Asignatura: Seguridad de la Información
Carrera: Ingeniería en Informática
Ciclo Lectivo: 2016
Docente/s: Ing. Carlos Alberto Schenone.
Carga horaria semanal: 4 horas.
Tipo de Asignatura: Teórico-práctica.

Fundamentación: Seguridad de la información es una materia obligatoria correspondiente al tercer año de la carrera Ingeniería en Informática. En la materia se abordan temáticas relacionadas con las vulnerabilidades y protección de la información visto como el principal activo de las organizaciones.
Las unidades teóricas y actividades prácticas vinculan lo académico con lo profesional de forma que los estudiantes integren las temáticas de la cursada con los conocimientos adquiridos en las asignaturas Redes de Computadoras I y Redes de Computadoras II. Durante el cuatrimestre se desarrolla un trabajo práctico integrador aplicando los nuevos conceptos, herramientas y recursos presentados en la asignatura en un entorno similar al ámbito laboral.

Objetivos:
Que los alumnos:
- sean capaces de identificar las amenazas a las que está expuesta la información.
- detecten e identifiquen los objetivos de la seguridad de la información.
- identifiquen los escenarios de las vulnerabilidades de la información.
- sean capaces de seleccionar y aplicar mecanismos de protección contra las amenazas a las que está expuesta la información.
- puedan evaluar el nivel de riesgos a los cuales están expuesta la información.

Contenidos mínimos: Conceptos básicos de seguridad. Terminología relacionada. Legislación nacional relacionada con la seguridad de la información. Criptografía. Firma digital. PKI. PGP. Esteganografía. SSL. Amenazas: Técnicas de descubrimiento, scanning, sniffing, etc. Mecanismos de protección: Firewalls, IDS y Honeypots. Nociones básicas de gestión de seguridad de la información.

Contenidos Temáticos o Unidades:
Unidad I. Conceptos de Seguridad de la Información. Elementos clave. Amenazas a la seguridad. Política de seguridad. Conceptos de seguridad en redes. Conceptos básicos de seguridad informática. Legislación nacional e internacional relacionada con la seguridad de la información. Organismos de consulta.

Unidad II. Descubrimiento y Escaneo. Conceptos de descubrimiento y escaneo. Técnicas de scanning y sniffing. Herramientas.

Unidad III. Código Malicioso. Tipo de código malicioso. Clasificación. Tipos de Virus y su clasificación. Daños que producen. Medidas de protección. Troyanos. Clasificación y medidas de protección. Cookies. Medidas de protección. Keyloggers. Clasificación y medidas de protección. Spyware. Medidas de protección.

Unidad IV. Seguridad en el acceso y Redes LAN Virtuales (VLAN). Conceptos de seguridad en el acceso. Arquitectura AAA. Métodos de autenticación. Implementaciones. Username y Password. One-Time-Password. Protocolo TACACS y RADIUS. Servidores de Acceso (NAS). Introducción a las VLAN. Tipos de VLANs. Ventajas y aplicaciones.

Unidad V. Análisis de Vulnerabilidades. Introducción a la vulnerabilidad en redes. Objetivo del análisis de vulnerabilidades. Tipos de análisis de vulnerabilidades. Conceptos de Test de penetración. Herramientas. Organismos de consulta. Metodologíasdel análisis de vulnerabilidades. Acuerdo de Confidencialidad. Conceptos de análisis de riesgos.

Unidad VI. Firewall y Listas de control de acceso. Introducción y tipos de firewall. Arquitecturas. Filtrado de tráfico. Concepto de Firewall personal y Sistemas de detección de intrusos (IDS). Conceptos de Proxy y Honeypots.

Unidad VII. Criptografía. Tipos de algoritmos. Ataques criptográficos. Claves. Algoritmos simétricos y asimétricos. Arquitectura PKI. Funciones Hash. Firma digital y sobres digitales. Esteganografia. PGP. SSL

Unidad VIII. Túneles y Redes Privadas Virtuales (VPN). Aspectos generales. Implementación de VPN. Ventajas y limitaciones. Tunelización. Protocolos de túnel.

