas e infraestructuras informáticas de las políticas y medidas de protección más adecuadas que garanticen el continuo desarrollo y sostenibilidad de sus actividades; en este sentido, cobra especial importancia el hecho de que puedan contar con profesionales especializados en las nuevas tecnologías de seguridad que implementen y gestionen de manera eficaz sus sistemas.

La administración eficiente de redes y de la seguridad informática toma cada vez más relevancia en la gestión corporativa apoyada en tecnologías informáticas y es en este sentido donde la oferta de esta Asignatura apunta a orientar elementos teóricos y prácticos de la seguridad, las técnicas de intrusión, medidas que contrarrestan la inseguridad y estrategias de programación segura.

En concordancia con lo mencionado, la Asamblea del Consejo Federal de Decanos de Ingeniería de la República Argentina ha aprobado la incorporación del descriptor de conocimiento “Seguridad Informática” para las carreras de Ingeniería en Informática en la Propuesta de estándares de segunda generación para la acreditación de carreras de ingeniería en la República Argentina “Libro Rojo de CONFEDI”. Ante dicha propuesta, surge la necesidad de que la FICH incorpore dichos contenidos al plan de estudio de la carrera Ingeniería en Informática.

OBJETIVOS DE LA ASIGNATURA

Objetivos General

Que el alumno logre una comprensión de los conceptos de seguridad de la información y los requisitos mínimos en la gestión de seguridad informática y seguridad de la información en infraestructuras TI a partir de los estándares internacionales para proyectar y dirigir lo referido a seguridad de la información y a seguridad informática.

Objetivos Específicos.

Que el alumno logre:

- Conocer los estándares internacionales relacionados con Seguridad de la Información.
- Entender la importancia de los controles de seguridad para asegurar los activos de información de una organización/entidad/empresa.
- Obtener los conocimientos teóricos y prácticos necesarios para establecer, documentar, implementar y realizar la gestión, implementación, mantenimiento y auditorias en Seguridad de la Información.
- Aprender a planificar, implementar, gestionar, medir y documentar correctamente un Sistema de Gestión de la Seguridad de la Información.
- Se orienten respecto de cómo gestionar y mejorar en forma continua la Seguridad de la Información en una organización/entidad/empresa.
- Obtener los conocimientos teóricos y prácticos necesarios para dirigir y controlar la implementación, operación y mantenimiento de lo anteriormente mencionado.

CONTENIDOS MINIMOS

Conceptos básicos de seguridad y terminología relacionada.
Criptografía y sus aplicaciones (Firma digital, PKI, Esteganografía)
Amenazas: Técnicas de descubrimiento, scanning, sniffing.
Vulnerabilidades de los sistemas - Ataques. Seguridad de aplicaciones WEB. Mecanismos de protección: Firewalls, IDS e IPS y honeypots.
Serie ISO 27000: prácticas recomendadas

PROGRAMA ANALÍTICO

Unidad 1 – Introducción a la seguridad
Conceptos de seguridad informática . Confidencialidad, integridad, autenticidad, no repudio.
Vulnerabilidad, Amenaza, Incidente. Gestión de la Seguridad: Estándares, procedimientos y guías.

Teoría: 2
Práctica: 5

Unidad 2 – Criptografía
Los principios, medios y métodos de protección de la información para asegurar su integridad, confidencialidad y autenticidad. Aplicaciones y usos de la criptografía. Protocolos y estándares. Criptografía simétrica y asimétrica. Firma digital. Gestión de claves. Public key infrastructure (PKI). Blockchain vs PKI. Ataques y criptoanálisis.

Teoría: 3
Práctica: 5

Unidad 3 – Control de acceso
Sistemas y metodologías que permiten crear una arquitectura segura para proteger los activos de los sistemas de información. Identificación y autenticación. Single sign-on. Acceso centralizado - descentralizado - distribuido. Metodologías de control. Monitorización y tecnologías de control de acceso.

Teoría: 3
Práctica: 5

Unidad 4 – Seguridad de las operaciones

Redundancia. Contingencia. Monitoreo. Separación de ambientes operativos. Autenticación de máquinas/dispositivos. Diseño de políticas de accesos remotos. Soluciones de acceso a redes basadas en infraestructura PKI, OTP, 802.1x. Plan de recuperación de desastres.

Teoría: 4
Práctica: 5

Unidad 5 – Seguridad de las comunicaciones
Gestión de la seguridad en las comunicaciones. Protocolos de red. Identificación y autenticación. Comunicación de datos. Seguridad de Internet y Web. Métodos de ataque. Seguridad en Multimedia.

Teoría: 4
Práctica: 4

Unidad 6 – Desarrollo seguro de las aplicaciones
Gestión del software. Análisis de Vulnerabilidades. Desarrollo, mantenimiento y testing de planes. Riesgos de seguridad más importantes en aplicaciones web: Inyección SQL, Pérdida de Autenticación, Exposición de Datos Sensibles, Pérdida de Control de Acceso, Configuración de Seguridad Incorrecta, Cross-Site Scripting (XSS), Deserialización Insegura, Uso de Componentes con Vulnerabilidades Conocidas, Registro y Monitoreo Insuficientes.

Teoría: 4
Práctica: 6

METODOLOGÍA DE ENSEÑANZA

Las clases se desarrollarán en el Laboratorio de Redes y Seguridad Informática. Se organizará en las modalidades teórico-prácticas con soporte de presentaciones digitales y prácticas en función de cada clase.

