

<b>1. Datos de la asignatura.</b>	
<b>Nombre de la asignatura:</b>	<b>Seguridad en la Web</b>
<b>Carrera:</b>	<b>Ingeniería en Sistemas Computacionales</b>
<b>Clave de la asignatura:</b>	<b>STD-1402</b>
<b>SATCA</b>	<b>2-3-5</b>

<b>2. Presentación.</b>
<b>Caracterización de la asignatura.</b>
<p>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.</p>
<b>Intención didáctica.</b>
<p>Este curso se encuentra dividido en cinco unidades temáticas.</p> <p>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.</p> <p>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.</p> <p>En la tercera unidad el alumno aprenderá de las técnicas necesarias para contrarrestar los errores de programación Web que crean vulnerabilidades.</p> <p>En la cuarta unidad el alumna aprenderá algunas de las estrategias y métodos más comunes para realizar una aplicación Web con la seguridad apropiada a la misma.</p> <p>En la quinta unidad el alumno aprenderá algunas de las herramientas y técnicas adicionales para garantizar una protección adecuada.</p>

### 3. Participantes en el diseño y seguimiento curricular del programa

Lugar y Fecha de elaboración o revisión	Participantes	Observaciones
Instituto Tecnológico de Toluca. Enero de 2014	Profesores de la especialidad de Seguridad en Tics.  M en C Martha Escamilla Zepeda Ing. Eugenio Falcón Insunza Ing. Rosa Elvira Moreno Lic. María Luisa Gómez Santamarina Dra. Ana Lilia Sosa Albarrán M en C Imelda Vertti Guzmán	Surge la elaboración de este programa en esta fecha. Por necesidades de la creación de una nueva especialidad llamada Seguridad e las Tics, para mantener el conocimiento de los alumnos lo más actualizado posible.

### 4. Competencias a desarrollar

Competencia general 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.
Competencias Genéricas:
1.- Competencias instrumentales: <ul style="list-style-type: none"><li>• Capacidad de análisis y síntesis</li><li>• Capacidad de organizar y planificar</li><li>• Conocimientos generales básicos</li><li>• Conocimientos especializados de la carrera</li><li>• Comunicación oral y escrita en su propia lengua</li><li>• Habilidades básicas de manejo de la computadora y lenguajes de programación</li><li>• Habilidades de gestión de información(habilidad para buscar y analizar información proveniente de fuentes diversas</li><li>• Solución de problemas</li></ul>

- Toma de decisiones.

2.- Competencias interpersonales:

- Capacidad de trabajar en equipo
- Capacidad crítica
- Aplicar a esta materia las competencias comunes de compromiso con el trabajo

3-Competencias sistémicas:

- Capacidad de aplicar los conocimientos en la práctica
- Habilidades de investigación
- Capacidad de aprender
- Capacidad de adaptarse a nuevas situaciones
- Capacidad de generar nuevas ideas (creatividad)
- Liderazgo
- Habilidad para trabajar en forma autónoma

**Competencias específicas.**

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 de otras asignaturas**

**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**

Temas		Subtemas
No.	Nombre	

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

Competencia específica y genéricas (a desarrollar y fortalecer por tema)	
<p><i>Competencia específica:</i></p> <ul style="list-style-type: none"> <li>Comprenda las necesidades, principios y definiciones inherentes a la seguridad en el desarrollo de aplicaciones Web.</li> </ul> <p><i>Competencias genéricas:</i></p> <ul style="list-style-type: none"> <li>Capacidad de comunicación oral y escrita</li> <li>Habilidades para buscar, procesar y analizar información procedente de fuentes diversas</li> <li>Capacidad de trabajo en equipo</li> <li>Habilidad para trabajar en forma autónoma</li> </ul>	
<b>Tema 1</b>	<b>Actividades de aprendizaje</b>
Introducción a la seguridad Web	<ul style="list-style-type: none"> <li>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.</li> </ul>

