PROGRAMA de Seguridad de la Información

Carreras: Tecnicatura Universitaria en Programación Informática - Licenciatura en Informática

Asignatura: Seguridad de la Información

Núcleo al que pertenece: Complementario

Profesor: Marcelo Cipriano

Asignaturas Correlativas: Laboratorio de Sistemas Operativos y Redes

Objetivos:

- Comprender la importancia de la seguridad informática y seguridad de la información en los distintos contextos.
- Comprender los aspectos técnico y no técnicos de la seguridad.
- Analizar cuestiones básicas de seguridad en una organización a nivel ofensivo y defensivo.
- Realizar prácticas básicas con herramientas profesionales de seguridad.
- Aplicar los conocimientos de programación en la realización de actividades relacionadas a la seguridad informática.

Contenidos mínimos:

- Introducción a la Seguridad de la Información. Conceptos fundamentales y objetivos.
- Gestión de la Seguridad de la Información. Riesgo: análisis y tratamiento.
- Conceptos de Criptografía. Criptografía Simétrica y Asimétrica. Algoritmos de Hash.
- Infraestructura de Clave Pública. Certificados digitales.
- Seguridad en Redes. Objetivos. Ataques, Servicios y Mecanismos de Seguridad. Seguridad en Redes Inalámbricas. Control de Acceso Lógico. Controles físicos de seguridad: seguridad en el centro de cómputos.
- Seguridad en las operaciones. Gestión de usuarios. Control de cambios. Métodos de Evaluación de seguridad: Auditor as, Evaluaciones funcionales, Vulnerability Assessment y Penetration Test. Gestión de Incidentes.
- Seguridad en Aplicaciones. Vulnerabilidades. Software malicioso. Problemática de las aplicaciones WEB.
- Leyes, Regulaciones y Estándares. Marcos legales nacional e internacional.

Carga horaria semanal: 4 hs

Programa analítico:

Unidad 1: Introducción

Introducción a la Seguridad de la Información. Confidencialidad, Integridad y Disponibilidad. Identificación, Autenticación, Autorización y Accountability. Definición de Activo de información, Vulnerabilidad, Amenazas y Riesgos.

Unidad 2: Sistemas de Gestión de la Seguridad de la Información (SGSI)

Introducción a los Sistemas de Gestión. Modelo PDCA. Enfoque Top Down Vs. Enfoque Bottom Up. Familia ISO/IEC 27.00X. Clasificación de la Información. Análisis de Riesgos como base de los SGSI.

Unidad 3: Criptografía

Elementos de criptografía. Requerimientos de la criptografía. Un poco de matemática. Tipos de cifrados. Hitos de la Criptografía. Cifrado Simétrico. Algoritmos estándares. Problemas de los algoritmos simétricos o de clave pública/privada. Cifrado Asimétrico. Funciones unidireccionales con trampa y problemas matemáticos. Criptografía híbrida.

Unidad 4: Algoritmos de Hash

Funciones unidireccionales. Funciones hash. Necesidad de las funciones hash. Funciones estándares. Integridad de los mensajes.

Unidad 5: Firma Digital e Infraestructura de Clave Pública

Introducción a PKI. Componentes. PGP. Autoridades de certificación internacionales. Firma electrónica y firma digital.

Unidad 6: Implementación de controles

Introducción al control de acceso. Tipos de controles de acceso. Controles preventivos, detectivos y correctivos. Controles Físicos, Lógicos y Administrativos.

Unidad 7: Seguridad en las operaciones

Seguridad en los sistemas. Hardening de sistemas. Gestión de usuarios. Métodos de Evaluación de Seguridad: Vulnerability Assessment y Test de Intrusiones. Monitoreo.

Unidad 8: Seguridad en Redes

Objetivos. Modelo OSI. Ataques, Servicios y Mecanismos de Seguridad. Modelo TCP/IP. Controles y dispositivos de seguridad. Seguridad en el perímetro. Firewalls y proxies. Redes Virtuales (VLANs). Redes Privadas Virtuales (VPNs). IPSec. Seguridad en redes inalámbricas.

Unidad 9: Seguridad en Aplicaciones

Introducción a la seguridad en el software. Problemática del desarrollo de aplicaciones. Ciclo de vida del desarrollo del software. Software malicioso: Troyanos, backdoors, virus y gusanos. Otros tipos de malware. Niveles de maduración. Problemática de las aplicaciones WEB. OWASP Top 10.

Bibliografía obligatoria:

- Stallings, William. “Fundamentos de Seguridad en Redes”, 2da. Edición. Ed. Pearson Prentice Hall. ISBN: 84-205-4002-1. 2004
- IRAM-ISO-IEC 27001, Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información. Requisitos. IRAM, 2015.

- Magerit v3, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Ministerio de Hacienda y Administraciones Públicas, 2012.- NIPO: 630-12-171-8.