En las clases se presentan los contenidos teóricos y se van resolviendo en forma conjunta ejemplos que ayuden a comprender los nuevos conceptos introducidos.

La formación práctica está basada en la resolución de problemas tipo y de actividades cuyas resoluciones se realizan principalmente en las computadoras, utilizando aplicaciones software libre diseñadas principalmente para la auditoría y seguridad informática para lograr un contacto directo con las tecnologías actuales.

Se utilizará la plataforma moodle, una plataforma virtual que sirve de apoyo para el desarrollo de la asignatura. En dicha plataforma se publicarán guías teóricas, trabajos prácticos, apuntes y será utilizada como medio de comunicación entre alumnos y docentes y entre los mismos alumnos.

REQUISITOS PARA EL CURSADO

Además del requisito del 6to. Cuatrimestre aprobado, el estudiante deberá contar con
Redes y Comunicaciones de Datos I: aprobada
Redes y Comunicaciones de Datos II: regularizada

BIBLIOGRAFÍA

Básica:

- Cryptography and Network Security, 6Th Edition – William Stallings. Prentice Hall

- Framework for Improving Critical Infrastructure Cybersecurity - NIST (National Institute of Standards and Technology) , v1.1 April 2018 https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- CEH v9: Certified Ethical Hacker Version 9 Study Guide
- Hacking con Kali Linux - v 2.7 , 2018 - Alonso Eduardo & Caballero Quezada http://www.reydes.com/archivos/Kali_Linux_v2_ReYDeS.pdf
- Graves, K. CEH – Certified Ethical Hacking. Study Guide. Wiley Publishing, Inc. ISBN 978-0-470-52520-3. Año 2010. Harris, S. CISSP – Certification Exam Guide, Sixth Edition. Editorial Mc Graw Hill

Complementaria:

- Norma ISO/IEC 27001:2013 –Information technology - Security techniques - Information security management systems - Requirements
- Norma ISO/IEC 27002:2013 –Information technology — Security techniques — Code of practice for information security controls
- The Open–source PKI Book: A guide to PKIs and Open–source Implementations - Symeon (Simos) Xenitellis, Version 2.4.6 Edition http://ospkibook.sourceforge.net/docs/OSPKI-2.4.7/OSPKI.pdf
- Trusted Computer System Evaluation Criteria ["Orange Book"] - Department of Defense, USA https://csrc.nist.gov/csrc/media/publications/conference-paper/1998/10/08/proceedings-of-the-21st-nissc-1998/documents/early-cs-papers/dod85.pdf
- OWASP Top 10 - 2017 - The Ten Most Critical Web Application Security Risks, The Open Web Application Security Project https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf
- OWASP Testing Guide v4 - The Open Web Application Security Project https://www.owasp.org/images/1/19/OTGv4.pdf
- ISBN 978-0-07-178173-2. Año 2011. Tanembaum, A. Computer Networks. 4ta Ed. Prentice Hall. Año 2011.
- Faircloth, Jeremy. Penetration Tester´s Open Source Toolkit, Third Edition. Año 2011. Denning, D. Cryptography and Data Security. Addison-Wesley. Año 1982. Kaufman, C.

CRONOGRAMA DE ACTIVIDADES

A continuación se presenta el cronograma para el aborde correspondiente:

Semana	Tema	Tipo*
1	Introducción a la Seguridad / Criptografía	T
2	Criptografía	P
3	Control de Acceso	T
4	Criptografía / Control de Acceso	P
5	Parcial 1	E
6	Seguridad de las operaciones	T
7	Seguridad de las operaciones	P
8	Seguridad de las comunicaciones	T
9	Seguridad de las comunicaciones	P
10	Desarrollo seguro de aplicaciones	T
11	Desarrollo seguro de aplicaciones	P
12	Desarrollo seguro de aplicaciones / Consultas	P
13	Parcial 2	E
14	Consultas	T/P
15	Recuperatorios	E

Referencias:
* T: teoría P: práctica E: evaluación

CONDICIONES PARA REGULARIZAR Y PROMOVER LA ASIGNATURA

De acuerdo al Régimen de Enseñanza de Grado y Pregrado Presencial de la FICH (Res. CD Nº 300/16, arts. 30, 31, 32 y 33).

Para regularizar:

- Tener al menos 80% de asistencia en clases teórico-prácticas
- Obtener al menos 40% en cada uno de los parciales
- Presentación de trabajos prácticos

Para promover:

- Tener al menos 80% de asistencia en clases teórico-prácticas
- Obtener un promedio mínimo de 70% y no menos del 60% en cada uno de los parciales o en sus respectivos recuperatorios
- Presentación de trabajos prácticos

EVALUACIONES

PARCIALES		
TEMAS	**ORAL/ESCRITO**	**FECHA**
Introducción a la Seguridad / Criptografía / Control de Acceso	Escrito	A definir
Seguridad de las operaciones / Seguridad de las comunicaciones / Desarrollo seguro de aplicaciones	Escrito	A definir
RECUPERATORIO		
TEMAS	**ORAL/ESCRITO**	**FECHA**
Introducción a la Seguridad / Criptografía / Control de Acceso	Escrito	A definir
Seguridad de las operaciones / Seguridad de las comunicaciones / Desarrollo seguro de aplicaciones	Escrito	A definir