2825 – PRINCIPIOS DE SEGURIDAD INFORMÁTICA

UASLP
Universidad Autónoma de San Luis Potosí

FACULTAD DE INGENIERÍA
Área de Ciencias de la Computación

Clave de la materia: 2825
Clave Facultad: 2825
Clave U.A.S.L.P.: ---- **Clave CACEI:** IA
Nivel del Plan de Estudios: I.S.I.: 6/I.I.: 10 **No. de créditos:** 8
Horas/Clase/Semana: 4 **Horas totales/Semestre:** 64
Horas/Práctica (y/o Laboratorio): 0
Prácticas complementarias: 0
Trabajo extra-clase Horas/Semana: 4
Carrera/Tipo de materia: I.S.I./Electiva de Área de Énfasis
I.I./Optativa
No. de créditos aprobados: 200 créditos del Núcleo Básico
Fecha última de Revisión Curricular: 26-junio-2020
Materia y clave de la materia requisito: I.S.I.:2822 – Redes de Computadoras y Seguridad
I.I.: 2830 – Telemática A

OBJETIVO DEL CURSO

Analizar los conceptos fundamentales y principios de la seguridad informática necesarios; además de ser capaces de aplicarlos para el funcionamiento de una organización.

CONTENIDO TEMÁTICO

1. AMENAZAS Y ATAQUES

Tiempo Estimado: 16 hrs.

Objetivo: Analizar y ser capaz de identificar los riesgos, amenazas y vulnerabilidades de seguridad informática, así como los ataques más comunes.

1.1. Principios de seguridad
1.2. Motivación del atacante
1.3. Malware
1.4. Denial of Service
1.5. Ingeniería Social

2. POLÍTICAS DE SEGURIDAD Y LEGISLACIÓN

Tiempo Estimado: 16 hrs.

Objetivo: Conocer y analizar las leyes, buenas prácticas, estándares nacionales e internacionales relacionados a la seguridad informática.

2.1. Políticas de privacidad
2.2. Buenas prácticas y estándares de seguridad

3. SEGURIDAD DE REDES

Tiempo estimado: 16 hrs.

Objetivo: Conocer las amenazas de seguridad para redes y saber aplicar las herramientas disponibles para evitarlas.

3.1. Amenazas y ataques para redes
3.2. Integridad y confidencialidad de los mensajes en la red
3.3. Protocolos seguros de comunicación
3.4. Mecanismos de defensa

4. PRINCIPIOS DE SOFTWARE SEGURO

Tiempo estimado: 16 hrs.

Objetivo: Conocer y aplicar los principios para diseñar y programar software seguro.

4.1. Principios de diseño seguro
4.2. Programación en defensa

METODOLOGÍA

Desarrollo del tema por parte del profesor siguiendo el método de aprendizaje basado en problemas. Se espera que el alumno investigue ciertos temas, siguiendo el método de aula invertida. Implementar estrategias de trabajo en equipo cuando sea conveniente (aprendizaje colaborativo).

EVALUACIÓN

Se realizarán cuatro exámenes parciales de forma colegiada en las fechas establecidas por la Facultad, de acuerdo con el Reglamento de Exámenes. La calificación de los exámenes parciales estará compuesta por la evaluación del examen parcial y por otras actividades, como: tareas, investigaciones, resolución de problemas, ejercicios, etc. La calificación del examen ordinario es el promedio de los cuatro parciales.

BIBLIOGRAFÍA

Bibliografía Básica

Whitman, M., Mattord H., *Principles of Information Security*. 6ª Ed., Cengage Learning, 2017.

Ozkaya, E. *Learn Social Engineering: Learn the Art of Human Hacking with an Internationally Renowned Expert*. Packt Publishing, 2018.

McClure, S., Scambray, J., Kurtz, G. *Hacking Exposed 7: Network Security Secrets & Solutions*. McGraw Hill, 2012.

Viega, J., McGraw, G. *Building Secure Software: How to Avoid Security Problems the Right Way*. Addison-Wesley, 2002.

Kurose, J.F., Ross, K.W. *Computer Networking: A top-down Approach Featuring the Internet*. 7a Ed., Addison-Wesley, 2016.

Bibliografía Complementaria

Grime, R. *Hacking the Hacker: Learn from the Experts Who Take Down Hackers*. Wiley, 2017.

Bass, L., Clements, P., Kazman, R. *Software Architecture in Practice*. 2nd Ed., Addison-Wesley, 2003.