1. Datos Generales de la asignatura

Nombre de la asignatura:	**Seguridad en Aplicaciones Web y Móvil**
Clave de la asignatura:	**TTD-1605**
SATCA[1]:	**2-3-5**
Carrera:	**Ingeniería en Sistemas Computacionales**

2. Presentación

Caracterización de la asignatura
La tendencia en el uso de dispositivos móviles presenta un campo que debe aprovecharse, sin descuidar el aspecto de la seguridad que debe ir implícita. Esta asignatura aporta al perfil del egresado la capacidad para desarrollar aplicaciones seguras para plataforma web y dispositivos móviles.
Intención didáctica
La asignatura cubre la necesidad que tiene el ingeniero al enfrentarse a la forma de intercambiar información a través de dispositivos móviles y en particular a la seguridad de las aplicaciones. La unidad 1 introduce al estudiante a conocer los conceptos básicos de seguridad y requerimientos para las aplicaciones mediante el uso normas y estándares. La unidad 2 aborda la seguridad que se debe tener en las aplicaciones desarrolladas del lado del cliente, del servidor y la comunicación. La unidad 3 se enfoca a implementar la seguridad en las aplicaciones desarrolladas en ambiente web. La unidad 4 se enfoca a implementar la seguridad en las aplicaciones desarrolladas para dispositivos móviles. El enfoque sugerido para la materia requiere que las actividades de aprendizaje construyan en el estudiante las competencias pertinentes sobre el manejo de las

[1] Sistema de Asignación y Transferencia de Créditos Académicos

herramientas de desarrollo web. En las actividades prácticas sugeridas, es conveniente que el profesor guíe a los estudiantes en el desarrollo de un proyecto integrador de la materia, mismo que deberá reflejar la solución a un caso real.

3. Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Lerma, Campeche del Instituto Tecnológico de Campeche del 2 al 18 de mayo de 2016	Academia de Sistemas y Computación del Instituto Tecnológico de Campeche	Definición de la Especialidad para la carrera de Ingeniería en Sistemas Computacionales

4. Competencia(s) a desarrollar

Competencia(s) específica(s) de la asignatura
Identifica las principales estrategias y tipos de ataques a dispositivos móviles y web para desarrollar y utilizar los diferentes modelos, herramientas y mecanismos de protección ante las vulnerabilidades y mantener un sistema confiable.

5. Competencias previas

- Analizar problemas y diseño de algoritmos.
- Desarrollar aplicaciones con programación estructurada y programación orientada a objetos.
- Instalar y usar diferentes sistemas operativos.
- Manejar el internet.

6. Temario

No.	Temas	Subtemas
1	Introducción a la Seguridad	1.1. Definición de Seguridad Informática 1.1.1. Conceptos básicos 1.1.2. Visión Global de la Seguridad 1.2. Análisis de Requerimientos de Seguridad 1.2.1. Amenazas 1.2.2. Vulnerabilidades 1.2.3. Riesgos 1.2.4. Servicios y Mecanismo de Seguridad 1.3. Identificación de las principales Normas, Protocolos y Estándares en Seguridad 1.3.1. Norma ISO 27001 1.3.2. ISACA 1.3.3. IEEE / ANSI / OWASP 1.3.4. SSL/TLS., HTTP sobre SSL (HTTPS), SET, IPSec. 1.4. Técnicas para el manejo de la Seguridad. 1.4.1. Hacking Ético 1.4.2. Computo Forense 1.4.3. Criptografía y Esteganografía 1.4.4. Firma Electrónica 1.4.5. Certificado Digital
2	Seguridad en el cliente, servidor, aplicaciones y comunicación	2.1 Seguridad en el Cliente 2.1.1 Código móvil 2.1.2 Lenguajes de Macro: VBA 2.1.3 Lenguajes de Script: JavaScript y VBScript 2.1.4 Applets Java 2.1.5 Controles ActiveX 2.2 Seguridad en el Servidor 2.2.1 Servidor Web

		2.2.2 Servidor de Bases de Datos 2.2.3 Lenguajes de servidor 2.3 Seguridad en la Aplicación 2.3.1 Control de acceso 2.3.2 Validación de datos de entrada 2.2. 4Programación segura 2.4 Seguridad en la Comunicación 2.4.1 5SSL
3	Seguridad en Aplicaciones WEB	3.1 Aplicaciones web seguras 3.1.1 identificando perfiles de aplicaciones. 3.1.2 Ataques a aplicaciones conocidas. 3.1.3 Programación segura 3.1.4 Fallos y errores de programación 3.2 Seguridad en la programación del lado del servidor. 3.2.1 Programación segura con CGI, API e ISAPI 3.2.2 Seguridad en ASP.net 3.2.3 Seguridad en Java 3.2.3 Seguridad en PHP 3.3 Servidores web seguros 3.3.1 Identificando perfiles de servidores. 3.3.2 Ataques a servidores web, al servicio de HTTP o a otros servicios disponibles. 3.3.3 Estrategias de control de acceso al servidor. 3.3.4 Control de acceso por URL oculto. 3.3.5 Control de acceso por dirección IP, nombre de host y dominio. 3.3.6 Control de acceso por nombre de usuario y contraseña.