Bibliografía Obligatoria:

- 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 ISBN 978-0-07-178173-2. Año 2011.
- Tanembaum, A. Computer Networks. 4ta Ed. Prentice Hall. Año 2011.

Bibliografía de consulta:

- Faircloth, Jeremy. Penetration Tester´s Open Sorce Toolkit, Third Edition. Año 2011.
- Denning, D. Cryptography and Data Security. Addison-Wesley. Año 1982.
- Kaufman, C.; Perlman, R.; Speciner, M.. Network Security. Prentice Hall. Año 1995.
- Stallings, W. Network and Internetwork Security. Prentice Hall. Año 1995.
- Chapman, D.; Zwicky E. Building Internet Firewalls. O'Reilly Media. Año 2000.
- Doraswamy, N.; Harkins, D. IPSec: the new security standard for the Internet, intranets, and virtual private networks. Prentice Hall. Año 1999.

- ISO 27000. Family of information security standards. ISO 27001: 2005.
- Designing And Implementing Linux Firewalls And QoS. Autor: Lucian Gheorghe
- Foster, J., Bayles, A. & Long, J. Penetration tester's open source toolkit.

Modalidad de dictado: Las clases se desarrollaran en el Laboratorio de informática. Se organizaran en las modalidades teórico-practicas 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 de proyecto y diseño, cuyas resoluciones se realizan principalmente en las computadoras, utilizando aplicaciones de uso en la industria que permitan un contacto directo con las tecnologías actuales.
El material correspondiente a las clases teóricas, así como los documentos de la práctica se encontraran disponibles a través de un grupo Web al cual los estudiantes tendrán acceso. Este mecanismo también será utilizado para realizar consultas simples.

Régimen de aprobación: La evaluación integradora de las instancias teóricas se realiza a través de dos parciales teóricos. Además, los estudiantes deberán desarrollar un trabajo práctico para cada unidad temática y un trabajo final donde se integren los temas vistos en la materia. Las clases son obligatorias ya que implican participación y debate que forman parte de la evaluación.
La asignatura puede aprobarse mediante el régimen de promoción directa, o por exámenes finales regulares o libres.
Al finalizar la cursada, cada estudiante tendrá una calificación correspondiente a la parte teórica (NT) obtenida del promedio de los dos parciales, una calificación de la parte teórica (NP) obtenida del promedio de los trabajos prácticos y una calificación de la defensa del Trabajo Integrador (NTI), así la nota final de la asignatura se obtiene de la siguiente manera:

NOTA CURSADA = 0.3 * NT + 0.3 * NP + 0.4 * NTI

Todas las instancias evaluativas tienen una posibilidad de un examen recuperatorio para quienes hayan obtenido entre 0 (cero) y 6 (seis) puntos y para quienes hayan estado ausentes con justificación en la evaluación parcial.
Para acceder a la promoción directa los alumnos deberán obtener como NOTA CURSADA un mínimo de 7 (siete) y con una nota mínima de 6 (seis) en cada instancia de evaluación. Para acceder a la promoción, en caso de haber obtenido 6 (seis) en alguno de los parciales, deberá obtener un mínimo de 8 (ocho) en el parcial restante.
Si se obtuviera una NOTA CURSADA inferior a 6 (seis) y superior o igual a 4 (cuatro), en cualquiera de las instancias puede acceder al recuperatorio para intentar mejorar la nota y acceder a la promoción directa; en caso que o logre alcanzar una NOTA CURSADA de

7 (siete) implica que no logra la promoción de la materia y deberá rendir un examen final que se aprobara con una nota no inferior a 4 (cuatro) puntos.
La asignatura se regulariza obteniendo una NOTA CURSADA de 4 (cuatro) o más puntos y cumpliendo el régimen de asistencia al 75% de las clases presenciales como mínimo.