Bibliografía de consulta:

- Stallings, William: Fundamentos de Seguridad en Redes, 2da. Edición. Ed. Pearson Prentice Hall. 2004. ISBN: 84-205-4002-1.
- Schneier, Bruce: Applied Cryptography, Octubre 2007. Ed. Wiley. ISBN: 978-0470226261.
- Alexander, Alberto. Diseño de un Sistema de Gestión de Seguridad de Información. Óptica ISO 27001:2005. Ed. Alfaomega. 2007. ISBN: 978-958-682-713-3.
- Kaufman, Perlman, and Speciner: Network Security, Prentice Hall. 2nd. Ed.; 2002. ISBN: 0130460192.
- Stallings, William: Criptography and Network Security, 6ta. Edición. Prentice Hall. 2013.
- Héctor Jara y Federico Pacheco: Ethical Hacking 2.0. 2012, MP Ediciones. ISBN: 978-987-1347-93-3
- Héctor Jara y Federico Pacheco: Hackers al Descubierto. 2009, MP Ediciones. ISBN: 978-987-663-008-5

Organización de las clases:

- Clases teóricas desarrolladas en base a presentaciones tipo Powerpoint desde la PC.
- Clases demostrativas donde se muestra el uso de aplicaciones y software especializado.
- Trabajos de laboratorio en los cuales se desarrollan actividades técnicas con consigna.

Trabajos prácticos:

Trabajo Práctico N°1: *Monografía con tema a elección.*
El objetivo de este trabajo es poner en práctica la escritura técnica a la vez que se explora algún contenido específico de la materia. La actividad requerida es una monografía breve sobre un tema a elección que se debe investigar entre los contenidos mencionados en clase. El entregable consta de un documento en formato de artículo de IEEE (plantilla provista por la cátedra) y la presentación oral del mismo en un tiempo predefinido. La realización del mismo es de manera individual.

Trabajo de Laboratorio N°1: *Quine*.
El objetivo de este trabajo es aplicar los conceptos vistos en clase en relación al principio de funcionamiento del software malicioso (malware) y en especial de los virus informáticos clásicos. La actividad requerida es el desarrollo de un programa en cualquier lenguaje, que cumpla con la condición del algoritmo de Quine, es decir que imprima por pantalla su propio código fuente. El entregable consta del programa en cuestión, con los comentarios correspondientes y un instructivo de ejecución. La realización del mismo es de manera individual.

Trabajo de Laboratorio N°2: *Criptografía*.
El objetivo de este trabajo es aplicar los conceptos vistos en clase en relación al principio de funcionamiento de los algoritmos criptográficos simétricos. La actividad requerida es el desarrollo de un programa en cualquier lenguaje, que reciba por su entrada un archivo y una contraseña, y le aplique el algoritmo criptográfico AES 256 bits con todos sus parámetros, utilizando de funciones de librería, para luego producir en la salida una versión del mismo archivo cifrado. Además, el pograma debe poder tomar el archivo resultante y realizar el proceso inverso. El entregable consta del programa en cuestión, con los comentarios correspondientes y un instructivo de ejecución. La realización del mismo es de manera individual.

Trabajo Práctico N°2: *Demostración práctica*.
El objetivo de este trabajo es poner en práctica la escritura técnica a la vez que se explora algún contenido práctico de la materia. La actividad requerida es una monografía sobre un tema a elección que se debe investigar entre los contenidos mencionados en clase, que se refleje en una demostración prática. El entregable consta de un documento en formato de artículo de IEEE (plantilla provista por la cátedra) y la presentación oral del mismo en un tiempo predefinido. La realización del mismo es de manera grupal.

Modalidad de evaluación:

Los mecanismos de evaluación en modalidades libre y presencial de esta asignatura están reglamentados según los siguientes artículos del Régimen de estudios de la UNQ (Res. CS 201/18)

En la modalidad de libre, se evaluarán los contenidos de la asignatura con un examen escrito, un examen oral e instancias de evaluación similares a las realizadas en la modalidad presencial.

CRONOGRAMA TENTATIVO

Semana	Tema/unidad	Actividad*				Evaluación
		Teórico	Práctico			
			Res Prob.	Lab.	Otros Especificar	
1	Introducción a la seguridad	X				
2	Vulnerability research y evaluaciones de seguridad	X				
3	Malware, botnets y cibercrimen	X		X		
4	Criptografía	X				
5	Criptografía y Esteganografía	X		X		
6	Seguridad en redes	X				
7	Seguridad en redes			X		
8	Presentaciones TP1	X			TP	
9	Sistemas de control de accesos	X				
10	Gestión de la seguridad y gestión de riesgos	X				
11	Seguridad en aplicaciones web	X				
12	Seguridad en el desarrollo de software	X				
13	Seguridad en el desarrollo de software	X				
14	Examen					X
15	Presentaciones TP2				TP	
16	Recuperatorios y cierre					

***INDIQUE CON UNA CRUZ LA MODALIDAD**

Firmado digitalmente por: SUAREZ Mariana Alejandra
Directora del Departamento de Ciencia y Tecnologla
UNIVERSIDAD NACIONAL DE QUILMES