		3.4 Instalación y configuración segura de servidores. 3.5 Caso práctico: Servidor Web Apache.
4	Seguridad en Dispositivos Móviles	4.1 Introducción Android, versiones, Infraestructura y conocimientos de los APK 4.1.1 Introducción sobre Android 4.1.2 Reconocimiento de S.O 4.1.3 Medidas de seguridad en dispositivos 4.1.4 Reconocimiento de herramientas de auditorías inalámbricas 4.1.5 Recomendaciones de seguridad 4.2 Metodologías de aplicación de seguridad en móviles 4.2.1 Uso correcto y buena implementación en las corporaciones 4.2.3 Políticas específicas de implementación 4.2.4 Políticas adicionales 4.3 Configuración y herramientas complementarias 4.3.1 Testeo de las mejores tools de seguridad 4.3.2 Uso de herramientas en función a la seguridad y conexión 4.4 Introducción IOS, versiones, Infraestructura y conocimientos 4.4.1 Introducción sobre IOS 4.4.2 Reconocimiento de S.O 4.4.3 Medidas de seguridad en dispositivos (Iphone – Ipad) 4.4.4 Reconocimiento de herramientas de auditorías inalámbricas

		4.5 Introducción a Windows Phone, Symbian y sistemas nativos 4.5.1 Introducción sobre los sistemas operativos 4.5.2 Reconocimiento de la estructura 4.5.3 Medidas de seguridad en dispositivos 4.5.5 Reconocimiento de herramientas de auditorías inalámbricas

7. Actividades de aprendizaje de los temas

Nombre de tema	
Competencias	Actividades de aprendizaje
Específica(s): **Identificar los principales elementos en la Seguridad Informática que permitan identificar y minimizar los riesgos a los activos de una organización evitando la denegación de servicio.** Genéricas: 1.Capacidad de abstracción, análisis y síntesis. 2.Capacidad de aplicar los conocimientos en la práctica. 3.Capacidad de comunicación oral y escrita. 4. Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. 5.Capacidad para tomar decisiones. 6. Valoración y respeto por la diversidad y multiculturalidad 7.Capacidad para formular y gestionar proyectos. 8.Compromiso ético. 9.Compromiso con la calidad.	● Buscar y seleccionar información sobre seguridad en aplicaciones ● Buscar, seleccionar y comentar sobre las normas y estándares de seguridad en el desarrollo de aplicaciones web y móviles ● Realizar un análisis de requerimientos de seguridad en el desarrollo de las aplicaciones web y móvil ● Buscar y seleccionar las técnicas de manejo de seguridad en el desarrollo de aplicaciones web y móviles
Nombre de tema	
Competencias	Actividades de aprendizaje
Específica(s):	● Busca, selecciona y comenta los

identifica los principales riesgos y amenazas del lado del cliente, del servidor, aplicaciones web y móviles, y las comunicaciones para el uso de herramientas y mecanismos de seguridad Genéricas: 1.Capacidad de abstracción, análisis y síntesis. 2.Capacidad de aplicar los conocimientos en la práctica. 3.Capacidad de comunicación oral y escrita. 4. Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. 5.Capacidad para tomar decisiones. 6. Valoración y respeto por la diversidad y multiculturalidad 7.Capacidad para formular y gestionar proyectos. 8.Compromiso ético. 9.Compromiso con la calidad.	riesgos de las aplicaciones desarrolladas por el lado del cliente y las aplicaciones web y móviles ● Busca, selecciona y comenta el top-ten de las amenazas de las aplicaciones desarrolladas por el lado del cliente y las aplicaciones web y móviles ● Busca y experimenta vulnerabilidades de aplicaciones desarrolladas previamente en ambientes web y móvil ● Busca y experimenta herramientas que permitan la detección de amenazas de seguridad en ambientes web y móviles
Nombre de tema	
Competencias	Actividades de aprendizaje
Específica(s): **Implementación de esquemas de seguridad para aplicaciones y servidores Web desarrollando casos prácticos de ataques y denegación de servicios.** Genéricas:	● Realiza el análisis de una aplicación web para identificar sus vulnerabilidades ● Realiza una propuesta de solución para mitigar las vulnerabilidades de aplicaciones web ● Implementa mecanismos de seguridad en aplicaciones web

1.Capacidad de abstracción, análisis y síntesis. 2.Capacidad de aplicar los conocimientos en la práctica. 3.Capacidad de comunicación oral y escrita. 4. Habilidades para buscar, procesar y analizar información procedente de fuentes diversas. 5.Capacidad para tomar decisiones. 6. Valoración y respeto por la diversidad y multiculturalidad 7.Capacidad para formular y gestionar proyectos. 8.Compromiso ético. 9.Compromiso con la calidad.	
Competencias	Actividades de aprendizaje
Específica(s): **Implementación de esquemas de seguridad para aplicaciones y dispositivos móviles desarrollando casos prácticos de ataques y denegación de servicios.** Genéricas: 1.Capacidad de abstracción, análisis y síntesis. 2.Capacidad de aplicar los conocimientos en la práctica. 3.Capacidad de comunicación oral y escrita. 4. Habilidades para buscar, procesar y analizar información procedente de fuentes diversas.	● Realiza el análisis de una aplicación móviles para identificar sus vulnerabilidades ● Realiza una propuesta de solución para mitigar las vulnerabilidades de aplicaciones móviles ● Implementa mecanismos de seguridad en aplicaciones móviles

5.Capacidad para tomar decisiones. 6. Valoración y respeto por la diversidad y multiculturalidad 7.Capacidad para formular y gestionar proyectos. 8.Compromiso ético. 9.Compromiso con la calidad.	