	<ul style="list-style-type: none"> <li>• Elaborar un reporte que sea una evidencia de aprendizaje de la investigación realizada.</li> </ul>
<p>Competencia específica y genéricas (a desarrollar y fortalecer por tema)</p>	
<p><i>Competencias específicas:</i></p> <ul style="list-style-type: none"> <li>• Comprende las Técnicas de análisis de riesgos.</li> <li>• Desarrolla actividades para el tratamiento de errores.</li> </ul> <p><i>Competencias genéricas:</i></p> <ul style="list-style-type: none"> <li>• Capacidad de abstracción, análisis y síntesis</li> <li>• Capacidad de aplicar los conocimientos en la práctica</li> <li>• Capacidad de comunicación oral y escrita</li> <li>• Habilidades para buscar, procesar y analizar información procedente de fuentes diversas</li> <li>• Capacidad para identificar, plantear y resolver problemas</li> <li>• Capacidad para tomar decisiones</li> <li>• Capacidad de trabajo en equipo</li> <li>• Habilidad para trabajar en forma autónoma</li> </ul>	
<p>Tema 2</p>	<p>Actividades de aprendizaje</p>
<ul style="list-style-type: none"> <li>• Técnicas de análisis y tratamiento de riesgo.</li> </ul>	<ul style="list-style-type: none"> <li>• Conocer las distintas técnicas de análisis y tratamiento de errores.</li> <li>• Investigar los requerimientos para la utilización de algunas de las técnicas y tratamientos de errores. Entrega una evidencia de aprendizaje.</li> <li>• Realizar una práctica en la que aplique una de las técnicas de tratamientos de errores.</li> </ul>
<p>Competencia específica y genéricas (a desarrollar y fortalecer por tema)</p>	
<p><i>Competencias específicas:</i></p> <ul style="list-style-type: none"> <li>• Conocer y Comprender las prácticas en el desarrollo de aplicaciones Web que originan huecos en la seguridad.</li> </ul> <p><i>Competencias Genéricas:</i></p> <ul style="list-style-type: none"> <li>• Capacidad de abstracción, análisis y síntesis</li> <li>• Capacidad de aplicar los conocimientos en la práctica</li> <li>• Capacidad de comunicación oral y escrita</li> <li>• Habilidades para buscar, procesar y analizar información procedente de fuentes diversas</li> <li>• Capacidad para identificar, plantear y resolver problemas</li> </ul>	

<ul style="list-style-type: none"> <li>• Capacidad para tomar decisiones</li> <li>• Capacidad de trabajo en equipo</li> <li>• Habilidad para trabajar en forma autónoma</li> </ul>	
Tema 3	Actividades de aprendizaje
Puntos débiles en Seguridad Web.	<p>El docente expone cómo son por malas prácticas de programación los puntos débiles en la Seguridad Web.</p> <p>El estudiante elabora prácticas correspondientes.</p>
Competencia específica y genéricas (a desarrollar y fortalecer por tema)	
<p><i>Competencia específica:</i></p> <ul style="list-style-type: none"> <li>• Conocer y comprender el Modelo de Seguridad de J2EE.</li> <li>• Conocer y comprender el establecimiento de procedimientos adecuados para la autenticación en servidores.</li> </ul> <p><i>Competencias Genéricas:</i></p> <ul style="list-style-type: none"> <li>• Capacidad de abstracción, análisis y síntesis</li> <li>• Capacidad de aplicar los conocimientos en la práctica</li> <li>• Capacidad de comunicación oral y escrita</li> <li>• Habilidades para buscar, procesar y analizar información procedente de fuentes diversas</li> <li>• Capacidad para identificar, plantear y resolver problemas</li> <li>• Capacidad para tomar decisiones</li> <li>• Capacidad de trabajo en equipo</li> <li>• Habilidad para trabajar en forma autónoma</li> </ul>	
Tema 4	Actividades de aprendizaje
Procedimientos para una programación segura.	<ul style="list-style-type: none"> <li>• El docente expone el Modelo de Seguridad de J2EE.</li> <li>• El estudiante elabora prácticas que sirvan de ejemplos de dicho modelo y entrega reportes de las mismas.</li> <li>• Investigar los procedimientos de autenticación para por lo menos dos diferentes tipos de servidores Web</li> <li>• El estudiante elabora una práctica de autenticación en un servidor en particular y entrega reporte.</li> </ul>
Competencia específica y genéricas (a desarrollar y fortalecer por tema)	
<i>Competencia Específica</i>	

- 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.

*Competencias Genéricas:*

- Habilidad para buscar y analizar información proveniente de fuentes diversas.
- Toma de decisiones.
- Trabajo en equipo
- Capacidad de aplicar los conocimientos en la práctica

Tema 5	Actividades de aprendizaje
Técnicas adicionales para protección.	<ul style="list-style-type: none"> <li>• El docente expone en clase los subtemas.</li> <li>• El estudiante realiza un y entrega un ensayo como evidencia de aprendizaje.</li> <li>• 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.</li> </ul>

**8. Prácticas (para fortalecer las competencias de los temas y de la asignatura)**

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 integrador (Para fortalecer las competencias de la asignatura con otras asignaturas de la especialidad)**

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

#### **10.- Evaluación por competencias (específicas y genéricas de la asignatura)**

La evaluación debe ser 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. Improving Web Application Security: Threats and Countermeasures, 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. The Art of Software Security Testing: Identifying Software Security Flaws, Chris Wysopal, Lucas Nelson, Elfriede Dustin, Dino Dai Zovi, Pearson Education.
7. Application Level Security Management, Michael Neuhaus, Diplomarbeiten Agentur.