1. Datos Generales de la asignatura

Nombre de la asignatura:	Seguridad en la web.
Clave de la asignatura:	STD-1902.
SATCA[1]:	2-3-5
Carrera:	Ingeniería en Sistemas Computacionales

2. Presentación

Caracterización de la asignatura
Esta asignatura forma parte de la especialidad de Seguridad en las Tecnologías de la Información y Comunicaciones. Debido al auge en el desarrollo web y su utilización a nivel mundial, es imperativo contar con los conocimientos necesarios, para que aquel que se dedique al desarrollo de aplicaciones Web proporcione a sus aplicaciones las características actualmente deseadas por las empresas que publican sitios Web como son: la confidencialidad, confiabilidad e integridad en el manejo de su información.
Intención didáctica
Este curso se encuentra divido en cinco unidades temáticas. En la primera unidad se encuentran los conceptos básicos, tanto fundamentales como los términos asociados a la seguridad Web, para que el alumno entienda el lenguaje asociado a la seguridad informática. En la segunda unidad se presenta al alumno como puede realizar un análisis sistemático de riesgos, y las técnicas de salvaguarda que deberá utilizar en la programación web. En la tercera unidad el alumno aprenderá de las técnicas necesarias para contrarrestar los errores de programación Web que crean vulnerabilidades. En la cuarta unidad el alumno aprenderá algunas de las estrategias y métodos más comunes para realizar una aplicación Web con la seguridad apropiada a la misma. En la quinta unidad el alumno aprenderá algunas de las herramientas y técnicas adicionales para garantizar una protección adecuada.

[1] Sistema de Asignación y Transferencia de Créditos Académicos

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Instituto Tecnológico Superior de Coatzacoalcos Noviembre 2018	H. Academia de Sistemas	Reunión de especialidad

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
Aplicar los paradigmas, técnicas y herramientas emergentes más utilizadas para establecimiento de la Seguridad dentro de la programación Web, para el desarrollo de aplicaciones Web seguras y confiables.

5. Competencias previas

Identificar la tecnología de la computación a través de las arquitecturas de diferentes modelos y desarrollar habilidades que le permitan sugerir soluciones óptimas utilizando los sistemas de cómputo.

Diseñar e implementar objetos de programación que permitan resolver situaciones reales y de ingeniería.

Diseñar e implementar aplicaciones Web que permitan resolver situaciones reales y de ingeniería.

6. Temario

No.	Temas	Subtemas
1	Introducción a la seguridad Web	1.1 Las fallas más comunes de seguridad en los sistemas de cómputo. 1.2 Políticas de Seguridad Informática.
2	Técnicas de análisis y tratamiento de riesgo.	2.1 Análisis de amenazas 2.2 Análisis de Activos 2.3 Análisis de Riesgos 2.4 Riesgo Residual y Salvaguardas
3	Puntos débiles en Seguridad Web.	3.1 Scripts 3.2 Http 3.3 Ingeniería Social 3.4 Ruteadores

4	Procedimientos para una programación segura.	4.1 J2EE Security Model 4.2 Autenticación en Servidores Web
5	Técnicas adicionales para protección.	5.1 Seguridad en instalaciones. 5.2 Seguridad en los usuarios. 5.3 Seguridad en los equipos.

7. Actividades de aprendizaje de los temas

1. Introducción a la seguridad Web	
Competencias	Actividades de aprendizaje
Específica(s) • Comprenda las necesidades, principios y definiciones inherentes a la seguridad en el desarrollo de aplicaciones Web. Genéricas: • Capacidad de comunicación oral y escrita. • Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. • Capacidad de trabajo en equipo. • Habilidad para trabajar en forma autónoma.	• Investiga las actividades que incluye la seguridad en los sistemas de cómputo en general tanto de un aspecto físico, incluyendo instalaciones, no sólo equipos, así como lo referente a los distintos esquemas de software. • Elaborar un reporte que sea una evidencia de aprendizaje de la investigación realizada.
2. Técnicas de análisis y tratamiento de riesgo.	
Competencias	Actividades de aprendizaje
Específica(s): • Comprende las Técnicas de análisis de riesgos. • Desarrolla actividades para el tratamiento de errores. Genéricas: • Capacidad de abstracción, análisis y síntesis • Capacidad de aplicar los conocimientos en la práctica • Capacidad de comunicación oral y escrita	• Conocer las distintas técnicas de análisis y tratamiento de errores. • Investigar los requerimientos para la utilización de algunas de las técnicas y tratamientos de errores. Entrega una evidencia de aprendizaje. • Realizar una práctica en la que aplique una de las técnicas de tratamientos de errores.