8. Práctica(s)

Práctica 1: Seguridad en el cliente "Código móvil"
- Creación de un formulario
- Validación de datos con JavaScript
- Formas de saltarse la validación JavaScript

Práctica 2: Seguridad en el servidor "Autenticación HTTP básica"
- Creación de una página web
- Creación de un usuario
- Creación de un fichero .htaccess
- Configuración del servidor web Apache

Práctica 3 Control de acceso
- Diseñar un mecanismo de control de acceso
- Definir usuarios
- Especificar nivel de acceso de los usuarios

Práctica 4: Validación de datos
- Validación de datos en el servidor
- Creación de un formulario en PHP con validación de los datos de entrada
- Uso de expresiones regulares para validar los datos de entrada

Práctica 5: SSL en Apache
- Creación de un certificado digital
- Configuración de Apache para utilizar el certificado en una conexión SSL

9. Proyecto de asignatura

El objetivo del proyecto que plantee el docente que imparta esta asignatura, es demostrar el desarrollo y alcance de la(s) competencia(s) de la asignatura, considerando las siguientes fases:

- **Fundamentación:** Se recomienda el uso de:
  - Referencia de Escritorio en Seguridad de Aplicaciones de OWASP
  - Guía de Desarrollo de OWASP
  - Guía de Pruebas de OWASP
  - La Guía de Revisión de Código de OWASP.

  Con el fin de que los estudiantes logran la comprensión de la realidad o situación que presentan las aplicaciones desarrolladas, las cuales cuidan la funcionalidad descuidando el aspecto de seguridad

- **Planeación:** Llevar a cabo el diagnóstico de vulnerabilidades de las aplicaciones web y móviles y hacer una lista y cronograma de las actividades a realizar para mitigar los problemas de este tipo de aplicaciones

- **Ejecución:** Llevar a cabo las actividades planteadas en la fase de planeación con el fin de aplicar los conocimientos adquiridos en las guías de mejores prácticas en el desarrollo de aplicaciones web y móviles.

- **Evaluación:** Entrega del documento del proyecto, así como las aplicaciones desarrolladas considerando el aspecto funcional y de seguridad de la aplicación, sometida a diversas pruebas de diagnóstico e identificación de vulnerabilidades.

10. Evaluación por competencias

Las técnicas, instrumentos y herramientas sugeridas para constatar los desempeños académicos de las actividades de aprendizaje.

Las técnicas, herramientas y/o instrumentos sugeridos que permiten obtener el producto del desarrollo las actividades de aprendizaje: mapas conceptuales, reportes de prácticas, estudios de casos, exposiciones en clase, ensayos, problemas, reportes de visitas, portafolio de evidencias, exámenes, proyecto de asignatura o integrador y cuestionarios.

Las técnicas, herramientas y/o instrumentos sugeridos que me permite constatar el logro o desempeño de las competencias del estudiante: listas de cotejo, listas de verificación, matrices de valoración, guías de observación, coevaluación y autoevaluación

Evaluación diagnóstica con el fin de conocer la disposición del alumno para aprender y el nivel de los conocimientos previos necesarios para el desarrollo de los nuevos aprendizajes.
Establecer junto con los alumnos, el porcentaje de las diferentes actividades del curso.
Participación en clase.
Participación en los talleres.
Presentación y calidad de los ensayos, informes de investigación y trabajos relacionados.
Participación en las dinámicas grupales.
Resolución de casos prácticos.
Conclusiones y resúmenes de estudio.
Presentaciones de las investigaciones encomendadas
Proyecto integrador.

11. Fuentes de información

1. Adrian Wiesmann, Andrew van der , Stock Mark ,Curphey Ray Stirbei , Guía OWASP 3.0 (Español), Free Software Foundation
2. Caballero Gil, Pino, *Seguridad informática: técnicas criptográficas.*México, D.F., Alfaomega
3. Gratton, Pierre, *Protección informática: en datos y programas; en gestión y operación; en equipos y redes; en Internet* México, Trillas 1998,
4. Referencia de Escritorio en Seguridad de Aplicaciones de OWASP (OWASP Application Security Desk Reference).2002-2008, Free Software Foundation
5. Guía de Desarrollo de OWASP, Free Software Foundation
6. Guía de Pruebas de OWASP, Free Software Foundation

7. La Guía de Revisión de Código de OWASP, Free Software Foundation