CENTRO DE INVESTIGACIÓN EN MATEMÁTICAS, A.C.

CIMAT

MAESTRÍA EN INGENIERÍA DE SOFTWARE

Plan de Estudios 2015

INFORMACIÓN GENERAL

Materia	Tópicos Selectos de Aseguramiento
Titular / Cotitular	Dr. Jezreel Mejia / Dr. Luis Julián Domínguez/ Dra. Mirna Muñoz
Fecha de elaboración	2015-04-14

INTRODUCCIÓN GENERAL DE LA MATERIA

Actualmente existe un crecimiento importante en el aseguramiento del software, principalmente debido a crecimiento potencial de los ataques a sistemas de software y a la severidad de las consecuencias en caso de fallos en los sistemas software. Se hace cada vez más necesario adquirir y dominar el conocimiento en temas relacionados con el aseguramiento del software.

El aseguramiento del software surge como una disciplina que proporciona requisitos de niveles de dependencia y seguridad en el desarrollo, adquisición y operación del software, abarcando actividades enfocadas en asegurar que los procesos del ciclo de vida del software y sus productos se adecuan a unos requerimientos, estándares y procedimientos de seguridad establecidos en las organizaciones.

OBJETIVO GENERAL

Brindar el conocimiento para en distintas metodologías y técnicas emergentes orientadas a mejorar el control de las Tecnologías de la información, como frameworks para desarrollo de software seguro, Informática forense y técnicas y herramientas de soporte para prevención y gestión de amenazas en TI.

OBJETIVOS PARTICULARES

- Dominar temas avanzados en aseguramiento
- Conocer frameworks para desarrollo de software seguro
- Conocer la relación e importancia entre calidad y seguridad en el desarrollo de software seguro
- Desarrollar habilidades para el uso de métodos y prácticas para el desarrollo de software seguro
- Desarrollar habilidades en temas relacionados con establecimiento de control en sistemas e informática forense
- Desarrollar habilidades para el aseguramiento de TICs mediante el uso de herramientas especializadas

TEMARIO

1. Frameworks para desarrollo de software seguro
2. Calidad y seguridad del software

    1.1 Calidad y Seguridad.
    1.2 El nuevo ciclo de vida de desarrollo del software orientado a la seguridad.
    1.3 Los requisitos de software y la seguridad
    1.4 La gestión del riesgo durante el desarrollo del software
    1.5 Las pruebas de seguridad del software
    1.6 Plan de calidad del software seguro
3. Auditoría Informática
    3.1 El marco de objetivos de control CobiT
    3.2 Conceptos de Informática Forense
    3.3 Nuevas tendencias
4. Laboratorio de seguridad Informática

BIBLIOGRAFÍA

No.	Título	Autor	Editorial	Año
1	CERT Resilience Management Model	Richard A. Caralli; Julia H. Allen; David W. White	Adison-Wesley	2011
2	The Web Application Hacker's Handbook: Finding and Exploiting Security Flaws (2 edition)	Stuttard, Dafydd,Pinto, Marcus	Wiley	2011
3	Software Vulnerability: Identification and Minimization	Alka Agrawal, Raees A Khan	Scholars' Press	2014
4	The Hacker Playbook: Practical Guide To Penetration Testing	Kim, Peter	CreateSpace Independent Publishing Platform	2014
5	The Database Hacker's Handbook: Defending Database Servers	Litchfield, David,Anley, Chris,Heasman, John,Grindlay, Bill	Wiley	2005

6	Estándares ISO 27000 27001 y 27002			
NOTA: La materia se apoyará con el uso de artículo científicos relacionados con los temas, por lo tanto, el docente y el alumno pueden hacer uso de la biblioteca digital http://www.cimat.mx/es/Catalogos_Servicios_en_Linea la cual pueden acceder utilizando su correo institucional, utilizando su cuenta y contraseña.				

EVALUACIÓN

ASPECTO A EVALUAR	PORCENTAJE
Asistencia (al menos 90% de las clases)	5%
Trabajos y exposiciones	20%
Prácticas	25%
Proyecto Final	50%