• Habilidades para buscar, procesar y analizar información procedente de fuentes diversas • Capacidad para identificar, plantear y resolver problemas • Capacidad para tomar decisiones • Capacidad de trabajo en equipo • Habilidad para trabajar en forma autónoma	
3. Puntos débiles en Seguridad Web.	
Competencias	Actividades de aprendizaje
Específica(s): • Conocer y Comprender las prácticas en el desarrollo de aplicaciones Web que originan huecos en la seguridad. Genéricas: • Capacidad de abstracción, análisis y síntesis • Capacidad de aplicar los conocimientos en la práctica • Capacidad de comunicación oral y escrita • Habilidades para buscar, procesar y analizar información procedente de fuentes diversas • Capacidad para identificar, plantear y resolver problemas • Capacidad para tomar decisiones • Capacidad de trabajo en equipo • Habilidad para trabajar en forma autónoma	• El docente expone cómo son por malas prácticas de programación los puntos débiles en la Seguridad Web. • El estudiante elabora prácticas correspondientes.
4. Procedimientos para una programación segura.	
Competencias	Actividades de aprendizaje
Específica(s): • Conocer y comprender el Modelo de Seguridad de J2EE.	• El docente expone el Modelo de Seguridad de J2EE. • El estudiante elabora prácticas que sirvan de ejemplos de dicho modelo y

• Conocer y comprender el establecimiento de procedimientos adecuados para la autentificación en servidores. Genéricas: • Capacidad de abstracción, análisis y síntesis • Capacidad de aplicar los conocimientos en la práctica • Capacidad de comunicación oral y escrita • Habilidades para buscar, procesar y analizar información procedente de fuentes diversas • Capacidad para identificar, plantear y resolver problemas • Capacidad para tomar decisiones • Capacidad de trabajo en equipo • Habilidad para trabajar en forma autónoma	entrega reportes de las mismas. • Investigar los procedimientos de autenticación para por lo menos dos diferentes tipos de servidores Web • El estudiante elabora una práctica de autenticación en un servidor en particular y entrega reporte.
5. Técnicas adicionales para protección.	
Competencias	Actividades de aprendizaje
Específica(s): • Conocer y comprender, las políticas utilizadas en las instalaciones de equipos de cómputo para mejorar la seguridad. • Conocer algunas de las estrategias implementadas en los equipos de cómputo para mejorar la seguridad. • Conocer, comprender e implementar las prácticas que refuerzan la seguridad con los usuarios de sistemas Web. Genéricas: • Habilidad para buscar y analizar información proveniente de fuentes diversas. • Toma de decisiones.	• El docente expone en clase los subtemas • El estudiante realiza un y entrega un ensayo como evidencia de aprendizaje. • El estudiante realiza una investigación documental (de textos en inglés), más a fondo sobre alguno de los subtemas expuestos, para lo cual deberá escribir y entregar un artículo de 5 cuadrillas.

• Trabajo en equipo • Capacidad de aplicar los conocimientos en la práctica	

8. Práctica(s)

Tema 2 Aplicar una de las técnicas de tratamiento de errores. Tema 3 Demostrar los errores en los scripts que ocasionan fallas en la seguridad. Tema 4 Crear un esquema de autenticación con roles en un servidor Web. Crear una aplicación que implemente el modelo de seguridad de J2EE

9. Proyecto de asignatura

Dado que en el programa se realizan únicamente prácticas sueltas de cada tema no se requiere de un proyecto integrador.

10. Evaluación por competencias

La evaluación debe es continua. Se hacen evaluaciones formativas El portafolio de evidencias constará de: Reportes escritos de investigación Reporte de prácticas

11. Fuentes de información

1. Hacking Exposed Web Applications, Joel Scambray and Mike Shema,McGraw-Hill/Osborne © 2002
2. ImprovingWebApplicationSecurity:ThreatsandCountermeasures,Microsoft Corporation , Microsoft Press © 2003
3. Auditing Web Applications, Nilesh Chaudhari, McGraw-Hill/Osborne © 2002
4. Information Security Practice and Experience, Kefei Chen, Springer
5. Network Security Tools, Nitesh Dhanjani, Justin Clarke, O'Really
6. TheArtofSoftwareSecurityTesting:IdentifyingSoftwareSecurityFlaws,Chris Wysopal, Lucas Nelson, Elfriede Dustin, Dino Dai Zovi, Pearson Education.
7. Application Level Security Management, Michael Neuhaus, Diplomarbeiten Agentur.

.